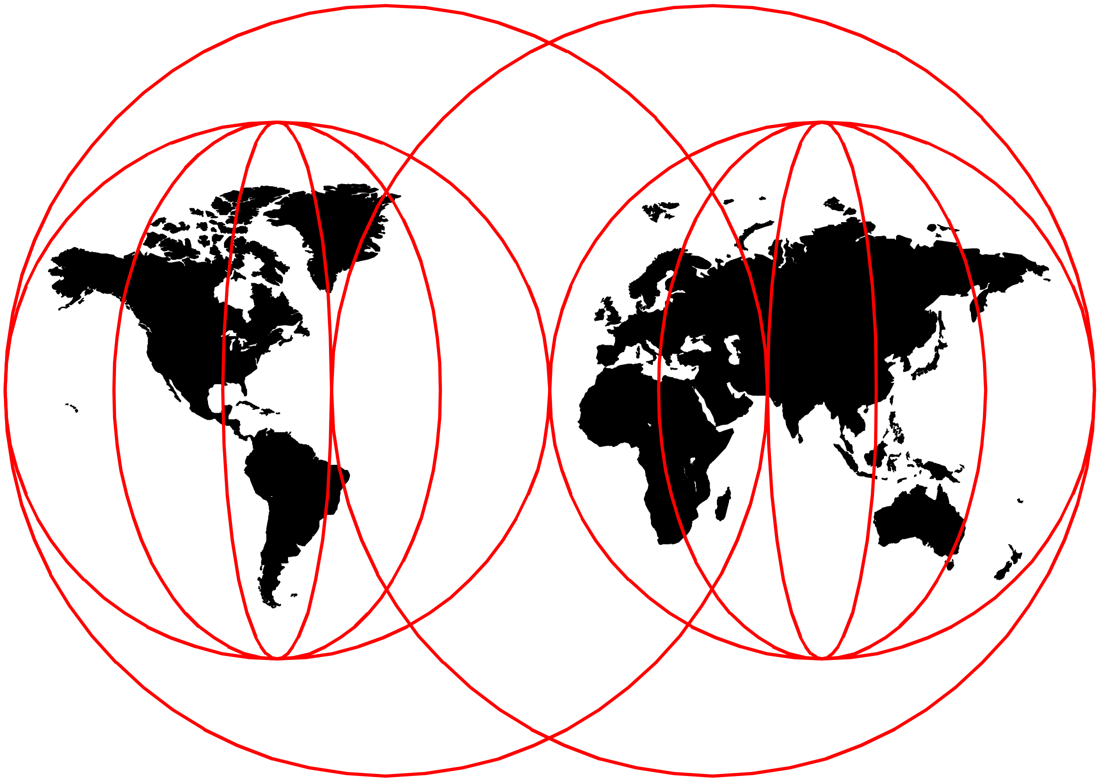
A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions

Martin W. Murhammer, Hyun Jeong Lee, Alexander Schmid
Orcun Atakan, Zikrun Badri, Beom Jun Cho



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5234-01

International Technical Support Organization

SG24-5234-01

A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions

November 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, "Special notices" on page 593.

Second Edition (November 1999)

This edition applies to Nways Multiprotocol Routing Services (MRS), Nways Multiprotocol Access Services (MAS) and Nways Access Integration Services (AIS) Version 3.3 for use with the IBM Nways 2210, 2212 and 2216 Multiprotocol Routers.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Preface

The Internet nowadays is not only a popular vehicle to retrieve and exchange information in traditional ways, such as e-mail, file transfer and Web surfing. It is being used more and more by companies to replace their existing telecommunications infrastructure with virtual private networks by implementing secure IP tunnels across the Internet between corporate sites as well as to business partners and remote locations.

This updated redbook includes the IPSec enhancements provided by Version 3.3 of the IBM Nways Multiprotocol Routing Services (MRS), Nways Multiprotocol Access Services (MAS) and Access Integration Services (AIS) that implement the Internet Key Exchange (IKE) protocol. This redbook also includes other new features, such as the policy engine, digital certificate and LDAP support, and QoS. The VPN scenarios are enhanced to reflect the latest implementation of IPSec and L2-tunneling functionality.

In this redbook we delve further into these scenarios by showing you how to implement solutions that exploit Data Link Switching (DLSw), IP Bridging Tunnels, Enterprise Extender (HPR over IP), APPN DLUR, TN3270, and Tunneling on layer 2 (L2TP, L2F, PPTP) through an IPSec tunnel.

A working knowledge of the IPSec protocols is assumed.

How this book is organized

This redbook is Volume II in the series on virtual private networks (VPNs).

- Volume I provides the reader with an understanding of the architecture and underlying technologies, including cryptographic concepts used in IP security. It also presents VPN scenarios based on IBM solutions using manually keyed IPSec.
- This redbook (Volume II) is a practical guide for use in configuring IPSec tunnels and applications of these tunnels with IBM Nways Multiprotocol Routers.
- Volume III illustrates interoperability scenarios based upon the full range of IBM VPN platforms that currently implement IKE: OS/390, AS/400, AIX, Nways routers and IPSec clients. It also includes interoperability with a variety of OEM VPN solutions.

For the benefit of customers who are still using MAS/MRS/AIS Versions 3.1 and 3.2 and who do not plan to upgrade to Version 3.3 for the time being, we have kept the VPN scenario descriptions pertaining to those earlier versions as they have been presented in the first release of this redbook.

For the benefit of customers who decide to start with MAS/MRS/AIS Version 3.3 or who are planning on migrating to that version, we have included full descriptions of the VPN scenarios based on that new version to keep references within this redbook at a minimum.

Therefore, the structure of this redbook presents itself as follows:

1. Part I discusses VPN architectures and technologies in general.

2. Part II describes the new features of MAS/MRS/AIS Version 3.3 and discusses VPN scenarios based on that version.
3. Part III discusses VPN scenarios - essentially the same as in Part II - based on MAS/MRA/AIS Versions 3.1 and 3.2.
4. Part IV presents the steps for basic router setup using either V3.3 or V3.1/3.2 of the Nways router service code.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center. The leader of this project was Martin W. Murhammer.

Martin W. Murhammer is a Senior I/T Availability Professional at the ITSO Raleigh Center. Before joining the ITSO in 1996, he was a Systems Engineer in the Systems Service Center at IBM Austria. He has 14 years of experience in the personal computing environment including areas such as heterogeneous connectivity, server design, system recovery, and Internet solutions. He is an IBM Certified OS/2 and LAN Server Engineer and a Microsoft Certified Professional for Windows NT. Martin has co-authored a number of redbooks at the ITSO Raleigh and Austin Centers. His latest publications are *TCP/IP Tutorial and Technical Overview*, sixth Edition, GG24-3376, and *IP Network Design Guide*, Second Edition, SG24-2580.

Hyun Jeong Lee is an IT Specialist in Network Services, IBM Korea where she has been working for eight years. She has six years of experience in the networking environment. She holds a Master degree in computer sciences from Yonsei University, Korea. Her areas of expertise include network analysis, design, SI, troubleshooting.

Alexander Schmid is a Senior Consultant for Information and Technology Management with IBM Unternehmensberatung GmbH (IBM UBG) in Germany. Before joining IBM UBG he did network design and sales support within IBM Global Network. He has 10 years of experience in the networking environment including network operations, systems programming, design, architecture and consulting. He holds a degree in computer sciences from the university of Erlangen, Germany. During his studies he worked in the IBM Zurich Research Lab for several months. He is currently studying towards a degree in Master of Business Administration (MBA) at the Open University in Milton Keynes, UK.

Orcun Atakan is an IT Security Specialist in Information Systems, IBM Turkey where he has been working for four years. His areas of expertise include IP security, security implementations, Java and electronic commerce. Orcun has previously co-authored the redbook *TCP/IP Tutorial and Technical Overview,* Sixth Edition, GG24-3376.

Zikrun Badri is a Networking Systems Specialist working in IBM Australia’s Networking Systems Division. His responsibilities include initial network design, migration, implementation and ongoing support of IBM’s networking customers. He is one of IBM Australia’s Networking Division’s VPN and IP Security specialists. He has had nine years of experience with IBM, the last five with the Networking Divison. He holds a degree in Computing Studies from the Unisveristy of Canberra. His area of expertise includes the complete range of

IBM's Networking offerings, particulary IBM's campus networking offerings. He has extensive experience in ATM networks and previously co-authored the redbook *IBM 8260 As a Campus ATM Switch*, SG24-5003.

Beom Jun Cho is an IT Architect in Network Services, IBM Korea. He has eight years of experience in network SI and managed network services. His areas of expertise include network/system management system and security solution design.

Thanks to the following people for their invaluable contributions to this project:

Erol Lengerli, Carla Sadtler, Tim Kearby, Juan Rodriguez, David Watts, Michael Haley, Shawn Walsh, Tate Renner, Linda Robinson, Gail Christensen
International Technical Support Organization, Raleigh Center

Skip Both, Bruce Dillon, John Crawbuck, Don Grosser, Christophe Henrion, Joseph Kerr, Phuong Nguyen, Leo Temoshenko, Mike Zibaie
IBM Research Triangle Park

Stephan Imhof
IBM Switzerland

John Alling, Jim Alumbaugh, Peter Fritz, Ulrich Hamm
Cisco Systems

Bill Moore, Ed Irvine, Jim Pickering
Network TeleSystems

Titus Peedikayil
RouterWare

Tim Kearby, Steven Boelaars, C. Steven Lingafelt, Kacir Samra
Authors of the first edition of this redbook

Andy Arrowood, Jason Cornpropst, Ellen Cybrybski, Bruce Dillon, Tamas Gaidosch, Luke Gibbons, Don Grosser, Charles Kunzinger, Lynda Linney, Garth Madella, Martin Murhammer, Laura Rademacher, Cliff Wang, Andreas Weinfurter
Contributors to the first edition of this redbook

Comments welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in "ITSO Redbook evaluation" on page 623 to the fax number shown on the form.
- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Send your comments in an Internet note to `redbook@us.ibm.com`

Part 1. Virtual private networks (VPNs) overview

Chapter 1. Virtual private network (VPN) introduction

This chapter provides an overview of the most important technologies employed to build VPNs today and emphasizes those used across the IBM product portfolio. The descriptions and explanations given in this chapter are based on the latest available standards for the discussed protocols and solutions and thus provide a valuable refresh and an update to existing VPN publications that are referenced as appropriate.

1.1 What is a VPN? A quick review

A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 1 on page 4.

It will help you to understand the concepts discussed in this redbook to summarize and return to the basic concepts that distinguish VPNs from other components of a networking infrastructure as well as from mere application security solutions:

It is virtual:

This means that the physical infrastructure of the network has to be transparent to any VPN connection. In most cases it also means that the physical network is not owned by the user of a VPN but is a public network shared with many other users. To facilitate the necessary transparency to the upper layers, protocol tunneling techniques are used. To overcome the implications of not owning the physical network, service level agreements with network providers should be established to provide, in the best possible way, the performance and availability requirements needed by the VPN.

It is private:

The term “private” in the VPN context refers to the privacy of the traffic that is to flow over the VPN. As mentioned before, VPN traffic often flows over public networks (hence the confusion with the word “private”) and therefore, precautions must be met to provide the necessary security that is required for any particular traffic profile that is to flow over a VPN connection. Those security requirements include:

- Data encryption
- Data origin authentication
- Secure generation and timely refresh of cryptographic keys needed for encryption and authentication
- Protection against replay of packets and address spoofing

It is a network:

Even though not physically existent, a VPN must effectively be perceived and treated as an extension to a company’s network infrastructure. This means that it must be made available to the rest of the network, to all or a specified subset of its devices and applications, by regular means of topology such as routing and addressing.

Having said all that, “secure tunneled connections” may be a more appropriate term to describe what a VPN technically is, but the term VPN has prevailed.

1.2 VPN benefits

With the explosive growth of the Internet, companies are beginning to ask: “How can we best exploit the Internet for our business?” Initially, companies were using the Internet to promote their image, products, and services by providing World Wide Web (WWW) access to corporate Web sites. Today, however, the Internet potential is limitless, and the focus has shifted to e-business, using the global reach of the Internet for easy access to key business applications and data that reside in traditional I/T systems. Companies are looking for the best solution to securely and cost-effectively extend the reach of their applications and data across the world. While Web-enabled applications can be used to achieve this, a virtual private network offers more comprehensive and secure solutions.

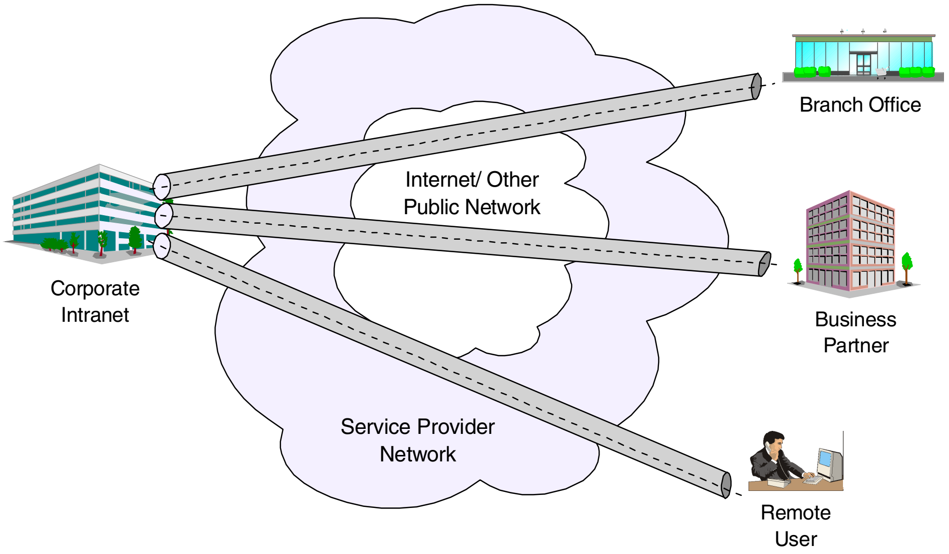


Figure 1. Virtual private network (VPN)

VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 1. Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive, leased lines, long-distance calls, and toll-free telephone numbers.

A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives may not be available.

Although the technology to implement these virtual private networks is just becoming standardized, not all the products in the market support all VPN methods. While some VPN methods can be used in conjunction with each other, some are alternative solutions to each other. A proper VPN solution should be determined according to your needs by taking the following issues into consideration:

- Business need
- Security
- Performance
- Interoperability of the solution with your current systems

The key to maximizing the value of a VPN is the ability for companies to evolve their VPNs as their business needs change and to easily upgrade to future technology. Vendors who support a broad range of hardware and software VPN products provide the flexibility to meet these requirements. IPSec-based VPN solutions today run mainly in the IPv4 environment, but it is important that they have the capability of being upgraded to IPv6 to remain interoperable with your business partner's and/or supplier's VPN solutions. Perhaps equally critical is the ability to work with a vendor who understands the issues of deploying a VPN. The implementation of a successful VPN involves more than technology. The vendor's networking experience plays heavily into this equation.

1.3 VPN requirements

Before implementing virtual private networks, you should not only be aware of the potential benefits of such a solution but also of potential exposures and how you can successfully thwart them. In this section we deal with problems that are commonly attributed to VPNs. We explain those considerations and what can be done to prevent them from jeopardizing a VPN solution.

Most of the time, security is seen as the biggest problem with VPNs, but we think that with today’s advanced cryptographic features and with careful planning and comprehensive security policies, this is the easiest problem to overcome when implementing VPNs. We will therefore discuss this topic first.

1.3.1 Security considerations for VPNs

The use of VPNs raises several security concerns beyond those that were present in traditional corporate networks. A typical end-to-end data path might contain:

- Several machines not under control of the corporation (for example, the ISP access box in a dial-in segment and the routers within the Internet).
- A security gateway (firewall or router) that is located at the boundary between an internal segment and an external segment.
- An internal segment (intranet) that contains hosts and routers. Some could be malicious, and some will carry a mix of intracompany and intercompany traffic.
- An external segment (Internet) that carries traffic not only from your company's network but also from other sources.

In this heterogeneous environment, there are many opportunities to eavesdrop, to change a datagram's contents, to mount denial-of-service attacks, or to alter a datagram's destination address, as outlined in the following sections. The IBM solutions provide the tools to counter these threats.

Let us have a look at a typical end-to-end path next so that we will be able to understand the security considerations raised with common scenarios.

1.3.1.1 A typical end-to-end path

To understand the issues with VPN end-to-end security, we look at the elements along an end-to-end path. While not all the elements may appear in a given path, some of them will appear in every VPN configuration. End-to-end traffic will usually flow over a mix of three basic segments: a dial-in segment, an external segment (Internet), and an internal segment (intranet).

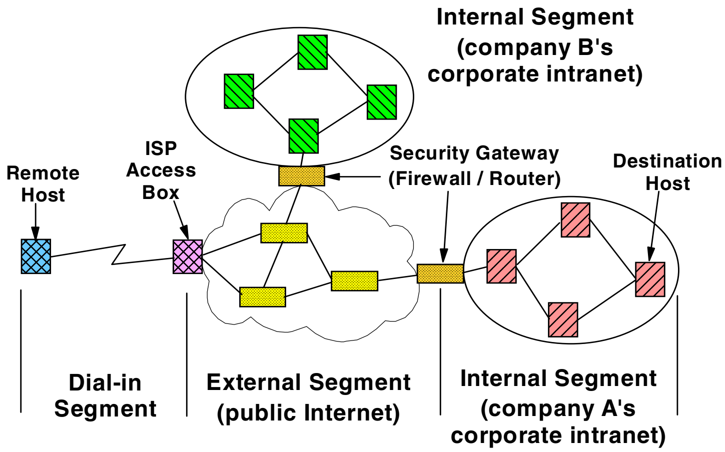


Figure 2. Typical elements in an end-to-end path

As shown in Figure 2, a path might include a first-hop dial-in connection to an Internet service provider (ISP), who in turn uses the backbone public Internet to carry the user's traffic back to a gateway at the perimeter of the corporate network. Then, the traffic eventually flows within an intranet to its ultimate destination. As we also see in Figure 2, intercompany communication can create a path that includes two separate intranets (for example, company A's and company B's).

For discussion purposes in this redbook, we refer to these elements as outlined below:

- **Dial-in segment:** In today's environment, remote access has become a necessity. Both work-at-home and on-the-road employees want convenient and secure dial-in access to their company's networks; and sometimes they even need to communicate with hosts located inside another company's network. We refer to both work-at-home and on-the-road users as *remote users*. This segment extends from a remote user's machine to an access box provided by the ISP. The protocols and procedures used on this link are specified by the Internet service provider. Today, most ISPs support the Point-to-Point Protocol (PPP) suite of protocols on this segment.
- **External network (Internet):** The Internet is not owned or operated by any single entity but is a collection of distinct routing domains, each operated by a different authority. The unifying factor is the standardized IP communications protocols defined by the Internet Engineering Task Force (IETF). The Internet Protocol (IP) suite of protocols will route data traffic at the network layer over a path that may span several ISPs' routing domains. Since IP is a

connectionless technology, each user datagram could potentially follow a different path. And in fact, traffic from several different companies could all flow simultaneously through a given backbone router in the Internet. For example, a datagram that originated in company A's intranet and a datagram that originated in company B's intranet could both flow through a common router located somewhere in the Internet. A company's traffic on the Internet can no longer be considered to be isolated from the outside world, as it would have been on a dedicated private network, since flows from different VPNs will be intermixed on the Internet backbone.

- **Internal network (intranet):** This segment appears at an endpoint of the communications path. It is under the control of the corporation, which typically operates and manages it. Traditionally, almost all traffic flowing within a corporate network was generated by the corporation's employees; very little traffic entered or exited the corporate network; and the protocols in the intranet were proprietary.

  Today, IP is becoming a popular protocol for use within corporate intranets, and data traffic enters and exits the corporate intranet regularly (consider Web browsers, FTP, or Telnet applications). In today's world of e-business, there are emerging requirements for external suppliers and business partners to have access to data stored on another company's internal servers. Since traffic flowing within an intranet at any given time may have been generated by several different companies, today it may no longer be possible to categorize a given intranet as *trusted* or *untrusted*. A company may consider its own intranets to be trusted, but at the same time its business partners may consider it to be untrusted. In this environment, a VPN designer may need to provide network security functions both on the intranet segments and on the Internet segment.

As shown in Figure 2, there are four classes of machines that occur along the path:

- Remote hosts (dial-up)
- Fixed hosts (sources and destinations, or clients and servers)
- ISP access box
- Security gateways (firewalls and/or routers)

Protocols in these machines are used to provide address assignment, tunneling, and IP security. Viable security solutions can be constructed by deploying IP security in some combination of remote hosts, firewalls, routers, and fixed hosts. But since each company should be responsible for its own security, there is no requirement for the ISP boxes or the routers in the Internet backbone to support IP security.

1.3.1.2 Exposures in a dial-in client

The dial-in client is where the communication starts so protection is on the physical access to the dial-in client. The client has to protect his or her PC/notebook when left unattended. A simple measure such as password protection, even when he or she leaves for a short duration, should be enforced. Locking up the physical PC and/or room must also be considered.

1.3.1.3 Exposures in a dial-in segment

The dial-in segment in Figure 2 delivers a user's data traffic directly to an Internet service provider (ISP). If the data is in cleartext (that is, not encrypted), then it is very easy for the ISP to examine sensitive user data, or for an attacker to eavesdrop on the data as it travels over the dial-in link.

Link-layer encryption between the remote host and the ISP can protect against passive eavesdropping, but it does not protect against a malicious ISP. Since the ISP can decrypt the user's data stream, sensitive data is still available to the ISP in cleartext format.

1.3.1.4 Exposures in the Internet

In some remote-access scenarios, an ISP builds a tunnel to extend the reach of the PPP connection so that its endpoints will be the access box and the security gateway. If the tunneling protocol does not incorporate robust security features, a malicious ISP could easily build a tunnel that terminates somewhere other than at the correct security gateway (see Figure 3). Thus, a user's data could be delivered via a false tunnel to a malicious impostor gateway where it could be examined or even altered.

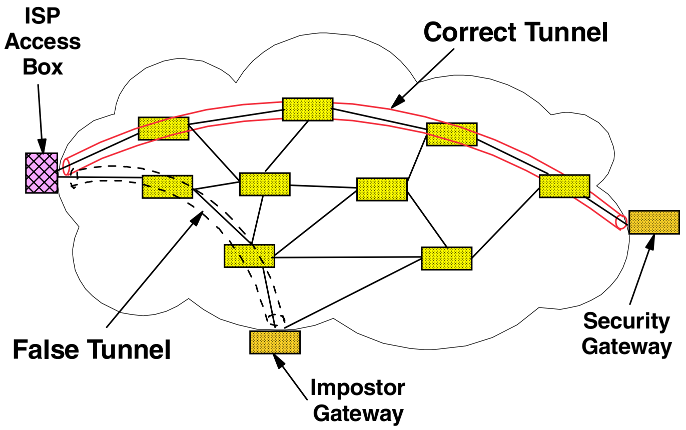


Figure 3. Exposures in the external (Internet) segment

There are also dangers as the datagram travels within the tunnel. As illustrated in Figure 3, user datagrams pass through routers in the Internet as they travel along a path toward the tunnel endpoint. If the datagrams are in cleartext, any of these routers could easily examine or modify the datagram, and passive attackers could eavesdrop on any of the links along the path.

Link-by-link encryption at each hop in the Internet backbone can thwart eavesdroppers but does not protect the user's data from a malicious router, since each router along the path would be capable of decrypting the user's data stream. Nor does link-by-link encryption protect against false tunnels, since the false tunnel endpoint would have access to cleartext data.

Even popular tunneling protocols such as Layer 2 Tunneling Protocol (L2TP) do not provide robust security. Therefore, the IETF has recommended that the tunnel traffic should be protected with the IPSec protocols.

1.3.1.5 Exposures in a security gateway

The security gateway (firewall/router) shown in Figure 2 also creates security exposures. Its main purpose is to enforce an access control policy (that is, to accept only the desired inbound traffic, to reject undesired inbound traffic, and to prevent internally generated traffic from indiscriminately leaving the corporate network). The firewall or router is under the control of the corporate network, but an internal attacker still has an opportunity to examine any traffic that the gateway decrypts and then forwards into the intranet in cleartext form.

Noncryptographic authentication provides some protection against unwanted traffic entering or leaving the network. Common techniques are passwords, packet filtering, and network address translation. However, these can be defeated by a variety of well-known attacks, such as address spoofing, and new attacks are being developed regularly. Each time a new packet filter is designed to thwart a known attack, hackers will devise a new attack, which in turn demands that a new filter rule be generated.

Because the cryptography-based authentication techniques require a long time to break, even with powerful computers, it becomes prohibitively expensive, both in time and in computer power, for a hacker to attempt to attack them. Hence, companies can deploy them with the confidence that they will provide robust protection against a hacker's attacks.

Link-by-link encryption does not prevent an intermediate box along the path from monitoring, altering, or rerouting valid traffic, since each intermediate box will have access to the cleartext form of all messages. Even host-to-gateway encryption suffers from the same weakness; the gateway still has access to cleartext.

1.3.1.6 VPN through firewalls and routers

In many environments, IP packet filtering is implemented on firewalls and routers to protect private networks from intrusions from the Internet. In situations where VPN connections traverse firewalls or routers that perform IP packet filtering as in Figure 4, the firewall or router configurations must be changed to allow VPN traffic across the firewalls or routers.

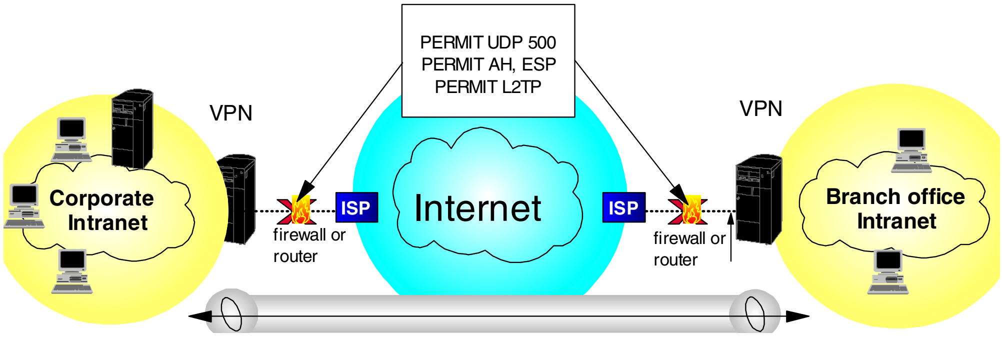


Figure 4. Allowing VPN traffic through firewalls

Specifically, the following configuration changes are required for the firewalls or routers:

- Enable IP forwarding
- Permit UDP port 500 for IKE
- Permit IP protocols 50 and 51 for ESP and AH
- Permit UDP port 1701 for L2TP and L2F
- Permit IP protocol 47 (GRE) and TCP port 1723 for PPTP

Note

To be effective, the firewall or router filter rules need to support filtering of the relatively new VPN protocols.

1.3.1.7 Exposures in an intranet

Although there is a popular belief that most security threats will occur in the public Internet, there have been studies showing that many of the attacks actually arise internally. Unless every host, gateway, and router within the intranet of Figure 2 can be fully trusted, it is possible for a malicious employee to modify an internal box, making it possible to monitor, alter, or reroute datagrams that flow within the corporate network. When data from several different networks flows within the intranet (for example, in the case where the VPN interconnects a manufacturer's intranet with the intranets of several suppliers) threats within the intranet need to be guarded against. Even if company A trusts that its own intranet is secure, the external supplier or business partner whose traffic must flow through company A's intranet may not trust it; after all, the partner's data is at risk if company A's intranet is in fact compromised in any fashion.

1.3.1.8 Conclusions

There are security exposures everywhere along an end-to-end path: on the dial-up link, in an ISP's access box, in the Internet, in the firewall or router, and even in the corporate intranet.

Previously, security solutions were developed to address just a subset of the exposures discussed in this section, but there was no framework that could protect against all these exposures using a single approach.

IP Security Architecture (IPSec) is the first definition of a comprehensive, consistent solution. It can provide end-to-end protection as well as segment-by-segment protection. Based on the work of the Internet Engineering Task Force (IETF) IBM chose to use IPSec for its VPN solutions.

In addition to IPSec, technologies such as layer-2 tunneling and remote access authentication servers provide the necessary flexibility to apply adequate security to any given VPN scenario.

1.3.2 Performance considerations

Next to security, performance is among the most critical requirements for virtual private networks. Again the problem lies in the task of finding a way to map a service guarantee from a private network to a virtual connection running over a public network.

1.3.2.1 Quality of Service (QoS)

In a virtual private network, just as in a conventional network, there will be a desire to provide distinct transport characteristics (quality of service) for packets as they travel from source to destination. The IP protocol provides Type of Service (TOS) bits that can be used for this purpose. The details of how to use these bits is a work in progress in the IETF Differentiated Services working group, but so far no firm standard solutions exist today.

As opposed to Integrated Services such as RSVP, which guarantee a quality of service for an entire path, differentiated services provide a class of service within domains where it is guaranteed that a certain TOS bit pattern will always be mapped to a certain level of service. Between DS domains - typically across the corporate-ISP boundary and between ISPs, service level agreements (SLAs) have to be in place to map TOS bits from one DS domain to another to guarantee the same level of service.

The problem with QoS is how to determine if it is required or if it is really provided when promised. Unless there are network congestions it is hardly possible to prove that specific QoS guarantees are in place. And unless you have time-critical applications, you may not even experience congestions if you provide enough bandwidth. Until QoS standards and adherent technologies are in place, ISPs and carriers in some parts of the world tend to pursue the bandwidth option rather than finding elaborate ways to guarantee service levels. Whether this is enough for the type of VPN you have in mind - and the bandwidth and response time requirements of the applications that ultimately drive this network - is only for you to find out by putting VPNs to the test.

However, looking forward to future requirements, the IPSec's AH protocol treats the TOS bits as mutable, thus allowing them to be changed as needed while an IPSec-protected datagram travels through the Internet. Thus, IPSec is already positioned to take advantage of the emerging QoS work as soon as it matures.

1.3.2.2 The toll of encryption processing

One of the key issues with respect to performance is the encryption factor. For example, if triple DES is employed, then the resources required to cipher and decipher will be significant. One solution is to use a hardware-based encryption card or adapter to off-load the VPN gateway. The performance of this hardware, however, is also limited. A reasonably good encryption hardware can drive up to 25 Mbps which is a lot of 64 kbps lines.

For determining the impact of encryption processing overhead you should distinguish the following types of systems that are incurring such overhead:

- End systems, typically VPN clients and servers with occasional VPN access, will most likely not notice much performance toll by using encryption because they only run one or up to a couple of concurrent connections.
- Servers with permanent VPN access will notice some encryption overhead run to a degree where it is advisable to separate the server from the encryption device. Where this point is reached needs to be determined per platform and cannot be generalized or measured in the number of concurrent tunnels or amount of traffic over time.
- VPN gateways will certainly absorb most of the encryption processing in almost any VPN scenario. Therefore, adding special encryption hardware or using dedicated VPN devices should be considered as an alternative before your firewall is breaking down or your router is no longer routing because it is bogged down by performing VPN operations.

1.3.2.3 The toll of logging

In a similar way, the logging of messages and events that relate to VPN traffic is likely to cause a performance impact. This impact will again be different on clients, servers and gateways. The problem to solve in this case is quite delicate:

1. If you abandon logging altogether, you risk compromising the security of your network because you will be unable to detect intrusion attempts and other attacks. A good security policy always includes a certain amount of logging.
2. If you log excessively you will lose a significant amount of processing power which will cause traffic delays and potential buffer or log space overflows. This may render your VPN systems inoperable and your whole VPN solution impractical.

It is good practice to set up a testbed for the systems that you want to deploy later to build your VPN environment. During a test phase, determine what can be logged by any of those systems, how much performance is lost due to logging and what the logs can actually tell you. That will provide you with a fair understanding of which events are significant to log permanently and which events should only be logged in case there are specific problems.

VPN gateways of several leading vendors also have the capability to log to a dedicated log server in order to avoid local resource overruns. That way you can collect and evaluate logging information in a central location which makes intrusion detection and trend determination much easier.

1.3.2.4 Conclusions

Some performance issues, such as encryption, are easier to tackle than others, such as quality of service. Standards are maturing toward providing the latter across public networks, but at the moment you are left to try a VPN to find out if your application requirements can be met, either in full or partially, or not at all. Encryption overhead can be easily absorbed by modern hardware encryption and dedicated VPN devices up to multiple T1 speeds, which should be adequate for most VPN scenarios.

1.3.3 Management considerations

With a private network, management used to be a piece of cake if done properly but could be a nightmare if you had no clue what you were doing. With VPNs, the bandwidth of error is much narrower because there is not enough technology available today to provide comprehensive VPN management. This sounds like bad news, but in fact it is good news because it shows that the topic of VPN management is not a rushed one. Customers are unlikely to implement large VPNs in great numbers over night. That is why vendors first provided the tools to build VPNs rather than to manage them. Once customers have had hands-on experience with VPNs, total management solutions will be in place as both standards and products.

For the time being, vendors of VPN technology provide you with limited features to manage some VPN functions within their particular VPN device, while network management vendors are still thinking of how VPNs can be included in their respective management suites. Expect a broader portfolio for the coming six to twelve months as the VPN market is spinning very fast.

What you can do today with IBM VPN products is explained in more detail in Chapter 8, “Network management for VPNs” on page 161.

1.3.4 General purpose encryption

Encryption is an efficient way to make data unreadable to unintended recipients. If handled properly, it is a very effective way to provide security. However, if handled poorly, encryption can be a threat to your data rather than a protection. Remember that encryption requires keys to transform cleartext into ciphertext and vice versa. If those keys get lost or stolen, for instance by a system administrator who leaves the company without handing in encryption keys previously in his or her custody, your data is compromised and, what is worse, you may not be able to access it anymore (but your competitors might).

Therefore, as part of your security policy, you should clearly define if encryption is at all necessary, and if so, for what types of data, at what points in the network, and who should be authorized to use it.

There are generally two ways to protect against the loss or theft of encryption keys:

Key escrow

This technique provides for the storage and retrieval of keys and data in case keys get lost or stolen. Keys are stored with a trusted third party (recovery agent or key guardian), as a whole or in parts, on independent storage media, to be retrieved as required. The trusted third party could be a company key administrator located on company premises, or an external agency. This ensures that the keys remain in a company’s possession even after a system administrator or whoever used the keys leaves the company.

Key recovery

This technique was designed to allow law enforcement agencies (LEAs) to recover the keys for decrypting secret messages of suspicious parties. Of course, you can also use this approach to recover your own keys yourself, but it is a rather complicated process and less practical than key escrow.

One way of implementing key recovery is by inserting key recovery blocks in the data stream at random intervals and/or when the keys change. Those key recovery blocks are encrypted with the public key of a trusted third party (key recovery agent). The key recovery agents can decrypt keys with their private keys, then encrypt retrieved keys with the public key of an LEA and send them to the LEA. LEAs can decrypt keys with their private keys and then decrypt the previously retrieved ciphertext messages.

1.3.4.1 Export/import regulations

Whenever you choose to use encryption you have to make sure what level of encryption is legally allowed to be used in your country and for the nature of your business. Usually, banks can employ higher levels of encryptions than home office users, and some countries are more restrictive than others. In the United States encryption is regulated by the Department of Commerce.

1.3.4.2 Dangers of end-to-end encryption

When end-to-end encryption is allowed, this opens up the firewalls to an untrusted zone. When implemented, the end-to-end encrypted traffic will not be seen even by the customer who implemented this except for the designated server/client. This also means once the intruder gets access to one end, the intruder can gain access all the way to the corporate intranet. Denial-of-service support on the VPN gateway or firewall will also be of no use then, and therefore the intruder can disrupt an important server/service.

1.4 A basic approach to VPN design and implementation

We mentioned in the preface that this redbook is not meant to be a VPN design guide so we will limit ourselves to a few words on the general process of VPN design and implementation. This will help you to put the remainder of this redbook in proper perspective.

What VPN scenarios are to be implemented?

To get started on VPNs, it helps to know which environment you want to implement:

- Branch office (intranet) VPN
- Business partner/supplier (extranet) VPN
- Remote access VPN
- Multiple combinations

Later in this chapter (see 1.5, “Common VPN scenarios” on page 15), we introduce you briefly to the characteristics of this redbook, and in Part 2, “VPN scenarios based on MRS/MAS/AIS Version 3.3” on page 77, we demonstrate how you can implement each of those scenarios using IBM VPN solutions and complementing solutions from other vendors.

What is your application mix?

We mentioned that applications ultimately drive any network, hence they do the same for VPNs. You have to evaluate the benefits of a VPN solution in light of the requirements of the applications and application infrastructure that you want to support and/or provide over a VPN. Things you should consider include:

- Are your applications based on a 2-tier or a 3-tier model?
- Are your applications Web enabled? If yes, what is the motivation for VPNs?
- Does the network need to provide end-to-end services?
- Are applications time-critical or bandwidth-intensive?
- Are security features such as authentication and encryption provided by applications or is the network expected to take care of that? This leads to a choice between specific or generic security technologies.

What are the required levels of protection?

This leads to the implementation of a security policy that covers all of the following:

- Authentication
- Encryption
- Key exchange and key refresh intervals
- Perfect forward secrecy (PFS) and replay protection
- End-to-end protection
- Performance
- Event logging
- Legal issues

What is the projected growth of the VPN topology to be deployed?

Scalability is often an important criterion for a network. With a VPN this includes issues such as the following:

- Dynamic (IKE) versus manual tunnels
- Pre-shared keys versus certificates
- Public key infrastructure (PKI)
- Geographical span
- Cost of implementation, migration and ownership

What is the VPN infrastructure going to look like and who will support it?

This includes topics such as the following:

- ISP bandwidth, geographical presence and access plans
- VPN technology support by ISPs (layer-2 tunneling, IPSec, PKI, LDAP)
- Network transition
- VPN gateway placement
- Quality of Service (QoS) and service level agreements (SLAs)
- Public key infrastructure (PKI)
- Cost of implementation and service

How will the VPN be managed?

This includes, among others, the following issues:

- Policies and configuration definition and delivery
- Directory infrastructure (for example, LDAP)
- Public key infrastructure (PKI)
- Monitoring, alerting and logging
- Authentication and accounting (for example, RADIUS)
- Virtual-to-physical network mappings
- Routing and backup paths
- Load balancing of traffic and devices
- Virus and content screening and intrusion detection
- Cost of implementation, migration, ownership and service

Which products are you finally going to settle on?

Best-of-breed or one-size-fits-all or single vendor? What is the cost factor and is it the ultimate decision criterion?

How will roll-out and maintenance be conducted?

In-house by your I/S department or outsourced using a service contractor or ISP? Again, what about the cost factor?

As you can see, making all these decisions is not easy and takes time and there is no guarantee that you will do everything right. This redbook helps you during several of the steps mentioned above. It describes VPN scenarios, technologies and products and it illustrates how you can use those products to implement VPNs.

1.5 Common VPN scenarios

In this section we look at the three most likely business scenarios well suited to the implementation of a VPN solution:

- Branch office connection network
- Business partner/supplier network

- Remote access network

1.5.1 Branch office interconnections

The branch office scenario securely connects two trusted intranets within your organization. Your security focus is on both protecting your company's intranet against external intruders and securing your company's data while it flows over the public Internet. For example, suppose corporate headquarters wants to minimize the costs incurred from communicating to and among its own branches. Today, the company may use frame relay and/or leased lines but wants to explore other options for transmitting its internal confidential data that will be less expensive, more secure, and globally accessible. By exploiting the Internet, branch office connection VPNs can be easily established to meet the company's needs.

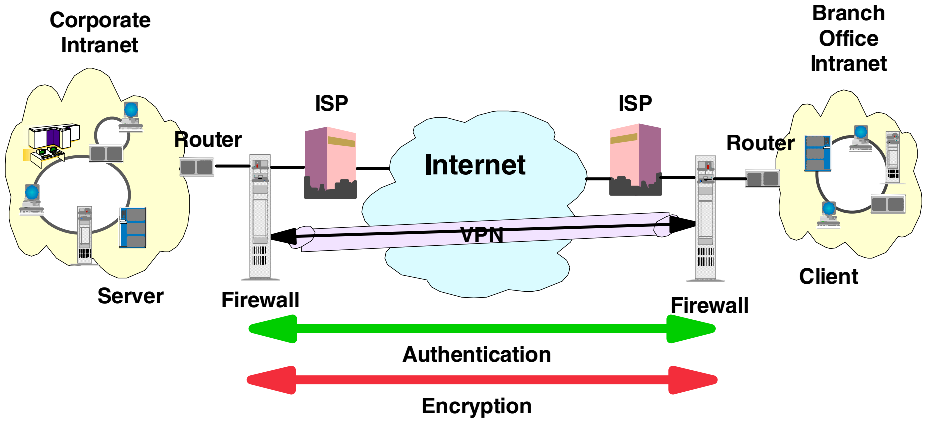


Figure 5. Branch office VPN

As shown in Figure 5 on page 16, one way to implement this VPN connection between the corporate headquarters and one of its branch offices is for the company to purchase Internet access from an ISP. Firewalls, or routers with integrated firewall functionality, or in some cases a server with IPSec capability, would be placed at the boundary of each of the intranets to protect the corporate traffic from Internet hackers. With this scenario, the clients and servers need not support IPSec technology, since the IPSec-enabled firewalls (or routers) would be providing the necessary data packet authentication and encryption. With this approach, any confidential information would be hidden from untrusted Internet users, with the firewall denying access to potential attackers.

With the establishment of branch office connection VPNs, the company's corporate headquarters will be able to communicate securely and cost effectively to its branches, whether located locally or far away. Through VPN technology, each branch can also extend the reach of its existing intranet to incorporate the other branch intranets, building an extended, enterprise-wide corporate network. And this company can easily expand this newly created environment to include its business partners, suppliers, and remote users, through the use of open IPSec technology.

1.5.2 Business partner/supplier networks

Industry-leading companies will be those that can communicate inexpensively and securely to their business partners, subsidiaries, and vendors. Many companies have chosen to implement frame relay and/or purchase leased lines to achieve this interaction. But this is often expensive, and geographic reach may be limited. VPN technology offers an alternative for companies to build a private and cost-effective extended corporate network with worldwide coverage, exploiting the Internet or other public network.

Suppose you are a major parts supplier to a manufacturer. Since it is critical that you have the specific parts and quantities at the exact time required by the manufacturing firm, you always need to be aware of the manufacturer′s inventory status and production schedules. Perhaps you are handling this interaction manually today, and have found it to be time consuming, expensive and maybe even inaccurate. You would like to find an easier, faster, and more effective way of communicating. However, given the confidentiality and time-sensitive nature of this information, the manufacturer does not want to publish this data on its corporate Web page or distribute this information monthly using an external report.

To solve these problems, the parts supplier and manufacturer can implement a VPN, as shown in Figure 6 on page 17. A VPN can be built between a client workstation, in the parts supplier's intranet, directly to the server residing in the manufacturer's intranet. The clients can authenticate themselves either to the firewall or router protecting the manufacturer's intranet, directly to the manufacturer's server (validating that they are who they say they are), or to both, depending on your security policy. Then a tunnel could be established, encrypting all data packets from the client, through the Internet, to the required server.

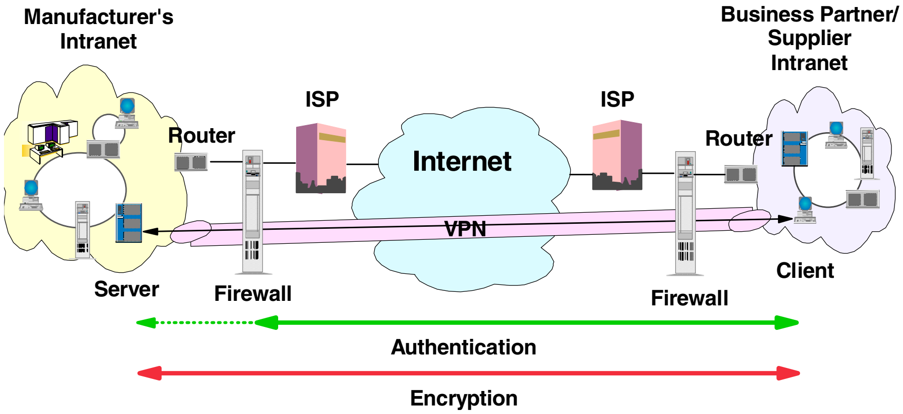


Figure 6. Extranet VPN

Optionally, the tunnels into the intranet could be terminated at a special VPN gateway in a DMZ. This would allow additional security checks, such as virus protection and content inspection, to be performed before data from an external system was allowed into the corporate network.

With the establishment of this VPN, the parts supplier can have global, online access to the manufacturer′s inventory plans and production schedule at all times during the day or night, minimizing manual errors and eliminating the need for additional resources for this communication. In addition, the manufacturer can be assured that the data is securely and readily available to only the intended parts supplier(s).

One way to implement this scenario is for the companies to purchase Internet access from an Internet service provider (ISP), then, given the lack of security of the Internet, either a firewall or IPSec-enabled router, or a server with IPSec capability can be deployed as required to protect the intranets from intruders. If end-to-end protection is desired, then both the client and server machines need to be IPSec-enabled as well.

Through the implementation of this VPN technology, the manufacturer would be able to easily extend the reach of its existing corporate intranet to include one or more parts suppliers (essentially building an extended corporate network) while enjoying the cost-effective benefits of using the Internet as its backbone. And, with the flexibility of open IPSec technology, the ability for this manufacturer to incorporate more external suppliers is limitless.

1.5.3 Remote access scenarios

A remote user, whether at home or on the road, wants to be able to communicate securely and cost effectively back to his or her corporate intranet. Although many still use expensive long-distance and toll-free telephone numbers, this cost can be greatly minimized by exploiting the Internet. For example, you are at home or on the road but need a confidential file on a server within your intranet. By obtaining Internet access in the form of a dial-in connection to an ISP, you can communicate with the server in your intranet and access the required file.

One way to implement this scenario is to use a remote access tunneling protocol such as L2TP, PPTP or L2F. Another way is to use an IPSec-enabled remote client and a firewall, as shown in Figure 7. Ideally, you may wish to combine both solutions which will provide the best protection and the most cost-effective way of remote access. The client accesses the Internet via dial-up to an ISP, and then establishes an authenticated and encrypted tunnel between itself and the firewall at the intranet boundary.

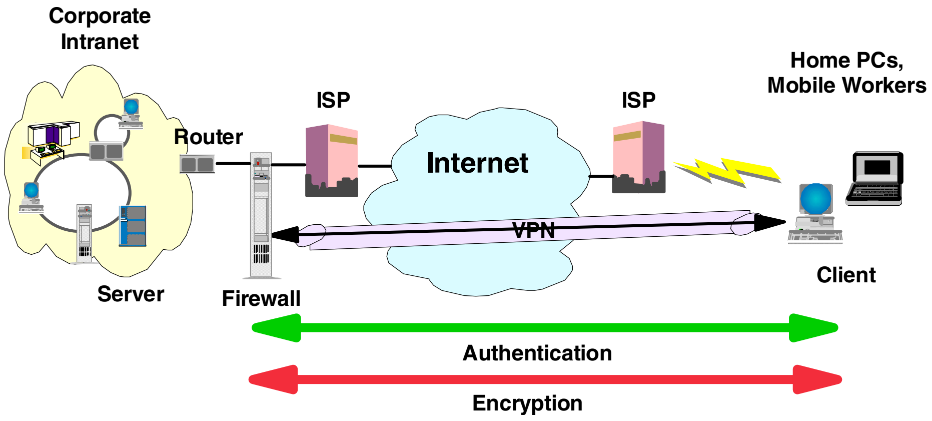


Figure 7. Remote access VPN

By applying IPSec authentication between the remote client and the firewall, you can protect your intranet from unwanted and possibly malicious IP packets. And by encrypting traffic that flows between the remote host and the firewall, you can prevent outsiders from eavesdropping on your information.

1.6 VPN technologies and security policies

The following protocols and systems are commonly used to provide various degrees of security services in a computer network. Some of them are described in more detail in later chapters in this redbook. This section provides an overview of what security technologies are available today and commonly used, which creates confidence, and which ones may be suitable for VPNs.

- IP packet filtering
- Network Address Translation (NAT)
- IP Security Architecture (IPSec)
- SOCKS
- Secure Sockets Layer (SSL)
- Application proxies
- Firewalls
- Kerberos, RADIUS, and other authentication systems (which are discussed in Chapter 9, “User authentication for remote access” on page 179)
- Antivirus, content inspection and intrusion detection systems

Figure 8 illustrates where those security solutions fit within the TCP/IP layers:

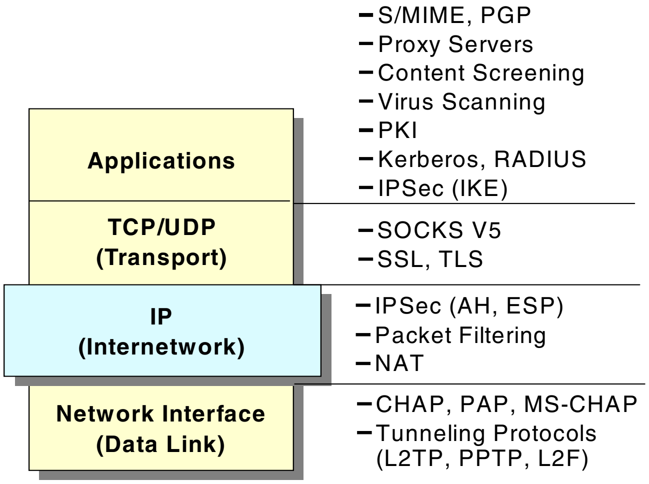
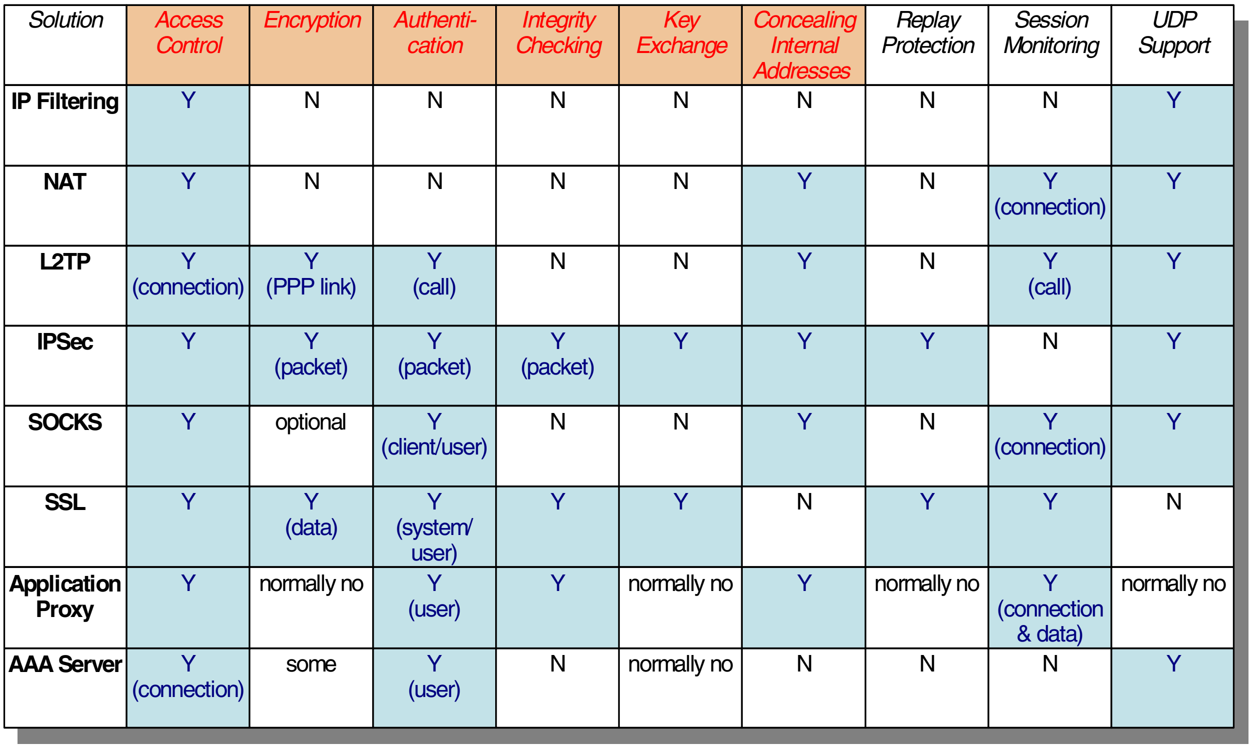


Figure 8. Security solutions in the TCP/IP layers

Figure 9 on page 20 summarizes the characteristics of some of the security solutions mentioned earlier and compares them to each other in light of specific VPN requirements. This should help anyone who needs to devise a security strategy to determine what combination of solutions will achieve a desired level of protection.



Solution	*Access Control*	*Encryption*	*Authentication*	*Integrity Checking*	*Key Exchange*	*Concealing Internal Addresses*	*Replay Protection*	*Session Monitoring*	*UDP Support*
IP Filtering	Y	N	N	N	N	N	N	N	Y
NAT	Y	N	N	N	N	Y	N	Y (connection)	Y
L2TP	Y (connection)	Y (PPP link)	Y (call)	N	N	Y	N	Y (call)	Y
IPSec	Y	Y (packet)	Y (packet)	Y (packet)	Y	Y	Y	N	Y
SOCKS	Y	optional	Y (client/user)	N	N	Y	N	Y (connection)	Y
SSL	Y	Y (data)	Y (system/ user)	Y	Y	N	Y	Y	N
Application Proxy	Y	normally no	Y (user)	Y	normally no	Y	normally no	Y (connection & data)	normally no
AAA Server	Y (connection)	some	Y (user)	N	normally no	N	N	N	Y

Figure 9. Characteristics of IP security technologies

As mentioned earlier, an overall security solution can, in most cases, only be provided by a combination of the listed options, for instance, by using a firewall. However, what your particular security requirements are needs to be specified in a security policy.

1.6.1 The need for a security policy

It is important to point out that you cannot implement security if you have not decided what needs to be protected and from whom. You need a security policy, a list of what you consider allowable and what you do not consider allowable, upon which to base any decisions regarding security. The policy should also determine your response to security violations.

An organization's overall security policy must be determined according to security analysis and business requirements analysis. Since a firewall, for instance, relates to network security only, a firewall has little value unless the overall security policy is properly defined. The following questions should provide some general guidelines:

- Exactly who do you want to guard against?
- Do remote users need access to your networks and systems?
- How do you classify confidential or sensitive information?
- Do the systems contain confidential or sensitive information?
- What will the consequences be if this information is leaked to your competitors or other outsiders?
- Will passwords or encryption provide enough protection?

- Do you need access to the Internet?
- How much access do you want to allow to your systems from the Internet and/or users outside your network (business partners, suppliers, corporate affiliates, etc.)?
- What action will you take if you discover a breach in your security?
- Who in your organization will enforce and supervise this policy?

This list is short, and your policy will probably encompass a lot more before it is complete. Perhaps the very first item you need to assess is the depth of your paranoia. Any security policy is based on how much you trust people, both inside and outside your organization. The policy must, however, provide a balance between allowing your users reasonable access to the information they require to do their jobs, and totally disallowing access to your information. The point where this line is drawn will determine your policy.

1.6.2 Network security policy

If you connect your system to the Internet then you can safely assume that your network is potentially at risk of being attacked. Your gateway or firewall is your greatest exposure, so we recommend the following:

- The gateway should not run any more applications than is absolutely necessary, for example, proxy servers and logging, because applications have defects that can be exploited.
- The gateway should strictly limit the type and number of protocols allowed to flow through it or terminate connections at the gateway from either side, because protocols potentially provide security holes.
- Any system containing confidential or sensitive information should not be directly accessible from the outside.
- Generally, anonymous access should at best be granted to servers in a demilitarized zone.
- All services within a corporate intranet should require at least password authentication and appropriate access control.
- Direct access from the outside should always be authenticated and accounted.

The network security policy defines those services that will be explicitly allowed or denied, how these services will be used and the exceptions to these rules. Every rule in the network security policy should be implemented on a firewall and/or Remote Access Server (RAS). Generally, a firewall uses one of the following methods:

Everything not specifically permitted is denied.

This approach blocks all traffic between two networks except for those services and applications that are permitted. Therefore, each desired service and application should be implemented one by one. No service or application that might be a potential hole on the firewall should be permitted. This is the most secure method, denying services and applications unless explicitly allowed by the administrator. On the other hand, from the point of users, it might be more restrictive and less convenient.

Everything not specifically denied is permitted.

This approach allows all traffic between two networks except for those services and applications that are denied. Therefore, each untrusted or potentially harmful service or application should be denied one by one. Although this is a flexible and convenient method for the users, it could potentially cause some serious security problems.

Remote access servers should provide authentication of users and should ideally also provide for limiting certain users to certain systems and/or networks within the corporate intranet (authorization). Remote access servers must also determine if a user is considered roaming (can connect from multiple remote locations) or stationary (can connect only from a single remote location), and if the server should use callback for particular users once they are properly authenticated.

1.6.3 VPN security policy

While a simple network security policy specifies which traffic is denied and which traffic is permitted to flow and where, a VPN security policy describes the characteristics of protection for a particular traffic profile. In a sense, it is a subset of a network security policy because it is more granular and it depends on the former to allow traffic between certain destinations before it can be protected. It should also be noted that traffic that should flow through a VPN and therefore be protected should not be allowed to flow otherwise, probably through nonsecure channels.

A VPN security policy typically describes the traffic profile to be protected (source and destination, protocols and ports) and the security requirements for the protection itself (authentication, encryption, transforms, key lengths and lifetimes, and so forth). VPN policies can be defined per device but should be implemented in a centralized directory to provide better scalability and management. Essentially, both devices need to have matching policies for the same traffic profile before such traffic can be allowed to flow between them. One policy can be more granular or restrictive than the other as long as both parties can agree on the same set of protection suites at any point in time.

Chapter 2. Layer-2 VPN protocols

In this chapter we discuss protocols that allow a layer-2 connection, typically PPP, to be tunneled over another network, typically IP. This sounds like a complicated approach involving a lot of overhead, but several benefits can be derived from this approach which are useful or even invaluable for building VPNs. In fact, the number of Internet VPN scenarios or variations thereof would be quite limited without the use of layer-2 tunneling techniques.

2.1 Layer 2 Tunneling Protocol (L2TP)

The Layer 2 Tunneling Protocol (L2TP) is one of the emerging techniques for providing a remote connection to the corporate intranet. The L2TP protocol has been developed merging two different protocols: the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F).

The remote dial-in user scenario is the most common situation for using L2TP. Remote users do not need to make a long-distance call or use a toll-free number to connect directly to the corporate servers but cost constraints suggest the use of ISPs' points of presence (POPs) as a more cost-effective solution. In this case the dial-in user connects to the nearest POP provided by the ISP and then the session is routed through the ISPs and/or the Internet cloud to reach the corporate LAN access. This environment has more than one point of critical security and reliability issues.

L2TP provides a technique for building a Point-to-Point Protocol (PPP) tunnel connection that, instead of being terminated at the ISP's nearest POP, is extended to the final corporate intranet access gateway. The tunnel can be initiated either by the remote host or by the ISP's gateway access. L2TP provides a reliable way of connecting remote users in a virtual private network that can support multiprotocol traffic, that is, all the network layer protocols supported by the PPP protocol. Moreover, it provides support for any network layer private addressing scheme for the connection over the Internet.

2.1.1 Overview and standards

L2TP can support remote LAN access using any network layer protocol supported by PPP over the tunnel session, and this is managed by terminating the PPP connection directly in the corporate intranet access gateway.

L2TP is defined in RFC 2661.

There are some elements that take part in the L2TP protocol scenario:

L2TP Access Concentrator (LAC)

The LAC is located at the ISP's POP to provide the physical connection of the remote user. In the LAC the physical media are terminated and can be connected to more public switched telephone network (PSTN) lines or integrated services digital network (ISDN) lines. Over these media the user can establish the L2TP connection that the LAC routes to one or more L2TP servers where the tunnels are terminated. Any 221x Nways router can support LAC functionality and based on the connection capabilities a 2210 Nways multiprotocol router or a 2212 Nways Access Utility can be correctly positioned on a different ISP's POPs as a LAC for the L2TP.

L2TP Network Server (LNS)

The LNS terminates the calls arriving from the remote users. Only a single connection can be used on the LNS to terminate multiple calls from remote users, placed on different media as ISDN, asynchronous lines, V.120, etc. The 221x Nways routers can support LNS capabilities. A 2216 Multiaccess Concentrator can be used also as LNS when it is used as the corporate intranet access gateway.

Network Access Server (NAS)

The NAS is the point-to-point access device that can provide on-demand access to the remote users across PSTN or ISDN lines.

The L2TP protocol is described in Figure 10. The session and tunnel establishments are handled in the following phases:

- The remote user initiates a PPP connection to the NAS.
- The NAS accepts the call.
- The end user authentication is provided by means of an authorization server to the NAS.
- The LAC is triggered by the end user’s attempt to start a connection with the LNS for building a tunnel with the LNS at the edge of the corporate intranet. Every end-to-end attempt to start a connection is managed by the LAC with a session call. The datagrams are sent within the LAC LNS tunnel. Every LAC and LNS device keeps track of the connected user’s status.
- The remote user is authenticated also by the authentication server of the LNS gateway before accepting the tunnel connection.
- The LNS accepts the call and builds the L2TP tunnel.
- The NAS logs the acceptance.
- The LNS exchanges the PPP negotiation with the remote user.
- End-to-end data is now tunneled between the remote user and the LNS.

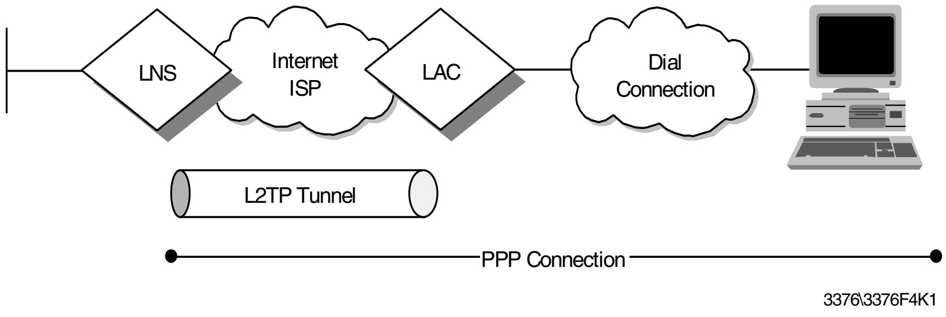


Figure 10. Layer 2 Tunnel Protocol (L2TP) scenario

L2TP can support the following functions:

- Tunneling of single user dial-in clients

- Tunneling of small routers, for example, a router with a single static route to set up based on an authenticated user's profile
- Incoming calls to an LNS from a LAC
- Multiple calls per tunnel
- Proxy authentication for PAP and CHAP
- Proxy LCP
- LCP restart in the event that proxy LCP is not used at the LAC
- Tunnel endpoint authentication
- Hidden attribute value pair (AVP) for transmitting a proxy PAP password
- Tunneling using a local lookup table
- Tunneling using the PPP user name lookup in the AAA subsystem

2.1.2 L2TP flows

There are a number of steps that occur for L2TP:

- Establish a control connection and tunnel.
- Initiate a call.
- Establish an L2TP session.
- Forward PPP packets.

Between two devices there may be more than one tunnel and each tunnel must have its own control connection. The control connection can be initiated by either the LSN or LAC.

Within the tunnel there can be many L2TP sessions and each session represents a single PPP stream between the LNS and the LAC. Normally this session is established by the LAC.

2.1.2.1 Control connection and tunnel

Below are the flows for establishing the control connection and its associated tunnel.

Table 1. L2TP control session establishment flow

LAC or LNS		LAC or LNS
Start_Control_Connection_Request	1 --->	
	<--- 2	Start_Control_Connection_Reply
Start_Control_Connection_Connected	3 --->	
	<--- 4	ZLB_Acknowledge

As you can gather from the table above either the LAC or LNS can set up the control connection and its tunnel. A series of messages are simply transferred between the peers requesting the setup of the connection. Message 4 is a Zero Length Body (ZLB) message which simply acknowledges receipt of the last message.

During this process authentication of the tunnel occurs. Note that this step is optional. This is achieved by sending a challenge in either message 1 or 2, and sending the reply in the following message. A shared secret is needed between the peers to generate and validate the challenge.

2.1.2.2 Establish session

A separate session must be established for each PPP stream. It is normally initiated by the receipt of a call from the LAC. This session can only be established after the control connection and its tunnel have been set up. The following shows the flows that occur in this process:

Table 2. L2TP incoming session establishment flow

LAC		LNS
Call detected		
Incoming_Call_Request	1 --->	
	<--- 2	Incoming_Call_Reply
Incoming_Call_Connected	3 --->	
	<--- 4	ZLB_Acknowledge

During this process the LAC can defer answering the call until it receives message 2 to ensure that this session should be established. LAC can answer the call and negotiate the LCP and PPP authentication and then use this information to choose the LNS to which it needs to establish a session.

The above flows show the process for establishing a session from the LAC. This is called an incoming call establishment. LT2P, however, allows you to establish a call from the other direction, that is, from the LNS. This is called an outgoing call request:

Table 3. L2TP outgoing session establishment flow

LAC		LNS
	<--- 1	Outgoing_Call_Request
Outgoing_Call_Reply	2 --->	
Perform call operation		
Outgoing_Call_Connected	3 --->	
	<--- 4	ZLB_Acknowledge

Once the session is established PPP packets can flow over the tunnel.

2.1.3 Compulsory and voluntary tunnel modes

L2TP supports two types of tunnels, the compulsory model and the voluntary model.

2.1.3.1 L2TP compulsory tunnels

With this model, the L2TP tunnel is established between a LAC, an ISP and an LNS at the corporate network. This requires the cooperation of a service provider that has to support L2TP in the first place and has to determine based upon authentication information whether L2TP should be used for a particular session, and where a tunnel should be directed. However, this approach does not require any changes at the remote client, and it allows for a centralized IP address assignment to a remote client by the corporate network. Also, no Internet access is provided to the remote client other than via a gateway in the corporate network that allows for better security control and accounting.

An L2TP compulsory tunnel, illustrated in Figure 11 on page 27, is established as follows:

1. The remote user initiates a PPP connection to an ISP.
2. The ISP accepts the connection and the PPP link is established.
3. The ISP now undertakes a partial authentication to learn the user name.
4. ISP-maintained databases map users to services and LNS tunnel endpoints.
5. LAC then initiates an L2TP tunnel to LNS.
6. If LNS accepts the connection, LAC then encapsulates PPP with L2TP and forwards the appropriate tunnel.
7. LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames.
8. LNS then uses PPP authentication to validate the user and then assigns the IP address.

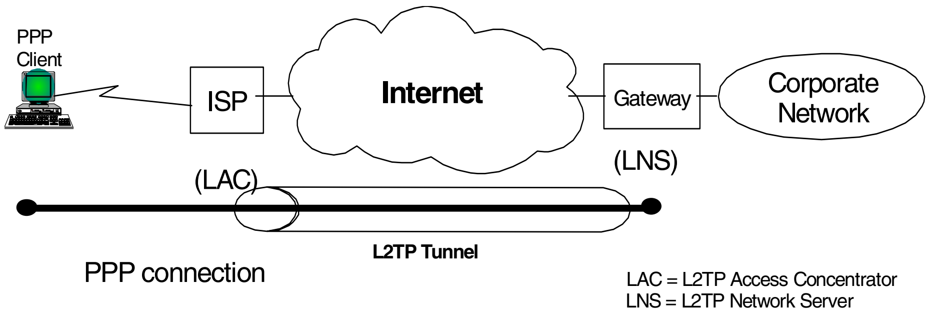


Figure 11. L2TP compulsory tunnel model

2.1.3.2 L2TP voluntary tunnels

With this model, the L2TP tunnel is established between a remote client (which is effectively acting as a LAC) and an LNS at a corporate network. This method is similar to PPTP and is essentially transparent to an ISP but requires L2TP support at the client. This approach allows the remote client to have Internet access as well as one or multiple VPN connections at the same time. However, the client ultimately ends up being assigned multiple IP addresses; one from the ISP for the original PPP connection, and one per L2TP VPN tunnel assigned from a corporate network. This opens the client as well as the corporate networks to potential attacks from the outside, and it requires client applications to determine the correct destinations for their data traffic.

An L2TP voluntary tunnel, illustrated in Figure 12, is established as follows:

1. The remote user has a pre-established connection to an ISP.
2. The L2TP Client (LAC) initiates the L2TP tunnel to LNS.
3. If LNS accepts the connection, LAC then encapsulates PPP and L2TP, and forwards through a tunnel.

4. LNS accepts these frames, strips L2TP, and processes them as normal incoming frames.
5. LNS then uses PPP authentication to validate the user and then assign the IP address.

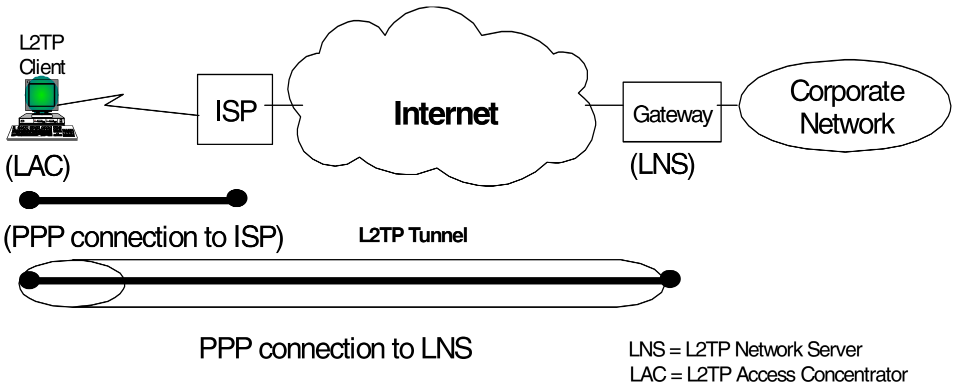


Figure 12. L2TP voluntary tunnel model

2.1.4 Securing the tunnels with IPSec

The L2TP protocol can provide a cost-effective solution for the remote access scenario using the virtual private network technology, but there are some issues mainly concerned with security. An L2TP tunnel is created by encapsulating an L2TP frame inside a UDP packet, which in turn is encapsulated inside an IP packet whose source and destination addresses define the tunnel's endpoints as can be seen in Figure 13. Since the outer encapsulating protocol is IP, clearly IPSec protocols can be applied to this composite IP packet, thus protecting the data that flows within the L2TP tunnel. The Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) protocols can all be applied in a straightforward way.

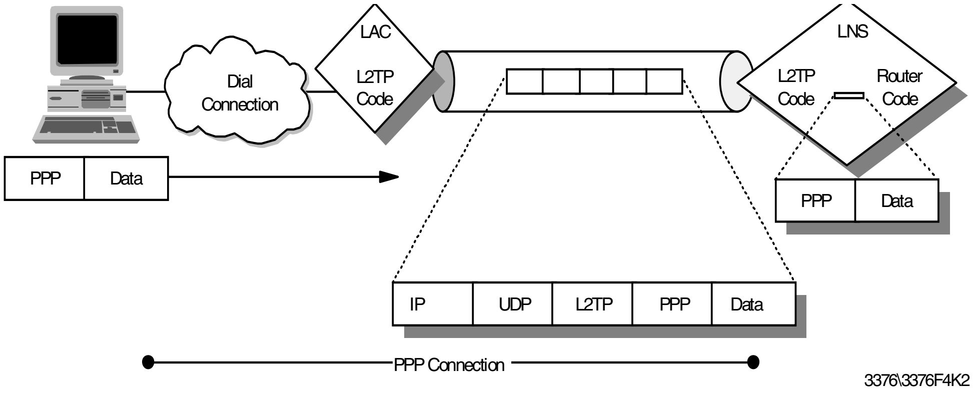


Figure 13. L2TP tunnel encapsulation

In fact a proposed solution to the security issues has been developed in the PPP Extensions Working Group in the IETF to make use of the IPSec framework to provide the security enhancements to the L2TP protocol. The use of IPSec technologies in conjunction with the L2TP protocol can provide a secured end-to-end connection between remote users and the corporate intranet that can support remote LAN connections (not only remote IP). The following reference provides additional information on how to use IPSec in conjunction with L2TP:

```
http://search.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-security-04
.txt
```

The IPSec framework can add to the L2TP protocol the per packet authentication mechanism and integrity checks instead of the simple authentication of the ending point of the tunnel that is not secured from attack by internetwork nodes along the path of the tunnel connection. Moreover, the IPSec framework adds to the L2TP protocol the encryption capabilities for hiding the cleartext payload and a secured way for an automated generation and exchange of cryptographic keys within the tunnel connection.

We have discussed the benefits of using L2TP for cost-effective remote access across the Internet. The shortcomings of that approach are the inherently weak security features of L2TP and the PPP connection that is encapsulated by L2TP. The IETF has therefore recommended to use IPSec to provide protection for the L2TP tunnel across the Internet as well as for the end-to-end traffic inside the tunnel.

Figure 14 illustrates how IPSec can be used to protect L2TP compulsory tunnels between a remote client and a corporate VPN gateway:

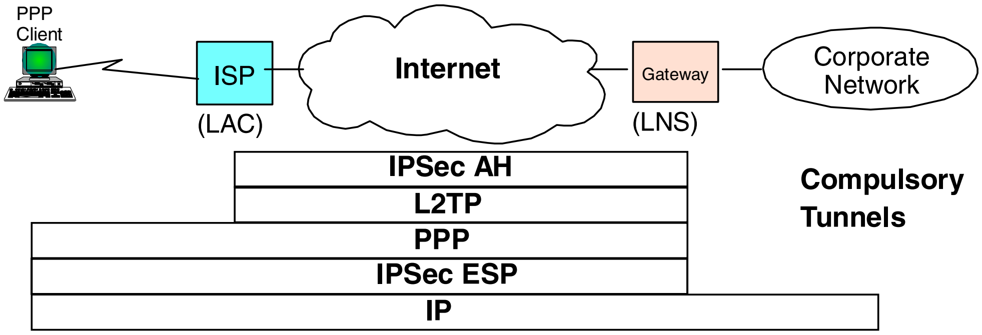


Figure 14. IPSec protection for L2TP compulsory tunnel to VPN gateway

Figure 15 illustrates how IPSec can be used to protect L2TP voluntary tunnels between a remote client and a corporate VPN gateway:

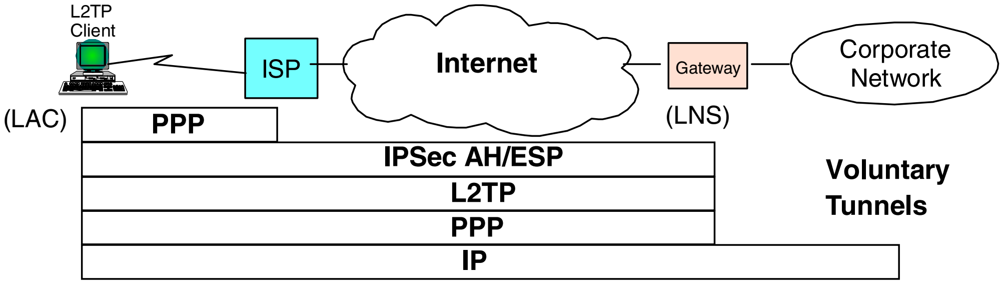


Figure 15. IPSec protection for L2TP voluntary tunnel to VPN gateway

Figure 16 illustrates how IPSec can be used to protect L2TP compulsory tunnels between a remote client and an IPSec-enabled system inside a corporate network:

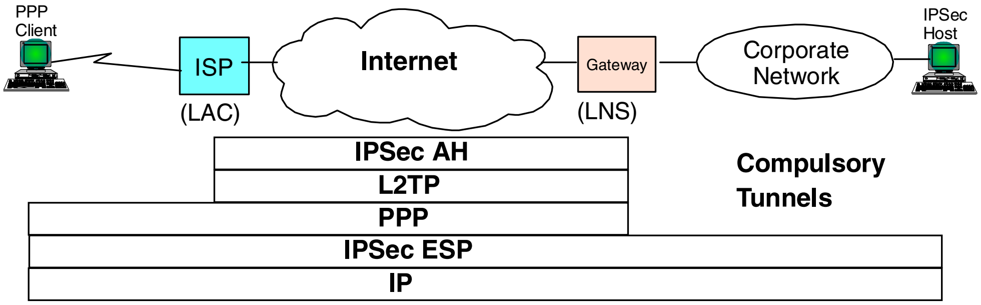


Figure 16. IPSec protection for L2TP compulsory tunnel end-to-end

Figure 17 illustrates how IPSec can be used to protect L2TP voluntary tunnels between a remote client and an IPSec-enabled system inside a corporate network:

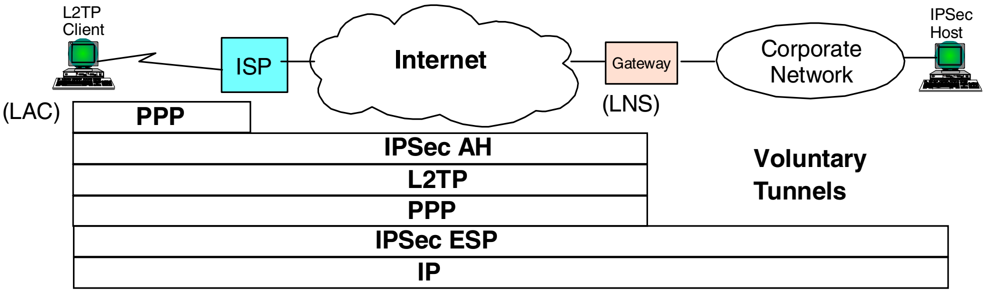


Figure 17. IPSec protection for L2TP voluntary tunnel end-to-end

When planning the use of VPN access in large environments the choice of whether or not to differentiate the functionalities of the corporate firewall, which provides the traditional Internet access from the VPN gateway, should be evaluated to simplify the management and the critical requirement of these resources. If the existing filtering policies are not changed when introducing the IPSec VPN remote access, then the IPSec authentication mechanisms will keep non-VPN traffic from accessing the corporate intranet.

2.1.5 Multiprotocol support

Because L2TP tunnels PPP sessions, any protocol that is supported over PPP can be tunneled by L2TP. Protocols such as SNA, IPX and others are carried as a PPP payload and therefore transparent to L2TP. This makes L2TP a good choice for connecting corporate networks that require multiprotocol support.

2.2 Point-to-Point Tunneling Protocol (PPTP)

One of the more “established” techniques for remote connection is the Point-to-Point Tunneling Protocol (PPTP). PPTP is a vendor solution that meets the requirements for a VPN. It has been implemented by Microsoft on the Windows NT, Windows 98 and Windows 95 (OSR2) platforms.

PPTP is an extension of the basic PPP protocol (see Figure 18). It is due to this fact that PPTP does not support multipoint connections, connections must be point-to-point.

PPTP supports only IP, IPX, NetBIOS and NetBEUI. Because these are the most commonly implemented network protocols, it is rarely an issue, especially for this book as we are concerned with IP network design. However, this must be considered when designing the network, more so when upgrading an existing network.

PPTP does not change the PPP protocol. PPTP only defines a new way, a tunneled way, of transporting PPP traffic.

PPTP is currently being replaced by implementations of L2TP. Microsoft has announced that Windows 2000 will support L2TP. However, some vendors are still developing solutions with PPTP.

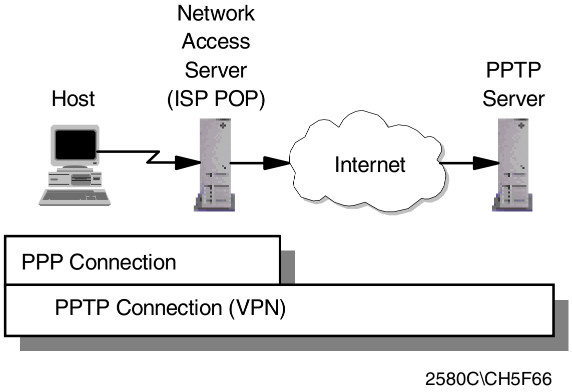


Figure 18. PPTP system overview

PPTP is defined in RFC 2637.

2.3 Layer 2 Forwarding (L2F)

Layer 2 Forwarding (L2F) was developed by Cisco Systems at the same time that PPTP was being developed. It is another protocol that enables remote hosts to access an organization’s intranet through public infrastructure, with security and manageability maintained.

Cisco submitted this technology to the Internet Engineering Task Force (IETF) for approval as a standard, and it is defined in RFC 2341.

As with PPTP, L2F enables secure private network access through public infrastructure by building a “tunnel” through the public network between the client and the host. The difference between PPTP and L2F is that L2F tunneling is not dependent on IP; it is able to work with other network protocols natively, such as frame relay, ATM or FDDI. The service requires only local dial-up capability, reducing user costs and providing the same level of security found in private networks.

An L2F tunnel supports more than one connection, a limitation of PPTP. L2F is able to do this as it defines connections within the tunnel. This is especially useful in situations where more than one user is located at a remote site, only one dial-up connection is required. Alternatively, if tunneling is used only between the POP and the gateway to the internal network, fewer connections are required from the ISP, reducing costs. See Figure 19.

L2F uses PPP for client authentication, as does PPTP, however, L2F also supports TACACS+ and RADIUS for authentication. L2F authentication comprises two levels, first when the remote user connects to the ISP's POP, and then when the connection is made to the organization's intranet gateway.

L2F passes packets through the virtual tunnel between endpoints of a point-to-point connection. L2F does this at the protocol level. A frame from the remote host is received at the POP; the linked framing/transparency bytes are removed. The frame is then encapsulated in L2F and forwarded over the appropriate tunnel. The organization's gateway accepts the L2F frame, removes the L2F encapsulation, and processes the incoming frame. Because L2F is a layer-2 protocol, it can be used for protocols other than IP, such as IPX and NetBEUI.

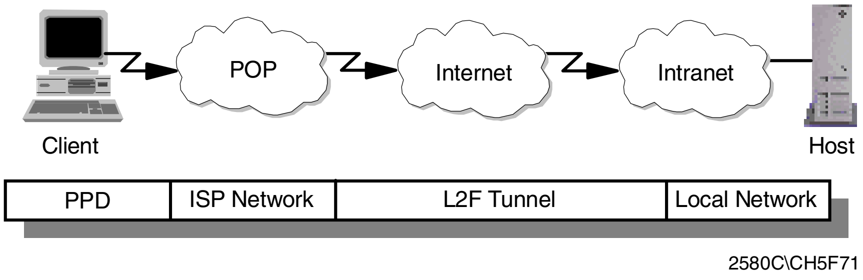


Figure 19. L2F tunnel from POP to intranet gateway

With L2F, a complete end-to-end secure VPN can be created and used. It is a reliable and scalable solution. However, it has shortcomings that are addressed with L2TP.

2.4 Comparing remote access tunneling protocols

The following table provides a quick comparison of the three predominant remote access tunneling protocols, L2TP, PPTP and L2F:

Table 4. Comparing remote access tunneling protocols

Feature	PPTP	L2F	L2TP
Standard/Status	RFC 2637 (informational)	RFC 2341 (informational)	RFC 2661 (standards track)
Carrier	IP/GRE	IP/UDP, FR, ATM	IP/UDP, FR, ATM

Feature	PPTP	L2F	L2TP
Private address assignments	Yes	Yes	Yes
Multiprotocol support	Yes	Yes	Yes
Call types	Incoming and outgoing	Incoming	Incoming and outgoing
Control protocol	Control over TCP Port 1723	Control over UDP Port 1701	Control over UDP Port 1701
Encryption	Microsoft PPP encryption (MPPE)	PPP encryption (MPPE); IPSec optional	PPP encryption (MPPE/ECP); IPSec optional
Authentication	PPP authentication (user)	PPP authentication (user); IPSec optional (packet)	PPP authentication (user); IPSec optional (packet)
Tunnel modes	Typically voluntary tunneling model	Compulsory tunneling model	Compulsory and voluntary models
Multiple calls per tunnel	No	Yes	Yes
PPP multilink support	No	Yes	Yes

2.5 Layer-2 tunneling authentication and encryption

In this section we discuss the options for authentication and encryption that are available with the aforementioned layer-2 tunneling protocols.

2.5.1 Authentication options

Authentication is one of the key requirements for VPNs. The following sections discuss some commonly used remote access authentication techniques and highlight their suitability for VPNs.

2.5.1.1 Password Authentication Protocol (PAP)

PAP was, and maybe still is, the most common authentication protocol for dial-up connection to ISPs. It authenticates the PPP user before a connection can be established, but it sends the user information and password in the clear which makes it entirely unsuitable to VPNs. PAP also authenticates the user only once, at connection establishment. Once connected, a cracker could potentially take over the connection and would not have to worry about further authentication requirements (even though they would be easy to meet with PAP if the cracker already listened in on the original authentication exchange).

2.5.1.2 Challenge Handshake Authentication Protocol (CHAP)

CHAP fixes some of the problems with PAP in that it requires the user and access server to have a shared secret between them. The server challenges the client for identification upon which the client responds with a hashed value (usually using MD5) of the secret. If that matches at the server where the same hash on the presumed secret is performed, the client is authenticated. This effectively avoids having to send cleartext passwords over the line. CHAP also provides for multiple authentication challenges by the server during a connection which makes it harder for crackers to take over. In the case of Microsoft PPTP, the secret shared between the client and the access server is the Windows NT domain password of the user at the client.

2.5.1.3 Microsoft CHAP (MS-CHAP)

MS-CHAP works the same way as CHAP but uses the RSA MD4 or DES hash functions instead of MD5. MD4 is the hash algorithm used by Windows NT as well as Windows 95 and Windows 98 dial-up networking clients for logon verification. DES is used by older Windows dial-up clients. Using MS-CHAP is fine if you have only Microsoft clients but is not supported by any other client platforms. However, it is the required PPP authentication option if you also want to use MPPE encryption (see 2.5.2.1, “Microsoft Point-to-Point Encryption (MPPE)” on page 35).

2.5.1.4 Shiva Password Authentication Protocol (SPAP)

SPAP is a proprietary method for authenticating DIALs clients and some Microsoft clients. It provides a 2-way handshake between client and server with an encrypted password. In some scenarios, SPAP can provide additional functionalities such as callback, change password, and virtual connections.

2.5.1.5 Extensible Authentication Protocol (EAP)

EAP (defined in RFC 2284) provides a more generic way to authenticate a remote user during PPP connection establishment. As opposed to other authentication methods such as PAP and CHAP, EAP is not performed during LCP setup but takes place after LCP has been completed and the PPP authentication phase begins. This allows for more connection parameters to be exchanged that can be used as authentication information. EAP offers a tie-in of back-end authentication servers in a similar way as RADIUS and TACACS, but EAP itself does not provide for authentication mechanisms. To use EAP, existing PPP implementations must be changed.

2.5.1.6 IP Security Architecture (IPSec)

IPSec has two protocols that offer authentication, the Authentication Header (AH) and the Encapsulating Security Payload (ESP) protocols. Both provide authentication per packet as long as a session is active, instead of per user at session establishment or at numerous times during a session. AH and ESP also provide replay protection. This makes IPSec authentication much more secure than traditional PPP authentication options, but it incurs a slightly higher processing overhead at the performing devices. IPSec is the recommended security protocol for L2TP and can be used with L2F and theoretically with PPTP as well. For more information on IPSec AH and ESP, please read 3.1, “IP Security Architecture (IPSec)” on page 37.

2.5.1.7 RADIUS and TACACS

RADIUS and TACACS provide centralized authentication for remote access users. Both technologies work in a similar way: A remote access server implements a RADIUS or TACACS client that forwards authentication requests to a central server where the request is processed and access granted or denied. That provides great flexibility and scalability over large numbers of access servers which is typically required by ISPs and large corporations. RADIUS and

TACACS also allow to pass on configuration information to the client from a central database which is convenient from a management standpoint. RADIUS can optionally be tied into other central authentication systems such as Kerberos, DCE or RACF. More information on RADIUS can be found in Chapter 9, “User authentication for remote access” on page 179.

2.5.1.8 SecureID

SecureID is developed by Security Dynamics, Inc. and is based on the principle of two-factor authentication. A user requires not only a password to authenticate successfully but also a secret PIN code in the form of a random number that changes over time. The password is stored in a database at the server and compared to that entered by a user at logon. The random number is generated at the server for each user and typically changes once every minute. The user is provided with a device in the form of a key chain token or smart card in which a microchip performs the same random number calculations as the server. That chip has a fairly synchronized clock to the server so the user is generally able to log on successfully by entering the password and the PIN that is displayed on the token device. SecureID is based on a client/server model similar to RADIUS and TACACS in that an access server acts as a SecureID client/proxy that forwards authentication requests to the central server called ACE/Server. SecureID can also be used as a secondary authentication system for RADIUS.

2.5.2 Encryption options

Encryption and key-exchange are two of the key requirements for VPNs. In the following sections we discuss some commonly used remote access encryption techniques and highlight their suitability for VPNs.

2.5.2.1 Microsoft Point-to-Point Encryption (MPPE)

MPPE uses the MD4 hash created during MS-CHAP authentication (see 2.5.1.3, “Microsoft CHAP (MS-CHAP)” on page 34) to derive a secret session key for a PPP connection. This is typically used for PPTP with Microsoft clients. The encryption algorithm used by MPPE is RC4 with 40-bit keys, which is considered very weak by the standard of today’s cracking techniques. Microsoft also offers a 128-bit key version for the U.S. market. Microsoft implementations of PPTP refresh a key every 256 packets, though the PPTP standards allow other intervals.

2.5.2.2 Encryption Control Protocol (ECP)

ECP can be used to negotiate encryption for a PPP link once the link is established and authenticated. ECP allows for using different encryption algorithms in each direction, but it does not provide key refresh. The standard encryption algorithm defined in the standard is DES, but vendors are free to implement any algorithm they wish.

2.5.2.3 IPSec

IPSec offers encryption with the Encapsulating Security Payload (ESP) protocols and uses the Internet Key Exchange (IKE) protocol for key generation and refresh. ESP provides encryption per packet as long as a session is active and offers a choice of low, medium, strong and very strong encryption algorithms, ranging from 40-bit DES to 192-bit triple-DES. IKE authenticates the parties that need to exchange secret information based on strong authentication algorithms and also encrypts the key refresh messages. The keys generated by IKE are then used by ESP (and also by AH). ESP optionally provides authentication per packet and replay protection. This makes IPSec encryption much more flexible and secure than traditional PPP authentication options, but it incurs a higher processing overhead at the performing devices. IPSec is the recommended security protocol for L2TP and can be used with L2F and theoretically with PPTP as well. For more information on IPSec AH and ESP, please read 3.1, “IP Security Architecture (IPSec)” on page 37.

Chapter 3. Layer-3 VPN protocols

In this chapter we discuss IPSec, a VPN technology that operates on the network layer, and its supporting component, the Internet Key Exchange (IKE) protocol. Even though IPSec is the architecture that implements layer-3 security and IKE uses an application running at or above layer-5, there is an inherent relationship between the two. IPSec protocols require symmetric keys to secure traffic between peers, but IPSec itself does not provide a mechanism for generating and distributing those keys. This is the role that IKE is playing to support IPSec peers by enabling key management for security associations. IKE, as you will see later, provides security for its own traffic in addition to providing IPSec protocols with the necessary cryptographic keys for authentication and encryption.

3.1 IP Security Architecture (IPSec)

In this section, we provide a brief overview of the Security Architecture for the Internet Protocol (IPSec) because this is the technology upon which the majority of VPN solutions are based, though a more detailed discussion of this topic is already available in *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions*, SG24-5201. This section presents a valuable addition to this redbook because it is based on the latest Internet standards.

3.1.1 Overview and standards

The IP Security Architecture (IPSec) provides a framework for security at the IP layer for both IPv4 and IPv6. By providing security at this layer, higher layer transport protocols and applications can use IPSec protection without the need of being changed. This has turned out to be a major advantage in designing modern networks and has made IPSec one of the most, if not the most attractive technologies to provide IP network security.

IPSec is an open, standards-based security architecture (RFC 2401-2412, 2451) that offers the following features:

- Provides authentication, encryption, data integrity and replay protection
- Provides secure creation and automatic refresh of cryptographic keys
- Uses strong cryptographic algorithms to provide security
- Provides certificate-based authentication
- Accommodation of future cryptographic algorithms and key exchange protocols
- Provides security for L2TP and PPTP remote access tunneling protocols

IPSec was designed for interoperability. When correctly implemented, it does not affect networks and hosts that do not support it. IPSec uses state-of-the-art cryptographic algorithms. The specific implementation of an algorithm for use by an IPSec protocol is often called a transform. For example, the DES algorithm used in ESP is called the ESP DES-CBC transform. The transforms, as the protocols, are published in RFCs and in Internet drafts.

3.1.2 Security associations

The concept of a security association (SA) is fundamental to IPSec. An SA is a unidirectional (simplex) logical connection between two IPSec systems, uniquely identified by the following triple:

```
<Security Parameter Index, IP Destination Address, Security Protocol>
```

The definition of the members is as follows:

Security Parameter Index (SPI) This is a 32-bit value used to identify different SAs with the same destination address and security protocol. The SPI is carried in the header of the security protocol (AH or ESP). The SPI has only local significance, as defined by the creator of the SA. The SPI values in the range 1 to 255 are reserved by the Internet Assigned Numbers Authority (IANA). The SPI value of 0 must be used for local implementation-specific purposes only. Generally the SPI is selected by the destination system during the SA establishment.

IP Destination Address This address may be a unicast, broadcast or multicast address. However, currently SA management mechanisms are defined only for unicast addresses.

Security Protocol This can be either AH or ESP.

An SA can be in either of two modes: transport or tunnel, depending on the mode of the protocol in that SA. You can find the explanation of these protocol modes later in this chapter.

Because SAs are simplex, for bidirectional communication between two IPSec systems, there must be two SAs defined, one in each direction.

An SA gives security services to the traffic carried by it either by using AH or ESP, but not both. In other words, for a connection that should be protected by both AH and ESP, two SAs must be defined for each direction. In this case, the set of SAs that define the connection is referred to as an *SA bundle*. The SAs in the bundle do not have to terminate at the same endpoint. For example, a mobile host could use an AH SA between itself and a firewall and a nested ESP SA that extends to a host behind the firewall.

An IPSec implementation maintains two databases related to SAs:

Security Policy Database (SPD) The Security Policy Database specifies what security services are to be offered to the IP traffic, depending on factors such as source, destination, whether it is inbound, outbound, etc. It contains an ordered list of policy entries, separate for inbound and or outbound traffic. These entries might specify that some traffic must not go through IPSec processing, some must be discarded and the rest must be processed by the IPSec module. Entries in this database are similar to the firewall rules or packet filters.

Security Association Database (SAD) The Security Association Database contains parameter information about each SA, such as AH or ESP algorithms and keys, sequence numbers, protocol mode and SA lifetime. For outbound processing, an SPD entry points to an entry in the SAD. That is, the SPD determines which SA is to be used for a given packet. For inbound processing, the SAD is consulted to determine how the packet must be processed.

Notes:

1. The user interface of an IPSec implementation usually hides or presents these databases in a more friendly way and makes the life of the administrator easier.
2. While IPSec SAs are unidirectional as described above, ISAKMP SAs used by IKE (see 3.2.1, “Overview and standards” on page 45) are essentially bidirectional because an IKE peer can usually act as both initiator or responder. For ISAKMP SAs, the cookies generated by the peers to identify the ongoing exchange are also used as SPI values.

3.1.3 IP Authentication Header (AH)

AH provides origin authentication for a whole IP datagram and is an effective measure against IP spoofing and session hijacking attacks. AH has the following features:

- Provides data integrity and replay protection
- Uses hashed message authentication codes (HMAC), based on shared secrets
- Cryptographically strong but economical on CPU load
- Datagram content is not encrypted
- Does not use changeable IP header fields to compute integrity check value (ICV), which are:
  - TOS, Flags, Fragment Offset, TTL, Checksum

AH adds approximately 24 bytes per packet that can be a consideration for throughput calculation, fragmentation, and path MTU discovery. AH is illustrated in Figure 20:

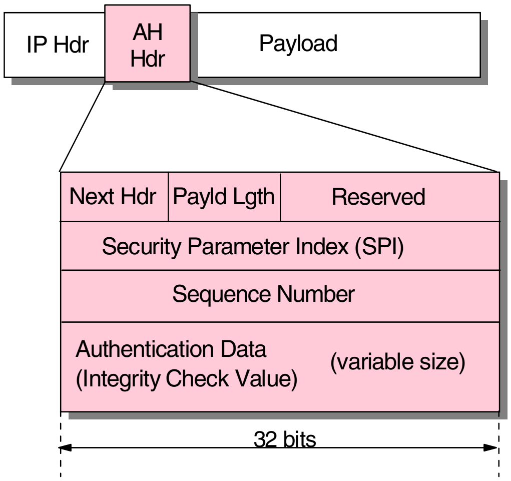


Figure 20. IPSec Authentication Header (AH)

The following transforms are supported with AH:

- Mandatory authentication transforms
  - HMAC-MD5-96 (RFC 2403)
  - HMAC-SHA-1-96 (RFC 2404)
- Optional authentication transforms

- DES-MAC
- Obsolete authentication transforms
  - Keyed-MD5 (RFC 1828)

AH can be used in tunnel or transport mode (see 3.1.5, “Tunnel and transport mode” on page 41) and also in combination with ESP (see 3.1.6, “SA combinations” on page 42).

3.1.4 Encapsulating Security Payload (ESP)

ESP encrypts the payload of an IP packet using shared secrets. The Next Header field actually identifies the protocol carried in the payload. ESP also optionally provides data origin authentication, data integrity, and replay protection in a similar way as AH. However, the protection of ESP does not extend over the whole IP datagram as opposed to AH.

ESP adds approximately 24 bytes per packet that can be a consideration for throughput calculation, fragmentation, and path MTU discovery. ESP is illustrated in Figure 21:

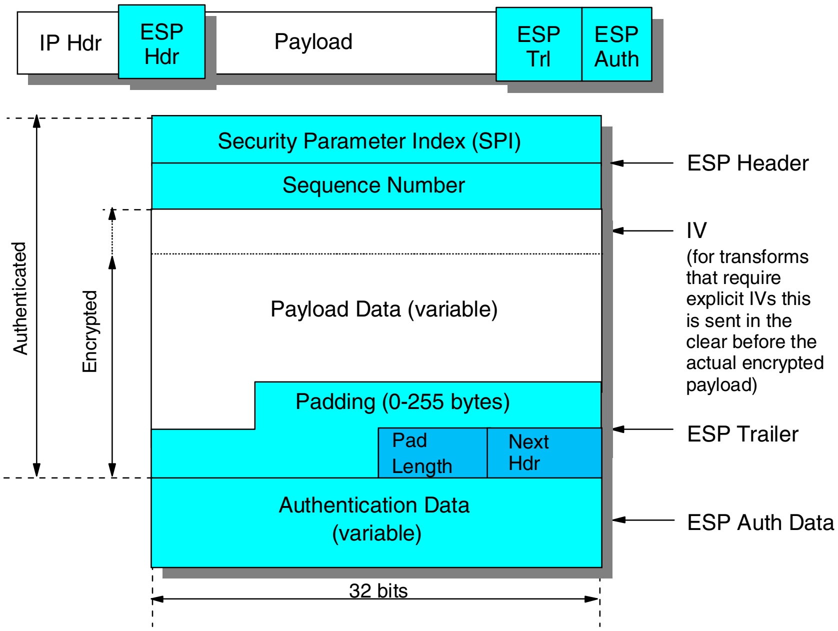


Figure 21. IPSec Encapsulating Security Payload (ESP)

The following transforms are supported with ESP:

- Mandatory encryption transforms
  - DES_CBC (RFC 2405)
  - NULL (RFC 2410)
- Optional encryption transforms
  - CAST-128 (RFC 2451)
  - RC5 (RFC 2451)
  - IDEA (RFC 2451)
  - Blowfish (RFC 2451)
  - 3DES (RFC 2451)

- Mandatory authentication transforms
  - HMAC-MD5-96 (RFC 2403)
  - HMAC-SHA-1-96 (RFC 2404)
  - NULL (RFC 2410)
- Optional authentication transforms
  - DES-MAC

Note: The NULL transform cannot be used for both encryption and authentication at the same time.

ESP can be used in tunnel or transport mode (see 3.1.5, “Tunnel and transport mode” on page 41) and also in combination with AH (see 3.1.6, “SA combinations” on page 42).

3.1.5 Tunnel and transport mode

IPSec protocols can implement security associations in two modes, transport mode and tunnel mode.

3.1.5.1 IPSec transport mode

In transport mode the original IP datagram is taken and the IPSec header is inserted right after the IP header, as it is shown in Figure 22 on page 41. In the case of ESP, the trailer and the optional authentication data are appended at the end of the original payload. If the datagram already has IPSec header(s), then the new header would be inserted before any of those but that is hardly ever the case and it would be better to use tunnel mode.

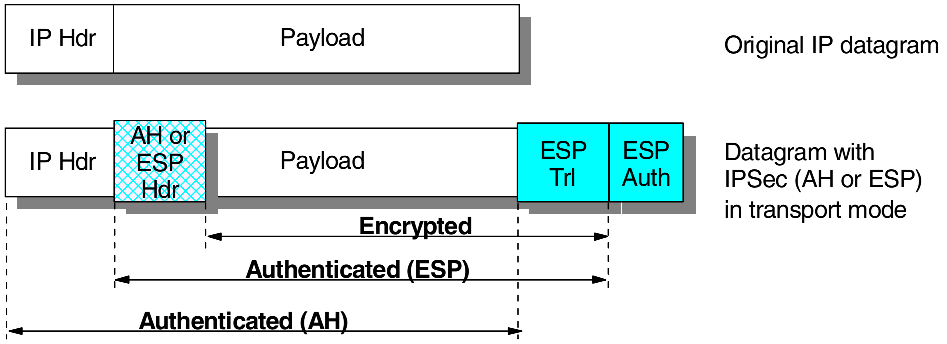


Figure 22. IPSec - transport mode

The transport mode is used by hosts, not by gateways. Gateways are not even required to support transport mode.

The advantage of the transport mode is less processing overhead.

One disadvantage is that the mutable fields are not authenticated. ESP in transport mode provides neither authentication nor encryption for the IP header. This is a disadvantage, since false packets (spoofing attack) might be delivered for ESP processing. Another disadvantage of transport mode is that the addresses of the original IP datagram must be used for delivery. This can be a problem where private IP addresses are used, or where internal addressing structures need to be hidden in the public network.

3.1.5.2 IPSec tunnel mode

With this mode the tunneling concept is applied, which means that a new IP datagram is constructed and the original IP datagram is made the payload of it. Then IPSec in transport mode is applied to the resulting datagram. See Figure 23 on page 42 for an illustration. In the case of ESP, the original datagram becomes the payload data for the new ESP packet, and therefore its protection is total if both encryption and authentication are selected. However, the new IP header is still not protected.

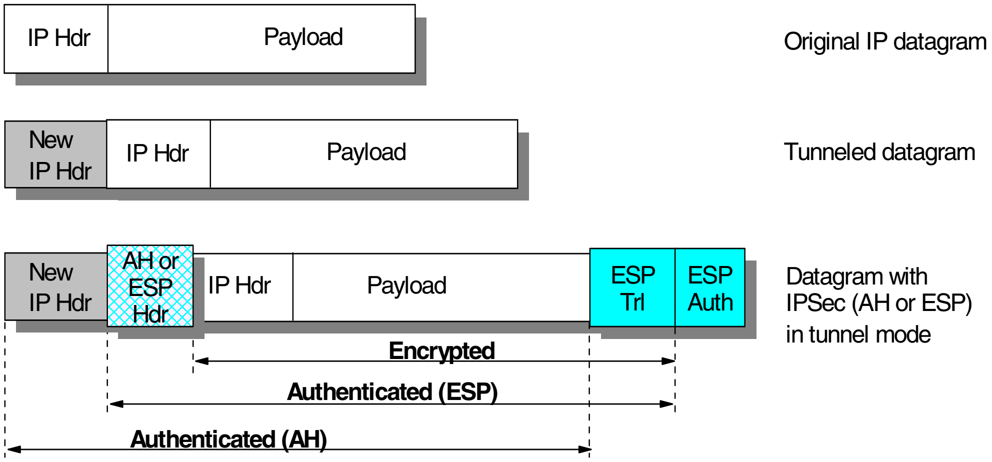


Figure 23. IPSec - tunnel mode

Tunnel mode is used whenever either end of a security association is a gateway. Thus, between two firewalls tunnel mode is always used for traffic that is passing through the firewalls between the secure networks through an IPSec tunnel.

Although gateways are supposed to support tunnel mode only, often they can also work in transport mode. This mode is allowed when the gateway acts as a host, that is, in cases when traffic is destined to itself. Examples are SNMP commands or ICMP echo requests.

In tunnel mode the outer headers' IP addresses do not need to be the same as the inner headers' addresses. For example, two security gateways may operate an AH tunnel which is used to authenticate all traffic between the networks they connect together. This is a very typical mode of operation. Hosts are not required to support tunnel mode, but often they do, and they have to support it for certain remote access scenarios.

The advantages of the tunnel mode are total protection of the encapsulated IP datagram and the possibility of using private addresses. However, there is an extra processing overhead associated with this mode.

3.1.6 SA combinations

The AH and ESP protocols can be applied alone or in combination. Given the two modes of each protocol, there is quite a number of possible combinations. To make things even worse, the AH and ESP SAs do not need to have identical endpoints, so the picture becomes rather complicated. Luckily, out of the many possibilities only a few make sense in real-world scenarios.

Combinations of IPSec protocols are realized with SA bundles and there are two approaches for their creation:

3.1.6.1 Transport adjacency

Both security protocols are applied in transport mode to the same IP datagram. This method is practical for only one level of combination.

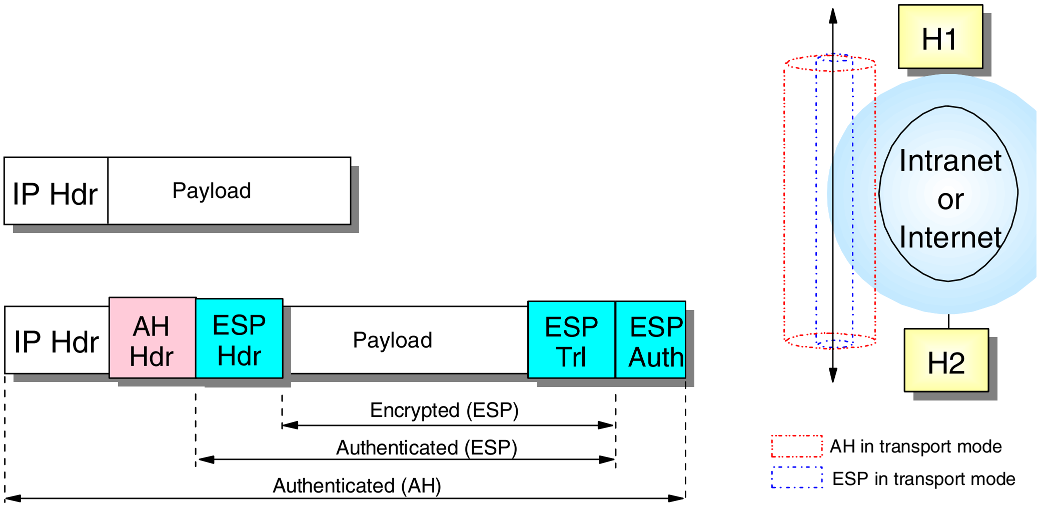


Figure 24. IPSec - transport adjacency

The IPSec standard dictates that transport adjacency can only be used in the way shown above. This means that for outbound packets, encryption (inner SA) has to be performed before authentication (outer SA), whereas for inbound packets authentication has to be performed before encryption. This is a logical sequence and also spares a system the load of decryption in case authentication of the packet fails in the first place.

3.1.6.2 Iterated (nested) tunneling

The security protocols are applied in tunnel mode in sequence. After each application a new IP datagram is created and the next protocol is applied to it. This method has no limit in the nesting levels. However, more than three levels are impractical.

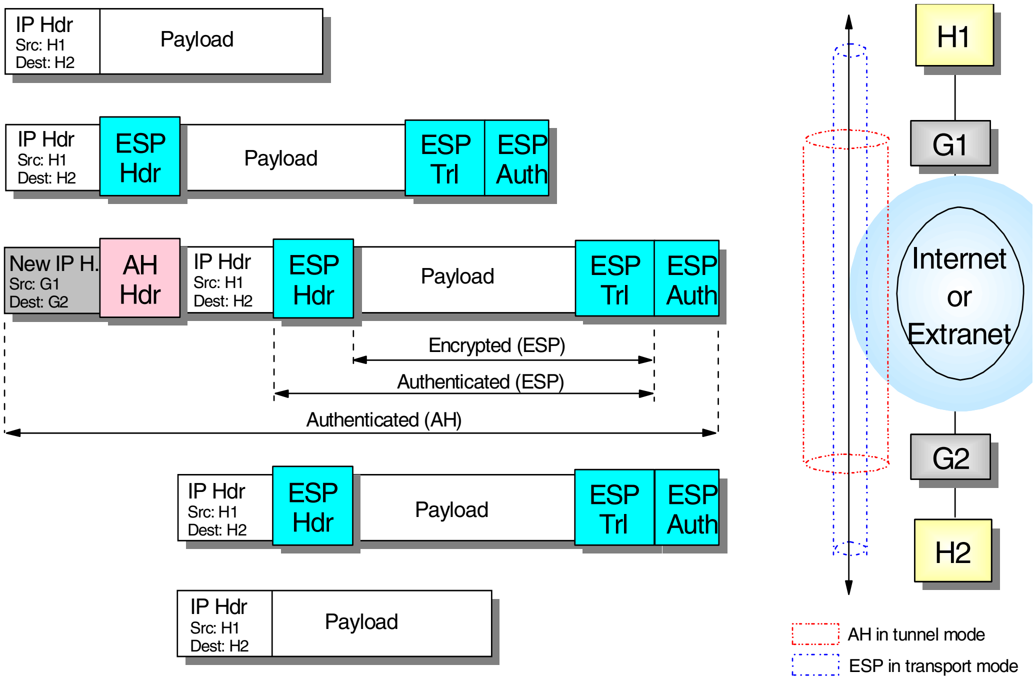


Figure 25. IPSec - iterated tunnels

3.1.6.3 Design considerations

SA bundle approaches can be combined. For example, an IP packet with transport adjacency IPSec headers can be sent through nested tunnels.

When designing a VPN, one should limit the IPSec processing stages applied to a certain packet to a reasonable level. In our view three applications is that limit over which further processing has no benefits. Two stages are sufficient for almost all the cases, and many times even only one stage using ESP with both authentication and encryption will be the level implemented in modern VPNs to reduce processing overhead. In that case, any spoofed packets would eventually fail ESP authentication though they may illegitimately enter the secure network.

Note that to be able to create an SA bundle in which the SAs have different endpoints, at least one level of tunneling must be applied. Transport adjacency does not allow for multiple source/destination addresses, because only one IP header is present. IKE provides for negotiation of such situations by allowing the peers to use different IDs for phase 1 (the outer tunnel) and phase 2 (the end-to-end traffic).

The practical principle of the combined usage is that upon the receipt of a packet with both protocol headers, the IPSec processing sequence should be authentication followed by decryption. It is a common sense decision not to bother with the decryption of packets of uncertain origin. In fact, the IPSec standards prescribe that the sender first apply ESP and then AH to the outbound traffic for transport mode.

As far as the modes are concerned, the usual way is that transport mode is used between the endpoints of a connection and tunnel mode is used between two machines when at least one of them is a gateway.

3.2 Coming to terms with the Internet Key Exchange (IKE) protocol

The following explanations and illustrations of the Internet Key Exchange (IKE) protocol reflect the latest developments.

3.2.1 Overview and standards

Internet Key Exchange (IKE), defined in RFC 2409, is the protocol used to establish security associations that are needed by various services, for example IPSec uses IKE to establish the security associations needed to generate and refresh its keys. To establish security associations, keys need to be formed in a secure and protected manner and IKE provides the mechanism to achieve this.

IKE was originally called ISAKMP/Oakley. Internet Security Association and Key Management Protocol (ISAKMP), defined in RFC 2408, provides the framework to establish security associations and cryptographic keys. The framework is not dependent on any technology and is able to be used with any security mechanism that may be available at the time. Since ISAKMP does not actually define the security mechanism, this is where Oakley, specified in RFC 2412, is used to define the key exchange protocol within ISAKMP.

IKE still uses ISAKMP as its framework but incorporates Oakley and SKEME as its key exchange protocol. IKE does not implement the whole Oakley and SMEME protocol but rather a subset of it.

IKE is made up of two phases as defined in the ISAKMP framework, and within these phases Oakley defines a number of modes that can be used.

Phase 1 is the process where the ISAKMP security association must be established. It assumes that no secure channel currently exists and therefore it must initially establish one to protect any ISAKMP messages. This SA is different from other SAs that are negotiated for other services in that it is owned by ISAKMP.

Phase 2 is where subsequent security associations required by various services are negotiated on their behalf. The ISKMP SA generated in Phase 1 protects all subsequent ISAKMP messages.

Two modes are available for use in Phase 1. Main mode and aggressive mode. Support for main mode is a mandatory requirement for IKE, while aggressive mode is optional. Main mode has the advantage of being able to protect the identities of the parties trying to establish the SA, while quick mode has the advantage of being able to use three rather than six message flows to establish the ISAKMP SA.

Within Phase 2, quick mode is used to negotiate the SAs for the services.

Informational mode is used to give the other party some information, normally abnormal conditions due to failures. For example, if signature verification failed, none of the proposals offered were acceptable or decryption failed. This exchange is normally associated with an SA that was negotiated in Phase 2.

The other mode is new group mode, which is used to negotiate private groups for Diffie-Hellman exchanges. Although protected by a Phase 1 exchange, this is not part of a Phase 2 exchange.

The IKE mechanism is quite efficient in that it is able to negotiate many security associations with relatively few messages. With a single Phase 1 negotiation, multiple Phase 2 negotiations can occur, and within a single Phase 2 negotiation, multiple security associations can be negotiated so an implementation is able to use the same number of message flows to negotiate several security associations as it would need to negotiate one.

3.2.2 Key management requirements for IPSec

The IPSec protocols AH and ESP require that shared secrets are known to all participating parties that require either manual key entry or out-of-band key distribution. The problem is that keys can become lost, compromised or simply expire. Moreover, manual techniques do not scale when there are many security associations to manage (for example, for an extranet VPN). A robust key exchange mechanism for IPSec must therefore meet the following requirements:

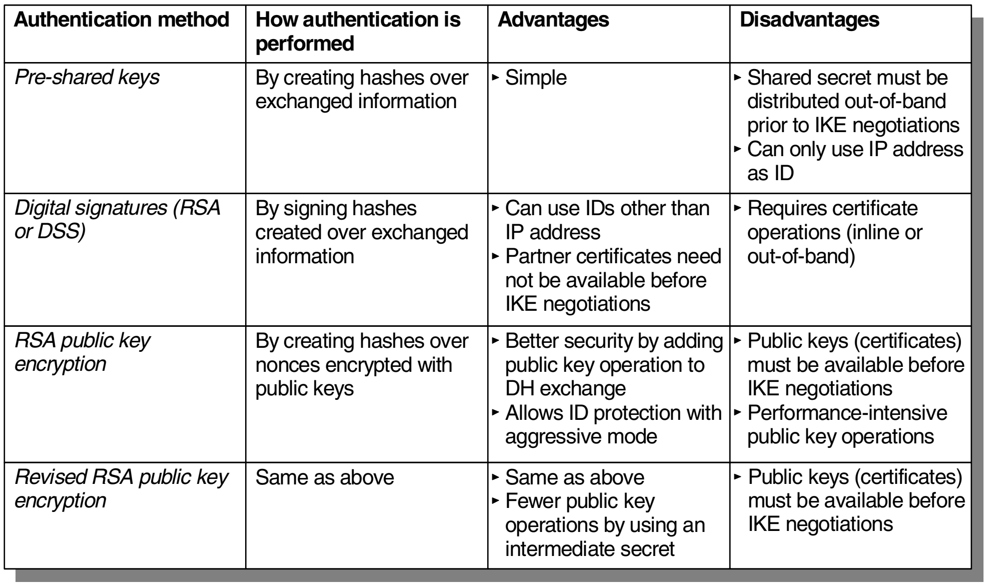
- Independent of specific cryptographic algorithms
- Independent of a specific key exchange protocol
- Authentication of key management entities
- Establish SA over “nonsecured” transport
- Efficient use of resources
- Accommodate on-demand creation of host and session-based SAs

The Internet Key Exchange (IKE) protocol has been designed to meet those requirements. It is based on the Internet Security Associations and Key Management Protocol (ISAKMP) framework and the Oakley key distribution protocol. IKE offers the following features:

- Key generation and identity authentication procedures
- Automatic key refresh
- Solves the “first key” problem
- Each security protocol (that is, AH, ESP) has its own Security Parameter Index (SPI) space
- Built-in protection
  - Against resource-clogging (denial-of-service) attacks
  - Against connection/session hijacking
- Perfect forward secrecy (PFS)
- Two-phased approach
  - Phase 1 - Establish keys and SA for key exchanges
  - Phase 2 - Establish SAs for data transfer
- Implemented as application over UDP, port 500
- Supports host-oriented (IP address) and user-oriented (long-term identity) certificates
- Uses strong authentication for ISAKMP exchanges
  - Pre-shared keys
    - No actual keys are shared, only a token used to create keying material
  - Digital signatures (using either DSS or RSA methods)
  - Public key encryption (RSA and revised RSA)

- For performance reasons revised RSA uses a generated secret key instead of a public/private key during the second Phase 1 exchange.

The differences between those authentication methods is illustrated in Figure 26:



Authentication method	How authentication is performed	Advantages	Disadvantages
Pre-shared keys	By creating hashes over exchanged information	▸ Simple	▸ Shared secret must be distributed out-of-band prior to IKE negotiations ▸ Can only use IP address as ID
Digital signatures (RSA or DSS)	By signing hashes created over exchanged information	▸ Can use IDs other than IP address ▸ Partner certificates need not be available before IKE negotiations	▸ Requires certificate operations (inline or out-of-band)
RSA public key encryption	By creating hashes over nonces encrypted with public keys	▸ Better security by adding public key operation to DH exchange ▸ Allows ID protection with aggressive mode	▸ Public keys (certificates) must be available before IKE negotiations ▸ Performance-intensive public key operations
Revised RSA public key encryption	Same as above	▸ Same as above ▸ Fewer public key operations by using an intermediate secret	▸ Public keys (certificates) must be available before IKE negotiations

Figure 26. Comparing IKE authentication methods

As mentioned before, IKE requires two phases be completed before traffic can be protected with AH and/or ESP.

3.2.3 IKE Phase 1 overview

During Phase 1, the partners exchange proposals for the ISAKMP SA and agree on one. This contains specifications of authentication methods, hash functions and encryption algorithms to be used to protect the key exchanges. The partners then exchange information for generating a shared master secret:

- Cookies that also serve as SPIs for the ISAKMP SA
- Diffie-Hellman values
- Nonces (random numbers)
- Optionally exchange IDs when public key authentication is used

Both parties then generate keying material and shared secrets before exchanging additional authentication information.

Note: When all goes well, both parties derive the same keying material and actual encryption and authentication keys without ever sending any keys over the network.

3.2.4 IKE Phase 2 overview

During Phase 2, the partners exchange proposals for Protocol SAs and agree on one. This contains specifications of authentication methods, hash functions and encryption algorithms to be used to protect packets using AH and/or ESP. To generate keys, both parties use the keying material from a previous Phase 1 exchange and they can optionally perform an additional Diffie-Hellman exchange for PFS.

The Phase 2 exchange is protected by the keys that have been generated during Phase 1, which effectively ties a Phase 2 to a particular Phase 1. However, you can have multiple Phase 2 exchanges under the same Phase 1 protection to provide granular protection for different applications between the same two systems. For instance, you may want to encrypt FTP traffic with a stronger algorithm than Telnet, but you want to refresh the keys for Telnet more often than those for FTP.

Systems can also negotiate protocol SAs for third-parties (proxy negotiation) which is used to automatically create tunnel filter rules in security gateways.

3.2.5 ISAKMP message structure

ISAKMP defines a very flexible method of building messages which can be adapted to almost any type of service, not just IPSec. ISAKMP messages are very modular in that all components are contained in various types of payloads. Currently there are 14 payload types defined:

- Security Association Payload
- Proposal Payload
- Transform Payload
- Key Exchange Payload
- Identification Payload
- Certificate Payload
- Certificate Request Payload
- Hash Payload
- Signature Payload
- Nonce Payload
- Notification Payload
- Notify Message Payload
- Delete Payload
- Vendor ID Payload

These payloads are the basic building blocks of an ISAKMP message. Each payload has a generic header indicating what the next payload is and the length of the payload. This gives the ability to chain payloads together and to nest payloads within another payload.

The following example shows the payload structure of message 1 of an aggressive mode exchange with pre-shared keys where two transforms are proposed.

ISAKMP Header

> SA Payload, (next payload = Key Exchange Payload)
>
> > Proposal Payload, (next payload = none)

Transform Payload, (next payload = Transform Payload)

Transform Payload, (next payload = none)

Key Exchange Payload, (next payload = Nonce Payload)

Nonce Payload, (next payload = Identification Payload)

Identification Payload, (next payload = none)

In addition to the payloads there is the ISAKMP Header which has the cookies to protect against denial-of-service attacks, the exchange type to indicate what type of flow is occurring (aggressive mode, for example), and a message ID to uniquely identify the message against an SA negotiation.

Payloads may also require certain attributes to be defined, and ISAKMP defines how data attributes are to be formatted within the payload.

How these payloads are coded or formatted are dependent on the services using ISAKMP. These definitions are known as the Domain of Interpretation (DOI) and also contain, for example, exchange types and naming conventions. Therefore, if IPSec is the service being used the IPSEC DOI for ISAKMP defines how the payloads are coded.

In conjunction with the DOI there is also the concept of a situation. A situation allows a device to make policy decisions with regard to security services that are being negotiated. For example, the IPSec DOI defines three situations:

- Identity only
- Secrecy
- Integrity

The DOI is documented in RFC 2407. The detailed specifications of the protocol structures and message constructs are useful for implementors of IKE software as well as for system administrators who have to debug IKE errors. To discuss the details of this specification would be far beyond the scope of this document and you are therefore kindly referred to study the RFC on this subject.

3.2.6 General Phase 1 process

As described earlier, during this phase the ISAKMP SA is established, which provides a secure mechanism for subsequent ISAKMP messages to flow. This phase assumes no protection whatsoever and must establish a secure and private channel where no privacy currently exists.

The objective of this phase is to establish keying material which can be used to derive keys that encrypt and authenticate ISAKMP messages, and to derive keys that will be used for non-ISAKMP security associations. In addition to this, Phase 1 also authenticates the two parties involved in the exchange.

There are four methods of authentication available (see Figure 26 on page 47):

1. Digital signatures
2. Public key encryption
3. Revised public key encryption
4. Pre-shared keys

During Phase 1 only a single SA is negotiated, that is the ISAKMP SA. Only one proposal is offered always proposing Oakley as the key exchange method. Within that proposal multiple transforms can be offered which negotiate the following parameters:

- Authentication method
- Lifetime/lifesize of the SA
- Diffie-Hellman group
- Hash algorithm
- Encryption algorithm

Using main mode there are basically six message flows:

In the first two messages a proposal is offered by the initiator with one or more transforms, and the responder accepts the proposal with the chosen transform. Additionally, cookies are generated to incorporate into the ISAKMP header. The cookies ensure protection against denial of service attacks and the pair of cookies (the initiator's cookie and responder's cookie) identify the ISAKMP SA.

During the next two messages an exchange occurs as a Diffie-Hellman key exchange along with some nonces. After these two messages each party now has the keying material to generate keys for encryption and authentication of subsequent ISAKMP messages. Keying material is also derived which will be used to generate keys for other non-ISAKMP SAs in Phase 2. All ISAKMP messages from this point are then encrypted.

In the last two messages of Phase 1 authentication occurs. Depending on the chosen authentication method the appropriate messages and identities are exchanged here so that each party can authenticate the other.

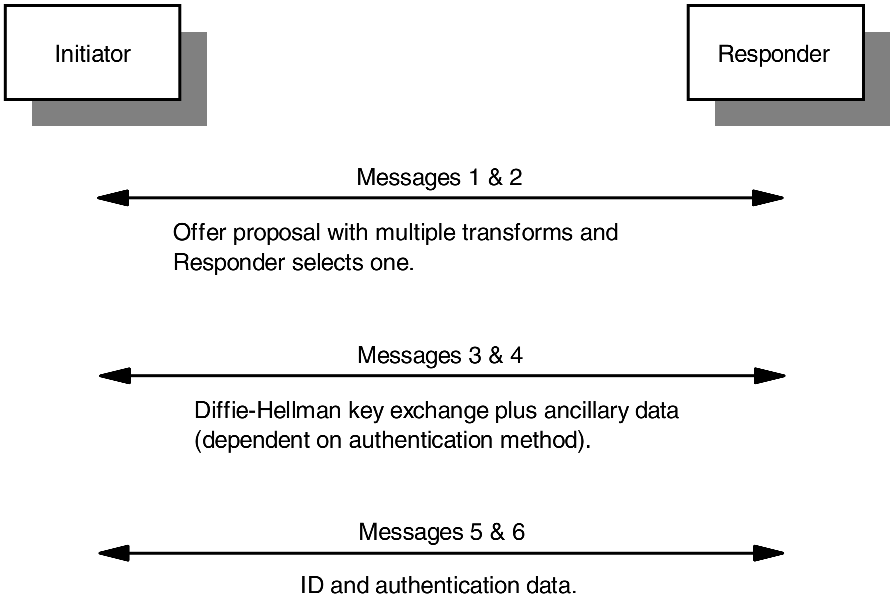

Initiator
Responder
Messages 1 & 2
Offer proposal with multiple transforms and Responder selects one.
Messages 3 & 4
Diffie-Hellman key exchange plus ancillary data (dependent on authentication method).
Messages 5 & 6
ID and authentication data.

Figure 27. Basic Phase 1 main mode flows

In aggressive mode only a total of three messages are needed to establish the SA, however, the identities of the parties involved are revealed.

In the first message the initiator sends the proposal, Diffie-Hellman key exchange, nonce and ID to the responder.

At this point the responder can generate its nonce and Diffie-Hellman key exchange, and in conjunction with what he has just received from the initiator has all the components to generate the keying material. The responder on the second messages also sends the same information to the initiator so that he can generate the keying material, but also attaches the information to be able to authenticate him.

When the initiator receives the second message he is able to generate the keying material and authenticate the responder. All that is required no is for the responder to authenticate the initiator. To achieve this the initiator sends the last Phase 1 message to the responder containing information that will enable the responder to authenticate the initiator.

As with main mode, the information that is exchanged to facilitate authentication is dependent on the negotiated authentication method.

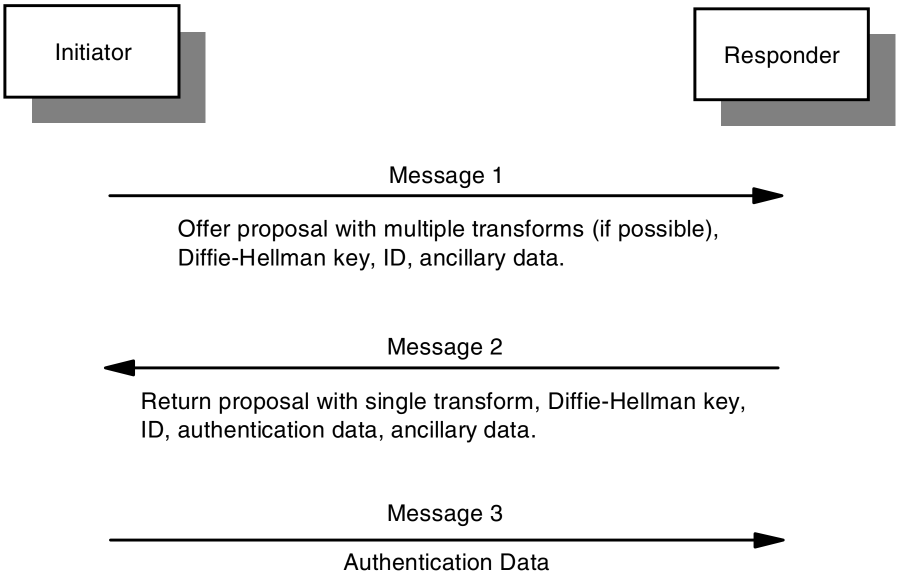

Initiator
Responder
Message 1
Offer proposal with multiple transforms (if possible),
Diffie-Hellman key, ID, ancillary data.
Message 2
Return proposal with single transform, Diffie-Hellman key,
ID, authentication data, ancillary data.
Message 3
Authentication Data

Figure 28. Basic Phase 1 aggressive mode flows

Note

The convention used in this chapter describes the information that is transferred or used in a particular function. Therefore, the same identifier used in this book may represent both the payload in one area or the actual value in another area.

For example, when a Diffie-Hellman public key is transferred, a Key Exchange payload containing the Diffie-Hellman public value is actually passed in the message, or when a nonce is transferred, a Nonce Payload containing the nonce is actually passed.

In the examples which show the inputs to a pseudo-random function, the actual value rather than the payload is normally used. For example, the actual value of a nonce is used as an input rather than the Nonce Payload with its associated headers.

Although the actual payload and information are strictly different entities, this chapter identifies them in the same way for readability. For example, an initiator's nonce contained in a nonce payload is identified in the same way as the actual value being used as an input to a pseudo-random function, that is, $\text{Nonce}_{\text{initiator}}$.

3.2.6.1 Derivation of keying material

In all message flows keying material and hashing methods must be derived. The only difference is the algorithm that is used.

In main mode the keying material is derived after the exchange of messages 3 and 4, while the hash is used in the authentication process at messages 5 and 6. In aggressive mode the responder is able to derive the keying material after the receipt of message 1, and the initiator after the receipt of message 2. The hash is used in the authentication which is used in message 2 and message 3.

When deriving keys and authenticating, a pseudo-random function is used. It generates a deterministic output which appears pseudo random. Potentially the pseudo-random function could be negotiated, but the current standard does define it. As such the HMAC version of the negotiated hash function is used, for example, HMAC-MD5. The function has two inputs, the key and message and is written in the form prf(key, message).

A value called SKEYID needs to be generated which is derived in different ways depending on the keying authentication method. This value is a string derived from secret information established during the exchange and is used to derive additional keying material. The following lists how SKEYID is determined for the different authentication methods:

- Digital signatures

  $\text{prf}(\text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}}, \text{DH}_{\text{shared\_secret}})$

  The pseudo-random function is applied using concatenation of the nonces as the key, and the Diffie-Hellman shared secret as the message.

- Public key encryption

  $\text{prf}(\text{hash}(\text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}}), \text{Cookie}_{\text{initiator}} + \text{Cookie}_{\text{responder}})$

The pseudo-random function is applied using a hash of the concatenation of the nonces as the key, and the concatenation of the cookies as the message. The hash function used here is the negotiated hash function in the SA.

- Pre-shared keys

  prf(pre-shared-key, $\text{Nonce}_{\text{initiator}}$ + $\text{Nonce}_{\text{responder}}$)

  The pseudo-random function is applied using the pre-shared key as the key and the concatenation of the nonces as the message.

Once SKEYID has been derived the keying material can then be derived. Three sets of keying material are derived:

1. SKEYID_d. This is the keying material used to derive keys material for non-ISAKMP security associations, IPSec, for example. It is derived from the application of the pseudo random in the following manner:

   prf(SKEYID, $\text{DH}_{\text{shared\_secret}}$ + $\text{Cookie}_{\text{initiator}}$ + $\text{Cookie}_{\text{responder}}$ + 0)

   The pseudo-random function is applied using SKEYID as the key and the concatenation of the Diffie-Hellman shared secret, the two cookies and the single octet value “0”.

2. SKEYID_a. This is keying material used by ISAKMP to generate keys to authenticate its messages. It is derived from the application of the pseudo random in the following manner:

   prf(SKEYID, SKEYID_d + $\text{DH}_{\text{shared\_secret}}$ + $\text{Cookie}_{\text{initiator}}$ + $\text{Cookie}_{\text{responder}}$ + 1)

   The pseudo-random function is applied using SKEYID as the key and the concatenation of the SKEYID_d, the Diffie-Hellman shared secret, the two cookies and the single octet value “1”.

3. SKEYID_e. This is keying material used by ISAKMP to generate keys to encrypt its messages. It is derived from the application of the pseudo random in the following manner:

   prf(SKEYID, SKEYID_a + $\text{DH}_{\text{shared\_secret}}$ + $\text{Cookie}_{\text{initiator}}$ + $\text{Cookie}_{\text{responder}}$ + 2)

   The pseudo-random function is applied using SKEYID as the key and the concatenation of the SKEYID_d, the Diffie-Hellman shared secret, the two cookies and the single octet value “2”.

How the keying material is used to derive the actual keys is dependent on the encryption algorithm that is being used. Detailed information can be found in the appropriate RFCs, however, an example will be described here. The encryption key used to encrypt ISAKMP messages using DES-CBC is derived from the first 8 bytes of SKEYID_e. The initialization vector that is to be used with the encryption (for use in protecting Phase 1 messages) is derived from a hash of the concatenation of the initiator’s public Diffie-Hellman value and responder’s public Diffie-Hellman value, using the negotiated hash function, that is:

hash($\text{DH}_{\text{initiator\_public\_value}}$ + $\text{DH}_{\text{responder\_public\_value}}$)

3.2.6.2 Derivation of hashes for authentication

During the authentication process the initiator and responder have to derive hash values. The initiator needs to derive the value HASH_I by:

$$prf(SKEYID, DH_{initiator\_public\_value} + DH_{responder\_public\_value} + Cookie_{initiator} + Cookie_{responder} + SA_{initiator} + ID_{initiator})$$

This is the application of the pseudo-random function using SKEYID as the key and the concatenation of: the initiator's Diffie-Hellman public value, the responder's Diffie-Hellman public value, the initiator's cookie, the responder's cookie, the whole SA payload (including all proposals and transforms) that was offered originally by the initiator and the complete ID payload of the initiator; as the message.

The responder needs to derive the value HASH_R by:

$$prf(SKEYID, DH_{responder\_public\_value} + DH_{initiator\_public\_value} + Cookie_{responder} + Cookie_{initiator} + SA_{initiator} + ID_{responder})$$

This is the application of the pseudo-random function using SKEYID as the key and the concatenation of: the responder's Diffie-Hellman public value, the initiator's Diffie-Hellman public value, the responder's cookie, the initiator's cookie, the whole SA payload (including all proposals and transforms) that was offered originally by the initiator and the complete ID payload of the initiator; as the message.

How HASH_I and HASH_R are used for authentication is dependent on the authentication process. If digital signatures are used, HASH_I and HASH_R are signed, and that signature is passed to the other party to be verified. While using public key encryption and pre-shared keys, the respective hash values are produced and passed to the other party where it is verified. Production of the correct hash value directly authenticates the other party in the public key encryption and pre-shared key authentication methods.

A more detailed description of the IKE Phase 1 and Phase 2 message flows is provided in the redbook *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*, SG24-5309.

3.2.7 General Phase 2 process

Phase 2 is where the SA is negotiated on behalf of other services, for example, IPSec. It requires that Phase 1 be successfully completed since it uses the ISAKMP SA established in Phase 1 to protect all Phase 2 messages.

The objective of this phase is to refresh keying material established in Phase 1, which can be used to derive keys needed required by the service. For example, these keys could be used to encrypt and authenticate messages.

Although perfect forward security (PFS) must be supported, it is optional as to whether it will be used. If PFS is required another Diffie-Hellman exchange is performed to achieve this.

Phase 2 can negotiate multiple security associations in a single exchange. This is achieved by incorporating multiple SA payloads into the message.

In each of the three messages a different hash is passed to guarantee the two parties' identities. Nonces are exchanged in messages 1 and 2, and the Diffie-Hellman exchange occurs in messages 1 and 2 if PFS is required. Additionally, the SA is also offered in message 1, and the chosen proposal is returned in message 2.

The IDs of the negotiated SA in Phase 2 are normally the IP addresses of the ISAKMP peers, and therefore, IDs do not need to be exchanged. There may be cases where ISAKMP is acting as a client negotiator on behalf of another party. In these situations the identities of the other parties must be passed in the exchange as shown above in messages 1 and 2 ($\text{ID\_Client}_{\text{initiator}}$ and $\text{ID\_Client}_{\text{responder}}$). This would normally be the case for IPSec in gateway implementations since the services that wants the IPSec security are the various IP addresses and subnets attached to the routers.

Although PFS must be supported it is not mandatory that it be used. If PFS is not required the flows are the same except the key exchange payloads carrying the temporary Diffie-Hellman public values in messages 2 and 3 are not exchanged.

PFS is achieved by incorporating a temporary Diffie-Hellman exchange. It is important that the Diffie-Hellman values that are generated are strictly temporary and only exist during this exchange. The value generated here must have absolutely no relationship with other Diffie-Hellman values in other exchanges, for example, the Diffie-Hellman values used during Phase 1.

During the flows three different hash values are derived to authenticate the exchange:

- Hash_1

  prf(SKEYID_a, Message_ID + Everything_after_Hash_1_in_ Message_1)

  The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message ID and everything after Hash_1 in message 1, as the message.

- Hash_2

  prf(SKEYID_a, Message_ID + $\text{Nonce}_{\text{initiator}}$ + Everything_after_Hash_2_in_ Message_2)

  The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the Message ID, initiator's nonce and everything after Hash_2 in message 2, as the message.

- Hash_3

  prf(SKEYID_a, 0 + Message_ID + $\text{Nonce}_{\text{initiator}}$ + $\text{Nonce}_{\text{responder}}$)

  The pseudo-random function is applied using SKEYID_a as the key and a concatenation of the single octet value "0", the Message ID, the initiator's nonce and the responder's nonce, as the message.

SKEYID_a was generated during Phase 1 as described in 3.2.6.1, "Derivation of keying material" on page 52. The message ID is a unique identifier generated by the initiator during Phase 2 negotiations and is contained in the ISAKMP header. *Everything_atfer_Hash_x_in_Message_x* includes the Diffie-Hellman key exchange payload and client identity payloads if they exist.

The keying material that is derived for the SA being negotiated in Phase 2 if PFS was not required is:

prf(SKEYID_d, Protocol + SPI + $\text{Nonce}_{\text{initiator}}$ + $\text{Nonce}_{\text{responder}}$)

The pseudo-random function is applied using SKEYID_d as the key and a concatenation of the Protocol, the SPI, the initiator's nonce and the responder's nonce, as the message.

The keying material that is derived for the SA being negotiated in Phase 2 if PFS was required is:

$\text{prf}(\text{SKEYID\_d}, \text{DH\_Temp}_{\text{shared\_secret}} + \text{Protocol} + \text{SPI} + \text{Nonce}_{\text{initiator}} + \text{Nonce}_{\text{responder}})$

The pseudo-random function is applied using SKEYID_d as the key and a concatenation of the temporary Diffie-Hellman shared secret, the Protocol, the SPI, the initiator's nonce and the responder's nonce, as the message.

The Protocol is carried in the proposal payload and indicates the protocol being negotiated, for example, IPSec ESP. The security parameter index (SPI) is a locally generated number, also carried in the proposal payload, that identifies the SA. Note that in a single SA negotiation, two SAs are generated, one for each direction, which implies two SPIs. Therefore, there are also two keys that are generated, one for each direction. The keying material for each side will differ for each side of the SA because a different SPI value will be used in the pseudo-random function. The SA from the initiator to responder will use the SPI generated by the responder, while the SA from the responder to the initiator will use the SPI generated by the initiator.

3.2.8 Summary of successful IKE negotiation

Once Phase 1 and Phase 2 exchanges have successfully completed, the peers have reached a state where they can start to protect traffic with IPSec according to applicable policies and traffic profiles. They have done all of the following:

1. Agreed on a proposal to authenticate each other and to protect future IKE exchanges
2. Exchanged enough secret and random information to create keying material for later key generation
3. Mutually authenticated the exchange
4. Agreed on a proposal to authenticate and protect data traffic with IPSec
5. Exchanged further information to generate keys for IPSec protocols
6. Finally confirmed the exchange and generated all necessary keys

This is illustrated in Figure 29 on page 57.

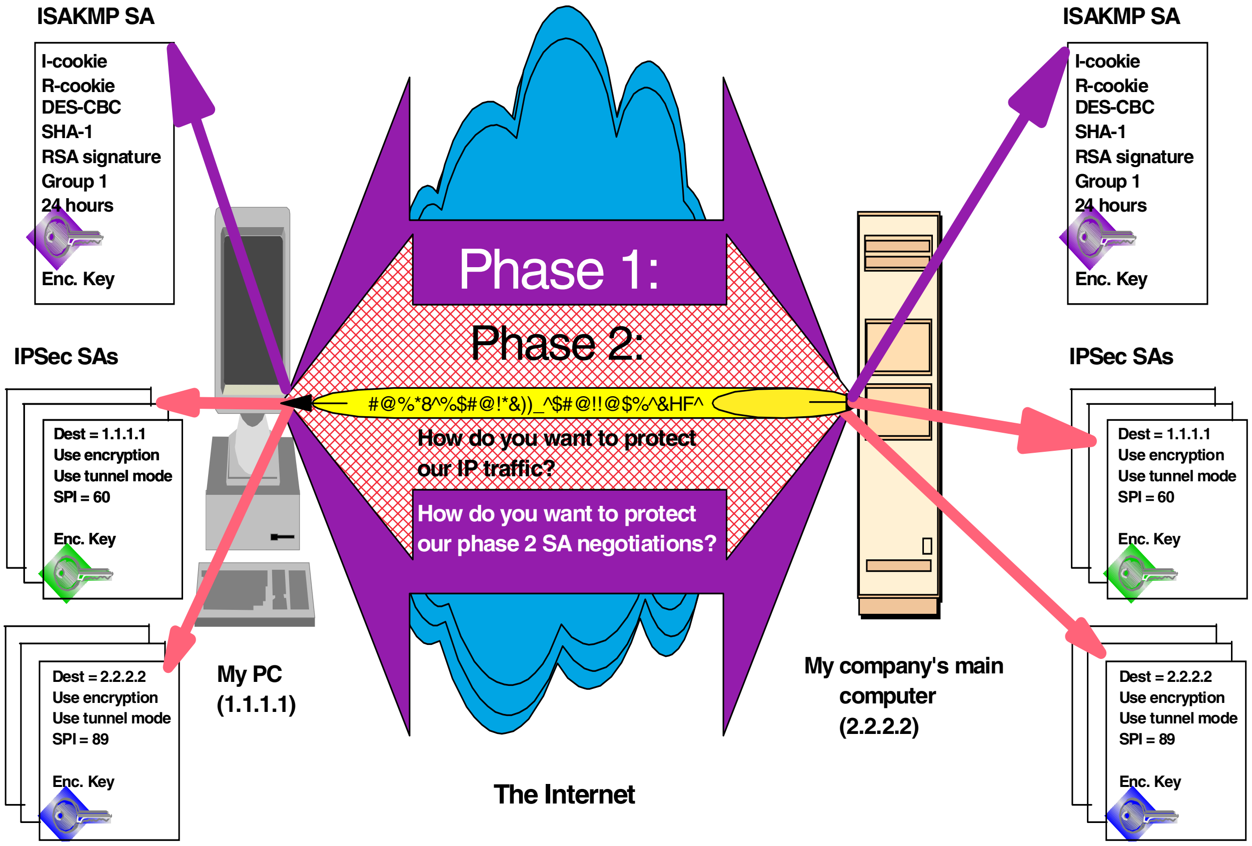


Figure 29. IKE negotiation summary

3.3 IPSec/IKE system processing

It is important to understand how systems process datagrams when it comes to using IPSec and IKE. With IP security in place, datagrams can no longer be simply processed, forwarded or discarded but must be subject to a security policy to determine if additional IPSec processing is required and when it has to occur. Even though there are slight differences among platforms as to how they implement IPSec on their particular IP stacks, the general principle of IPSec processing for host and gateway systems can be summarized as follows:

3.3.1 Outbound IPSec processing for host systems

With IPSec active, any outbound packet is subject to the security policy database (SPD) to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the security associations database (SAD) is searched for an existing security association (SA) for which the packet matches the profile. If that is not the case and IKE as well as on-demand outbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of the desired SA(s) for this packet. Finally, IPSec is applied to the packet as required by the SA and the packet is delivered. This process is illustrated in Figure 30 on page 58.

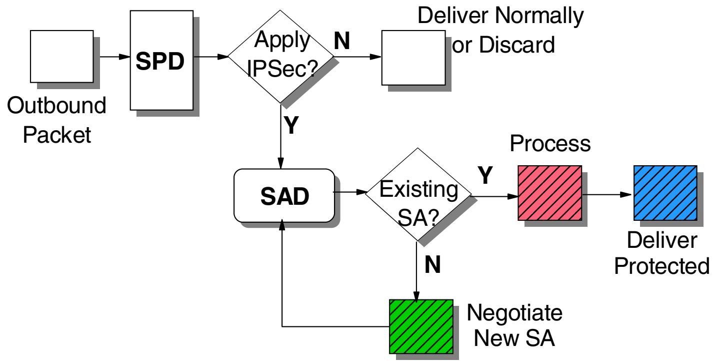


Figure 30. IPSec - outbound processing for host systems

Note

In general, the routing table is consulted to determine if the packet can be delivered at all. If no route is found, IPSec processing should not be performed but the user should be informed instead of this problem.

We are assuming, however, that host systems usually have a default router defined so that packets get sent in any case.

3.3.2 Inbound processing for host systems

With IPSec active, any inbound packet is subject to the SPD to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the SAD is searched for an existing security parameter index (SPI) to match the SPI value contained in the packet. If that is not the case, there are essentially two options:

1. Silently discard the packet (do not inform the sender but log the event if configured). This is the default action performed by most of today's IPSec implementations.
2. If IKE as well as on-demand inbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of SA(s) to the sender of the original packet. In this case, it does not matter if the original packet was IPSec protected or in the clear, which would only depend upon the local policy. However, it requires that the sender of the original packet respond to the IKE negotiations, and it would mean that packets were discarded until an SA is established.

Finally, IPSec is applied to the packet as required by the SA and the payload is delivered to the local process. This is illustrated in Figure 30 on page 58.

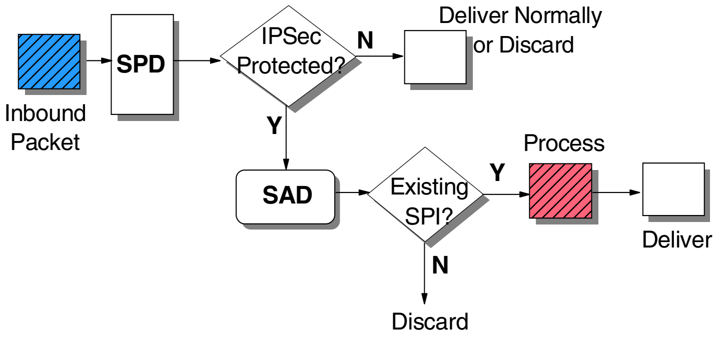


Figure 31. IPSec - inbound processing for host systems

3.3.3 Outbound processing for gateway systems

On a gateway system, any outbound packet is usually subject to the SPD of the secure interface to determine what to do with it. If the decision is to route the packet, the routing table is consulted to determine if the packet can be delivered at all. If no route is found, IPSec processing should not be performed, but the original sender may be informed instead of this problem using ICMP network unreachable messages.

We are assuming, however, that gateway systems either employ routing protocols or have a default router defined so that a successful routing decision can be made.

From this stage on, processing is essentially the same as on host systems. The packet is then forwarded to the SPD of a non-secure interface to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the SAD is searched for an existing SA for which the packet matches the profile. If that is not the case and IKE as well as on-demand outbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of the desired SA(s) for this packet. Finally, IPSec is applied to the packet as required by the SA and the packet is delivered. This process is illustrated in Figure 30 on page 58.

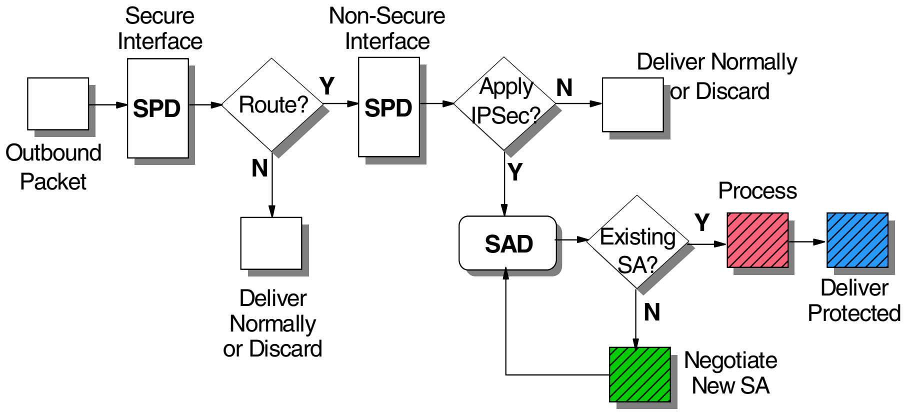


Figure 32. IPSec - outbound processing for gateway systems

3.3.4 Inbound processing for gateway systems

On a gateway system with IPSec active, any inbound packet is subject to the SPD to determine if IPSec processing is required or what else to do with the packet. If IPSec is required, the SAD is searched for an existing SPI to match the SPI value contained in the packet. If that is not the case, there are essentially two options:

1. Silently discard the packet (do not inform the sender but log the event if configured). This is the default action performed by most of today's IPSec implementations.
2. If IKE as well as on-demand inbound SAs are supported, a new IKE negotiation is started that ultimately results in the establishment of SA(s) to the sender of the original packet. In this case, it does not matter if the original packet was IPSec protected or in the clear, which would only depend upon the local policy. However, it requires that the sender of the original packet respond to the IKE negotiations, and it would mean that packets were discarded until an SA is established.

Once the packet has been successfully processed by IPSec, which may be an iterative process for SA bundles, a routing decision has to be made as to what to do with the packet next. If the packet is destined to another host it is delivered over the appropriate interface according to the routing tables. If the packet is destined to the gateway itself, the payload is delivered to the local process. This is illustrated in Figure 30 on page 58.

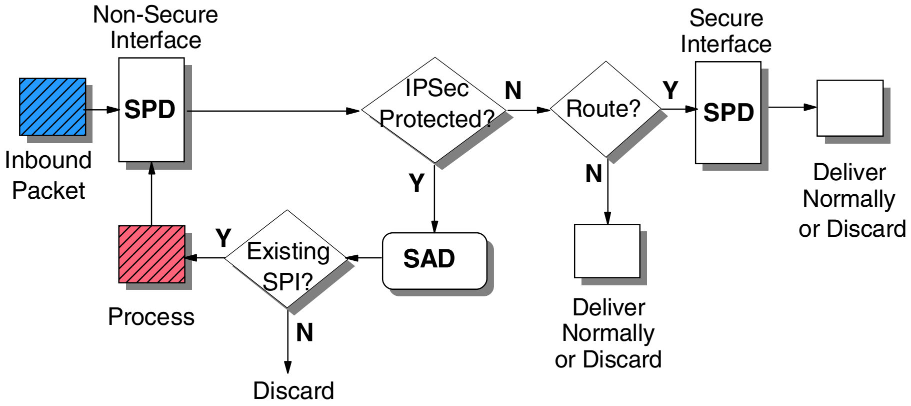


Figure 33. IPSec - inbound processing for gateway systems

Note

If the gateway receives a packet with IPSec applied in an iterated tunnel SA bundle, it only has to process the outer SA which is carried in a datagram destined to the gateway. The inner SA is carried in a datagram destined to another host and will therefore be forwarded by the gateway (provided the policy permits it), irrespective of its IPSec protection.

Chapter 4. Addressing and routing

An essential step in planning and designing VPNs is the provision for IP addressing and routing schemes that take into account that the backbone network is a public network where global addresses must be used but private routing tables should not be exposed. It should also consider the fact that business partners or suppliers as well as remote clients may have to connect to this VPN using all sorts of private and global addresses that may not fit the corporate addressing structure. In this chapter we discuss these issues and provide solutions for them.

4.1 Addressing considerations

When discussing VPN addressing issues, it helps if you know which VPN scenario you are talking about. The basic VPN scenarios are described in 1.5, “Common VPN scenarios” on page 15.

4.1.1 Addressing issues with branch office VPNs

We assumed that company A previously had a traditional network in place, where its various intranets were interconnected over private facilities, such as leased lines or frame relay. We also assumed that company A has already developed an address plan for its network. Since the network was self-contained and the backbone used only private facilities, company A could have used either globally ambiguous (private) IP addresses (that is, of the form 10.x.y.z) or globally unique (public) addresses obtained from the Network Information Center (NIC).

Because assignment of public IP addresses is coordinated through a global authority, they are unambiguous. Public addresses are routable everywhere. However, because private address assignments are facilitated locally without coordination by a global authority, they are ambiguous when used in the public Internet; they are routable only within a company's own private network.

In summary:

1. If company A uses public addresses in its network, the addresses can continue to be used without change in the VPN environment. If it is desired to hide them while the datagram is in transit over the Internet, an ESP tunnel can be used between firewalls.
2. If company A uses private IP addresses in its network, the addresses can also continue to be used on all subnets that have no physical connection to the public Internet. But for those subnets that do connect to the public Internet, typically the exit links at the boundary of the intranet, a public IP address must be used.

IPSec in tunnel mode between VPN gateways, in particular ESP, handles both situations. The tunnel's new IP header will use the global addresses of the two firewalls, allowing datagrams to be routed over the Internet between the two firewalls (or routers). The header of the original (inner) IP datagram will use the IP addresses assigned for use in the intranet; since these addresses will be hidden from view by ESP's encryption protocol, they can be either publicly or privately assigned. AH can be used to provide the tunnel as well as authentication and replay protection, but it will not hide the internal addressing structure.

4.1.2 Addressing issues with partner/supplier VPNs

Unlike the branch office case, where we could assume that a consistent addressing plan had been applied across all the company's intranets, in this configuration it is very likely that company X and each of its suppliers have administered their own addressing plan independently of one another. For example, it would be possible that supplier A and supplier B both used private (globally ambiguous) IP addresses in their networks, and it would be possible for some or all of their addresses to overlap. In this case, conventional IP routing protocols will not be able to resolve these ambiguities. Hence, we will make the assumption that the IP addresses of all systems, both in the corporate intranet and in the suppliers' intranets, have been assigned so that they are non-overlapping. That is, we will assume that when private IP addresses are used, there will be coordination between the communicating intranets.

NAT will not help in this case because it will change IP address information which will cause IPSec authentication to fail. In fact, since we need to build end-to-end IPSec tunnels in this scenario, NAT will prohibit the proper setup of security associations altogether.

4.1.3 Addressing issues with remote access VPNs

Unlike in the branch office connection or business partner/supplier scenarios, here we have one endpoint of the tunnels in the Internet. The clients will have automatically assigned public IP addresses by the ISP at connect time. These are routable everywhere. The router installed by the ISP at company A's site knows how to route to the Internet. Therefore, the only requirement for the internal routers is to have routes that direct Internet traffic to the corporate firewall, which in turn routes to the ISP's router. This should be the case anyway.

The IPSec code at the dial-in clients should be capable of differentiating between the corporate traffic which is to be tunneled and the ordinary Internet traffic that requires no special treatment. If they sent all traffic through the tunnel, then the remote user would lose the ability to access Internet resources while operating that tunnel, because the firewall normally would drop the packets retrieved from a tunnel that have non-secure source and destination addresses.

The addressing scheme of the intranet needs no modification to support dial-in clients. If the intranet uses private addresses, it will still be reachable, because packets with private IP addresses are tunneled and the tunnel endpoints have public addresses. Only the subnets with direct connection to the Internet need to have public addresses. This is not a new requirement.

4.2 Routing considerations

For VPNs to be ready to replace dedicated telecommunications lines, routing protocols must be supported. Some routing protocols use multicast or broadcast addresses, for example, OSPF and RIP. IPSec currently only defines the use of unicast addresses which means these routing protocols can only be supported using a layer-2 tunnel which can then be secured using an IPSec tunnel. This does, however, add unnecessary overhead to support the layer-2 tunnel even though the only traffic that would be flowing would be layer-3 IP traffic.

BGP is a routing protocol that uses unicast addresses. Many organizations use this protocol to interconnect branch offices because of the small amount of bandwidth it takes, and its strong ability to control and filter the routing tables that are propagated and advertised in the network.

4.2.1 Network environment

We will be configuring a network where BGP will be used as the routing protocol. There are two forms of BGP: EBGP and IBGP. EBGP connects disparate autonomous systems (ASs) which are directly connected with a common network. IBGP connects ASs that are not directly connected with a common network.

You can find a detailed description of BGP in the redbook *TCP/IP Tutorial and Technical Overview,* Sixth Edition, GG24-3376.

Normally the choice is clear as to which protocol to use. If the ASs can be directly connected with a common network link then EBGP is used, if they cannot then IBGP is used. The use of IPSec tunnels will actually give the network designer the choice of doing either method so you must consider the relative methods of each protocol. EBGP has the advantage over IBGP in that it has greater flexibility in controlling routing tables using AS numbers. IBGP requires that the two systems have the same AS number which means routing tables cannot be controlled.

The network that we will configure will be using EBGP as its routing protocol.

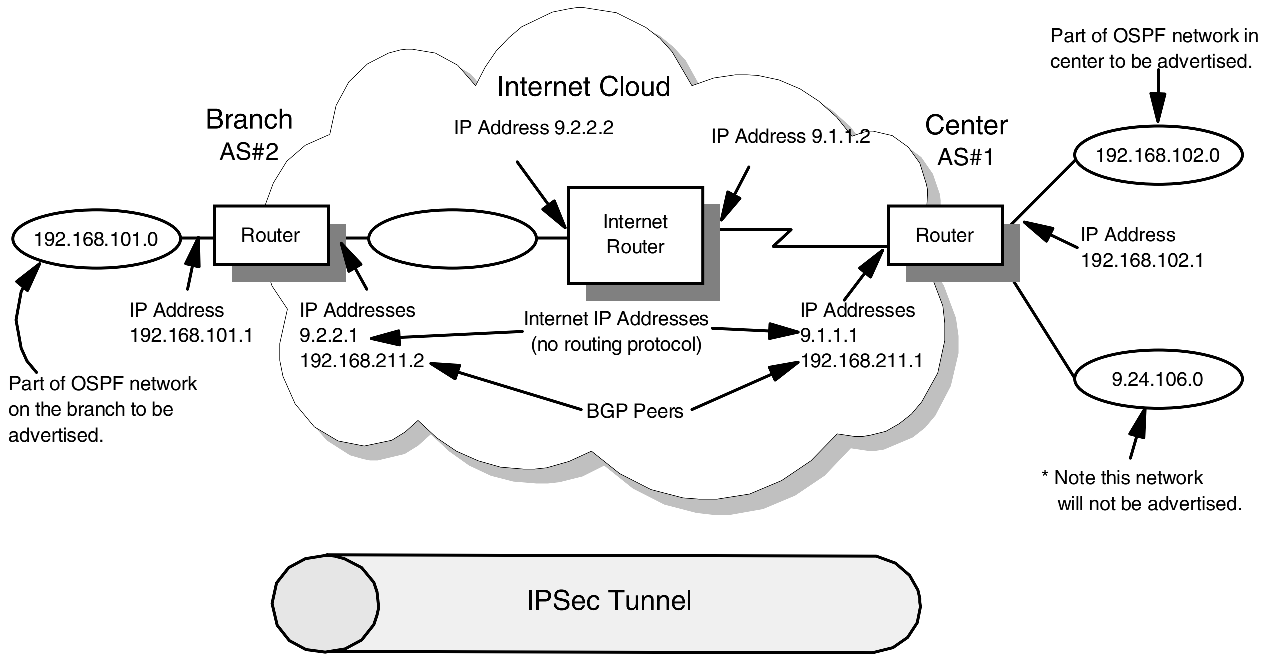


Figure 34. Routing network diagram

What we want is have the two intranet networks (192.169.102.0 and 192.168.101.0) to know the existence of each other and to be able to reach each other. We have simulated the Internet with a single router in the middle. This router simply forwards IP packets to and from the Internet networks (9.1.1.0 and

9.2.2.0). All routing protocols have been disabled on this router to simulate a realistic ISP Internet that does not allow you to participate in routing protocols.

As mentioned earlier two BGP ASs must have a common network which joins them. The BGP speakers must be on this network so that they can find their peers. In our scenario this network will be the 192.168.211.0 network. This is why in Figure 34 the central and branch routers both have an address on this network. Those addresses are defined on the same interface that connects to the Internet. Note that the physical interface that these addresses are defined on is irrelevant because traffic to and from these interfaces will be transported over an IPSec tunnel. In this way the BGP peers will appear on the same network and will be able to communicate with each other.

4.2.2 Router configuration

Below you can see the IP address configuration on the central router with the two IP addresses on interface 2.

```
Center IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0  192.168.102.1    255.255.255.0    Local wire broadcast, fill 1
   intf     1  9.24.106.17      255.255.255.0    Local wire broadcast, fill 1
   intf     2  9.1.1.1          255.255.255.0    Local wire broadcast, fill 1
               192.168.211.1    255.255.255.0    Local wire broadcast, fill 1
```

The first step in configuring this scenario is to define the correct policy. This process has been described in detail in other parts in the book. The policy that we want to define must emulate a dedicated telecommunications line, that is, the policy must allow any type of traffic to flow. The key difference is that it must flow over the secured IPSec tunnel.

4.2.2.1 Defining a policy

To define this policy you have to define a traffic profile with no restriction on the IP addresses.

```
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? routing
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]?
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? routing
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]?
Enter IPV4 Source Mask [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]?
Enter IPV4 Destination Mask [0.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]: y
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]:
```

Figure 35. VPN routing - policy definition

4.2.2.2 Defining interface pairs

Next we must define the interface pair. This is how we make sure that everything going out goes over the tunnel. Make sure that you enter two interface pairs, one for the secondary IP address that BGP will use (192.168.211.1) and one for the Internet address that the tunnel will actually go over (9.1.1.1).

```
The Source and/or Destination Address information you specified
includes all addresses.  You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy.  The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]: y
Interface Pair Groups:
        0: New Ifc Pair
Number of Ifc Pair Group [1]? 0
Enter a Group Name (1-29 characters) for this Interface Pair []? routing
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]? 9.1.1.1
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: routing
                  In:Out=255.255.255.255 : 9.1.1.1

Number of Ifc Pair Group [1]? 0
Enter a Group Name (1-29 characters) for this Interface Pair []? routing
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]? 192.168.211.1
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: routing
                  In:Out=255.255.255.255 : 9.1.1.1
                  In:Out=255.255.255.255 : 192.168.211.1

Number of Ifc Pair Group [1]?


Here is the Profile you specified...


Profile Name    = routing
        sAddr:Mask=       0.0.0.0 : 0.0.0.0        sPort=    0 : 65535
        dAddr:Mask=       0.0.0.0 : 0.0.0.0        dPort=    0 : 65535
        proto     =             0 : 255
        TOS       =           x00 : x00
        Remote Grp=All Users
        1.  In:Out=255.255.255.255 : 9.1.1.1
        2.  In:Out=255.255.255.255 : 192.168.211.1
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: routing

Enter number of the profile for this policy [1]?
```

Figure 36. VPN routing - interface pairs

4.2.2.3 IPSec and IKE configuration

The rest of the configuration is identical to other IPSec examples shown earlier in this chapter. In this scenario we defined an IPSec tunnel with pre-shared keys. Remember that the tunnel goes over the Internet IP address, that is, 9.1.1.1 for the central router and 9.2.2.1 for the remote router.

```
List of Validity Periods:
        0: New Validity Period

Enter number of the validity period for this policy [0]?
Enter a Name (1-29 characters) for this Policy Valid Profile []? always
Enter the lifetime of this policy. Please input the
information in the following format:
                yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?

Here is the Policy Validity Profile you specified...

Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
Is this correct? [Yes]:
List of Validity Periods:
        0: New Validity Period
        1: always

Enter number of the validity period for this policy [1]?
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]? 0
Enter a Name (1-29 characters) for this IPsec Action []? routing
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]? 2
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [192.168.102.1]? 9.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 9.2.2.1
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]: n
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
```

Figure 37. VPN routing - validity period and IPSec action

```
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
Enter a Name (1-29 characters) for this IPsec Proposal []? routing
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: y
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]?
Enter a Name (1-29 characters) for this IPsec Transform []? routing
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]? 1
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]? 1
List of ESP Cipher Algorithms:
     1)  ESP DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 1
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]?
Security Association Lifetime, in seconds (120-2147483647) [3600]?

Here is the IPSec transform you specified...

Transform Name  = routing
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
        0: New Transform
        1: routing

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:
```

Figure 38. VPN routing - IPSec proposal

```
Here is the IPSec proposal you specified...

Name  = routing
        Pfs   = N
        ESP Transforms:
                routing
Is this correct? [Yes]:
List of IPSEC Proposals:
        0: New Proposal
        1: routing

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

IPSECAction Name = routing
        Tunnel Start:End         =        9.1.1.1 : 9.2.2.1
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                routing
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: routing

Enter the Number of the IPSEC Action [1]?
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? routing

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]? 1
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]: n
```

Figure 39. VPN routing - ISAKMP action

```
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal

Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? routing

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  Certificate (RSA SIG)

Select the authentication method (1-2) [1]? 1

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 1

List of Cipher Algorithms:
     1)  DES

Select the Cipher Algorithm (1-2) [1]? 1
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

Here is the ISAKMP Proposal you specified...

Name = routing
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: routing

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name     = routing
        Mode                    =            Main
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =              No
        ISAKMP Proposals:
                routing
Is this correct? [Yes]:
```

Figure 40. VPN routing - ISAKMP proposal

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: routing

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = routing
        State:Priority =Enabled    : 5
        Profile        =routing
        Valid Period   =always
        IPSEC Action   =routing
        ISAKMP Action  =routing
Is this correct? [Yes]:
To authenticate the ISAKMP Peer with Pre-Shared Key a User
must be added.  Add a USER now? [Yes]:
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 9.2.2.1
Group to include this user in []?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (8 characters) in ascii:

Here is the User Information you specified...

Name      = 9.2.2.1
        Type      = IPV4 Addr
        Group     =
        Auth Mode =Pre-Shared Key
Is this correct? [Yes]:
```

Figure 41. VPN routing - policy user

The definitions in the remote router are identical except for the IP addresses.

4.2.2.4 BGP configuration

The next step is to set up the BGP routing protocol.

In the BGP configuration the central router will have the AS number 1 while the remote router will have the AS number 2. The first step is to define the neighbor being 192.168.211.2 and AS number 2. Then we configure the policies on what routing tables get propagated. The original policies will dictate what routing table entries, discovered by the interior gateway protocol used in the AS (OSPF), will be used by BGP. The receive policies will dictate what routing table entries received by other BGP peers will be used by this router. The send policies will dictate what routing table entries it will send to its peers. As you can see from the configuration shown in Figure 42 on page 72 we basically had no restrictions.

```
Center Config>PROTOCOL BGP
Border gateway protocol user configuration
Center BGP Config>ENABLE BGP
AS [2]? 1
TCP segment size [1024]?
Center BGP Config>ADD NEIGHBOR
Neighbor address [0.0.0.0]? 192.168.211.2
AS [0]? 2
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1024]?
Center BGP Config>ADD ORIGINATE-POLICY INCLUSIVE
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Tag [0]?
Center BGP Config>ADD RECEIVE-POLICY INCLUSIVE
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]? 2
Adjacent AS# [0]? 2
IGP-metric [0]?
Center BGP Config>ADD SEND-POLICY INCLUSIVE
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 2
Center BGP Config>LIST ALL

                BGP Protocol:             Enabled
                AS:                    1
                TCP-Segment Size:      1024

Neighbors and their AS:
                                    Init    Conn    Hold    TCPSEG
Address            State     AS     Timer   Timer   Timer   Size
9.2.2.1            ENABLD    2      12      120     90      1024

Receive-Policies:
Index  Type  Prefix           Mask             Match  OrgAS  AdjAS  IGPmetric
1      INCL  0.0.0.0          0.0.0.0          Range  2      2      0

Send-Policies:
Index  Type  Prefix           Mask             Match  Tag    AdjAS
1      INCL  0.0.0.0          0.0.0.0          Range  0      2

Originate-Policies:
Index  Type  Prefix           Mask             Match  Tag
1      INCL  0.0.0.0          0.0.0.0          Range  0

No aggregation records in configuration.
No no-receive-AS records in configuration.
classless-bgp is disabled.
compare-med-from-diff-as is disabled.
IP-route-table-scan-timer value is 1 seconds.
```

Figure 42. VPN routing - BGP configuration

4.2.2.5 Interior routing protocol configuration

The last step is to enable the interior gateway protocol that BGP will use to originate its routes and then to reload the router.

```
Center OSPF Config>ENABLE OSPF
Estimated # external routes [100]?
Estimated # OSPF routers [50]?
Maximum Size LSA [2048]?
Center OSPF Config>SET INTERFACE
Interface IP address [0.0.0.0]? 192.168.101.1
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]?
Router Priority [1]?
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
TOS 0 cost [1]?
Demand Circuit (Yes or No)? [No]:
Authentication Type (0 - None, 1 - Simple) [0]?
```

Figure 43. VPN routing - interior routing protocol configuration

All configuration steps on the remote router are identical to the center except for the IP addresses.

If you enable IKE and BGP messages on the event log you will be able to see the IPSec tunnel come up followed by the BGP messages. The messages shown in Figure 44 on page 74 are taken from the branch router.

```
00:00:30  IKE.009: Begin Main mode - Initiator
00:00:30  IKE.013: To Peer: 9.1.1.1 MM HDR SA
00:00:30  IKE.001: Trace IKE packet to 9.1.1.1
00:00:31  IKE.001: Trace IKE packet from 9.1.1.1
00:00:31  IKE.013: From Peer: 9.1.1.1 MM HDR SA
00:00:31  IKE.014: Oakley proposal is acceptable. Peer:  9.1.1.1
00:00:31  IKE.013: To Peer: 9.1.1.1 MM HDR KE NONCE
00:00:31  IKE.001: Trace IKE packet to 9.1.1.1
00:00:32  IKE.001: Trace IKE packet from 9.1.1.1
00:00:32  IKE.013: From Peer: 9.1.1.1 MM HDR KE NONCE
00:00:32  IKE.003: Processing ISA_KE
00:00:32  IKE.003: Processing NONCE
00:00:32  IKE.013: To Peer: 9.1.1.1 MM HDR* ID HASH
00:00:32  IKE.002: Trace IKE payload before encryption to Peer: 9.1.1.1
00:00:32  IKE.001: Trace IKE packet to 9.1.1.1
00:00:32  IKE.001: Trace IKE packet from 9.1.1.1
00:00:32  IKE.013: From Peer: 9.1.1.1 INFO HDR HASH
00:00:32  IKE.001: Trace IKE packet from 9.1.1.1
00:00:32  IKE.002: Trace IKE payload after decryption from Peer: 9.1.1.1
00:00:32  IKE.013: From Peer: 9.1.1.1 MM HDR* ID HASH
00:00:32  IKE.014: ValidatePhase1ID: cpeP1Handles match. Peer:  9.1.1.1
00:00:32  IKE.013: To Peer: 9.1.1.1 QM HDR* HASH SA NONCE ID ID
00:00:32  IKE.002: Trace IKE payload before encryption to Peer: 9.1.1.1
00:00:32  IKE.001: Trace IKE packet to 9.1.1.1
00:00:32  IKE.001: Trace IKE packet from 9.1.1.1
00:00:32  IKE.002: Trace IKE payload after decryption from Peer: 9.1.1.1
00:00:32  IKE.013: From Peer: 9.1.1.1 QM HDR* HASH SA NONCE ID ID
00:00:32  IKE.003: Processing Quick Mode ID
00:00:32  IKE.003: Processing Quick Mode ID
00:00:32  IKE.015: Acceptable phase 2 proposal # 1
00:00:32  IKE.003: Processing NONCE
00:00:32  IKE.008: Load Out SA: Alg=18 Prot=3 Sec=3600 KB=50000 SPI=767964316
00:00:32  IKE.008: Load In SA: Alg=18 Prot=3 Sec=3600 KB=50000 SPI=2787471637
00:00:32  IKE.013: To Peer: 9.1.1.1 QM HDR* HASH
00:00:32  IKE.002: Trace IKE payload before encryption to Peer: 9.1.1.1
00:00:32  IKE.001: Trace IKE packet to 9.1.1.1
00:00:56  BGP.015: conn to 192.168.211.1 open on sprt 179 dprt 1027
00:00:56  BGP.069: BGP state change; nbr 192.168.211.1 ev 3 oldst 3 newst 4
00:00:56  BGP.016: OPEN sent to 192.168.211.1
00:00:56  BGP.056: OPEN rcvd from 192.168.211.1
00:00:56  BGP.069: BGP state change; nbr 192.168.211.1 ev 8 oldst 4 newst 5
00:00:56  BGP.059: KEEPALIVE sent to 192.168.211.1
00:00:56  BGP.057: KEEPALIVE rcvd from 192.168.211.1
00:00:56  BGP.072: Add NLRI 192.168.101.0 len 3 updt for nbr 192.168.211.1
00:00:56  BGP.072: Add NLRI 192.168.211.0 len 3 updt for nbr 192.168.211.1
00:00:56  BGP.072: Add NLRI 9.0.0.0 len 1 updt for nbr 192.168.211.1
00:00:56  BGP.069: BGP state change; nbr 192.168.211.1 ev 9 oldst 5 newst 6
00:00:56  BGP.050: UPDATE(s) sent to 192.168.211.1, len 51
00:00:56  BGP.052: UPDATE rcvd from 192.168.211.1, len 51
00:00:56  BGP.044: New or updtd RIB entry 192.168.211.0 from 192.168.211.1
00:00:56  BGP.044: New or updtd RIB entry 192.168.102.0 from 192.168.211.1
00:00:56  BGP.044: New or updtd RIB entry 9.0.0.0 from 192.168.211.1
00:00:56  BGP.072: Add NLRI 192.168.102.0 len 3 updt for nbr 192.168.211.1
00:00:56  BGP.050: UPDATE(s) sent to 192.168.211.1, len 47
00:00:57  BGP.052: UPDATE rcvd from 192.168.211.1, len 47
00:00:57  BGP.043: NLRI 192.168.101.0 rej by ext policy from 192.168.211.1
00:01:00  BGP.015: conn to 192.168.211.1 open on sprt 1024 dprt 179
00:01:00  BGP.016: OPEN sent to 192.168.211.1
00:01:00  BGP.056: OPEN rcvd from 192.168.211.1
00:01:00  BGP.049: Closing conn to 192.168.211.1 sprt 1024 dprt 179; conn collision
00:01:00  BGP.058: Notify sent to 192.168.211.1
00:01:26  BGP.059: KEEPALIVE sent to 192.168.211.1
00:01:27  BGP.057: KEEPALIVE rcvd from 192.168.211.1
```

Figure 44. VPN routing - IKE and BGP startup messages

If you dump the routing table you can confirm that new routes have been learned from BGP. The screen below shows the remote router learning about the 192.168.102.0 network, which is attached to the center router:

```
Branch *TALK 5

CGW Operator Console

Branch +PROTOCOL IP
Branch IP>DUMP
Type   Dest net         Mask      Cost     Age       Next hop(s)

Sbnt   9.0.0.0          FF000000  1        76        None
Stat*  9.1.1.0          FFFFFF00  1        82        9.2.2.2
 Dir*  9.2.2.0          FFFFFF00  1        82        TKR/1
 SPF*  192.168.101.0    FFFFFF00  1        81        TKR/0
BGPR   192.168.102.0    FFFFFF00  0        51        192.168.211.1
 Dir*  192.168.211.0    FFFFFF00  1        82        TKR/1

Routing table size: 768 nets (52224 bytes), 6 nets known
                      0 nets hidden, 0 nets deleted, 1 nets inactive
                      0 routes used internally, 761 routes free
```

Figure 45. VPN routing - routing table dump

4.2.3 Summary

Depending on the size and complexity of the intranet VPN you want to build, there are basically three options as far as exchanging routing information across VPNs is concerned:

Static routing Use this option if you have very few VPN connections between your sites and a meshed topology is not necessarily required. In this case, it helps to make the VPN gateways the default routers for the networks attached to them. It also helps if the branch networks have a flat structure so that no dynamic routing is required inside them.

IBGB Use this option if you have a complex network structure that needs to be mapped over VPNs and requires the exchange of complex routing tables across VPN connections.

EBGB This option allows you to do the same as with IBGP, but it also gives you greater flexibility in controlling the routing table information that gets exchanged over VPN connections.

Part 2. VPN scenarios based on MRS/MAS/AIS Version 3.3

Chapter 5. New features in MRS/MAS/AIS Version 3.3

In this chapter we provide an overview of all new functions in CC5 MRS/AIS/MAS V3.3 with more extensive descriptions of VPN-related features. The subsequent chapters in this part configure new VPN features on Nways routers as described in 5.1, “IKE implementation” on page 79 through 5.3, “Policy-based networking” on page 82 with realistic scenarios. At a glance the major changes are:

- Secure an exchange of keys with Internet Key Exchange (IKE) for IPSec.
- Use tunneling and encryption technologies to create a secured VPN.
- Enhance performance of token-ring, Thin server, and frame relay.
- Benefit from Dynamic Host Configuration Protocol Server and Dynamic IP addressing.
- Improve bandwidth usage for IPv4 with Service Differentiation for PPP or frame relay links.
- Administer and configure your network using a central directory server.
- Transport voice/fax services over your frame relay network.

5.1 IKE implementation

In IPSec a security association (SA) contains all the relevant information that communicating systems need. For example, the SA will identify the cryptographic algorithm to be used, the keying information, the identities of the parties. For a simple configuration of two IPSec devices communicating, four SAs need to be configured. That is two on each peer, one for incoming traffic and one for outgoing traffic. Clearly this does not scale well. Also, once the keys are configured, they remain constant until they are reconfigured. This can leave a security hole. In a recent study it took distributed.net team, a non-profit organization of computer hobbyists, just over 22 hours to decipher a DES-encoded message. Internet Key Exchange (IKE) addresses all of these problems. The keys are negotiated between IKE peers, and are regenerated at frequent time intervals. While some configuration is needed, it is far more manageable than the manual key configuration scenario which is only supported in CC4.

Now IKE is implemented on all IBM routers. Therefore, key generation is automatically performed through pre-shared keys and digital signature using public key infrastructures while providing simplified management and enhanced key security on all IBM routers.

Now let us look at the specific IKE features supported by IBM routers:

- Securing IPv4 traffic only
- Phase 1 in main and aggressive mode
- Phase 1 encryption algorithms: DES, 3DES
- Phase 1 Hash algorithms: SHA, MD5
- Diffie-Hellman groups 1 and 2
- Authentication by pre-shared keys or certificates from a single CA
- Phase 2 encryption algorithms: DES, 3DES, CDMF

- Phase 2 authentication algorithms: HMAC-SHA, HMAC-MD5
- IKE with remote access (see Figure 46): responder's IP address must be known in advance

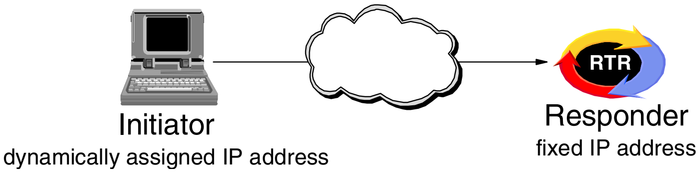


Figure 46. IPSec IKE remote access

IKE can be negotiated with a peer as long as the responder's IP address is known in advance. So the initiator's IP address can be dynamically assigned. This allows IKE to work in a remote access scenario, where the initiator is either a mobile platform or a remote office which is connected using the Internet. Note that for most remote access scenarios you will need to perform Phase 1 in aggressive mode.

If you are performing authentication using pre-shared keys, you must use aggressive mode negotiations because you need to know the identity of the remote end before the master key is calculated.

If you are using digital signatures, you will have to use aggressive mode unless you know, in advance, what subnet that remote user will be on. In this (rare) case, the router is configured with a generic policy for the subnet with some minimal Phase 1 configuration. When the remote user dials in with a dynamically assigned address from that subnet the generic policy is used by the gateway to negotiate the Phase 1 SA up to message 5. When the router receives the ID of the remote access user in message 5, it does a policy lookup on the ID to confirm that the policy associated with this ID is compatible with the generic policy. If it is compatible, the negotiation finishes. If not, the negotiation is stopped and the router initiates a Phase 1 negotiation with the remote user using the more specific policy.

Finally we list the features not yet available on IBM routers:

- Certificates from different CAs
- Encryption using certificate
- Checking certificate revoke list (CRL)
- No MIB defined for IKE

Authentication is supported by pre-shared keys and by digital signatures, as long as the digital signatures are signed by a single CA. We do not support multiple CAs in this release.

Background: If there are more multiple CAs a hierarchy may exist. The root CA is at the top of the hierarchy and all subordinate CAs will have their certificates signed by the root CA.

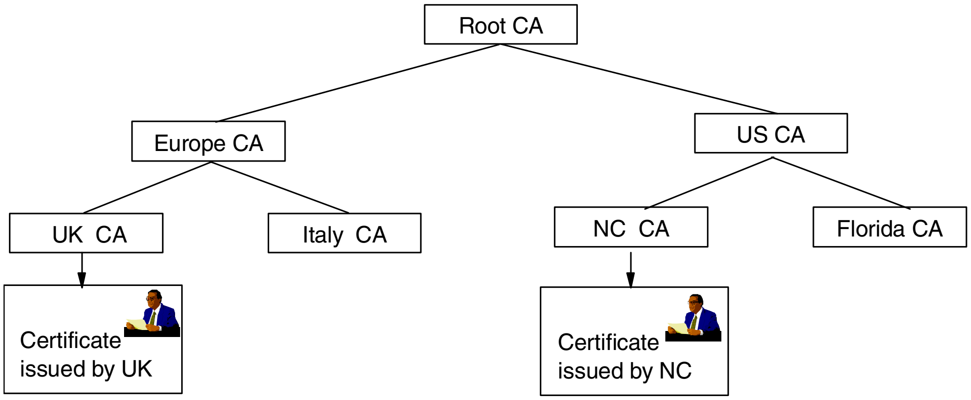


Figure 47. CA hierarchies

CA hierarchies in Figure 47 are reflected in certificate chains. A certificate chain is a series of certificates issued by successive CAs. A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy. Imagine the scenario where one IKE peer has a certificate issued by a CA in the U.K. and the other peer has a certificate from a CA in North Carolina. When the peer wishes to check the validity of its peer certificate it would need to follow a chain to determine the validity. There is an added complication if the CAs do not have a common root. Say for example, one peer has a certificate issued by Entrust and another by Verisign. To achieve verification cross-certification must be available.

5.2 Layer-2 tunnel support

In previous versions IBM routers only supported L2TP tunnel. However, CC5 V3.3 software supports layer-2 tunnels including L2TP, PPTP, and L2F.

A miscellaneous enhancement regarding L2TP is an L2TP router client known as the client initiated (voluntary tunneling) model. This function provides secure, tunneled multi-protocol VPN services regardless of service provider topology. This function brings the client and LAC into one physical piece of hardware.

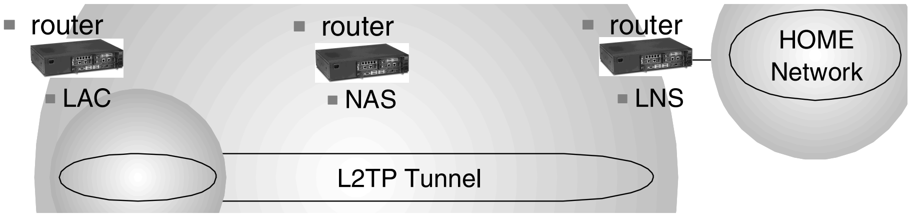


Figure 48. Router client L2TP

5.2.1 PPTP tunnel support

Point-to-Point Tunneling Protocol (PPTP) has the same aim as L2TP, which is to tunnel PPP packets across an IP network. L2TP was developed by the IETF and is based heavily on PPTP and L2F (Cisco's equivalent). But at this time Microsoft does not support L2TP - it is currently planned for Windows NT 5.0. Therefore, to establish a tunnel with a Microsoft device, IBM routers need to support PPTP. IBM Nways router can initiate or terminate the PPTP tunnel as shown in Figure 49:

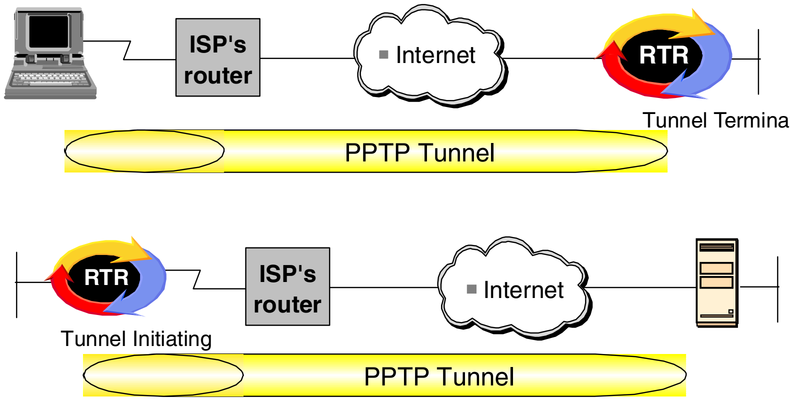


Figure 49. PPTP tunnel

5.2.2 L2F tunnel support

L2F is a tunneling protocol which was developed by Cisco. It was developed to tunnel link layers so that the location of the initial dial-up server could be divorced from the location at which the protocol termination and access to the network is provided. It provides the same solutions as L2TP - in fact when the IETF developed L2TP it reused some of Cisco’s L2F and Microsoft’s PPTP. Note that the RFC is an informational RFC, not a standards track one.

IBM routers are implementing L2F to be the L2F peer with a Cisco router. It was not developed to use L2F between two IBM routers, since we already have L2TP to perform that function. L2F terminology defines two devices - an NAS and a home gateway, GW. A remote user initiates a PPP connection to an NAS which undertakes partial authentication of the end system/user. The NAS uses the user name field to determine to which home gateway that users wishes to be tunneled. Cisco routers only support the compulsory tunneling scenario - their L2F implementation does not provide an equivalent function to our L2TP voluntary tunneling or client-initiated model. The IBM router can either be the NAS or the GW, with the other L2F peer being either a Cisco router or any other device which supports L2F.

5.3 Policy-based networking

Some of the recent IP developments have stated that network devices should determine if an action should be applied to received traffic. For example, should this traffic be secured by IP Security; does this traffic have special QoS requirements. While this has given excellent functionality to networks, it has made the configuration of modern IP devices repetitive and difficult to scale to large networks. Managing a modern network would be easier if the repetitive parts of the configuration could be easily installed in all devices. The accepted method of storing, searching and sharing this kind of data is in a database. In a modern IP network, a network device that forwards traffic may need to determine if any special handling is required. The handling requirements must be configured in the networking device in advance. A common example of a handling requirement is traffic going between a branch to a head office should be secured - this handling requirement is known as a *policy*.

A network device, for example, a router, needs to know how to identify the packets going from the branch to the head office and how to secure them. Typically a router would inspect certain fields of the IP header to identify the traffic (for example, source and destination address) and then process accordingly. So a policy is comprised of *conditions*, how does the device recognize the packet, and *actions*, what does the device do with the packet that meets the conditions. If each device in the network has its own database, all of the policies can be stored in the database. When a packet is received, the database is searched to see if there is a matching policy and if there is, the action is applied. Within the database, it is likely that many of the policies will have common attributes. Consider a network secured by IPSec. There may be many different conditions (for example, many traffic flows), but the action could be similar - for example, secure using IPSec AH. A database structure allows actions and conditions to be shared between multiple policies. Therefore, the action only needs to be configured once and then it can be used by as many policies as required.

In summary, within a network device there may be a single configuration detail which is applicable to multiple policies and within a network, multiple devices may have the same policy. So we have to find how to create a database in each network device.

One option for entering the policies into the database is to manually configure each device shown in Figure 50, Alt 1. The use of a database simplifies the configuration of that device because information only needs to be entered once, and if that information is then need by another policy, it can be retrieved from the database. But while this minimizes the repetitive configuration within a device, it still does not scale to a large network. A proposed solution is to input all the policies into a central server and configure each network device to retrieve its policies from the central server. The IETF has proposed that the central server is an LDAP server and each network device is an LDAP client. LDAP will be discussed in detail later in 5.3.2, “LDAP clients in routers” on page 85 - at this time, the concept is that an LDAP server can store the policies as shown in Figure 50, Alt 2.

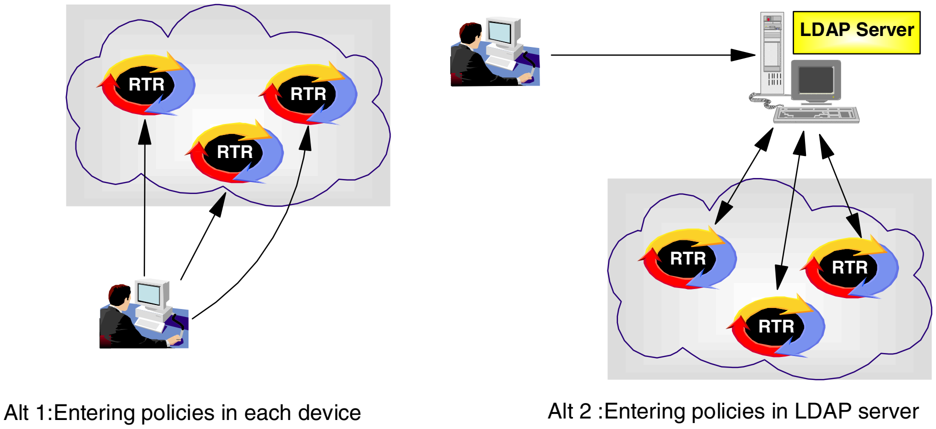

RTR
RTR
RTR
LDAP Server
RTR
RTR
RTR
Alt 1:Entering policies in each device
Alt 2 :Entering policies in LDAP server

Figure 50. Entering policies

Up until now, we have reviewed the concept of policy-based networking and how to store the policies; we will now look at how this is being implemented in IBM routers in a new release.

In this release, V3.3 of the code, four protocols will be able to use the policy database. These protocols are ones with repetitive data - repetitive within a node and possibly within the network. Here are examples of what can be repetitive:

- *RSVP* - this was first shipped in V3.2 of the routers' code. An RSVP policy may define that traffic between A and B should be allowed to reserve 10% of the bandwidth. Another traffic flow might also wish to reserve 10% of the bandwidth, so that action can be shared among multiple policies.
- *DiffServ* - this is new in V3.3 and is discussed in detail in another presentation. DiffServ policies define that certain traffic needs to be marked and then receive special handling requirements. The handling requirements can be common to several policies.
- *IKE* - is also new in V3.3 and provides key generation for IPSec. The key generation mechanisms can be common for many policies.
- *IPSec* - this requires the traffic configuration of keys and tunnels in peer devices - if this information can be shared between peers, configuration will be easier.

5.3.1 Combined policy engine in IBM Nways routers

The population of the policy database is performed using the command line in talk 6 on the router. You can configure a policy with two different starting points. You can either configure all the actions, validity periods, etc. in advance and then define which of these actions a specific policy will use. As an alternative you can start with the `add policy` command and the router will prompt you through the creation of attributes which do not exist. This makes policy configuration easy and flexible. The added benefit of this function is that you no longer have to define packet filters for IP security. In earlier releases you had to create packet filters to pass the traffic to IPSec, allow the secured packets in and out of the router, and then define a filter to confirm that the correct tunnel was used. The policy database creates all of these for you.

There are very few restrictions in terms of what can exist in a policy. You cannot have a single policy which defines an RSVP and IPSec action; you clearly cannot have an IPSec manual tunnel action and IKE action. The policy database currently only applies to IPv4 traffic, not IPv6.

5.3.2 LDAP clients in routers

This new feature allows routers to retrieve RSVP, IKE, IPSec and DiffServ policies from LDAP V2/V3 server using LDAP client in a router. Supported LDAP servers are:

- IBM eNetwork Directory Server
- University of Michigan SLAPD
- Microsoft Active Directory
- Novell NDS
- Netscape Directory Server

This centralized configuration makes scalable policy management possible.

5.4 Others

Up until now we have described VPN related CC5 MRS/AIS/MAS V3.3 new features. In this part we look at other enhancements briefly.

5.4.1 IP enhancements

DHCP server

The DHCP server provides IP addresses and other configuration information for LAN-attached DHCP clients. The default configuration enables address allocation from a private IP pool, making it easy to use. DHCP server will work on serial interfaces, token-ring, and Ethernet. Dynamic IP, PPP interfaces can be configured to retrieve a public IP address from an Internet service provider (ISP). When combined with NAT/NAPT, LAN-attached devices in a private network can connect to a public network using an ISP. The DHCP Server can also be used to provide IP addresses for the LAN-attached DHCP clients. All communications between clients and server use the private IP address while communications between the server and the ISP use the assigned public IP address.

IPv4 currency

The generic IP route policy provides a subset of routes that are selected and the action taken for selected routes. Each route policy indicates that the route should be included or excluded. In addition to matching on address and mask, additional criteria may be configured for more granular route selection.

- Protocol (for example, OSPF, RIP, BGP)
- Autonomous System (AS) Number
- Gateway Address (Matches on a range defined by an address and mask)
- Net (Matches on outgoing network numbers)
- Metric Range
- Source Gateway (applicable only to RIP receive policy)

Once a route is selected, one of the following actions is performed:

- Set the advertised/installed metric.
- Manually set the advertised tag.
- Automatically set the tag using the current heuristic.

IPv6 phase II

IP Version 6 will now provide the same level of dynamic reconfiguration support as IP Version 4, that is:

- Delete interface
- Activate interface
- Reset interface
- Reset IPv6
- Reset IP parameter — The following talk 6 commands take effect immediately in the running system: "add route", "delete route", "change route", "enable icmp-redirect", "disable icmp-redirect", "set access-control", "set ttl" and "set path-mtu-aging-timer" (new for IPv6)
- PIM6 talk 6 commands to "enable", "disable", "delete" an interface, and "set interface" take effect immediately

Previously only delete interface was supported.

Additional packet filtering:

- Inbound packets
- Exclusive packets
- Protocol range
- TCP and UDP port ranges
- Global access list
- Automatic tunnel

DHCP6 Relay Agent — this will allow the box to act as a DHCP6 relay agent in the case where router advertisements have been configured to allow hosts to utilize "stateful" configuration.

5.4.2 SDLC enhancement

SDLC primary group poll

Primary group poll works with a 3174 gateway to token-ring configuration. The 3174 is attached to the 2216 with an SDLC link. Since the 3174 may have many downstream token-ring attached PUs (which the 2216 sees as separate SDLC attached PUs) performance suffers because of the extreme amount of polling overhead. Primary group poll alleviates this performance problem by providing a mechanism to poll a group of PUs at a time rather than having to poll every PU individually.

SDLC two-way simultaneous

With this support, link scheduling for a full duplex station can be done in a two-way simultaneous mode instead of the currently supported two-way alternating mode. This improves link utilization and compatibility with IBM 37xx controllers.

5.4.3 Voice support

The 2216 provides the following capabilities in an integrated voice/data network:

FRF.12

FRF.12, which is a UNI (DTE-DCE) fragmentation, or NNI, network-to-network fragmentation, will be used to allow real-time and data frames to share the same interface. FRF.12 is the Frame Relay Forum implementation agreement for this fragmentation.

Voice packet forwarding over frame relay

Voice forwarding over frame relay enables the 2216 to pass voice packets through it between frame relay PVCs. The voice traffic to be forwarded may be on a separate PVC from the data or may be on the same PVC with the data. In a typical configuration, the voice traffic would be forwarded to a locally attached voice capable device. To properly support the voice traffic, BRS has been enhanced to support a traffic class for voice.

5.4.4 Web server cache enhancements

Scalable, high-availability support allows up to sixteen server caches to be clustered to operate as a single high capacity Web server cache. If any single 2216 Web Server Cache 2 becomes non-functional, pages will continue to be cached by other Web server caches in the cluster. If additional throughput is needed to meet the capacity demands of a fast-growing Web server, cache nodes can be added non-disruptively to extend the capacity of the cluster. Also, the cache memory across the Web server cache nodes is shared so that additional caching space can be provided by a cluster of nodes. Hot pages are automatically replicated across the Web server cache nodes for better performance during normal operation and after the loss of a Web server cache node. An external network dispatcher is required for this support. The network dispatcher must be running MAS, AIS, or MRS V3.3. The External Cache Control Manager provides a protocol that could be used by a Web server to load the cache partition prior to the request for the URL. The External Cache Control Manager can also be used to modify and display information about the cache partition. With these enhancements, Web server cache clusters can be built and extended to meet the demands of the most demanding e-business environment.

5.4.5 Channel enhancements

MAS V3.3 incorporates improvements made in PTF01 for MAS V3.2 which added the following capabilities:

- The ability to add a new LPAR or change an existing LPAR without disrupting the operation of other LPARs
- Doubling the number of LPARs per adapter to 64 when using LSA and 32 when using LCS or MPC+
- The ability to use the same logical CU address for multiple LPARs, reducing system definition complexity
- Improved channel performance, especially IP over MPC+

5.4.6 IPX enhancements

- Configurable IPX RIP Ticks — allow the user to configure the tick value associated with an IPX circuit. This will enhance the user's ability to weigh one route over another.
- IPXWAN over FR SVCs
- SRTB Support for IPX — this enhancement to the translational bridging support allows IPX endstations on different LAN types to communicate. The support will be compatible with the 8209 and 6611 SRTB bridges.

5.4.7 DLSw currency

Two new configuration parameters are added to limit the number of NetBIOS and non-NetBIOS non-session SSSSP messages to queue to each DLSw partner. This prevents huge numbers of frames being queued up to a poorly performing TCP session.

5.4.8 X.25 dynamic reconfiguration

This adds support for reset protocol. Reset protocol allows IP and IPX protocols running over X.25 to be changed and issue the reset protocol to activate configuration changes. Command line configuration changes may be made for X.25 and will become active when the reset protocol is issued. All circuits will be reset/cleared associated with the reset protocol.

5.4.9 BAN MIB

The new MIB consists of one table which provides basic configuration information, counter statistics and an important status indicator for the upstream LLC connection.

5.4.10 Dial MIB

This provides improved monitoring of individual dial circuits, providing information such as call duration, call history, transmission and receipt of packets and bytes, peer address and call state.

5.4.11 WAN reroute MIB

This provides MIB support for the WAN Restoral, WAN Reroute and Dial-on-Overflow functions. The new MIB will consist of two tables, one for WRS and one covering WAN Reroute and Dial-on-Overflow. Each table will provide basic configuration information, counter and secondary/alternate link duration statistics and, most importantly, a status indicator for the primary and secondary/alternate link.

5.4.12 Thin server enhancements

Improved performance and a "push" function to allow a central site to refresh the files cached by the Thin server.

Chapter 6. Configuring IPSec and IKE with IBM Nways routers

In this chapter we explain how to configure IPSec tunnels using Nways Multiprotocol Routing Services (MRS), Access Integrated Services (AIS) and Nways Multiprotocol Access Services (MAS) V3.3. We will show the relationship between policy and the IPSec feature and explain how policies are used by IPSec to direct traffic to and from IPSec tunnels. In earlier releases, we only had IPSec using manually configured tunnels and keys. You had to define the IPSec tunnel with all the relevant keying information and then define IP Packet filters: one to pass the traffic to IPSec to allow the secured packets in and out of the router, and one to confirm that the correct tunnel was used. For more information about IPSec configuration with prior releases, refer to Chapter 23, “Configuring IPSec with IBM Nways routers” on page 439. With the introduction of the policy database, you no longer have to create two of the packet filters. As you define the policy, you define the “packet filter”, now referred to as a rule, to pass the traffic to IPSec. The database also generates the rule to check that the traffic used the correct tunnel. You can define the manual tunnel either from the IPSec feature or from the policy feature. We will configure all three approaches for configuring the IPSec tunnel including the manual tunnel as below:

1. Manual tunnel with policy in CC5 (IP packet filters are used in CC4 instead of policy): manual key generation
2. IKE with pre-shared key which is a new feature in CC5 for key management: automatic key generation
3. IKE with PKI which is a new feature in CC5 for key management: automatic key generation with digital certification from CA

Next we will describe several useful commands to monitor IKE in order to give a basic understanding of the commands that are available, what they can show and how you can determine if IKE Phase 1 and 2 negotiations were successful.

Finally we will give a brief discussion of adding routing protocols (default gateways, static routes and dynamic routes) to an IPSec configuration.

6.1 Policy engine

The policy engine was introduced in the MAS/MRS/AIS 3.3. This policy engine is extensively described in Chapter 19 “Using the Policy Feature” of *Nways Access Integration Services V3.3 Using and Configuring Features*, SC30-3989.

The policy engine is a component that determines whether a packet should be secured by IPSec. RSVP and differentiated services are also used by the policy engine. The most important aspect of the policy engine is that it is engaged on the outbound port after the access control lists (ACLs). That is a port enters the router and passes the port’s input ACL, goes to the routing engine and passes the global ACL, gets forwarded by the routing engine to an outbound port where it passes the port’s output ACL, and then the packet is interrogated by the policy engine. The packet must pass all ACLs; otherwise, the router would have discarded the packet before it reached the policy engine.

The other important point is that a packet must be forwarded before in order for it to be processed by the policy engine. To do this there must be a routing table entry for the packet. The examples in this chapter use static routes to ensure that the router will forward the packet. If you do not wish to use static routes, perhaps due to the administrative overhead, you must enable a routing protocol, as described in Chapter 4, “Addressing and routing” on page 61.

The policy engine cannot support multicast packets. This is not normally a problem because IPSec curently only defines unicast packets. The reason for this is that the multicast packets are processed in a different part of the router from where unicast packets are processed. This part bypasses the policy engine altogether. This is why OSPF cannot be used as the routing protocol that traverses the IPSec tunnel, unless it is encapsulated in another protocol like a layer-2 tunneling protocol.

The following diagram describes the steps a packet goes through and how it interacts with the policy engine:

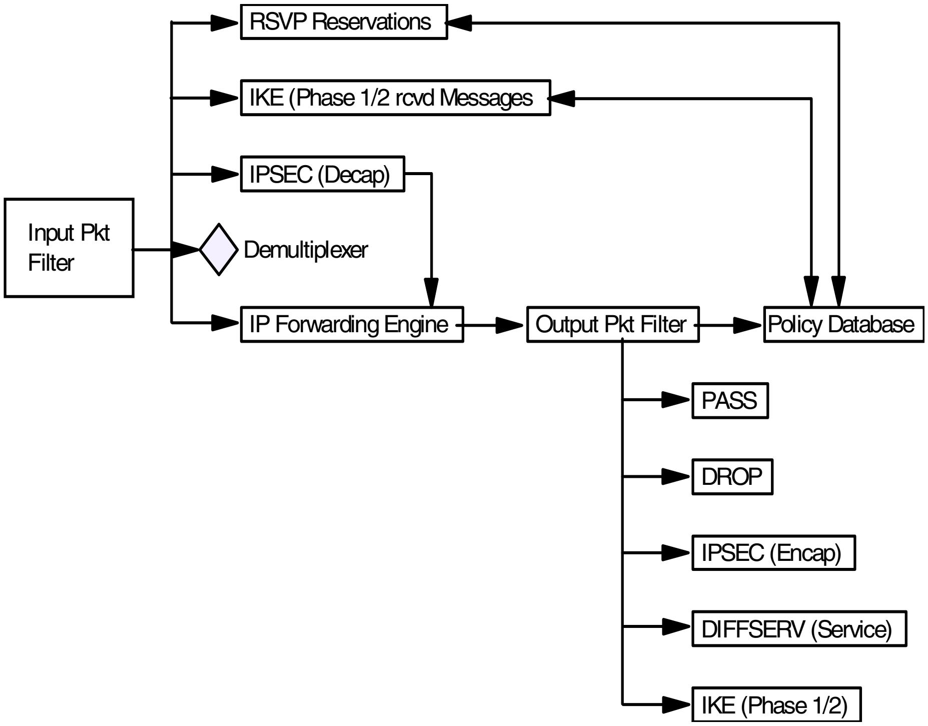


Figure 51. IP packet flow and the policy database

IP packets first must pass the input packet filter before any other actions can be taken. If the input packet filter has rules present then the packet may have some action taken on it. If there is a filter match that excludes the packet or there is no match found in the input packet filter then the packet is dropped.

If the packet passes the input packet filter then it goes to a demultiplexing filter, which checks to see whether the packet is locally destined. If it is, then depending on the type of packet, it is passed to other modules. These modules may be IPSec, IKE, RSVP, or others. If the packet is locally destined for IPSec, IKE, or RSVP then those modules may query the policy database to determine which action to take.

If the packet is not locally destined then it is given to the forwarding engine and a routing decision is made. If the routing decision does not drop the packet (policy-based routing may decide to drop the packet), then the packet goes to the output packet filter. If filter rules are present in the output packet then the packet may have network address translation (NAT) performed, may be passed or may be dropped. If no filter rules are present then the packet is passed. If filter rules are present and no match is found then the packet is dropped. If the packet passes the Output Packet filter then the IP Engine queries the policy database to determine whether any other actions should be performed on this packet.

6.2 Configuring IPSec on an Nways router

The following steps in Figure 52 are recommended when configuring IPSec tunnels. However, depending on your current router configuration, some of these steps may be omitted.

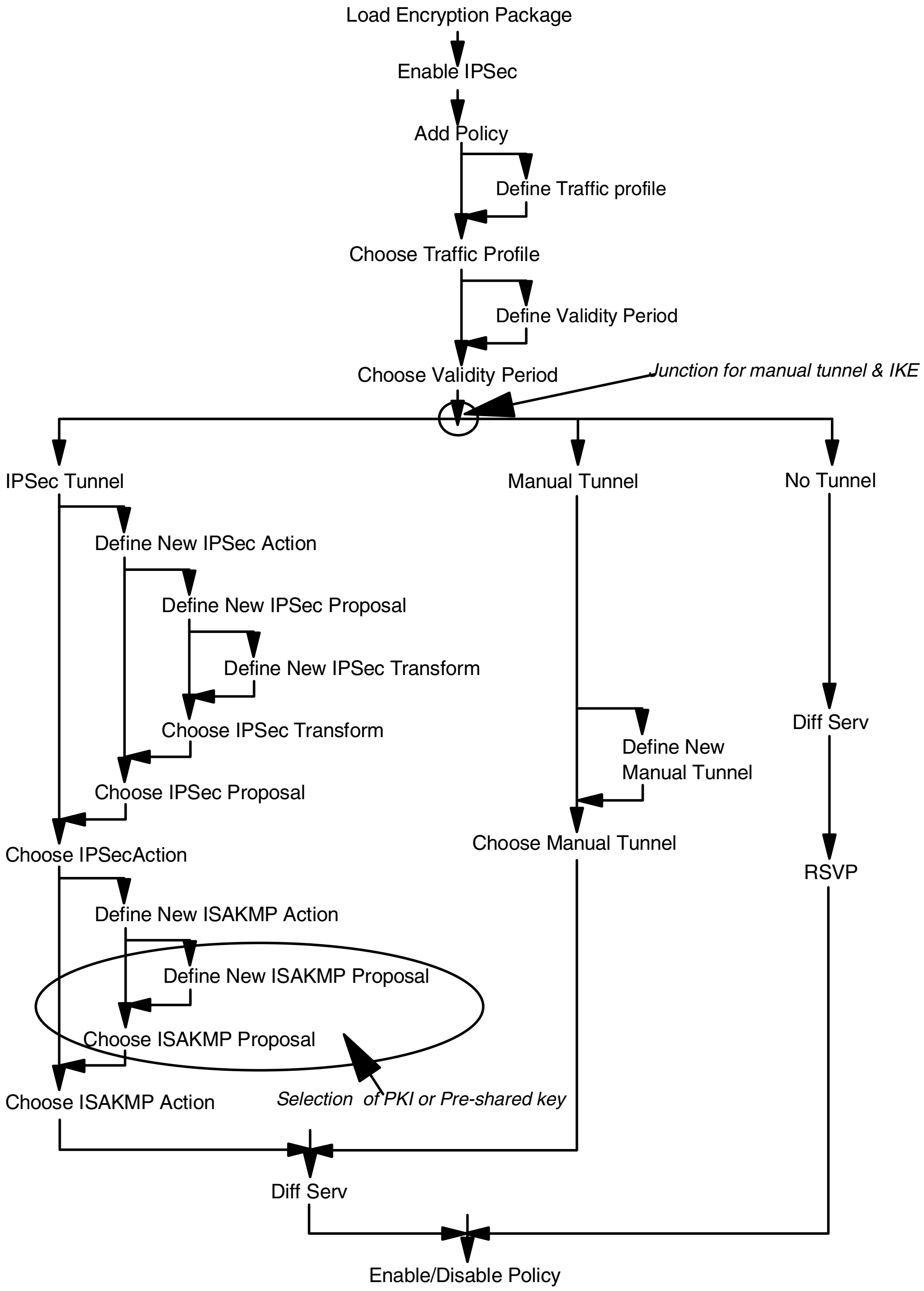


Figure 52. General steps for IPSec configuration

After choosing validity period, you are asked whether to use manual tunnel or IKE at the first circled junction in Figure 52 using the following questions:

```
Should this policy enforce an IPSEC action? [No]:
```

```
Do you wish to Map a Manual IPsec to this Policy? [No]:
```

And you select the authentication method (PKI or pre-shared key) at the second circled point. According to your selection, you configure different steps. For pre-shared key only one more step is required to *add remote end user*.

For PKI, the following additional steps in Figure 53 should be performed:

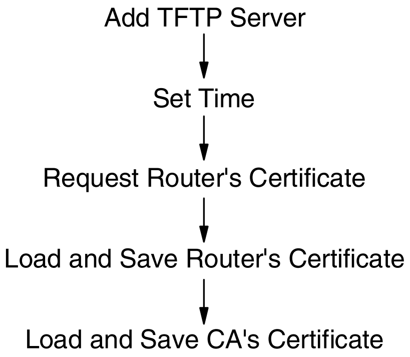

Add TFTP Server
Set Time
Request Router's Certificate
Load and Save Router's Certificate
Load and Save CA's Certificate

Figure 53. Steps for PKI configuration

Each of these steps is explained in the following sections. As an aid in understanding the different parameters used, we reference the sample network in Figure 54. In this configuration we want to authenticate all the traffic going between the 192.168.101.0 and 192.168.102.0 and the endpoints of the tunnel are 192.168.211.1 and 192.168.211.2.

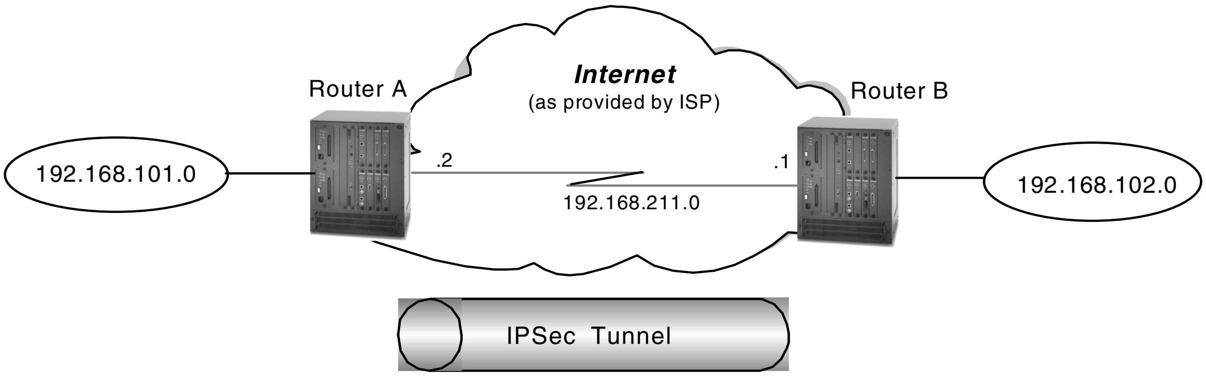


Figure 54. Sample network used in IPSec tunnel definition

To configure IPSec with MRS/AIS/MAS, an encryption package is required. For 2210, the encryption package is the part of the running image. But IBM 2212 and 2216 routers need to load the encryption package. `RELOAD` (not restart) the router to make effects of loading the encryption package.

```
Config (only)>LOAD ADD PACKAGE encryption
encryption package configured successfully
This change requires a reload.
Config (only)>RELOAD y
```

Figure 55. Loading encryption package

Another prerequisite for defining an IPSec tunnel is to configure your hardware interfaces, IP addresses and masks on each router interface that will serve as an IPSec tunnel endpoint. There are multiple ways to accomplish this using both the Config tool and the command line interface from the router console. These methods are not discussed in this redbook. However, Appendix 31, “Basic router configuration with MRS/AIS/MAS V.3.3” on page 567 shows one way to do it using the quick config command dialog from the router console.

Enabling IPSec is the final common step for three different IPSec tunnels. See Figure 56 to enable IPSec:

```
Branch *TALK 6
Branch Config>FEATURE IPSec
IP Security feature user configuration
Branch IPsec config>IPV4
Branch IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
Branch IPV4-IPsec config>EXIT
Branch IPsec config>
Branch *RESTART
```

Figure 56. Enabling IPSec

Now the IPSec architecture defines a policy database that is used to determine which packets should be processed by IPSec. Steps for defining the policy are composed of several various substeps according to the type of IPSec tunnel. 6.2.1, “Configuring manual IPSec tunnels” on page 94,Chapter 6.2.2, “Configuring IKE with pre-shared keys” on page 104, 6.2.3, “IKE with PKI configuration” on page 119 show how to configure each type of tunnel.

6.2.1 Configuring manual IPSec tunnels

Let us start with the manual tunnel that uses manual key for IPSec tunnel. The examples are based on configuring router A; router B is configured the same way. We choose to define the policy starting at the top of the tree and allowing the router to guide us through the creation of all the branch and leaves. Figure 57 shows what the contents of the policy tree are while configuring the manual tunnel in our sample network.

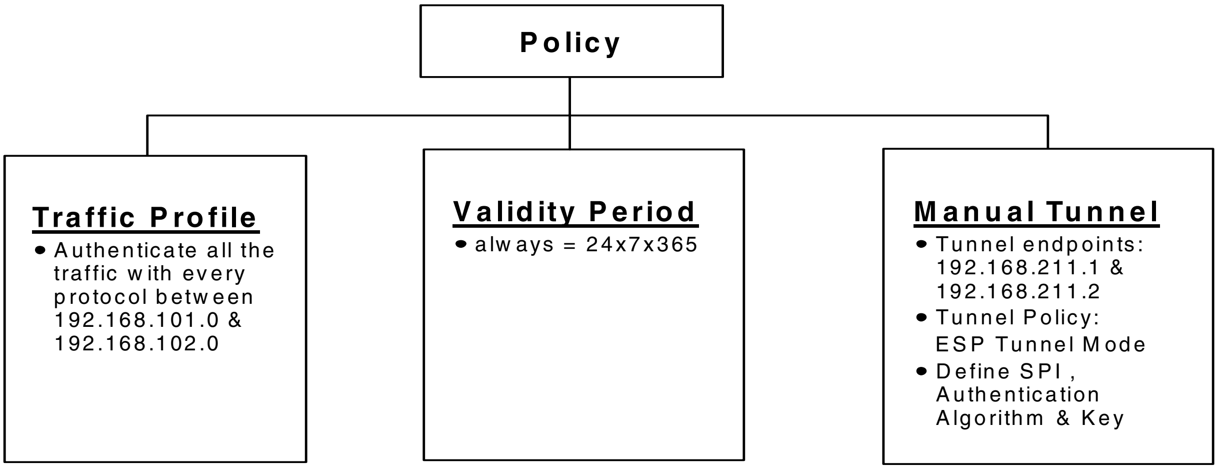

Policy
Traffic Profile
• Authenticate all the traffic with every protocol between 192.168.101.0 & 192.168.102.0
Validity Period
• always = 24x7x365
Manual Tunnel
• Tunnel endpoints: 192.168.211.1 & 192.168.211.2
• Tunnel Policy: ESP Tunnel Mode
• Define SPI , Authentication Algorithm & Key

Figure 57. Policy tree for manual tunnel

6.2.1.1 Adding policy

The policy is configured from the policy feature through the `add policy` command. You are prompted for a name for the policy, which can be any name of your choice. The next question is the priority of this policy. The larger the numerical value of the number, the higher the priority. This is taken into consideration if a traffic flow matches more than two policies. Figure 58 shows this command:

```
Branch Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ipsec_man_101_102
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
```

Figure 58. Adding policies

6.2.1.2 Defining profiles in manual tunnel

Traffic profile details are defined in a left leaf of the policy tree as shown in Figure 57 on page 95. Figure 59 gives router commands for this configuration. As a profile does not exist, the only profile offered is option 0:new profile. If you had defined any profiles using the add profile command they would be listed here. The profile defines to what traffic this policy will be applied. The router can look at the source and destination IP addresses, protocol number, source and destination port, and TOS byte. As we selected option 0 we will be guided through creating a profile. You are asked for the name of the profile, so try to make the name as meaningful as possible, especially if you are going to use this profile in other policies. You are then prompted for the IP addresses. For both the source and destination you are asked if the address is netmask, range or single address. Netmask allows you to define a profile for a subnet, range defines a specific range of IP addresses. The subsequent questions for netmask are shown in Figure 59. For range you are asked for the starting IP address and ending IP address. In this scenario, we want the traffic profile to be going from the 192.168.101.0 network to the 192.168.102.0 network.

Note

If you say that the source and destination addresses are 0.0.0.0 with a mask of 0.0.0.0, that is all IP addresses.

After you are asked for details on the destination address format, you are asked about the IP protocol. You can say TCP only, UDP only, all protocols, or a specific range. If you take option 4 you will be asked for the starting protocol number and the ending protocol number. We want all the protocols to be secured.You are then asked which port numbers - both source and destination. If you want all port numbers, take 0 for the start and 65,535 for the end. You can only define one range per policy. In this example we want all ports. The next field of interest in the IP header is the DS-byte - this used to be the TOS byte and has been renamed with the introduction of Differentiated Services. You are asked for the mask to be applied to the byte - this asks at which of the bits you wish to look. So 0 means that I do not care about the setting of this byte; FF would mean I care about the setting of all of these bits; E0 would mean I only care about the setting of the first three bits, etc. You are then asked for the value to match against after the mask has been applied. Let us look at a few examples:

- Mask of FF, value 00 = this policy will only apply to packets with zero in the DS-byte.
- Mask of FF, value E0 = this policy will only apply to packets with a DS-byte of 1110000.
- Mask of E0, value E0 = this policy will only apply to packets with the first three bits set, that is, we do not care what the remaining 5 bits are.
- Mask of E0, value A0 = this policy will only apply to packets with the first three bits being 101 and we do not care about the remaining 5 bits.

This has completed which parts of the packets the router should look at and what values we wish to match against to apply this policy. You are then asked if you wish to configure local and remote IDs for ISAKMP - this tells the router how to identify an IKE peer. As we are using manually keyed tunnels, we cannot use IKE and therefore, we do not need to configure the ISAKMP details. As there are not interface pair groups defined there are none listed.

```
List of Profiles:
0: New Profile

Enter number of the profile for this policy [0]?
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? 101.0-to-102.0
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 1
Enter IPV4 Source Address [0.0.0.0]? 192.168.101.0
Enter IPV4 Source Mask [255.255.255.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 1
Enter IPV4 Destination Address [0.0.0.0]? 192.168.102.0
Enter IPV4 Destination Mask [255.255.255.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:
```

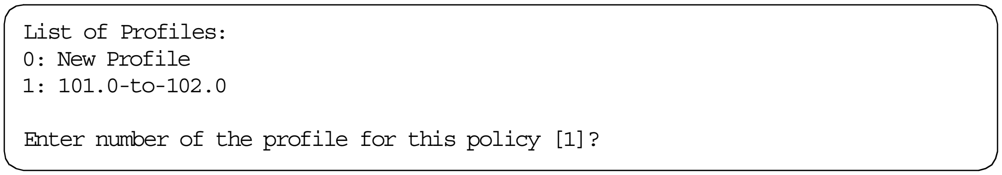
Figure 59. Defining traffic profiles

Now the router lists the profile you have created. You enter `yes` to confirm the profile or if you find anything to modify, enter `no`.

```
Here is the Profile you specified...

 Profile Name    = 101.0-to-102.0
sAddr:Mask=  192.168.101.0 : 255.255.255.0   sPort=    0 : 65535
dAddr:Mask=  192.168.102.0 : 255.255.255.0   dPort=    0 : 65535
proto     =              0 : 255
TOS       =            x00 : x00
Remote Grp=All Users
 Is this correct? [Yes]: Yes
```

Figure 60. Verifying traffic profiles

After verification, as a profile now exists, we are asked which profile do we wish to use with this policy, the one we have just created or do we wish to create another one. We will choose the one we have just created, *101.0-to-102.0,* which is option 1.



```
List of Profiles:
0: New Profile
1: 101.0-to-102.0

Enter number of the profile for this policy [1]?
```

Figure 61. Choosing traffic profiles for policy

6.2.1.3 Defining validity periods

The next leaf of Figure 57 is the validity period. Configuring the validity period is shown in Figure 62. As one does not exist, we are asked to create one. You are prompted for a name. The next piece is the lifetime of the policy - how long with this policy be valid. You can configure a start and end date which is in the numerical format of year, month, day, hour, minute and second. We want the policy to be valid forever so we have entered *. You are then asked for which months the policy is valid within that validity period. We want it to be valid for all months so we have chosen the default of all. You can define that a policy should only be valid for certain days of the week - we have chosen every day. You can define time slots within a day - we have chosen * for all day. If you enter a start time you will be prompted for the finishing time. Note that this is in 24-hour clock format. If you are going to use a policy that specifies times and dates always ensure that your clock is correct within your router. You can inspect the time by doing:

```
Config>time list

07:52:55 Monday July 19, 1999

Set by: internal clock

Time Host: 0.0.0.0 Sync Interval: 0 seconds

GMT Offset: 0 minutes

Config>
```

You can change the time using the `time set` command. There are also other options, such as synchronizing clocks between routers - see *MAS V3.2 Software User's Guide,* SC30-3886 for more details.

```
List of Validity Periods:
             0: New Validity Period

Enter number of the profile for this policy [0]?

Enter a Name (1-29 characters) for this Policy Valid Profile []?
always
Enter the lifetime of this policy. Please input the
information in the following format:
                 yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
[*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
[ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
[ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
[*]?
Here is the Policy Validity Profile you specified...

Validity Name = always
         Duration   = Forever
         Months     = ALL
         Days         = ALL
         Hours       = ALL Day
Is this correct? [Yes]:
```

Figure 62. Configuring validity periods

The validity period is listed in Figure 63. As a validity period now exists we are asked if we wish to take the period we have just defined called “always” or create a new period. We will take the one we have just added.

```
List of Validity Periods:
0: New Validity Period
1: always

Enter number of the validity period for this policy [1]?
```

Figure 63. Defining policies - validity periods

Note

There are five predefined menus for the validity period in 2216:

`0: New Validity Period`

`1: allTheTime` : 24hoursx365days

`2: allTheTimeMonThruFri` : 24hours at Monday through Friday

`3: 9to5MonThruFri` : 9:00 a.m. to 5:00 p.m. at Monday through Friday

`4: 5to9MonThruFri` : 5:00 p.m. to 9:00 a.m. at Monday through Friday

6.2.1.4 Defining manual tunnel details

We are now asked to what sort of actions this policy should apply as shown in Figure 64 on page 103. We want a manual tunnel so we say no for an IPSec action and yes to manual. As no manual tunnels exist we are prompted to create one. The questions asked are exactly the same as the ones that were asked in early releases when you used the `add tunnel` command from the IPSec feature. In fact you can still add the tunnels from there, if you wish, but the policy can only be defined from the policy feature.

When the manual tunnel has been defined you are asked for which IPSec tunnel you wish to use - option 1 for one that we have just created, option 0 to create another tunnel. We have chosen option 1. The first part of the dialog defines the tunnel name, ID, tunnel lifetime, encapsulation mode, and tunnel policy. The tunnel lifetime defaults to 46080 minutes, which converts to 32 days. The maximum is 525600 minutes, which is one year. The tunnel encapsulation mode can be set to either tunnel mode or transport mode per the IPSec architecture. Tunnel mode is the normal case between routers that are using the public network to create a VPN. Transport mode is used to create a tunnel between two end stations.

The difference between the two modes is that with tunnel mode, the entire original IP packet is encapsulated within a new IP packet. This new packet has IP source and destination addresses of the tunnel endpoints. With transport mode, the original IP header is used with the original source and destination IP addresses. From Figure 64, you can see that there are four choices for the tunnel policy:

AH This is the choice if you want to perform only authentication (the IPSec AH protocol) on packets going over this tunnel.

ESP This is the choice if you want to perform encryption (the IPSec ESP protocol) on packets going over this tunnel. Note that if you make this selection, you can also do authentication on the packets since the ESP protocol has an optional authentication feature.

AH_ESP This is the choice if you want to perform encryption and authorization using both the IPSec ESP and AH protocols. This selection indicates that for packets in the outbound direction, the packets will be encrypted first using the ESP protocol, then the AH algorithms will be run on the encrypted payload.

ESP_AH This choice also allows you to do both encryption and authorization using both the IPSec ESP and AH protocols. However, the order is reversed. With this selection, packets in the outbound direction will go through the AH algorithms first, then they will be encrypted using the ESP protocol.

At this point, the basic tunnel has been defined. Since we specified that this tunnel will use AH, the dialog now prompts us for the parameters that the AH algorithms will use. Figure 64 shows an example of these prompts.

This first series of prompts are for the AH parameters at the local end of the tunnel (the router you are configuring is router A in Figure 54 in this example). We input Router A WAN interface IP address 192.168.211.2 as a local tunnel endpoint while we define a tunnel between 192.168.211.1 and 192.168.211.2. The parameters in local authentication must be the same as the parameters in remote authentication of the router at the other side of the tunnel. For example, if you choose the HMAC-MD5 algorithm for the local authentication algorithm, then you must configure HMAC-MD5 as the other router's *remote* AH algorithm. In effect, you are defining parameters for two unidirectional Security Associations (SAs) and each tunnel endpoint must agree on the parameters used for each SA. (Remember that two SAs exist for each IPSec tunnel: one in each direction.)

You can use different parameters for the SAs in each direction. However, the parameters specified for each SA have to match at each end of the IPSec tunnel. For example:

- The local key entered in router A must match the remote key entered in router B.
- The remote key entered in router A must match the local key entered in router B.

The same principle holds true for the SPI and the AH algorithm specified.

With this said, however, we recommend that you use the same parameters for both SAs unless you have a good reason to do otherwise.

SPI is the security parameter index. You can think of this as an index into the database where the parameters for this tunnel will be stored.

Since we configured the manual tunnel, this means that we manually enter the keys that will be used for the AH and ESP algorithms. We use simple keys in this example. We will configure the IBM Nways router to use ISAKMP/Oakley, in 6.2.2, “Configuring IKE with pre-shared keys” on page 104, the automated key management protocols will set the keys and refresh them periodically. The IPSec architecture specifies ISAKMP/Oakley as the protocols to use for its Integrated Key Exchange (IKE) framework.

In total, you have to enter four keys when configuring AH:

- Local key in router A
- Remote key in router A
- Local key in router B
- Remote key in router B

Also remember that each of the above keys must be typed twice to prevent mistakes. At the time of this writing, any typing mistakes will terminate the `add tunnel` command and you must start over.

After these parameters have been entered, the prompts switch to questions about the AH parameters for the remote end of the tunnel. As you might expect, the parameters entered for remote authentication must match parameters entered for local authentication of the router at the other side of the tunnel. For example, if you specify at the far end that outgoing packets should use the HMAC-MD5 algorithm to generate the Integrity Check Value (ICV), then you need to specify that incoming packets here at this end of the tunnel will be authenticated using the same HMAC-MD5 algorithm (and the same key). This is the idea behind configuring the parameters used at the remote end here at the local end of the tunnel. Figure 64 shows an example of these prompts.

The IPSec architecture defines a technique for ensuring that a hacker cannot intercept a datagram and play it back at some later time without being detected. This is called anti-replay or replay prevention support. Per the architecture, MRS/AIS/MAS implements this support using a sequence number that is included in the AH header of every packet. If enabled, the receiving side of the SA checks all sequence numbers on incoming packets to make sure that they fall within a window and have not been received previously. The sequence number is a 32-bit field in the header and is initialized to zero at the inception of the SA.

For manual IPSec implementations, it is not recommended to enable anti-replay support. This is because the architecture stipulates that the sequence number cannot wrap when it reaches the highest number in the range (2^{32}=4.29 billion packets). This means that if you enable anti-replay support, you have to ensure that the SA is re-established every 4.29 billion packets. When MRS/AIS/MAS implements ISAKMP/Oakley, there will be automated ways to refresh the SAs and hence this will not be a restriction.

You are then asked if the manual tunnel flows into another tunnel - this relates to the tunnel-in-tunnel feature that was first shipped in V3.2 of the code. We do not wish to use DiffServ or RSVP so our policy is completed.

```
Should this policy enforce an IPSEC action? [No]:
Do you wish to Map a Manual IPsec to this Policy? [No]: yes
Manual IPsec tunnels:
0: New IPSEC Manual Tunnel

Enter Tunnel ID of the Manual Tunnel Record [0]?
Adding tunnel 1.
Tunnel Name (optional) []? tun-101.0-102.0
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ah
Local IP Address [192.168.101.1]? 192.168.211.2
Local Authentication SPI (>= 256) [256]?
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex
(0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 192.168.211.1
Remote Authentication SPI (>= 256) [256]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex
(0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
A new tunnel is added. The policy must be configured
and reset.
Manual IPsec tunnels:
0: New IPSEC Manual Tunnel
Tunnel ID: 1Tunnel Start 192.168.211.2Tunnel End 192.168.211.1

Enter Tunnel ID of the Manual Tunnel Record [0]? 1
Does this manual tunnel flow into another Secure Tunnel? [No]:
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?
```

Figure 64. Configuring manual tunnel detail

After the tunnel definition is completed, you can list the definition back out to check for errors such as mistyped IP addresses. Figure 65 shows an example of this command:

```
Here is the Policy you specified...

Policy Name     = ipsec_man_101_102
State:Priority =Enabled    : 5
Profile        =101.0-to-102.0
Valid Period   =always
Manual Tunnel  =1
TunnelInTunnel =No
Is this correct? [Yes]:
Branch Policy config>
```

Figure 65. Verifying manual tunnel detail

Note

This policy could have also been generated from the leaves with the following individual commands:

1. Create a profile *101.0-to-102.0* using the `add profile` command.
2. Create a validity period *always* using the `add validity-period` command.
3. Create a manual tunnel *`tun-101.0-102.0`* using the `add tunnel`.
4. Finally pull all the items together using the `add policy` command.

6.2.1.5 Activating policies defined

We could use either way to make the configuration changes active. Use the `reset database` command in the talk 5 policy feature as shown in Figure 66:

```
Center *TALK 5
Center +FEATURE Policy
IP Network Policy console
Center Policy console>RESET DATABASE
Policy Database reset successful
```

Figure 66. Resetting database

Or use `restart` command as shown in Figure 67:

```
Branch *restart
```

Figure 67. Restarting router

6.2.2 Configuring IKE with pre-shared keys

Now we will create a secure IPSec tunnel between router A and router B that will use automatic key generation with pre-shared keys. The examples are based on configuring router B; router A is configured the same way.

Since the previous encryption package has been loaded, router interfaces with IP address are defined and IPSec is enabled, we start with defining a policy for IKE with a pre-shared key. We also will define the policy starting at the top of the tree and allowing the router to guide us through the creation of all the branches and leaves. Figure 68 defines the contents of the policy tree while configuring the IPSec tunnel using IKE with a pre-shared key in our sample network.

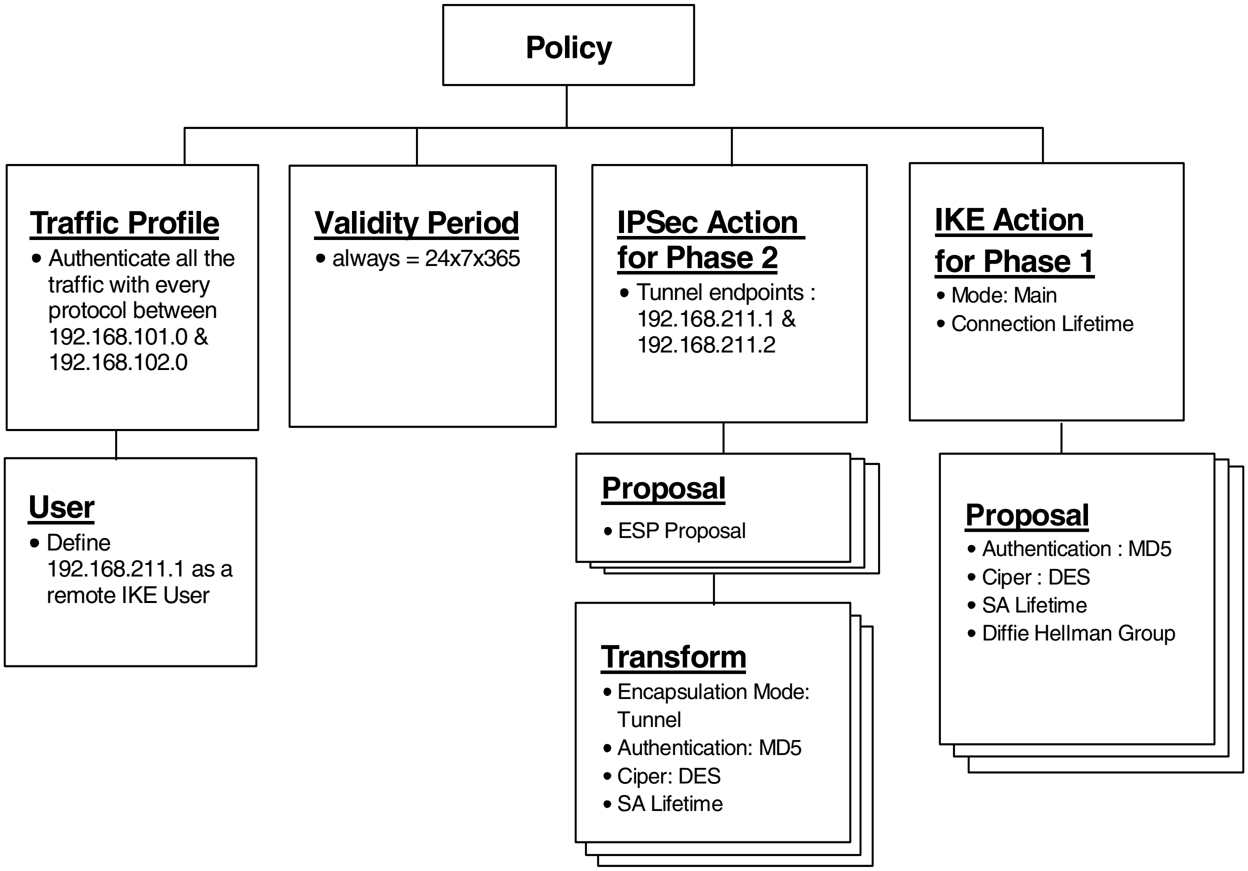


Figure 68. Policy tree for pre-shared key

6.2.2.1 Adding IKE peer user

The first step for configuring the policy for IKE pre-shared key is to define the remote IKE peer with pre-shared keys. The pre-shared keys of every remote peer need to be configured. This highlights why the use of pre-shared keys is not very scalable. Remember though that it is more secure than the manual tunnel approach (as shipped since V3.1 of the router code) because the derived keys are refreshed. The keys are defined in the policy feature.

The talk 6 `add user` command in the policy feature is used to configure the remote IKE peer and the keys shown in Figure 69 on page 106. The identifier chosen was the IP address. This must be the IP address of the tunnel endpoint - in this scenario, the IP address on the WAN interface. When you are defining the profile in the remote peer, ensure that “Enter local identification to send to remote” matches what was configured as the way to identify the user in the local router. Select the identifier of the remote end with care if you are performing Phase 1 negotiations in main mode. Recall that in main mode the identity of the peer is not exchanged until messages 5 and 6, but before reaching these messages the IKE peer must know the pre-shared key when it generates the keys. So at the time of performing the key generations, the only method of identifying the remote device is by its IP address. If the remote device’s IP address is dynamically assigned, you must perform Phase 1 negotiations in aggressive mode as the identities are exchanged prior to the key generation.

Users can be grouped together, but it is most likely that the grouping will be used when the authentication is through digital signatures. Groups should be considered in situations in which the policy is wild-carded out for the destination addresses and you wish to specify a list of peers that are to be allowed access. These peers will still be authenticated by their key, but the policy database will perform an additional authentication step by ensuring that the local ID sent by the remote peer matches one of the IDs specified in the group of the policy's profile. Later we will see when a group of users can be associated with a particular policy. Add a user (for the remote IKE peer) and the pre-shared key. The IP address must be the same as the tunnel endpoint. The pre-shared secret does not show as you type it in. The talk 6 `add user` command in the policy feature is used to configure the keys shown in Figure 69:

```
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>ADD USER
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 192.168.211.2
Group to include this user in [ ]?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (8 characters) in ascii:
```

Figure 69. Adding user as a pre-shared key of remote end

Verify the user you defined as shown in Figure 70:

```
Here is the User Information you specified...

Name      = 192.168.211.2
        Type      = IPV4 Addr
        Group     =
        Auth Mode =Pre-Shared Key
Is this correct? [Yes]:
```

Figure 70. Verifying user created

6.2.2.2 Adding policy

The pre-shared key has been configured; the next step is to add the policy. Now configure the policy of IPSec tunnel with the IKE pre-shared key *ike-pre-101-102* through the `add policy` command in Figure 71:

```
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-pre-101-102
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
```

Figure 71. Adding policy

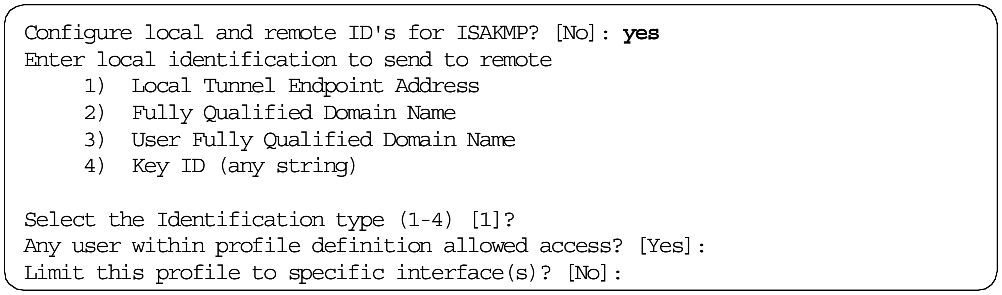
6.2.2.3 Defining profiles

After configuring a policy name, the next step is to define the profile as shown in Figure 72. The profile defines to what traffic flow this policy applies. The router can check the source and destination IP addresses, protocol number, source and destination port number, DS (TOS) byte in the IP header to determine if a traffic flow matches the policy. The router will list all the available profiles. As we defined a manual tunnel in 6.2.1, “Configuring manual IPSec tunnels” on page 94, the router offers you two choices, 0 for a new profile and 1 for *101.0-to-102.0* defined for the manual tunnel. Since we created a new profile for IKE tunnel with a pre-shared key, choose 0. The profile could have been defined using the `add profile` command. In this scenario, we want the traffic profile to go from the 192.168.101.0 network to the 192.168.102.0 network with all protocols.

```
List of Profiles:
        0: New Profile
        1: 101.0-to-102.0

Enter number of the profile for this policy [1]? 0
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to
the Remote Client Proxy
Enter a Name (1-29 characters) for this Profile [101.0-to-102.0]?
101.0-to-102.0-pre
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.0
Enter IPV4 Source Mask [255.255.255.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 192.168.101.0
Enter IPV4 Destination Mask [255.255.255.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
```

Figure 72. Defining traffic profiles

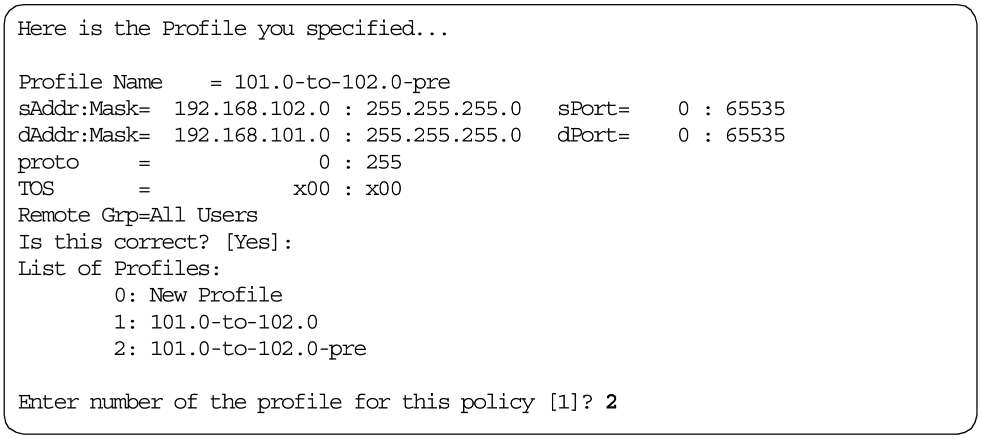
You are then prompted to configure IDs for ISAKMP as shown in Figure 73. You must do this or the other peer will not be able to identify you. The method chosen here must match what you configure in the remote peer when defining the shared key - that is, to ensure your methods of identification are consistent. You are asked if this profile should be used by any users. Normally you will not need to restrict a profile to specific users since all ISAKMP Phase 1 negotiations are authenticated with either public certificates or pre-shared keys. However, in some remote access situations in which the policy is wild-carded out for the destination addresses, it may be wise to specify a list of users that are allowed access. These users will be authenticated through the normal ISAKMP authentication methods, but the policy database will perform an additional authentication step by ensuring that the local ID sent by the remote peer matches one of the IDs specified in the group of the policy’s profile. In this example we are not restricting the profile to a specific set of users. Figure 73 shows how to configure an ID for ISAKMP:



```
Configure local and remote ID's for ISAKMP? [No]: yes
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:
```

Figure 73. Configuring ID for ISAKMP

Confirm the traffic profile you create. Option 2 selects *101.0-to-102.0-pre* that has just been created.

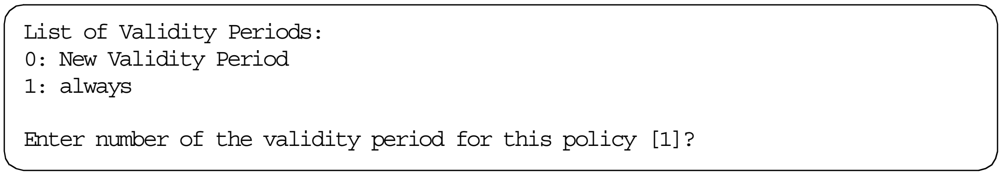


```
Here is the Profile you specified...

Profile Name    = 101.0-to-102.0-pre
sAddr:Mask=  192.168.102.0 : 255.255.255.0   sPort=    0 : 65535
dAddr:Mask=  192.168.101.0 : 255.255.255.0   dPort=    0 : 65535
proto     =              0 : 255
TOS       =            x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: 101.0-to-102.0
        2: 101.0-to-102.0-pre

Enter number of the profile for this policy [1]? 2
```

Figure 74. Verifying traffic profile

6.2.2.4 Defining validity periods

The next step is to define the validity period as you can see in the policy tree in Figure 68 on page 105. Because we defined validity period “always” in 6.2.1, “Configuring manual IPSec tunnels” on page 94, the router prompts two choices, 0 for new and 1 for “always”. The validity period could have been defined using the add validity period. Refer to 6.2.1, “Configuring manual IPSec tunnels” on page 94 for a predefined validity period menu of 2216 and how to define a new validity period.



```
List of Validity Periods:
0: New Validity Period
1: always

Enter number of the validity period for this policy [1]?
```

Figure 75. Configuring validity period

6.2.2.5 Defining IPSec action for IKE Phase 2

The next step is to create an IPSec action as shown in Figure 68 on page 105. In Figure 73 on page 108 as you create an IPSec action you will be prompted for details about the tunnel endpoints, and then be asked for the IKE Phase 2 proposals and transforms. As no IPSec actions exist you are prompted to create one, which we will call “tun-101-102”. You would be prompted through the same questions if you used the `add ipsec-action` command.

The router will prompt whether this action is to block or permit. If you say block, the traffic will not be secured or forwarded. If you say permit, the traffic will be forwarded and the next question asks whether it should be in the clear or secured. If the answer is in the clear, the traffic will not be handled by IP Security. Clearly we need option 2, and now the router will prompt you through the details of the IPSec SAs. Our tunnel endpoint is our WAN interface of both routers, 192.168.211.1 and 192.168.211.2. Remember that we chose that our peers would be identified by the tunnel endpoint address so take care to ensure that this value matches the identifier that will be configured in the remote peer. Conversely ensure that the value you enter for the remote tunnel endpoint matches that configured for the identifier of the remote system. Note that if you are doing IPSec in a remote access scenario, you may not know the IP address in advance. In this case you would use a different identifier for the user (such as a fully qualified domain name) and specify the remote tunnel endpoint address as 0.0.0.0. The remote device must initiate the IKE negotiations and you must perform Phase 1 negotiations in aggressive mode as you need to know the identity of the remote end to locate the correct pre-shared keys so the master key can be generated.

You are then asked if this traffic will flow into another IPSec tunnel. This relates to the tunnel-in-tunnel function shipped in V3.2 of the router code. A sample diagram of this function is shown in Figure 76. Either tunnel can have any IPSec characteristics:

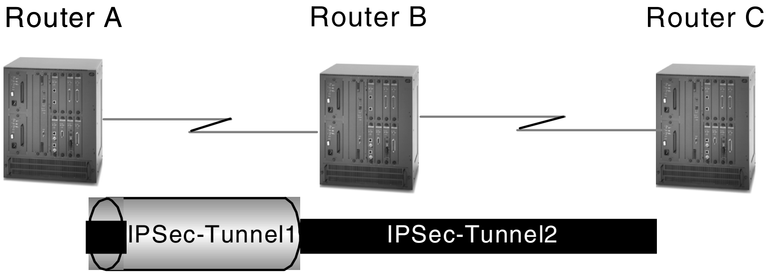


Figure 76. Tunnel-in-tunnel function

The router then prompts you through the SA characteristics for this tunnel. You are asked about percentages of the lifesize/time that are acceptable. This is used if the peer offers a different value of lifetime - if the SA lifesize/time received is less than 75% it will not be acceptable. When the IPSec header is created, many of the fields of the IP header are copied from the header of the packet being secured. You can control how the do not fragment field is set. You can either copy from the original packet, set the DF bit or if it is turned on in the original packet, turn it off.

“Enable replay prevention” defines whether the sequence numbers should be checked on received packets. The next question is whether this SA should be created as a system startup. Specifying no indicates that this SA should only be negotiated when packets are received that match this policy. We have now defined the contents of the IPSec header. We know we need to define what type of SA will be negotiated. That is what we need to define an IKE Phase 2 proposal and transform. As no proposals exist, we are prompted to create one. You would be prompted through the same questions if you used the `add ipsec-proposal` command.

.

```
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? tun-101-102
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [9.24.104.203]? 192.168.211.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 192.168.211.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
```

Figure 77. Configuring IPSec action for IKE Phase 2

6.2.2.6 Defining IPSec proposal for IKE Phase 2

We are going to create a proposal called “esp-prop1” which states that we want to do ESP, but we do not require PFS. Each proposal requires a transform; the router prompts us to create one by choosing option 0.

```
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
List of IPSEC Proposals:
        0: New Proposal
        1: strongP2EspProp
        2: strongP2EspAhProp
        3: veryStrongP2EspProp
        4: veryStrongP2EspAhProp

Enter the Number of the IPSEC Proposal [1]? 0
Enter a Name (1-29 characters) for this IPsec Proposal []? esp-prop1
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: yes
```

Figure 78. Configuring IPSec proposal

There are four predefined menus for the ESP proposal in 2216. Table 5 shows the predefined ESP proposals:

Table 5. Predefined ESP proposal

ESP proposal	DH Grp	Encap	Transform name	Auth	Ciper
StrongP2ESPProp	Grp1	Tunnel	ESPTunnelMD5andDES	HMAC-MD5	DES
			ESPTunnelSHAandDES	HMAC-SHA	DES
StrongP2ESPAhProp	Grp1	Tunnel	ESPTunnelDES	None	DES
			ESPTunnel3DES	None	3DES
VeryStrongP2ESPProp	Grp1	Tunnel	ESPTunnelMD5and3DES	HMAC-MD5	3DES
			ESPTunnelSHAand3DES	HMAC-SHA	3DES
VeryStrongP2ESPAhProp	Grp1	Tunnel	ESPTunnel3DES	None	3DES

6.2.2.7 Defining IPSec transform for IKE Phase 2

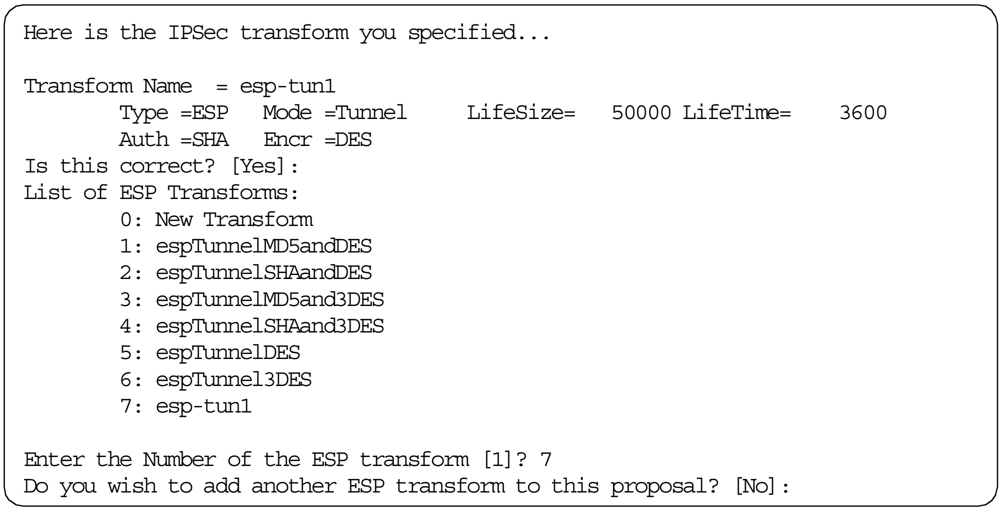
We will make a transform called “esp-tun1” which is an ESP SA in tunnel mode. Figure 79 shows how to create an IPSec transform. You would be prompted through the same questions if you used the `add ipsec-transform` command.

There are six predefined menus for ESP transform in 2216. Now we create a new one by choosing option 0. We will do authentication using HMAC_MD5 and encryption using DES. You are prompted for the SA lifetime/lifesize of the Phase 2 tunnel. When the SA lifetime expires, IKE will perform another Phase 2 calculation to refresh the keys.

```
List of ESP Transforms:
        0: New Transform
        1: espTunnelMD5andDES
        2: espTunnelSHAandDES
        3: espTunnelMD5and3DES
        4: espTunnelSHAand3DES
        5: espTunnelDES
        6: espTunnel3DES
Enter the Number of the ESP transform [1]? 0
Enter a Name (1-29 characters) for this IPsec Transform [ ]? esp-tun1
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [2]?
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]?
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]?
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]?
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]?
Security Association Lifetime, in seconds (120-2147483647) [3600]?
```

Figure 79. Configuring IPSec transform

The router will list the transform you have defined. If it is correct, enter `yes` . The router prompts you for which transform the IKE proposal “esp-prop1” should use. Selecting option 7 takes the transform just created “esp-tun1”, or you could choose to add additional transforms at this time. If you take the transform, you will then be asked if this proposal has more than one transform. In this example, we will only offer one transform. You could offer another ESP transform with different algorithms for authentication or encryption algorithms.

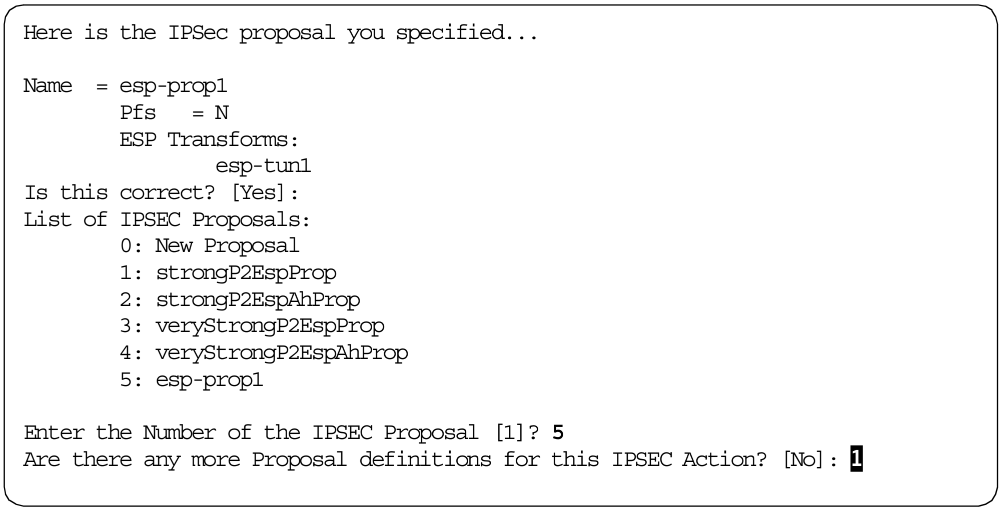


```
Here is the IPSec transform you specified...

Transform Name  = esp-tun1
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
        0: New Transform
        1: espTunnelMD5andDES
        2: espTunnelSHAandDES
        3: espTunnelMD5and3DES
        4: espTunnelSHAand3DES
        5: espTunnelDES
        6: espTunnel3DES
        7: esp-tun1

Enter the Number of the ESP transform [1]? 7
Do you wish to add another ESP transform to this proposal? [No]:
```

Figure 80. Verifying IPSec transform

6.2.2.8 Choosing proposal and transform for IKE Phase 2

In Figure 81 you are prompted for which proposal this IPSec action should use. Option 5 selects the proposal that has just been created, or choose option 0 to create another one. If you wanted to have multiple proposals for this action you would answer yes to question 1 and you would be prompted to create more proposals (and transforms). Remember that a proposal is a set of transforms from which the IKE peer can choose. A proposal can have either or both of the IPSec protocols offered.



```
Here is the IPSec proposal you specified...

Name  = esp-prop1
        Pfs   = N
        ESP Transforms:
                esp-tun1
Is this correct? [Yes]:
List of IPSEC Proposals:
        0: New Proposal
        1: strongP2EspProp
        2: strongP2EspAhProp
        3: veryStrongP2EspProp
        4: veryStrongP2EspAhProp
        5: esp-prop1

Enter the Number of the IPSEC Proposal [1]? 5
Are there any more Proposal definitions for this IPSEC Action? [No]: 1
```

Figure 81. Verifying IPSec proposal

Now the router shows the IPSec action you defined in Figure 82. By choosing option 1 we select *tun-101-102* as our IPSec action.

```
Here is the IPSec Action you specified...

IPSECAction Name = tun-101-102
        Tunnel Start:End        =  192.168.211.1 : 192.168.211.2
        Tunnel In Tunnel        =            No
        Min Percent of SA Life  =            75
        Refresh Threshold       =            85 %
        Autostart               =            No
        DF Bit                  =          COPY
        Replay Prevention       =      Disabled
        IPSEC Proposals:
                esp-prop1
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: tun-101-102

Enter the Number of the IPSEC Action [1]?
```

Figure 82. Verifying IPSec action

6.2.2.9 Defining ISAKMP action for IKE Phase 1

The only missing information from our policy tree is what we wish to offer for IKE Phase 1. As no ISAKMP action exists, we are prompted to create one. You would be prompted through the same questions if you used the `add isakmp-action` command.

We are creating an ISAKMP action called “ike-1” which occurs in main mode in Figure 83. The lifesize and lifetime parameters define how long an IKE Phase 1 tunnel can exist even through refreshes. Once this parameter has been reached, the tunnel must be started from the beginning, rather than just generating refreshed keys. Note that in this release, the router actually rebuilds the tunnel when the SA lifesize/time is reached. You can also control if the SA is negotiated at system initialization or only when traffic is received that matches the policy (answer = no). The router needs to know what IKE Phase 1 proposals offer and as none exist, the router prompts the creation of one in Figure 83. You would be prompted through the same questions if you used the `add isakmp-proposal` command.

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: generalPhase1Action

Enter the Number of the ISAKMP Action [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Action []? ike-1
List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]:
```

Figure 83. Configuring ISAKMP action

6.2.2.10 Defining ISAKMP proposal for IKE Phase 1

We will create an IKE Phase 1 proposal, called “ike-prop1” that offers pre-shared keys, with authentication using MD5, encryption by DES, an SA lifetime as shown in Figure 84 on page 116. The lifetime/lifesize is defined as the amount of time/size that the Phase 1 SA can exist before the keys are refreshed. Actually, in this release, this parameter defines when the Phase 1 SA tunnel will be torn down and negotiated from the beginning.

So what is the difference between connection lifetime and SA lifetime?

Assume that the connection lifetime is 15 hours and the SA lifetime is set to 1 hour. The Phase 1 tunnel can be refreshed every hour up to a maximum of 15 hours where the connection lifetime is hit and no refreshes are allowed without rebuilding from the ground up. In this release, the connection lifetime/size is the same as the SA lifetime/size. This means that the Phase 1 tunnel is torn down each time the SA lifetime/size is hit and not really refreshed. It will be rebuilt, however, when the Phase 2 tunnel needs to be refreshed. The parameter is still there because it is needed if the policy has been retrieved from LDAP.

Note

A predefined menu for IPSec action in 2216 is `generalPhase1Action`. IPSec action by `generalPhase1Action` is as follows:

- Exchange Mode: Main
- Lifetime in seconds: 30000
- Lifesize in KB: 5000
- ESP proposals
    - StrongP1PropSharedKey
    - StrongP1PropRSACert
    - VeryStrongP1PropSharedKey
    - VeryStrongP1PropRSACert

Refer to Table 6 for details of each proposal.

```
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal
        1: strongP1PropSharedKey
        2: strongP1PropRSACert
        3: veryStrongP1PropSharedKey
        4: veryStrongP1PropRSACert

Enter the Number of the ISAKMP Proposal [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Proposal []? ike-prop1

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  Certificate (RSA SIG)

Select the authentication method (1-2) [1]?

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]?

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2
```

Figure 84. Configuring ISAKMP Proposal

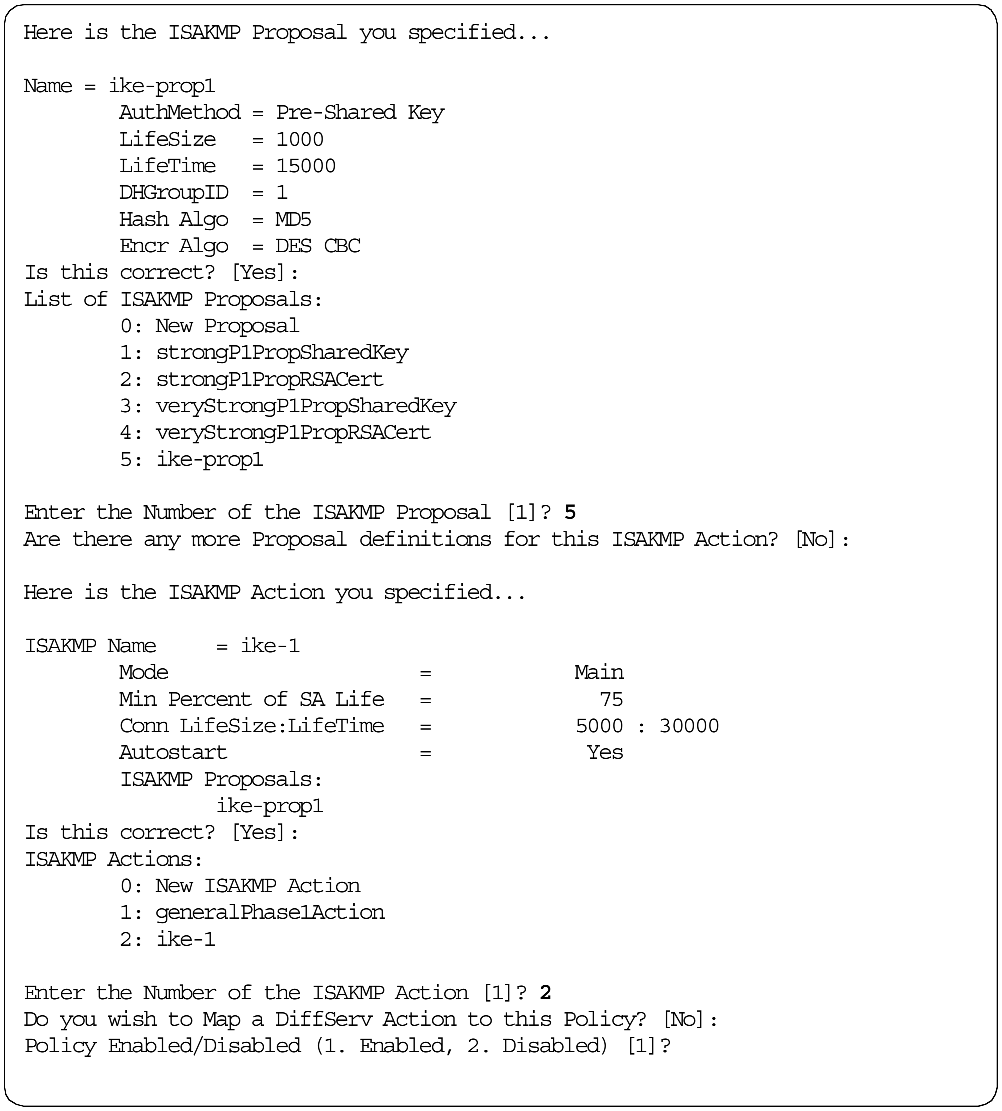
There are four predefined menus for the ISAKMP proposal in 2216. Table 6 shows the predefined ISAKMP proposals.

Table 6. Predefined ESP proposal

ESP proposal	Auth	Hash	Ciper	DH Grp	Lifetime (sec)	Lifetime (KByte)
StrongP1PropSharedKey	Pre-Shared	MD5	DES	Grp1	15,000	1,000
StrongP1PropRSACert	RSA Signature	MD5	DES	Grp1	15,000	1,000
VeryStrongP1PropSharedKey	Pre-Shared	SHA	3DES	Grp1	15,000	1,000
VeryStrongP1PropRSACert	RSA Signature	SHA	3DES	Grp1	15,000	1,000

6.2.2.11 Choosing ISAKMP action and policy

Now confirm your ISAKMP proposal and if it is correct, choose option 5 created now. Next verify the ISAKMP action you specified and if it is correct then select option 2. This is shown in Figure 85.

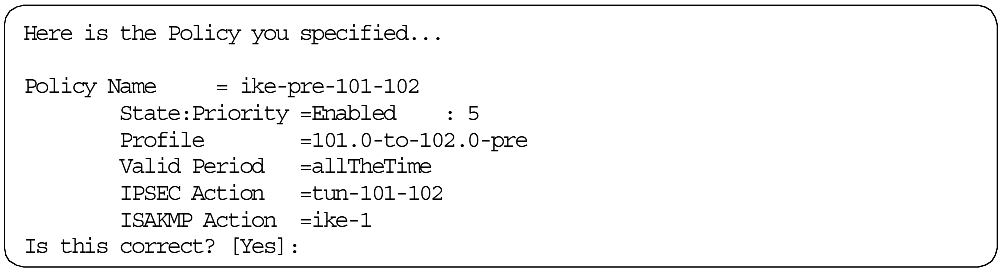


```
Here is the ISAKMP Proposal you specified...

Name = ike-prop1
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: strongP1PropSharedKey
        2: strongP1PropRSACert
        3: veryStrongP1PropSharedKey
        4: veryStrongP1PropRSACert
        5: ike-prop1

Enter the Number of the ISAKMP Proposal [1]? 5
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name     = ike-1
        Mode                     =            Main
        Min Percent of SA Life   =              75
        Conn LifeSize:LifeTime   =            5000 : 30000
        Autostart                =             Yes
        ISAKMP Proposals:
                ike-prop1
Is this correct? [Yes]:
ISAKMP Actions:
        0: New ISAKMP Action
        1: generalPhase1Action
        2: ike-1

Enter the Number of the ISAKMP Action [1]? 2
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?
```

Figure 85. Verifying ISAKMP Proposal and ISAKMP Action

6.2.2.12 Verifying defined policy

We have defined every leaf for the policy ike-pre-101-102 now. Finally the router is prompted for confirming the policy as shown in Figure 86:



```
Here is the Policy you specified...

Policy Name     = ike-pre-101-102
        State:Priority =Enabled    : 5
        Profile        =101.0-to-102.0-pre
        Valid Period   =allTheTime
        IPSEC Action   =tun-101-102
        ISAKMP Action  =ike-1
Is this correct? [Yes]:
```

Figure 86. Verifying policy

Note

The same configuration could have been created by using the following commands from the bottom of the policy tree:

- `add profile` to create the profile "101.0-to-102.0-pre"
- `add validity` to create the validity period "always"
- `add ipsec-transform` to create the IKE Phase 2 transform, "esp-tun1"
- `add ipsec-proposal` to create the IKE Phase 2 proposal "esp-prop1" which uses transform "esp-tun1"
- `add ipsec-action` to define the Phase 2 tunnel, "tun-101-102" using proposal "esp-prop1" and transform "esp-tun1"
- `add iskamp-proposal` to define the IKE Phase 1 proposal "ike-prop1"
- `add isakmp-action` to define the IKE Phase 1 tunnel "ike-1" which uses proposal "ike-prop1"
- `add policy` which uses profile "ike-pre-101-102", validity period "always", IPSec action "tun-101-102" and ISAKMP action "ike-1"

6.2.2.13 Viewing defined policy and disabling unused policy

After finishing defining policies we could list all the policies created and disable the policies we do not use. Since we have finished defining the required policy we list all the policies created and we disable the policy for the manual tunnel as shown in Figure 87:

```
Center Policy config>LIST POLICY ALL

Policy Name     = ipsec_man_101_102
        State:Priority =Enabled   : 5
        Profile        =101.0-to-102.0
        Valid Period   =allTheTime
        Manual Tunnel  =1
        TunnelInTunnel =No

Policy Name     = ike-pre-101-102
        State:Priority =Enabled   : 5
        Profile        =101.0-to-102.0-pre
        Valid Period   =allTheTime
        IPSEC Action   =tun-101-102
        ISAKMP Action  =ike-1
Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
 [?]?

        1: ipsec_man_101_102
        2: ike-pre-101-102

Number of policy [1]? 1
```

Figure 87. Listing and disabling policy

6.2.2.14 Activating policies defined

We could use either way to make the configuration changes active. Use `reset database` command in the talk 5 policy feature as shown in Figure 88.

```
Center *TALK 5
Center +FEATURE Policy
IP Network Policy console
Center Policy console>RESET DATABASE
Policy Database reset successful
```

Figure 88. Resetting database

Or use the `write` and `reload` or `restart` commands as shown in Figure 89:

```
Center Config>WRITE
Config Save: Using bank A and config number 3
ranch Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 89. Reloading router

6.2.3 IKE with PKI configuration

We will now implement a configuration that uses PKI (or certificates) for authentication. In this example define a PKI authenticated tunnel between Router A and Router B and enforce a policy where traffic originating from Router A destined to Router B (and vice versa) will be made to flow over the tunnel. This example could easily be extended to force other traffic flows over the tunnel, for example, traffic between subnets 198.168.100.0 and 198.168.101.0.

The first step is to disable all existing policies to avoid confusion and to assist in problem determination by isolating the scope of any problems that may be encountered. This is achieved by the `TALK 6, FEATURE POLICY, DISABLE POLICY` commands.

6.2.3.1 Define a policy

Once all the existing policies have been disabled the next step is to define a new traffic policy. This is done in the same way as described in previous examples in this chapter except the policy using PKI as its authentication method. The traffic profile that we will define in this example will send traffic to and from Router A and Router B over the PKI authenticated tunnel.

The traffic policy will be called *ike-ds-211-211*. The following screen shows what the definition looks like in Router A:

```
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-ds-211-211
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
```

Figure 90. Definition of a new policy for PKI authentication

The router then prompts us for a traffic profile. We will define a new profile for this policy. Once the new profile has been defined the router prompts us again for the traffic profile. This time we select the profile that has just been defined.

```
List of Profiles:
        0: New Profile
        1: 101.0-to-102.0
        2: 101.0-to-102.0-pre
        3: 3.0-to-100.0.pre
        4: 211.0-to-211.0-pre

Enter number of the profile for this policy [1]? 0
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? 211.0-to-211.0-ds
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.211.1
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Destination Address [0.0.0.0]? 192.168.211.2

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]: y
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]? 1
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:


Here is the Profile you specified...



Profile Name    = 211.0-to-211.0-ds
        sAddr     =  192.168.211.1 :  sPort=    0 : 65535
        dAddr     =  192.168.211.2 :  dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]: y
```

Figure 91. Definition of a new profile for PKI authentication

```
List of Validity Periods:
        0: New Validity Period
        1: allTheTime
        2: allTheTimeMonThruFri
        3: 9to5MonThruFri
        4: 5to9MonThruFri

Enter number of the validity period for this policy [1]?
```

Figure 92. Setting the validity period of the profile

The next step is to enter the profile's validity period.

The router then asks for an IPSec action. We will define a new IPSec action.

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action
        1: tun-101-102

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? tun-101-102-ds
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [192.168.211.1]?
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 192.168.211.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]: y
```

Figure 93. Defining a new IPSec action for PKI authentication

As part of the definition of the IPSec action, the router prompts us for an IPSec proposal.

```
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
List of IPSEC Proposals:
        0: New Proposal
        1: strongP2EspProp
        2: strongP2EspAhProp
        3: veryStrongP2EspProp
        4: veryStrongP2EspAhProp

Enter the Number of the IPSEC Proposal [1]? 1
Are there any more Proposal definitions for this IPSEC Action? [No]:


Here is the IPSec Action you specified...


IPSECAction Name = tun-101-102-ds
        Tunnel Start:End         =  192.168.211.1 : 192.168.211.2
        Tunnel In Tunnel         =            No
        Min Percent of SA Life   =            75
        Refresh Threshold        =            85 %
        Autostart                =           Yes
        DF Bit                   =          COPY
        Replay Prevention        =      Disabled
        IPSEC Proposals:
                strongP2EspProp
Is this correct? [Yes]: y
```

Figure 94. Defining a new IPSec proposal for PKI authentication

Now that the IPSec action has been fully defined, the router then prompts us again for the IPSec action that we wish to use. We will respond with the one that was just defined.

The router then prompts us to define for an ISAKMP action. In this example we will define a new action. It is here where we actually define the fact that we want to use certificate-based authentication under the ISAKMP proposal strongP1PropRSACert.

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: generalPhase1Action
        2: ike-1

Enter the Number of the ISAKMP Action [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Action []? ds-act1

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]:
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal
        1: strongP1PropSharedKey
        2: strongP1PropRSACert
        3: veryStrongP1PropSharedKey
        4: veryStrongP1PropRSACert

Enter the Number of the ISAKMP Proposal [1]? 2
Are there any more Proposal definitions for this ISAKMP Action? [No]:


Here is the ISAKMP Action you specified...


ISAKMP Name     = ds-act1
        Mode                     =            Main
        Min Percent of SA Life   =              75
        Conn LifeSize:LifeTime   =            5000 : 30000
        Autostart                =             Yes
        ISAKMP Proposals:
                strongP1PropRSACert
Is this correct? [Yes]:
ISAKMP Actions:
        0: New ISAKMP Action
        1: generalPhase1Action
        2: ike-1
        3: ds-act1

Enter the Number of the ISAKMP Action [1]? 3
```

Figure 95. Defining a new ISAKMP action and proposal for PKI authentication

The last set of parameters enable the policy and confirm the definitions of the policy.

```
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?


Here is the Policy you specified...


Policy Name     = ike-ds-211-211
        State:Priority =Enabled    : 5
        Profile        =211.0-to-211.0-ds
        Valid Period   =allTheTime
        IPSEC Action   =tun-101-102-ds
        ISAKMP Action  =ds-act1
Is this correct? [Yes]: y
```

Figure 96. Enabling and confirming the new policy for PKI authentication

A similar process must be performed on Router B except the IP addresses are swapped around.

6.2.3.2 Configure the certificates

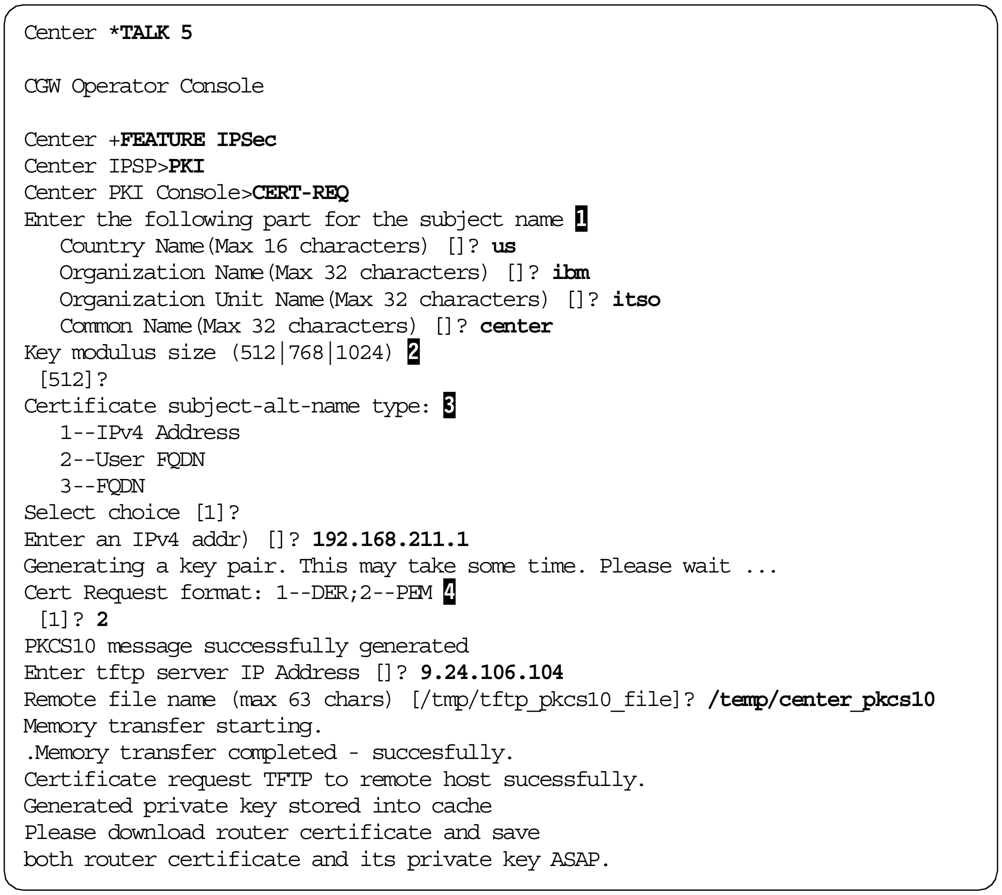
Now that the policy has been defined all that is required is to load the certificates into the router. The current level of the router software supports a PKI where there is only one CA. This means that the router can only authenticate other devices whose certificates were issued by the same CA.

Certificates and certificate requests are transferred to and from the router using TFTP. Therefore, a TFTP server must be initially configured to support this. Additionally, it is important that the router’s clock is correctly set to UMT, since certificates and certificate requests have a time stamp which can cause problems if not set correctly. Once these two operations have been done the router must be restarted/reloaded.

```
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>PKI
Center PKI config>ADD SERVER
Name ? (max 65 chars) []? tftp server
Enter server IP Address []? 9.24.106.104
Transport type (Choices: TFTP/LDAP)  [TFTP]?
Center PKI config>EXIT
Center IPsec config>EXIT
Center Config>
Center *TALK 6

Center Config>TIME SET
year (YYYY) [1999]?
month (MM) [7]?
date (DD) [8]?
hour (hh) [24 hour format] [16]? 20
minute (mm) [55]?
second (ss) [54]?
Date and time updated successfully
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
The configuration has been changed, save it? (Yes or [No] or Abort): y
Config Save: Using bank B and config number 4
The configuration has been saved.
```

Figure 97. Setting the TFTP server to transfer certificates and the router's clock to UMT

Once the router has been restarted/reloaded the next step is to get the router to generate a public and private key pair and to generate a certificate request with its identity and the public key. All management and configuration of certificates are done through `TALK 5 > IPSEC > PKI`.



```
Center *TALK 5

CGW Operator Console

Center +FEATURE IPSec
Center IPSP>PKI
Center PKI Console>CERT-REQ
Enter the following part for the subject name 1
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? ibm
   Organization Unit Name(Max 32 characters) []? itso
   Common Name(Max 32 characters) []? center
Key modulus size (512|768|1024) 2
 [512]?
Certificate subject-alt-name type: 3
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 192.168.211.1
Generating a key pair. This may take some time. Please wait ...
Cert Request format: 1--DER;2--PEM 4
 [1]? 2
PKCS10 message successfully generated
Enter tftp server IP Address []? 9.24.106.104
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]? /temp/center_pkcs10
Memory transfer starting.
.Memory transfer completed - succesfully.
Certificate request TFTP to remote host sucessfully.
Generated private key stored into cache
Please download router certificate and save
both router certificate and its private key ASAP.
```

Figure 98. Generating a certificate request

1 Subject name is the X.500 name in the certificate.

2 Key modulus size is the modulus key size that will be used in generating the public and private key pairs.

3 Subject-Alt-Name is the name used in the certificate to identify the party.

4 Certificate request format is either in Distinguished Encoding Rules (DER) or Privacy Enhanced Mail (PEM). DER is a binary format while PEM is a text-based format. You must choose the format that your CA uses.

What you have just done is made the router generate a public and private key pair and formed a certificate request with that public key in the file which was uploaded to the TFTP server. The private key never leaves the router. If the router is restarted before the certificate has been downloaded to the router and saved a new certificate request must be performed.

Once you have the certificate request you then must ask the CA for a certificate. This is dependent on how your CA has implemented the issuing of certificates. In this example we will use the Entrust Web site (`http://www.entrust.com`) which issues temporary demonstration certificates at no cost. The Web site simply asks you to copy and paste the certificate request after which it generates a certificate that you can copy and paste. This is why PEM was used in this example so that it could be manipulated with a text editor.

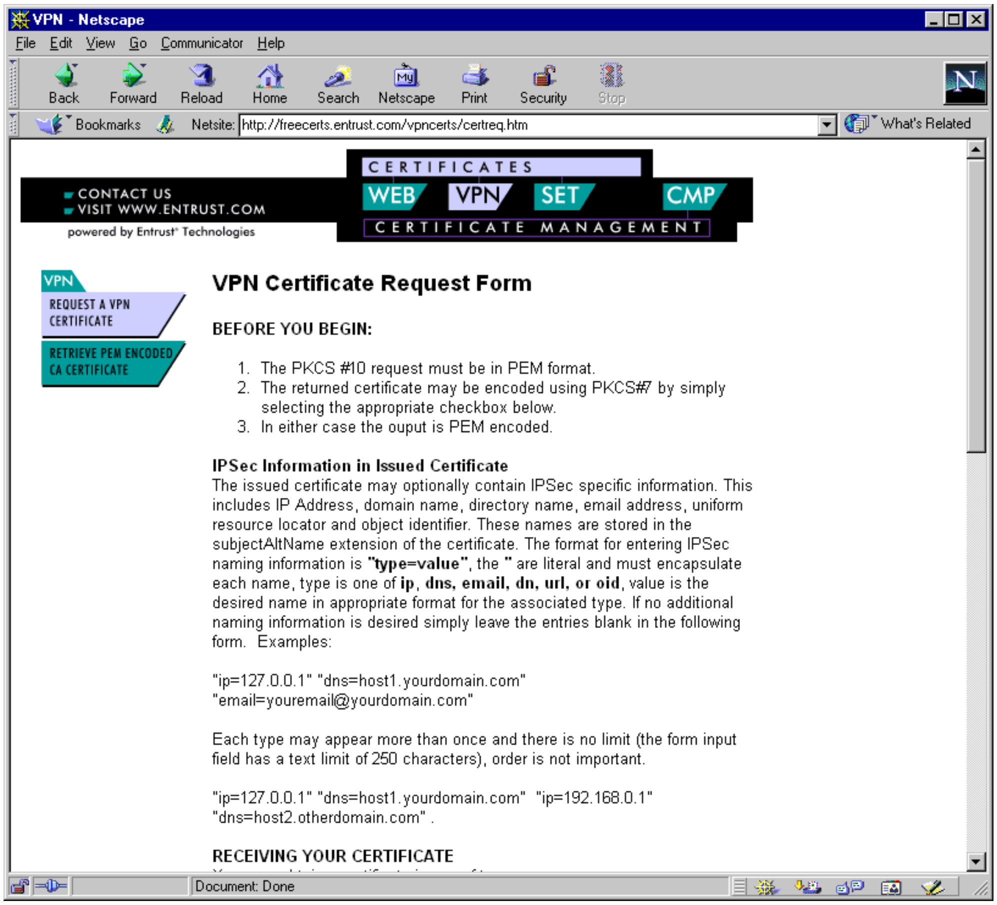
The first step is to copy the certificate request onto the clipboard. You could use Notepad or Wordpad to do this, but these editors seem to have trouble with the CR/LF characters at the end of each line in the certificate request. The best way is to simply perform a DOS `TYPE` command to display the certificate request and then to mark and copy straight out of the DOS window.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB0zCCATwCAQAwSzELMAkGA1UEBhMCVVMxDTALBgNVBAgTBE4uQy4xDDAKBgNV
BAoTA0lCTTENMAsGA1UECxMESVRTTzEQMA4GA1UEAxMHcGM3NTAtcjCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAg5jIPsbpJ1Cn2Uxl9si60CFQqpUYGKIEBZg/
HRoqhEwOi/51jYV0SLiXD86WYliQx6rVtLBYLhwZUlbIhjJcYnyZ6sMMndX3OigB
hKogJkGQF+7v6OxmxCXYR4ng+Pod04m1K0siGgX7s8AYsC9qR2sjGAzlvjXkD0qa
/VwqLSkCAwEAAaBIMEYGCSqGSIb3DQEJDjE5MDcwNQYDVR0RBC4wLIcErBADB4ES
cGM3NTAtckB1cy5pYm0uY29tghBpdHNvLnJhbC5pYm0uY29tMA0GCSqGSIb3DQEB
BAUAA4GBADDk31RQma1sIJmdi63bhTZ57W1eaXCf4/d5YuyZzp5gjswTozP0zohy
F+ZVChamLWlE7Iv0+3eL/iPpVUJb8ysGAM89AZUqhwdR58ITblSetFeT4lWljNcU
p1UhD7M9peEw9mWZPaqWDE9NCPcoAZn4GlNSK6gUgiuEv+5ACUk6
-----END NEW CERTIFICATE REQUEST-----
```

Figure 99. Using the DOS TYPE command to display the certificate request

Make sure when you mark the window you include the header and footer which mark the start and end of the certificate.

Once the certificate request has been copied onto the clipboard, go to the Entrust Web site at `http://www.entrust.com` to request a free demonstration certificate. The free certificates are accessible from the downloads section where you will be able to request a VPN certificate. Some personal details must be entered before you can request the certificate.



VPN - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: http://freecerts.entrust.com/vpncerts/certreq.htm
What's Related
CONTACT US
VISIT WWW.ENTRUST.COM
powered by Entrust Technologies
CERTIFICATES
WEB VPN SET CMP
CERTIFICATE MANAGEMENT
VPN
REQUEST A VPN CERTIFICATE
RETRIEVE PEM ENCODED CA CERTIFICATE
Document: Done

VPN Certificate Request Form

BEFORE YOU BEGIN:

1. The PKCS #10 request must be in PEM format.
2. The returned certificate may be encoded using PKCS#7 by simply selecting the appropriate checkbox below.
3. In either case the ouput is PEM encoded.

IPSec Information in Issued Certificate
The issued certificate may optionally contain IPSec specific information. This includes IP Address, domain name, directory name, email address, uniform resource locator and object identifier. These names are stored in the subjectAltName extension of the certificate. The format for entering IPSec naming information is **"type=value"**, the **"** are literal and must encapsulate each name, type is one of **ip**, **dns, email, dn, url, or oid**, value is the desired name in appropriate format for the associated type. If no additional naming information is desired simply leave the entries blank in the following form. Examples:

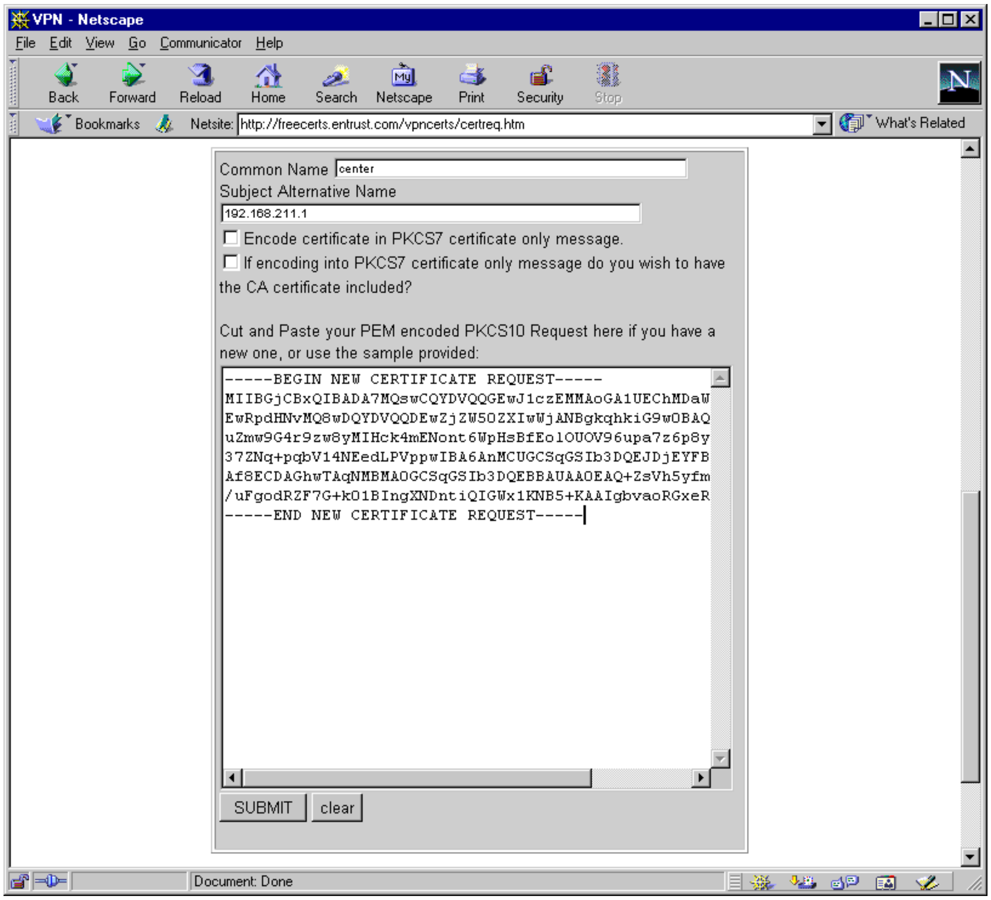
"ip=127.0.0.1" "dns=host1.yourdomain.com"
"email=youremail@yourdomain.com"

Each type may appear more than once and there is no limit (the form input field has a text limit of 250 characters), order is not important.

"ip=127.0.0.1" "dns=host1.yourdomain.com" "ip=192.168.0.1"
"dns=host2.otherdomain.com" .

RECEIVING YOUR CERTIFICATE

Figure 100. Entrust certificate request Web page - top half


VPN - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: http://freecerts.entrust.com/vpncerts/certreq.htm
What's Related
Document: Done

Common Name center

Subject Alternative Name

192.168.211.1

□ Encode certificate in PKCS7 certificate only message.

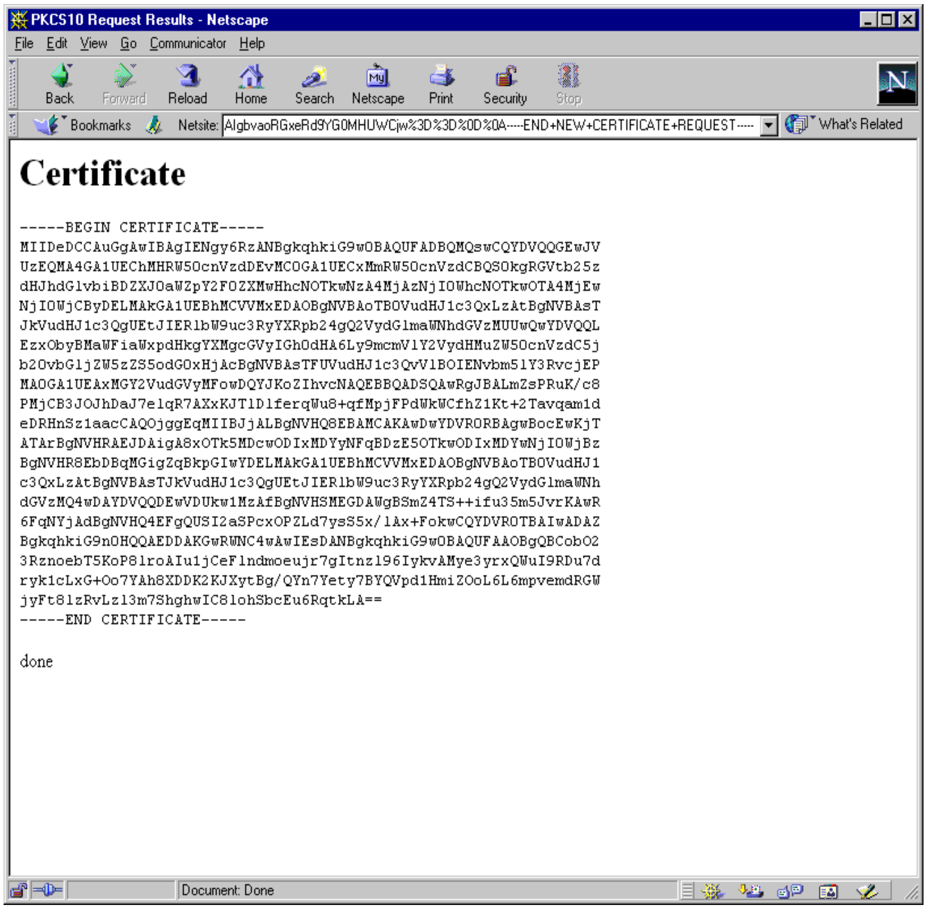
□ If encoding into PKCS7 certificate only message do you wish to have the CA certificate included?

Cut and Paste your PEM encoded PKCS10 Request here if you have a new one, or use the sample provided:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBGjCBxQIBADA7MQswCQYDVQQGEwJ1czEMMAoGA1UEChMDaW
EwRpdHNvMQ8wDQYDVQQDEwZjZW50ZXIwWjANBgkqhkiG9w0BAQ
uZmw9G4r9zw8yMIHck4mENont6WpHsBfEo1OUOV96upa7z6p8y
37ZNq+pqbV14NEedLPVppwIBA6AnMCUGCSqGSIb3DQEJDjEYFB
Af8ECDAGhwTAqNMBMA0GCSqGSIb3DQEBBAUAA0EAQ+ZsVh5yfm
/uFgodRZF7G+k01BIngXNDntiQIGWx1KNB5+KAAIgbvaoRGxeR
-----END NEW CERTIFICATE REQUEST-----
```

Figure 101. Entrust certificate request Web page - bottom half

Once you have reached the page to request a certificate, simply paste the certificate request into the appropriate area, fill in the fields for Common Name and Subject Alternative Name, uncheck the option, Encode certificate in PKCS7 certificate only message, and then click **SUBMIT**. Then after a period of time a certificate will be generated.


PKCS10 Request Results - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: AlgbvaoRGxeRd9YG0MHUWCjw%3D%3D%0D%0A-----END+NEW+CERTIFICATE+REQUEST-----
What's Related
Document: Done

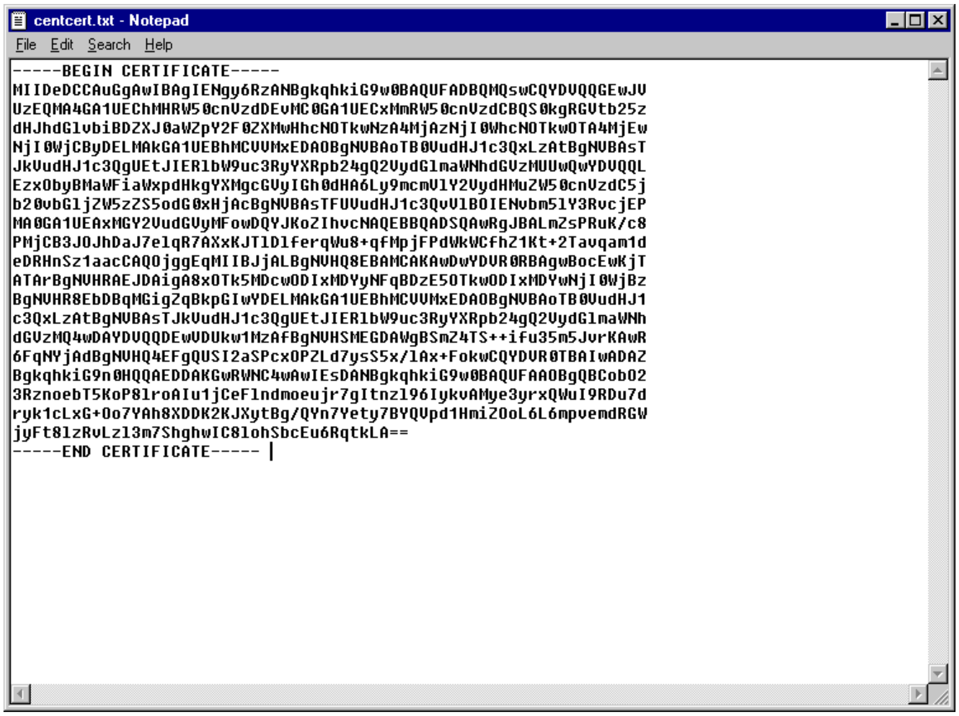
Certificate

```
-----BEGIN CERTIFICATE-----
MIIDeDCCAuGgAwIBAgIENgy6RzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25z
dHJhdGlvbiBDZXJ0aWZpY2F0ZXMwHhcNOTkwNzA4MjAzNjI0WhcNOTkwOTA4MjEw
NjI0WjCByDELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VudHJ1c3QxLzAtBgNVBAsT
JkVudHJ1c3QgUEtJIERlbW9uc3RyYXRpb24gQ2VydGlmaWNhdGVzMUUwQwYDVQQL
EzxObyBMaWFiaWxpdHkgYXMgcGVyIGh0dHA6Ly9mcmVlY2VydHMuZW50cnVzdC5j
b20vbGljZW5zZS5odG0xHjAcBgNVBAsTFUVudHJ1c3QvV1BOIENvbm5lY3RvcjEP
MA0GA1UEAxMGY2VudGVyMFowDQYJKoZIhvcNAQEBBQADSQAwRgJBALmZsPRuK/c8
PMjCB3JOJhDaJ7elqR7AXxKJTlDlferqWu8+qfMpjFPdWkWCfhZ1Kt+2Tavqam1d
eDRHnSz1aacCAQOjggEqMIIBJjALBgNVHQ8EBAMCAKAwDwYDVR0RBAgwBocEwKjT
ATArBgNVHRAEJDAigA8xOTk5MDcwODIxMDYyNFqBDzE5OTkwODIxMDYwNjI0WjBz
BgNVHR8EbDBqMGigZqBkpGIwYDELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VudHJ1
c3QxLzAtBgNVBAsTJkVudHJ1c3QgUEtJIERlbW9uc3RyYXRpb24gQ2VydGlmaWNh
dGVzMQ4wDAYDVQQDEwVDUkw1MzAfBgNVHSMEGDAWgBSmZ4TS++ifu35m5JvrKAwR
6FqNYjAdBgNVHQ4EFgQUSI2aSPcxOPZLd7ysS5x/lAx+FokwCQYDVR0TBAIwADAZ
BgkqhkiG9n0HQQAEDDAKGwRWNC4wAwIEsDANBgkqhkiG9w0BAQUFAAOBgQBCobO2
3RznoebT5KoP8lroAIu1jCeFlndmoeujr7gItnzl96IykvAMye3yrxQWuI9RDu7d
ryk1cLxG+Oo7YAh8XDDK2KJXytBg/QYn7Yety7BYQVpd1HmiZOoL6L6mpvemdRGW
jyFt8lzRvLzl3m7ShghwIC8lohSbcEu6RqtkLA==
-----END CERTIFICATE-----
```

done

Figure 102. Router's certificate generated by the Entrust Web page

Once the certificate has been generated simply mark and copy the certificate including the header and footer which mark the beginning and end of the certificate. Using Notepad, paste it into an empty document and save the file to an area accessible by the TFTP server.



```
-----BEGIN CERTIFICATE-----
MIIDeDCCAuGgAwIBAgIENgy6RzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25z
dHJhdGlvbiBDZXJ0aWZpY2F0ZXMwHhcNOTkwNzA4MjAzNjI0WhcNOTkwOTA4MjEw
NjI0WjCByDELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VudHJ1c3QxLzAtBgNVBAsT
JkVudHJ1c3QgUEtJIERlbW9uc3RyYXRpb24gQ2VydGlmaWNhdGVzMUUwQwYDVQQL
EzxObyBMaWFiaWxpdHkgYXMgcGVyIGh0dHA6Ly9mcmVlY2VydHMuZW50cnVzdC5j
b20vbGljZW5zZS5odG0xHjAcBgNVBAsTFUVudHJ1c3QvVlBOIENvbm5lY3RvcjEP
MA0GA1UEAxMGY2VudGVyMFowDQYJKoZIhvcNAQEBBQADSQAwRgJBALmZsPRuK/c8
PMjCB3JOJhDaJ7elqR7AXxKJTlDlferqWu8+qfMpjFPdWkWCfhZ1Kt+2Tavqam1d
eDRHnSz1aacCAQOjggEqMIIBJjALBgNVHQ8EBAMCAKAwDwYDVR0RBAgwBocEwKjT
ATArBgNVHRAEJDAigA8xOTk5MDcwODIxMDYyNFqBDzE5OTkwODIxMDYwNjI0WjBz
BgNVHR8EbDBqMGigZqBkpGIwYDELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VudHJ1
c3QxLzAtBgNVBAsTJkVudHJ1c3QgUEtJIERlbW9uc3RyYXRpb24gQ2VydGlmaWNh
dGVzMQ4wDAYDVQQDEwVDUkw1MzAfBgNVHSMEGDAWgBSmZ4TS++ifu35m5JvrKAwR
6FqNYjAdBgNVHQ4EFgQUSI2aSPcxOPZLd7ysS5x/lAx+FokwCQYDVR0TBAIwADAZ
BgkqhkiG9n0HQQAEDDAKGwRWNC4wAwIEsDANBgkqhkiG9w0BAQUFAAOBgQBCobO2
3RznoebT5KoP8lroAIu1jCeFlndmoeujr7gItnzl96IykvAMye3yrxQWuI9RDu7d
ryk1cLxG+Oo7YAh8XDDK2KJXytBg/QYn7Yety7BYQVpd1HmiZOoL6L6mpvemdRGW
jyFt8lzRvLzl3m7ShghwIC8lohSbcEu6RqtkLA==
-----END CERTIFICATE-----
```

Figure 103. Router's certificate copied into Notepad

You should now have a certificate for the router stored as a text file on the TFTP server. The next step is to load the certificate onto the router.

```
Center PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]? 2
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? tftp server
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /temp/centce
rt.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Router Certificate  loaded into run-time cache
```

Figure 104. Loading the certificate onto the router

A problem that may occur at this time is that the certificate fails to load.

```
Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Error occurred in storing certificate in cache!
```

Figure 105. Failing to load the router's certificate

The corresponding messages in the event log are:

```
00:06:29  DOLOG: DEBUG: BSAFE req allocated

00:06:29  DOLOG: DEBUG: came out of wait with opc = 0

00:06:29  DOLOG: CERT: get_DN_DER()  è¯•@: , ,Ÿlè¯Àè°ñ

00:07:32  DOLOG: der =286 pem =382
```

Figure 106. Event log when the router failed to load its certificate

If you encounter this problem then the most likely reason for the failure is the clock in the router. It is imperative that the clock is set correctly before the certificate request is generated.

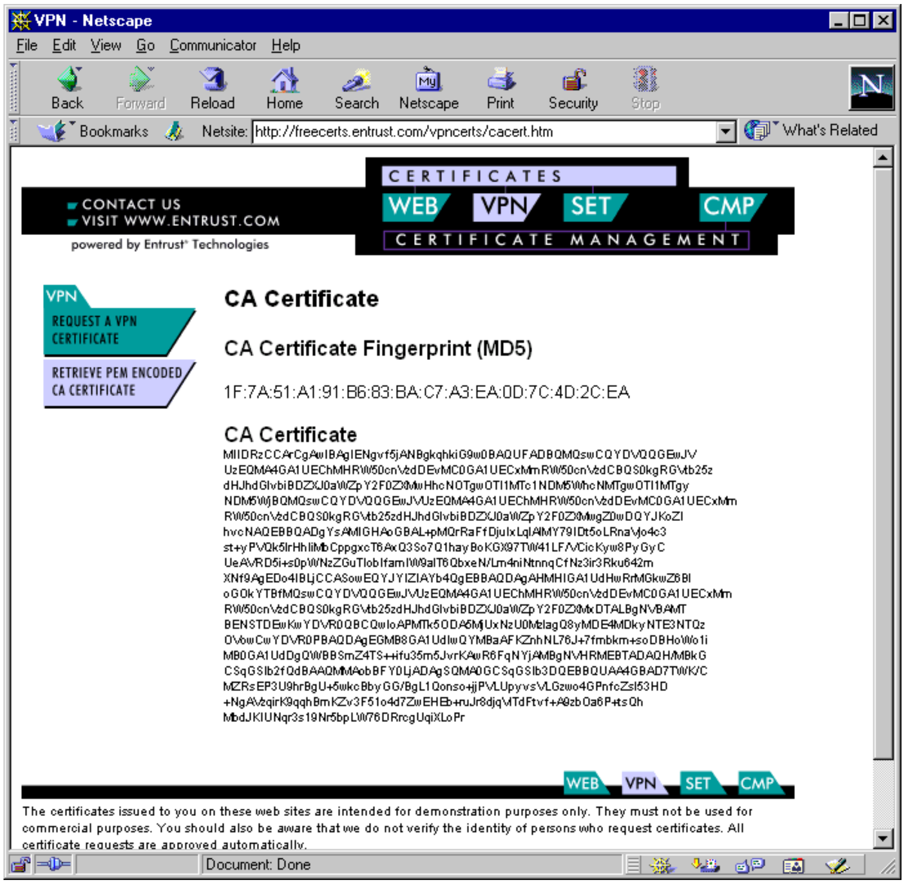
Once the router has successfully loaded its certificate you must then save the certificate to ensure the certificate and its corresponding private key are stored in nonvolatile memory.

```
Center PKI Console>CERT-SAVE
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]? 2
SRAM Name for certificate and private key []? entrust-center-19990708
Load as default router certificate at initialization? [No]: y
Both Router Certificate and private key saved into SRAM successfully
```

Figure 107. Saving the router’s certificate and private key into nonvolatile memory

The router can now be restarted without losing its private key and corresponding certificate.

The next step is to load the certificate of the CA. This is done in exactly the same way as loading the router’s certificate. The certificate of the CA can be found at the CA, and is basically a self-signed certificate. At the Entrust Web site there is a link in the VPN Certificates page. Instead of hitting the button which requests a certificate, there is a link that allows you to retrieve a PEM-encoded CA certificate. Again you will be prompted to enter personal information before you get to the page with the actual certificate.


VPN - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: http://freecerts.entrust.com/vpncerts/cacert.htm What's Related
CERTIFICATES
WEB VPN SET CMP
CERTIFICATE MANAGEMENT
CONTACT US
VISIT WWW.ENTRUST.COM
powered by Entrust® Technologies
VPN
REQUEST A VPN CERTIFICATE
RETRIEVE PEM ENCODED CA CERTIFICATE
WEB VPN SET CMP
Document: Done

CA Certificate

CA Certificate Fingerprint (MD5)

1F:7A:51:A1:91:B6:83:BA:C7:A3:EA:0D:7C:4D:2C:EA

CA Certificate

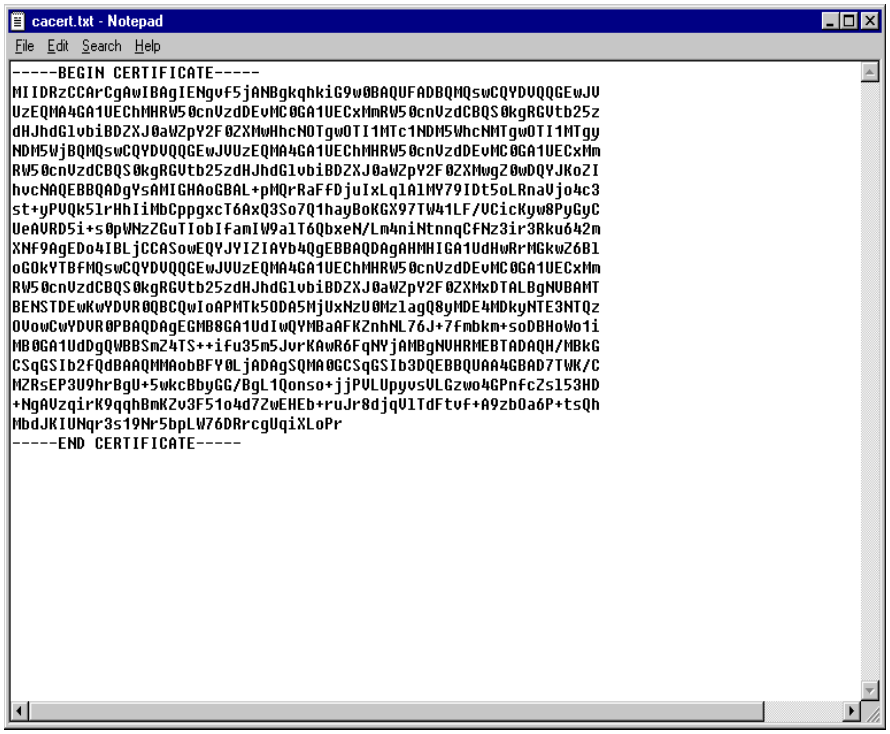
```
MIIDRzCCArCgAwIBAgIENgvf5jANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25z
dHJhdGlvbiBDZXJ0aWZpY2F0ZXMwHhcNOTgwOTI1MTc1NDM5WhcNMTgwOTI1MTgy
NDM5WjBQMQswCQYDVQQGEwJVUzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMm
RW50cnVzdCBQS0kgRGVtb25zdHJhdGlvbiBDZXJ0aWZpY2F0ZXMwgZ0wDQYJKoZI
hvcNAQEBBQADgYsAMIGHAoGBAL+pMQrRaFfDjuIxLqlAIMY79IDt5oLRnaVjo4c3
st+yPVQk5IrHhIiMbCppgxcT6AxQ3So7Q1hayBoKGX97TW41LF/VCicKyw8PyGyC
UeAVRD5i+s0pWNzZGuTIobIfamIW9aIT6QbxeN/Lm4niNtnnqCfNz3ir3Rku642m
XNf9AgEDo4IBLjCCASowEQYJYIZIAYb4QgEBBAQDAgAHMHIGA1UdHwRrMGkwZ6Bl
oGOkYTBfMQswCQYDVQQGEwJVUzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMm
RW50cnVzdCBQS0kgRGVtb25zdHJhdGlvbiBDZXJ0aWZpY2F0ZXMxDTALBgNVBAMT
BENSTDEwKwYDVR0QBCQwIoAPMTk5ODA5MjUxNzU0MzlagQ8yMDE4MDkyNTE3NTQz
OVowCwYDVR0PBAQDAgEGMB8GA1UdIwQYMBaAFKZnhNL76J+7fmbkm+soDBHoWo1i
MB0GA1UdDgQWBBSmZ4TS++ifu35m5JvrKAwR6FqNYjAMBgNVHRMEBTADAQH/MBkG
CSqGSIb2fQdBAAQMMAobBFY0LjADAgSQMA0GCSqGSIb3DQEBBQUAA4GBAD7TWK/C
MZRsEP3U9hrBgU+5wkcBbyGG/BgL1Qonso+jjPVLUpyvsVLGzwo4GPnfcZsI53HD
+NgAVzqirK9qqhBmKZv3F51o4d7ZwEHEb+ruJr8djqVITdFtvf+A9zbOa6P+tsQh
MbdJKIUNqr3s19Nr5bpLW76DRrcgUqiXLoPr
```

The certificates issued to you on these web sites are intended for demonstration purposes only. They must not be used for commercial purposes. You should also be aware that we do not verify the identity of persons who request certificates. All certificate requests are approved automatically.

Figure 108. The CA's certificate from the Entrust Web page

We only need the information directly under CA Certificate, so simply mark and copy that area onto the clipboard. Using the Notepad paste the contents of the clipboard into an empty document. Then add the header and footer to indicate the beginning and end of the certificate. These are exactly the same as those found in the Router certificate.

]



```
-----BEGIN CERTIFICATE-----
MIIDRzCCArCgAwIBAgIENgvf5jANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25z
dHJhdGlvbiBDZXJ0aWZpY2F0ZXMwHhcNOTgwOTI1MTc1NDM5WhcNMTgwOTI1MTgy
NDM5WjBQMQswCQYDVQQGEwJVUzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMm
RW50cnVzdCBQS0kgRGVtb25zdHJhdGlvbiBDZXJ0aWZpY2F0ZXMwgZ0wDQYJKoZI
hvcNAQEBBQADgYsAMIGHAoGBAL+pMQrRaFfDjuIxLqlAlMY79IDt5oLRnaVjo4c3
st+yPVQk5lrHhIiMbCppgxcT6AxQ3So7Q1hayBoKGX97TW41LF/VCicKyw8PyGyC
UeAVRD5i+s0pWNzZGuTIobIfamIW9alT6QbxeN/Lm4niNtnnqCfNz3ir3Rku642m
XNf9AgEDo4IBLjCCASowEQYJYIZIAYb4QgEBBAQDAgAHMHIGA1UdHwRrMGkwZ6Bl
oGOkYTBfMQswCQYDVQQGEwJVUzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMm
RW50cnVzdCBQS0kgRGVtb25zdHJhdGlvbiBDZXJ0aWZpY2F0ZXMxDTALBgNVBAMT
BENSTDEwKwYDVR0QBCQwIoAPMTk5ODA5MjUxNzU0MzlagQ8yMDE4MDkyNTE3NTQz
OVowCwYDVR0PBAQDAgEGMB8GA1UdIwQYMBaAFKZnhNL76J+7fmbkm+soDBHoWo1i
MB0GA1UdDgQWBBSmZ4TS++ifu35m5JvrKAwR6FqNYjAMBgNVHRMEBTADAQH/MBkG
CSqGSIb2fQdBAAQMMAobBFY0LjADAgSQMA0GCSqGSIb3DQEBBQUAA4GBAD7TWK/C
MZRsEP3U9hrBgU+5wkcBbyGG/BgL1Qonso+jjPVLUpyvsVLGzwo4GPnfcZsl53HD
+NgAVzqirK9qqhBmKZv3F51o4d7ZwEHEb+ruJr8djqVlTdFtvf+A9zbOa6P+tsQh
MbdJKIUNqr3s19Nr5bpLW76DRrcgUqiXLoPr
-----END CERTIFICATE-----
```

Figure 109. CA's certificate copied into Notepad with a header and footer

Once the header and footer are in place save the file to an area accessible to the TFTP server.

The next step is to load the CA certificate onto the router and save it into nonvolatile memory. The process is almost exactly the same as described for the router's certificate.

```
Center PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]? 1
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? tftp server
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /temp/cacert
.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Root CA Certificate  loaded into run-time cache
Center PKI Console>CERT-SAVE
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]? 1
SRAM Name to store Root Certificate? []? entrust-ca-19990708
Load as default root certificate at initialization? [No]: y
Root Certificate saved into SRAM successfully.
```

Figure 110. Loading and saving the CA's certificate

You can view the certificates that have been loaded onto the router.

```
Center PKI Console>LIST CERTIFICATE
Router   certificate
      Serial Number:   906803783
      Subject  Name:   /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
/ou=No Li/c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
      Issuer   Name:   /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
   Subject alt Name:   192.168.211.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/7/8 20:36:24 -- 1999/9/8 21:06:24

Root CA  certificate
      Serial Number:   906747878
      Subject  Name:   /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
      Issuer   Name:   /c=US/o=Entrust/ou=Entrust PKI Demonstration Certificates
           Validity:   1998/9/25 17:54:39 -- 2018/9/25 18:24:39
```

Figure 111. Viewing certificates that have been loaded onto the router

6.2.3.3 Event log

By displaying all IKE and PKI subsystem messages you are able to see the process that the router goes through to set up a tunnel using certificate-based authentication.

```
00:00:00   GW.002: Portable CGW Center Rel 2216-MAS Feature 2895 V3.3 Mod 0 PTF
0 RPQ 0 MAS.FF6 cc50_9d
 strtd
00:00:00   GW.005: Bffrs: 400 avail 400 idle   fair 51 low 80
00:00:00  PKI.041: X500DN initialized. Total X500 Attribute name 11

00:00:00  PKI.070: Store my private key into cache success. key buffer length=34
4
00:00:00  PKI.065: PKI Cert key usuage (Signature) check success
00:00:00  PKI.009: Validity check: success. Current date: 1999/7/9, Time: 1:23:1
1. Cert valid date: 1999/7/8 20:6:24 -- 1999/9/8 20:6:24.

00:00:00  PKI.066: Store local cert life from router start 5341393

00:00:00  PKI.056: PKI cert validity check status successful

00:00:00  PKI.053: PKI alt-name IPv4 Addr Value 192.168.211.1

00:00:00  PKI.061: PKI cert alt-name processing status: successful

00:00:00  PKI.059: PKI store Router cert ID  status successful

00:00:00  PKI.060: PKI processing Router cert successful

00:00:00  PKI.069: Store my cert into cache success. cert length=892
00:00:00  PKI.034: Load Router Cert Success. cert ID=ENTRUST-CENTER-19990708

00:00:00  PKI.071: Store root cert into cache success. cert length=843
00:00:00  PKI.034: Load Root CA Cert Success. cert ID=ENTRUST-CA-19990708

00:00:00  PKI.048: PKI initialized.
```

Figure 112. PKI initialization in the event log

You can see what the router tries to do immediately after bootup. Initially it loads its private key into cache and checks the validity of its own certificate. If everything is OK it then loads its certificate into cache. The last step in the PKI initialization is to load the CA's certificate. This is shown in Figure 112 on page 135.

After the PKI initialization the router then tries to set up the tunnel. The router tries to initiate the tunnel by starting an IKE Phase 1 main mode negotiation. (See Figure 113 on page 137.)

The router receives a Phase 1 main mode initiator message from the other router so it quickly terminates the Phase 1 negotiations it started and starts the Phase 1 negotiation as the responder. The first two messages of Phase 1 negotiate the ISAKMP SA policies. This router examines the proposals that the other router sent and chooses one. In our configuration there was only one proposal. This router finds the proposal acceptable and responds to the other router by sending a message with that proposal.

The next two messages exchange information to determine the shared secret keys that will be used in subsequent messages. Here you see the router receive the components to be able to perform a Diffie-Hellman operation to generate the keys. This router also responds to the other router in the same way. Notice that each party requested the certificate of the other party. This request will be satisfied in the next two message flows.

Now all subsequent messages will be encrypted with the keys that were just generated. The next two messages authenticate the routers. Each router will send a signed message containing its ID and certificate. Each router will then perform the following checks on the messages they have just received:

- Certificate can be used for signing
- Validity date of the certificate is still current
- Certificate was issued by the correct CA
- Validates the identity in the certificate with the identity in the message
- Checks the signature

Phase 1 negotiations have now been completed.

```
00:00:00  IKE.018: IKE Public Key module init success. Exit point: Normal 0
00:00:00  IKE.009: Begin Main mode - Initiator
00:00:00  IKE.013: To Peer: 192.168.211.2 MM HDR SA
00:00:00  IKE.001: Trace IKE packet to 192.168.211.2
00:00:00  DOLOG: .....Remote Logging Facility is now available.....

00:00:05  IKE.011: No response from Ike peer: Retransmit packet
00:00:05  IKE.001: Trace IKE packet to 192.168.211.2
00:00:10  IKE.011: No response from Ike peer: Retransmit packet
00:00:10  IKE.001: Trace IKE packet to 192.168.211.2
00:00:12  IKE.001: Trace IKE packet from 192.168.211.2
00:00:12  IKE.013: From Peer: 192.168.211.2 MM HDR SA
00:00:12  IKE.014: Phase 1 SA DELETED for Peer:  192.168.211.2
00:00:12  IKE.014: Phase 2 SA DELETED for Peer:  192.168.211.2
00:00:12  IKE.009: Begin Main mode - Responder
00:00:13  IKE.014: Oakley proposal is acceptable. Peer:  192.168.211.2
00:00:13  IKE.013: To Peer: 192.168.211.2 MM HDR SA
00:00:13  IKE.001: Trace IKE packet to 192.168.211.2
00:00:13  IKE.001: Trace IKE packet from 192.168.211.2
00:00:13  IKE.013: From Peer: 192.168.211.2 MM HDR KE NONCE CERT_REQ
00:00:13  IKE.003: Processing ISA_KE
00:00:14  IKE.003: Processing NONCE
00:00:14  IKE.013: To Peer: 192.168.211.2 MM HDR KE NONCE CERT_REQ
00:00:14  IKE.001: Trace IKE packet to 192.168.211.2
00:00:14  IKE.001: Trace IKE packet from 192.168.211.2
00:00:14  IKE.002: Trace IKE payload after decryption from Peer: 192.168.211.2
00:00:14  IKE.013: From Peer: 192.168.211.2 MM HDR* ID CERT SIG
00:00:14  PKI.065: PKI Cert key usuage (Signature) check success
00:00:14  PKI.009: Validity check: success. Current date: 1999/7/9, Time: 1:23:2
5. Cert valid date: 1999/7/8 20:59:3 -- 1999/9/8 20:59:3.

00:00:14  PKI.066: Store local cert life from router start 5340952
00:00:14  PKI.056: PKI cert validity check status successful
00:00:14  PKI.010: Root CA in cache? Yes length=843.
00:00:14  PKI.057: PKI cert root CA check status successful
00:00:14  PKI.058: PKI store peer public key status success
00:00:14  PKI.058: PKI store peer public key status successful

00:00:14  PKI.053: PKI alt-name IPv4 Addr Value 192.168.211.2

00:00:14  PKI.061: PKI cert alt-name processing status: successful

00:00:14  PKI.059: PKI store Peer cert ID  status successful

00:00:14  PKI.060: PKI processing Peer cert successful

00:00:14  IKE.016: process_cert: ID match: cert ID:  192.168.211.2
00:00:14  IKE.016:                   ID payload ID:  192.168.211.2
00:00:14  IKE.003: Processing RSA signature
00:00:14  PKI.068: Retrieve peer cert public key successful
00:00:14  IKE.020: IKE signature public key verification success
00:00:14  IKE.021: IKE signature matched
00:00:14  IKE.014: ValidatePhase1ID: cpeP1Handles match. Peer:  192.168.211.2
00:00:14  PKI.072: Get my cert from cache success. cert length=32026724
00:00:14  IKE.019: IKE signature private key signing success
00:00:14  IKE.010: Finished Main mode -responder
00:00:14  IKE.013: To Peer: 192.168.211.2 MM HDR* ID CERT SIG
00:00:14  IKE.002: Trace IKE payload before encryption to Peer: 192.168.211.2
00:00:14  IKE.001: Trace IKE packet to 192.168.211.2
```

Figure 113. Phase 1 negotiation in the event log

Notice that a challenge to encrypt a random message does not need to occur. This is because the signature process effectively does the same thing, encrypting a hash of the message. The original message itself contains information from messages 1 through 4 and the generated master key, which effectively makes the message random.

The Phase 2 negotiations must now occur. (See Figure 114.) This router tries to initiate the Phase 2 negotiation but soon realizes that the other router has already started and therefore terminates the one it started and begins acting as responder for Phase 2.

There are only three messages in a Phase 2 negotiation. The first message was received by this router indicating that the remote router wishes to initiate a Phase 2 negotiation. This router examines the request and checks all the relevant fields. It then sends a similar message back to the other router. Notice that there is no key exchange attribute in these first two messages. This is because PFS was not requested, because the key exchange is only needed to perform a new Diffie-Hellman operation for PFS.

The third message from the other router is to ensure the liveliness of the operation.

The router then loads two SAs, one for each direction of traffic.

```
00:00:14  IKE.009: Begin Quick mode - Initiator
00:00:14  IKE.013: To Peer: 192.168.211.2 QM HDR* HASH SA NONCE ID ID
00:00:14  IKE.002: Trace IKE payload before encryption to Peer: 192.168.211.2
00:00:14  IKE.001: Trace IKE packet to 192.168.211.2
00:00:14  IKE.001: Trace IKE packet from 192.168.211.2
00:00:14  IKE.009: Begin Quick mode - Responder
00:00:14  IKE.002: Trace IKE payload after decryption from Peer: 192.168.211.2
00:00:14  IKE.013: From Peer: 192.168.211.2 QM HDR* HASH SA NONCE ID ID
00:00:14  IKE.003: Processing Quick Mode ID
00:00:14  IKE.003: Processing Quick Mode ID
00:00:14  IKE.015: Acceptable phase 2 proposal # 1
00:00:14  IKE.003: Processing NONCE
00:00:14  IKE.013: To Peer: 192.168.211.2 QM HDR* HASH SA NONCE ID ID
00:00:14  IKE.002: Trace IKE payload before encryption to Peer: 192.168.211.2
00:00:14  IKE.001: Trace IKE packet to 192.168.211.2
00:00:14  IKE.001: Trace IKE packet from 192.168.211.2
00:00:14  IKE.011: isakmp_input: drop incoming retransmitted message
00:00:14  IKE.001: Trace IKE packet from 192.168.211.2
00:00:14  IKE.002: Trace IKE payload after decryption from Peer: 192.168.211.2
00:00:14  IKE.013: From Peer: 192.168.211.2 QM HDR* HASH
00:00:14  IKE.008: Load Out SA: Alg=18 Prot=3 Sec=3600 KB=50000 SPI=705313650
00:00:14  IKE.008: Load In SA: Alg=18 Prot=3 Sec=3600 KB=50000 SPI=470776623
```

Figure 114. Phase 2 negotiation in the event log

6.2.3.4 Controlling user access

With certificate-based authentication you have the ability to easily scale up your VPN network. All that is required is to deploy your own CA which controls what certificates are issued and therefore, access to the network. There are cases where you will want to deny access even if the device was issued with a valid certificate.

1. The current level of software does not check for CRL. This means that if you wish to revoke access to a device or user the fact that the router does not

check the CRL means that access will still be permitted. The router simply checks that they have a valid certificate, that is, signed and issued by the authorized CA and has not expired.

2. Some organizations may not want to deploy their own PKI, and instead will outsource the issuing of certificates to another organization. In situations like these you only want to give access to those users and devices within your organization, rather than anybody who has had a certificate issued by the same CA.

What is required is the ability to deny access to users. Even if they passed the certificate authentication it is like saying that you definitely knew the identity of the other person but you still do not want to give access. The example above allows access to all users who were authenticated because we took the default answer of yes when we were asked the question, Any user within profile definition allowed access?, when defining the traffic profile (see Figure 91 on page 120).

If you wish to restrict access to a particular set of users you must first define users into a user group:

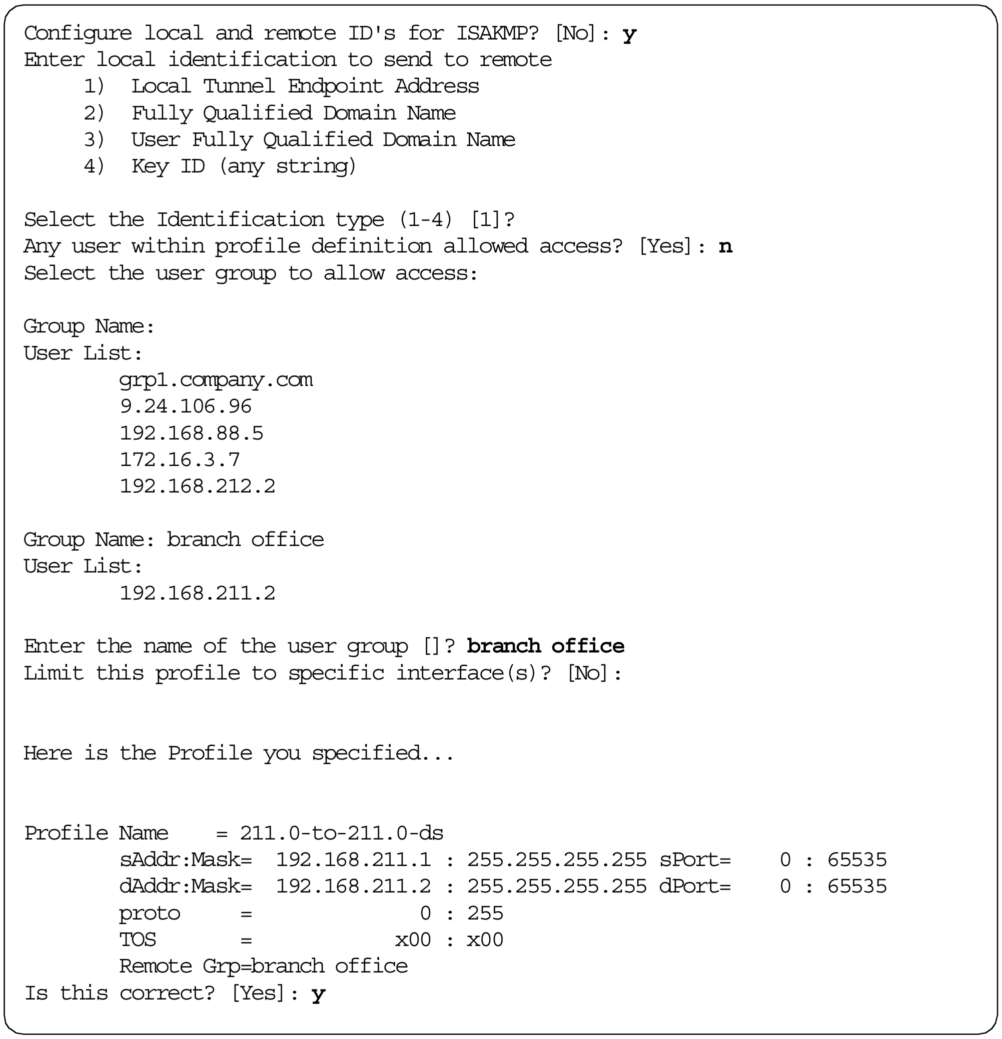
```
Center Policy config>ADD USER
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 192.168.211.2
Group to include this user in []? branch office
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]? 2


Here is the User Information you specified...

Name      = 192.168.211.2
        Type      = IPV4 Addr
        Group     =branch office
        Auth Mode =Certificate
Is this correct? [Yes]: y
```

Figure 115. Add a user into a user group

Once you have defined all your users into the user group you then simply change the traffic profile to restrict access. Keep all the existing values the same until you get to the question, "Any user within profile definition allowed access?"

Note

To answer the "Any user within profile definition allowed access?" question, you must say yes to the "Configure local and remote IDs for ISAKMP?"question.



```
Configure local and remote ID's for ISAKMP? [No]: y
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]: n
Select the user group to allow access:

Group Name:
User List:
        grp1.company.com
        9.24.106.96
        192.168.88.5
        172.16.3.7
        192.168.212.2

Group Name: branch office
User List:
        192.168.211.2

Enter the name of the user group []? branch office
Limit this profile to specific interface(s)? [No]:


Here is the Profile you specified...


Profile Name    = 211.0-to-211.0-ds
        sAddr:Mask=  192.168.211.1 : 255.255.255.255 sPort=    0 : 65535
        dAddr:Mask=  192.168.211.2 : 255.255.255.255 dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=branch office
Is this correct? [Yes]: y
```

Figure 116. Allowing access to a particular user group only

6.3 Monitoring VPNs using router commands

There are several useful commands to monitor IKE in `talk 5`.

6.3.1 The status of IKE Phase 1

From `feature IPSec` in `talk 5`, there are now submenus, one of which is IKE. From this menu you can determine the status of Phase 1 IKE negotiations. The command `list all` shows the IKE Phase 1 SA. It shows the IP address of the IKE peer, whether the peer is acting as the initiator or the responder, whether Phase 1 occurred in main or aggressive mode, if it occurred at system initialization (Y), the current state of the tunnel, and how authentication occurred - pre-shared or digital signatures (rsasig). Figure 117 is for two peers which are being authenticated using pre-shared keys.

```
Center *TALK 5
Center +FEATURE IPSec
Center IPSP>IKE
Center IKE>LIST ALL
Phase 1 ISAKMP Tunnels for IPv4:
------------------------------------------------------
Peer Address    I/R  Mode  Auto    State        Auth
---------------  ---  ----  ----  ----------  ------------
192.168.211.2   I   Main   Y    QM_IDLE      pre-shared
```

Figure 117. The status of IKE Phase 1

6.3.2 IKE negotiations

You can display IKE negotiations statistics using the `stats` command from `IKE`, `feature IPSec` in `talk 5`. If you are trying to debug a problem with IKE this `stats` command gives some insight into problems - for example, may be the proposals were invalid or rejected.

```
Center IKE>STATS
Peer address [192.168.211.2]?
Peer IP address......:     192.168.211.2
Active time (secs)...:             490
                                       In               Out
                                       ---              ---
Octets..............:             464              540
Packets.............:               4                5
Drop pkts...........:               0                0
Notifys.............:               0                0
Deletes.............:               0                0
Phase 2 Proposals....:              1                1
Invalid Proposals....:              0
Rejected Proposals...:              0                0
```

Figure 118. IKE negotiations

6.3.3 Tunnel display

The `list tunnel` command expands the output of `list all`. This command shows the negotiated encryption algorithms, hash algorithms, Diffie-Hellman group, the lifetime of the Phase 1 SA, the refresh threshold and the identity of the peer as shown in Figure 119:

```
Center IKE>LIST TUNNEL
Peer address [192.168.211.2]?
Peer IKE address: 192.168.211.2
Local IKE address: 192.168.211.1
Role: Initiator
Exchange: Main
Autostart: Yes
Oakley State: QM_IDLE
Authentication Method: Pre-shared Key
Encryption algorithm: des
Hash function: md5
Diffie-Hellman group: 1
Refresh threshold: 85
Lifetime (secs): 15000
Peer ID: 192.168.211.2
```

Figure 119. Tunnel display

6.3.4 IPSec traffic statistics

Confirm that IPSec processing is occurring using `Stats` from `ipv4`, `feature IPSec`, and `talk 5` as shown `in` Figure 120. If IKE has successfully completed Phase 2 negotiations and generated the keys for securing a user's data, the router is ready to process the user's data. The same options are available as in earlier releases to determine if IPSec processing is occurring. The `stats` command shows the number of packets being processed - both as packets sent and received, and displayed as a total, and per security protocol.

```
Center IPV4-IPsec>STATS

                            Global IPSec Statistics
Received:
total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
----------   ----------   -----------   -----------   ----------   ----------
3            0             3            528          264          264
Sent:
total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
----------   ----------   -----------   -----------   ----------   ----------
3            0             3            312            0          312
Receive Packet Errors:
total errs    AH errors   AH bad seq    ESP errors   ESP bad seq
----------   ----------   ----------    ----------   -----------
0            0            0             0             0
Send Packet Errors:
total errs    AH errors   ESP errors    Exceed MTU
----------   ----------   ----------    ----------
0            0            0             0
```

Figure 120. IPSec traffic statistics

6.3.5 Policy lists

In the policy feature, list the policies defined, and confirm the policies are enabled and valid. Figure 121 shows this command.

```
Center +FEATURE Policy
IP Network Policy console
Center Policy console>LIST POLICY BASIC
1: (Disabled,Valid)     ipsec_man_101_102
2: (Enabled,Valid)      ike-pre-101-102
Number of Policy to display (0 for All) [0]? 2
        Policy Name: ike-pre-101-102
        loaded from: Local
        State: Enabled and Valid
        Priority:    5
        Hits:        0
        Profile:     101.0-to-102.0-pre
        Validity:    allTheTime
        IPSEC:       tun-101-102
        ISAKMP:      ike-1
```

Figure 121. Policy lists

6.3.6 Applicable policy test

If you are trying to work out (a) if you configured your policy correctly or (b) which rule is applied to what traffic, the `test fowarder-query` command allows you to enter a traffic flow and the router will tell you which rule will be applied to that traffic as shown in Figure 122:

```
Center Policy console>TEST FORWARDER-QUERY
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.5
Enter IPV4 Destination Address [0.0.0.0]? 192.168.101.7
Enter the value for the Source Port [0]?
Enter the value for the Destination Port [0]?
Enter the value for the IP Protocol ID [0]?
Enter the value for the IP TOS Byte [0]?
Results of Test:
   Policy (IPSEC):  ike-pre-101-102.traffic
   IPSEC Action:  tun-101-102
```

Figure 122. Applicable policy test

6.3.7 Policy statistics

You can also see the detail statistics of the policies as shown in Figure 123 on page 144.

```
Center +FEATURE Policy
IP Network Policy console
Center Policy console>LIST STATS
+--------------------------------------------------+
|Name                                      |Hits   |
+--------------------------------------------------+
|ike-pre-101-102.p1out                     |      1|
|    ike-1                         (ISAKMP)|      2|
+--------------------------------------------------+
|ike-pre-101-102.p1in                      |      1|
|    ike-1                         (ISAKMP)|      2|
+--------------------------------------------------+
|ike-pre-101-102.traffic                   |      4|
|                          tun-101-102(IPSEC)|    7|
+--------------------------------------------------+
|ike-pre-101-102.inBoundTunnel             |      3|
|           ipsecPermitIfInboundTunnel(IPSEC)|    3|
+--------------------------------------------------+
```

Figure 123. Policy statistics

6.3.8 Using ELS subsystems

ELS has been updated with two new subsystems - *IKE* and *PKI* (for authentication using digital signatures). *IPSP*, the subsystem for IPSec, has also been updated. Useful information can also be obtained from the *IP* and *PLCY* subsystems.

Configure the ELS to monitor the IKE, PKI and PLCY subsystems. You may want to set these up in talk 6 and restart the router to capture the messages upon startup at `talk 2`:

```
Center *TALK 6
Gateway user configuration
Centerp Config>EVENT
Event Logging System user configuration
Center ELS config>DISPLAY SUBSYSTEM ipsp all all
Center ELS config>DISPLAY SUBSYSTEM ike all all
Center ELS config>DISPLAY SUBSYSTEM pki all all
Center ELS config>DISPLAY SUBSYSTEM plcy all all
```

Figure 124. Enabling IPSec-related ELS subsystems

Chapter 7. Directory-assisted policy management

Networks grow rapidly and the complexity of networks increases. The management of networks is a big issue from the viewpoint of scalability and security. To enable cost-effective administration of distributed network and enforce security policy in a virtual private network (VPN), directory-assisted policy management is a must.

One of the possible alternatives is Lightweight Directory Access Protocol (LDAP), which was developed to provide standards for accessing the data in network directories. As the use of LDAP grew and its benefits became apparent, the stand-alone LDAP server can build directories that could be accessed by the LDAP client. A common directory infrastructure encourages new uses. The Directory Enabled Networks (DEN) specification allows information about network configuration, protocol information, router characteristics, and so on to be stored in an LDAP directory.

LDAP can be used to deploy IPSec security policy to distributed network devices through the Internet.

7.0.1 The benefits of directory-assisted policy management

An advantage of using a directory server to store policy information as opposed to more traditional methods of locally stored configurations is the ability to make a change in one place and have that change applied across all the devices in the extended network. This includes devices in the local administrative domain as well as devices across public boundaries. Take for example, an IPSec transform definition that resides in the directory. To change the corporate policy for encryption from DES to 3DES normally would require a change in the configuration of each device in the extended network. If the directory server is used to deploy the policies then one IPSec transform would need to be changed in the LDAP server and then each policy-enabled device in the network would need to rebuild the internal policy database. Another good example would be if a DiffServ action named "GoldService" needed to be changed from 40% of bandwidth to 45% of bandwidth. The LDAP server and policy infrastructure allows these types of configuration changes to scale much better and reduce configuration mismatches.

This section is excerpted from the document "Configuration and Setup Instructions for Reading Policies from a LDAP Server" on the IBM Networking Web site. For more information, visit the following URL:

```
http://www.networking.ibm.com/support/code.nsf
```

then select either 2210, 2212 or 2216. Next click **LDAP Server Configuration Information.**

7.0.2 Directory client and servers

The network devices that support LDAP can be an LDAP client and can access required information from LDAP server. The information needed to configure the VPN tunnel is stored in a central LDAP server. The router or security gateway can be an LDAP client. To take advantage of this feature an LDAP server operating at RFC Version 2 or 3 is required.

7.0.3 LDAP schema

An LDAP schema is the set of rules and information that comprise the class and attribute definitions that define the entries that ultimately exist in the directory. LDAP schema is typically written in ASN1 syntax similar to SNMP MIBs.

7.0.4 Directory security

Directories are likely to contain sensitive information that needs to be protected from unauthorized access and modification. When sending data over networks, sensitive information may also need to be protected against eavesdropping and modification during transportation. LDAP supports both basic client authentication using a distinguished name and password and Secure Sockets Layer (SSL), which provides mutual authentication between clients and servers as well as data security through encryption. LDAP Version 3 supports the Simple Authentication and Security Layer (SASL), a framework for adding additional authentication mechanisms.

More information on LDAP can be found in the following redbooks:

- *Understanding LDAP*, SG24-4986
- *LDAP Implementation Cookbook,* SG24-5110

7.1 Nways router policy administration with LDAP

In this scenario, an LDAP server is installed on an AIX system (AIXSRV1) and two routers (2216 center and 2216 branch) are used as LDAP clients. The network diagram for the test is shown in Figure 125 on page 147:

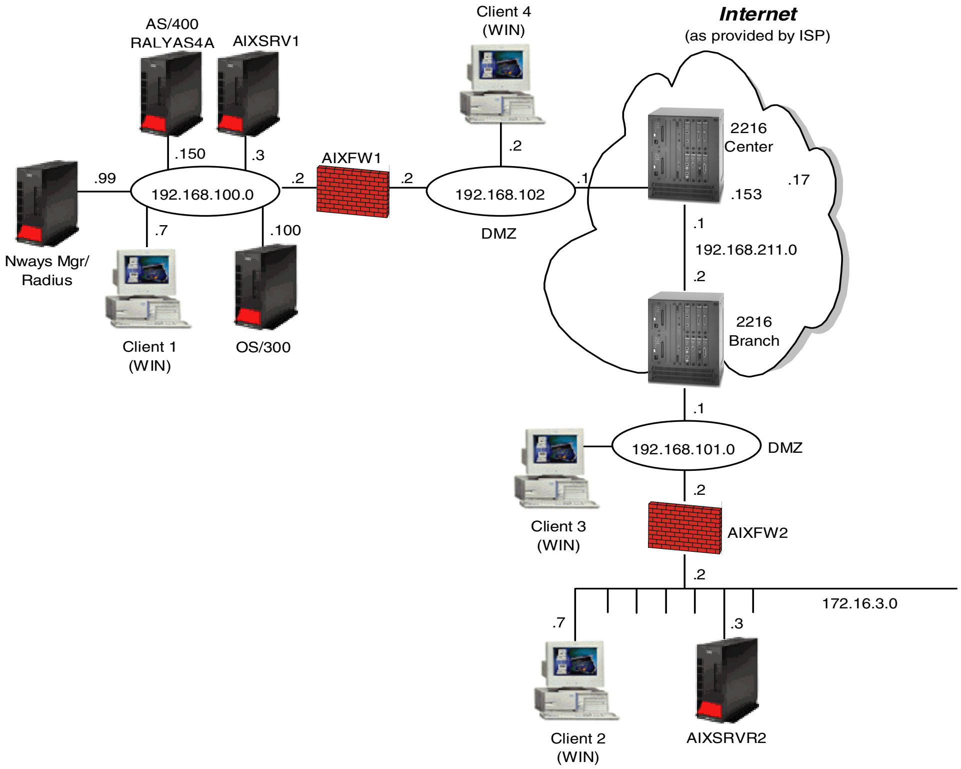


Figure 125. Router-to-router tunnel using LDAP

7.1.1 LDAP server configuration

IBM eNetwork LDAP Directory Server V2.1 is used as LDAP server on AIXSRV1 (AIX V4.3.2). The LDAP server provides a native, scalable directory based on the IETF LDAP Version 2 (RFC 1777) plus some extensions for IETF LDAP Version 3. IBM Universal Database Version 5 is packaged with the LDAP server and used as the directory storage facility. Lotus Domino Go V4.6.2 is used for LDAP server configuration and administration.

LDAP Directory Server V2.1 is bundled in AIX V4.3.2 CD (CD #2). The required components are as follows:

- ldap.client: LDAP No-ssl Client
- ldap.html.lang: LDAP HTML Installation/Configuration Guide
- ldap.server: LDAP No-ssl Server

DB2 will be installed automatically during LDAP server installation.

For SSL Version 3 support, the following components that are in AIX V4.3.2 Bonus Pack must be installed after LDAP client and server installation:

- gskru301: 128-bit encryption for LDAP
- gskrf301: 40-bit encryption for LDAP

Note

For security reasons, SSL is needed to protect information transferred between LDAP client and server. The SSL feature is added by installing IBM GSkit packages. The GSkit packages include Secure Sockets Layer (SSL) Version 3 support and associated RSA technology. There are two GSkit packages available: U.S. and Export. They come with different encryption strength. For AIX, the appropriate GSKit packages are included in the AIX 4.3.2 Bonus Pack.

7.1.1.1 Obtaining and installing LDAP server configuration files

To communicate with IBM 221x router using LDAP, the following files which define attributes, object class and security policies for 221x router are required. The IBM networking Web site `http://www.networking.ibm.com` provides these file sets.

Visit the Web site mentioned above and select **Support** and choose 2216, 2210, or 2212 from the Product list, then select **Downloads**. From the Download page, select **LDAP Server Configuration Information** and then download the files from the LDAP Server Configuration Files menu.

Files in the LDAP server configuration are listed below:

`policyTemplates.ldif`	Pre-defined policy objects
`policyExamples.ldif`	Some examples of security policies
`ibmPolicySchema.txt`	Description file for IBM's Policy Classes
`policySchema_oc.conf`	The objectclass file for the LDAP server
`policySchema_netscape_at.conf`	The attribute file for the Netscape LDAP server
`policySchema_ibm_at.conf`	The attribute file for the IBM LDAP server
`policySchema_openLdap_at.conf`	The attribute file for the OpenLdap server

To apply these configurations to the LDAP server, perform the following configuration steps:

The first two steps include the Objectclass file (policySchema_oc.conf) and Attributes file (policySchema_ibm_at.conf) in the LDAP server.

1. Locate the LDAP server configuration file. This typically is the slapd.conf file. On AIX this is in the /etc directory.
2. Edit the slapd.conf file and add the following lines (these lines should be added after any other include statements in the config file).

```
include <path>/policySchema_ibm_at.conf
include <path>/policySchema_oc.conf
```

The next step is adding and modifying policy entries to the LDAP server. The LDAP server parses the LDAP Data Interchange Format (LDIF) file to translate into the format necessary to use the LDAP protocol, and then handle the request(s) with the directory server.

3. Add the policy templates first:
   - Remove comments from the file using the following command:

```
grep -v '^#' policyTemplates.ldif > out.ldif
```

- Add the entries in the new out.ldif file using the ldapmodify client:

```
ldapmodify -h <hostname> -D <user dn> -w <password> -rac -f out.ldif
```

4. Make any modifications to the example policies supplied and then perform the following steps. Modification of the policy file is explained in 7.1.1.2, “Modifying LDAP server policy files for 221x router” on page 149.

   - Remove comments from the file using the following command:

   ```
   grep -v '^#' policyExamples.ldif > out.ldif
   ```

   - Add the entries in the new out.ldif file using the ldapmodify client:

   ```
   ldapmodify -h <hostname> -D <user dn> -w <password> -rac -f out.ldif
   ```

7.1.1.2 Modifying LDAP server policy files for 221x router

The policy class structure is shown in Figure 126 on page 150 and the policy search agent in the IBM 221x Router will retrieve all the policy information in the directory server that is intended for that device. The starting point for the policy search is DeviceProfile.

Two key objects in the Policy schema that allow the Policy Search Agent to search for and find the necessary policies for the device are the DeviceProfile and the DevicePolicyRules. The DeviceProfile has information about the device's mandatory DevicePolicyRules reference. Devices can be grouped together into one DeviceProfile or each device in the network can have its own DeviceProfile. This really will depend on whether more than one box in the network needs to fetch the same set of rules. Typically for Security Gateways this will not be true since every gateway will have a different tunnel endpoint. For QoS only boxes, it would be conceivable that a group of devices would all read the same set of policies. The DevicePolicyRules object will be retrieved based on the value in the DeviceProfile that is fetched for the device. Once the DevicePolicyRules object has been retrieved, then the list of PolicyRules for that device can be retrieved. If any of the objectclass is not found or if an error is detected during a consistency check on an object then the search is aborted and messages will be displayed for the PLCY ELS subsystem denoting the error detected.

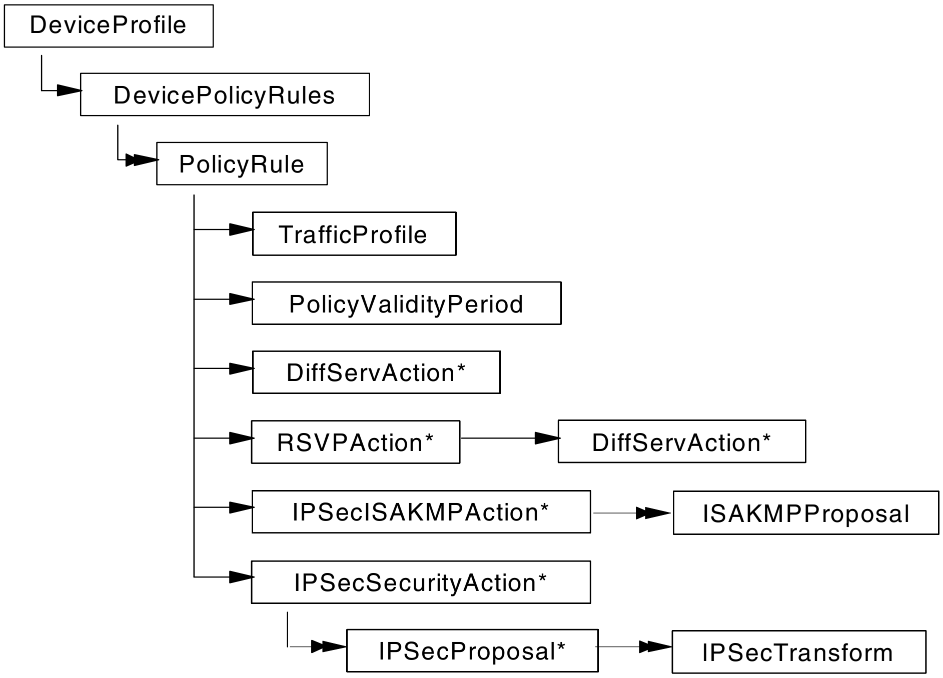


Figure 126. Policy class structure of LDAP configuration for 221x router

Modified policyExamples.ldif is shown below:

```
###########################################################################
###
### securing traffic between branch offices
###
### The policies in this file assume that the directory has been
### loaded with the pre-defined templates in "policyTemplates.ldif".
###
###########################################################################
### Branch office policy for securing traffic from 192.168.211.1 to
### 192.168.211.2. This policy consists of the information needed to
### setup the security association for the Security Gateway (2216CTR
### - public IP Address = 192.168.211.1) protecting the 192.168.102.0
### network and the information needed for the Security Gateway (2216BR
### - public IP Address = 192.168.211.2) protecting the 192.168.101.0
### network.
###########################################################################

# Profile for 2216CTR
dn: cn=G1toG2, o=ibm, c=us
objectclass: trafficprofile
cn: G1toG2
sourceaddressrange: 1:192.168.102.0-255.255.255.0
destinationaddressrange: 1:192.168.101.0-255.255.255.0

#IPSEC Action for 2216CTR
dn: cn=secureG1toG2, o=ibm, c=us
objectclass: IPSecSecurityAction
cn: secureG1toG2
securityaction: permit
ipsectunnelstart: 192.168.211.1
ipsectunnelend: 192.168.211.2
ipsecproposalreference: 1: cn=strongP2EspProp, o=ibm, c=us
ipsecproposalreference: 2: cn=strongP2EspAhProp, o=ibm, c=us
ipsecproposalreference: 3: cn=veryStrongP2EspProp, o=ibm, c=us
ipsecproposalreference: 4: cn=veryStrongP2EspAhProp, o=ibm, c=us

#Policy for 2216CTR
dn: cn=policySecureG1toG2, o=ibm, c=us
```

```
objectclass: policyrule
cn: policySecureG1toG2
rulepriority: 20
policyscope: isakmp
policyscope: ipsec
trafficprofilereference: cn=G1toG2, o=ibm, c=us
policyvalidityperiodreference: cn=allTheTime, o=ibm, c=us
ipsecsecurityactionreference: cn=secureG1toG2, o=ibm, c=us
ipsecisakmpactionreference: cn=generalPhase1Action, o=ibm, c=us

# Profile for 2216BR
dn: cn=G2toG1, o=ibm, c=us
objectclass: trafficprofile
cn: G2toG1
sourceaddressrange: 1:192.168.101.0-255.255.255.0
destinationaddressrange: 1:192.168.102.0-255.255.255.0

#IPSEC Action for 2216BR
dn: cn=secureG2toG1, o=ibm, c=us
objectclass: IPSecSecurityAction
cn: secureG2toG1
securityaction: permit
ipsectunnelstart: 192.168.211.2
ipsectunnelend: 192.168.211.1
ipsecproposalreference: 1: cn=strongP2EspProp, o=ibm, c=us
ipsecproposalreference: 2: cn=strongP2EspAhProp, o=ibm, c=us
ipsecproposalreference: 3: cn=veryStrongP2EspProp, o=ibm, c=us
ipsecproposalreference: 4: cn=veryStrongP2EspAhProp, o=ibm, c=us

#Policy for 2216BR
dn: cn=policySecureG2toG1, o=ibm, c=us
objectclass: policyrule
cn: policySecureG2toG1
rulepriority: 20
policyscope: isakmp
policyscope: ipsec
trafficprofilereference: cn=G2toG1, o=ibm, c=us
policyvalidityperiodreference: cn=allTheTime, o=ibm, c=us
ipsecsecurityactionreference: cn=secureG2toG1, o=ibm, c=us
ipsecisakmpactionreference: cn=generalPhase1Action, o=ibm, c=us

# DEVICEPOLICYRULES LIST for 2216CTR
dn: cn=rulesFor2216CTR, o=ibm, c=us
objectclass: devicepolicyrules
cn: rulesFor2216CTR
policyrulereference: cn=policySecureG1toG2, o=ibm, c=us

# DEVICEPROFILE for 2216CTR
dn: cn=deviceProfileFor2216CTR, o=ibm, c=us
objectclass: deviceprofile
cn: deviceProfileFor2216CTR
devicerulesreference: cn=rulesFor2216CTR, o=ibm, c=us

# DEVICEPOLICYRULES LIST for 2216BR
dn: cn=rulesFor2216BR, o=ibm, c=us
objectclass: devicepolicyrules
cn: rulesFor2216BR
policyrulereference: cn=policySecureG2toG1, o=ibm, c=us

# DEVICEPROFILE for 2216BR
dn: cn=deviceProfileFor2216BR, o=ibm, c=us
objectclass: deviceprofile
cn: deviceProfileFor2216BR
devicerulesreference: cn=rulesFor2216BR, o=ibm, c=us
```

In this scenario, pre-shared key mode is used on two 221x routers. It means that the certificate-based IKE Phase 1 negotiation definition should be removed or move down in ISAKMP proposal reference. To do this modify generalPhase1Action in the policyTemplates.ldif file like this:

```
dn: cn=generalPhase1Action, o=ibm, c=us
```

```
objectclass: ipsecisakmpaction
cn: generalPhase1Action
isakmpexchangemode: 2
isakmpproposalreference: 1: cn=veryStrongP1PropSharedKey, o=ibm, c=us
isakmpproposalreference: 2: cn=strongP1PropSharedKey, o=ibm, c=us
isakmpconnectionlifetimesec: 30000
isakmpconnectionlifetimekbytes: 5000
isakmpautostartflag: 0
```

LDAP server configuration for the 221x router is done and ready to access from routers.

7.1.2 LDAP client configuration on the IBM NWays 221x routers

We show in this chapter only the configuration of the router in the center. The configuration of the branch router will be almost identical.

7.1.2.1 Overview

Policies on the router are stored in a database. This simplifies the configuration because information that is used by different policies must only be entered once.

If this database is maintained on each router this solution does not scale. Therefore, it is advisable to provide this database centrally where it is much easier to maintain the policies for all different devices. All policy changes can be done in one place.

Therefore, the IETF has proposed a central database concept where the central server is an LDAP server and each network device is an LDAP client.
LDAP is a protocol that allows a directory server to be searched and modified.
LDAP is a lightweight version of the X.500 standard.

The 221x family of routers (with V3.3 or greater) allow the repository of policy information to be a Lightweight Directory Access Protocol (LDAP) server. The routers support the ability to search (not modify) for information in the directory server. The policy search agent in the router will retrieve all the policy information in the directory server that is intended for that device.

When the policy exists in the LDAP server you should enable the routers to retrieve their policy from the LDAP server. You have to do the following steps:

- Set the default policy.
- Define the IP address of the LDAP server.
- Set the bind parameters to authenticate to the LDAP server.
- Configure the name of the DeviceProfile in the LDAP server.
- Enable retrieving policy from the LDAP server.
- List the LDAP configuration.
- Activate the LDAP configuration.

These bullets will be explained in more detail in the following chapters.

7.1.2.2 Set default policy

We have to consider the time frame when the router is working but has not yet built its policy database:
When a router boots it looks at the default rule. The default rule describes what a

router should do with traffic while it is building its database. The options are forward all traffic or drop all traffic except LDAP traffic, or drop all traffic and secure LDAP traffic. The default is to forward all traffic.

If you are defining security policies you will probably wish to drop the traffic until the policy database is built - if not, the data would be forwarded without security. If you are retrieving you are also retrieving those polices using LDAP which you also want to use to forward your LDAP traffic. Therefore, you can define that LDAP should be secured. This default action is defined using the `set default` command. If you choose to secure your LDAP traffic you will be guided through creating an IPSec and ISAKMP action.

7.1.2.3 Define the IP address of the LDAP server

In `talk 6` and `feature policy` you have to define the IP address of the (primary) LDAP server. You could also define the IP address of a secondary LDAP server which we did not do in our lab environment (`SET LDAP SECONDARY-SERVER`).

If the LDAP client gets no response from the primary LDAP server after the “retry interval” it will contact the secondary server. If the secondary server is available, it will retrieve the policies. If the secondary is unavailable, the router will then contact the primary again. The primary and then the secondary server will continue trying at the time interval specified in the “retry interval” until the router manages to retrieve the policies. The interval can be configured from `talk 6`, `feature policy`. While the router is trying other servers, it needs to know what to do with traffic. This is described in the default error handling procedure which is also configured using the `set default` command. The options are flush the whole database and apply the default rule or flush any LDAP rules and apply the local rules. This error handling also describes what happens if there is an error reading the rules.

If you are using LDAP and also define local rules, it is advisable to choose to apply the local rules if for any reason you cannot read the LDAP rules.

See Figure 127 on page 153 for the configuration of the primary LDAP server:

```
Center *TALK 6
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>SET LDAP PRIMARY-SERVER 192.168.100.3
Center Policy config>
```

Figure 127. Set IP address of LDAP server

7.1.2.4 Set the bind parameters

LDAP defines that LDAP clients can either bind to the server without any authentication or with a user ID and password. Without authentication is known as anonymous. Note that by default not all servers will support anonymous binds.

If you want to define authentication then set the bind parameters. First enable the sending of authentication parameters by issuing the following command (These parameters must match a user defined in your authentication server):

```
Center Policy config>
Center Policy config>SET LDAP ANONYMOUS-BIND
Do you wish to bind to the LDAP server anonymously? [Yes]: no
Center Policy config>SET LDAP BIND-NAME cn=root
Center Policy config>SET LDAP BIND-PW byte2eat
Center Policy config>
```

Figure 128. Set the LDAP bind parameters

7.1.2.5 Configure the name of the DeviceProfile in the LDAP server

When the router has bound with the LDAP server, it then performs its search for its policies. It identifies where it starts by sending in a start point. This value should be the distinguished name of the router as configured in the deviceprofile.

Figure 130 shows the configuration of the distinguished name of the deviceprofile object in the LDAP server for this device.

```
Center Policy config>
Center Policy config>SET LDAP POLICY-BASE cn=DeviceProfileFor2216ctr, o=ibm, c=us
Center Policy config>
```

Figure 129. Configure the name of the DeviceProfile in the LDAP server

7.1.2.6 Enable retrieving policy from the LDAP server

To enable the retrieve function use the following command:

```
Center Policy config>
Center Policy config>ENABLE LDAP POLICY-SEARCH
Center Policy config>
```

Figure 130. Enable retrieving policy from the LDAP server

7.1.2.7 List LDAP configuration

The command `list ldap` lists the LDAP configuration (Figure 131):

```
Center Policy config>
Center Policy config>LIST LDAP
LDAP CONFIGURATION information:
        Primary Server Address:             192.168.100.3
        Secondary Server Address:           0.0.0.0
        Search timeout value:               3 sec(s)
        Retry interval on search failures:  1 min(s)
        Server TCP port number:             389
        Server Version number:              2
        Bind Information:
        Bind Anonymously:                   No
        Device Distinguished Name:          cn=root
        Base DN for this device's policies: cn=DeviceProfileFor2216ctr, o=ibm,
        Search policies from LDAP Directory: Enabled
Center Policy config>
```

Figure 131. Listing LDAP configuration

7.1.2.8 Activate the LDAP configuration

For the changes made above to take effect, the user must either restart/reload the router or go into talk 5 and use the dynamic reconfiguration feature of the router to activate the changes.

This procedure is shown in Figure 132 on page 155:

```
Center *TALK 5
Center Policy console>RESET LDAP-CONFIG
LDAP Policy Configuration reset successfully
Center Policy console>
Center Policy console>RESET DATABASE
Policy Database reset successful
Center Policy console>
```

Figure 132. Activating the LDAP configuration

7.1.2.9 Tests and troubleshooting

Beside listing the current LDAP configuration `list ldap` (Figure 131 on page 154) there are more commands to do testing and troubleshooting:

List policies

The `list policy all` command provides you with a list of all defined policies and their status (disabled/enabled). You also see the corresponding profile, the validity period, the IPSec action and the ISAKMP action.

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled   : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-act1
       .......
```

Figure 133. Output of the command list policy all

The `list policy basic` command (in talk 5) lists all the defined policies. The command also shows from where the policies were loaded. It also shows the status (enabled/disabled, valid/invalid). If the policy shows as enabled/invalid this might point to a policy that only applies at certain times.

```
Center *TALK 5
Center +FEATURE Policy
IP Network Policy console
Center Policy console>LIST POLICY BASIC
1: (Disabled,Valid)     ipsec_man_101_102
2: (Disabled,Valid)     ike-pre-101-102
3: (Disabled,Valid)     ike-pre-3-100
4: (Disabled,Valid)     ike-pre-211-211
5: (Enabled,Valid)      cn=policySecureG1toG2, o=ibm, c=us
Number of Policy to display (0 for All) [0]? 5
Policy Name: cn=policySecureG1toG2, o=ibm, c=us
Loaded from: LDAP Server
State:       Enabled and Valid
Priority:    20
Hits:        0
Profile:     cn=G1toG2, o=ibm, c=us
Validity:    cn=allTheTime, o=ibm, c=us
IPSEC:       cn=secureG1toG2, o=ibm, c=us
ISAKMP:      cn=generalPhase1Action, o=ibm, c=us
Center Policy console>
```

Figure 134. Output of the command list policy basic

Test forwarder-query

If you want to check your policy actions in the way you want, there are four different test commands which can be used. With `test forwarder-query` you specify an IP packet. The policy database will then be searched if there is a rule in the policy database that matches the IP packet.

The `test isakmp-query` command returns the ISAKMP policy to be enforced based on packet information. The `test ipsec-query` command returns the IPSEC policy to be enforced based on packet information. The `test rsvp-query` command returns the RSVP policy to be enforced based on packet information.

See Figure 135 on page 156 for an example of `test forwarder-query`:

```
Center Policy console>TEST FORWARDER-QUERY
Enter IPV4 Source Address [0.0.0.0]? 192.168.211.1
Enter IPV4 Destination Address [0.0.0.0]? 192.168.211.2
Enter the value for the Source Port [0]?
Enter the value for the Destination Port [0]?
Enter the value for the IP Protocol ID [0]?
Enter the value for the IP TOS Byte [0]?
No match found
Center Policy console>TEST FORWARDER-QUERY
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.5
Enter IPV4 Destination Address [0.0.0.0]? 192.168.101.7
Enter the value for the Source Port [0]?
Enter the value for the Destination Port [0]?
Enter the value for the IP Protocol ID [0]?
Enter the value for the IP TOS Byte [0]?
Results of Test:
Policy (IPSEC):  ike-pre-101-102.traffic
       IPSEC Action:  tun-101-102
Center Policy console>
```

Figure 135. Result of the command test forwarder-query

List status of policy

The command `status` (talk 5) shows whether the last refresh of the policy was successful and whether the router was able to read the policy from the LDAP server (Figure 136 on page 157):

```
Center *TALK 5

Center Policy console>STATUS
Status of Last Search:       Successful
Time since last refresh:     21 hours, 11 minutes and 13 seconds
Next Policy Refresh not scheduled

Number of Active IKE Negotiated IPSEC Tunnels:  2
Maximum Number of IKE Negotiated IPSEC Tunnels: 100
Center Policy console>
```

Figure 136. Output of the command status

LDAP version

You can also check the LDAP version on the client:

```
Center *TALK 6

Center Policy config>SET LDAP VERSION
Enter the LDAP Version number of the LDAP server (2 or 3) [2]? 2
Center Policy config>
Center Policy config>
```

Figure 137. LDAP version

ELS trace

Use ELS for troubleshooting. The command `NODISPLAY SUBSYSTEM ALL ALL` switches off all ELS subsystems. Afterward you should use the command `DISPLAY SUBSYSTEM subsystem ALL` to enable all ELS-messages that you think are relevant for your problem determination (Figure 138 on page 157):

```
Center ELS>NODISPLAY SUBSYSTEM all all
Complete
Center ELS>DISPLAY SUBSYSTEM LDAP all
Center ELS>
```

Figure 138. ELS commands

The following subsystems may be important for troubleshooting LDAP problems:

- LDAP
- PPP
- IKE
- PKI
- IPSP (for IPSec)
- PLCY

Support from IBM Networking home page

Check the networking home page for LDAP server configuration information. It can be found at

`http://www.networking.ibm.com/support/code.nsf/2210ldap?OpenView`

In "Configuration and Setup Instructions for Reading Policies from a LDAP Server" you can find further hints for troubleshooting LDAP.

7.1.3 Secure transmission of LDAP traffic using tunnels

LDAP traffic flows through the Internet, and is therefore assumed to be non-secure. Because of this, from a security point of view, secure transmission of LDAP data between client and server is needed.

The best way to make LDAP traffic secure is using Secure Sockets Layer (SSL) between LDAP client and LDAP server. If the network devices do not support Secure Sockets Layer, other secure channels between them are needed.

We consider IKE tunnel or manual tunnel between LDAP client and server only for LDAP traffic.

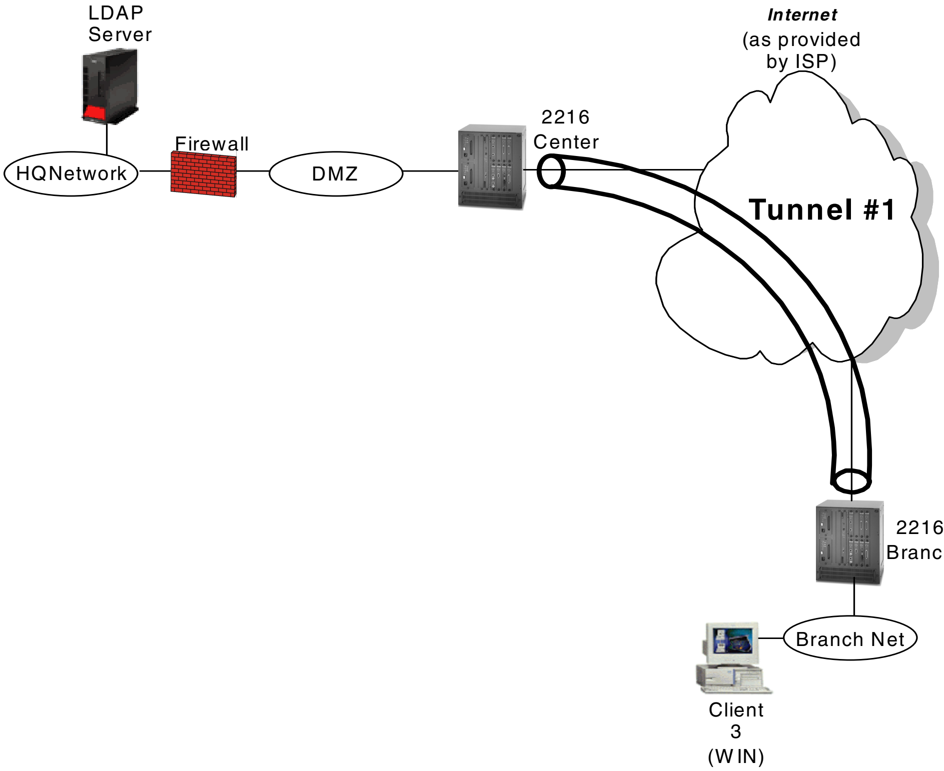


Figure 139. Initial tunnel for LDAP traffic

The following steps explain the procedure of securing LDAP information using a tunnel:

1. Before installing the 2216 branch router, IKE tunnel or manual tunnel definition that only allows IP Security and LDAP traffic (see Tunnel #1 in Figure 139 on page 158) must be in place in the 2216 branch router and corresponding tunnel definition must be in place in the 2216 center router.

2. The 2216 branch router will initiate a predefined tunnel to the 2216 center router and establish a tunnel for a secure LDAP data transfer at boot-up.
3. The 2216 branch router will request tunnel configuration information to the LDAP server through a predefined tunnel.
4. The 2216 branch router makes tunnels according to the configuration information from LDAP server for normal data traffic.
5. The 2216 branch router may release a predefined tunnel if possible.

The predefined tunnel can be established directly between the LDAP server and 2216 branch router if there is no Network Address Translation (NAT) issue.

This method may be useful and efficient for a service provider to deploy an Internet VPN solution without human error.

Chapter 8. Network management for VPNs

With the growth of a network the complexity increases and the ability to manage it decreases. Therefore, everybody who is responsible for running a network should pay attention to this aspect of management:
The network management function should enable the support functions to maintain the network effectively and efficiently.

In this section we describe the general concept of network management and design considerations specific for the Internet VPN.

Details concerning VPN management with the IBM product Nways Manager Suite (Version 2) are given in 8.6, “VPN management using Nways VPN Manager” on page 170.

8.1 Systems management

The management requirements are categorized into disciplines. A discipline is a broad category of systems management tasks and the functions that address those tasks. The disciplines, therefore, are categories for systems management processes. You can, for example, formalize this into the following six systems management disciplines:

Business management

The business management discipline focuses on managing the tasks that support a wide range of enterprise-wide business and administrative functions to improve control of information system assets and provide efficient and effective administrative processes.

Change management

The change management discipline focuses on managing the introduction of change into an information system environment.

Configuration management

The configuration management discipline focuses on managing the set of resources (hardware and software) and connectivity that provide the exchange of business information within an enterprise and with external customers.

Operations management

The operations management discipline focuses on managing the use of systems and resources to support the workloads of the enterprise’s information systems.

Problem management

The problem management discipline focuses on managing problems and potential problems from their detection to their resolution.

Performance management

The performance management discipline focuses on managing the effectiveness with which information systems deliver services to their users.

In general, from the network management viewpoint, the above six disciplines can be applied to the Internet VPN management. Comparing traditional network management, the Internet VPN has distinct characteristics that will be discussed in this section.

- For change management, the gateways (for example, routers) are physically connected through the Internet and the VPNs are logically controlled by tunnel definition on the gateways. The management of changes in VPN is logical rather than physical.
- For configuration management, the topology, tunnel definition, and applied security policy are maintained centrally in addition to traditional network configuration. The remote access user information must be maintained. The secure key distribution including certification and directory-based policy management will be the critical part of the configuration management.
- For problem management, there are two aspects of connectivity problems in VPN. One is the IP connectivity to the Internet and another is the secure VPN tunnel connectivity over IP connectivity. The VPN tunnel establishment and status monitoring in addition to IP connectivity monitoring must be done to identify the problem.
- For performance management, the normal IP traffic and secure VPN traffic through a tunnel is transferred using one physical line. And normally the performance degradation will occur to VPN traffic. The performance for each tunnel may be also measured as physical line traffic.

8.2 Design considerations

There are two topology viewpoints, physical topology and logical topology. From the point of view of an Internet VPN service provider, both physical topology and logical topology must be maintained and monitored. In other words, companies that use Internet VPN from a service provider only need logical topology management.

The topology of the traditional IP network is a star or tree from the physical and logical viewpoint. But, for Internet VPN, the physical network topology is mesh. From the network management viewpoint, the physical network is considered a network cloud such as a frame relay network and each router is connected to that network cloud. Logical topology is more important than physical topology.

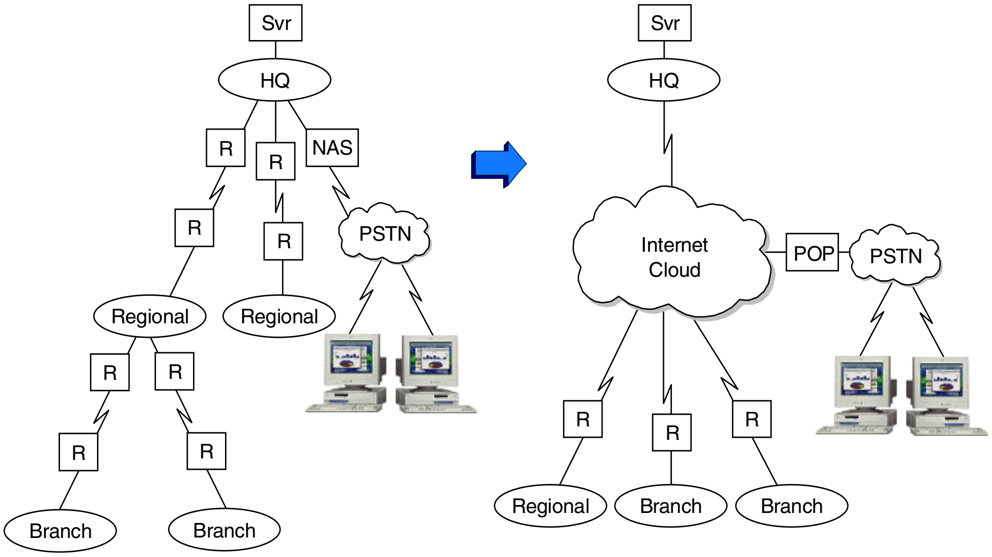


Figure 140. Comparison of conceptual topology

8.3 SNMP management

The network management system uses the following protocols:

- Simple Network Management Protocol (SNMP)
- ICMP echo/reply

SNMP is based on a manager-agent interaction. The network elements, such as gateways, routers, bridges, and hosts, contain SNMP agents that act as servers and perform the network management functions requested by the network managers. The network managers act as clients; they run the management applications that monitor and control the agents.

SNMP uses request/response processing as a means of communicating between the network managers and the agents in the network elements to send and receive information about network resources. This information can be status information, counters, identifiers, and more. Request/response processing involves the exchange of information among different entities through requests that are received by an entity for processing, after which it generates a response to be sent back to the originator of the request. SNMP uses this type of protocol to transfer data between managers and agents. The SNMP manager can send a request to the SNMP agent which will in return send a response. The SNMP request/response process is shown in Figure 141 on page 164.

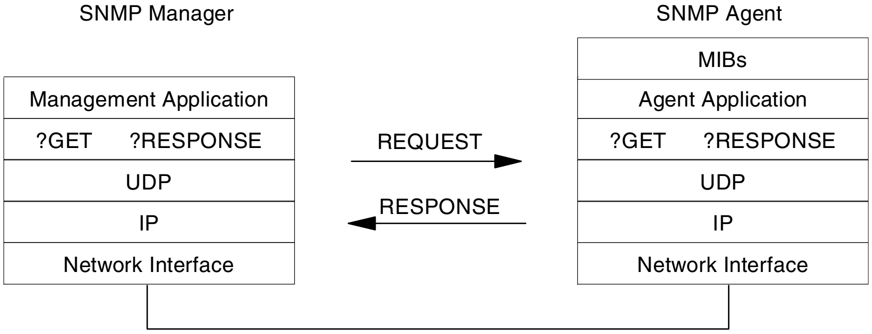


Figure 141. SNMP request/response process

An agent system can also generate SNMP messages called traps without a prior request from the managing system. The purpose of a trap message is to inform the managing system of an extraordinary event that has occurred at the agent system. The SNMP trap process is shown in Figure 142.

An SNMP protocol entity receives messages at UDP port 161 on the system with which it is associated, except for those that report traps. Messages that report traps should be received on UDP port 162.

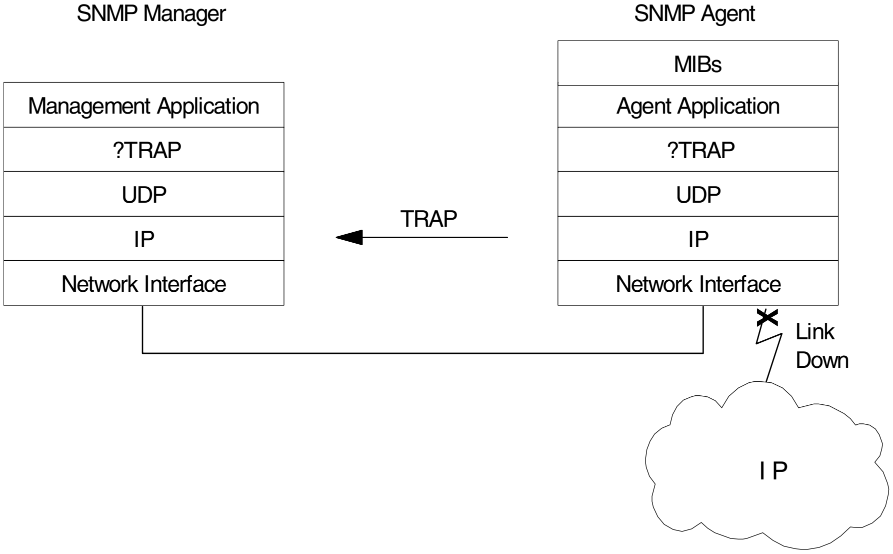


Figure 142. SNMP trap process

An SNMP community is an administrative relationship between an SNMP agent and one or more SNMP managers. Each community consists of a community name, an object access specification, and a list of SNMP managers' IP addresses. The SNMP manager needs to provide a valid community name to the SNMP agent before the agent will honor any requests from that manager. In this manner, the community acts as a password.

Even though SNMP uses community to authenticate a requested party, SNMP traffic flows in clear text and can be sniffed easily and the critical network information is included in SNMP traffic. The secure SNMP data transmission through the Internet is required. The management tunnels must be used for securing SNMP traffic. The data tunnel can also be used as the management tunnel. If a dedicated management tunnel is used, proper filter rules for SNMP and ICMP should be implemented to ensure security.

8.4 SNMP management and VPNs

We describe network design consideration for network management function, especially management tunnels. From the network management viewpoint, the Internet VPN is categorized as below:

Figure 143 on page 165 and Figure 144 on page 166 show typical network configurations for VPNs.

The general design consideration for Internet VPN is limiting the automatic network discovery function using a seed file when NMS discovers a network. For a normal IP network, NMS can discover as many network nodes as the network has. But in case of Internet VPN, specific IP addresses for each node must be defined before discovery. Sometimes, intermediate routers could not provide IP address and interface information at the NMS’s request.

The network management system can also use data tunnel between the center gateway and the remote gateway to transfer management traffic between NMS and managed gateways. In this case, no special design considerations exist.

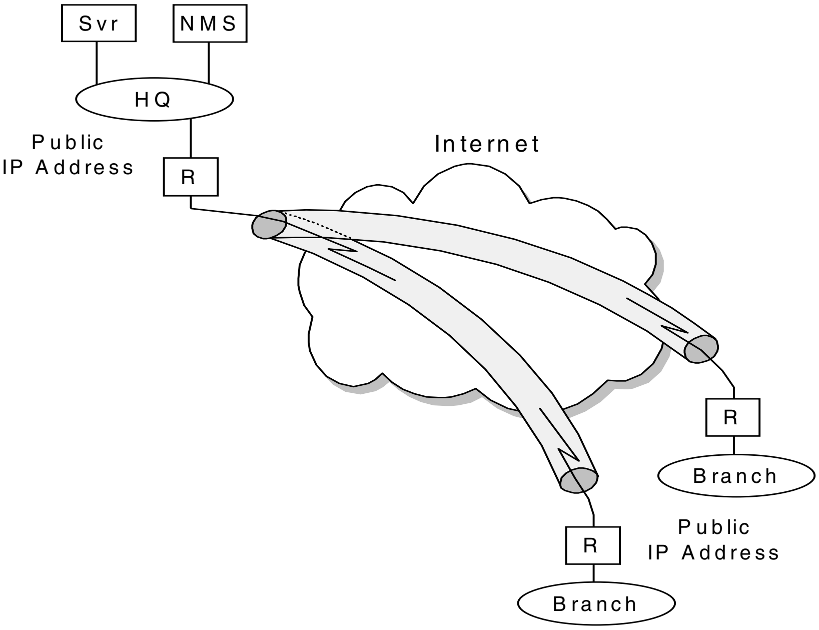


Figure 143. Gateway-to-gateway network connection with public IP addresses

For gateway-to-gateway tunnel connections these subnetworks use public IP addresses; NMS displays public addresses.

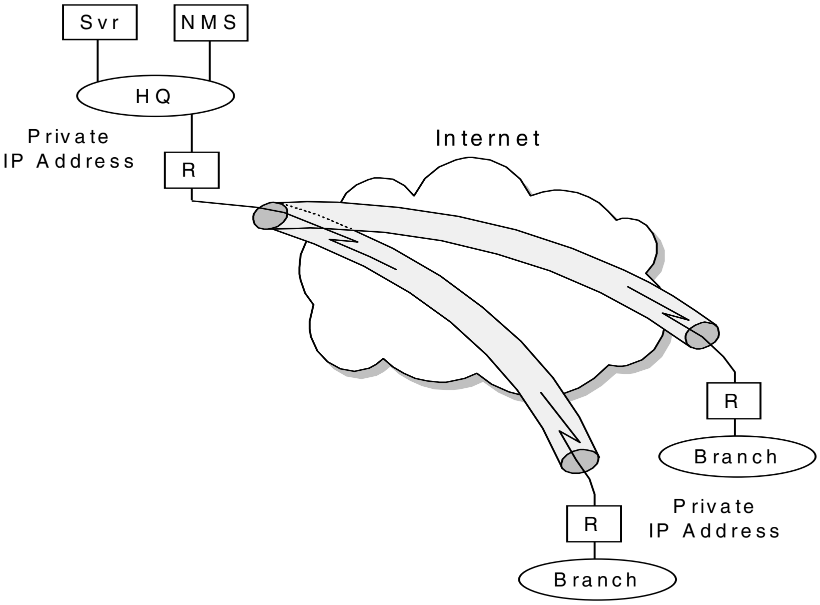


Figure 144. Gateway-to-gateway network connection with private IP addresses

For gateway-to-gateway tunnel connections these subnetworks use private IP addresses; NMS displays public IP addresses for Internet connected interfaces and private IP addresses for subnet connected to LAN interface. The tunnels provide a transparent view to NMS and NMS can recognize private IP addresses of the subnet on a remote site. The design consideration for these cases is the scope of managed objects. For example, for simple network management, the management scope may be the network between gateways. The management scope may include network, gateways, and LAN in remote sites. Before designing NMS, it is necessary to determine the management scope.

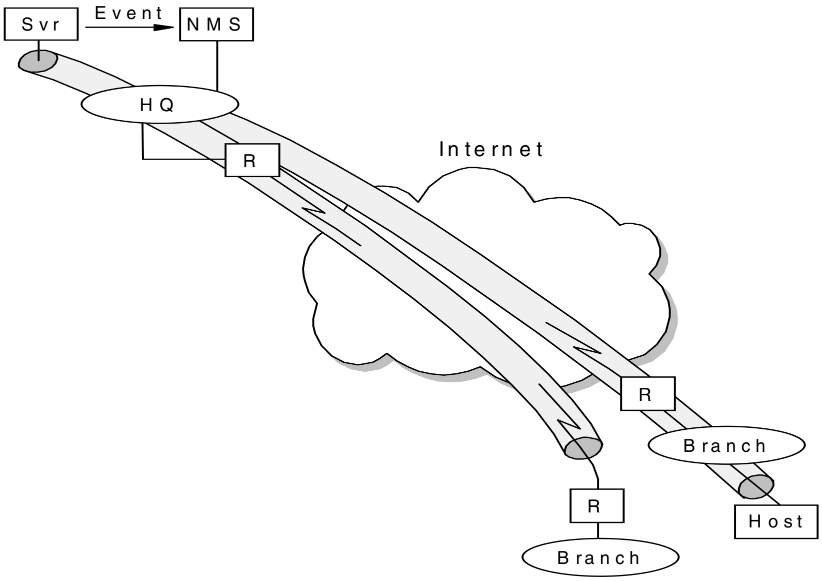


Figure 145. Gateway-to-host network connection and host-to-host network connection

For the gateway-to-host network connection, the NMS can monitor these types of tunnel connections through gateways. But if the NMS is located in a central site and the gateway is located in a remote site, it is not easy to monitor a gateway from NMS when the tunnel or physical line has a problem.

For the host-to-host network connection, the NMS cannot monitor host-to-host tunnel connections. In this case, special design consideration is required. One of the possible solutions is using a system management tool such as Tivoli Distributed Monitor to detect changes in the host and integrate an event to NMS. Before considering the above solution, checking if the host supports IPSec MIB may be needed.

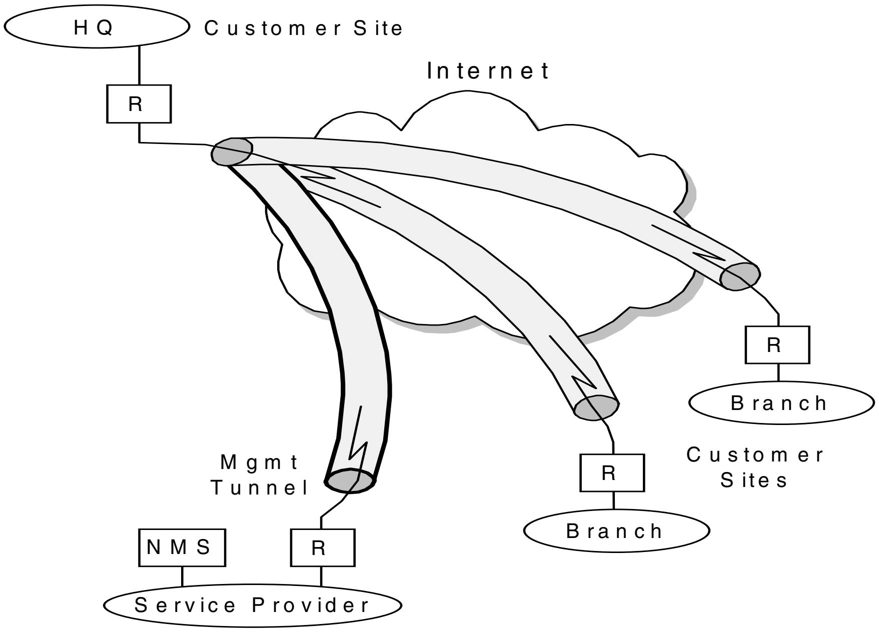


Figure 146. Internet VPN service provider

From the Internet VPN service provider viewpoint, an additional tunnel for management traffic between a service provider's network to the gateway in a customer's center site must be implemented to monitor a customer's VPNs. In this case, the filtering to protect traffic flow among a customer's network must be implemented and assured. The physical topology and IP connectivity should be monitored and maintained on behalf of the customer.

8.4.1 Management objects for Internet VPN

The physical and logical characteristics of a system make up a collection of information that can be managed through SNMP. The individual pieces of information make up Management Information Base (MIB) objects. A MIB is comprised of MIB objects, and they reside on the agent system, where they can be accessed and changed by the agent at the manager's request.

The MIBs that may be used for IPSec are categorized below:

- Monitoring and status MIBs for IPSec
- Configuring IPSec implementation
- Policy information

Currently, only monitoring and status MIBs for IPSec is in draft, `draft-ietf-ipsec-mib-03.txt`. These MIBs provide capabilities to determine operating conditions, perform system operational level monitoring of the IPSec portion of a network and statistics.

The IPSec MIB provides information related to both Phase 1 or IKE SAs and Phase 2 (or IPSec) SAs. SA configuration is provided as are statistics related to the SAs. A number of aggregate totals is provided for taking snapshots of system behavior or traffic trend without excessive SNMP traffic. This statistics MIB is useful to VPN service providers.

Four tables are used to define IPSec:

- The IKE control channel
- The IKE SAs
- The IPSec virtual tunnel
- The IPSec protection suite

Some information about SAs has been left out for security considerations if SNMP traffic becomes compromised.

The SNMP traps to notify error condition and status changes from IPSec function are used. A transient tunnel such as a dial-in connection will go up and down frequently and notification from this tunnel is not necessary for system administration. A permanent tunnel such as a gateway-to-gateway connection is considered a significant resource and the notifications from this tunnel should be monitored and handled properly.

The traps are forwarded from an IPSec-enabled device when the Phase 1 or 2 negotiation failed, the packets with an invalid sequence number or selector are received, or ESP, AH packets with unknown SPIs are detected.

8.4.2 Integration into other management tools

For proactive management and system-network combined management, the network management system may cooperate with other management tools or directory server.

The Lightweight Directory Access Protocol (LDAP) server contains network configuration information centrally and NMS can be notified when configuration information in the LDAP server for certain network nodes is changed or NMS can issue configuration refresh action to a network node.

Normally NMS can monitor a gateway-to-gateway tunnel, but NMS cannot monitor host-to-host tunnel connection. In this case, the system management tool that provides system resource monitoring functions, such as Tivoli Distributed Monitor, can detect the status changes of the VPN tunnel between two hosts and forward the event to NMS. This seamless event integration can be helpful to network and system administrators to identify a problem cause and isolate a problem source.

8.5 Network management objects for IBM Nways routers

For the Nways family of routers, two MIBs are defined for VPNs:

- ibmipsec.mib: IP Security MIB
- ibmvpnpolicy.mib: VPN Policy MIB

These two MIBs can be found under the IBM Enterprise Specific MIB tree.

The IP Security MIB has the following object groups:

- IPSec Levels Group:
  Describes the level of the IBM IPSec MIB used.
- IPSec Phase-1 Group:
  Consists of an Internet Key Exchange (IKE) tunnel table that has IKE tunnel configuration information.
- IPSec Phase-2 Group:
  Consists of Phase-2 tunnel statistics, tunnel information, client information related to Phase-2 tunnel, and security protection suite.
- IPSec History Group:
  Consists of previous Phase-2 tunnel history and failure records.
- IPSec TRAP Control Group:
  Consists of objects that control the sending of IPSec TRAPs.

The VPN Policy MIB has the following object groups:

- The System Group: Consists of a global system parameter such as policy source and LDAP configuration information.
- The Policy Group: Consists of policies, policy rules such as priorities, and correlations to VPN polices with VPN policy rules.
- The Conditions Group: Consists of traffic profile and traffic interface which controls traffic, remote identification methods such as authentication, and validity period.
- The Actions Group: Consists of actions for RSVP, Differential Services, ISAKMP, which includes ISAKMP proposal, and Security, which includes security proposals and AH, ESP transforms.
- The Test Group: Consists of table for policy test.

The supported IP Security related traps are list in Figure 147 on page 170. These traps are defined in IP Security MIB and the enterprise value is ibmIROCroutingIpSec (1.3.6.1.4.1.2.6.119.4.9).

Trap Name	Trap No.	Description
ikeTunnelStart	1	Generation of this trap occurs each time an IPSec IKE Phase-1 tunnel is created.
ikeTunnelStop	2	Generation of this trap occurs each time an IPSec IKE Phase-1 tunnel is terminated.
ipSecTunnelStart	3	Generation of this trap occurs each time an IPSec Phase-2 tunnel is created.
ipSecTunnelStop	4	Generation of this trap occurs each time an IPSec Phase-2 tunnel is terminated.
ipSecAuthFail	5	Generation of this trap occurs each time an IPSec Phase-2 authentication failure is detected.
ipSecDecryptFail	6	Generation of this trap occurs each time an IPSec Phase-2 decryption failure is detected.

Figure 147. Traps defined in IP Security MIB

IBM provides VPN management function of the 221x router, status monitoring and policy management. To manage VPN networks that consist of IBM 221x router, the following components are required:

- Tivoli NetView
- Nways VPN Manager

In addition to traditional management functions, topology management and device management, the Nways VPN manager provides VPN specific functions:

- Supporting layer 2 and 3 VPNs, including IKE tunnel
- Validating VPN policies and tunnels
- Policy test simulating traffic against VPN policies in the router
- Layer-2 test for dial-in users to replicate dial-in response time and connectivity
- Forwarding of VPN events to the network management console such as Tivoli NetView
- Operational control to prompt policy refresh from the LDAP server

8.6 VPN management using Nways VPN Manager

Managing a VPN network can be done in two ways:

You either use the router-based commands, where you can get all relevant information which is necessary to keep your network running. This approach, however, does not scale well.

Alternatively you can use an application with a GUI that also does automation for you. This approach is especially recommended if you have a large and meshed VPN network using different VPN protocols. An outstanding tool to operate your VPN network is IBM VPN Manager.

We used the VPN manager in our environment and it helped us a lot to verify, test and troubleshoot our VPN installation.

We will show in this chapter the practical usage of VPN manager. To give a complete picture we describe the router-based commands in the following chapters.

8.6.1 Overview

The VPN manager is IBM's product to operate VPNs. It is standards based and it is multivendor compatible, as it requires only one endpoint to be an IBM router. The prerequisite is that the other endpoint hardware supports the standards for IPSec, Layer 2 Tunneling Protocol (L2TP) or migration paths to the standard (Layer 2 Forwarding [L2F] or Point-to-Point Tunneling Protocol [PPTP]).

The prerequisite for using Nways VPN Manager in an Nways router environment is a code level of at least V3.3 (CC5) on the routers.

As already mentioned before, the Nways VPN Manager supports four activities for validating VPN tunnels and policies:

- Policy and session testing
- Point-in-time monitoring
- Logging and forwarding of VPN-related events to the management console
- Operational control to disable a VPN or refresh its policy

All four activities will be explained in more detail in this chapter. But we will start with a description of the basic usage of Nways VPN Manager:

8.6.2 Usage of the VPN manager

In this subchapter we will give a brief overview of how to start and how to handle Nways Manager.

8.6.2.1 Starting VPN manager

You start the VPN manager from Tivoli Netview menu:
Tools-> IBM Nways Java-> Open VPN View

After starting the VPN manager you will see a menu to select between the VPN List Manager Control and the Nways Device List.

The *VPN List Manager Control* provides you with information of the basic settings, for example, the log file and administration of passwords.

8.6.2.2 VPN Device List

The Nways VPN Device List allows you to view a list of devices that are being maintained by an Nways service called the VPN List Manager. This service receives devices from users of this application.

This application allows user control of the VPN List Manager. The user may reset or add to the VPN List Manager's list. The user may choose to add devices to the list by accessing a manual list, or by rechecking the system database.

The application presents the user with a list of devices in tabular form that allows scrolling, searching, and sorting. By clicking a device in the list, you can see more details about that device. Double-clicking will launch the Nways VPN Monitor Application (see 8.6.2.3, “VPN Monitor Application” on page 172) so you can view specific VPN information on this device.

8.6.2.3 VPN Monitor Application

The VPN Monitor Application will provide monitoring, event reporting, operational control, troubleshooting and application launching functions. The monitoring function will provide the ability to view active and previous VPN tunnels, view active and previous VPN clients and view defined and active VPN policies. The event reporting function will provide the information on VPN tunnel starts and when a VPN device experiences a security attack. The operational control function will provide the ability to disable/inactivate a VPN tunnel, disable/inactivate a VPN client and refresh VPN policies. The troubleshooting function provides the ability to proxy-ping a VPN device and view VPN event failure logs. The application launching function provides the ability to launch the device management applications, Telnet, and MIB browsing.

8.6.2.4 Help

In the VPN manager you can find Help in the HTLML format by clicking **Help->Contents.**

8.6.3 Overview of VPN Monitor Application functions

In the VPN Monitor Application you have many available functions. Figure 148 on page 173 gives a brief overview.

Note

The following screenshots from Nways Manager have been manipulated to provide better print quality. The application does not provide for changing foreground and background colors so actual application screens may appear different.

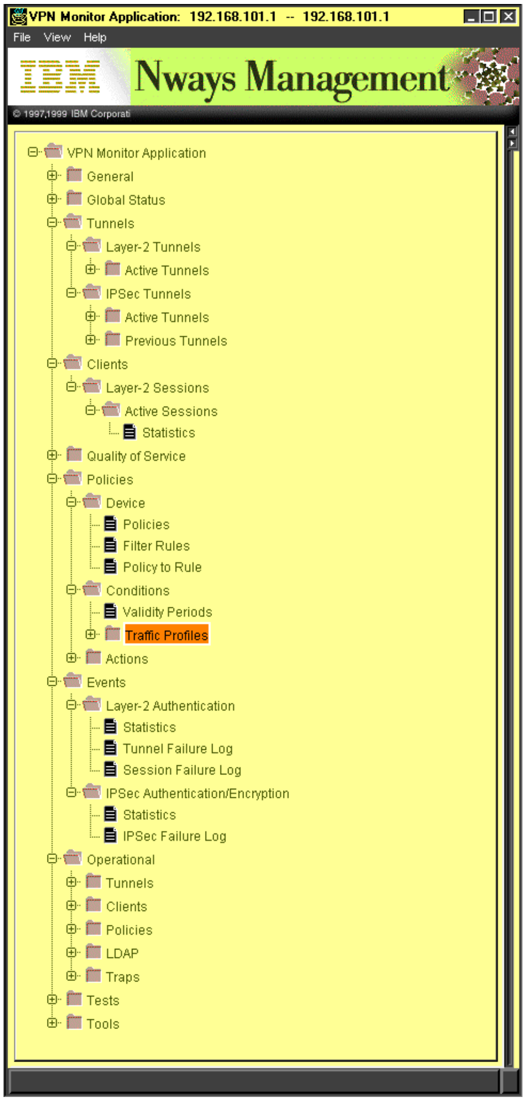


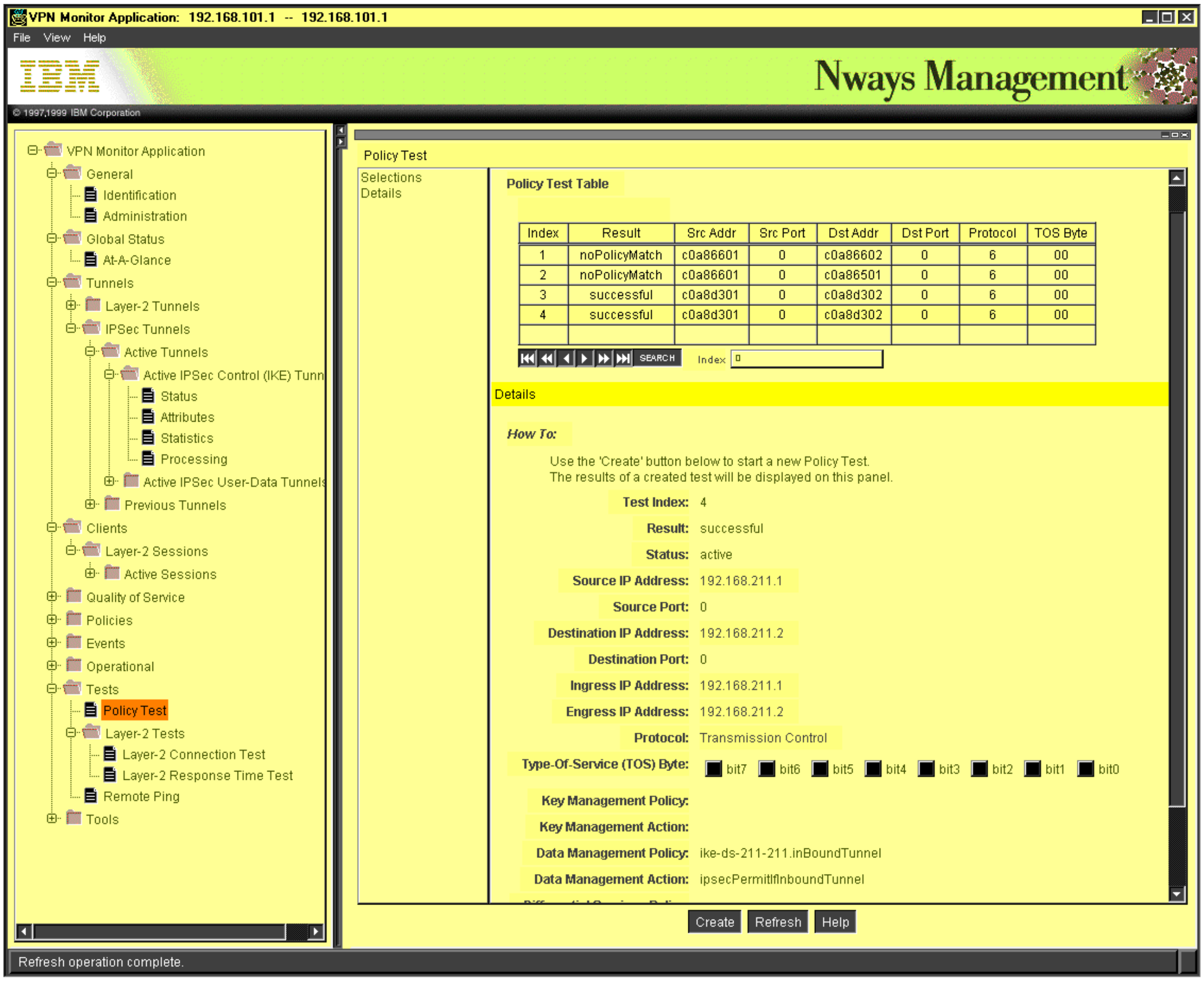
Figure 148. Overview of VPN Monitor Application functions

8.6.4 Policy and session testing

Three IBM-exclusive, patent-pending tests support the network administrator and help desk. The policy test simulates the effect of traffic against router policies. It helps the network administrator validate that policies will perform as expected before they are implemented under live traffic conditions. Two layer-2 tests aid the help desk operator in diagnosing remote access VPN problems by replicating the response time and connectivity conditions that the user experiences when dialing in over layer-2 VPNs.

In the policy test you specify the source and destination of an IP packet. The VPN manager checks whether this packet matches a policy (Figure 149 on page 174).

This command is similar to the router command `test forwarder-query` :



Index	Result	Src Addr	Src Port	Dst Addr	Dst Port	Protocol	TOS Byte
1	noPolicyMatch	c0a86601	0	c0a86602	0	6	00
2	noPolicyMatch	c0a86601	0	c0a86501	0	6	00
3	successful	c0a8d301	0	c0a8d302	0	6	00
4	successful	c0a8d301	0	c0a8d302	0	6	00

Index: 0

How To:

Use the 'Create' button below to start a new Policy Test.
The results of a created test will be displayed on this panel.

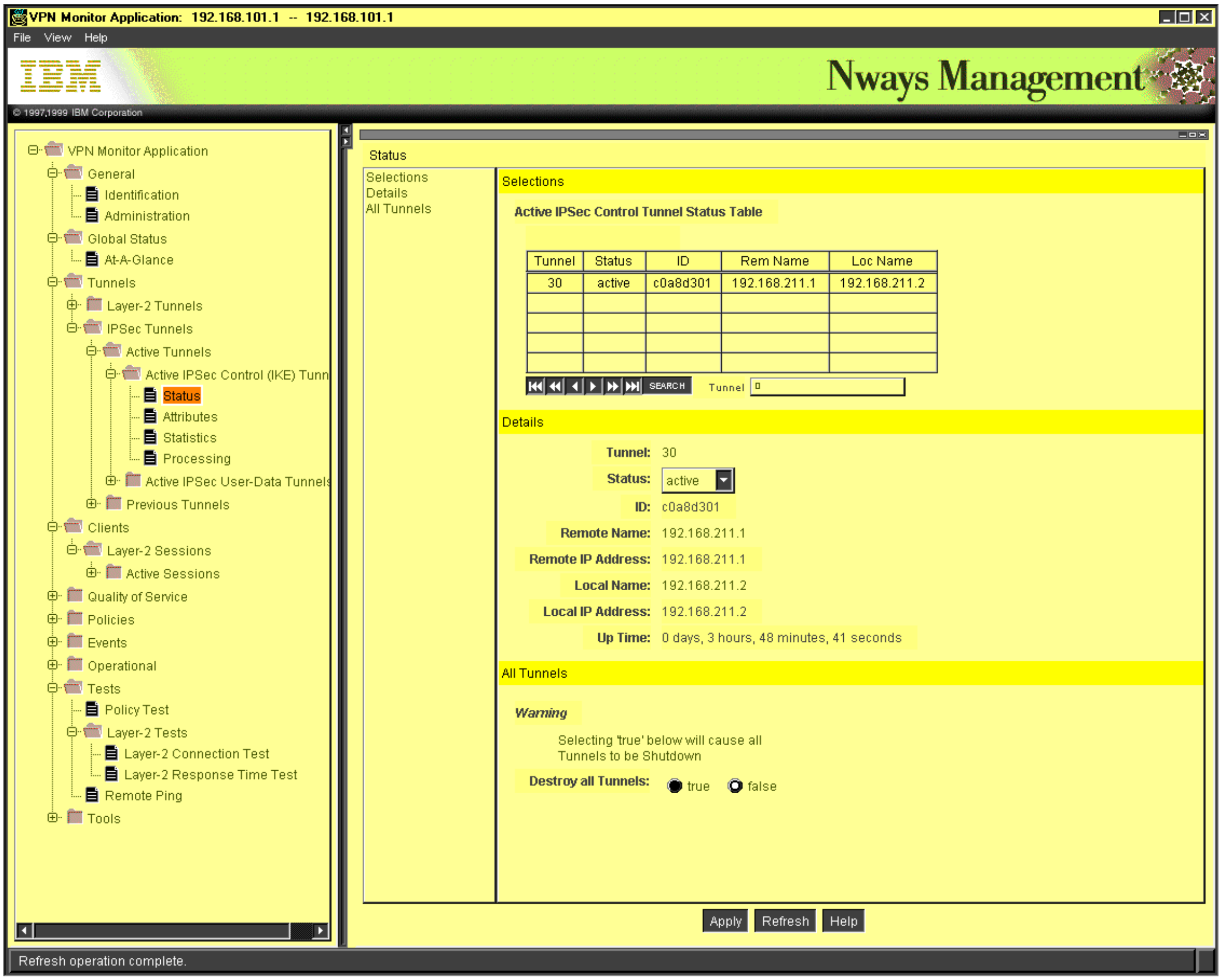
Test Index: 4
Result: successful
Status: active
Source IP Address: 192.168.211.1
Source Port: 0
Destination IP Address: 192.168.211.2
Destination Port: 0
Ingress IP Address: 192.168.211.1
Engress IP Address: 192.168.211.2
Protocol: Transmission Control
Type-Of-Service (TOS) Byte: ■ bit7 ■ bit6 ■ bit5 ■ bit4 ■ bit3 ■ bit2 ■ bit1 ■ bit0
Key Management Policy:
Key Management Action:
Data Management Policy: ike-ds-211-211.inBoundTunnel
Data Management Action: ipsecPermitIfInboundTunnel

Refresh operation complete.

Figure 149. Policy test of the VPN manager

8.6.5 Point-in-time monitoring

The VPN manager supports point-in-time monitoring for VPN tunnels (Figure 150 on page 175), policies (Figure 151 on page 176) and clients. Subnet and wildcard searches and autodiscovery of IBM VPN routers support device as well as tunnel management. Cumulative counters indicate how long a tunnel has been active and represent currently and historically active tunnels. The application also indicates whether Reservation Protocol (RSVP) or DiffServ Quality of Service (QoS) policies are active. Both layer-2 sessions and layer-3 (IP) VPN tunnels are supported, and at the IP layer, the VPN Manager provides status on both the data tunnel and the IKE tunnel.



Selections

Active IPSec Control Tunnel Status Table

Tunnel	Status	ID	Rem Name	Loc Name
30	active	c0a8d301	192.168.211.1	192.168.211.2

Tunnel 0

Details

Tunnel: 30

Status: active

ID: c0a8d301

Remote Name: 192.168.211.1

Remote IP Address: 192.168.211.1

Local Name: 192.168.211.2

Local IP Address: 192.168.211.2

Up Time: 0 days, 3 hours, 48 minutes, 41 seconds

All Tunnels

Warning

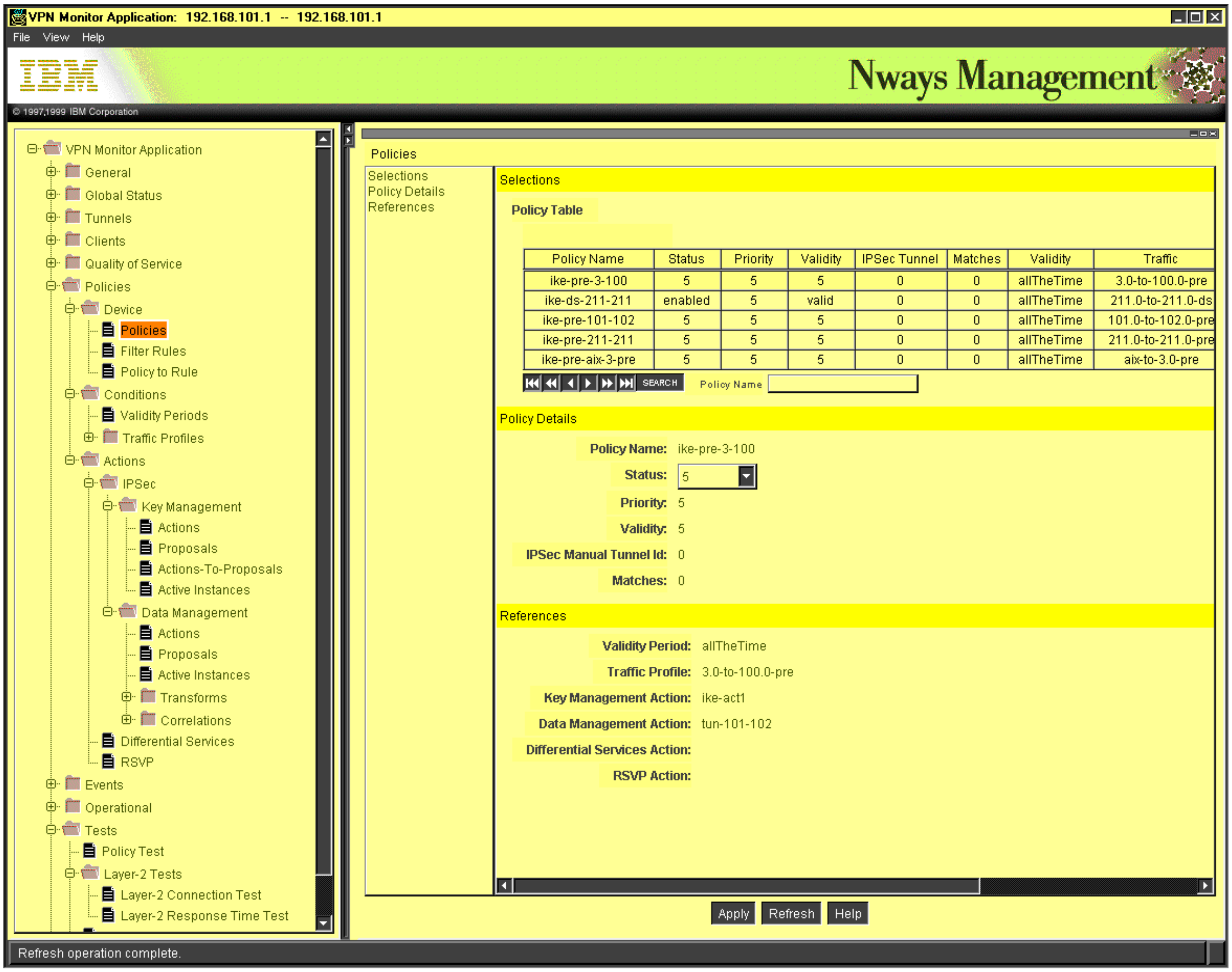
Selecting 'true' below will cause all Tunnels to be Shutdown

Destroy all Tunnels: ● true ○ false

Refresh operation complete.

Figure 150. Monitoring of tunnels

Figure 151 on page 176 shows a screenshot from monitoring policies.



Selections

Policy Table

Policy Name	Status	Priority	Validity	IPSec Tunnel	Matches	Validity	Traffic
ike-pre-3-100	5	5	5	0	0	allTheTime	3.0-to-100.0-pre
ike-ds-211-211	enabled	5	valid	0	0	allTheTime	211.0-to-211.0-ds
ike-pre-101-102	5	5	5	0	0	allTheTime	101.0-to-102.0-pre
ike-pre-211-211	5	5	5	0	0	allTheTime	211.0-to-211.0-pre
ike-pre-aix-3-pre	5	5	5	0	0	allTheTime	aix-to-3.0-pre

Policy Name

Policy Details

Policy Name: ike-pre-3-100
Status: 5
Priority: 5
Validity: 5
IPSec Manual Tunnel Id: 0
Matches: 0

References

Validity Period: allTheTime
Traffic Profile: 3.0-to-100.0-pre
Key Management Action: ike-act1
Data Management Action: tun-101-102
Differential Services Action:
RSVP Action:

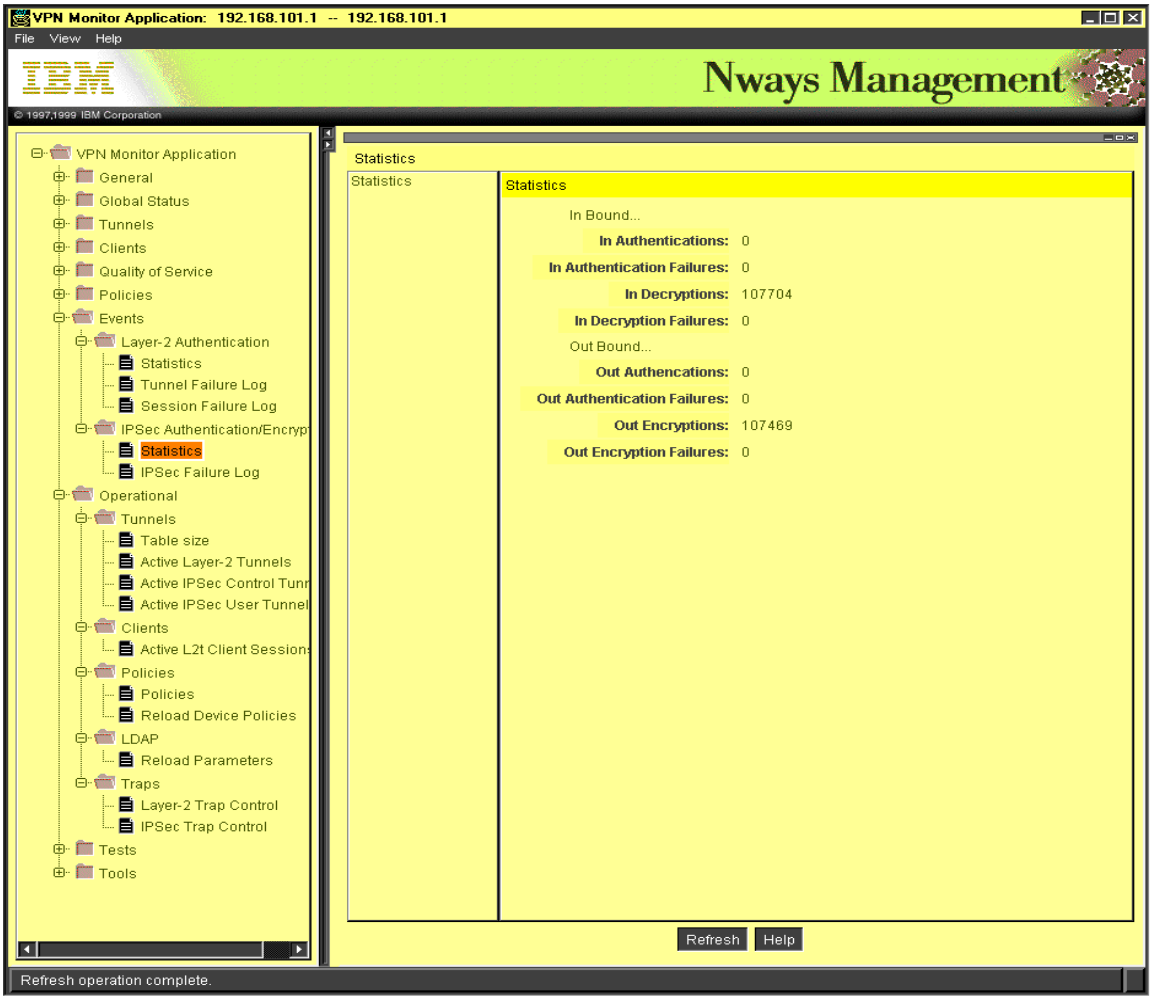
Refresh operation complete.

Figure 151. Monitoring policies

The various monitoring features for policies allow you to monitor their status (enabled/disabled), their priority, the affected tunnel, statistics based on matching policy, etc.

8.6.6 Logging and forwarding of VPN-related events

The Nways VPN Manager is designed to log and forward security-related events to the systems management console (Tivoli NetView or HP OpenView Network Node Manager). Among other notifications, the VPN manager logs and traps tunnel starts, stops, and authentication and decryption failures (Figure 152 on page 177):



In Bound...

In Authentications: 0

In Authentication Failures: 0

In Decryptions: 107704

In Decryption Failures: 0

Out Bound...

Out Authencations: 0

Out Authentication Failures: 0

Out Encryptions: 107469

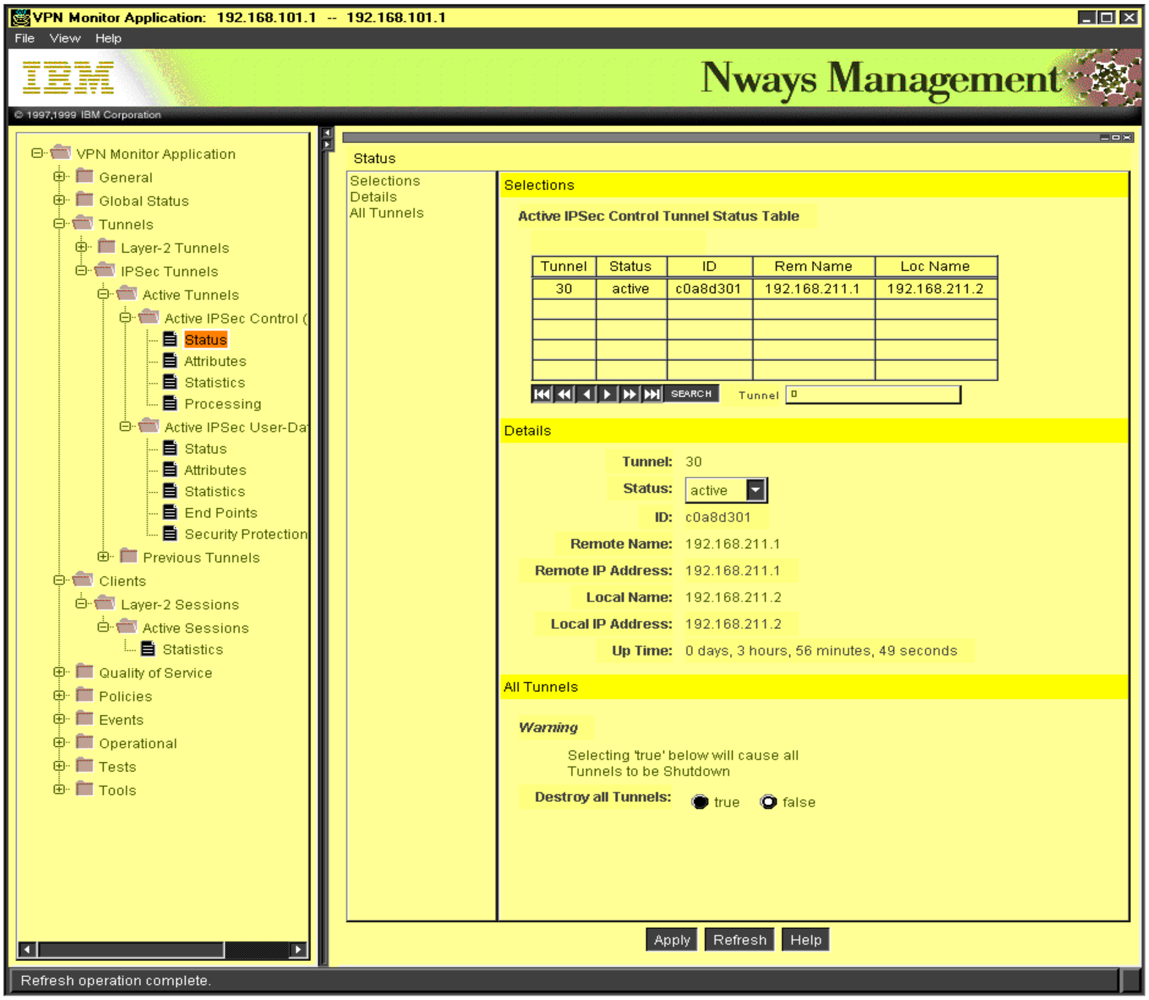
Out Encryption Failures: 0

Refresh operation complete.

Figure 152. Statistics of IPSec authentication/encryption

8.6.7 Operational control to disable a VPN or refresh its policy

The VPN manager is designed to destroy single or multiple VPNs on command if there is a need to discontinue connectivity. It can also prompt routers to refresh their policy from the LDAP server or from the router SRAM if the policy is stored on the router itself. When partnered with the IBM 2210, 2212, 2216 or Network Utility, the Nways VPN Manager supports a managed VPN solution. The VPN manager is supported on AIX, HP-UX and Windows NT. It is fully integrated and compatible with the IBM Nways Manager family of network management products (Figure 153 on page 178):



Selections

Active IPSec Control Tunnel Status Table

Tunnel	Status	ID	Rem Name	Loc Name
30	active	c0a8d301	192.168.211.1	192.168.211.2

Tunnel 0

Details

Tunnel: 30
Status: active
ID: c0a8d301
Remote Name: 192.168.211.1
Remote IP Address: 192.168.211.1
Local Name: 192.168.211.2
Local IP Address: 192.168.211.2
Up Time: 0 days, 3 hours, 56 minutes, 49 seconds

All Tunnels

Warning

Selecting 'true' below will cause all
Tunnels to be Shutdown

Destroy all Tunnels: ● true ○ false

Refresh operation complete.

Figure 153. Shutdown of tunnels

8.6.8 Next phase of VPN management

The next releases of Nways Manager will be even more powerful. They will allow you to configure policies between tunnel endpoints. That means that policies can be defined on the management machine without router definitions.

It will also allow you to generate device definitions for logical policies. These logical policies can be downloaded to the LDAP server.

It will also trigger the load of new policies into devices.

Chapter 9. User authentication for remote access

Remote dial-in to the corporate intranet, as well as to the Internet, has made the Remote Access Server (RAS) a very vital part of today's internetworking services. As mentioned previously, more and more mobile users are requiring access not only to central-site resources but to information sources on the Internet. The widespread use of the Internet and the corporate intranet has fueled the growth of remote access services and devices. There is an increasing demand for a simplified connection to corporate network resources from mobile computing devices such as notebook computers or palm-sized devices.

9.1 Overview

The emergence of remote access has caused significant development work in the area of security. The Authentication, Authorization and Accounting (AAA) security model has been developed to address the issues of remote access security. AAA answers the questions who, what, and when, respectively. A brief description of each of the three As in the AAA security model is presented below:

Authentication

This is the action of determining who a user (or entity) is. Authentication can take many forms. Traditional authentication utilizes a name and a fixed password. Most computers work this way. However, fixed passwords have limitations, mainly in the area of security. Many modern authentication mechanisms utilize one-time passwords or a challenge-response query. Authentication generally takes place when the user first logs on to a machine or requests a service from it.

Authorization

This is the action of determining what a user is allowed to do. Generally authentication precedes authorization, but again, this is not required. An authorization request may indicate that the user is not authenticated, that we do not know who he or she is. In this case it is up to the authorization agent to determine if an unauthenticated user is allowed the services in question. In current remote authentication protocols authorization does not merely provide yes or no answers, but it may also customize the service for the particular user.

Accounting

This is typically the third action after authentication and authorization. But again, neither authentication nor authorization is required. Accounting is the action of recording what a user is doing, and when he or she has done it.

In the distributed client/server security database model, a number of communication servers, or clients, authenticate a dial-in user's identity through a single, central database, or authentication server. The authentication server stores all the information about users, their passwords and access privileges. Distributed security provides a central location for authentication data that is more secure than scattering the user information on different devices throughout a network. A single authentication server can support hundreds of communication servers, serving up to tens of thousand of users. Communication servers can access an authentication server locally or remotely over WAN connections.

Several remote access vendors and the Internet Engineering Task Force (IETF) have been in the forefront of this remote access security effort, and the means whereby such security measures are standardized. The Remote Authentication Dial-In User Service (RADIUS) and the Terminal Access Controller Access Control System (TACACS) are two such cooperative ventures that have evolved out of the Internet standardizing body and remote access vendors.

Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a distributed security system developed by Livingston Enterprises. RADIUS was designed based on a previous recommendation from the IETF's Network Access Server Working Requirements Group. An IETF Working Group for RADIUS was formed in January 1996 to address the standardization of the RADIUS protocol; RADIUS is now an IETF-recognized dial-in security solution (RFC 2058 and RFC 2138).

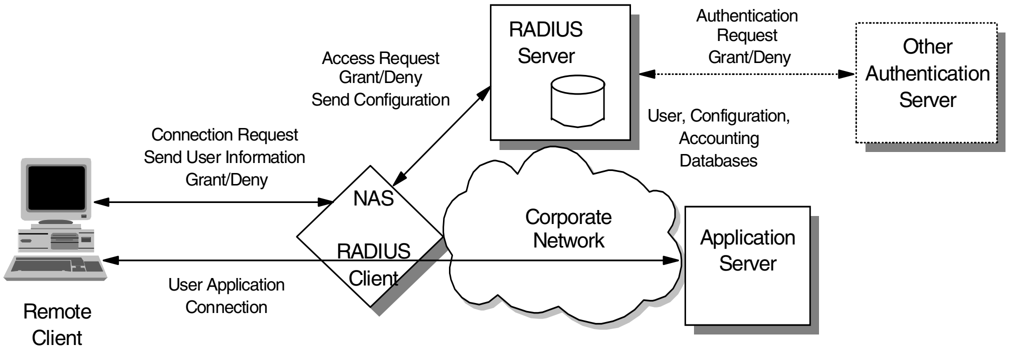

RADIUS Server
Authentication Request Grant/Deny
Other Authentication Server
Access Request Grant/Deny Send Configuration
User, Configuration, Accounting Databases
Connection Request Send User Information Grant/Deny
NAS
RADIUS Client
Corporate Network
Application Server
User Application Connection
Remote Client

Figure 154. RADIUS

Terminal Access Controller Access Control System (TACACS)

Similar to RADIUS, Terminal Access Controller Access Control System (TACACS) is an industry standard protocol specification, RFC 1492. Similar to RADIUS, TACACS receives authentication requests from a network access server (NAS) client and forwards the user name and password information to a centralized security server. The centralized server can be either a TACACS database or an external security database. Extended TACACS (XTACACS) is a version of TACACS with extensions that Cisco added to the basic TACACS protocol to support advanced features. TACACS+ is another Cisco extension that allows a separate access server (the TACACS+ server) to provide independent authentication, authorization, and accounting services.

9.2 RADIUS operation

RADIUS was originally developed by Livingston Enterprises but is now in the domain of the IETF and is an open protocol and a reference implementation distributed in source code format that can be modified by anyone. Any client that supports the RADIUS client protocol can talk to the corresponding RADIUS server.

Although RADIUS was originally developed for the administration of NAS products support was recently added for further devices/applications such as firewalls, access to individual Web pages, e-mail accounts and other authentication-related Internet security situations.

RADIUS consists of two parts: There is the RADIUS client, for example, the NAS or any other software like a firewall, that sends an AAA request to the RADIUS server. On the other hand there is the RADIUS server, which checks the request according to preconfigured data. The RADIUS standard specifies the format and traffic flow of the packets between theses devices that provides AAA services.

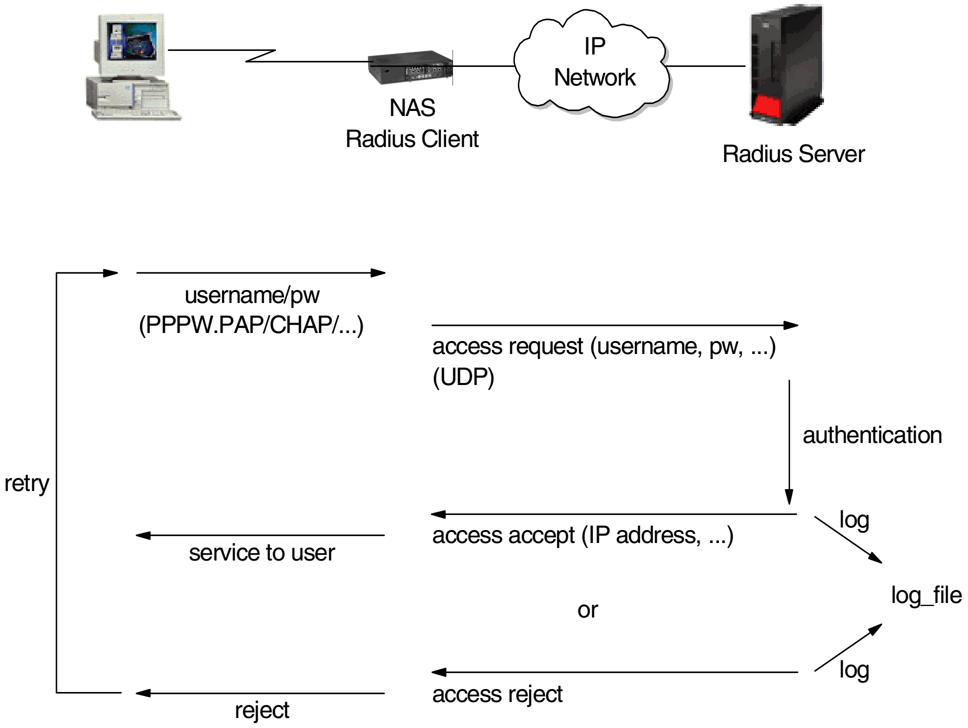


Figure 155. Traffic flow in RADIUS

Although RADIUS and TACACS authentication servers can be set up in a variety of ways, depending upon the security scheme of the network they are serving, the basic process for authenticating a user is essentially the same. Using a modem, a remote dial-in user connects to a remote access server (also called the network access server or NAS), with a built-in analog or digital modem. Once the modem connection is made, the NAS prompts the user for a name and password. The NAS then creates the so-called authentication request from the supplied data packet, which consists of information identifying the specific NAS device sending the authentication request, the port that is being used for the modem connection, and the user name and password.

A very important role is done by the authentication server, which is a server in the network that validates user IDs and passwords for the network. If a device is configured for authentication through an authentication server and the device receives a packet from an authentication protocol, the device passes a user ID and password to the server for authentication.

If the user ID and password are correct, the server responds positively. The device can then communicate with the originator of the request. If the server does not find the user ID and password that it receives from the device, it responds negatively to the device. The device then rejects the session from which it got the authentication request.

The authentication server can be the RADIUS server itself or a different server based on other central authentication technologies such as Kerberos, DCE, SecureID (by Security Dynamics) or RACF. A RADIUS server can be configured to forward authentication requests to such a central authentication server and pass access or deny information and configuration back to the client.

For protection against eavesdropping by hackers, the NAS, acting as the RADIUS or TACACS client, encrypts the password before it sends it to the authentication server. If the primary security server cannot be reached, the security client or NAS device can route the request to an alternate server. When an authentication request is received, the authentication server validates the request and then decrypts the data packet to access the user name and password information. If the user name and password are correct, the server sends an authentication acknowledgment packet. This acknowledgment packet may include additional filters, such as information on the user's network resource requirements and authorization levels. The security server may, for instance, inform the NAS that a user needs TCP/IP and/or Internet Packet Exchange (IPX) using PPP, or that the user needs SLIP to connect to the network. It may include information on the specific network resource that the user is allowed to access.

To circumvent snooping on the network, the security server sends an authentication key, or signature, identifying itself to the security client. Once the NAS receives this information, it enables the necessary configuration to allow the user the necessary access rights to network services and resources. If at any point in this log-in process all necessary authentication conditions are not met, the security database server sends an authentication reject message to the NAS device and the user is denied access to the network.

9.2.1 Using RADIUS with layer-2 tunnels

RADIUS can be used to authenticate layer-2 tunnels as well as PPP connections which is important for VPNs. There are two models of layer-2 tunnels, voluntary and compulsory. RADIUS can be used in both cases to authenticate a user and grant or deny a tunnel setup or session establishment. This adds one layer of security to the layer-2 VPN scenario because unless the tunnel is up and the session established, no traffic can flow over the tunnel, and authentication and access to those tunnels can be centrally controlled.

Figure 156 on page 183 illustrates yet another way of using RADIUS in a VPN environment where compulsory tunnels are used that involve an ISP to establish a tunnel or start a new session over an existing tunnel on behalf of a remote client. The ISP can use a RADIUS proxy server to forward client authentication back to the corporate authentication server so that there is no need to maintain user information at two locations, the ISP and the corporate server.

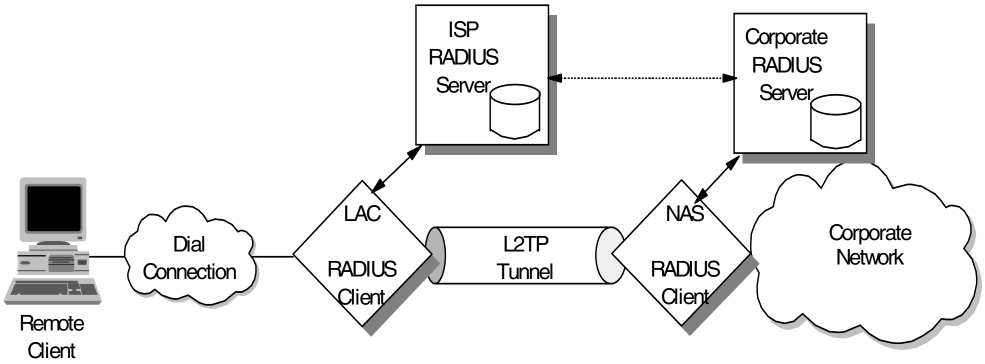


Figure 156. Using RADIUS with layer-2 tunnels

9.3 Support on IBM routers

The IBM Nways routers support RADIUS, TACACS and TACACs+. In this documentation we will concentrate on RADIUS, as it provides many more attributes and allows for vendor-specific attributes.

We will show here only an overview and the first basic steps. Details can be found in *Nways Multiprotocol Routing Services Software User's Guide* SC30-3681.

Authentication can be configured locally or can be configured to consolidate user configuration using authentication servers that are available on the network to service authentication requests for the entire network. The IBM Nways routers implement locally maintained authentication as well as authentication using RADIUS, TACACS and TACACS+.

9.3.0.1 Using AAA

Authentication, Authorization, and Accounting (AAA) security are configurable protocols that allow you to control access to your services. You can configure AAA to perform for local or remote authentication.

You can configure a security protocol for three types of functions:

- PPP links
- Login users (Telnet/Console Login)
- Tunnels

The configuring is done by setting a primary and secondary server. The server information is configured and stored separately from the AAA configuration. You use a server profile by a name that is provided at configuration time.

Under all circumstances accounting cannot be done locally and must be either Radius or TACACS+ based. Authorization can only be done locally, or through remote authentication that uses Radius or TACACS+.

The following are valid PPP security protocols on the Nways routers:

Authentication methods
Local, RADIUS, TACACS+, TACACS

Authorization methods
Local, RADIUS, TACACS+

Accounting methods
RADIUS, TACACS+

9.3.0.2 Predefined on router

By design, the local list attributes are the attributes defined to be supported on the box. Depending on the type of user, PPP, Tunneled, or Admin differing attributes will apply.

For PPP the LocalList authentication protocol will read the profiles of users added to the system through the ADD PPP-USER command.

9.3.0.3 Remote authentication

Remote authentication servers that perform AAA functions are supported by common code implementations since CC3. CC2 did provide simple remote authentication support for PPP.

Remote authentication includes the use of RADIUS, TACACS and TACACS+. Authorization and accounting are provided by RADIUS and TACACS+.

- PPP, layer-2 tunnels and console login can use AAA functionality
- In addition IPSec tunnels can also use accounting

The Nways RADIUS client implementation is based on RFC 2138 and 2139.

9.3.1 Description of the IBM Nways implementation of RADIUS

A RADIUS client submits an access request to the RADIUS server and expects a response, either an access accept or access reject.

Standard RADIUS will reply with authorization attributes during an authentication request (access request), but because the IBM model of AAA treats each A-function separately we submit an authentication request simply to validate the user name and password, then submit another access request to obtain the attributes. However, it is possible to configure the RADIUS client to submit only the one authentication request and accept the attributes that come during that transaction, which is referred to as authorize at authentication. When authorizing at authentication, care must be taken to ensure that both authentication and authorization are configured for the same RADIUS server profile and authorize at authentication is set to yes.

9.3.2 Description of the test environment

We had the following environment (Figure 157 on page 185):

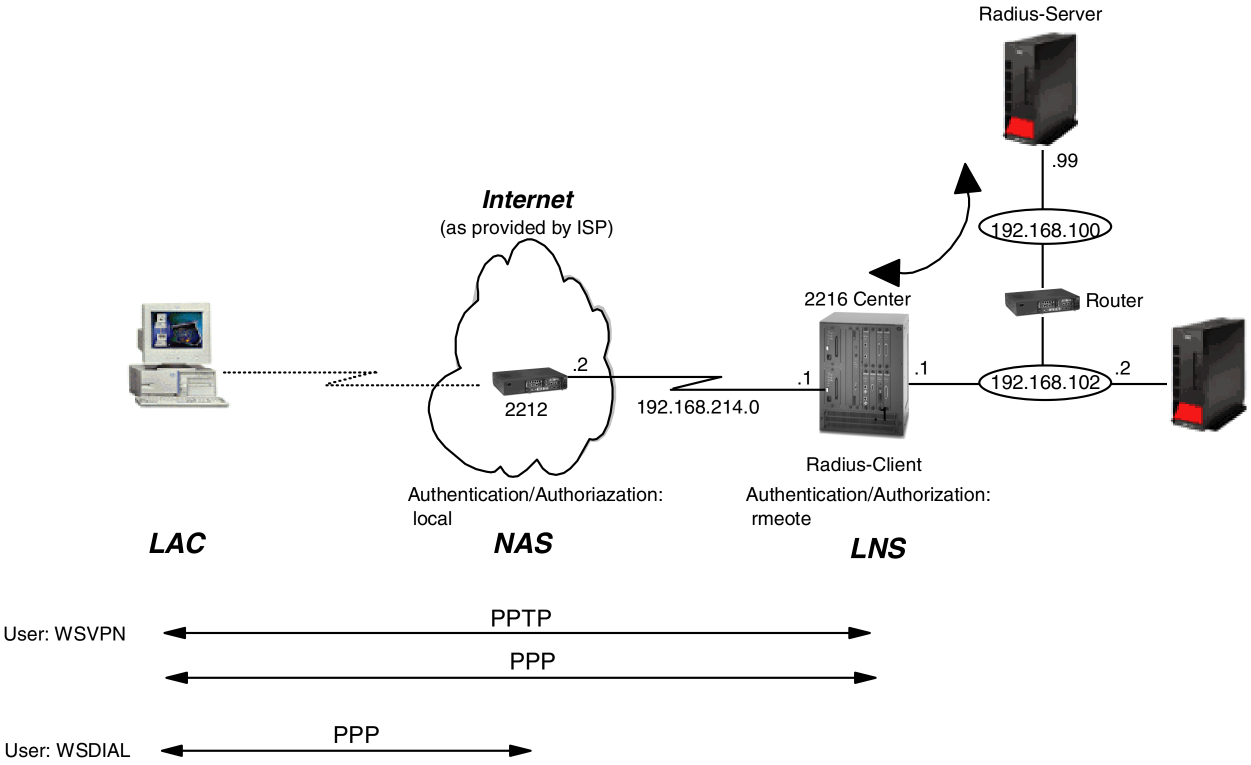


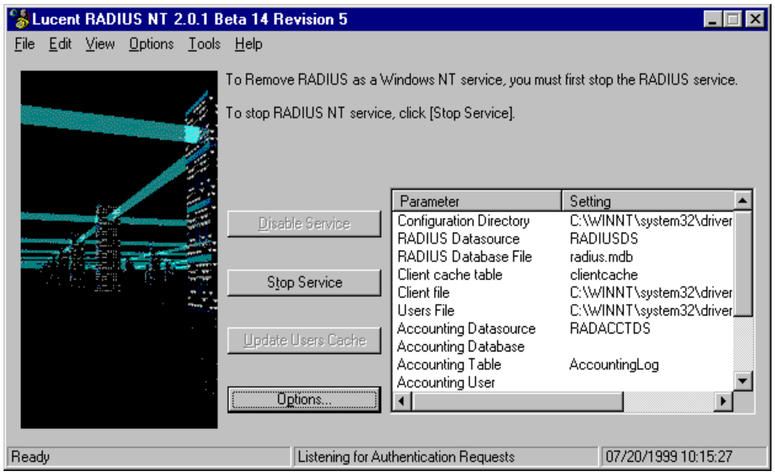
Figure 157. Scenario for using the RADIUS server

We have a remote PC that works as the LAC. The PC does a PPP connection to the NAS; afterward it tries to get an authorization from the LNS. This authorization is done by a RADIUS server. If authorization is given a PPTP connection is built between the PC (LAC) and the router in the center (LNS).

In this case the RADIUS client is the IBM 2216. The RADIUS server is a Windows NT-based Lucent installation.

9.3.3 Configuration of RADIUS server

In our test environment we used a Windows NT-based RADIUS installation from Lucent (Lucent Radius NT Service Version 2.01). It has a GUI that allows you to do all necessary customizing steps (Figure 158 on page 186):



Lucent RADIUS NT 2.0.1 Beta 14 Revision 5
File Edit View Options Tools Help
Disable Service
Stop Service
Update Users Cache
Options...

To Remove RADIUS as a Windows NT service, you must first stop the RADIUS service.

To stop RADIUS NT service, click [Stop Service].

Parameter	Setting
Configuration Directory	C:\WINNT\system32\driver
RADIUS Datasource	RADIUSDS
RADIUS Database File	radius.mdb
Client cache table	clientcache
Client file	C:\WINNT\system32\driver
Users File	C:\WINNT\system32\driver
Accounting Datasource	RADACCTDS
Accounting Database	
Accounting Table	AccountingLog
Accounting User	

Ready | Listening for Authentication Requests | 07/20/1999 10:15:27

Figure 158. RADIUS-GUI (Lucent)

9.3.3.1 RADIUS file structure

The Lucent RADIUS software is organized in a hierarchical file structure. All files and directories are in the RADIUS database raddb (see Figure 159).

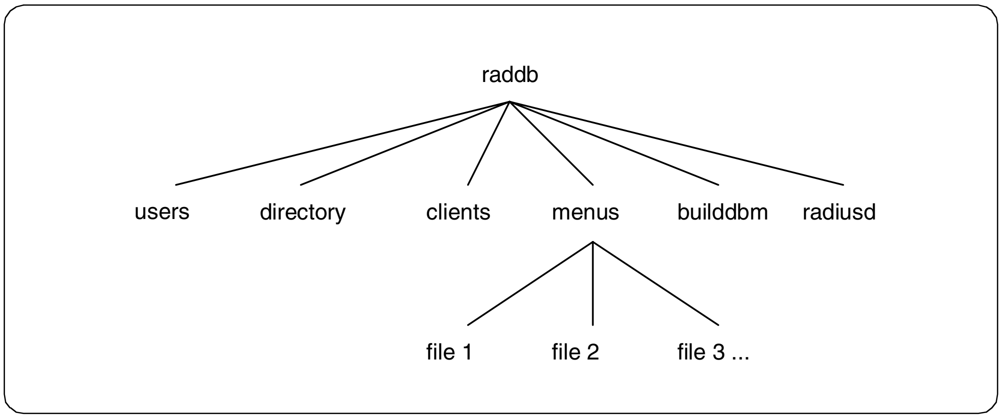


Figure 159. File structure of the RADIUS database raddb

For a simple configuration as we used it we only have to modify the users file and the clients file.

9.3.3.2 Users file

The users file is in the raddb directory of the RADIUS server and it contains the user profiles with security and configuration information for each user. It is a simple text file.

When a user logs in to the NAS with a user name and password the users file in the RADIUS server will be parsed top-down to find a matching entry for the user. If a match is found, the user will be authenticated. If no match is found, the RADIUS server tries to match the user with the DEFAULT profile which is defined at the end of the users file.

In our case we defined the following user in the users file (see Figure 160):

```
#----------------------------------------------------------------------------
#
# @(#)users1.1 2/28/96  Copyright 1991 Livingston Enterprises Inc
#
#----------------------------------------------------------------------------
#
#    This file contains security and configuration information for
#    each user.  The first field is the user's name and can be up to
#    8 characters in length.  This is followed (on the same line)
#    with the list of authentication requirements for that user.
#    This can include password, comm server name, comm server port
#    number, and an expiration date of the user's password.  When an
#    authentication request is received from the comm server, these
#    values are tested.  Special users named "DEFAULT", "DEFAULT2",
#    "DEFAULT3" can be created (and should be placed at the end of
#    the user file) to specify what to do with users not contained
#    in the user file.
#
#    Indented (with the tab character) lines following the first
#    line indicate the configuration values to be passed back to
#    the comm server to allow the initiation of a user session.
#    This can include things like the PPP configuration values
#    or the host to log the user onto.
#
#    Delete or comment out these examples before using this file!

wsvpn    Password = "wsvpn", Expiration = "Dec 24 1999"
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 192.168.102.11,
         Framed-Routing = None,
         Filter-Id = "std.ppp",
         Framed-MTU = 1500,
         Framed-Compression = Van-Jacobson-TCP-IP
```

Figure 160. Users file of the RADIUS database

You can use an existing user from the sample file and modify it. The user name, password and IP address are important.

9.3.3.3 Clients file

The clients file is a text file that contains the names and passwords of the RADIUS clients. The clients file will be used to check an authentication request from the NAS. The passwords given by the NAS and the passwords defined in the clients file are the base for the handshaking between the RADIUS client and the RADIUS server.

In our case we had the following clients file (Figure 161 on page 188):

```
#---------------------------------------------------------------------------
#
# @(#)clients2.0.1 2/15/98  Copyright 1998 Livingston Enterprises Inc
#
#---------------------------------------------------------------------------
#
#This file contains a list of clients which are allowed to
#make authentication requests and their encryption key.
#The first field is a valid hostname.
#The second field (separated by blanks or tabs) is the
#encryption key.
#
#Client Name      Key
#-------------    ----------------------
#portmaster1      testing123
localhost         secret
center            secret
mmradius          secret
```

Figure 161. Clients file of the RADIUS database

9.3.3.4 RADIUS authentication test utility

The RADIUS installation also comprises a test utility to test the authentication requests (Figure 163 on page 189):

It enables you to test RADIUS authentication request packets and to verify that authentication is working and it helps you to troubleshoot some user problems. Doing the following steps you can test whether the RADIUS server can successfully authenticate a user:

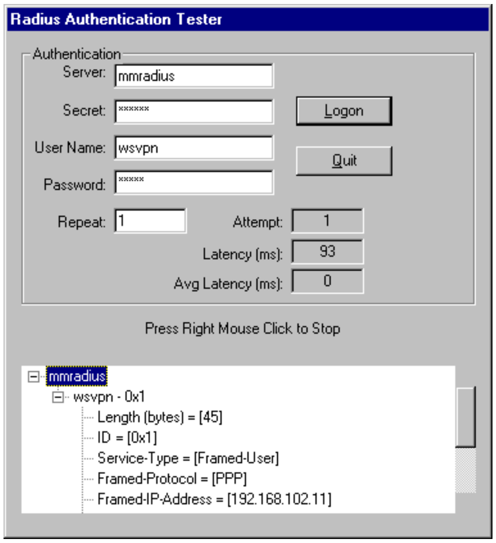
- Start the authentication test utility in the GUI from Tools (Figure 158 on page 186).
- Provide values for server/secret and for user name/password. You can also specify the number of cycles.
  If you do not want to use the name `localhost` as the RADIUS server you can also use different names, but make sure that this IP host name can be properly resolved. We used in the example the name `mmradius` of the RADIUS server. Therefore, we defined `mmradius` in the IP hosts file (in Windows NT this is normally C:\WINNT\system32\drivers\etc\hosts). You see also in this file that `localhost` is defined with the loopback address - see Figure 162 on page 189.
- Click **Logon** to the authentication.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
#
# The following entry was created by NetView based on Registry information.
#
192.168.100.99      mmradius       mmradius.itso.ral.ibm.com
192.168.102.1       center         center.itso.ral.ibm.com
```

Figure 162. Hosts file in the RADIUS server (in Windows NT normally C:\WINNT\system32\drivers\etc\hosts)

The authentication test utility sends an authentication request packet to the RADIUS server. It receives the response from the RADIUS server (which in our case is the same machine) and it measures the latency of the authentication response for each test packet. It also gives us the average latency over the set of test packets. The attributes are parsed and displayed in the browser below the test fields.

The tool is especially useful if you test user names that are causing problems.



Server: mmradius
Secret: ******
User Name: wsvpn
Password: *****
Repeat: 1
Attempt: 1
Latency (ms): 93
Avg Latency (ms): 0

```
⊟ mmradius
   ⊟ wsvpn - 0x1
      Length (bytes) = [45]
      ID = [0x1]
      Service-Type = [Framed-User]
      Framed-Protocol = [PPP]
      Framed-IP-Address = [192.168.102.11]
```

Figure 163. RADIUS authentication test utility (Lucent)

9.3.3.5 Stop and start service

After modifying the file of the RADIUS database you should stop the RADIUS server and start it again.

9.3.4 Configuration of Nways 221x-Client

If you do not work with locally defined authentication on the Nways router but with remote authentication with RADIUS you have to perform the following steps:

- Enter the AAA mode.
- Define RADIUS server on the Nways RADIUS client.
- Quickset of the AAA definitions.
- Verify router definitions.

9.3.4.1 Enter AAA mode

You enter the AAA mode with the command `feature auth`:

```
Center Config>
Center Config>FEATURE AUTH
AAA Configuration
Center AAA Config>
```

Figure 164. Enter AAA mode on the Nways router

9.3.4.2 Defining the RADIUS server on the Nways RADIUS client

The command `servers add` allows you to define the remote RADIUS server on the Nways router.

```
Center AAA Config>
Center AAA Config> SERVERS ADD
Enter server id:  []? mmradius
Server profile does not currently exist.
Creating new one.
Server Type:  (RADIUS, TACACSPLUS, TACACS): [RADIUS]
Authorize at Authentication?  (Yes, No): [Yes]
Enter primary:  [0.0.0.0]? 192.168.100.99
Enter secondary:  [0.0.0.0]?
Request tries [1-100]:  [3]? 5
Request interval (sec) [1-60]:  [3]?
Set server secret?  (Yes, No): [No] yes
Set key to default?  (Yes, No): [No]
Password: secret
to verify Enter password again: secret
Center AAA Config>
```

Figure 165. Defining the RADIUS server on the Nways RADIUS client

We gave the RADIUS server the same name as on the RADIUS server itself. Actually this is not necessary and you can use different names. The RADIUS server name is used only on the client side to distinguish between different RADIUS servers.

Note that the server secret/password does not appear on the screen, it was only added here in the book.

9.3.4.3 Quickset of the AAA definitions

```
Center AAA Config> QUICKSET
Configure for what type of AAA services? (LOCAL, REMOTE, BOTH, quit): [LOCAL] remote
What type of remote servers do you want to configure? (RADIUS,
    TACACSPLUS, TACACS, many, quit): [RADIUS]
Add server information now? (Yes, No): [Yes] n
Configure AAA for PPP? (LOCAL, REMOTE, quit): [REMOTE]
Specify the server...
Enter server id:  []? mmradius
Assigning authentication ppp protocol: mmradius
Assigning authorization ppp protocol: mmradius
Assigning accounting ppp protocol: mmradius
Disable accounting for PPP? (Yes, No): [No] yes
accounting ppp disabled
Configure AAA for Tunnels? (LOCAL, REMOTE, quit): [REMOTE]
Specify the server...
Enter server id:  []? mmradius
Assigning authentication tunnel protocol: mmradius
Assigning authorization tunnel protocol: mmradius
Assigning accounting tunnel protocol: mmradius
Disable accounting for TUNNELs? (Yes, No): [No] y
accounting tunnel disabled
Configure AAA for Login? (LOCAL, REMOTE, quit): [REMOTE] local
Assigning authentication login protocol: locallist
Assigning authorization login protocol: locallist
accounting login disabled
AAA Configuration...

ppp authentication          : Radius        mmradius
ppp authorization           : Radius        mmradius
ppp accounting              : Disabled
tunnel authentication       : Radius        mmradius
tunnel authorization        : Radius        mmradius
tunnel accounting           : Disabled
login authentication        : locallist
login authorization         : locallist
login accounting            : Disabled
Center AAA Config>
```

Figure 166. Quickset command for configuring AAA on the router

We did not add a RADIUS server with `quickset` because we had already added it before with the command `servers add`. You see the three blocks of functions: PPP, Tunnel and Login. As we are using PPP only these parameters are relevant for our environment.

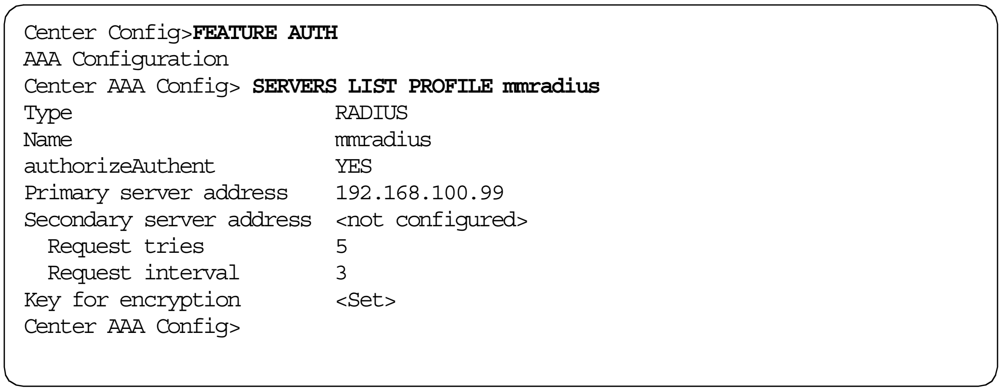
9.3.4.4 Verify definitions on Nways RADIUS client

List RADIUS server profile

The command `SERVERS LIST PROFILE mmradius` gives you important definitions of the RADIUS server.

Authentication and authorization can be done in two steps: Authentication is normally done first: The RADIUS server gives back the request accept and also the IP address, which is not used by the client at that moment. In the authorization phase the client requests the IP address from the server.

The parameter `authorizeAuthent=YES` means that authentication and authorization are done together in one step instead of two steps as described before.

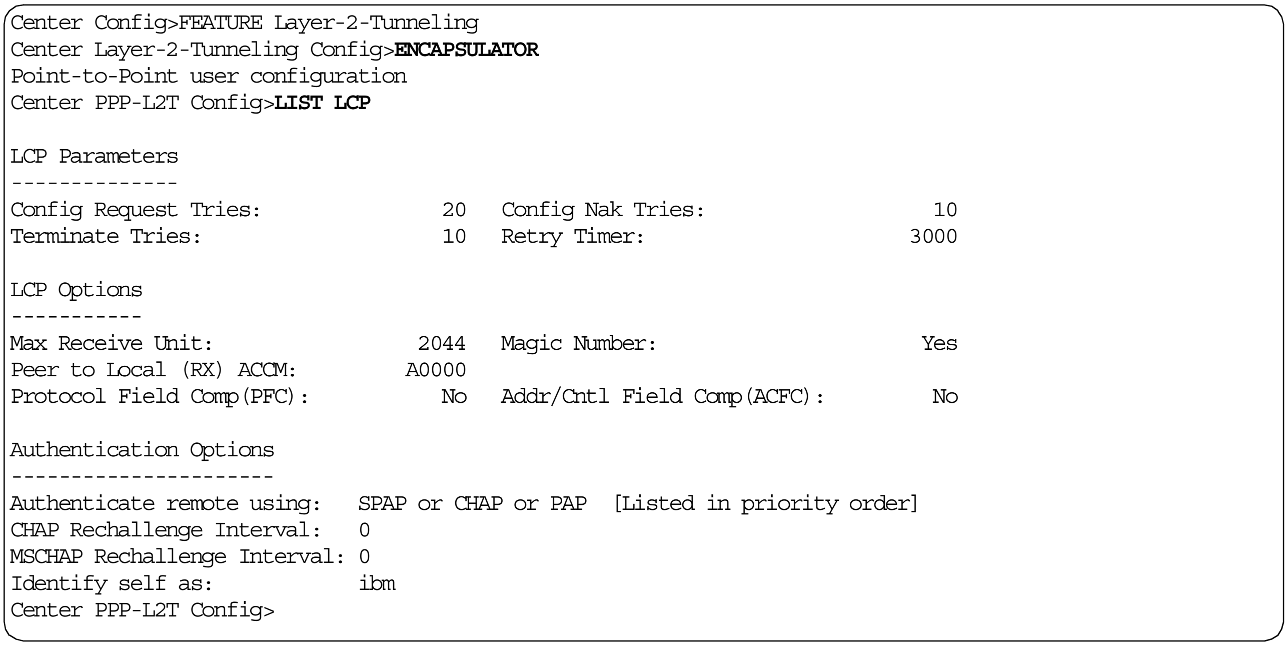


```
Center Config>FEATURE AUTH
AAA Configuration
Center AAA Config> SERVERS LIST PROFILE mmradius
Type                       RADIUS
Name                       mmradius
authorizeAuthent           YES
Primary server address     192.168.100.99
Secondary server address   <not configured>
  Request tries            5
  Request interval         3
Key for encryption         <Set>
Center AAA Config>
```

Figure 167. List profile of RADIUS server

List lcp

The current authentication definitions can be checked with the command `list lcp` (Figure 168 on page 192):



```
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>LIST LCP

LCP Parameters
--------------
Config Request Tries:             20   Config Nak Tries:                 10
Terminate Tries:                  10   Retry Timer:                    3000

LCP Options
-----------
Max Receive Unit:               2044   Magic Number:                    Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):         No   Addr/Cntl Field Comp(ACFC):       No

Authentication Options
----------------------
Authenticate remote using:   SPAP or CHAP or PAP  [Listed in priority order]
CHAP Rechallenge Interval:   0
MSCHAP Rechallenge Interval: 0
Identify self as:            ibm
Center PPP-L2T Config>
```

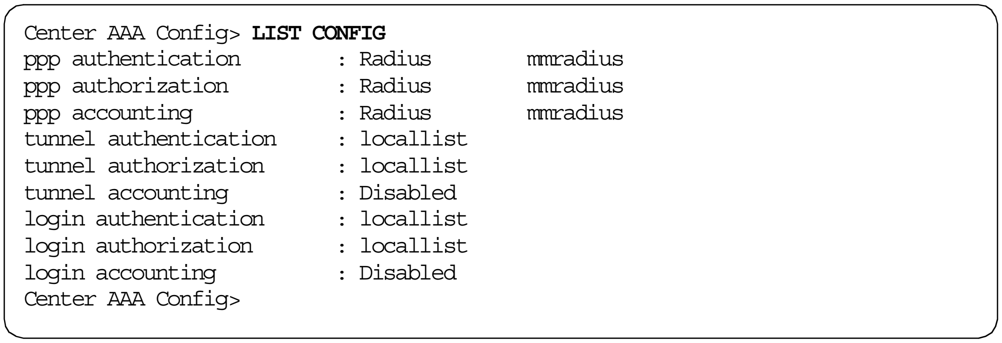
Figure 168. List LCP command after disable mschap

Note

It is very important to remember that MSCHAP is not enabled because the Nways router do not support MSCHAP together with a RADIUS server. Therefore, check whether MSCHAP is enabled (`list lcp`) and disable it if necessary. The command `enable mschap` prompts you if you want to disable it.

List Config

You get an overview of the defined parameters with the command `list config` (Figure 169 on page 193):



```
Center AAA Config> LIST CONFIG
ppp authentication        : Radius        mmradius
ppp authorization         : Radius        mmradius
ppp accounting            : Radius        mmradius
tunnel authentication     : locallist
tunnel authorization      : locallist
tunnel accounting         : Disabled
login authentication      : locallist
login authorization       : locallist
login accounting          : Disabled
Center AAA Config>
```

Figure 169. List Config

9.3.5 Monitoring and troubleshooting

In the following section we describe how you can monitor the operation of the router and the RADIUS server and what you can do if it fails.

9.3.5.1 On the RADIUS server

In case of problems, perform the following on the RADIUS server:

Stop and restart RADIUS server

After changing the configurations file on the RADIUS server you should stop and restart the RADIUS server (9.3.3.5, “Stop and start service” on page 190).

RADIUS authentication test utility

There is a special authentication test utility which is especially useful to troubleshoot user problems; see 9.3.3.4, “RADIUS authentication test utility” on page 188.

9.3.5.2 On the Nways router

In case of problems, perform the following on the router:

Check MSCHAP

The current status of the authentication option to the server can be checked with the command `list lcp` (Figure 170 on page 194).

Note

MSCHAP is not supported for authentication to the RADIUS server.

Therefore, check whether MSCHAP is enabled (`list lcp`) and disable it if necessary. The command `enable mschap` prompts you if you want to disable it.

List lcp

```
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>LIST LCP

LCP Parameters
--------------
Config Request Tries:              20   Config Nak Tries:               10
Terminate Tries:                   10   Retry Timer:                  3000

LCP Options
-----------
Max Receive Unit:                2044   Magic Number:                  Yes
Peer to Local (RX) ACCM:        A0000
Protocol Field Comp(PFC):          No   Addr/Cntl Field Comp(ACFC):     No

Authentication Options
----------------------
Authenticate remote using:   MSCHAP or SPAP or CHAP or PAP  [Listed in priority
order]
CHAP Rechallenge Interval:   0
```

Figure 170. List lcp command before disable mschap

Disable mschap

You can disable mschap with the command `mschap`. The Nways router reminds you automatically that MSCHAP is not supported and suggests to disable MSCHAP (Figure 171 on page 194):

```
Center PPP-L2T Config>ENABLE MSCHAP

WARNING: MSCHAP does not support authentication with
the currently configured authentication server.
For users to be correctly authenticated with MSCHAP,
the Local List database must be used for authentication

Do you want to continue enabling MSCHAP ? (Yes, No): [No] n
MSCHAP disabled
Center PPP-L2T Config>
```

Figure 171. Disable mschap

The configuration can be checked again with the command `list lcp`.

Set Internal IP address on router

Depending on the RADIUS server implementation the internal IP address of the client is used as identification. Therefore, ensure that this address is set. It can be set with the command `set internal-ip-address` (Figure 172 on page 194):

```
Center IP config>SET INTERNAL-IP-ADDRESS
Internal IP address [172.16.220.253]? 192.168.211.1
Center IP config>EXIT
```

Figure 172. Setting the internal IP address on a router

Display AAA subsystem

There is a subsystem of its own for AAA on the Nways router. You can enable it with the command `display subsystem AAA all`.

Chapter 10. Connecting the data center to the branch office

As discussed in 1.5, “Common VPN scenarios” on page 15, one application of VPNs is in connecting branch office intranets to a central site (perhaps a mainframe data center) using a non-secured public network such as the Internet. In this section of the redbook, we provide step-by-step procedures for implementing such a scenario using the IPSec feature of the IBM Nways 2210/2216 routers.

In this chapter, we configure a secure tunnel to establish basic TCP/IP connectivity between the branch office intranet and the central intranet located in the corporate data center.

The current chapter relies heavily on the preceding Chapter 6, “Configuring IPSec and IKE with IBM Nways routers” on page 89 where we showed the basic procedure and commands to define VPNs in a router environment.

The current chapter will be the base for the following branch office and business partner scenarios. In these sections, we extend the configuration of the routers so that more protocols and features make use of the secure connection between the intranet sites. The following protocols and features are demonstrated:

1. DLSw for NetBIOS and SNA
   (Chapter 11, “Branch: data link switching over IPSec” on page 215)
2. Bridging tunnel for LAN-to-LAN bridging over TCP/IP
   (Chapter 12, “IP bridging through an IPSec tunnel” on page 231)
3. APPN / HPR over IP
   (Chapter 13, “Branch: APPN through an IPSec tunnel” on page 241)
4. APPN Dependent LU Requester function (DLUR)
   (Chapter 14, “Branch: dependent LU requester (DLUR)” on page 263)
5. TN3270E server function
   (Chapter 15, “Configuring TN3270E server” on page 291)
6. Connecting Business Partners and Suppliers
   (Chapter 16, “Connecting business partners and suppliers” on page 303)
7. PPTP function
   (Chapter 17, “Connecting remote users with voluntary tunneling” on page 317)
8. L2TP function
   (Chapter 18, “Connecting remote users with compulsory tunneling” on page 371)
9. L2F function
   (Chapter 18, “Connecting remote users with compulsory tunneling” on page 371)
10. IPSEC dial-in function
    (Chapter 20, “Connecting remote users with IPSec dial-up” on page 403

To make each chapter self contained we give in each chapter a complete description of all necessary steps. We will refer back to preceding (sub) chapters where possible and reasonable to avoid duplicate subchapters.

10.1 Description of the environment

We are using the scenario of Figure 173 as our basic configuration scenario, which we will expand and modify in the following chapters:

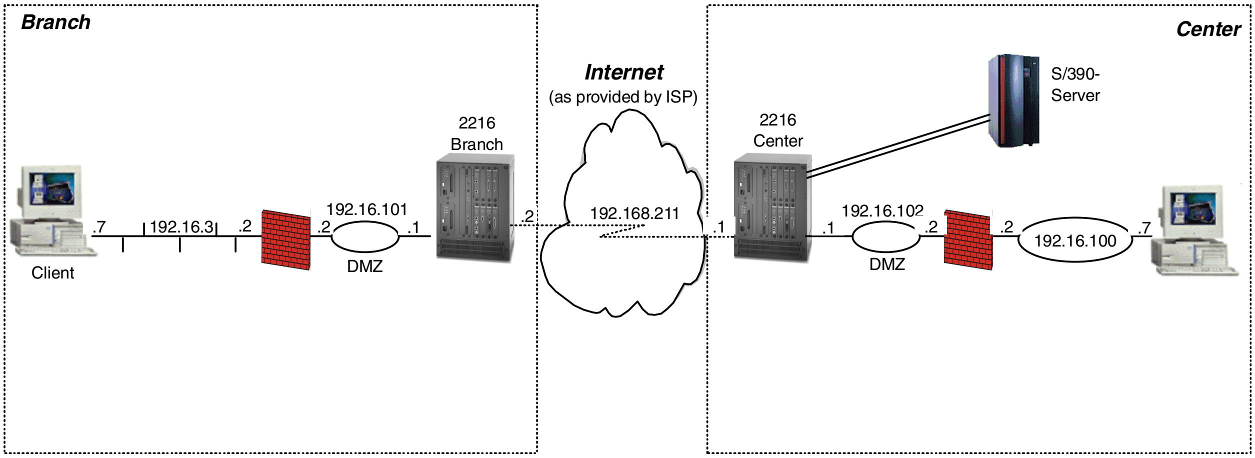


Figure 173. Branch office/connection with a VPN

Note

The following scenarios are designed for the branch office connection to the data center. However, these scenarios are often also applicable for many cases where a business partner or supplier wants to connect to another business partner. We have a separate chapter where these scenarios are handled in more detail (Chapter 16, “Connecting business partners and suppliers” on page 303).

The main corporate site consists of a token-ring LAN with a server. This segment is cascaded behind a demilitarized zone (DMZ). The main site is connected to the Internet using an IBM 2216. The IBM 2216 in the main site is called the *center.*

The branch office/business partner is also protected by a DMZ and consists of a token-ring segment with a client. The branch office/business partner is connected to the Internet with an IBM 2216. The IBM 2216 in the branch office is called the *branch*.

In our test environment the nonsecure network is modeled by a PPP link between the IBM 2216 in the center and the IBM 2216 in the branch. We refer to this nonsecure network as the "Internet" and to the interfaces of the 2216 connected to this network as the "public interfaces".

For the more protocol-specific tests we expanded and/or modified this basic configuration to show the peculiarities of each scenario.

For testing purposes, we placed different kinds of clients and servers (FTP, Telnet, HTTP, IPX and NetBIOS), APPN/HPR network nodes, 3270 clients and an OS/390 server in our Internet. The OS/390 server was connected to a channel adapter in the 2216 on the main site. In the scenario where we start using the host connectivity, an example of the configuration of this connection is provided.

10.2 Description of the scenario

In this scenario we not only transport the traffic between the LANs that are directly attached to the routers over a VPN connection. Here we will transport the following traffic:

- Traffic between the DMZs
- Traffic between the production LANs
- Router-to-router traffic

Having a tunnel that permits/denies certain traffic makes it very easy to define further permits/denials. You define a new policy and can use most definitions of the already existing policy. All you have to do is to specify the additional source and destination of the new permit/denial.

Defining policies can be done in two ways:

- You either work with *deny* policies and permit everything that is not denied.
- You can also work with *permit* policies and deny everything that is not explicitly permitted (drop-out policy).
  This approach is a more secure one and should be pursued in all security approaches. You deny everything by default and you explicitly permit only those connections that you really want to permit.
  Although you work with permit policies there are cases where you need additional deny policies. This may be the case when you have functions within your location (for example, contractors) that use a dedicated IP address within the address range of the location. To deny access to the contractors you would do a permit policy for the whole location range and would do a deny for the embedded range of the contractors. Make sure, however, that in this case the deny policy has a higher priority than the permit rule; otherwise, the permit policy would always match before the deny policy.

10.2.1 Traffic between the DMZs

In Chapter 6, “Configuring IPSec and IKE with IBM Nways routers” on page 89 only the traffic between the router-attached LANs went over the VPN tunnel.

This corresponds in the current scenario to permit the traffic between the demilitarized zones (DMZ). We now expand this scenario and also put the traffic between the two production LANs (data center and branch) on the VPN tunnel. This is done by the addition of a policy.

10.2.2 Traffic between the production LANs

To enable traffic flow between the production LANs you configure a new policy. But instead of specifying all parameters again, you only specify those parameters that differ. In our case it is the Policy Profile (Table 9) with the permit of further source and destination addresses that has to be specified again.

In the Policy Profile you normally specify the source and destination address range with an IP address together with the corresponding subnetmask. The permit/denial of further combinations requires to define a further Policy Profile. This definition of Policy Profiles emphasizes the importance of a well-done IP address design. All IP networks that cannot be covered together with other IP networks by a broader subnetmask, need a separate policy profile. That means for an any-to-any VPN connection between the center with *n* and the branch with *m* independent IP address ranges you need to define the *m x n* policy profiles.

10.2.3 Router-to-router traffic

Later in our scenario, we create several configurations that involve router-to-router traffic that we also need to secure using IPSec (DLSw, IP bridging tunnel, Enterprise Extender, DLUR). This also includes traffic that is caused by routing protocols because in this case the router is the source or destination of the traffic. Depending on the IP addresses that are used by the protocol (address on the interface or the internal IP address) you have to check the corresponding policies.

10.2.4 Tunnel mode versus transport mode VPN connection

In the case of traffic between DMZs or the production LANs you have to use tunnel mode in the VPN connections.

For the router-to-router traffic, however, you could either use tunnel mode or transport mode tunnels. Technically the routers act as IP hosts. It is common practice to use transport mode tunnels for host-to-host traffic because there is no need to camouflage the IP addresses in the original IP headers as is done with tunnel mode.

However, it is not required to use a transport mode tunnel for router-to-router communication. We could use the same tunnel mode tunnel that we use for communication between the intranet LANs.

There are trade-offs either way. If you use the existing tunnel mode tunnel, you will create larger IP packets than is strictly necessary, since you add an IP header and trailer. On the other hand you keep your tunnel database smaller, thus reducing processing by the router. So you have to make a trade-off between more overhead in your traffic (you will use more bandwidth) or more processing in your router (you will consume slightly more DRAM and processing power).

In our scenario, we chose to use the existing tunnel for the router-to-router communication.

In your environment you will probably also use existing tunnel mode connections instead of new transport mode connections. The reason is that you try to minimize your VPN tunnel to keep your environment clear and easy to manage.

10.3 Definition of IPSec on the routers

Now we define IPSec on the routers. We use IKE with pre-shared keys.

The definition is almost the same as in Chapter 6, “Configuring IPSec and IKE with IBM Nways routers” on page 89. We start to do a tunnel between the two production LANs.

To avoid repeating the configuration we list the used parameters in the following matrixes. Note that this matrix is only valid if you are working with the IBM Nways family of routers. If you use different devices the input parameters in the matrixes will probably change.

The IKE policy definition with pre-shared keys is done according to the following steps:

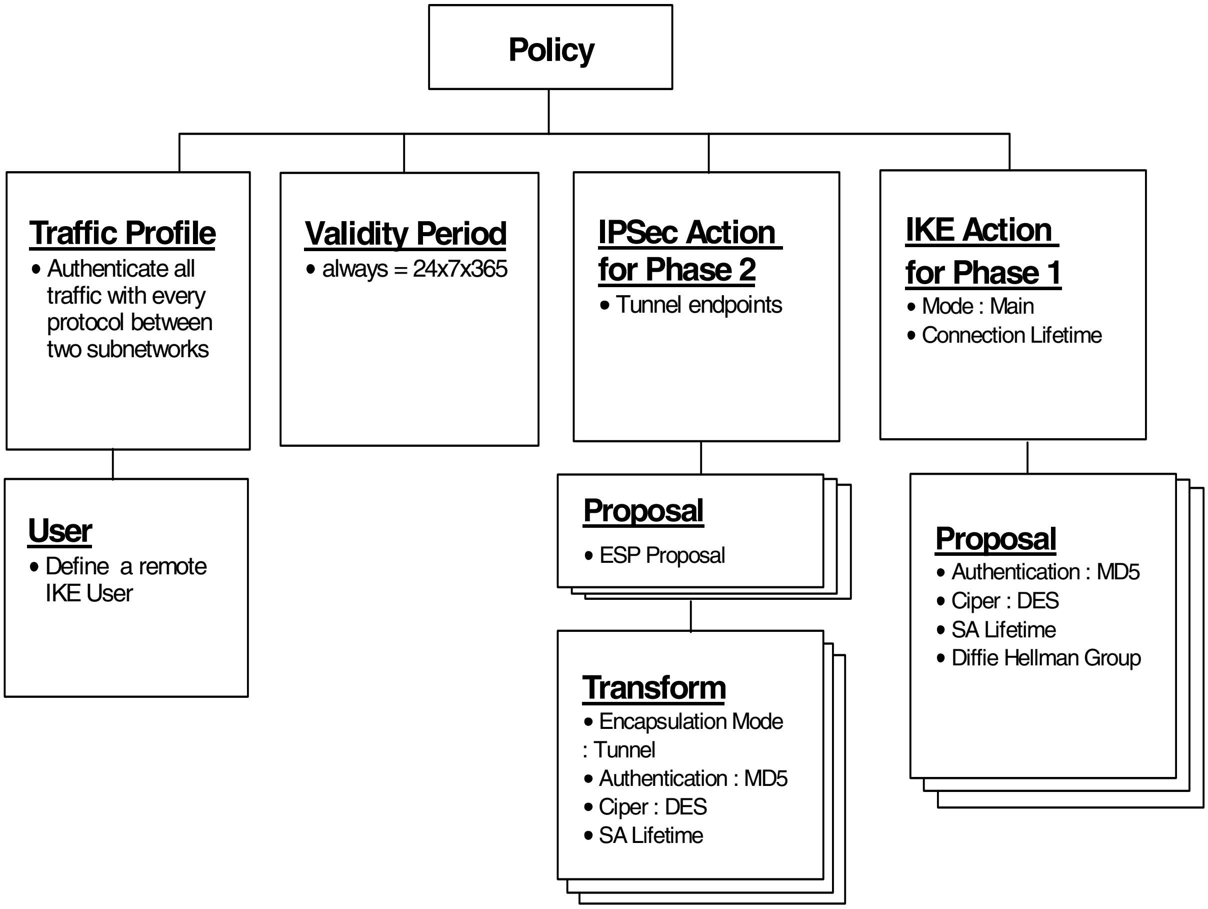


Figure 174. Policy tree for pre-shared key

10.3.1 Definition of policy for DMZ traffic

To verify the configuration, we recommend you check the parameters in the table together with the corresponding figure (Figure 173 on page 198). The order of tables is the same as the order you get when specifying the command add policy.

We have the following matrixes:

- Remote User Definition (Table 7)
- Policy Definitions (Table 8)
- Definition of the Policy Profile (Table 9)
- Definition of the Policy Validity Profile (Table 10)
- Definition of IPSec Action Profile Phase 2 (Table 11)
- IPSec Proposal (Table 12)
- IPSec Transform for IKE Phase 2 (Table 13)
- Definition of ISAKMP Action for IKE Phase 1 (Table 14)
- Definition of ISAKMP Proposal for IKE Phase 2 (Table 15)

In the matrixes you have besides the specification column two further columns: one for the definitions in the branch router and one for the definitions in the center router.

In most cases we can work with the default values, only in some cases will you have to modify the default values. We marked these cases in **boldface**.

You also see that for most of the boxes the entries between the branch and the center router do not differ. We shaded those boxes where they differ:

Table 7. Remote user definitions

Information you need to create your VPN	**Branch Router**	**Center Router**
How to identify the remote IKE peer (user): 1: IP address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID	Option 1: IP-address	Option 1: IP-address
IP Address that distinguishes this user?	**192.168.211.1**	**192.168.211.2**
Authenticate user with: 1: Pre-shared key 2: Public certificate	pre-shared key	pre-shared key
Mode in which you will enter the pre-shared key: 1: ASCII 2: HEX	Option 1: ASCII	Option 1: ASCII
Pre-shared key (even number of characters):	**87654321**	**87654321**

Table 8. Policy definitions

Information you need to create your VPN	**Branch Router**	**Center Router**
Policy name:	**ike-pre-101-102**	**ike-pre-101-102**
Priority of this policy in case of multiple policies:	5	5

Table 9. Definition of the Policy Profile

Information you need to create your VPN	**Branch Router**	**Center Router**
Profile name:	**101.0-to-102.0-pre**	**101.0-to-102.0-pre**
Source address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
IPv4 Source address	**192.168.101.0**	**192.168.102.0**
IPv4 Source Mask (255.255.255.0)	255.255.255.0	255.255.255.0
Destination address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask

Information you need to create your VPN	**Branch Router**	**Center Router**
Destination address	**192.168.102.0**	**192.168.101.0**
IPv4 Destination Mask (255.255.255.0)	255.255.255.0	255.255.255.0
Select the protocol to filter on: 1: TCP 2: UDP 3: All protocols 4: Specify range	Option 3: All protocols	Option 3: All protocols
Starting value for the source port:? 0 for all protocols	0	0
Ending value for the source port: 65535 for all protocols	65535	65535
Starting value for the destination port: 0 for all protocols	0	0
Ending value for the destination port: 65535 for all protocols	65535	65535
Enter the mask to be applied to the Received-DS-byte:	0	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte	0	0
Do you want to configure local and remote IDs for ISAKMP?	**Yes**	**Yes**
Select the identification type of the local ID to be sent to the remote IKE peer 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string)	Option 1: local tunnel endpoint address	Option 1: local tunnel endpoint address
Any user within profile allowed access	Yes	Yes
Do you want to limit this profile to specific interface(s)?	No	No

Table 10. Definition of the Policy Validity Profile

Information you need to create your VPN	**Branch Router**	**Center Router**
Validity profile name:	Option 1: always	Option 1: always
Enter the lifetime of this policy yyyymmddhhmmss:yyyymmddhhmmss or * denotes forever	*	*
During which months should this profile be valid? ALL to signify all year round	all	all
During which days should this profile be valid? ALL to signify all week	all	all

Information you need to create your VPN	**Branch Router**	**Center Router**
During which hours should this profile be valid? * denotes all day	*	*

Table 11. Definition of IPSec Action Profile Phase 2

Information you need to create your VPN	**Branch Router**	**Center Router**
IPSec action profile name:	**tun-101-102**	**tun-101-102**
Select the IPSec security action type: 1: Block 2: Permit	permit	permit
Should the traffic flow into a secure tunnel or in the clear? 1: Clear 2: Secure tunnel	Secure tunnel	Secure tunnel
What is the tunnel start-point IP address?	**192.168.211.2**	**192.168.211.1**
What is the tunnel end-point IP address?	**192.168.211.1**	**192.168.211.2**
Does this IPSec tunnel flow within another IPSec tunnel?	No	No
Percentage of SA lifesize/lifetime to use as the acceptable minimum? Default is 75 %	75	75
Security association refresh threshold in percent Default is 85 %	85	85
Select the option for the DF bit in the outer header 1: Copy 2: Set 3: Clear	Copy	Copy
Do you want to enable replay prevention?	Disable	Disable
Do you want to negotiate the security association at system initialization (autostart)?	No	No

Table 12. IPSec Proposal

Information you need to create your VPN	**Branch Router**	**Center Router**
What name do you want to give this IPSec proposal?	**esp-prop1**	**esp-prop1**
Does this proposal require Diffie Hellman Perfect Forward Secrecy?	No	No
Do you wish to enter any AH transforms for this proposal?	No	No
Do you wish to enter any ESP transforms for this proposal?	**Yes**	**Yes**

Table 13. IPSec Transform for IKE Phase 2

Information you need to create your VPN	Branch Router	Center Router
IPSec ESP transform name:	**esp-tun1**	**esp-tun1**
Select the protocol ID: 1: IPSec AH 2: IPSec ESP	Option 2: IPSec ESP	Option 2: IPSec ESP
Select the encapsulation mode: 1: Tunnel 2: Transport	Option 1: Tunnel	Option 1: Tunnel
Select the ESP authentication algorithm: 1: HMAC_MD5 2: HMAC_SHA	Option 1: HMAC_MD5	Option 2: HMAC_MD5
Select the ESP cipher algorithm: 1: ESP DES 2: ESP 3DEC 3: ESP CDMF 4: ESP NULL	Option 1: ESP DES	Option 1: ESP DES
What is the SA lifesize, in kilobytes Default is 50000 kilobytes	50000	50000
What is the SA lifetime? Default is 3600 sec	3600	3600

Table 14. Definitions for ISAKMP Action for IKE Phase 1

Information you need to create your VPN	Branch Router	Center Router
ISAKMP action name:	**ike-1**	**ike-1**
Select the ISAKMP exchange mode: 1: Main 2: Aggressive	Option 1: Main	Option 1: Main
Percentage of SA lifesize/lifetime to use as the acceptable minimum: Default is 75 %	75	75
What is the ISAKMP connection lifesize, in kilobytes? Default is 5000 kilobytes	5000	5000
What is the ISAKMP connection lifetime in seconds? Default is 30000 sec	30000	30000
Do you want to negotiate the SA at system initialization (autostart)?	Yes	Yes

Table 15. Definitions for ISAKMP Proposal for IKE Phase 2

Information you need to create your VPN	Branch Router	Center Router
ISAKMP proposal name:	**ike-prop1**	**ike-prop1**

Information you need to create your VPN	Branch Router	Center Router
Select the authentication method 1: Pre-shared key 2: Digital certificate	Option 1: Pre-shared key	Option 1: Pre-shared key
Select the hashing algorithm 1: MD5 2: SHA	Option 1: MD5	Option 1: MD5
Select the cipher algorithm 1: DES 2: 3DES	Option 1: DES	Option 1: DES
What is the SA lifesize, in kilobytes? Default is 1000 kilobytes	1000	1000
What is the SA lifetime? Default is 15000 sec	15000	15000
Select the Diffie Hellman Group ID 1: Diffie Hellman Group 1 2: Diffie Hellman Group 2	Option 1: Diffie Hellman Group 1	Option 1: Diffie Hellman Group 1
Do you wish to map a DiffServ Action to this policy?	No	No
What will the status of the policy be? 1: Enabled 2: Disabled	Option 1: Enabled	Option 1: Enabled

10.3.2 Traffic between the production LANs

You have the production LAN in the branch (172.16.3.0) and the production LAN in the center (192.168.100.0).

To permit traffic between these two networks you do not need to specify all parameters again. You can reuse most of the existing policy. All you have to specify are the new parameters. That means in this case you define a new policy definition with a new profile name and new source and destination addresses (see the shaded boxes in Table 16):

Table 16. Definition of the Policy Profile for the traffic between the production LANs

Information you need to create your VPN	Branch Router	Center Router
Profile name:	**3.0-to-100.0-pre**	**3.0-to-100.0-pre**
Source address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
IPv4 Source address	**172.16.3.0**	**192.168.100.0**
IPv4 Source Mask (255.255.255.0)	255.255.255.0	255.255.255.0

Information you need to create your VPN	Branch Router	Center Router
Destination address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
Destination address	**192.168.100.0**	**172.16.3.0**
IPv4 Destination Mask (255.255.255.0)	255.255.255.0	255.255.255.0
Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range	Option 3: All protocols	Option 3: All protocols
Starting value for the source port:? 0 for all protocols	0	0
Ending value for the source port: 65535 for all protocols	65535	65535
Starting value for the destination port: 0 for all protocols	0	0
Ending value for the destination port: 65535 for all protocols	65535	65535
Enter the mask to be applied to the Received-DS-byte:	0	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte	0	0
Do you want to configure local and remote IDs for ISAKMP?	**Yes**	**Yes**
Select the identification type of the local ID to be sent to the remote IKE peer 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string)	Option 1: local tunnel endpoint address	Option 1: local tunnel endpoint address
Any user within profile allowed access	Yes	Yes
Do you want to limit this profile to specific interface(s)?	No	No

10.3.3 Router-to-router traffic

On the tunnel between the routers there is not only traffic between the DMZs and traffic between the production LANs, but there is also IP traffic that has the routers as source or destination (for example, DLSw, routing protocol).

We assume that the addresses on the WAN link (192.168.212.1 and 192.168.212.2) are the source or destination addresses. In this case you have to add a new policy with these new addresses as source or destination (see shaded boxes in Table 17). Note that you specify in this case 255.255.255.255 as the source/destination subnetmask.

If the router-to-router traffic uses other IP addresses of the routers as source/destination you have to modify these addresses accordingly.

Table 17. Definition of the Policy Profile for the traffic between the production LANs

Information you need to create your VPN	**Branch Router**	**Center Router**
Profile name:	**211.0-to-211.0-pre**	**211.0-to-211.0-pre**
Source address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
IPv4 Source address	**192.168.211.2**	**192.168.211.1**
IPv4 Source Mask (255.255.255.0)	**255.255.255.255**	**255.255.255.255**
Destination address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
Destination address	**192.168.211.1**	**192.168.211.2**
IPv4 Destination Mask (255.255.255.0)	**255.255.255.255**	**255.255.255.255**
Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range	Option 3: All protocols	Option 3: All protocols
Starting value for the source port:? 0 for all protocols	0	0
Ending value for the source port: 65535 for all protocols	65535	65535
Starting value for the destination port: 0 for all protocols	0	0
Ending value for the destination port: 65535 for all protocols	65535	65535
Enter the mask to be applied to the Received-DS-byte:	0	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte	0	0
Do you want to configure local and remote IDs for ISAKMP?	**Yes**	**Yes**
Select the identification type of the local ID to be sent to the remote IKE peer 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string)	Option 1: local tunnel endpoint address	Option 1: local tunnel endpoint address
Any user within profile allowed access	Yes	Yes

Information you need to create your VPN	Branch Router	Center Router
Do you want to limit this profile to specific interface(s)?	No	No

10.3.4 Defining a drop-out policy

As all traffic is passed through the policy database, either directly or through the flow cache, policies can be defined to drop all traffic that does not match the configured policies. This removes the need to configure filters on the interfaces.

10.3.4.1 Drop-out policy for outgoing traffic

Therefore, on the center router we could define a filter that drops outbound traffic, which is leaving over the 192.168.211.1 interface and does not match any of the defined policies and the generated rules.

This policy should have the lowest priority of any rule configured (remember: policies with higher priority are checked first). As no profiles exist we are prompted through the creation of a profile. We are not going to specify the source or destination addresses but actually specify the rule in terms of the ingress-egress interfaces (you get this prompt because we specify the source and/or destination address as 0.0.0.0).

This policy (Table 18) tackles traffic outgoing from the center on the WAN link (column 2). In the last column you see the policy that tackles traffic outgoing from the branch on the WAN link.

We also need a policy for incoming traffic - this is done in the next section (10.3.4.2, “Drop-out policy for incoming traffic” on page 210).

Table 18. Definition of a ’drop-out policy for outgoing traffic on the two routers

Information you need to create your VPN	Branch Router	Center Router
Profile name:	**drop_out_outgoing**	**drop_out_outgoing**
Source address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
Priority of this policy	**1**	**1**
IPv4 Source address	**0.0.0.0**	**0.0.0.0**
IPv4 Source Mask (255.255.255.0)	**0.0.0.0**	**0.0.0.0**
Destination address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
Destination address	**0.0.0.0**	**0.0.0.0**
IPv4 Destination Mask (255.255.255.0)	**0.0.0.0**	**0.0.0.0**

Information you need to create your VPN	Branch Router	Center Router
Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range	Option 3: All protocols	Option 3: All protocols
Starting value for the source port:? 0 for all protocols	0	0
Ending value for the source port: 65535 for all protocols	65535	65535
Starting value for the destination port: 0 for all protocols	0	0
Ending value for the destination port: 65535 for all protocols	65535	65535
Enter the mask to be applied to the Received-DS-byte:	0	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte	0	0
Do you want to configure local and remote IDs for ISAKMP?	No	No
Do you want to further qualify which traffic to filter	**Yes**	**Yes**
Ingress Interface IP Address (255.255.255.255 means any ingress)	255.255.255.255	255.255.255.255
Egress Interface IP Address (255.255.255.255 means any egress)	**192.168.211.1**	**192.168.211.2**
Validity Period	always	always
Should policy enforce IPSec action?	**Yes**	**Yes**
Name of IPSec action	**drop-no-match**	**drop-no-match**
IPSec action type: 1: block 2: permit	**Option 1:** **block**	**Option 1:** **block**

10.3.4.2 Drop-out policy for incoming traffic

Besides the filtering of outgoing traffic we must also filter all incoming traffic from the Internet.

Therefore, we define on each router a filter which drops incoming traffic on the interface 192.168.211.1 or 192.168.211.2, unless this traffic is explicitly permitted by a match with any of the defined policies and the generated rules.

This policy should have the lowest priority of any rule configured (remember: policies with higher priority are checked first). As no profiles exist we are prompted through the creation of a profile.

As in the case of the outgoing drop-out we also specify here 0.0.0.0 as source and destination mask. We are then prompted to specify the rule in terms of the ingress-egress interfaces. We specify the IP address of the WAN link here as an ingress interface and 255.255.255.255 (any interface) as an egress interface.

This policy (Table 19) tackles traffic incoming to the center router (column 2). In the last column you see the policy that tackles traffic incoming to the branch router.

Table 19. Definition of a drop-out policy for outgoing traffic on the two routers

Information you need to create your VPN	**Branch Router**	**Center Router**
Profile name:	**drop_out_incoming**	**drop_out_incoming**
Source address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
Priority of this policy	**1**	**1**
IPv4 Source address	**0.0.0.0**	**0.0.0.0**
IPv4 Source Mask (255.255.255.0)	**0.0.0.0**	**0.0.0.0**
Destination address format 1: NetMask 2: Range 3: Single address	NetMask	NetMask
Destination address	**0.0.0.0**	**0.0.0.0**
IPv4 Destination Mask (255.255.255.0)	**0.0.0.0**	**0.0.0.0**
Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range	Option 3: All protocols	Option 3: All protocols
Starting value for the source port:? 0 for all protocols	0	0
Ending value for the source port: 65535 for all protocols	65535	65535
Starting value for the destination port: 0 for all protocols	0	0
Ending value for the destination port: 65535 for all protocols	65535	65535
Enter the mask to be applied to the Received-DS-byte	0	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte	0	0
Do you want to configure local and remote IDs for ISAKMP?	No	No

Information you need to create your VPN	Branch Router	Center Router
Do you want to further qualify which traffic to filter?	**Yes**	**Yes**
Ingress Interface IP Address (255.255.255.255 means any ingress)	**192.168.211.1**	**192.168.211.2**
Egress Interface IP Address (255.255.255.255 means any egress)	**255.255.255.255**	**255.255.255.255**
Validity Period	always	always
Should policy enforce IPSec action?	**Yes**	**Yes**
Name of IPSec action	**drop-no-match**	**drop-no-match**
IPSec action type: 1: block 2: permit	**Option 1: block**	**Option 1: block**

10.3.5 Defining a default policy

Especially when working together will the Lightweight Directory Access Protocol (LDAP) we should also define a default policy.

The above mentioned drop-out policy tackles traffic for which there are no policy matches. But what happens when you work with the Lightweight Directory Access Protocol (LDAP) when you do not yet have policies loaded from the LDAP server?

For this case you have to define a default policy.

When a router boots it looks at the default rule. The default rule describes what a router should do with traffic while it is building its database. The options are forward all traffic or drop all traffic except LDAP traffic or drop all traffic and secure LDAP traffic. The default is to forward all traffic. If you are defining security policies you will probably want to drop the traffic until the policy database is built - if not, the data would be forwarded without security. If you are retrieving you are also retrieving polices using LDAP and you will want to forward your LDAP traffic and define that LDAP be secured. This default action is defined using the `set default` command (Figure 175 on page 213).

If you choose to secure your LDAP traffic you will be guided through creating an IPSec and ISAKMP.

```
Branch Policy config>feature policy
Branch Policy config>SET DEFAULT-POLICY
List of default policy rules:
  1)  Accept and Forward all IP Traffic
  2)  Permit LDAP traffic, drop all other IP Traffic
  3)  Permit and Secure LDAP traffic, drop all other IP Traffic
Select the default policy rule to use during policy refresh periods [1]? 3
List of default error handling procedures:
  1)  Reset Policy Database to Default Rule
  2)  Flush any rules read from LDAP, load local rules
Select the error handling behavior for when loading Policy Database  [1]? 2
Please enter the set of Security Information for encrypting and
authenticating the LDAP traffic generated by the device when
retrieving policy information from the LDAP Server
Enter phase 1 ISAKMP negotiation parameters:
List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2
Select the Diffie Hellman Group ID from this proposal (1-2) [1]?
List of Hashing Algorithms:
     1)  MD5
     2)  SHA
Select the hashing algorithm(1-2) [1]?
List of Cipher Algorithms:
     1)  DES
     2)  3DES
Select the Cipher Algorithm (1-2) [1]?
Authentication: (1)Pre-shared Key or (2)Certificate(RSA Sig) [1]? 1
Enter the Pre-Shared Key (an even number of 2-29 ascii chars):12345678
Enter the Pre-Shared Key again (8 characters) in ascii:12345678
Enter phase 2 IPSEC negotiation parameters:
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA
Select the ESP Authentication Algorithm (0-2) [1]?
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL
Select the ESP Cipher Algorithm (1-4) [1]?
Tunnel Start IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 192.168.211.2
Tunnel End Point IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 192.168.100.6
Tunnel Start IPV4 Address (Secondary LDAP Server)
 [192.168.211.1]?
Tunnel End Point IPV4 Address (Secondary LDAP Server)
 [192.168.100.6]?
```

Figure 175. Definition of a default policy

A prerequisite is that the LDAP server is capable of performing IKE. If the server is not capable you could secure the traffic to a device close to the server.

The tunnel start address is an interface on the router over which the server can be reached, the endpoint address is the IP address of the IKE peer, that is, either the LDAP server or a device acting on behalf of the server.

Once the router has determined how to handle traffic while building the database, it starts to build the database. It starts by loading the local policies. When this is completed, and if LDAP is enabled it will then try to retrieve policies from the database. The router will contact the first LDAP server, retrieve the policies and store them in the local database. At this point the database will be populated, and the traffic will then be forwarded according to the policies.

Remember that if the traffic does not match any policy it is forwarded (default); if there is a clash between a local policy and an LDAP policy, the local policy will take priority. If a client gets no response from the primary LDAP server after the “retry interval” it will contact the secondary server. If the secondary server is available, it will retrieve the policies. If the secondary is unavailable, the router will then contact the primary again. The router will continue to try the primary and secondary server at the time interval specified in the “retry interval” until the router manages to retrieve the policies. The interval can be configured from talk 6, feature policy.

While the router is trying other servers, it needs to know what to do with traffic. This is described in the default error handling procedure which is also configured using the `set default` command. The options are flush the whole database and apply the default rule or flush any LDAP rules and apply the local rules. This error handling also describes what happens if there is an error reading the rules. If you are using LDAP and also define local rules, it is advisable to choose to apply the local rules if for any reason you cannot read the LDAP rules.

Chapter 11. Branch: data link switching over IPSec

Now that the IPSec tunnel is in place between the branch and the data center, we have the capability to securely route IP traffic between these two locations over our virtual private network. However, most enterprise environments today are not IP-only networks. Therefore, in order to get the maximum utility of the tunnel, we need to add support for other protocols like SNA and NetBIOS.

DLSw is an IBM-invented standard technology for transporting connection-oriented protocols, mainly SNA and NetBIOS, across IP backbone networks. DLSw routers on the edges of an IP network process link establishment requests from native SNA and NetBIOS endstations, search among peer DLSw routers for one serving the target endstation, then set up a path and relay application data between the endstations through the peer router.

With an IPSec tunnel defined between the routers, we can easily define a DLSw connection that uses this tunnel. In this chapter we describe the procedures for implementing a DLSw connection in a VPN environment using the IBM Nways 2210/2216 routers.

Note

This chapter assumes you are already familiar with DLSw. For more information on using DLSw, please see *IBM 2210 Nways Multiprotocol Router IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume II*, SG24-4956.

11.1 Description of the scenario

We use the same configuration here as in Chapter 10, “Connecting the data center to the branch office” on page 197. We simply build on it to add the DLSw capability. All the same we will show all the necessary steps here.

Figure 176 on page 216 shows the network along with the DLSw-related parameters:

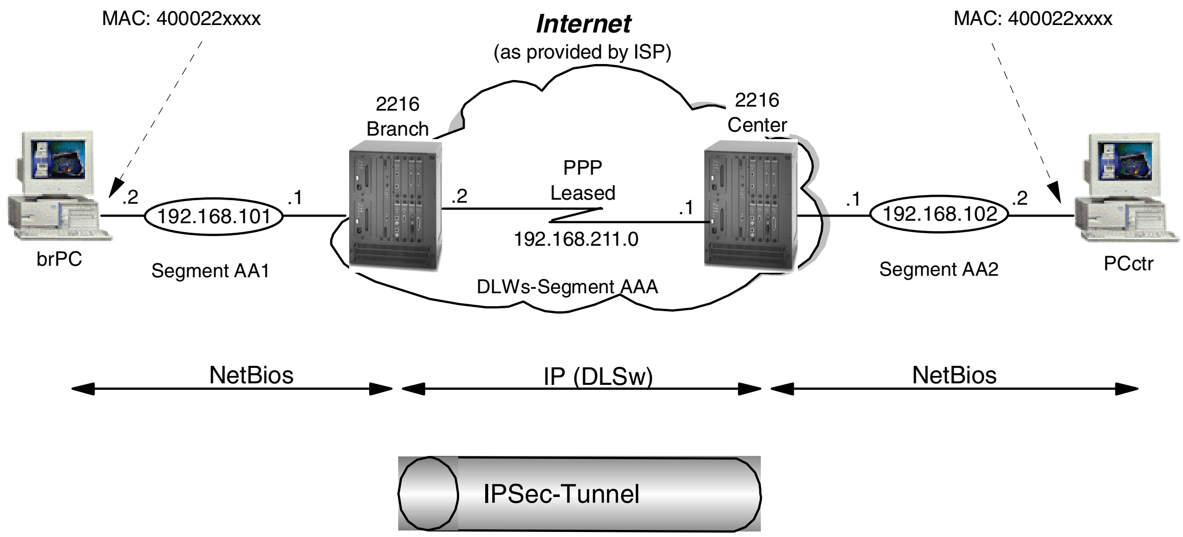


Figure 176. Data link switching through an IPSec tunnel

11.1.1 Traffic flow

The SNA/NetBIOS traffic comes into the branch router as an LLC frame over the token-ring interface. The branch router, acting as a DLSw router, decides to encapsulate the SNA/NetBIOS traffic into IP and to send it to its destination over the (virtual bridged) DLSw segment.

At this point, the policy that we define on the router redirects the packet to the IPSec engine where it is processed for AH and ESP headers before being sent out on the physical interface.

A similar process occurs in the reverse direction. As the IP packet reaches the end of the tunnel, it gets decapsulated and decrypted by the IPSec engine, then passed to the IP stack where it is determined that it must be further handled by DLSw in the router. The DLSw headers are stripped off the DLSw packet and the packet is further processed/bridged by the router.

11.1.2 Environment

We use the IPSec installation from Chapter 10, “Connecting the data center to the branch office” on page 197 to securely transport the IP-traffic, that is, we use pre-shared keys and we have a tunnel between the two routers in the branch and center.

We put the SNA client not in the production LAN of the branch but in the LAN that is directly attached to the branch router. This scenario is more realistic because branches rarely have a dedicated DMZ. With this scenario we also avoid bridging SNA/NetBIOS frames over the firewall.

We use two Windows PCs as NetBIOS nodes. These machines are labeled brPC and PCctr in the diagram.

To configure DLSw in the VPN environment, we perform the following procedures:

1. Configure the center router (bridging and DLSw).
2. Configure the branch router (bridging and DLSw).
3. Test DLSw (IPSec disabled).
4. Enable IPSec and policies.
5. Test DLSw (IPSec enabled).

Each of these steps is explained in detail in the following sections.

11.2 IPSec and policy

As discussed in 10.2.4, “Tunnel mode versus transport mode VPN connection” on page 200, we could use either an IPSec tunnel mode tunnel or a transport mode tunnel. One reason a company would use tunnel mode versus transport mode is to hide internal IP addresses used in the network. Another might be to use unregistered IP addresses. When packets use tunnel mode, they are encapsulated with a new IP header and the original source and destination addresses are no longer visible.

However, in the case of DLSw, the IP traffic originates in the router where the NetBIOS traffic is encapsulated and terminates in the router where it is decapsulated. In our scenario, the routers where the NetBIOS traffic is encapsulated are the same routers used as our IPSec tunnel endpoints. In other words, only the Internet addresses of these two routers will appear in IP/DLSw packets. Using tunnel mode in this situation does not offer any advantages over transport mode in terms of hiding the source and destination IP addresses of the sender and receiver.

For our scenario, we used the existing tunnel to carry our DLSw traffic. This tunnel was defined in 10.3.3, “Router-to-router traffic” on page 207.

11.3 Definition of the router in the center

In this section we describe the necessary steps to set up the center router.

11.3.1 Preparation

Perform the initial steps as outlined below before you set up the VPN scenario.

11.3.1.1 Define internal IP address

We define an internal IP address which will be the endpoint of our DLSw tunnel:

```
Center IP config>SET INTERNAL-IP-ADDRESS
Internal IP address [172.16.220.253]? 192.168.211.1
Center IP config>EXIT
```

Figure 177. Setting the internal IP address on the router in the central site

11.3.1.2 Disable the policy and IPSec

You have to disable the policy (Figure 178 on page 218) and IPSec (Figure 179 on page 218):

The command `list policy all` provides you with a list of all defined policies and their status (disabled/enabled). With the command `disable policy` you can disable them.

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled   : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-act1
       .......
Center Policy Config>
Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
 [?]?
        1: ike-pre-101-102
        2: ike-pre-3-100
        3: ike-pre-211-211
Number of policy [1]?
```

Figure 178. Disabling the policies on the router in the center

The command `disable IPSec stop` stops IPSec. The current status of IPSec can be seen with the command `list status`.

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>DISABLE IPSEC STOP
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
```

Figure 179. Disabling IPSec on the router in the center

11.3.2 Defining the bridge

Now we configure the bridging and the DLSw function (see Figure 180).

We then disable the ports that we are not using in this configuration. Only the bridged LAN port should be active (Figure 181 on page 219).

For more information on configuring bridging, please see *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I*, SG24-4446.

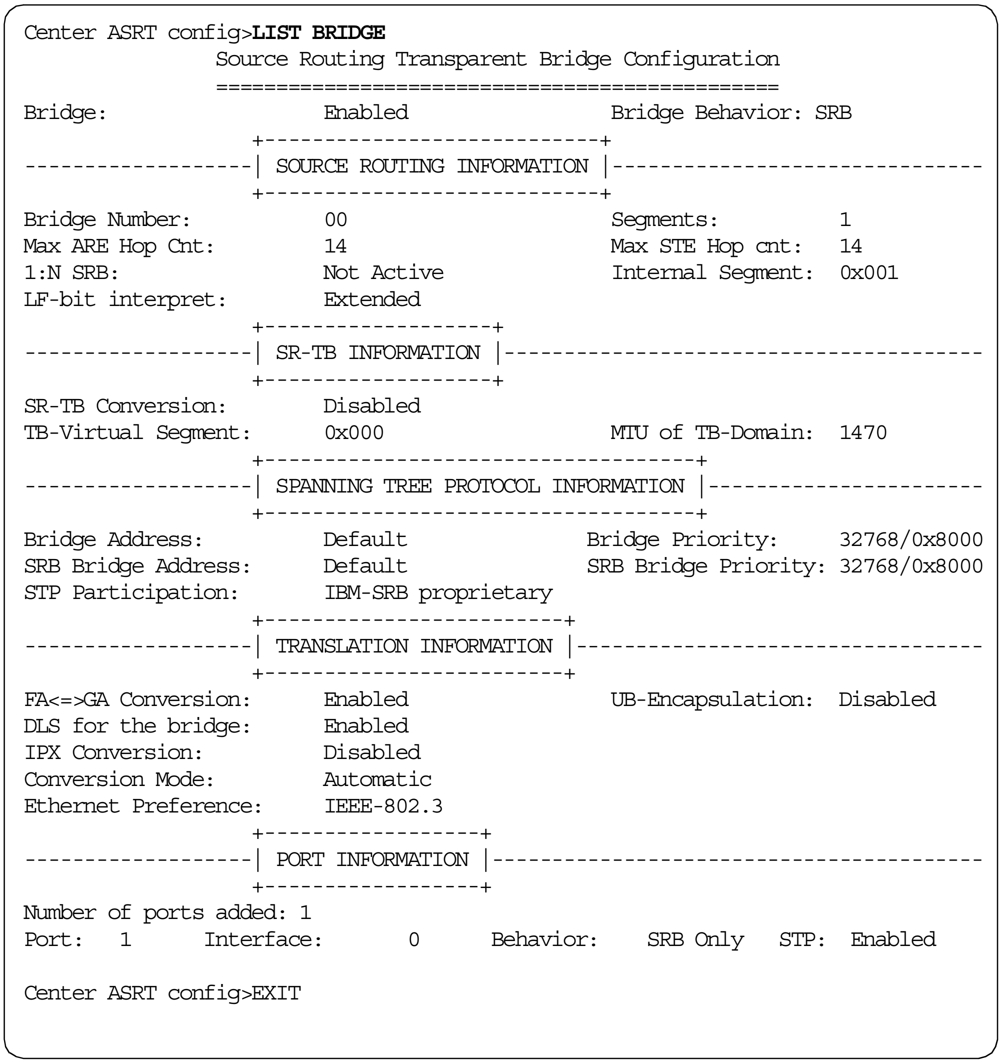
```
Center Config>PROTOCOL ASRT
Adaptive Source Routing Transparent Bridge user configuration
Center ASRT config>
Center ASRT config>ENABLE BRIDGE
Center ASRT config>ENABLE DLS
```

Figure 180. Enabling bridging and DLSw on the router in the center

```
Center Config>PROTOCOL ASRT
Adaptive Source Routing Transparent Bridge user configuration
Center ASRT config>ADD PORT
Interface Number [0]? 0
Port Number [1]? 1
Center ASRT config>
Center ASRT config>DISABLE TRANSPARENT 1
Center ASRT config>ENABLE SOURCE-ROUTING 1
Segment Number for the port in hex(1 - FFF) [001]? aa1
```

Figure 181. Configuring ASRT on the data center router

Now we list the bridge configuration back out to verify that we made the correct changes. This is shown in Figure 182:



```
Center ASRT config>LIST BRIDGE
                Source Routing Transparent Bridge Configuration
                ===============================================
Bridge:                  Enabled                 Bridge Behavior: SRB
                   +----------------------------+
-------------------| SOURCE ROUTING INFORMATION |-------------------------------
                   +----------------------------+
Bridge Number:           00                      Segments:          1
Max ARE Hop Cnt:         14                      Max STE Hop cnt:   14
1:N SRB:                 Not Active              Internal Segment:  0x001
LF-bit interpret:        Extended
                   +--------------------+
-------------------| SR-TB INFORMATION |---------------------------------------
                   +--------------------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  1470
                   +------------------------------------+
-------------------| SPANNING TREE PROTOCOL INFORMATION |-----------------------
                   +------------------------------------+
Bridge Address:          Default               Bridge Priority:     32768/0x8000
SRB Bridge Address:      Default               SRB Bridge Priority: 32768/0x8000
STP Participation:       IBM-SRB proprietary
                   +-------------------------+
-------------------| TRANSLATION INFORMATION |----------------------------------
                   +-------------------------+
FA<=>GA Conversion:      Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:      Enabled
IPX Conversion:          Disabled
Conversion Mode:         Automatic
Ethernet Preference:     IEEE-802.3
                   +------------------+
-------------------| PORT INFORMATION |----------------------------------------
                   +------------------+
Number of ports added: 1
Port:   1      Interface:      0      Behavior:    SRB Only   STP:  Enabled

Center ASRT config>EXIT
```

Figure 182. Configuring ASRT on the data center router

11.3.3 Definition of DLSw

Now we configure DLSw. This involves enabling it at the box level and also opening SAPs for the traffic that you want to carry across the DLSw connection. These steps are illustrated in the following figures:

11.3.3.1 DLSw enabling at the box level

See Figure 183:

```
Center ASRT config>
Center Config>PROTOCOL DLSW
DLSw protocol user configuration
Center DLSw config>ENABLE DLSW
Data Link Switching is now enabled
Center DLSw config>SET SRB aaa
DLSw segment number has been set.
Center DLSw config>
```

Figure 183. Enabling DLSw on the data center router

11.3.3.2 Opening SAPs for DLSw traffic

See Figure 184:

```
Center ASRT config>
Center Config>PROTOCOL DLSW
DLSw protocol user configuration
Center DLSw config>OPEN-SAP
Enter Interface number [0]? 0
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? sna
SAP(s)  0  4  8  C opened on interface 0
Center DLSw config>OPEN-SAP
Enter Interface number [0]? 0
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? nb
SAP(s) F0 opened on interface 0
Center DLSw config>LIST OPEN
Interface SAP(s)
    0      0  4  8  C F0
Center DLSw config>
```

Figure 184. Opening SAPs for DLSw traffic

11.3.3.3 Adding DLSw neighbors

Now we add the DLSw neighbor (the other end of the DLSw pipe). The neighbor DLSw IP address added here must be the internal IP address of the peer DLSw router. In our case, this is the router at the other end of the IPSec tunnel although it could be any router in the branch office that has a valid IP connection.

In our example, the internal address has been set to the interface address of the public network (our IPSec tunnel endpoint). This has an implication regarding the policy for IPSec. DLSw packets have source and destination IP addresses of the TCP connection endpoints which are the internal addresses of the two routers at the endpoints. The policy should allow DLSw to get through the tunnel.

```
Center DLSw config>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 192.168.211.2
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]? e
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neigÿÿor has been added
Center DLSw config>
Center DLSw config>LIST TCP
                   Xmit    Rcv     Max     Keep-    SesAlive
Neighbor       CST Bufsize Bufsize Segsize Alive    Spoofing Priority
-------------- --- ------- ------- ------- -------- -------- --------
192.168.211.2   a    5120    5120     1024 ENABLED  DISABLED MEDIUM
Center DLSw config>
```

Figure 185. Configuring TCP neighbors on the data center router

11.3.4 Activate

This completes the configuration of the data center router. You need to restart or reload the router before the new DLSw configuration changes will become active (see Figure 186):

```
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): B
```

Figure 186. Reloading the router in the center

11.4 Definition of the router in the branch

The configuration of the branch router is almost the same as in the data center router and can be done correspondingly.

11.5 Definitions on the client PCs

We used two Windows NT peers, which access the remote disk of their peers with the NetBIOS protocol.

11.6 Testing DLSw (IPSec disabled)

Perform the following steps to test DLSw without IPSec.

11.6.1 Disable IPSec

As a first step in adding DLSw to our configuration, we temporarily disable IPSec and the policy. This allows us to define and test the DLSw configuration independently of any IPSec functions. After the DLSw configuration is working, we re-enable the policy’s control and IPSec.

Note: We recommend that you do this first to facilitate any problem determination that may be necessary while bringing up DLSw. Otherwise, if you do experience problems, it will be difficult for you to determine if the problem is in the DLSw configuration or if there is an IPSec problem such as a filter definition.

Figure 187 on page 223 shows the command used to disable the policy and IPSec. As can be seen from the figure, this command is executed from within the IP configuration in the talk 6 process.

Note

It is essential that you disable IPSec and the policy definitions. If you only disable IPSec and the policies are still active, the router tries to perform the necessary IPSec actions which cannot be performed and that case and the packet will be dropped.

Figure 189 on page 224 also illustrates that after you disable the policy and IPSec, you must reset IP to make these changes effective.

You have to disable the policy (Figure 187) and IPSec (Figure 188 on page 224):

The command `list policy all` provides you with a list of all defined policies and their status (disabled/enabled). With the command `disable policy` you can disable them.

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled   : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-act1
       .......
Center Policy Config>
Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
 [?]?
        1: ike-pre-101-102
        2: ike-pre-3-100
        3: ike-pre-211-211
Number of policy [1]?
```

Figure 187. Disabling the policies on the router in the center

The command `disable IPSec stop` stops IPSec. The current status of IPSec can be seen with the command `list status`.

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>DISABLE IPSEC STOP
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
```

Figure 188. Disabling IPSec on the router in the center

```
Center Policy config>EXIT
Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 189. Reload of the router in the center

11.6.2 List DLSw neighbors

Figure 190 lists the DLSw neighbors:

```
Center DLSw config>
Center DLSw config>LIST TCP
                    Xmit    Rcv     Max     Keep-    SesAlive
Neighbor        CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --- ------- ------- ------- -------- -------- --------
192.168.211.2    a     5120    5120    1024 ENABLED  DISABLED MEDIUM
Center DLSw config>
```

Figure 190. Listing of DLSw neighbors

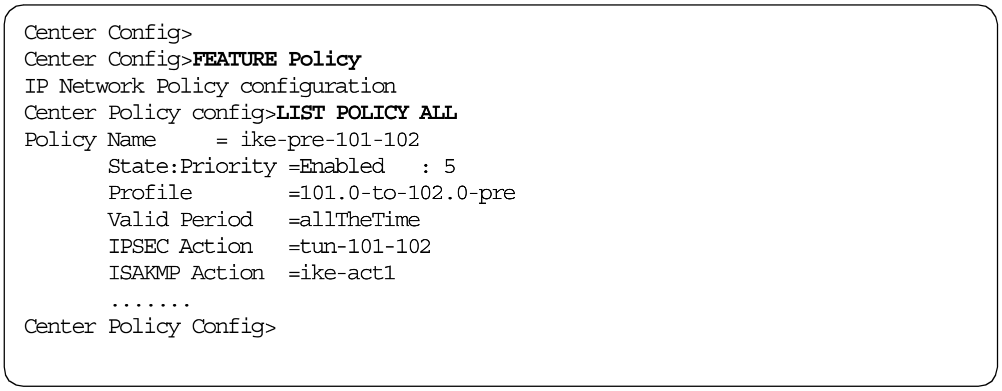
11.6.3 Checking the status of IPSec and the policies

The IPSec command `list status` lists the corresponding status (Figure 191):

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
```

Figure 191. Listing the status of IPSec on the router in the center

The command `list policy all` provides you with a list of all defined policies and their status (disabled/enabled).



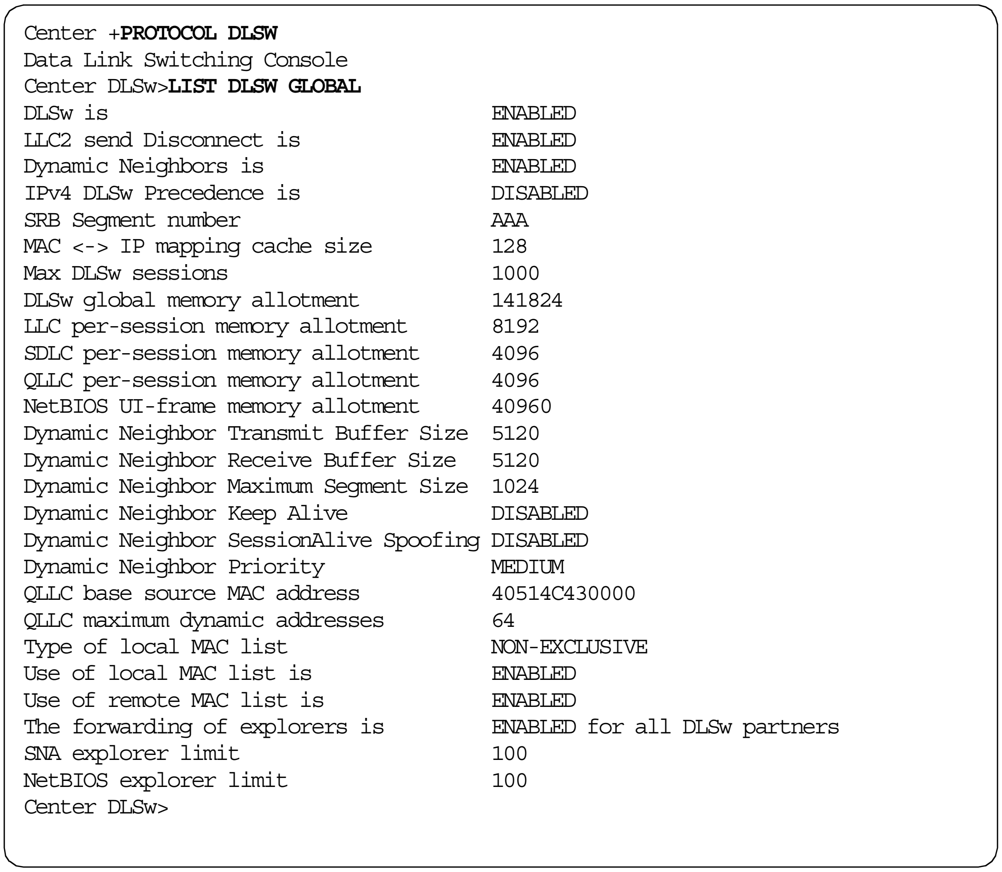
```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled   : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-act1
       .......
Center Policy Config>
```

Figure 192. Listing the status of the policies on the router in the center

11.6.4 Testing the DLSw connection

At this point, you would stop and test the DLSw configuration and make sure that it is working like you intended. You can see if the connection between the TCP neighbors is established and also if there is a DLS session.

Figure 193 shows how to check the DLSw definitions:



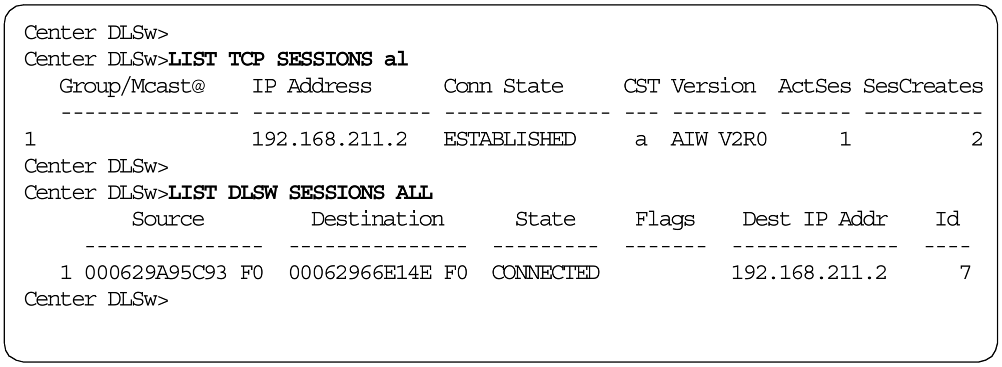
```
Center +PROTOCOL DLSW
Data Link Switching Console
Center DLSw>LIST DLSW GLOBAL
DLSw is                                ENABLED
LLC2 send Disconnect is                ENABLED
Dynamic Neighbors is                   ENABLED
IPv4 DLSw Precedence is                DISABLED
SRB Segment number                     AAA
MAC <-> IP mapping cache size          128
Max DLSw sessions                      1000
DLSw global memory allotment           141824
LLC per-session memory allotment       8192
SDLC per-session memory allotment      4096
QLLC per-session memory allotment      4096
NetBIOS UI-frame memory allotment      40960
Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor SessionAlive Spoofing DISABLED
Dynamic Neighbor Priority              MEDIUM
QLLC base source MAC address           40514C430000
QLLC maximum dynamic addresses         64
Type of local MAC list                 NON-EXCLUSIVE
Use of local MAC list is               ENABLED
Use of remote MAC list is              ENABLED
The forwarding of explorers is         ENABLED for all DLSw partners
SNA explorer limit                     100
NetBIOS explorer limit                 100
Center DLSw>
```

Figure 193. Listing the TCP and DLS sessions on the router in the center

Figure 194 on page 226 shows that a NetBIOS session has been established between the PC in the branch and the PC in the center. This is indicated by the

F0 Service Access Point (SAP) in the MAC address/SAP pairs for the DLS session.

This figure also shows that there is a TCP connection to the router in the branch (192.168.211.2).



```
Center DLSw>
Center DLSw>LIST TCP SESSIONS al
   Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
   --------------- --------------- -------------- --- -------- ------ ----------
1                  192.168.211.2   ESTABLISHED     a  AIW V2R0      1          2
Center DLSw>
Center DLSw>LIST DLSW SESSIONS ALL
         Source         Destination      State     Flags    Dest IP Addr    Id
     ---------------  ---------------  ---------  -------  --------------  ----
   1 000629A95C93 F0  00062966E14E F0  CONNECTED           192.168.211.2      7
Center DLSw>
```

Figure 194. TCP and DLS sessions on the router in the center

11.7 Testing DLSw (IPSec enabled)

After we have verified that DLSw is working correctly, it is time to re-enable the policies and IPSec.

Here we show how to do these steps for the router in the center. It is the same for the 2216 in the branch.

11.7.1 List the defined policies

Figure 195 on page 227 shows the commands to list the defined policies.

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
Center IPV4-IPsec config>EXIT
Center IPsec config>EXIT
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled    : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-1
Policy Name     = ike-pre-3-100
       State:Priority =Enabled    : 10
       Profile        =3.0-to-100.0.pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-1
Policy Name     = ike-pre-211-211
       State:Priority =Enabled    : 5
       Profile        =211.0-to-211.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-1
Center Policy config>
```

Figure 195. List the defined policies on the router in the center

11.7.2 Enable policy

Figure 196 shows the command `enable policy` to enable the policies:

```
Branch Policy config>ENABLE POLICY
Enter the Name of the Policy to enable (? for a List)
[?]?
1: ike-pre-101-102
2: ike-pre-3-100
3: ike-pre-211-211
Number of policy [1]? 3
```

Figure 196. Enable the policies in the router in the center

Notice that we do not need to enable the policy between the LAN 192.168.100.0 in the center and the LAN 172.16.3.0 in the branch. Neither do we need to enable the policy between the LAN 192.168.100.0 (the former DMZ in the center) and the LAN 172.16.3.0 (the former DMZ in the branch).

The reason for this is that the DLSw establishes an IP session between the internal IP addresses, which in our case are the IP addresses of the public network. Only the IP address of these DLSw nodes appear in the Internet.

11.7.3 Enable IPSec

Figure 197. shows the command `enable ipsec` to re-enable IPSec.

```
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
Center IPV4-IPsec config>EXIT
Center IPsec config>EXIT
```

Figure 197. Enable IPSec on the 2216 in the center

11.7.4 Reload

After enabling IPSec, you must restart the router to make the changes effective. When the router comes back up, IPSec and the policy are enabled. Figure 198 shows the reload of the router in the center:

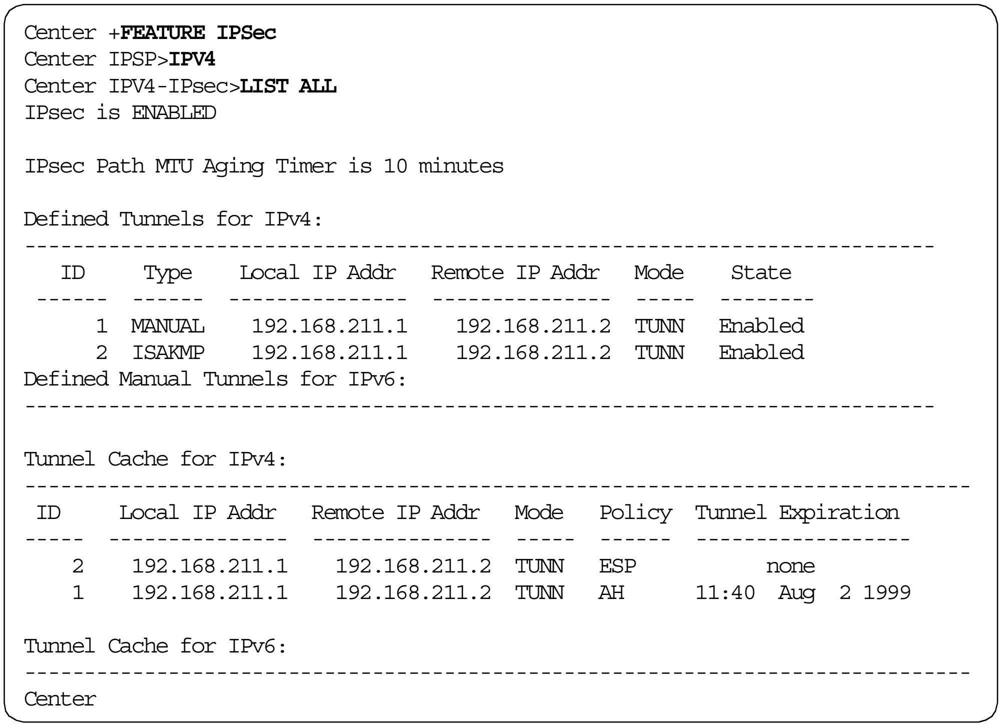
```
Center Policy config>EXIT
Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 198. Reload of the router in the center

11.7.5 Checking IPSec status

After restarting the router, we check to verify that IPSec and our tunnels are enabled. As shown in Appendix 199, “Testing DLSw with IPSec enabled” on page 229, you can use the `list all` command at the IPSec prompt.

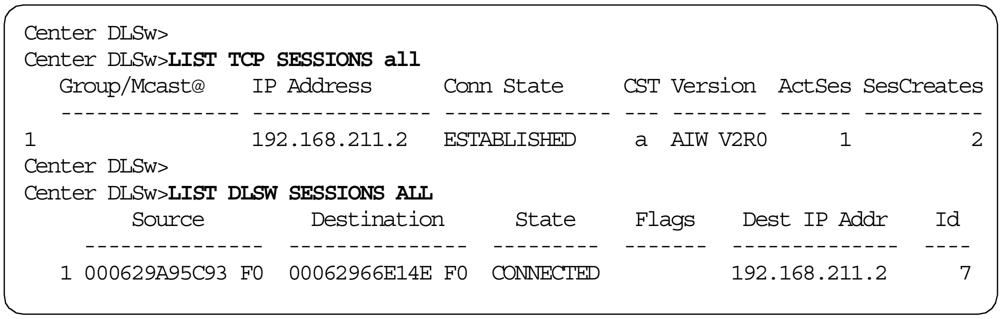
From Figure 199, we can see that IPSec is enabled and that the tunnel is enabled. Tunnel number 2 is the important one for DLSw as that is the one that all our DLSw traffic will go through:.



```
Center +FEATURE IPSec
Center IPSP>IPV4
Center IPV4-IPsec>LIST ALL
IPsec is ENABLED

IPsec Path MTU Aging Timer is 10 minutes

Defined Tunnels for IPv4:
---------------------------------------------------------------------------
   ID     Type    Local IP Addr   Remote IP Addr   Mode    State
 ------  ------  ---------------  ---------------  -----  --------
      1  MANUAL    192.168.211.1    192.168.211.2  TUNN   Enabled
      2  ISAKMP    192.168.211.1    192.168.211.2  TUNN   Enabled
Defined Manual Tunnels for IPv6:
---------------------------------------------------------------------------

Tunnel Cache for IPv4:
------------------------------------------------------------------------------
 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2    192.168.211.1    192.168.211.2  TUNN   ESP           none
    1    192.168.211.1    192.168.211.2  TUNN   AH      11:40  Aug  2 1999

Tunnel Cache for IPv6:
------------------------------------------------------------------------------
Center
```

Figure 199. Testing DLSw with IPSec enabled

Next, we verify that DLSw is still working with IPSec enabled. Figure 200 shows that the TCP and DLSw sessions are still active with IPSec enabled:



```
Center DLSw>
Center DLSw>LIST TCP SESSIONS all
   Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
   --------------- --------------- -------------- --- -------- ------ ----------
1                  192.168.211.2   ESTABLISHED     a  AIW V2R0      1          2
Center DLSw>
Center DLSw>LIST DLSW SESSIONS ALL
         Source         Destination      State     Flags    Dest IP Addr    Id
     ---------------  ---------------  ---------  -------  --------------  ----
   1 000629A95C93 F0  00062966E14E F0  CONNECTED           192.168.211.2      7
```

Figure 200. TCP and DLSw session with IPSec enabled

We test the DLSw connection by using the PCs in the center and in the branch to access each other’s disks. Be sure that IP on the PCs is disabled and that the NB protocol is used.

11.7.6 Check statistics

To make sure that the DLSw traffic is actually going through the IPSec tunnel, we check the IPSec statistics and see if the counters are increasing. Figure 201 on page 230 shows the statistics for tunnel number 2, the tunnel that handles the traffic originated by the routers that includes our DLSw traffic.

```
Center IPV4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         387            0           387        386992       193496       193496

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         359            0           359         42504            0        42504

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors   Exceed MTU
  ----------   ----------   ----------   ----------
           0            0            0            0

Center IPV4-IPsec>
```

Figure 201. Checking the IPSec statistics on the router in the center

Chapter 12. IP bridging through an IPSec tunnel

Multiple protocols except TCP/IP can be secured in an nonsecure network by our IPSec tunnel through the IP Bridging Tunnel feature of the IBM Nways 221X routers. The bridging tunnel (encapsulation) is another feature of the ASRT bridge software. By encapsulating packets in industry-standard TCP/IP packets, the bridging router can dynamically route these packets through large IP internetworks to the destination end stations.

End stations see the IP path (the tunnel) as a single hop, regardless of the network complexity. This helps overcome the usual 7-hop distance limit encountered in source routing configurations. It also lets you connect source-routing end stations across non-source-routing media like Ethernet networks.

This chapter shows you how to configure IP bridging over our VPN by using our IPSec tunnel defined in Chapter 10, “Connecting the data center to the branch office” on page 197*.*

12.1 Scenario descriptions

Figure 202 shows our sample network again with some additional MAC addresses that we use in this scenario:

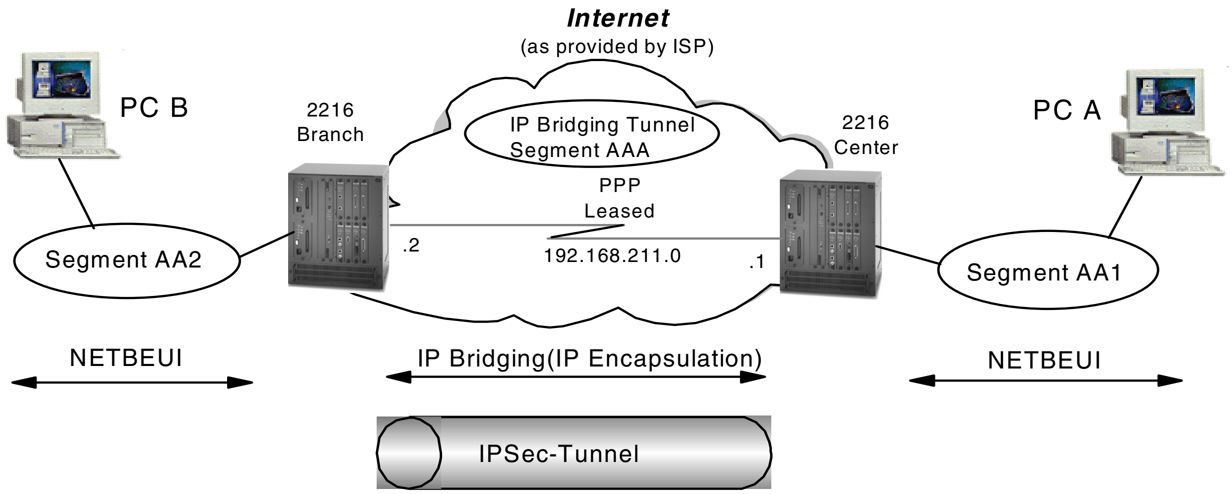


Figure 202. IP bridging tunnel through an IPSec tunnel

For this scenario, we want the Branch 2216 to be configured as a source route bridging (SRB) on both token-ring interface 0 (secure network side) and PPP interface 1(non-secure network).

We want the Branch 2216 PPP interface 1 to route IP. It has an IP address of 192.168.211.2 with a subnet mask of 255.255.255.0.

We want the Center 2216 also to be a source routing bridge (SRB) on the token-ring interface 0 and PPP interface 3 using our IP bridged tunnel.

We also want the Center 2216 PPP interface 0 to route IP. It has an IP address of 192.168.211.1 with a subnet mask of 255.255.255.0.

We have a PC configured with NetBIOS in the data center which is labeled PC A. Another PC, labeled PC B, is located in the branch office and is also configured with NetBIOS. From PC A we access a remote disk on PC B using the IP bridging tunnel which is passed through the IPSec tunnel.

12.2 IPSec and policy definitions

We defined an IPSec tunnel configured between the 192.168.211.1 and 192.168.211.2. We also defined a policy number 4, ike-pre-211-211, in Chapter 10, “Connecting the data center to the branch office” on page 197 for traffic between 192.168.211.1 and 192.168.211.2 which is router-to-router traffic to go through the tunnel.

In our scenario, since PC A sends NetBIOS read request without an IP header, using NETBEUI and Center 2216 router attaches the IP header with its PPP IP address 192.168.211.1 as a source and Branch 2216 PPP IP address 1192.168.211.2 as a destination, IP bridging packets are regarded as router-to-router traffic. Therefore, we use policy 4 with an IP tunnel for the IP bridging scenario.

As discussed in a previous chapter, we recommend that you make these configuration additions and test them first with the policy and IPSec feature disabled. This will help you with problem determination if you experience any problems in setting up the bridged tunnel.

12.3 Configuring the center router

Now we configure the router at the center.

12.3.1 Enabling bridge

The first step is to enable the Adaptive Source Route Transparent (ASRT) bridge function of the router. This command is shown in Figure 203 along with the command to list the ASRT bridge characteristics.

```
Center Config>PROTOCOL ASRT
Adaptive Source Routing Transparent Bridge user configuration
Center ASRT config>ENABLE BRIDGE
Center ASRT config>LIST BRIDGE

                Source Routing Transparent Bridge Configuration
                ==================================================

Bridge: Enabled                 Bridge Behavior: SRB
-------------------| SOURCE ROUTING INFORMATION |-------------------------------
Bridge Number: 00                      Segments: 1
Max ARE Hop Cnt: 14                     Max STE Hop cnt: 14
1:N SRB: Not Active              Internal Segment: 0x001
LF-bit interpret: Extended
-------------------| SR-TB INFORMATION |---------------------------------------
SR-TB Conversion: Disabled
TB-Virtual Segment: 0x000                   MTU of TB-Domain: 1470
-------------------| SPANNING TREE PROTOCOL INFORMATION |-----------------------
Bridge Address: Default              Bridge Priority: 32768/0x8000
SRB Bridge Address: Default              SRB Bridge Priority:32768/0x8000
STP Participation: IBM-SRB proprietary
-------------------| TRANSLATION INFORMATION |---------------------------------
FA<=>GA Conversion: Enabled                 UB-Encapsulation: Disabled
DLS for the bridge: Disabled
IPX Conversion: Disabled
Conversion Mode: Automatic
Ethernet Preference: IEEE-802.3
-------------------| PORT INFORMATION |----------------------------------------
Number of ports added:1
```

Figure 203. Enabling the bridge

12.3.2 Configuring bridge port

IP bridging in our scenario requires two bridge ports, one is token-ring interface 0 connected to PC A and the other is PPP interface 3 which will be configured as an IP bridging tunnel in 12.3.3, “Adding a bridging tunnel” on page 234.

Listing the bridge configuration as shown in Figure 203 is an easy way to get the currently configured bridge port and characteristics. We can see bridge port 1 added in Chapter 11, “Branch: data link switching over IPSec” on page 215 with SRB enabled from Figure 203. Remember the ASRT bridge behavior defaults to transparent bridging (STB) while source route translational bridging (SR-TB) is disabled. Therefore, we disabled the STB function and enabled SRB on port 1 and defined the segment number attaching to this token-ring port to be AA1 and the Center 2216 bridge number to be 1. This is shown in Figure 204:

```
Center ASRT config>ADD PORT
Interface Number [0]?
Port Number [1]?
Center ASRT config>DISABLE TRANSPARENT 1
Center ASRT config>ENABLE SOURCE-ROUTING 1
Segment Number for the port in hex(1 - FFF) [001]? aa1
his is screen.
```

Figure 204. Adding and configuring bridge port

Note: In case of connecting token-ring with Ethernet, enable source route translational bridging (SR-TB).

12.3.3 Adding a bridging tunnel

At this point, we define the IP bridging tunnel. This is done simply with the `add tunnel` command as shown in Figure 205. As a result, a new bridge port 2 for PPP interface 3 is added with a default behavior of transparent bridging (STB). We also disabled the STB function and enabled SRB on port 2 and defined the segment number attaching to this token-ring port to be AAA.

```
Center ASRT config>ADD TUNNEL
Port Number [2]?
Center ASRT config>DISABLE TRANSPARENT 2
Center ASRT config>ENABLE SOURCE-ROUTING 2
Segment Number for the port in hex(1 - FFF) [001]? aaa
Center ASRT config>LIST BRIDGE

            Source Routing Transparent Bridge Configuration
            ================================================
Bridge: Enabled                  Bridge Behavior:SRB
-------------------| SOURCE ROUTING INFORMATION |-------------------------------
Bridge Number: 00                      Segments: 2
Max ARE Hop Cnt: 14                      Max STE Hop cnt: 14
1:N SRB: Not Active               Internal Segment: 0x001
LF-bit interpret: Extended
-------------------| SR-TB INFORMATION |---------------------------------------
SR-TB Conversion: Disabled
TB-Virtual Segment: 0x000                  MTU of TB-Domain: 1470
-------------------| SPANNING TREE PROTOCOL INFORMATION |-----------------------
Bridge Address: Default               Bridge Priority: 32768/0x8000
SRB Bridge Address: Default               SRB Bridge Priority:32768/0x8000
STP Participation: IBM-SRB proprietary
-------------------| TRANSLATION INFORMATION |---------------------------------
FA<=>GA Conversion: Enabled                UB-Encapsulation: Disabled
DLS for the bridge: Disabled
IPX Conversion: Disabled
Conversion Mode: Automatic
Ethernet Preference: IEEE-802.3
-------------------| PORT INFORMATION |----------------------------------------
Number of ports added: 2
Port: 1      Interface: 0      Behavior: SRB Only   STP: Enabled
Port: 2      Interface: Tunnel      Behavior: SRB Only   STP: Enabled
```

Figure 205. Adding a bridging tunnel

We need to specify the destination IP address of the other end of the IP bridging tunnel. This is shown in Figure 206. The IP address of the other end of the IP bridging tunnel is the PPP interface address and also the internal IP address of the Branch 2216 router.

Note: It is very important to remember we use the policy of which source and destination address is PPP interface addresses of both routers so that this router-to-router traffic packets in the IP bridging tunnel can be processed by IPSec.

```
Center ASRT config>TUNNEL
Tunnel interface configuration
Center TNL config>ADD ADDRESS
Enter the address to be added [0.0.0.0]? 192.168.211.2
Center TNL config>LIST ALL
IP Tunnel Addresses

    192.168.211.2 his is screen.
```

Figure 206. Defining destination IP address of bridging tunnel

12.4 Configuring the branch router

We need to do the same steps almost exactly to configure the 2216 in branch office for our bridging tunnel. In this section we take you step by step through this process.

12.4.1 Enabling bridge

Again, the first step is to enable the bridge and list the configuration so that we can see the port numbers that have been defined. This is illustrated in Figure 207:

```
Branch Config>PROTOCOL ASRT
Adaptive Source Routing Transparent Bridge user configuration
Branch ASRT config>ENABLE BRIDGE
Branch ASRT config>LIST BRIDGE

              Source Routing Transparent Bridge Configuration
              ===============================================

Bridge: Enabled                 Bridge Behavior:SRB
-------------------| SOURCE ROUTING INFORMATION |-------------------------------
Bridge Number: 01                      Segments: 1
Max ARE Hop Cnt: 14                      Max STE Hop cnt: 14
1:N SRB: Not Active              Internal Segment: 0x002
LF-bit interpret: Extended
-------------------| SR-TB INFORMATION |----------------------------------------
SR-TB Conversion: Disabled
TB-Virtual Segment: 0x000                   MTU of TB-Domain: 1470
------------------| SPANNING TREE PROTOCOL INFORMATION |------------------------
Bridge Address: Default              Bridge Priority: 32768/0x8000
SRB Bridge Address: Default              SRB Bridge Priority:32768/0x8000
STP Participation: IBM-SRB proprietary
-------------------| TRANSLATION INFORMATION |----------------------------------
FA<=>GA Conversion: Enabled                 UB-Encapsulation: Disabled
DLS for the bridge: Disabled
IPX Conversion: Disabled
Conversion Mode: Automatic
Ethernet Preference: IEEE-802.3
-------------------| PORT INFORMATION |-----------------------------------------
Number of ports added:1
Port: 1      Interface: 0      Behavior: SRB Only   STP: Enabled
```

Figure 207. Enabling the bridge

12.4.2 Configuring bridge ports

Again IP bridging in our scenario requires two bridge ports, one is token-ring interface 0 connected to PC B and the other is PPP interface 3 which will be configured as an IP bridging tunnel in 12.4.3, “Adding a bridging tunnel” on page 236.

We also can see bridge port 1 added in Chapter 11, “Branch: data link switching over IPSec” on page 215 with SRB enabled from Figure 207. Disable the STB function and enable SRB on port 1 and define the segment number attaching to this token-ring port to be AA2. This is shown in Figure 208:

```
Branch ASRT config>DISABLE TRANSPARENT 1
Branch ASRT config>ENABLE SOURCE-ROUTING 1
Segment Number for the port in hex(1 - FFF) [001]? aa2
```

Figure 208. Adding and configuring bridge port

12.4.3 Adding a bridging tunnel

Next, we add the IP bridging tunnel port. This is illustrated in Figure 209. Note that the tunnel port is STB by default. We also disabled the STB function and enabled SRB on port 2 and defined the segment number as AAA since the 2216 regards IP bridging tunnel as the same segment.

```
Branch ASRT config>ADD TUNNEL
Port Number [2]?
Branch ASRT config>DISABLE TRANSPARENT 2
Branch ASRT config>ENABLE SOURCE-ROUTING 2
Segment Number for the port in hex(1 - FFF) [001]? aaa
Branch ASRT config>LIST BRIDGE

              Source Routing Transparent Bridge Configuration
              ===============================================

Bridge: Enabled                Bridge Behavior:SRB
-------------------| SOURCE ROUTING INFORMATION |------------------------------
Bridge Number: 01                     Segments: 2
Max ARE Hop Cnt: 14                     Max STE Hop cnt: 14
1:N SRB: Not Active            Internal Segment: 0x002
LF-bit interpret: Extended
-------------------| SR-TB INFORMATION |---------------------------------------
SR-TB Conversion: Disabled
TB-Virtual Segment: 0x000                  MTU of TB-Domain: 1470
-------------------| SPANNING TREE PROTOCOL INFORMATION |----------------------
Bridge Address: Default              Bridge Priority: 32768/0x8000
SRB Bridge Address: Default              SRB Bridge Priority:32768/0x8000
STP Participation:       IBM-SRB proprietary
-------------------| TRANSLATION INFORMATION |---------------------------------
FA<=>GA Conversion: Enabled                UB-Encapsulation: Disabled
DLS for the bridge: Disabled
IPX Conversion: Disabled
Conversion Mode: Automatic
Ethernet Preference: IEEE-802.3
-------------------| PORT INFORMATION |----------------------------------------
Number of ports added:2
Port: 1      Interface: 0      Behavior: SRB Only   STP: Enabled
Port: 2      Interface: Tunnel      Behavior: SRB Only   STP: Enabled
```

Figure 209. Adding a bridge tunnel port

Next, we add the destination IP address of the other side of the tunnel. This is illustrated in Figure 210:

```
Branch ASRT config>TUNNEL
Tunnel interface configuration
Branch TNL config>ADD ADDRESS
Enter the address to be added [0.0.0.0]? 192.168.211.1
Branch TNL config>LIST ALL
IP Tunnel Addresses

    192.168.211.1
```

Figure 210. Configuring a bridging tunnel

Finally, we reload the router to activate the configuration. This is illustrated in Figure 211:

```
Branch Config>WRITE
Config Save: Using bank A and config number 2
Branch Config>
Branch *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 211. Reloading the router

12.5 Testing IP bridging with IPSec disabled

Now, we test the IP bridging tunnel configuration to make sure that it is working like we intended. PC A accesses PC B’s shared directory with NetBIOS using IP bridging tunnel without IPSec.

12.6 Testing IP bridging with IPSec enabled

Now we re-enable policy, IPSec and reload the router. Note that policy number 4 on Center 2216 is the one that we defined to carry the router-to-router traffic through the IPSec tunnel. Figure 212 shows enabling IPSec and policy on the Center 2216. Use the same steps in the Branch 2216.

12.6.1 Enable IPSec and the policy

First you have to enable IPSec.

```
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
Center IPV4-IPsec config>EXIT
Center IPsec config>EXIT
Center Config>FEATURE Policy
IP Network Policy configuration
Branch Policy config>ENABLE POLICY
Enter the Name of the Policy to enable (? for a List)
[?]?
1: ipsec_man_101_102
2: ike-pre-101-102
3: ike-pre-3-100
4: ike-pre-211-211
Number of policy [1]? 4
```

Figure 212. Enabling IPSec and policy on center 2216

12.6.2 List IPSec statistics

Finally, to be sure that the IP bridging traffic is going through the IPSec tunnel, we list the IPSec statistics and check to see that the counters are increasing. This is shown in Figure 213:

```
Branch *TALK 5
CGW Operator Console
Branch +FEATURE IPSec
Branch IPSP>IPV4
Branch IPV4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

                  Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
  194            0           194         48096        24048        24048

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
  153            0           153         19496            0        19496

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
  0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors   Exceed MTU
  ----------   ----------   ----------   ----------
  0            0            0            0
```

Figure 213. Checking the IPSec statistics

Chapter 13. Branch: APPN through an IPSec tunnel

Advanced Peer-to-Peer Networking (APPN) is another very important protocol to transport across our virtual private network.

Therefore, now we describe a scenario where an APPN/HPR peer in the branch wants to communicate with an APPN/HPR peer in the center. Unlike in other scenarios where we use DLSw and/or TN3270e for similar purposes we will show here the use of Enterprise Extender.

The Enterprise Extender feature of MRS/MAS allows us to transport our APPN/HPR traffic over an IP backbone, in this case, the Internet. Since Enterprise Extender (also called HPR over IP) uses IP encapsulation, we can use IPSec to protect these packets as they traverse the public network.

13.1 Description of the scenario

In our scenario (see Figure 214), we have an APPN end node (EN) in the branch office (brPC) that needs to communicate with another EN in the data center (PCctr). The 2216 router in the branch (CPNAME BR2216) is configured as an APPN network node (NN) and is providing APPN directory services for device brPC. The 2216 in the center (CPNAME VPN2216A) is also configured as an NN and is providing directory services for the device PCctr.

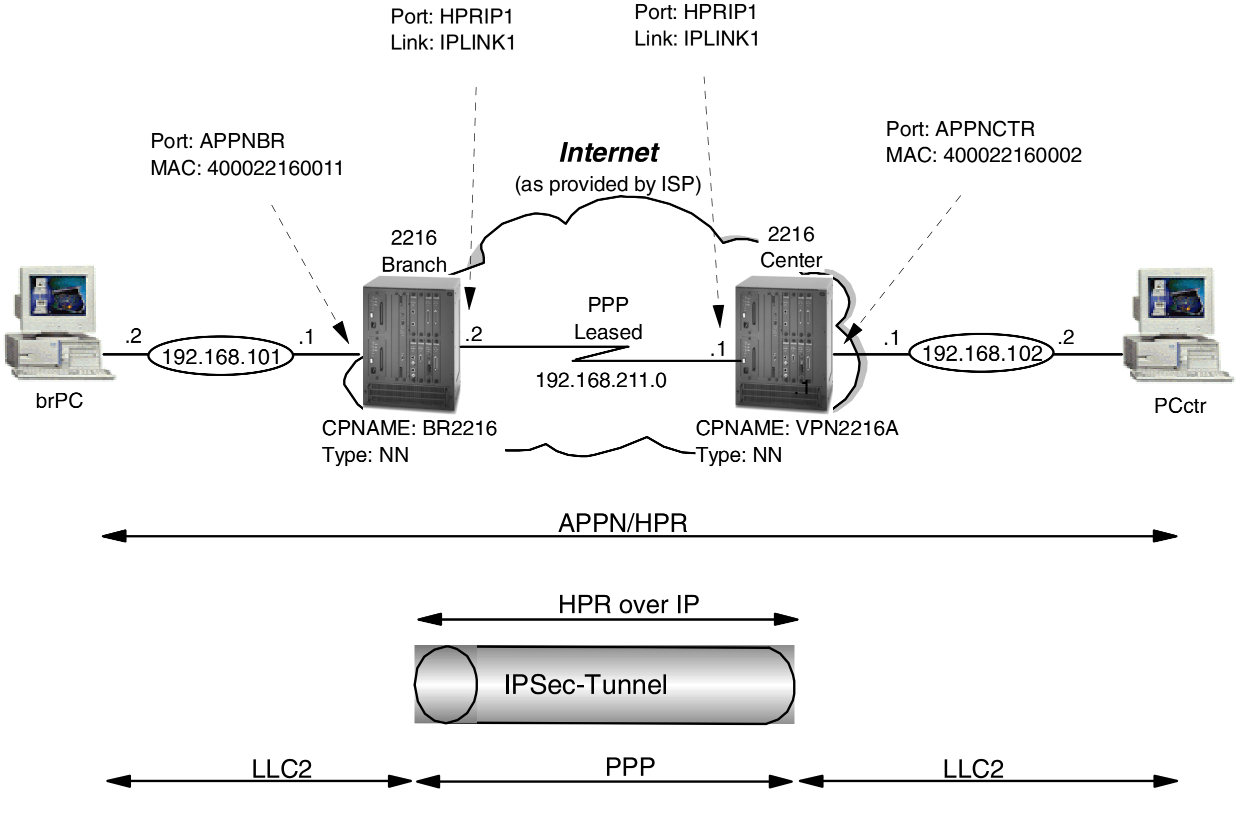


Figure 214. APPN/HPR using Enterprise Extender (HPR over IP) through an IPSec tunnel

The APPN traffic comes into the branch router as an LLC frame over the token-ring interface (which is also defined as an APPN port). The branch router, acting as an APPN network node, decides to route the traffic to its destination over the HPR over IP port. The HPR over IP engine in the router encapsulates the APPN LLC frame into an IP packet (using UDP) and then passes it to the IP routing element. IP then sends the packet to the other token-ring interface (our interface to the public network).

At this point, the outbound packet filter that we define on the token-ring interface redirects the packet to the IPSec engine where it is processed for AH and ESP headers before being sent out on the physical interface.

A similar process occurs in the reverse direction. As the IP packet reaches the end of the tunnel, it gets decapsulated and decrypted by the IPSec engine, then passed to the IP stack where it is determined that it must be directed to the HPR over IP port in the router. The HPR over IP function strips off the IP and UDP headers and passes the APPN LLC frame to APPN. The APPN network node routes the frame to its destination.

We use the IPSEC installation from Chapter 31, “Basic router configuration with MRS/AIS/MAS V.3.3” on page 567 to securely transport this traffic, that is, we use pre-shared keys and we have a tunnel between the two routers in the branch and center.

With the support for setting the IP precedence bits that became available in MRS/MAS Version 3.1, you can map the SNA priority (for example, HPR) of these connections into the IP packets.

This priority is preserved even if you are using IPSec tunnel mode, where the original packet is completely encapsulated in another one.

As you can see from Figure 214 on page 241, we put the SNA client not in the production LAN of the branch/center but in the LAN that is directly attached to the routers. With this scenario we avoid bridging APPN/HPR frames over the firewall.

We use two Windows PCs with eNetwork Personal Communications as our APPN end nodes. These machines are labeled brPC and PCctr in the diagram. We show how to configure these two end nodes.

13.2 IPSec and policy

As discussed in 10.2.4, “Tunnel mode versus transport mode VPN connection” on page 200, we could use either an IPSec tunnel mode tunnel or a transport mode tunnel. One reason a company would use tunnel mode versus transport mode is to hide internal IP addresses used in the network. Another might be to use unregistered IP addresses. When packets use tunnel mode, they are encapsulated with a new IP header and the original source and destination addresses are no longer visible.

However, in the case of APP/NHPR over IP, the IP traffic originates in the router where the APPN/HPR traffic is encapsulated and terminates in the router where it is decapsulated. In our scenario, the routers where the APPN/HPR traffic is encapsulated are the same routers used as our IPSec tunnel endpoints. In other words, only the Internet addresses of these two routers will appear in the HPR over IP packets. Using tunnel mode in this situation does not offer any advantages over transport mode in terms of hiding the source and destination IP addresses of the sender and receiver.

For our scenario, we used the existing tunnel to carry our APPN traffic (as well as all the other router-to-router traffic). This tunnel was defined in 10.3.3, “Router-to-router traffic” on page 207.

13.3 Definition of the router in the center

In this section we describe the necessary steps to set up the center router.

13.3.1 Preparation

Perform the initial steps as outlined below before you set up the VPN scenario.

13.3.1.1 Load encryption package

Load the encryption package on the 2216 unless it has already been done:

```
Center Config>LOAD ADD PACKAGE encryption
encryption package configured successfully
This change requires a reload.
Center Config>WRITE
Config Save: Using bank B and config number 4
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 215. Loading the encryption package on the IBM 2216 router in the center

The load of the encryption package requires a reboot of the machine.

13.3.1.2 Define internal IP address

We define an internal IP address which will be the endpoint of our HPR over IP network. In our case we use the IP address of the PPP link to the Internet/ISP.

```
Center IP config>SET INTERNAL-IP-ADDRESS
Internal IP address [172.16.220.253]? 192.168.211.1
Center IP config>EXIT
```

Figure 216. Setting the internal IP address on the router in the central site

13.3.1.3 Load APPN package

Before we can configure APPN on the 2216, we first have to load the APPN package. This is shown in Figure 217 on page 244. Once this command has been issued, the APPN module will be loaded during each subsequent IPL of the router.

If you are using a 2210 you must ensure that you have an operational code that supports APPN.

Pre-packed operational code can be downloaded from the IBM networking home page at:

http://www.networking.ibm.com/

and select support / 2210 / download / 2210 operational code

The operational code is at:
http://www.networking.ibm.com/support/code.nsf/2210oper?OpenView

```
Center Config>LOAD ADD PACKAGE appn
appn package configured successfully
This change requires a reload.
Center Config>EXIT
You are already at the top of the Configuration Menus.
(To return to the MOS Operator Console prompt (*), press Control-P)
Center Config>
Center *TALK 6
Center Config>WRITE
Config Save: Using bank A and config number 2
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
***
*** DISCONNECT
*** time 06:43:59
***
```

Figure 217. Loading the APPN package on the router in the central site

The addition of the APPN package requires a reload.

13.3.2 APPN definitions

Ensure that the APPN package is loaded on the 2216.

13.3.2.1 Defining the APPN node

After the router comes back up, we go to the talk 6 APPN protocol menus and set the APPN node characteristics.

This is done using the set node command as shown in Figure 218:

```
Center Config>PROTOCOL APPN
Center APPN config>SET NODE
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) []? USIBMRA
Control point name (Max 8 characters) []? VPN2216A
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
```

Figure 218. Defining the APPN node on the 2216 in the center

As you can see, the only parameters that are absolutely necessary are the APPN CP name and the Network ID. The other parameters can be left at their default values.

13.3.2.2 Add APPN port for HPR over IP to the branch

The next step is to add the APPN ports that will be used to carry our APPN traffic.

In Figure 219, we add an HPR over IP port to the branch:

.

```
Center APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Enable IP Precedence: (Y)es (N)o [N]?
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 219. Adding an APPN port for HPR over IP to the branch

Again, we use the defaults for most of the parameters. The critical one is the port type (I for HPR over IP). Note that you do not need to specify an interface number because there is only one HPR over IP port per router. We also give it a port name that we can easily recognize on the monitoring console.

One question on this screen deals with the IPv4 precedence bits. If you respond yes to this question to enable setting of the precedence bits, then the 3 precedence bits in the TOS field of the IPv4 header will be set based on the HPR priority of the traffic. This allows you to preserve your SNA priorities using the Bandwidth Reservation System (BRS) feature even on encrypted packets. Please see *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

13.3.2.3 Add link to 2216 in branch

Next, we add a link station on the newly defined HPR over IP port. This is shown in Figure 220 on page 246.

```
Center APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? HPRIP1
Station name (Max 8 characters) [ ]? IPLINK1
Activate link automatically (Y)es (N)o [Y]? y
        IP address of adjacent node  [0.0.0.0]? 192.168.211.2
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type  [0]? 1
        TG Number (0-20) [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Center APPN config>
```

Figure 220. Adding a link station for the HPR over IP link

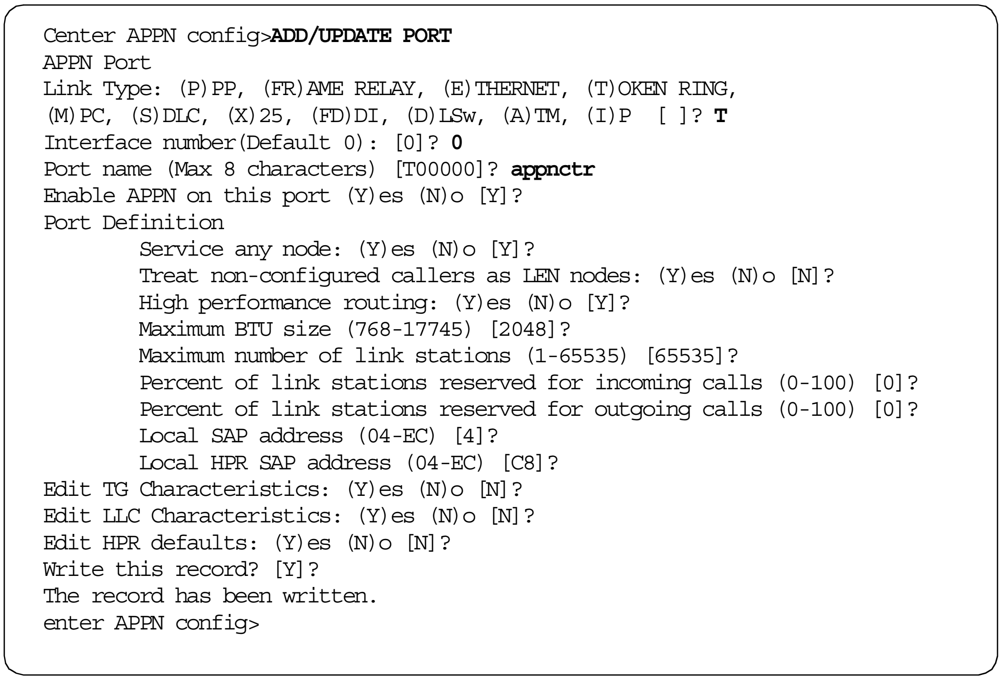
By specifying the port name for this link station, the router knows that it is an HPR over IP port. Therefore, it knows to prompt you for an IP address as opposed to a MAC address that it would need if we were defining a link station for a LAN port.

The IP address that we specify is the *internal address* of the router in the branch office. This is the endpoint of our HPR over IP network. The other end of the HPR over IP link is always at the router that will decapsulate the packets and *not* the next hop router in the path. Intermediate routers, if any, merely perform IP routing on the encapsulated packets.

The router internal address is configured from the talk 6 `protocol ip` prompt.

13.3.2.4 Add APPN port for HPR over IP to local token-ring

The next step is to add an APPN port for the local token-ring in the center (Figure 221 on page 247).



```
Center APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? T
Interface number(Default 0): [0]? 0
Port name (Max 8 characters) [T00000]? appnctr
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-65535) [65535]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
enter APPN config>
```

Figure 221. Adding an APPN port for HPR over IP for the local token-ring

We do not need to define any link stations on this port as the workstations (APPN end nodes) will create implicit links when they initialize with their network node (in this case, the 2216 in the center itself).

13.3.3 List the APPN configuration

Now we list the complete APPN configuration as shown in Figure 222 on page 248. The 2216 in the branch and in the center are providing automatic network routing (ANR) services as an intermediate APPN node.

In this configuration, we only make use of the token-ring port (APPNCTR) and the enterprise extender port (HPRIP1). The MPC port (MPC00005) is not used.

```
Center APPN config>LIST ALL
NODE:
       NETWORK ID: USIBMRA
       CONTROL POINT NAME: VPN2216A
       XID: 00000
       APPN ENABLED: YES
       BREX OR BORDER NODE: NEITHER
       MAX SHARED MEMORY: 5108
       MAX CACHED: 4000
DLUR:
       DLUR ENABLED: NO
       PRIMARY DLUS NAME:
CONNECTION NETWORK:
            CN NAME       LINK TYPE  PORT INTERFACES
       -------------------------------------------------------------
COS:
       COS NAME
       --------
         #BATCH
        #BATCHSC
        #CONNECT
         #INTER
        #INTERSC
         CPSVCMG
        SNASVCMG
MODE:
        MODE NAME  COS NAME
       ---------------------
PORT:
         INTF     PORT      LINK      HPR    SERVICE   PORT
        NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
       ------------------------------------------------------
        65535    HPRIP1     HPR_IP    YES      YES      YES
            0   APPNCTR   IBMTRNET    YES      YES      YES
            5  MPC00005       MPC+    YES      YES      YES
STATION:
        STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
         NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
       ------------------------------------------------------------
        IPLINK1   HPRIP1     192.168.211.2     YES     YES       0
         TOVTAM MPC00005      000000000000     YES     YES       0
LU NAME:
            LU NAME        STATION NAME          CP NAME
       ------------------------------------------------------------
Center APPN config>
```

Figure 222. Listing the APPN configuration

13.3.4 Activate the APPN connection

It is not necessary to restart the router at this point. To activate the changes to the APPN configuration, we simply issue the `activate` command from the `APPN Config>` prompt. This is illustrated in Figure 223:

```
Center APPN config>ACTIVATE_NEW_CONFIG
```

Figure 223. Activating the new APPN configuration in the center

This completes the steps necessary to configure the 2216 in the center for this scenario.

13.4 Definition on the router in the branch

This section takes you step by step through the APPN definition of the 2216 in the branch. The steps are almost identical to the ones for configuring the 2216 in the data center.

13.4.1 Preparation

As on the 2216 in the center you have to:

- Load the encryption package (see Figure 215 on page 243).
- Define the internal IP address (see Figure 216 on page 243).
- Load the APPN package (see Figure 217 on page 244).

13.4.2 APPN definitions

13.4.2.1 Defining the APPN node

First we set the APPN node characteristics. This is shown in Figure 224:

```
Branch *TALK 6
Gateway user configuration
Branch Config>PROTOCOL APPN
Branch APPN config>SET NODE
Enable APPN (Y)es (N)o [Y]?Y
Network ID (Max 8 characters) [USIBMRA]? USIBMRA
Control point name (Max 8 characters) [NN2216]? br2216
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Branch APPN config>
```

Figure 224. Setting the APPN node characteristics for the branch router

Note that the network ID must match at both ends of the HPR over IP link

13.4.2.2 Add APPN port for HPR over IP to the center

Next we add an HPR over IP port. This is shown in Figure 225 on page 250:

```
Branch APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [1]?
        Enable IP Precedence: (Y)es (N)o [N]? y
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [10]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Branch APPN config>EXIT
```

Figure 225. Adding an APPN port for the WAN interface on the 2216 branch router

Note that we use the same port name as we used for the 2216 in the center. This is just for our convenience as the port name is only used at the router where it is defined and has no correlation to any other port names on any other routers.

Now that we have the port defined, the next step would normally be to define a link station to the next hop APPN node. However, in this case, it is not necessary because an implicit link will be created when the 2216 in the data center establishes a connection with this 2216 in the branch office.

13.4.2.3 Add APPN port for HPR over IP to the center

Next, we add a token-ring APPN port for the LAN-connected end nodes (brPC) to connect to the 2216 as their NN server. This is shown in Figure 226 on page 251.

```
Branch IP config>
Branch Config>PROTOCOL APPN
Branch APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? T
Interface number(Default 0): [0]? 0
Port name (Max 8 characters) [T00000]? APPNBR
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-65535) [65535]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Branch APPN config>EXIT
Branch Config>
```

Figure 226. Adding an APPN port for the LAN interface on the 2216 branch router

We do not need to define any link stations on this port as the workstations (APPN end nodes) will create implicit links when they initialize with their network node (in this case, the 2216 in the branch itself).

This completes the APPN definition on the branch router.

13.4.3 Activate the APPN definitions

We activate the new configuration and restart the gateway as shown in Figure 227:

```
Branch APPN config>ACTIVATE_NEW_CONFIG
Branch APPN config>EXIT
Branch Config>WRITE
Config Save: Using bank A and config number 2
Branch Config>
Branch *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
***
*** DISCONNECT
*** time 07:20:47
***
```

Figure 227. Enabling the APPN configuration in the branch router

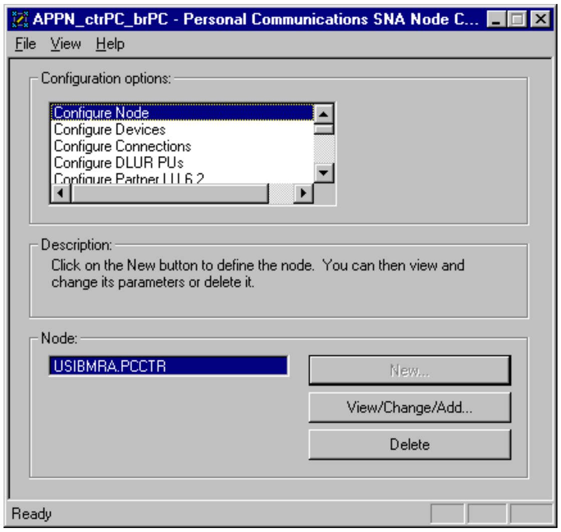
13.5 Definition on the client PC

We used a Windows 95 Client with eNetwork Personal Communications Version 4.2 as SNA/APPN client.

To configure you have to enter the following in the menus of the SNA node configuration.

You have to configure:

- The node (Figure 228)
- The device (Figure 230 on page 253)
- The connection (Figure 231 on page 254)



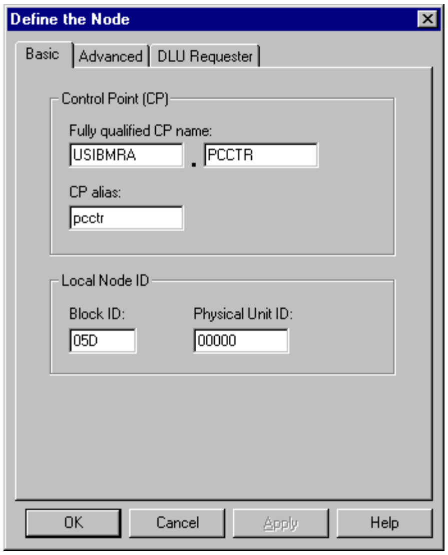
Click on the New button to define the node. You can then view and change its parameters or delete it.

Node: USIBMRA.PCCTR

Figure 228. Configuring the node of an APPN client

13.5.0.1 Basic node definitions for the PC in the center

In the basic definitions of the APPN node you specify the CP name. It is only necessary that the NetID matches the other NetID definitions in your network.



Define the Node

Basic | Advanced | DLU Requester

Control Point (CP)

Fully qualified CP name: USIBMRA . PCCTR

CP alias: pcctr

Local Node ID

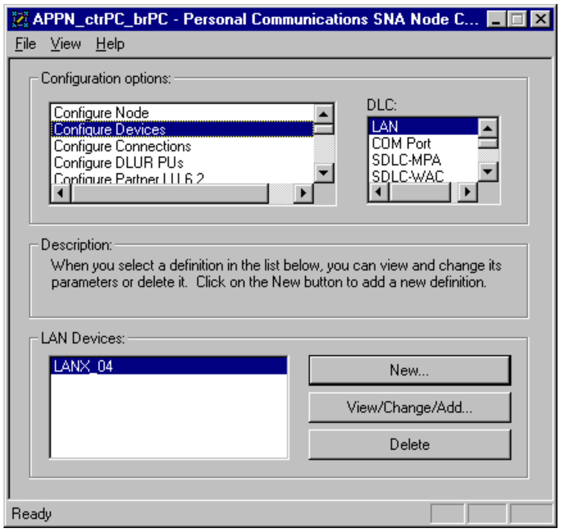
Block ID: 05D

Physical Unit ID: 00000

Figure 229. Basic definitions for an APPN node

13.5.0.2 Defining the APPN devices for the PC in the center

Defining the APPN device you can work with the defaults (Figure 230). Ensure that the correct LAN adapter is used (Folder Basic).



APPN_ctrPC_brPC - Personal Communications SNA Node C...

Configuration options:

- Configure Node
- Configure Devices
- Configure Connections
- Configure DLUR PUs
- Configure Partner LU 6.2

DLC:

- LAN
- COM Port
- SDLC-MPA
- SDLC-WAC

Description:

When you select a definition in the list below, you can view and change its parameters or delete it. Click on the New button to add a new definition.

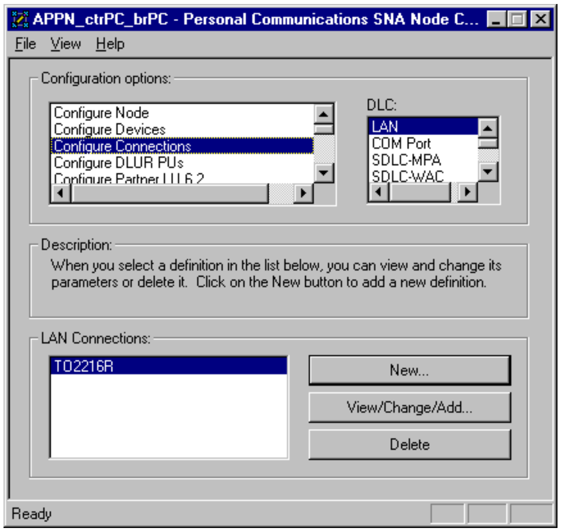
LAN Devices:

LANX_04

Figure 230. Defining the APPN device

13.5.0.3 Definition of the connection for the PC in the center

After configuring the devices you configure the connections (see Figure 231):

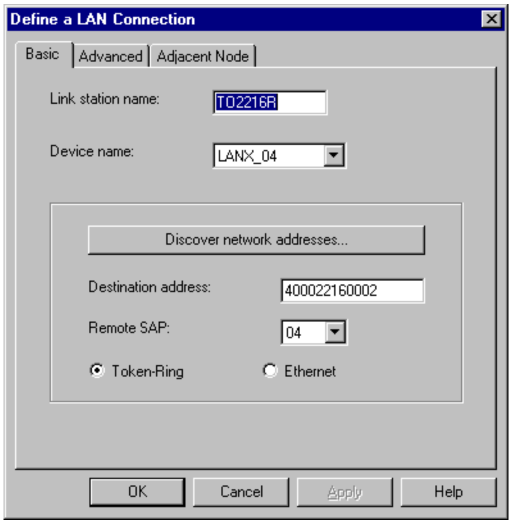

APPN_ctrPC_brPC - Personal Communications SNA Node C...

When you select a definition in the list below, you can view and change its parameters or delete it. Click on the New button to add a new definition.

LAN Connections: TO2216R

Figure 231. Defining the APPN connections

In the basic definitions you specify a link station name and the destination address which is the MAC address of the 2216 LAN interface of the local LAN. (Figure 232).


Define a LAN Connection

Link station name: TO2216R

Device name: LANX_04

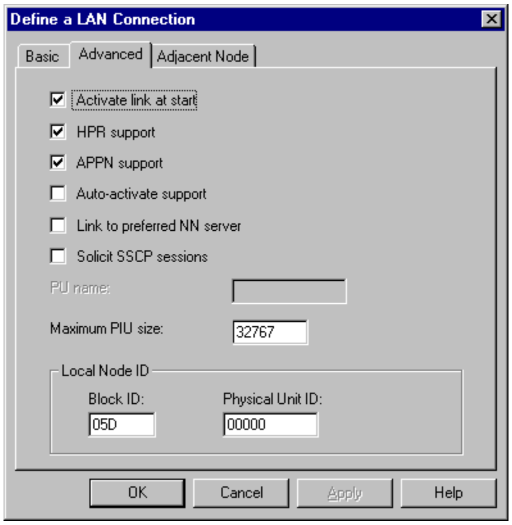
Destination address: 400022160002

Remote SAP: 04

● Token-Ring ○ Ethernet

Figure 232. Basic definitions for the APPN connections

In the advanced definitions you can specify whether APPN or HPR is used (see Figure 233):


Define a LAN Connection

☑ Activate link at start
☑ HPR support
☑ APPN support
□ Auto-activate support
□ Link to preferred NN server
□ Solicit SSCP sessions

PU name:

Maximum PIU size: 32767

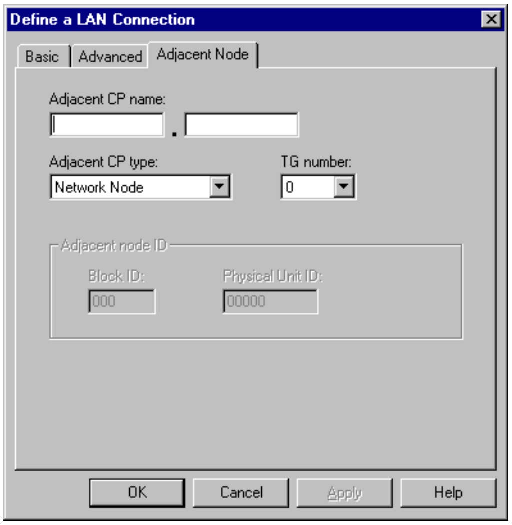
Local Node ID

Block ID: 05D

Physical Unit ID: 00000

Figure 233. Advanced definitions for the APPN connections

In the adjacent node definitions you specify the adjacent node (2216) as an APPN Network Node (see Figure 234):


Define a LAN Connection

Adjacent CP name: .

Adjacent CP type: Network Node

TG number: 0

Adjacent node ID

Block ID: 000

Physical Unit ID: 00000

Figure 234. Adjacent node definitions for the APPN connections

13.6 Testing APPN (IPSec disabled)

At this point, the configuration of both routers is complete. IPSec and the IPSec policies will be temporarily disabled. Before enabling IPSec and the policies we need to test the APPN function.

We used on both sides a Windows 95 Client with eNetwork Personal Communications Version 4.2 as the APPN client. These clients are connected to the token-ring segment of the 2216 in the center or branch.

13.6.1 Checking the status of IPSec and policies

The current IPSec status can be checked with the following command:

```
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
Center IPV4-IPsec config>
```

Figure 235. Checking the current status of IPSec

The current status of the policies can be checked with the following command:

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled   : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-act1
       .......
Center Policy Config>
```

Figure 236. Checking the current status of the policies

13.6.2 Disable IPSec and the policies

Before testing the APPN connection IPSec should be temporarily disabled on the router in the center and on the router in the branch. You have to disable the policy (Figure 237) and IPSec (Figure 238 on page 257).

With the command `disable policy` you can disable the policies:

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy Config>
Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
 [?]?
        1: ike-pre-101-102
        2: ike-pre-3-100
        3: ike-pre-211-211
Number of policy [1]?
```

Figure 237. Disabling the policies on the router in the center

The command `disable IPSec stop` stops IPSec. The current status of IPSec can be seen with the command `list status.`

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>DISABLE IPSEC STOP
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
```

Figure 238. Disabling IPSec on the router in the center

13.6.3 Check APPN node status

We check the APPN node definitions as shown in Figure 239:

```
Center APPN config>LIST NODE
Node:
       Network ID: USIBMRA
       Control point name: VPN2216A
       XID: 00000
       APPN enabled: YES
       Branch extender: NO
       Permit search for unregistered LUs: NO
       Border Node: No
       Route addition resistance: 128
       Use enhanced BATCH COS: Y
       Use enhanced BATCHSC COS: Y
       Use enhanced INTER COS: Y
       Use enhanced INTERSC COS: Y
       Max shared memory: 5108
       Max cached: 4000
       Percent buffer memory: 11
Center APPN config>
```

Figure 239. Checking the APPN node definitions

13.6.4 Check the APPN links

We check the status of the APPN ports on the 2216 in the center. Figure 240 shows that the port to the 2216 in the branch (port 6) and the port to the local token-ring (port 0) are in the active (ACT_PORT) state:

```
Center APPN >LIST LINK_INFORMATION
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
========================================================================
 IPLINK1      HPRIP1     6     USIBMRA.BR2216   NN    ACTIVE     ACT_LS
     @@0     APPNCTR     0     USIBMRA.PCCTR    EN    ACTIVE     ACT_LS
```

Figure 240. Listing and checking port information

From the figure, you can see that an end node (USIBMRA.PCCTR) is connected over the token-ring port (APPNCTR) through an implicit link (@@0).

Note: If the HPR over IP link does not become active, first re-check your configuration. If the configuration looks correct, try and ping each router's internal address: first from the router to its own internal address, then to the other router's internal address. Repeat this test from the other router. The internal address of each router must be reachable for the HPR over IP link to function.

The status of each port can be seen in more detail with the following command:

```
Center APPN config>LIST PORT
PORT:
Port name (Max 8 characters) [ ]? hprip1
        Interface number: 65535
       PORT enable: YES
       Service any node: YES
       Treat non-configured caller as LEN node: NO
       Link Type: HPR_IP
       MAX BTU size: 1469
       MAX number of Link Stations: 65535
       Percent of link stations reserved for incoming calls: 0
       Percent of link stations reserved for outgoing calls: 0
       UDP port number for XID exchange: 12000
       UDP port number for low priority traffic: 12004
       UDP port number for medium priority traffic: 12003
       UDP port number for high priority traffic: 12002
       UDP port number for network priority traffic: 12001
       IP Network Type (0 = CAMPUS, 1 = WIDEAREA): 0
       LDLC Retry Count: 3
       LDLC Timer Period: 15
       Enable IP Precedence: YES       Branch uplink: NO
       Subnet visit count: 3
       Adjacent node subnet affiliation: Negotiable
       Cost per connect time: 0
       Cost per byte: 0
       Security:(0 = Nonsecure, 1 = Public Switched Network
          2 = Underground Cable, 3 = Secure Conduit,
          4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
       Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
          3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
       Effective capacity: 75
       First user-defined TG characteristic: 128
       Second user-defined TG characteristic: 128
       Third user-defined TG characteristic: 128
Center APPN config>
```

Figure 241. Checking the status of the port to the 2216 in the branch

13.6.5 List the APPC sessions

Finally, we verify that there is an APPC session between the branch router and VTAM. This is done from talk 5 by listing the active APPC sessions as shown in Figure 242. (Remember VTAM is USIBMRA.RA03M.)

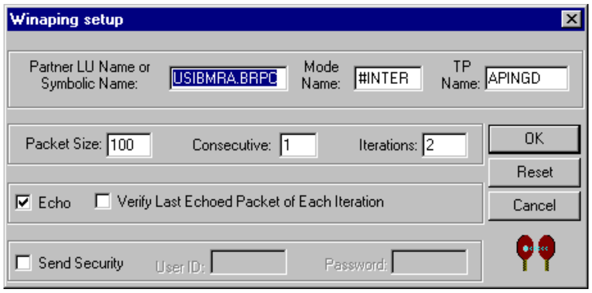
```
Center APPN >LIST APPC_SESSIONS
LU Name             Mode  Type  FSM
=====================================
USIBMRA.BR2216    CPSVCMG  Pri  ACT
USIBMRA.BR2216    CPSVCMG  Sec  ACT
Center APPN >
```

Figure 242. Listing the APPC sessions before enabling IPSec and policies

13.6.6 Testing the connection

We used on both sides a Windows 95 Client with eNetwork Personal Communications Version 4.2 as the APPN end nodes.

We used APing to do some APPN pings between these end nodes (see Figure 243). You can find APing by clicking **Personal Communications ->Utilities -> APPC & CPIC Utilities-> Check Connection**:



Winaping setup

Partner LU Name or Symbolic Name: USIBMRA.BRPC
Mode Name: #INTER
TP Name: APINGD

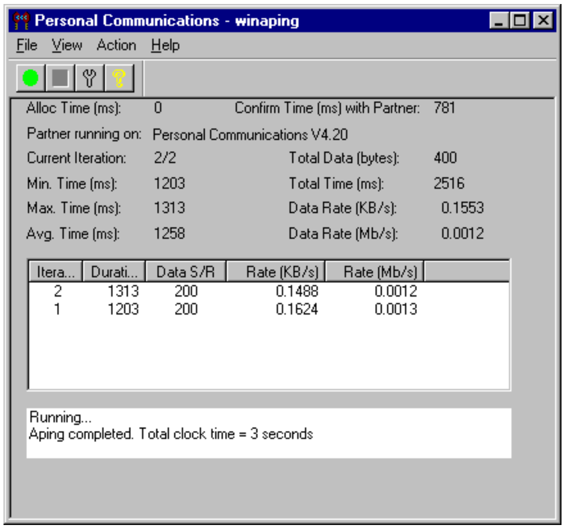
Packet Size: 100
Consecutive: 1
Iterations: 2

☑ Echo
☐ Verify Last Echoed Packet of Each Iteration

☐ Send Security
User ID:
Password:

Figure 243. APing from PCctr to BRpc

The results can be seen in Figure 244:



```
Alloc Time (ms):      0          Confirm Time (ms) with Partner:   781
Partner running on:   Personal Communications V4.20
Current Iteration:    2/2               Total Data (bytes):        400
Min. Time (ms):       1203              Total Time (ms):           2516
Max. Time (ms):       1313              Data Rate (KB/s):          0.1553
Avg. Time (ms):       1258              Data Rate (Mb/s):          0.0012
```

Itera...	Durati...	Data S/R	Rate (KB/s)	Rate (Mb/s)
2	1313	200	0.1488	0.0012
1	1203	200	0.1624	0.0013

```
Running...
Aping completed. Total clock time = 3 seconds
```

Figure 244. Results from APing between the PC in the center to the PC in the branch

13.7 Testing APPN (IPSec enabled)

At this point, we can re-enable IPSec and the policies to make sure that our configuration works through our VPN tunnel. To re-enable IPSec and the policies, we use the same procedures that we used in Chapter 12.6.1, “Enable IPSec and the policy” on page 238.

After these steps have been performed, we first check the status of the defined tunnels to make sure that they are in fact enabled. This is shown in Figure 245 where you can see that our previously defined tunnel has been re-enabled.

```
Center +FEATURE IPSec
Center IPSP>IPV4
Center IPV4-IPsec>LIST ALL

IPsec is ENABLED

IPsec Path MTU Aging Timer is 10 minutes

Defined Tunnels for IPv4:
--------------------------------------------------------------------------
   ID     Type    Local IP Addr   Remote IP Addr   Mode    State
 ------  ------  ---------------  ---------------  -----  --------
      1  ISAKMP    192.168.211.1    192.168.211.2  TUNN   Enabled

Defined Manual Tunnels for IPv6:
--------------------------------------------------------------------------

Tunnel Cache for IPv4:
-----------------------------------------------------------------------------
ID     Local IP Addr   Remote IP Addr  Mode   Policy  Tunnel Expiration
-----  --------------  --------------  -----  ------  ------------------
    1   192.168.211.1    192.168.211.2  TUNN   ESP          none

Tunnel Cache for IPv6:
-----------------------------------------------------------------------------
Center IPV4-IPsec>
```

Figure 245. Checking IPSec status

Next, we check to see that the APPC sessions are still active on the 2216. This is shown in Figure 246:

```
Center APPN >LIST APPC_SESSIONS
LU Name            Mode  Type  FSM
====================================
USIBMRA.BR2216    CPSVCMG  Pri  ACT
USIBMRA.BR2216    CPSVCMG  Sec  ACT
Center APPN >
```

Figure 246. Listing the active APPC sessions after enabling IPSEC and policies

Now, to make sure that the APPN traffic is actually going through the IPSec tunnel, we check the IPSec statistics before and after doing some APings.

Figure 247 on page 261 shows the counters after the APings. It shows the counter after reboot, when all counters were reset.

```
Center *TALK 5
CGW Operator Console
Center +FEATURE IPSec
Center IPSP>IPV4
Center IPV4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?
                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         315            0           315         56576        28288        28288

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         315            0           315         33136            0        33136

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors   Exceed MTU
  ----------   ----------   ----------   ----------
           0            0            0            0
Center IPV4-IPsec>
```

Figure 247. Checking the IPSec statistics

This completes the section on the configuration and testing of APPN through an IPSec tunnel.

Chapter 14. Branch: dependent LU requester (DLUR)

Now we describe a scenario where an SNA client in the branch wants to access the host in the center. We will show the use of DLUR and similar to the case of the APPN connection we will show the use of Enterprise Extender.

The dependent LU requester (DLUR) feature available in both MRS and MAS allows you to connect PU Type 2.0 or T2.1 devices containing dependent LUs to your SNA host using APPN. The DLUR function in the router works in conjunction with a dependent LU server (DLUS) located in VTAM. The router can either be configured as an APPN network node or an APPN end node.

Enterprise Extender (also called HPR over IP) uses IP encapsulation to transport APPN/HPR packets over IP.

We use the IPSec installation from our previous scenario to securely transport this traffic, that is, we use pre-shared keys and we have a tunnel between the two routers in the branch and center.

This chapter is very similar to the preceding scenario with APPN (see Chapter 13, “Branch: APPN through an IPSec tunnel” on page 241). All the same we will show all the necessary steps.

14.1 Description of the scenario

In our VPN scenario (see Figure 248 on page 264), we have a T2.0 device (and its associated dependent LUs) in the branch that we want to connect back to the data center. We put the DLUR function in the branch router, then use APPN transport between the DLUR and VTAM. Then, we use HPR over IP to carry the APPN traffic over the IP backbone (the Internet in this case) and hence, IPSec to protect these packets.

With the support for setting the IP precedence bits that became available in MRS/MAS Version 3.1, you can map the SNA priority (for example, HPR) of these connections into the IP packets.

This priority is preserved even if you are using IPSec tunnel mode, where the original packet is completely encapsulated in another one.

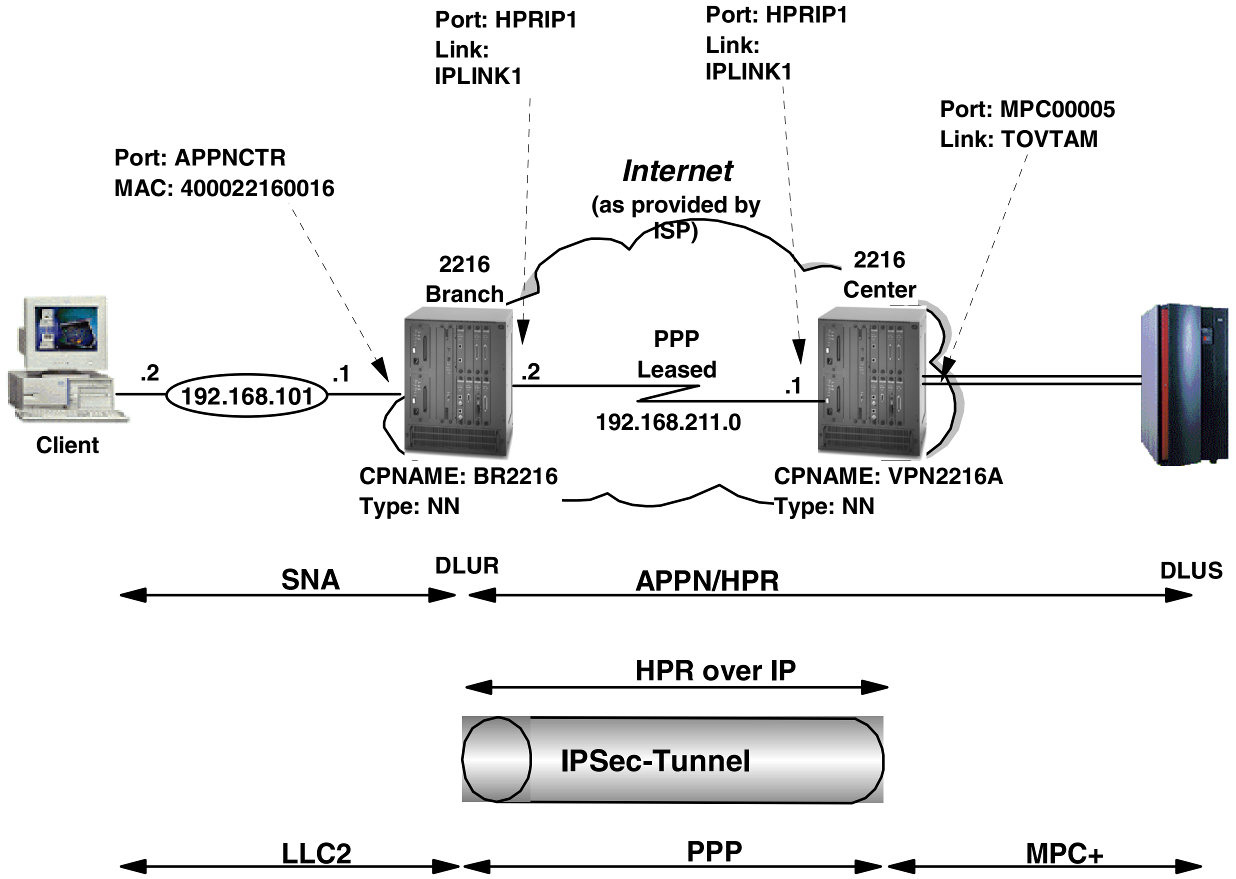


Figure 248. DLUR using APPN/HPR over IP through an IPSec tunnel

We put the SNA client, not in the production LAN of the branch, but in the LAN that is directly attached to the branch router. This scenario is more realistic because branches rarely have a dedicated DMZ. With this scenario we also avoid bridging SNA frames over the firewall.

The SNA traffic comes into the branch router as an LLC frame over the token-ring interface (which is also defined as an APPN port). The branch router, acting as an APPN network node, decides to route the traffic to its destination over the HPR over IP port. The HPR over IP engine in the router encapsulates the APPN LLC frame into an IP packet (using UDP) and then passes it to the IP routing element. IP then sends the packet to the other token-ring interface (our interface to the public network).

At this point, the policy we will define on the branch router redirects the packet to the IPSec engine where it is processed for AH and ESP headers before being sent out on the physical interface.

A similar process occurs in the reverse direction. As the IP packet reaches the end of the tunnel, it gets decapsulated and decrypted by the IPSec engine, then passed to the IP stack where it is determined that it must be directed to the HPR over IP port in the router. The HPR over IP function strips off the IP and UDP headers and passes the APPN LLC frame to APPN. The APPN network node routes the frame to its destination.

We use a Windows PC with eNetwork Personal Communications as our PU T2.0 with a dependent LU. We configure the PC in the branch to access the host by using the DLUR in the 2216 in the branch. On the PC in the branch we only have to provide the MAC address of the token-ring interface of the 2216 in the branch. This is the LAN destination MAC address for the 3270 gateway.
The MAC address of the 2216 TR in the branch is 400022160011.

As for the 2216 configuration, we use the same environment that we used in Chapter 13, “Branch: APPN through an IPSec tunnel” on page 241, except that we enable DLUR support in the router.

In the 2216 in the center, we use an MPC+ connection over the ESCON channel to VTAM. This is a very high performance connection and will generally provide the highest data throughout. Additionally, the required APPN support for DLUR is available over MPC+. Not shown in the figure is an IBM 9032 ESCON Director (ESCD) between the 2216 and the S/390.

To configure it, we simply define the MPC+ connection and then add an APPN port for this new connection to the existing APPN configuration. Also as in that scenario, we use HPR over IP between the routers and send that traffic through the IPSec tunnel already configured between them.

To provide the complete configuration we will list all necessary steps in this chapter.

14.2 IPSec and policy

As discussed in Chapter 10, “Connecting the data center to the branch office” on page 197, we could use either an IPSec tunnel mode tunnel or a transport mode tunnel. One reason a company would use tunnel mode versus transport mode is to hide internal IP addresses used in the network. Another might be to use unregistered IP addresses. When packets use tunnel mode, they are encapsulated with a new IP header and the original source and destination addresses are no longer visible.

However, in the case of HPR over IP packets, the IP traffic originates in the router where the APPN traffic is encapsulated and terminates in the router where it is decapsulated. In our scenario, the routers where the APPN traffic is encapsulated are the same routers used as our IPSec tunnel endpoints. In other words, only the Internet addresses of these two routers will appear in the HPR over IP packets. Using tunnel mode in this situation does not offer any advantages over transport mode in terms of hiding the source and destination IP addresses of the sender and receiver.

For our scenario, we used the existing tunnel (see Chapter 14, “Branch: dependent LU requester (DLUR)” on page 263) to carry our APPN traffic (as well as all the other router-to-router traffic).

14.3 VTAM startup parameters

In this section, we present the basic VTAM definitions we used for our scenario. This is not meant to be a complete reference on the subject. For more information on configuring VTAM, refer to *OS/390 SecureWay Communications Server: SNA Resource Definition Reference*, SC31-8565.

DLUS support requires that VTAM be configured as an APPN network node. This requires certain parameters to be specified in the VTAM startup parameters to specify the use of APPN and HPR. These are shown in Figure 249. Set the CONNTYPE to APPN and the NODETYPE to a Network Node (NN).

```
ASYDE=TERM,IOPURGE=5M,
CONFIG=I0,
CONNTYPE=APPN,
CPCP=YES,
CSALIMIT=0,
DYNADJCP=YES,
ENCRYPTN=NO,
GWSSCP=YES,
HOSTPU=ISTPUS18,
HOSTSA=18,
HPR=RTP,
NETID=USIBMRA,
NODETYPE=NN,
NOTRACE,TYPE=VTAM,IOINT=0
PPOLOG=YES
SORDER=APPN,
SSCPDYN=YES,
SSCPID=18,
SSCPNAME=RAI,
SSCPORD=PRIORITY,
SUPP=NOSUP,
TNSTAT,CNSL,
VRTG=YES
OSITOPO=LLINES,
OSIMGMT=YES
XNETALS=YES
```

Figure 249. VTAM startup parameters

14.4 Definition on the router in the center

In this section we describe the necessary steps to set up the center router.

14.4.1 Preparation

Perform the initial steps as outlined below before you set up the VPN scenario.

14.4.1.1 Load encryption package

Load the encryption package on the 2216 unless it has already been done:

```
Center Config>LOAD ADD PACKAGE encryption
encryption package configured successfully
This change requires a reload.
Center Config>WRITE
Config Save: Using bank B and config number 4
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 250. Loading the encryption package on the IBM 2216 router in the main site

The load of the encryption package requires a reboot of the machine.

14.4.1.2 Define internal IP address

We define an internal IP address which will be the endpoint of our HPR over IP network.

```
Center IP config>SET INTERNAL-IP-ADDRESS
Internal IP address [172.16.220.253]? 192.168.211.1
Center IP config>EXIT
```

Figure 251. Setting the internal IP address on the router in the central site

14.4.1.3 Load APPN package

Before we can configure APPN on the 2216, we first have to load the APPN package. This is shown in Figure 252.

In case you use a 2210 and you need an operational code that supports APPN you can download it from the IBM networking Web site. This is described in 13.3.1.3, “Load APPN package” on page 243.

```
Center Config>LOAD ADD PACKAGE appn
appn package configured successfully
This change requires a reload.
Center Config>EXIT
You are already at the top of the Configuration Menus.
(To return to the MOS Operator Console prompt (*), press Control-P)
Center Config>
Center *TALK 6
Center Config>WRITE
Config Save: Using bank A and config number 2
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y•
***
*** DISCONNECT
*** time 06:43:59
***
```

Figure 252. Loading the APPN package on the router in the central site

The load of the APPN package requires a reload.

14.4.2 APPN definitions

Ensure that the APPN package is loaded on the 2216.

14.4.2.1 Defining the APPN node

After the router comes back up, we go to the talk 6 APPN protocol menus and set the APPN node characteristics.

This is done using the `set node` command as shown in Figure 253:

```
Center Config>PROTOCOL APPN
Center APPN config>SET NODE
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) []? USIBMRA
Control point name (Max 8 characters) []? VPN2216A
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
```

Figure 253. Defining the APPN node on the 2216 in the center

As you can see, the only parameters that are absolutely necessary are the APPN CP name and the Network ID. The other parameters can be left at their default values.

14.4.2.2 Add APPN port for HPR over IP to branch

The next step is to add the APPN ports that will be used to carry our APPN traffic. In Figure 254, we add an HPR over IP port:

```
Center APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Enable IP Precedence: (Y)es (N)o [N]?
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

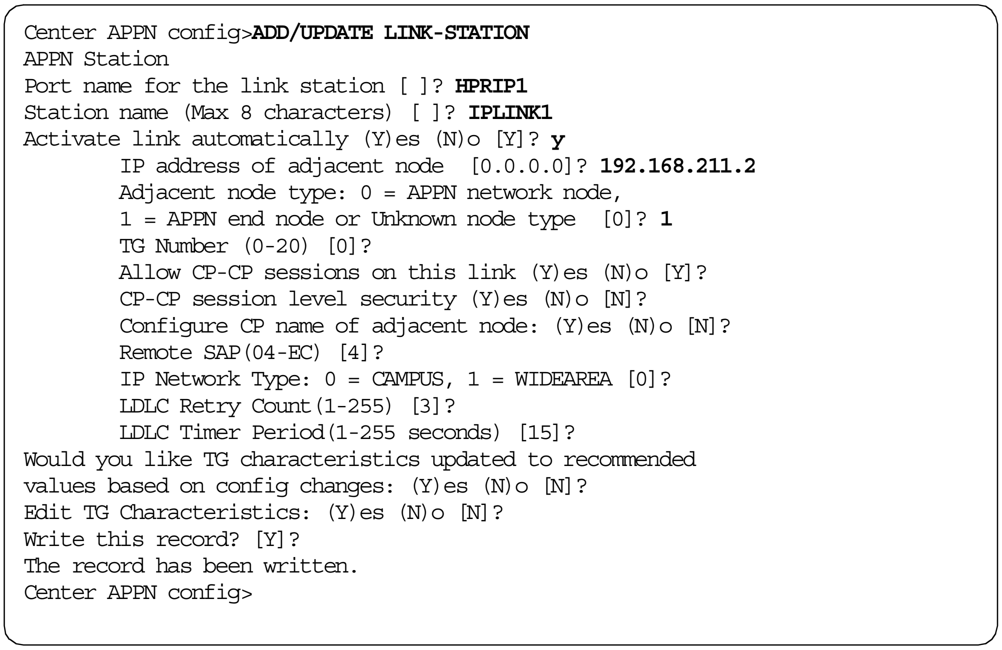
Figure 254. Adding an APPN port for HPR over IP

Again, we use the defaults for most of the parameters. The critical one is the port type (I for HPR over IP). Note that you do not need to specify an interface number because there is only one HPR over IP port per router. We also give it a port name that we can easily recognize on the monitoring console.

One question on this screen deals with the IPv4 precedence bits. If you respond yes to this question to enable setting of the precedence bits, then the 3 precedence bits in the TOS field of the IPv4 header will be set based on the HPR priority of the traffic. This allows you to preserve your SNA priorities using the Bandwidth Reservation System (BRS) feature even on encrypted packets. Please see *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

14.4.2.3 Add link to 2216 in branch

Next, we add a link station on the newly defined HPR over IP port. This is shown in Figure 255:



```
Center APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? HPRIP1
Station name (Max 8 characters) [ ]? IPLINK1
Activate link automatically (Y)es (N)o [Y]? y
        IP address of adjacent node  [0.0.0.0]? 192.168.211.2
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type  [0]? 1
        TG Number (0-20) [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Center APPN config>
```

Figure 255. Adding a link station for the HPR over IP link

By specifying the port name for this link station, the router knows that it is an HPR over IP port. Therefore, it knows to prompt you for an IP address as opposed to a MAC address that it would need if we were defining a link station for a LAN port.

The IP address that we specify is the *internal address* of the router in the branch office. This is the endpoint of our HPR over IP network. The other end of the HPR over IP link is always at the router that will decapsulate the packets and *not* the next hop router in the path. Intermediate routers, if any, merely perform IP routing on the encapsulated packets.

14.4.2.4 Add APPN port for local token-ring

Although it is not needed for the connection between the branch and the center we also added a port for the local token-ring. This definition supports users in the local token-ring in the center (Figure 256 on page 270).

```
Center APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? T
Interface number(Default 0): [0]? 0
Port name (Max 8 characters) [T00000]? appnctr
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-65535) [65535]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
enter APPN config>
```

Figure 256. Adding an APPN port for HPR over IP for the local token-ring

We do not need to define any link stations on this port as the workstations (APPN end nodes) will create implicit links when they initialize with their network node (in this case, the 2216 in the center itself).

14.4.3 Activate

The configuration of the 2216 in the center is now complete except the MPC+ connection. To activate the changes, we reload the router:

```
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): B
```

Figure 257. Reloading the IBM 2216 router in the center

14.5 Definition of the MPC+ connection

In this section we describe the configuration of an MPC+ connection between a S/390 and a 2216 router.

14.5.1 S/390 - 2216 parameter relationships - MPC+

Figure 258 on page 271 shows the relationship between the MPC+ definitions on the S/390 server and the corresponding definitions on the 2216 in the center.

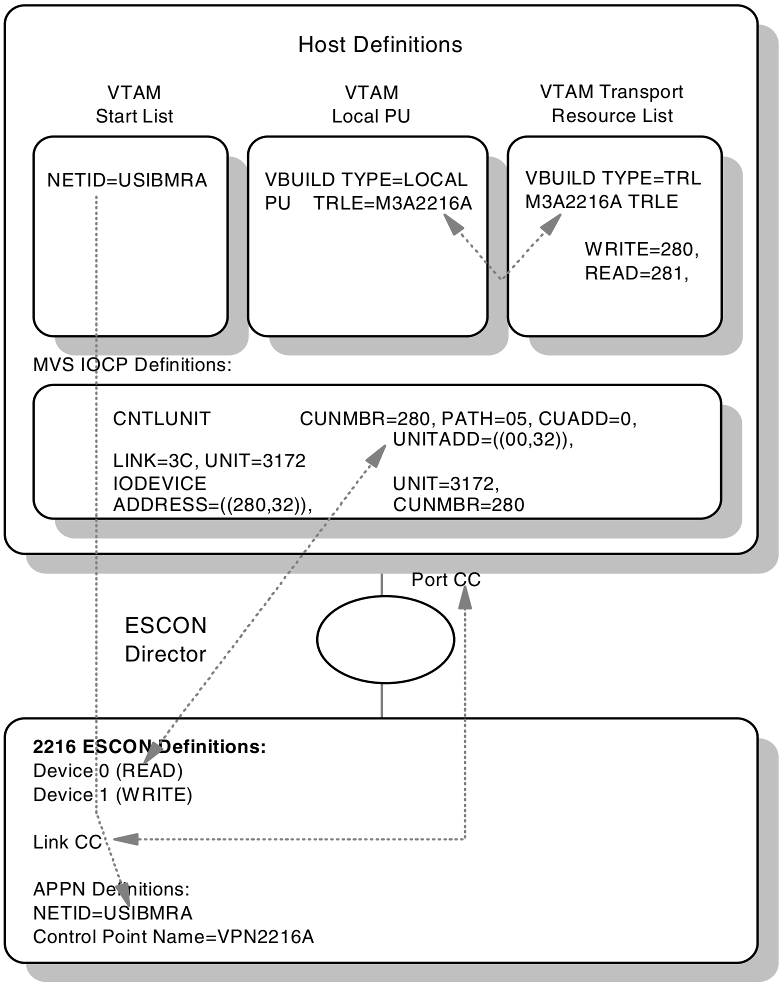


Figure 258. Host/2216 parameter relationships - MPC+

Notes:

1. The device addresses specified in the 2216 MPC+ interface definition must be within the range specified in the UNITADD parameter in the CNTLUNIT macro from the IOCP. For example, the UNITADD parameter in Figure 258 shows that 32 (decimal) device addresses starting at 00 (hex) are being reserved for the 2216 definition. Device addresses 00 and 01 have been specified for the 2216 MPC+ interface. Since 00 and 01 are in the range between 00 and 1F hex, this is OK as long as no other device (or interface on this 2216) tries to use these same subchannels.

2. The values specified in the VTAM TRL major node definition must be within the range specified in the ADDRESS parameter in the IODEVICE macro from the IOCP. For example, the TRL major node definition in Figure 258 specifies 280 and 281 which are in the range between 280 and 29F that the ADDRESS parameter in the IODEVICE statement specifies.

3. The values specified for the ADDRESS parameter in the IODEVICE macro and the UNITADD parameter in the CNTLUNIT macro are related *by convention only*. When defining device addresses on the 2216 MPC+

definition, use the UNITADD parameter and not the ADDRESS parameter to determine the valid range of values.

14.5.2 Definitions in VTAM for an MPC+ connection

An MPC+ connection requires entries in two VTAM control blocks:

- The Local major node
- The Transport Resource List (TRL) major node

Figure 259 shows a sample definition for a local SNA major node for a 2216 MPC+ connection. This is the local PU that resides in VTAM that supports the channel connection defined in the TRL. The connection type must be APPN and you also need to enable HPR.

```
LOCN2216 VBUILD TYPE=LOCAL
PU2216   PU     TRLE=M3A2216A,
                XID=YES,
                CONNTYPE=APPN,
                CPCP=YES,
                HPR=YES
```

Figure 259. VTAM local major node definition

Notes:

1. TYPE must equal LOCAL on the VBUILD statement.
2. TRLE identifies the TRL being used. The name must match the name of an existing TRL.
3. XID indicates whether XIDs will be exchanged. It must be XID=YES.
4. CONNTYPE must be set to CONNTYPE=APPN since APPN is the only protocol that VTAM uses with an MPC+ connection.
5. CP-CP specifies that CP-CP connections with APPN can be established over this MPC+ connection. This could be set either to YES or NO, depending upon your APPN topology.
6. HPR specifies that APPN HPR traffic can flow over this MPC+ connection. HPR is normally used by default, but setting this value to YES ensures it. This is important because an MPC+ connection requires RTP (and HPR).

Next, you need a transport resource list for the MPC+ connection from the 2216. An example definition is shown in Figure 260:

```
         VBUILD TYPE=TRL
M3A2216A TRLE   LNCTL=MPC,
                MAXBFRU=9,
                READ=281,
                WRITE=280,
                MPCLEVEL=HPDT,
                REAPLYTO=3.0
```

Figure 260. VTAM Transport Resource List (TRL) definition

Notes:

1. TYPE must be TRL.
2. M3A2216A is the name that identifies the TRL. It must match what is specified in the TRLE= field in the local major node definition (See Figure 259).
3. LNCTL identifies the connection type. It must be LCNTL=MPC.
4. MAXBFRU is the number of 4K pages per read subchannel.
5. READ/WRITE specifies the subchannels in the MPC+ group, and indicates their direction. The subchannel numbers must be in the range of addresses specified in the IODEVICE statement in the IOCP definition. There can be multiple READ and WRITE parameters in the TRLE statement but there must be at least one of each.

   Note: The designations READ and WRITE here are from the HOST perspective. In the 2216 MPC+ definition, the designations are from the 2216 perspective. Therefore, subchannels designated as READ on the host *must* be designated as WRITE on the 2216, and vice versa.
6. REPLYTO is the reply timeout value in seconds.

14.5.3 Definition on the router for an MPC+ connection

In this section, we show the steps necessary to:

1. Configure the 2216 for an ESCON MPC+ connection to the host.
2. Add an APPN port for this connection.

14.5.3.1 Add ESCON device

To connect the 2216 to the host using the ESCON adapter, you first need to add an ESCON interface for the router and configure it. Figure 261 shows this step. As can be seen from the figure, if you list the devices after adding the ESCON adapter, it will appear at the bottom of the list. You should check that the slot number is correct. Also remember that the interface numbers are dependent on the order in which you added the devices to the configuration.

```
Center *TALK 6

Center Config>ADD DEVICE ESCON
Device Slot #(1-8) [1]? 8
Adding ESCON Channel device in slot 8  port 1 as interface #2
Use "net 2" to configure ESCON Channel parameters
Ifc 0     Token Ring                        Slot: 1      Port: 1
        (40 Receive Buffers)
Ifc 1     Token Ring                        Slot: 1      Port: 2
        (40 Receive Buffers)
Ifc 2     ESCON Channel                     Slot: 3      Port: 1
        (255 Receive Buffers)
Ifc 3     LSA - ESCON Channel               Base Net: 2
Ifc 4     EIA-232E/V.24 PPP                 Slot: 8      Port: 0
        (24 Receive Buffers)
Ifc 5     Loopback APPN - Channel
```

Figure 261. Adding the ESCON adapter

14.5.3.2 Add MPC+ virtual interface

Now that we have the ESCON interface defined we need to add the MPC+ virtual interface. This MPC *virtual net handler* will perform all the MPC protocol functions for our connection to the host. Figure 262 shows this step:

```
Center *TALK 6
Gateway user configuration
Center Config>LIST DEVICES
Ifc 0     Token Ring                      Slot: 1     Port: 1
        (40 Receive Buffers)
Ifc 1     Token Ring                      Slot: 1     Port: 2
        (40 Receive Buffers)
Ifc 2     ESCON Channel                   Slot: 3     Port: 1
        (255 Receive Buffers)
Ifc 3     LSA - ESCON Channel             Base Net: 2
Ifc 4     EIA-232E/V.24 PPP               Slot: 8     Port: 0
        (24 Receive Buffers)
Ifc 5     Loopback APPN - Channel         Slot: 0     Port: 0
Center Config>NETWORK 2
Center ESCON Config>ADD MPC
```

Figure 262. Adding the MPC+ virtual interface

As can be seen in Figure 262, the prompt will change to the `ESCON Config>` prompt. From here you define the read and write subchannels that will be used for this connection.

14.5.3.3 Add read subchannel

```
Center ESCON Config>
Center ESCON Add Virtual>SUBchannels ADDRead
Center ESCON Add MPC+ Read Subchannel>Device
Device address (range 0x00-0xFF): [0]? 00
Center ESCON Add MPC+ Read Subchannel>LINk
Link address (ESCD Port) (range 0x01-0xFE): [1]? cc
Center ESCON Add MPC+ Read Subchannel>CU
Control Unit Logical Address (range 0x0-0xF): [0]? 1
Center ESCON Add MPC+ Read Subchannel>LPAR
LPAR number (range 0x0-0xf): [0]? 1
Center ESCON Add MPC+ Read Subchannel>Exit
Center ESCON Add Virtual>
```

Figure 263. Adding a read subchannel

You will need to provide the appropriate values for the following parameters:

Device address The unit address transmitted on the channel path to select the 2216 over another device on the channel. It is also referred to as the subchannel number in the S/370 I/O architecture. It is a two-digit hexadecimal value that may range from 00-FF. This value is defined in the host Input/Output Configuration Program (IOCP) by the UNITADD statement on the CNTLUNIT macro instruction for the real device. The value entered here will relate to the entry made in the TRL major node in VTAM for the *write* subchannel address. Remember that the write subchannel defined to VTAM will be your read subchannel for the 2216 and vice versa (see Figure 258 on page 271).

Link address The ESCON Director (ESCD) port number which is attached to the *host*. Note that this is *not* the ESCD port number on which the 2216 is attached. If you are using EMIF and not an ESCD, then the link address must be set to 1 and the LPAR parameter is used to select the logical partition.

CU address The control unit address defined in the host for the 2216. This must match the entry defined in the host IOCP CUADD parameter in the CNTLUNIT macro.

LPAR number Allows multiple partitions in a logically partitioned (LPAR) host to share one ESCON fiber. If you are using EMIF on the host, the value entered here must be the logical partition number for this connection. If you are using an ESCD, then it must be set to 1.

14.5.3.4 Add write subchannel

Because MPC+ operates with at least one subchannel for each direction you need to add a write subchannel address next. This step, shown in Figure 264, is very similar to adding a read subchannel:

```
Center ESCON Add Virtual>SUBchannels ADDWrite
Center ESCON Add MPC+ Write Subchannel>Device
Device address (range 0x00-0xFF): [81]?01
Center ESCON Add MPC+ Write Subchannel>LINk
Link address (ESCD Port) (range 0x01-0xFE): [CC]?
Center ESCON Add MPC+ Write Subchannel>CU
Control Unit Logical Address (range 0x0-0xF): [1]?
Center ESCON Add MPC+ Write Subchannel>LPAR
LPAR number (range 0x0-0xf): [1]?
Center ESCON Add MPC+ Write Subchannel>Exit
```

Figure 264. Adding a write subchannel

Remember that the write subchannel defined to VTAM will be your read subchannel for the 2216 and vice versa (see Figure 258 on page 271).

14.5.3.5 Verify the configuration

Next, we list the subchannels that we just defined to check that we have entered the parameters correctly. This is shown in Figure 265:

```
Center ESCON Add Virtual>SUBchannels LIst
         Read Subchannels:
         Sub  0   Device address   : 80   LPAR number        : 1
                  Link address     : CC   CU Logical Address : 1
         Write Subchannels:
         Sub  1   Device address   : 81   LPAR number        : 1
                  Link address     : CC   CU Logical Address : 1
Center ESCON Add Virtual>Exit
```

Figure 265. List of the configured subchannels

Finally, we list all the interface parameters for our ESCON interface as shown in Figure 266. This shows the listing of the ESCON interface (for which we accepted the defaults) as well as the newly defined read and write subchannels.

```
Center ESCON Config>LIst all
Net:  5   Protocol: APPN Loopback   LAN type: Token-Ring/802.5
          APPN loopback MAC address: 40002216000C

Net:  3   Protocol: LSA    LAN type: Token Ring      LAN number:  0
          Maxdata: 2052
          Loopback is enabled.
          MAC address: 40002216000A
          Block Timer:   10 ms   ACK length:   10 bytes
          Sub  0   Dev addr:  4  LPAR: 1  Link addr: CC  CU addr: 1

Net:  6   Protocol: MPC+   LAN type: MPC+            LAN number:  0
          Maxdata: 2048
          Reply TO: 45000   Sequencing Interval Timer: 3000
          Outbound protocol data blocking is enabled
          Block Timer:    5 ms   ACK length:   10 bytes
          Read Subchannels:
          Sub  0   Dev addr: 80  LPAR: 1  Link addr: CC  CU addr: 1
          Write Subchannels:
          Sub  1   Dev addr: 81  LPAR: 1  Link addr: CC  CU addr: 1
Center ESCON Config>
```

Figure 266. List of the ESCON interface

14.5.3.6 Reloading

When you exit the ESCON configuration you will be prompted if you want to keep the changes. You must answer yes. Also, before continuing with the configuration, you need to reload the router. Figure 267 shows these steps. This completes the steps necessary to add the ESCON adapter and the MPC+ virtual interface.

```
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 267. Reloading the router

14.5.3.7 Check the MPC+ interface

After the router comes back up, use the `list device` command to see the MPC+ virtual interface that was added in the last step. Figure 268 on page 277 shows that a new MPC+ interface (interface 5) was added to our configuration.

```
Center Config>LIST DEVICES
Ifc 0     Token Ring                        Slot: 1      Port: 1
       (40 Receive Buffers)
Ifc 1     Token Ring                        Slot: 1      Port: 2
       (40 Receive Buffers)
Ifc 2     ESCON Channel                     Slot: 3      Port: 1
       (255 Receive Buffers)
Ifc 3     EIA-232E/V.24 PPP                 Slot: 8      Port: 0
       (24 Receive Buffers)
Ifc 4     Loopback APPN - Channel           Slot: 0      Port: 0
Ifc 5    MPC - ESCON Channel          Base Net: 2
Center Config>
```

Figure 268. Checking for the MPC+ interface

14.5.3.8 Add an APPN port for the MPC+ interface

The next step is to add an APPN port for our new MPC+ interface. This is done from the APPN protocol menu as shown in Figure 269:

```
Center Config>
Center Config>PROTOCOL APPN
Center APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? M
Interface number(Default 0): [0]? 5
Port name (Max 8 characters) [MPC00005]? MPC00005
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        Maximum BTU size (768-32768) [2048]?
Edit MPC+ Sequencing Interval Timer: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Center APPN config>
```

Figure 269. Adding an APPN port for the MPC+ interface

Note: You might notice that the menus do not prompt you whether to enable High Performance Routing (HPR) on this port. This is because MPC+ supports HPR only. It does not support APPN Intermediate Session Routing (ISR).

14.5.3.9 Add a link to VTAM

Next, we add a link station to the host. This is shown in Figure 270 on page 278. The port name specified is the name of the APPN port that we created in the last step. The adjacent node type is 0 because we defined VTAM as a network node in the VTAM startup parameters.

```
Center APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? mpc00005
Station name (Max 8 characters) [ ]? tovtam
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type [0]? 0
        TG Number (0-20) [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Center APPN config>
```

Figure 270. Adding a link to VTAM

14.5.3.10 List the APPN configuration

Now we list the complete APPN configuration as shown in Figure 271 on page 279. Note that DLUR is not enabled for this node. DLUR support is not needed on the 2216 in the center. In this configuration, the 2216 is merely providing Automatic Network Routing (ANR) services as an intermediate APPN node.

DLUR is needed on the 2216 as it is that router that is providing the DLUR support for the downstream PUs in the branch. The DLUR configuration for the 2216 in the branch will be shown later.

From the port section in the listing, it can be seen that our new MPC+ port has been added and is enabled. In this configuration, we only make use of this port (MPC00005) and the Enterprise Extender port (HPRIP1).

In the link station list, our new link station (TOVTAM) appears. This is the MPC+ connection between the 2216 and the host over the ESCON channel.

```
Center APPN config>LIST ALL
NODE:
       NETWORK ID: USIBMRA
       CONTROL POINT NAME: VPN2216A
       XID: 00000
       APPN ENABLED: YES
       BREX OR BORDER NODE: NEITHER
       MAX SHARED MEMORY: 5108
       MAX CACHED: 4000
DLUR:
       DLUR ENABLED: NO
       PRIMARY DLUS NAME:
CONNECTION NETWORK:
             CN NAME       LINK TYPE  PORT INTERFACES
       -------------------------------------------------------------
COS:
       COS NAME
       --------
         #BATCH
        #BATCHSC
        #CONNECT
         #INTER
        #INTERSC
         CPSVCMG
        SNASVCMG
MODE:
        MODE NAME  COS NAME
       ---------------------
PORT:
         INTF     PORT      LINK      HPR    SERVICE   PORT
        NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
       ------------------------------------------------------
        65535    HPRIP1     HPR_IP    YES      YES      YES
            0   APPNCTR   IBMTRNET    YES      YES      YES
            5  MPC00005       MPC+    YES      YES      YES
STATION:
        STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
         NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
       ------------------------------------------------------------
        IPLINK1   HPRIP1     192.168.211.2     YES     YES       0
         TOVTAM MPC00005      000000000000     YES     YES       0
LU NAME:
             LU NAME        STATION NAME          CP NAME
       ------------------------------------------------------------
Center APPN config>
```

Figure 271. Listing the APPN configuration

14.5.3.11 Activate the APPN connection

It is not necessary to restart the router at this point. To activate the changes to the APPN configuration, we simply issue the `activate` command from the `APPN Config>` prompt. This is illustrated in Figure 272:

```
Center APPN config>ACTIVATE_NEW_CONFIG
```

Figure 272. Activating the new APPN configuration

This completes the steps necessary to configure the 2216 in the center for this scenario.

14.6 Definition on the router in the branch

In this section we take you step-by-step through the DLUR definition of the 2216 in the branch. The steps are almost identical to the ones for configuring the 2216 in the data center.

After some preparations you define the APPN node. Afterward you define the APPN port to the center. We do not need to define a link station to the center, because an implicit link will be created when the router in the center establishes a connection to the router in the branch.

We do not need to define an APPN port on the local token-ring in the branch because we have native subarea traffic. The DLUR of the 2216 in the branch is the interface between subarea SNA in the branch and APPN to the center.

14.6.1 Preparation

As on the 2216 in the center you have to:

- Load the encryption package (see Figure 250 on page 267).
- Define the internal IP address (see Figure 251 on page 267).
- Load the APPN package (see Figure 252 on page 267).

14.6.2 APPN definitions

In this section we describe the necessary steps to set up APPN on the branch router.

14.6.2.1 Load APPN

Load the APPN package into the 2216 (see Figure 252 on page 267).

14.6.2.2 Defining the APPN node

First we set the APPN node characteristics. This is shown in Figure 273:

```
Branch *TALK 6
Gateway user configuration
Branch Config>PROTOCOL APPN
Branch APPN config>SET NODE
Enable APPN (Y)es (N)o [Y]?Y
Network ID (Max 8 characters) [USIBMRA]? USIBMRA
Control point name (Max 8 characters) [NN2216]? br2216
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Branch APPN config>
```

Figure 273. Setting the APPN node characteristics for the branch router

Note that the network ID must match at both ends of the HPR over IP link.

14.6.2.3 Add APPN port for HPR over IP to center

Next we add an HPR over IP port. This is shown in Figure 274:

```
Branch APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
 (M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Treat non-configured callers as LEN nodes: (Y)es (N)o [N]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [1]?
        Enable IP Precedence: (Y)es (N)o [N]? y
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [10]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Branch APPN config>EXIT
```

Figure 274. Adding an APPN port for the WAN interface on the 2216 branch router

Note that we use the same port name as we used for the 2216 in the center. This is just for our convenience as the port name is only used at the router where it is defined and has no correlation to any other port names on any other routers.

Now that we have the port defined, the next step would normally be to define a link station to the next hop APPN node. However, in this case, it is not necessary because an implicit link will be created when the 2216 in the data center establishes a connection with this 2216 in the branch office.

14.6.2.4 Activation of the APPN definitions

This completes the APPN definition on the branch router. We restart the gateway to activate APPN as shown in Figure 275 on page 281.

```
Branch Config>
Branch *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
***
*** DISCONNECT
*** time 07:07:00
***
```

Figure 275. Reloading the branch router

14.6.3 DLUR definitions

In 13.4, “Definition on the router in the branch” on page 249 we added APPN support on the branch router specifying it as a network node and using HPR over IP to communicate to the router in the data center. For this scenario, the only change necessary to the router configuration in the branch is to add the DLUR support to this existing APPN configuration.

Adding DLUR support is quite simple. From the APPN configuration, we specify to enable DLUR. Then, we provide the CP name of the primary DLUS (VTAM). Finally, we activate the DLUR configuration in the router. These steps are shown in Figure 276:

```
Branch *TALK 6
Gateway user configuration
Branch Config>PROTOCOL APPN
Branch APPN config>SET DLUR
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
Branch APPN config>
```

Figure 276. Enabling DLUR in the branch router

For more information about DLUR configuration, refer to *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885.

This completes the steps necessary to configure the 2216 in the branch for DLUR support in this scenario.

14.6.4 Activate

Activate the DLUR definitions in the branch router as shown in Figure 277:

```
Branch APPN config>ACTIVATE_NEW_CONFIG
Branch APPN config>EXIT
Branch Config>WRITE
Config Save: Using bank A and config number 2
Branch Config>
Branch *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
***
*** DISCONNECT
*** time 07:20:47
***
```

Figure 277. Enabling DLUR in the branch router

14.7 Definition on the client PC

We used a Windows 95 client with eNetwork Personal Communications Version 4.2 as the SNA client.

To configure you have to enter the configuration menus: you choose **Configure** in the menu Communication.

Afterward you have to specify 802.2 as the protocol (see Figure 278):

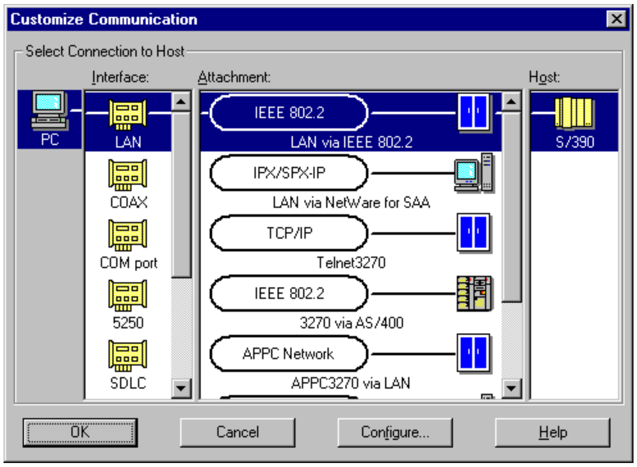
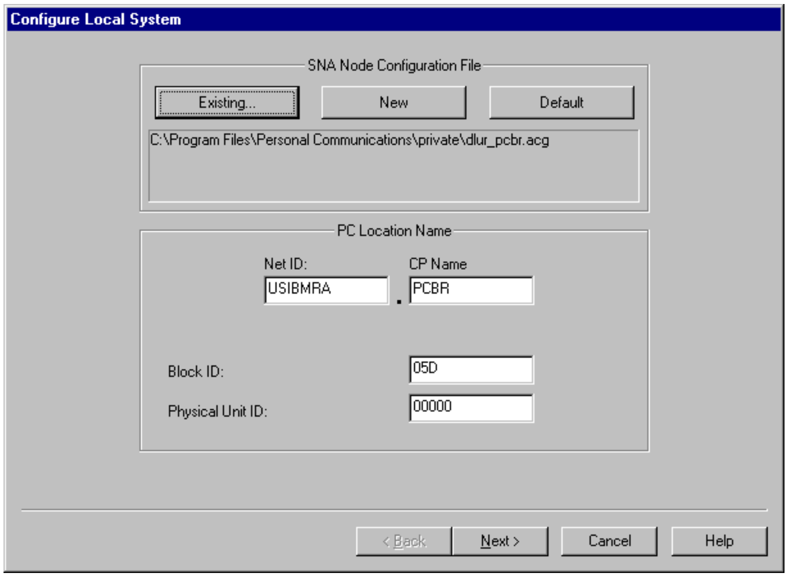


Figure 278. Configuring the 802.2 protocol

Configuring the local system you have to specify the Net ID which has to match the Network ID which you specified on the routers. The CP name you specify can be chosen (see Figure 279).



C:\Program Files\Personal Communications\private\dlur_pcbr.acg

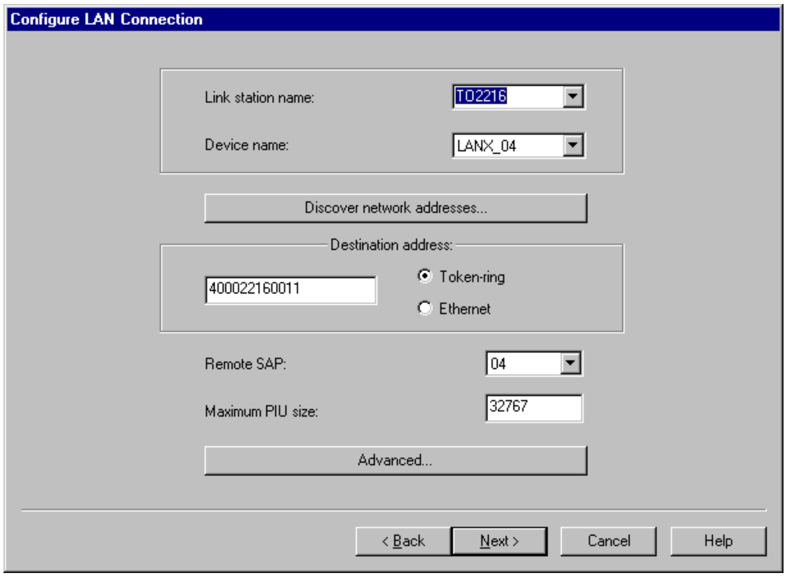
Net ID: USIBMRA . CP Name PCBR

Block ID: 05D

Physical Unit ID: 00000

Figure 279. Specifying Net ID and CP name

Finally you specify the link station name which you can choose. And you specify the destination MAC address, which is the LAN MAC address of your local router in the branch (see Figure 280):



Configure LAN Connection

Link station name: TO2216

Device name: LANX_04

Destination address: 400022160011

● Token-ring

○ Ethernet

Remote SAP: 04

Maximum PIU size: 32767

Figure 280. Specifying the link station name and the destination MAC address

14.8 Testing DLUR (IPSec disabled)

At this point, the configuration of both routers and the configuration of the S/390 server and of the PC in the branch is complete. IPSec and the IPSec policies will be temporarily disabled. Before enabling IPSec and the policies we need to test the DLUR function.

We used our Windows 95 Client with eNetwork Personal Communications Version 4.2 as the SNA client which is connected to the token-ring segment of the 2216 in the branch.

This device is configured with one 3270 session back to the host in the data center.

14.8.1 Checking the status of IPSec and policies

The current IPSec status can be checked with the following command:

```
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
Center IPV4-IPsec config>
```

Figure 281. Checking the current status of IPSec

The current status of the policies can be checked with the following command:

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy config>LIST POLICY ALL
Policy Name     = ike-pre-101-102
       State:Priority =Enabled   : 5
       Profile        =101.0-to-102.0-pre
       Valid Period   =allTheTime
       IPSEC Action   =tun-101-102
       ISAKMP Action  =ike-act1
       .......
Center Policy Config>
```

Figure 282. Checking the current status of the policies

The current IPSec status can be checked with the following command:

```
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
Center IPV4-IPsec config>
```

Figure 283. Checking the current status of IPSec

14.8.2 Disable IPSec and the policies

Before testing the DLUR connection IPSec should be temporarily disabled on the router in the center (see Figure 285 on page 286) and on the router in the branch: You also have to disable the policy (see Figure 284):

With the command `disable policy` you can disable the policies.

```
Center Config>
Center Config>FEATURE Policy
IP Network Policy configuration
Center Policy Config>
Center Policy config>DISABLE POLICY
Enter the Name of the Policy to disable (? for a List)
 [?]?
        1: ike-pre-101-102
        2: ike-pre-3-100
        3: ike-pre-211-211
Number of policy [1]?
```

Figure 284. Disabling the policies on the router in the center

The command `disable IPSec stop` stops IPSec. The current status of IPSec can be seen with the command `list status`.

```
Center *TALK 6
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>DISABLE IPSEC STOP
Center IPV4-IPsec config>LIST STATUS
IPsec is DISABLED (STOP mode)
IPSec Path MTU Aging Timer is 10 minutes
```

Figure 285. Disabling IPSec on the router in the center

14.8.3 Check APPN node status

We check the APPN node definitions with the command `list node` (Figure 286):

```
Center APPN config>LIST NODE
Node:
       Network ID: USIBMRA
       Control point name: VPN2216A
       XID: 00000
       APPN enabled: YES
       Branch extender: NO
       Permit search for unregistered LUs: NO
       Border Node: No
       Route addition resistance: 128
       Use enhanced BATCH COS: Y
       Use enhanced BATCHSC COS: Y
       Use enhanced INTER COS: Y
       Use enhanced INTERSC COS: Y
       Max shared memory: 5108
       Max cached: 4000
       Percent buffer memory: 11
Center APPN config>
```

Figure 286. Checking the APPN node definitions

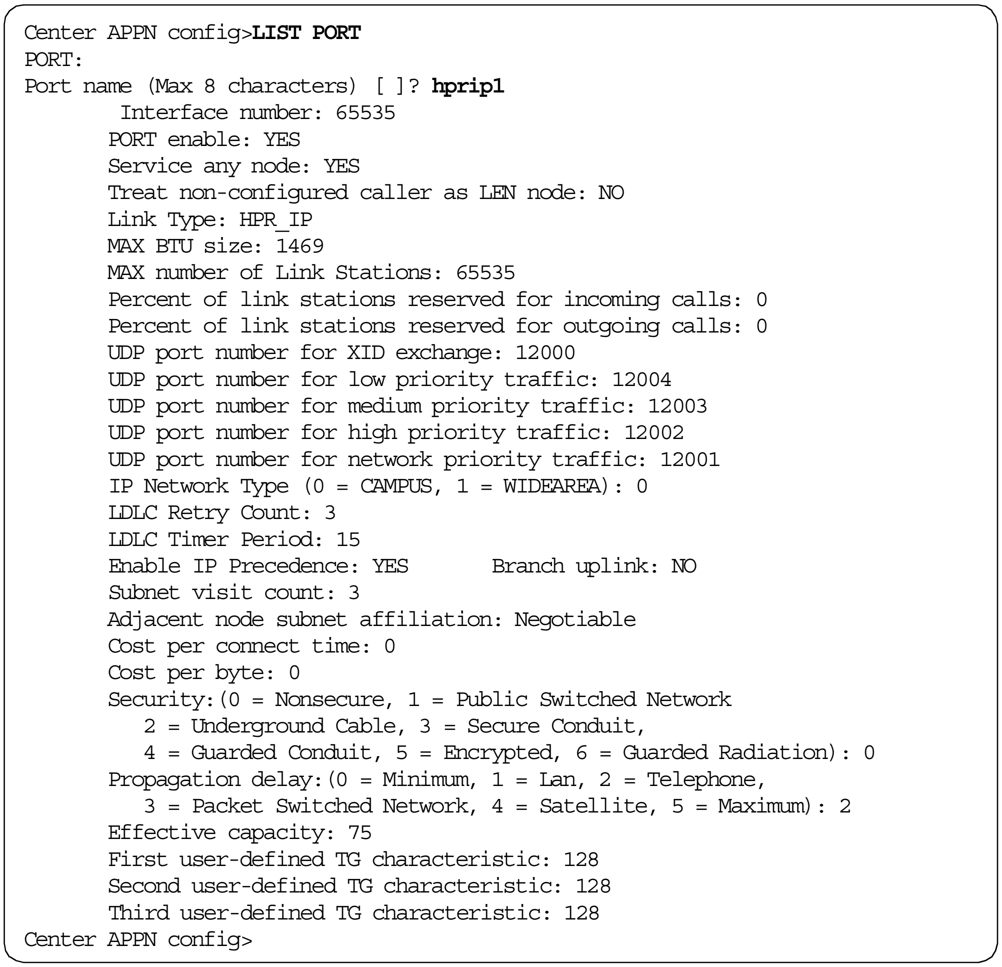
14.8.4 Check the MPC+ port status

We check the status of the APPN ports on the 2216 in the center. Figure 287 shows that the port to the 2216 in the branch (port 6), the MPC+ port to the S/390 server (port 4) and the port to the local token-ring (port 0) is in the active (ACT_PORT) state:

```
Center +PROTOCOL APPN
APPN GWCON
Center APPN >LIST PORT_INFORMATION
  Intf        Name       DLC Type        HPR          State
============================================================
    6       HPRIP1         HPR_IP       TRUE       ACT_PORT
    4     MPC00005           MPC+       TRUE       ACT_PORT
    0      APPNCTR       IBMTRNET       TRUE       ACT_PORT
Center APPN >
```

Figure 287. Listing and checking port information

The status of each port can be examined in more detail with the following command:



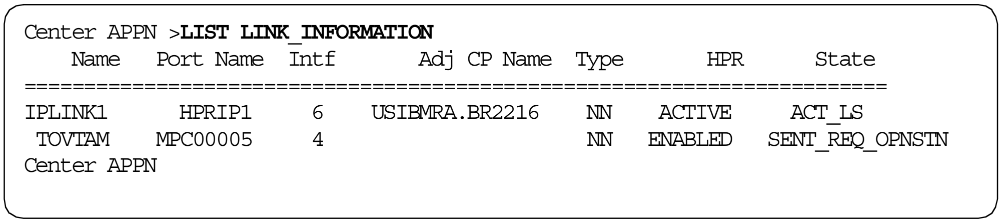
```
Center APPN config>LIST PORT
PORT:
Port name (Max 8 characters) [ ]? hprip1
        Interface number: 65535
       PORT enable: YES
       Service any node: YES
       Treat non-configured caller as LEN node: NO
       Link Type: HPR_IP
       MAX BTU size: 1469
       MAX number of Link Stations: 65535
       Percent of link stations reserved for incoming calls: 0
       Percent of link stations reserved for outgoing calls: 0
       UDP port number for XID exchange: 12000
       UDP port number for low priority traffic: 12004
       UDP port number for medium priority traffic: 12003
       UDP port number for high priority traffic: 12002
       UDP port number for network priority traffic: 12001
       IP Network Type (0 = CAMPUS, 1 = WIDEAREA): 0
       LDLC Retry Count: 3
       LDLC Timer Period: 15
       Enable IP Precedence: YES       Branch uplink: NO
       Subnet visit count: 3
       Adjacent node subnet affiliation: Negotiable
       Cost per connect time: 0
       Cost per byte: 0
       Security:(0 = Nonsecure, 1 = Public Switched Network
          2 = Underground Cable, 3 = Secure Conduit,
          4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
       Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
          3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
       Effective capacity: 75
       First user-defined TG characteristic: 128
       Second user-defined TG characteristic: 128
       Third user-defined TG characteristic: 128
Center APPN config>
```

Figure 288. Checking the status of the port to the 2216 in the branch

14.8.5 Check the status of the link to VTAM

Next, we verify the status of the link stations on the routers. This is shown in Figure 289 for the 2216. From the figure, you can see that the link between the two routers (interface 6) is in active state (ACT_LS).

However, the link to the S/390 server (interface 4) is not active (SENT_REQ_OPNSTN).



```
Center APPN >LIST LINK_INFORMATION
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=======================================================================
IPLINK1      HPRIP1     6    USIBMRA.BR2216    NN    ACTIVE     ACT_LS
 TOVTAM    MPC00005     4                      NN   ENABLED   SENT_REQ_OPNSTN
Center APPN
```

Figure 289. Checking the status of the link to VTAM before activating the corresponding VTAM PU

The reason is that the link to VTAM does not get into active state (ACT_LS) unless the corresponding VTAM PU is active.

Note

To get the MPC+ link from the 2216 to VTAM active you have to activate the corresponding VTAM Majornode *after* the reload of the router.

After activating the PU we get the following link information:

```
Center APPN >LIST LINK_INFORMATION
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=======================================================================
 IPLINK1     HPRIP1     6    USIBMRA.BR2216    NN    ACTIVE     ACT_LS
 TOVTAM    MPC00005     4     USIBMRA.RA03M    NN    ACTIVE     ACT_LS
```

Figure 290. Checking the status of the link to VTAM after activating the corresponding VTAM PU

14.8.6 List the APPC sessions

Finally, we verify that there are APPC sessions to the branch router and to VTAM. This is done from talk 5 by listing the active APPC sessions as shown in Figure 291. (Remember VTAM is USIBMRA.RA03M.)

```
Center APPN >LIST APPC_SESSIONS
LU Name            Mode  Type  FSM
====================================
USIBMRA.BR2216    CPSVCMG  Pri  ACT
USIBMRA.BR2216    CPSVCMG  Sec  ACT
USIBMRA.RA03M     CPSVCMG  Pri  ACT
USIBMRA.RA03M     CPSVCMG  Sec  ACT
Center APPN >
```

Figure 291. Listing the APPC sessions before enabling IPSec and policies

Note: The CPSVRMGR sessions will not come up until the downstream link to the SNA client comes up. This triggers the DLUR to activate its DLUR-DLUS session to VTAM.

14.9 Testing DLUR (IPSec enabled)

In this chapter we will test DLUR with IPSec enabled.

14.9.1 Enable IPSec

At this point, we can re-enable IPSec and the policies to make sure that our configuration works through our VPN tunnel. To re-enable IPSec and the policies, we use the same procedures that we used in 11.7.2, “Enable policy” on page 227.

We then check the status of the defined tunnels to make sure that they are enabled. This is shown in Figure 292, where you can see that our previously defined tunnel has been re-enabled:

```
Center IPSP>IPV4
Center IPV4-IPsec>LIST ALL
IPsec is ENABLED

IPsec Path MTU Aging Timer is 10 minutes

Defined Tunnels for IPv4:
---------------------------------------------------------------------------
   ID     Type    Local IP Addr   Remote IP Addr   Mode    State
 ------  ------  ---------------  ---------------  -----  --------
      1  ISAKMP    192.168.211.1    192.168.211.2  TUNN   Enabled

Defined Manual Tunnels for IPv6:
---------------------------------------------------------------------------

Tunnel Cache for IPv4:
------------------------------------------------------------------------------
 ID     Local IP Addr   Remote IP Addr  Mode   Policy  Tunnel Expiration
-----  ---------------  --------------- -----  ------  ------------------
    1    192.168.211.1    192.168.211.2 TUNN   ESP           none

Tunnel Cache for IPv6:
------------------------------------------------------------------------------
Center IPV4-IPsec>
```

Figure 292. Checking the status of the defined IPSec tunnels

14.9.2 List APPC sessions

Next, we check to see that the APPC sessions are still active on the 2216. This is shown in Figure 293:

```
Center APPN >
Center APPN >LIST APPC_SESSIONS
LU Name            Mode  Type  FSM
=====================================
USIBMRA.BR2216    CPSVCMG  Pri  ACT
USIBMRA.BR2216    CPSVCMG  Sec  ACT
USIBMRA.RA03M     CPSVCMG  Pri  ACT
USIBMRA.RA03M     CPSVCMG  Sec  ACT
Center APPN >
Center APPN >
```

Figure 293. Listing the active APPC sessions after enabling IPSec and policies

Now, to make sure that the APPN traffic is actually going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 294 on page 290. It shows the counter after reboot, when all counters were reset and after initiating an SNA session.

```
Center +FEATURE IPSec
Center IPSP>IPV4
Center IPV4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes   AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         119            0           119         33072        16536        16536

Sent:
  total pkts   AH packets   ESP packets   total bytes   AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         131            0           131         21832            0        21832

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors   Exceed MTU
  ----------   ----------   ----------   ----------
           0            0            0            0

Center IPV4-IPsec>
```

Figure 294. Checking the IPSec statistics

This completes the section for configuration and testing of DLUR through an IPSec tunnel.

Chapter 15. Configuring TN3270E server

The TN3270E server function available in both MRS, AIS and MAS provides a gateway function for Telnet 3270 clients that are downstream of an SNA host. These clients connect to the gateway using a TCP connection that is mapped to an SNA-dependent LU-LU session that the gateway maintains with the SNA host. Thus, the TN3270E server handles the conversion between the TN3270 data stream and an SNA 3270 data stream. Since the connections between TN3270E server and clients is based on TCP/IP, we can use IPSec to protect these connections.

In this chapter we show you how to configure TN3270E server with IPSec tunnel.

15.1 Scenario descriptions

Figure 295 shows the configuration used to produce our TN3270E scenario:

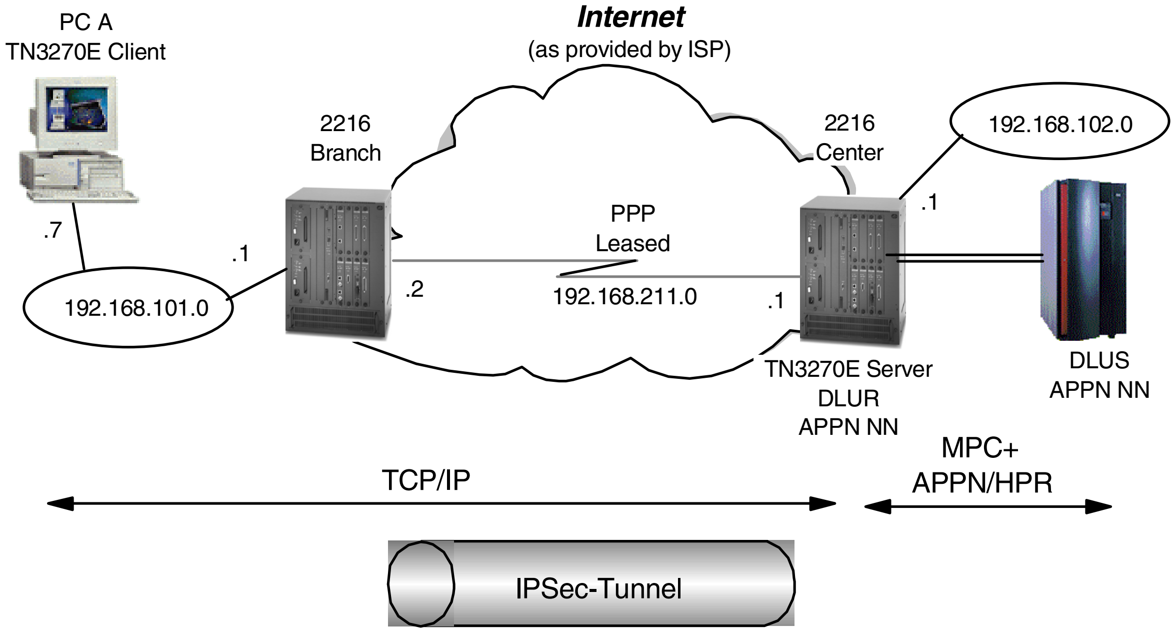


Figure 295. TN3270E through an IPSec tunnel

In our scenario, the TN3270 clients in the branch office connect to the host through the TN3270E server and DLUR configured on the 2216 in the corporate data center. We use our IPSec tunnel once again to protect them.

An MRS/AIS/MAS TN3270E server can connect to an SNA host either by APPN or by a subarea connection (V3.1 or later). In this case, we chose to use the APPN over MPC+ connection that we defined in Chapter 14, “Branch: dependent LU requester (DLUR)” on page 263**.**

We placed a PC on the branch token-ring running Telnet 3270 (in PCOMM for Windows NT). This PC is labeled PC A in the diagram. PC A connects to the TN3270E server in the 2216 located in the corporate data center at IP address 192.168.102.1. (This is an interface address on the 2216.)

The 2216 in the branch will act as a normal IP router. All TN3270 traffic between the two routers will go through the IPSec tunnel that we have configured. For example, PC A will telnet to the TN3270E server address of 192.168.102.1. This TCP/IP traffic will be funneled through the IPSec tunnel using policy 2 previously configured in Chapter 10, “Connecting the data center to the branch office” on page 197.

Note: We could also configure the 2216 router in the branch as a TN3270E server (instead of putting it in the 2216). The TN3270E server support in MRS/AIS/MAS is very flexible and allows you to make the decision to centralize or distribute this function based on your company's requirements. If we had chosen to distribute the TN3270E server function out to the branch, the DLUR configuration would be the same as in Chapter 14, “Branch: dependent LU requester (DLUR)” on page 263. The TN3270E server would use the DLUR function configured in the branch router to communicate with the DLUS in VTAM. We would use HPR/IP through our IPSec tunnel between the two routers.

15.2 IPSec and policy definitions

We defined an IPSec tunnel configured between the 192.168.211.1 and 192.168.211.2. We also defined a policy number 2, ike-pre-101-102, in Chapter 10, “Connecting the data center to the branch office” on page 197 for traffic between 192.168.101.0 and 192.168.102.0 to go through the tunnel.

In our scenario, PC A telnets to 192.168.102.1, and center 2216 router token-ring interfaces with PC A’s source IP address 192.168.101.7. Therefore, we use policy number 2, ike-pre-101-102, so that this Telnet packet goes to center 2216, TN3270E server through IPSec tunnel.

We also recommend that you make these configuration additions and test them first with the policy and IPSec feature disabled. This will help you with problem determination if you experience any problems in setting up TN3270E server.

15.3 VTAM definitions

In this scenario, three kinds of VTAM definitions are required including VTAM definitions created in Chapter 14, “Branch: dependent LU requester (DLUR)” on page 263, since we use APPN DLUR over MPC+ connection with the host and TN3270E.

For APPN DLUR of the TN3270E server to communicate with the host, we can use the same VTAM definitions that we made in 14.3, “VTAM startup parameters” on page 265.

Second we need to make additional VTAM definitions for the PUs used by the TN3270E server. We need to make a definition for each PU in the TN3270E server. For example, each PU in the TN3270E server can support up to 253 LUs. If you need 500 3270 sessions, then you will need two PUs in the router and two PU definitions in VTAM. Figure 296 shows the host VTAM switched major node definition for the TN3270E server PU for our scenario.

```
************************************************************************
*                                                                      *
*         VTAM SNA MAJNODE FOR 2216 TO MVS03                           *
************************************************************************
L032216  VBUILD TYPE=SWNET
M22163   PU    ADDR=01,ISTATUS=ACTIVE,VPACING=0,                       *
               DISCNT=NO,PUTYPE=2,SSCPFM=USSSCS,USSTAB=US327X,         *
               IDBLK=077,IDNUM=02216,IRETRY=YES,MAXDATA=521,           *
               MAXOUT=7,MAXPATH=8,PASSLIM=7,PACING=0,ANS=CONTINUE
**********************************************************************
P22163   PATH  PID=1,DLCADDR=(1,C,INTPU),DLCADDR=(2,X,07702216),      *
               DLURNAME=M22163
**********************************************************************
JC03ALU2 LU    LOCADDR=2
JC03ALU3 LU    LOCADDR=3
JC03ALU4 LU    LOCADDR=4
JC03ALU5 LU    LOCADDR=5
```

Figure 296. VTAM definitions for the TN3270E server configuration

Note

MRS/AIS and MAS CC5 V3.3 support the feature of host-initiated dynamic LU definitions. LUs are defined only in VTAM without LU definitions on 221X routers. For this new feature, an additional parameter, INCLUD0E=YES, is required in the PU definition with VTAM V4R4, APAR OW31805.

Finally we use the same definition in 14.5.2, “Definitions in VTAM for an MPC+ connection” on page 272 for MPC+ connection in VTAM.

15.4 Configuring the center router

Now that we have defined the necessary parameters, we will configure the 2216 center router for APPN DLUR, TN3270E server with IPSec disabled.

15.4.1 Preparation

Perform the initial steps as outlined below before you set up the VPN scenario.

15.4.1.1 Load necessary packages

For this scenario, we need to add the encryption package, APPN package and 3270E server package to the router's IPL sequence since we used IKE, APPN for the SNA host connection and TN3270E server function. Load these packages unless it has already been done. This is shown in Figure 297 on page 294. Once these commands have been issued, these modules will be loaded during each subsequent IPL of the router.

Note

Both APPN and subarea connectivity options for the TN3270E server require APPN support to be installed on the router. This is true even though a pure subarea configuration does not use the APPN function. This is an implementation statement as the TN3270E server function uses the APPN SNA stack for both subarea and APPN connections to the host.

```
Center Config>LOAD ADD PACKAGE encryption
encryption package configured successfully
This change requires a reload.
Center Config>LOAD ADD PACKAGE appn
appn package configured successfully
This change requires a reload.
Center Config>LOAD ADD PACKAGE tn3270e
tn3270e package configured successfully
This change requires a reload.
Center Config>WRITE
Config Save: Using bank B and config number 3
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 297. Configuring the necessary 2216 modules

15.4.1.2 Configuring APPN over MPC+ connections

Now we configure APPN over the MPC+ connection to connect the SNA host in the 2216 center router. Since we used the same connection and already defined it for the DLUR scenario in Chapter 14, “Branch: dependent LU requester (DLUR)” on page 263 refer to the definition in 14.5.3, “Definition on the router for an MPC+ connection” on page 273.

15.4.2 Enabling DLUR

We go to the talk 6 APPN protocol menus and we enable DLUR and configure the primary CP name of the DLUS in VTAM. This is shown in Figure 298:

```
Center *TALK 6
Gateway user configuration
Center Config>PROTOCOL APPN
Center APPN config>SET DLUR
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]? y
The record has been written.
```

Figure 298. Enabling DLUR on the 2216

15.4.3 Adding a local PU

Next, we add a local PU on the 2216. This local PU will be used by the TN3270E server to establish a CP-CP session to VTAM. Note that the Local Node ID in Figure 299 is the IDNUM of the switched major node configured on VTAM. (See Figure 296 on page 293.)

```
Center APPN config>ADD/UPDATE LOCAL-PU
Local PU information
    Station name (Max 8 characters) []? M22163
    Fully-qualified CP name of primary DLUS [USIBMRA.RA03M]?
    Fully-qualified CP name of a backup DLUS []?
    Local Node ID (5 hex digits) [00000]? 02216
    Enable Host Initiated Dynamic LU Definition (y/n) [N]?
    Autoactivate (y/n) [Y]?
Write this record? [Y]? y
The record has been written.
```

Figure 299. Configuring a local PU

Note

1. Each PU can handle 253 LUs, so if we needed more than 253 LUs, we would have to define another local PU that corresponds to another VTAM switched major node with a different IDNUM value.

2. To use the new feature of the MRS/AIS/MAS V3.3 host initiated dynamic LU definition, please answer y for the question, Enable Host Initiated Dynamic LU Definition (y/n) [N]? in Figure 299.

15.4.4 Configuring TN3270E server

Next, we enable and configure the TN3270E server. The TN3270E server is configured from within the protocol APPN configuration. This is shown in Figure 300:

```
Center APPN config>TN3270E
Center TN3270E config>SET
TN3270E Server Parameters
    Enable TN3270E Server (Y/N) [Y]? y
    TN3270E Server IP Address [0.0.0.0]? 192.168.102.1
    Port Number [23]?
    Enable Client Address Mapping (Y/N) [N]?
    Default Pool name (Max 8 characters) [PUBLIC]?
    NetDisp Advisor Port Number [10008]?
    Keepalive type:
    0 = none,
    1 = Timing Mark,
    2 = NOP [0]?
    Automatic Logoff (Y/N) [N]?
    Enable IP Precedence (Y/N) [N]?
Write this record? [Y]? y
The record has been written.
```

Figure 300. Enabling TN3270E server

Please keep in mind the following notes when configuring the TN3270E server:

IP Address The address that will be used by the TN3270 clients to reach the server. This address can be any interface address or the internal IP address of the router. However, keep in mind that whatever address you use for the TN3270E server will be unavailable to use as a normal Telnet to the router unless you change the port number on which the TN3270E server listens.

Reminder

> You must configure a policy that allows the TN3270E clients to access the IP address that you have defined for the TN3270E server; in this case, from the 192.168.101.0 subnet to the 192.168.102.0 subnet. (See policy number 2, ike-pre-101-102, in Chapter 10, “Connecting the data center to the branch office” on page 197.) This policy funnels the TN3270 traffic (and all other IP traffic to/from these subnets) through the IPSec tunnel.

Port Number The port number on which the TN3270E server will listen.

Keepalive Type Whether and how the server polls clients to see if they are still active. Possible values are:

None Server does not poll clients, and will only discover client absence when trying to send data.

NOP Server polls clients at the TCP level. Client software need not have capability to respond.

Timing Mark Server polls clients at the TN3270 level, and client software must respond within a certain time window.

Automatic Logoff Whether or not the server disconnects clients after a period of inactivity (with no data flowing in either direction).

IP Precedence This would be used, for example, if we had put the TN3270E server function on the branch router instead of the data center. It is used when the SNA traffic from/to the TN3270E server is encapsulated in IP packets. If enabled, then the 3 precedence bits in the TOS field of the IPv4 header will be set to a value of '011'B for all packets between the TN3270E server and the host. This allows you to preserve your SNA priorities when using BRS even on encrypted packets. Please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

Next, we define our downstream LU resources that the clients will access. The downstream LUs can be defined either as explicit or implicit:

- Use explicit definitions when you need to ensure that the device will always use the same LU name. (For example, printers would normally use explicit definitions.)
- Use implicit definitions when you have a large group of devices that can use a common pool of available LUs and do not need to use the same LU name every time.

In Figure 301 on page 297, we define an implicit pool of LUs for our TN3270E server. We specify the station name (local PU) from which the LUs will be allocated and specify the number of LUs available in this pool.

```
Center TN3270E config>**ADD/UPDATE IMPLICIT-POOL**
TN3270E Server Implicit Definitions
Pool name (Max 8 characters) [<DEFLT>]?
Station name (Max 8 characters) []? **m22163**
LU Name Mask (Max 5 characters) [@01LU]?
LU Type  ( 1 - 3270 mod 2 display
2 - 3270 mod 3 display
3 - 3270 mod 4 display
4 - 3270 mod 5 display) [1]?
Specify LU Address Ranges(s) (y/n) [N]?
Number of Implicit LUs in Pool(1-253) [1]? **4**
Write this record? [Y]?
The record has been written.
```

Figure 301. Adding LU definitions for TN3270E server

The `@01LU` is a template that will be used to create the actual LU names in the pool. In this example, with four LUs in the pool, the LU names generated are `01LU2, 01LU3, 01LU4, and 01LU5` which correspond to LOCADDRs 2-5 for the PU defined in VTAM.

Next, we list our TN3270E server configuration as shown in Figure 302 so that we can check our work:

```
Center TN3270E config>**LIST ALL**
TN3270E Server Definitions
N3270E enabled: YES
N3270E IP Address: 192.168.102.1
TN3270E Port Number: 23
Default Pool Name : PUBLIC
NetDisp Advisor Port Number: 10008
Client IP Address Mapping : N
Keepalive type: NONE
Automatic Logoff: N        Timeout: 30
      Enable IP Precedence: N
DLUS Link Station: M2216A
      Fully-qualified CP name of primary DLUS: USIBMRA.RA03M
      Fully-qualified CP name of backup DLUS:
      Local Node ID: 02216
      Auto activate : YES
      Host Initiated Dynamic LU Definition : NO
      Implicit Pool Information
      Pool Name : <DEFLT>
        Number of LUs: 4
        LU Mask: @01LU
      LU Name   NAU addr     Class Assoc LU Name   Assoc NAU addr
      -----------------------------------------------------------

Client IP Address mapping
--------------------------
Client IP Address   Address Mask       Resource Name
------------------------------------------------------

Multiple Port
------------------------------------------------------------------
PORT NUMBER    ENABLE TN3270E    RESOURCE NAME   DISABLE FILTERING
```

Figure 302. Listing TN3270E server configuration

Finally, we activate our changes to the configuration as shown in Figure 303. Note that since we have already enabled APPN previously, we can just issue the `activate` command instead of having to reload the router.

```
Center TN3270E config>ACTIVATE_NEW_CONFIG
```

Figure 303. Activating the TN3270E server configuration

15.5 Configuring the branch router

In our scenario, 2216 in the branch routes Telnet packets from PC A to 2216 in the data center. There is no required SNA function in 2216 branch.

15.6 Configuring TN3270 client in the branch office

PC A with PCOMM for Windows NT in the branch is the TN3270 client. The way to customize the TN3270 client is simple. At first, please choose Telnet3270 as shown in Figure 304:

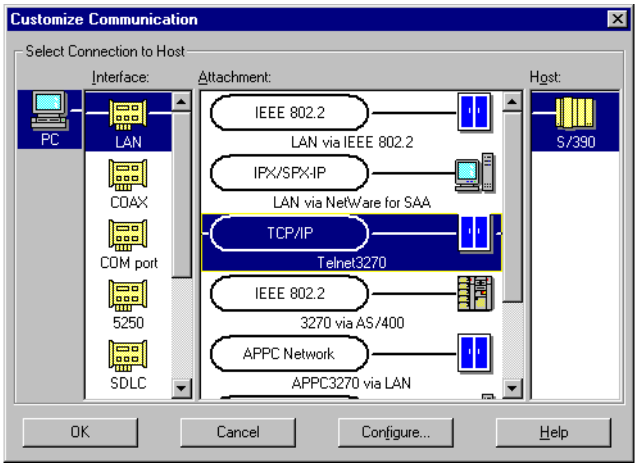
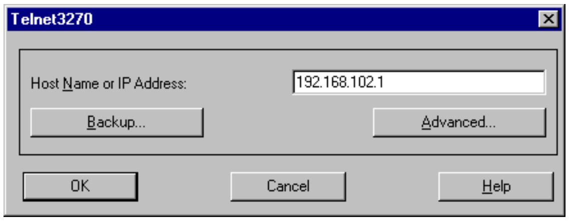


Figure 304. Choosing TN3270 configuration from PCOMM menu

Now click **Configure** and enter `192.168.102.1`, the token-ring interface of the 2216 center that we defined as a TN3270 server address in 15.4.4 on page 295:


Telnet3270

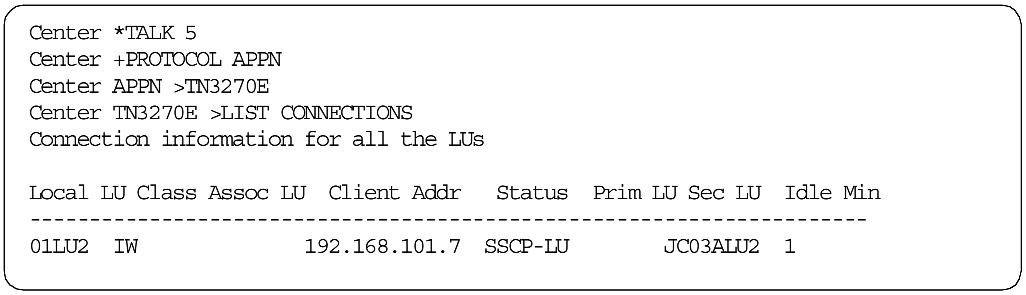
Host Name or IP Address: 192.168.102.1

Figure 305. Entering TN3270 server IP address on PCOMM

15.7 Testing TN3270E with IPSec disabled

Now it is time to test if the configuration is working as we intended. For this we see if there is an SSCP-LU session between the TN3270E server and client. (We also check our TN3270 client and see if it has an active connection to the host.)

From talk 5, in the TN3270 monitor, we issue the `list connections` command as shown in Figure 306. As you can see, there is one LU that has a connection from client PC A 192.168.101.7:



```
Center *TALK 5
Center +PROTOCOL APPN
Center APPN >TN3270E
Center TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU Class Assoc LU  Client Addr   Status  Prim LU Sec LU  Idle Min
----------------------------------------------------------------------
01LU2  IW              192.168.101.7  SSCP-LU        JC03ALU2  1
```

Figure 306. Checking the TN3270E server for LU status

15.8 Testing TN3270E with IPSec enabled

Next, we re-enable policy and IPSec, then check if the TN3270E server is still working. In Figure 307, we check the IPSec status. We see that both our policies as well as the IPSec feature are enabled.

```
Center Config>FEATURE Policy
Center Policy config>LIST POLICY ALL
    Policy Name     = ipsec_man_101_102
    State:Priority =Disabled   : 5
    Profile        =101.0-to-102.0
    Valid Period   =allTheTime
    Manual Tunnel  =1
    TunnelInTunnel =No

    Policy Name     = ike-pre-101-102
    State:Priority =Enabled    : 5
    Profile        =101.0-to-102.0-pre
    Valid Period   =allTheTime
    IPSEC Action   =tun-101-102
    ISAKMP Action  =ike-1

    Policy Name     = ike-pre-3-100
    State:Priority =Enabled    : 10
    Profile        =3.0-to-100.0.pre
    Valid Period   =allTheTime
    IPSEC Action   =tun-101-102
    ISAKMP Action  =ike-1

    Policy Name     = ike-pre-211-211
    State:Priority =Enabled    : 5
    Profile        =211.0-to-211.0-pre
    Valid Period   =allTheTime
    IPSEC Action   =tun-101-102
    ISAKMP Action  =ike-1
Center Policy config>EXIT
Center Config>FEATURE IPSec
IP Security feature user configuration
Center IPsec config>IPV4
Center IPV4-IPsec config>LIST ALL

IPsec is ENABLED
IPSec Path MTU Aging Timer is 10 minutes
IPv4 Tunnels
-------------------------------------------------------------------
ID    Name         Local IPv4 Addr  Rem IPv4 Addr    Mode    State
-- --------------  ---------------  ---------------  -----  --------
1 tun_101.0-102.0  192.168.211.1    192.168.211.2    TUNN   Enabled
```

Figure 307. Listing IPSec enabled

To make sure that the TN3270 client traffic is going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 308.

```
Center +FEATURE IPSec
Center IPSP>IPV4
Center IPV4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

                             Global IPSec Statistics
Received:
total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
----------   ----------   -----------   -----------   ----------   ----------
351            0            351         61184        30592        30592
Sent:
total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
----------   ----------   -----------   -----------   ----------   ----------
362            0            362         53064            0        53064
Receive Packet Errors:
total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
----------   ----------   ----------   ----------   -----------
0            0            0            0              0
Send Packet Errors:
total errs    AH errors   ESP errors   Exceed MTU
----------   ----------   ----------   ----------
0            0            0            0
```

Figure 308. Checking IPSec statistics

Chapter 16. Connecting business partners and suppliers

In this chapter we describe how IBM VPN solutions can be used to implement virtual private networks based on the business partner/supplier scenario. Essentially, this means building an extranet between different companies and so there are two major issues to be considered:

Access Control: While it may be a business necessity for supplier A to have access to some of company X's internal resources (such as databases), there will also be valid business reasons to prevent the supplier from having access to all of company X's databases.

Data Confidentiality: Clearly the data should be hidden from general view while it is in transit over the public Internet. But there may be even more stringent requirements. Company X may consider its own intranet to be trusted, but its suppliers may not. For example, a supplier may want to ensure that its sensitive data, while traveling through Company X's intranet, is hidden until it reaches its final destination. For example, the supplier may be worried that an unscrupulous eavesdropper inside Company X may try to intercept the data and sell it to a competitor. And Company X may have the same concerns about its data as it travels though the supplier's intranet. Thus, it will not be unusual for each party to treat the other's intranet as untrusted.

In a previous chapter we created a router-to-router tunnel as a branch office scenario. To accomplish above access control and data confidentiality between business partners, companies want to terminate their tunnel at their data endpoints. Therefore, an end-to-end (host-to-host) tunnel or a host-to-gateway tunnel is an additional requirement.

The scenarios for an end-to-end (host-to-host) tunnel are extensively described in the redbook *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*, SG24-5309. This redbook also provides more details of considerations for business partner/suppliers connections.

In this chapter we will configure AIX to a router tunnel as an example of a host-to-gateway tunnel as a business partner solution. However, the router is configured in the same way regardless of the machine type of the remote end host, so you could refer to this configuration for any host-to-gateway tunnel.

16.1 Scenario description

In this scenario, we are presenting a business partner relationship between an enterprise and a small vendor. The vendor needs not access the enterprise’s entire resources but access only the enterprise’s one AIX server over the Internet. Not only does it want the data to flow securely over the public network, but the enterprise does not fully trust its vendor and therefore, the enterprise wants to ensure the connection is protected by IPSec protocols to the very hosts the vendor wants to connect. Figure 309 represents this scenario.

The vendor subnetwork for clients to access the enterprise is 192.168.101.0 and the enterprise’s AIX IP address is 192.168.100.3, which is located behind a firewall. We configure the ESP tunnel mode tunnel between the router interface to the Internet, 192.168.211.2, and the AIX IP address 192.168.100.3. Therefore, the firewall should be configured to permit only IPSec protocols with destination 192.168.100.3 and source address 192.168.101.0, which is the vendor subnetwork.

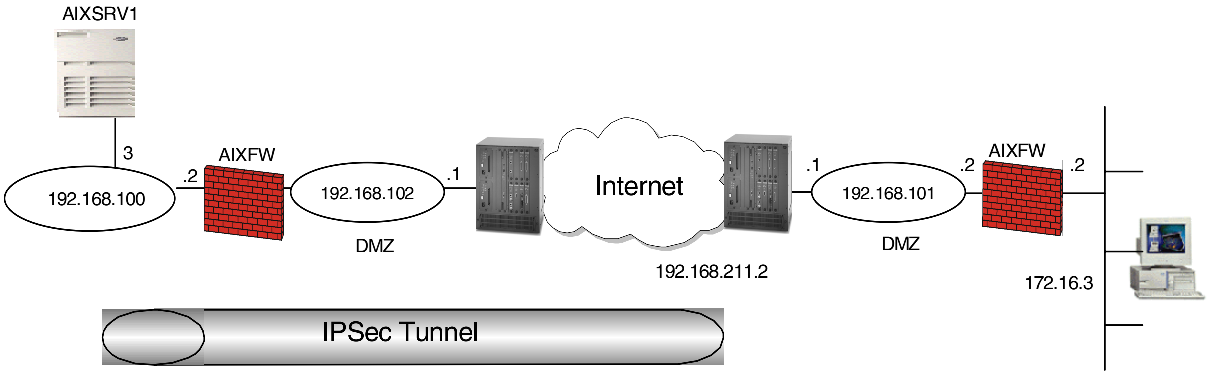


Figure 309. IPSec tunnel between AIX and 2216 router

16.2 Configuring 2216 business partner router

To define the router parameter, we use the same table used in Chapter 10, “Connecting the data center to the branch office” on page 197.

We have the following matrixes:

- Remote User Definition (Table 20)
- Policy Definitions (Table 21)
- Definition of the Policy Profile (Table 22)
- Definition of the Policy Validity Profile (Table 23)
- Definition of IPSec Action Profile Phase 2 (Table 24)
- IPSec Proposal (Table 25)
- IPSec Transform for IKE Phase 2 (Table 26)
- Definition of ISAKMP Action for IKE Phase 1 (Table 27)
- Definition of ISAKMP Proposal for IKE Phase 2 (Table 28)

In the table you have two specification columns for the router-to-router tunnel definition, but we define only one column as the partner is not router but AIX. We will use another planning sheet for AIX configuration in 16.3, “Configuring AIX” on page 309.

In the very most cases we can work with the default values, only in some cases you have to modify the default values. We marked these cases in **boldface**.

Table 20. Remote User Definitions

Information you need to create your VPN	**BP router**
How to identify the remote IKE peer (user): 1: IP address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID	Option 1: IP-address
IP Address that distinguishes this user?	**192.168.100.3**
Authenticate user with 1: Pre-shared key 2: Public certificate?	pre-shared key
Mode in which you will enter the pre-shared key: 1: ASCII 2: HEX	Option 1: ASCII
Pre-shared key (even number of characters):	**12345678**

Table 21. Policy definitions

Information you need to create your VPN	**BP router**
Policy name:	**ike-pre-aix-3-pre**
Priority of this policy in case of multiple policies:	5

Table 22. Definition of the Policy Profile

Information you need to create your VPN	**BP router**
Profile name:	**101.0-to-102.0-pre**
Source address format 1: NetMask 2: Range 3: Single address	1:NetMask
IPv4 Source address	**172.16.3.0**
IPv4 Source Mask (255.255.255.0)	255.255.255.0
Destination address format 1: NetMask 2: Range 3: Single address	**3:Single address**
Destination address	**192.168.100.3**
Select the protocol to filter on 1: TCP 2: UDP 3: All protocols 4: Specify range	Option 3: All protocols
Starting value for the source port: 0 for all protocols	0

Information you need to create your VPN	BP router
Ending value for the source port: 65535 for all protocols	65535
Starting value for the destination port: 0 for all protocols	0
Ending value for the destination port: 65535 for all protocols	65535
Enter the mask to be applied to the Received-DS-byte:	0
Enter the value to match against after the mask has been applied to the Receive-DS-byte	0
Do you want to configure local and remote IDs for ISAKMP?	**Yes**
Select the identification type of the local ID to be sent to the remote IKE peer 1: Local tunnel endpoint address 2: Fully qualified domain name 3: User fully qualified domain name 4: Key ID (any string)	Option 1: local tunnel endpoint address
Any user within profile allowed access	Yes
Do you want to limit this profile to specific interface(s)?	No

Table 23. Definition of the Policy Validity Profile

Information you need to create your VPN	BP router
Validity profile name:	Option 1: allTheTime

Table 24. Definition of IPSec Action Profile Phase 2

Information you need to create your VPN	BP router
IPSec action profile name:	**tun-aix-3**
Select the IPSec security action type: 1: Block 2: Permit	permit
Should the traffic flow into a secure tunnel or in the clear? 1: Clear 2: Secure tunnel	Secure tunnel
What is the tunnel start-point IP address?	**192.168.211.2**
What is the tunnel end-point IP address?	**192.168.100.3**
Does this IPSec tunnel flow within another IPSec tunnel?	No

Information you need to create your VPN	BP router
Percentage of SA lifesize/lifetime to use as the acceptable minimum? Default is 75 %	75
Security association refresh threshold in percent Default is 85 %	85
Select the option for the DF bit in the outer header 1: Copy 2: Set 3: Clear	Copy
Do you want to enable replay prevention?	Disable
Do you want to negotiate the security association at system initialization (autostart)?	No

Table 25. IPSec Proposal

Information you need to create your VPN	BP router
What name do you want to give this IPSec proposal?	**esp-pre-aix-prop**
Does this proposal require Diffie Hellman Perfect Forward Secrecy?	No
Do you wish to enter any AH transforms for this proposal?	No
Do you wish to enter any ESP transforms for this proposal?	**Yes**

Table 26. IPSec Transform for IKE Phase 2

Information you need to create your VPN	BP router
IPSec ESP transform name:	**esp-tun-aix**
Select the protocol ID: 1: IPSec AH 2: IPSec ESP	Option 2: IPSec ESP
Select the encapsulation mode: 1: Tunnel 2: Transport	Option 1: Tunnel
Select the ESP authentication algorithm: 0: None 1: HMAC_MD5 2: HMAC_SHA	Option 1: HMAC_MD5
Select the ESP cipher algorithm: 1: ESP DES 2: ESP 3DEC 3: ESP CDMF 4: ESP NULL	Option 1: ESP DES

Information you need to create your VPN	BP router
What is the SA lifesize, in kilobytes Default is 50000 kilobytes	50000
What is the SA lifetime? Default is 3600 sec	**1800**

Table 27. Definitions for ISAKMP Action for IKE Phase 1

Information you need to create your VPN	BP router
ISAKMP action name:	**act-aix**
Select the ISAKMP exchange mode: 1: Main 2: Aggressive	Option 1: Main
Percentage of SA lifesize/lifetime to use as the acceptable minimum: Default is 75 %	75
What is the ISAKMP connection lifesize, in kilobytes? Default is 5000 kilobytes	5000
What is the ISAKMP connection lifetime in seconds? Default is 30000 sec	**28800**
Do you want to negotiate the SA at system initialization (autostart)?	Yes

Table 28. Definitions for ISAKMP Proposal for IKE Phase 2

Information you need to create your VPN	BP router
ISAKMP proposal name:	**ike-pre-aix-prop**
Select the authentication method 1: Pre-shared key 2: Digital certificate	Option 1: Pre-shared key
Select the hashing algorithm 1: MD5 2: SHA	Option 1: MD5
Select the cipher algorithm 1: DES 2: 3DES	Option 1: DES
What is the SA lifesize, in kilobytes? Default is 1000 kilobytes	1000
What is the SA lifetime? Default is 15000 sec	15000
Select the Diffie-Hellman Group ID 1: Diffie-Hellman Group 1 2: Diffie-Hellman Group 2	Option 1: Diffie Hellman Group 1

Information you need to create your VPN	BP router
Do you wish to map a DiffServ Action to this policy?	No
What will the status of the policy be? 1: Enabled 2: Disabled	Option 1: Enabled

16.3 Configuring AIX

Now we configure the IPSec tunnel in AIX. First we complete the planning sheet for the parameters and second we show the practical configuration steps.

16.3.1 Completing AIX planning worksheet

Complete the AIX planning worksheet as shown in Table 29. The planning worksheet allows you to gather all the configuration data before the actual implementation. We completed this planning worksheet from the perspective of AIXSVR1 in this scenario.

Table 29. AIX planning worksheet - Internet Key Exchange (IKE) tunnels configuration

Information you need to configure VPN in the AIX server	Scenario answers
Key server host name	AIXSVR1
IP Address	192.168.100.3
Role	responder
Key Management Tunnel (Phase 1)	
Mode	Main
Encryption	DES
Authentication Algorithm	MD5
Key Exchange Group	1
Key Lifetime	28800 sec (default)
Negotiation ID	IP Address
Pre-shared key	3132333435363738 (12345678 in ASCII)
Data Management Tunnel (Phase 2) **Security Protocols**	
AH (Authentication)	
✓ ESP (Encryption)	DES
✓ ESP (Authentication)	MD5
Encapsulation mode	Transport
Perfect Forward Secrecy (PFS)	No
Tunnel Lifetime	30 min

16.3.2 Defining IPSec tunnel in AIX

Perform the following steps to configure a host-to-host VPN on AIXSRV1 using the Web System Management tool:

1. Start Web System Management tool.
2. Double-click the **Network** icon.
3. Right-click **Internet Key Exchange (IKE) Tunnels** and select **Start IP Security** from the pull-down menu to enable IPSec.
4. Double-click **Internet Key Exchange (IKE) Tunnels** on the Network panel to open the Internet Key Management (IKE) Tunnel configuration panel.

The Internet Key Exchange (IKE) Tunnels configuration panel is displayed in Figure 310:

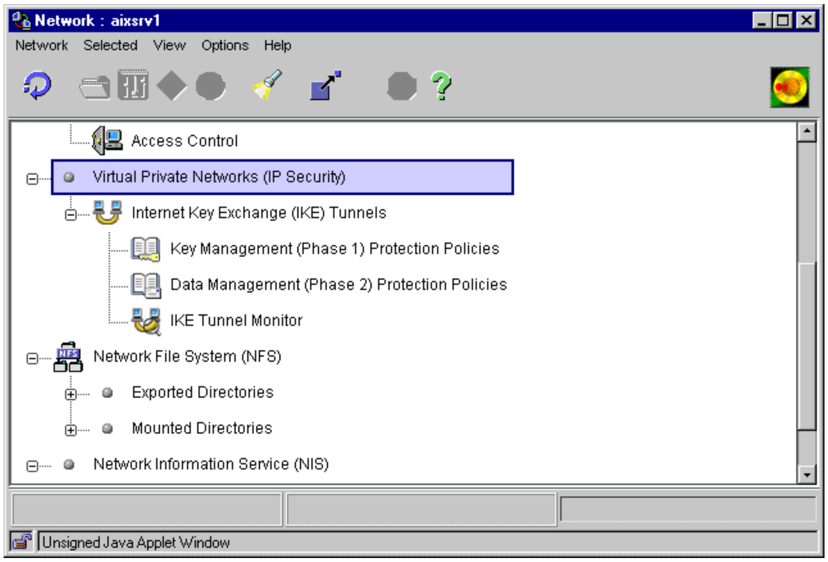
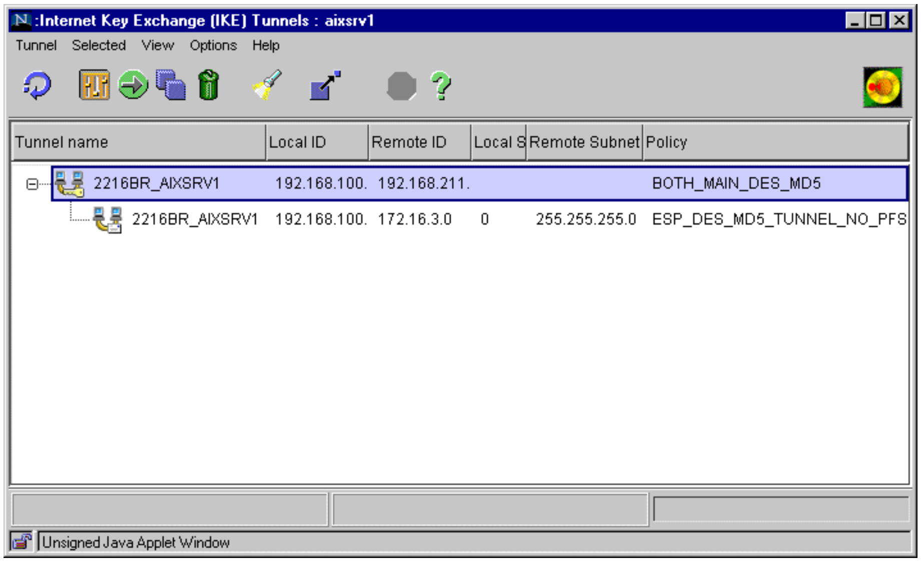

Network : aixsrv1
Network
Selected
View
Options
Help
Access Control
Virtual Private Networks (IP Security)
Internet Key Exchange (IKE) Tunnels
Key Management (Phase 1) Protection Policies
Data Management (Phase 2) Protection Policies
IKE Tunnel Monitor
Network File System (NFS)
Exported Directories
Mounted Directories
Network Information Service (NIS)
Unsigned Java Applet Window

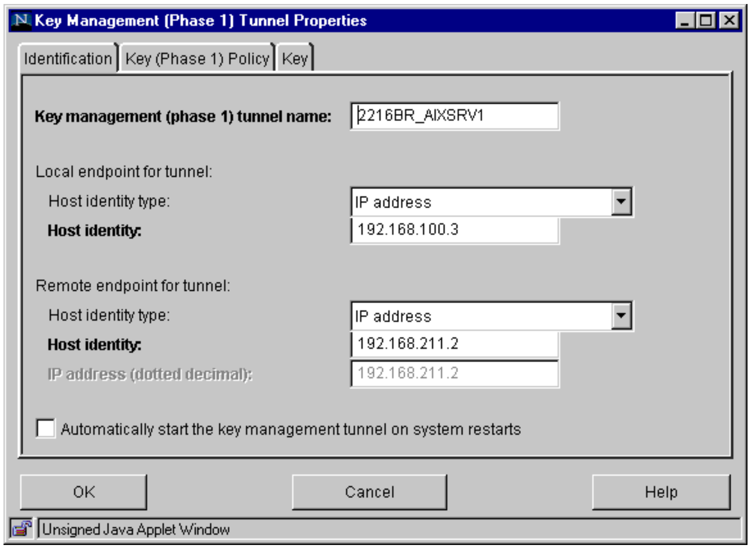
Figure 310. Network panel - VPN menu


:Internet Key Exchange (IKE) Tunnels : aixsrv1
Tunnel
Selected
View
Options
Help
Unsigned Java Applet Window

Tunnel name	Local ID	Remote ID	Local S	Remote Subnet	Policy
2216BR_AIXSRV1	192.168.100.	192.168.211.			BOTH_MAIN_DES_MD5
2216BR_AIXSRV1	192.168.100.	172.16.3.0	0	255.255.255.0	ESP_DES_MD5_TUNNEL_NO_PFS

Figure 311. Internet Key Exchange (IKE) Tunnel configuration panel

5. Select **Tunnel -> New Key Management Tunnel** to open the Key Management (Phase 1) Tunnel Properties window as shown in Figure 311:


Key Management (Phase 1) Tunnel Properties
Identification
Key (Phase 1) Policy
Key
OK
Cancel
Help
Unsigned Java Applet Window

Key management (phase 1) tunnel name: 2216BR_AIXSRV1

Local endpoint for tunnel:
Host identity type: IP address
Host identity: 192.168.100.3

Remote endpoint for tunnel:
Host identity type: IP address
Host identity: 192.168.211.2
IP address (dotted decimal): 192.168.211.2

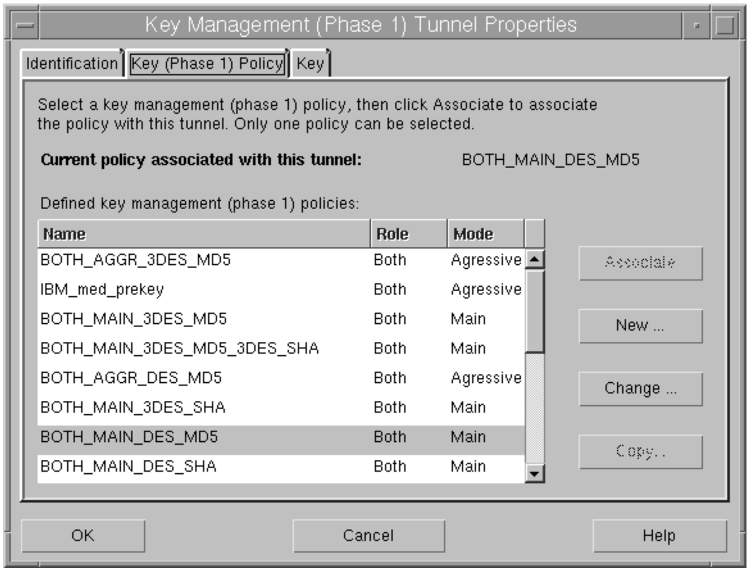
☐ Automatically start the key management tunnel on system restarts

Figure 312. Key Management (Phase 1) Tunnel Properties: Identification

6. On the Identification panel, enter the key management tunnel name; in this scenario, 2216BR_AIXSRV1.

7. Select **IP address** as Host identity type for the local and remote endpoint for the tunnel and enter the IP addresses of the local and remote hosts.

8. Select the **Key (Phase 1) Policy** window. The Key Management (Phase 1) Tunnel Properties panel (Figure 312) is displayed.



Select a key management (phase 1) policy, then click Associate to associate the policy with this tunnel. Only one policy can be selected.

Current policy associated with this tunnel: BOTH_MAIN_DES_MD5

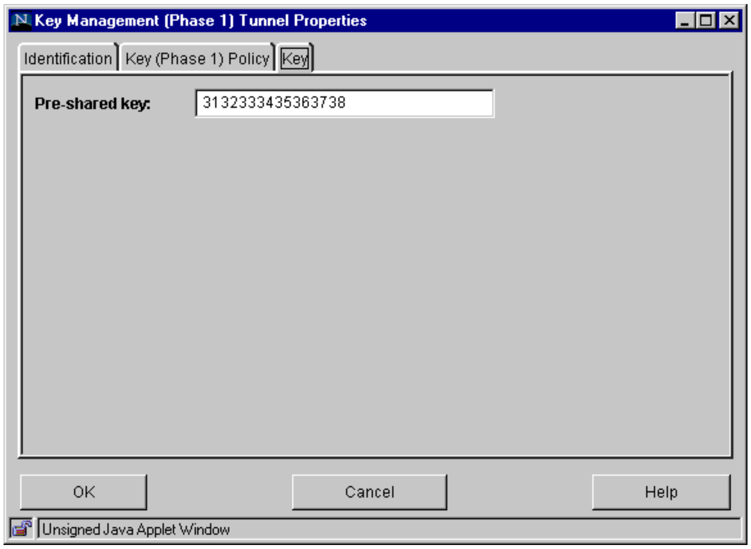
Defined key management (phase 1) policies:

Name	Role	Mode
BOTH_AGGR_3DES_MD5	Both	Agressive
IBM_med_prekey	Both	Agressive
BOTH_MAIN_3DES_MD5	Both	Main
BOTH_MAIN_3DES_MD5_3DES_SHA	Both	Main
BOTH_AGGR_DES_MD5	Both	Agressive
BOTH_MAIN_3DES_SHA	Both	Main
BOTH_MAIN_DES_MD5	Both	Main
BOTH_MAIN_DES_SHA	Both	Main

Figure 313. Key Management (Phase 1) Tunnel Properties: Key (Phase 1) Policy

9. Select **BOTH_MAIN_DES_MD5** policy from Defined key management (phase 1) policies and click **Associate**.

10.Select **Key.** The Key Management (Phase I) Tunnel Properties is displayed in Figure 313:


Key Management (Phase 1) Tunnel Properties
Identification
Key (Phase 1) Policy
Key
OK
Cancel
Help
Unsigned Java Applet Window

Pre-shared key: 3132333435363738

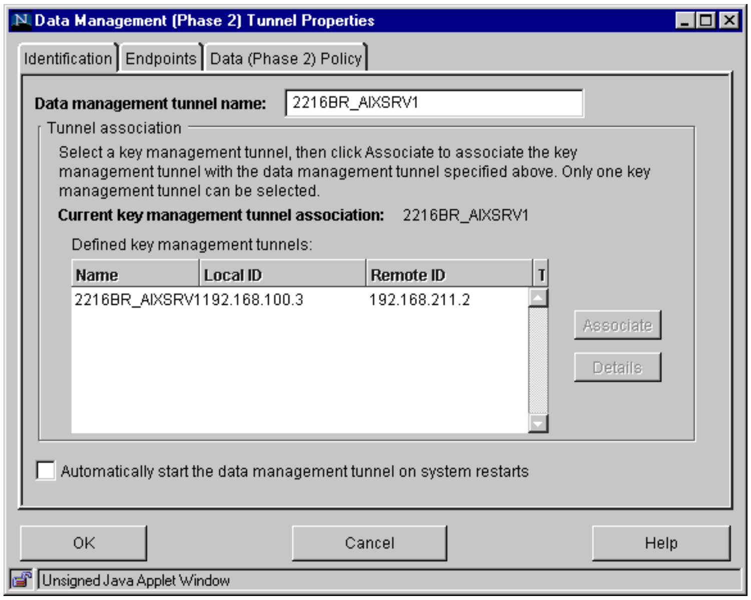
Figure 314. Key Management (Phase 1) Tunnel Properties: Key

11.Enter the pre-shared key. Use the hexadecimal notation. For example, Hex 31, 32 is equivalent to the ASCII decimal value 1, 2, etc. entered on the router configuration.

12.Click **OK.**

You have now completed the key management tunnel configuration. Next, configure the data management tunnel associated with the key management tunnel.

13.Select **Tunnel -> New Data Management Tunnel** on the Internet Key Exchange (IKE) Tunnels configuration panel (Figure 311 on page 310) to open the Data Management (Phase 2) Tunnel Properties window (see Figure 315).



Data management tunnel name: 2216BR_AIXSRV1

Tunnel association

Select a key management tunnel, then click Associate to associate the key management tunnel with the data management tunnel specified above. Only one key management tunnel can be selected.

Current key management tunnel association: 2216BR_AIXSRV1

Defined key management tunnels:

Name	Local ID	Remote ID	T
2216BR_AIXSRV1	192.168.100.3	192.168.211.2	

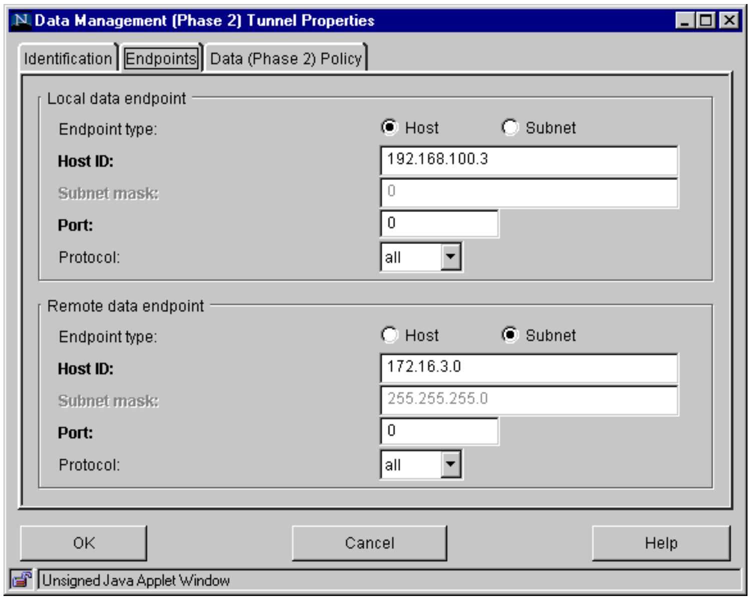
□ Automatically start the data management tunnel on system restarts

Figure 315. Data Management (Phase 2) Tunnel Properties: Identification

14.On the Identification panel, enter the data management tunnel name; in this scenario, 2216BR_AIXSRV1.

15.Select the key management tunnel that should be associated with this data management tunnel; in this scenario, 2216BR_AIXSRV1, and click **Associate**.

16.Click **Endpoints.** The Data Management (Phase 2) Tunnel Properties window (Figure 316) is displayed.


Data Management (Phase 2) Tunnel Properties
Identification
Endpoints
Data (Phase 2) Policy
OK
Cancel
Help
Unsigned Java Applet Window

Local data endpoint

Endpoint type: ● Host ○ Subnet

Host ID: 192.168.100.3

Subnet mask: 0

Port: 0

Protocol: all

Remote data endpoint

Endpoint type: ○ Host ● Subnet

Host ID: 172.16.3.0

Subnet mask: 255.255.255.0

Port: 0

Protocol: all

Figure 316. Data Management (Phase 2) Tunnel Properties: Endpoints

17.For Local data endpoint enter:

Endpoint type:**Host** (this is a host-to-gateway scenario)

Host ID: `192.168.100.3`

Port: `0` (every port is allowed)

Protocol: **all** (every protocol is allowed)

18.For Remote data endpoint enter:

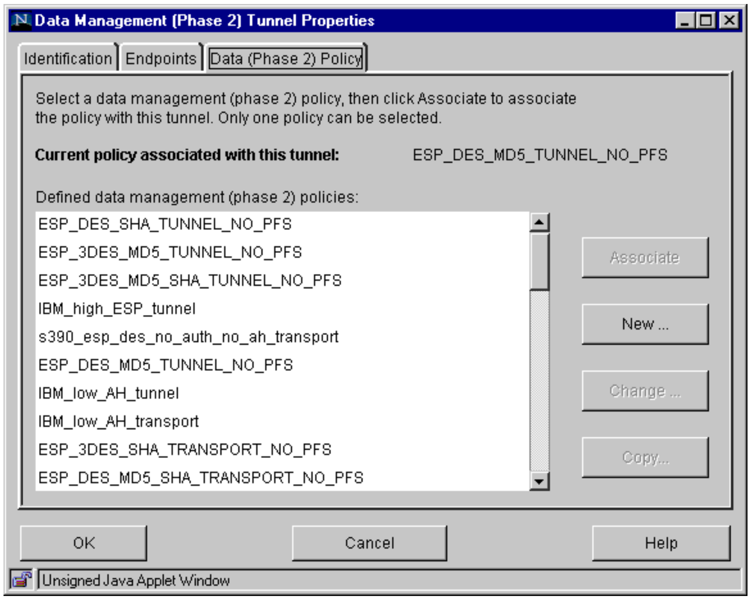
Endpoint type:**Sub net** (this is a host-to-gateway scenario)

Host ID: `192.168.211.2`

Port: `0` (every port is allowed)

Protocol: **all** (every protocol is allowed)

19.Click **Data (Phase 2) Policy.** The Data Management (Phase 2) Tunnel Properties panel (Figure 317) is displayed.



Data Management (Phase 2) Tunnel Properties

Select a data management (phase 2) policy, then click Associate to associate the policy with this tunnel. Only one policy can be selected.

Current policy associated with this tunnel: ESP_DES_MD5_TUNNEL_NO_PFS

Defined data management (phase 2) policies:

ESP_DES_SHA_TUNNEL_NO_PFS
ESP_3DES_MD5_TUNNEL_NO_PFS
ESP_3DES_MD5_SHA_TUNNEL_NO_PFS
IBM_high_ESP_tunnel
s390_esp_des_no_auth_no_ah_transport
ESP_DES_MD5_TUNNEL_NO_PFS
IBM_low_AH_tunnel
IBM_low_AH_transport
ESP_3DES_SHA_TRANSPORT_NO_PFS
ESP_DES_MD5_SHA_TRANSPORT_NO_PFS

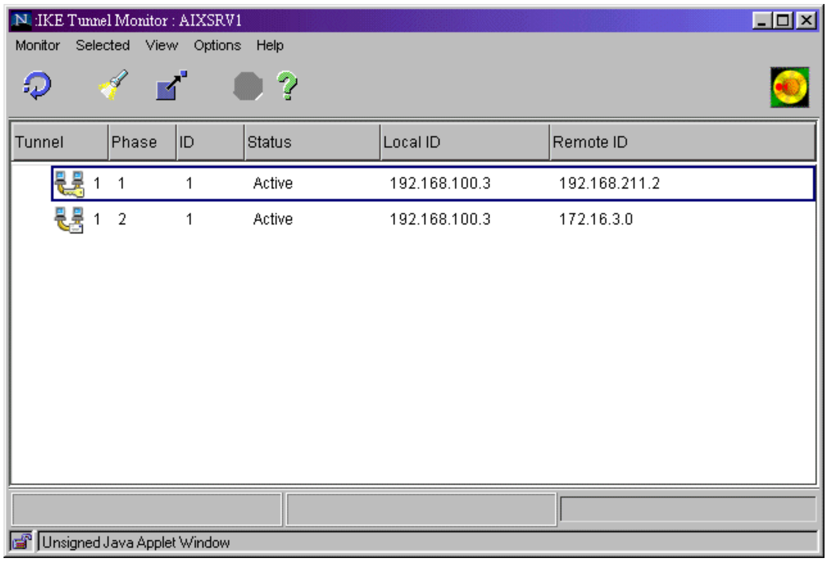
Unsigned Java Applet Window

Figure 317. Data Management (Phase 2) Tunnel Properties: Data (Phase 2) Policy

20.Select **ESP_DES_MD5_TRANSPORT_NO_PFS** policy from Defined data management (phase 2) policies and click **Associate.**

21.Click **OK.**

Now the data management tunnel is configured. The IKE Tunnel Monitor is used to check the status of IKE tunnels. Double-click **IKE Tunnel Monitor** under the Virtual Private Networks (IP Security) Network panel. The status of the Phase 1 and Phase 2 tunnels is displayed in Figure 318:



Tunnel	Phase	ID	Status	Local ID	Remote ID
1	1	1	Active	192.168.100.3	192.168.211.2
1	2	1	Active	192.168.100.3	172.16.3.0

Figure 318. IKE Tunnel Monitor

16.4 Testing the IPSec tunnel in the router

As we validated the tunnel is active on IKE Tunnel Monitor in AIX, we want to check the IPSec tunnel in the router. Through the `TALK 5, FEATURE IPSec, IPV4, LIST TUNNEL ACTIVE` commands, we view the ESP tunnel between the 192.168.211.2 BP router and 192.168.100.3 AIX server.

```
Branch *TALK 5
Branch +FEATURE IPSec
Branch IPSP>IPV4
Branch IPV4-IPsec>LIST TUNNEL ACTIVE
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Tunnel Cache for IPv4:
--------------------------------------------------------------------------
 ID     Local IP Addr   Remote IP Addr  Mode   Policy  Tunnel Expiration
-----  --------------- --------------- -----  ------  ------------------
    1    192.168.211.2    192.168.100.3  TUNN   ESP           none
```

Figure 319. Active tunnel list

To make sure that the traffic between the AIX server and client in 172.16.3.0 is going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 320:

```
Branch IPV4-IPsec>STATS
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

                       Statistics For Secure Tunnel 1
Received:
 total ops    AH ops       ESP ops       total bytes   AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          65            0            65         11440         5720         5720

Sent:
  total ops    AH ops       ESP ops       total bytes   AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          65            0            65          6760            0         6760

Receive Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

Send Errors:
   AH errors   ESP errors   Exceed MTU
  ----------   ----------   ----------
           0            0            0
```

Figure 320. IPSec statistics

Finally, check that the appropriate policy is used from statistics in `FEATURE Policy`, `TALK 5`.

```
Branch +FEATURE Policy
IP Network Policy console
Branch Policy console>LIST STATS
+-------------------------------------------------------+
|Name                                          |Hits    |
+-------------------------------------------------------+
|ike-pre-aix-3-pre.p2in                        |       1|
|                             tun-aix-3(IPSEC)|     167|
+-------------------------------------------------------+
|ike-pre-aix-3-pre.p1in                        |       3|
|    act-aix                         (ISAKMP)|       3|
+-------------------------------------------------------+
|ike-pre-aix-3-pre.traffic                     |      83|
|                             tun-aix-3(IPSEC)|     167|
+-------------------------------------------------------+
|ike-pre-aix-3-pre.inBoundTunnel               |      83|
|           ipsecPermitIfInboundTunnel(IPSEC)|      83|
+-------------------------------------------------------+
```

Figure 321. Policy statistics

Chapter 17. Connecting remote users with voluntary tunneling

Voluntary tunneling is where the tunnel is initiated from the client or LAC. All that is required is an IP infrastructure between the LAC and LNS and no other device needs to be involved. The IP connectivity could be achieved through a temporary connection by dialing in to an ISP or through a permanent connection such as a LAN interface. As far as voluntary tunneling is concerned it does not matter as long as the IP connectivity is there. As a result you do not have to establish a trust relationship (service level agreement) with the ISP as it is totally transparent to the process.

17.1 Voluntary tunneling with IBM routers

IBM's 221x routers support voluntary tunneling using L2TP and Microsoft's PPTP. Both methods are implemented in the same manner. With voluntary tunneling you can emulate a dial-up PPP connection where you get a dynamic IP address that is owned by the LNS, or you can emulate a nondial-up PPP connection where static IP addresses are used on each end of the point-to-point PPP connection.

The following will describe how the components of the IBM routers fit into a voluntary layer-2 tunneling framework in both these situations.

17.1.1 Emulating nondial-up PPP

It is important to remember that all layer-2 technologies eventually form a network structure where the network sees the layer-2 tunnel as a PPP link. Therefore, when the LAC builds the tunnel to the LNS, as far as the corporate network is concerned it looks just like a standard PPP connection to the corporate gateway. We will use this as our reference point when showing how the IBM routers fit into the layer-2 framework (see Figure 322).

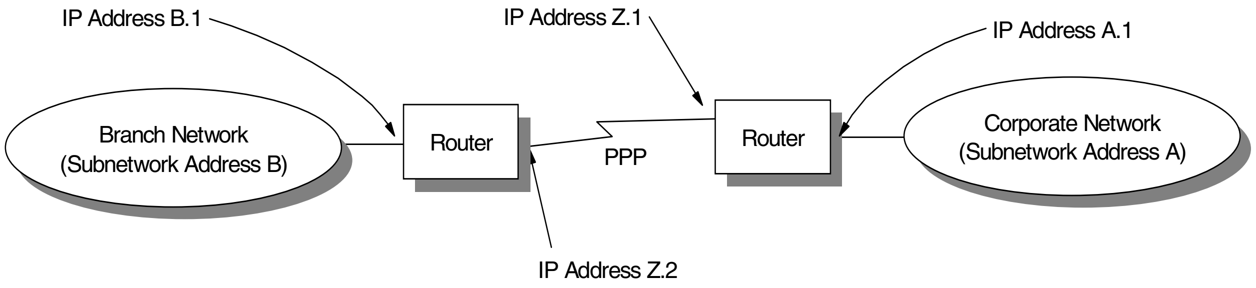


Figure 322. PPP reference diagram

Since the layer-2 tunneling structure tries to emulate a simple PPP infrastructure we should initially examine how an IBM 221x router implements its components to support such an environment.

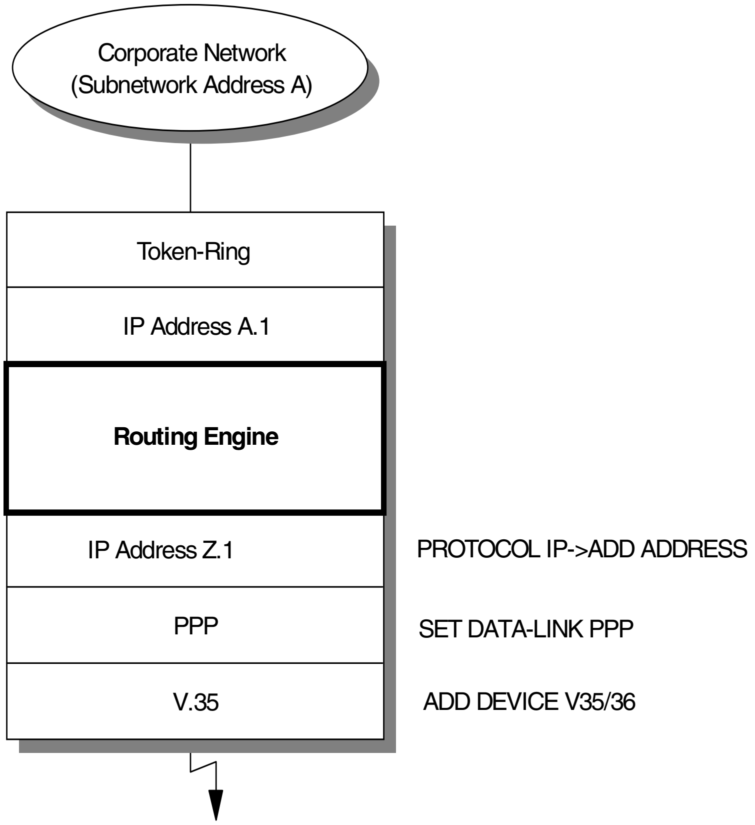


Figure 323. IBM router implementation with PPP

Figure 323 shows how the IBM router implements a standard PPP interface. The implementation is identical whether it is the branch or corporate router. With layer-2 tunneling we try to emulate this PPP infrastructure, however, the architecture differentiates two ends of the emulated PPP link as the LAC and LNS, representing the branch and corporate routers. In practice there is no difference when emulating a nondial-up PPP connection, just the setup of the connection direction.

The following are the basic steps required to set up PPP on an IBM router:

1. Define the physical interface.
2. Define PPP.
3. Define the IP components.

Referring to Figure 324 on page 319, we can see how the above three steps are applied to a virtual PPP interface running in a layer-2 tunnel.

Voluntary tunneling assumes that there is already IP connectivity between the LNS and LAC. This could have been achieved by any method including permanent connections like Ethernet or even temporary dial-up connections as described in Chapter 19, “Connecting dial-up routers with L2TP” on page 387.

The IP connectivity forms part of step 1. The rest of step 1 is done by building a layer-2 tunnel which can then carry the PPP stream over a layer-3 IP network to the LNS. This layer-2 tunnel is generated by the command `ADD TUNNEL-PROFILE`. In this step you configure the IP address of the tunnel endpoint, the name of the tunnel (which is the local name of the tunnel at the LNS) and the local name of the tunnel. In addition you have to configure a secret password. These parameters will authenticate the tunnel. Once authenticated the PPP circuit can go through the tunnel.

The router must now be configured with a PPP interface (step 2). The problem is that a PPP interface does not exist, for example, there is no serial port that could be used to run PPP. Therefore, the IBM router must put in place a virtual layer-2 interface with the command `ADD DEVICE LAYER-2 TUNNELING`.

Step 3 requires that an IP address be assigned and that is done in the normal manner by `PROTCOL IP-->ADD ADDRESS`.

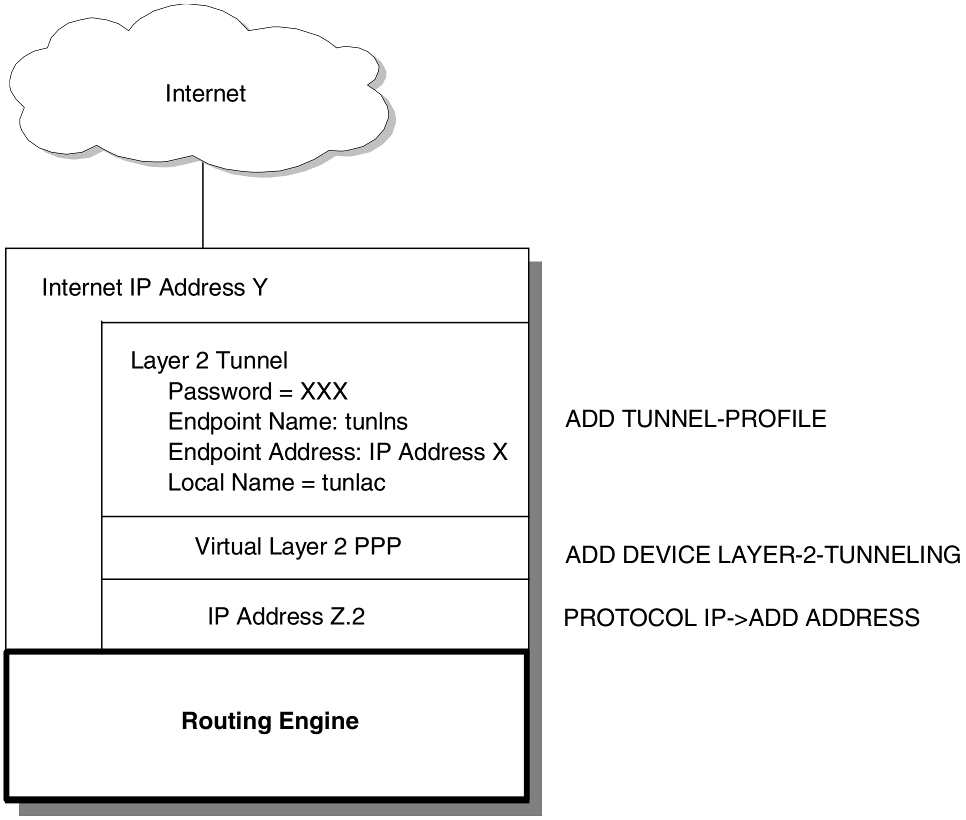


Figure 324. IBM router implementation of LAC

The configuration steps in the LNS are identical see Figure 325 on page 320. The only real difference is the connection direction, which is defined in the virtual layer-2 interface.

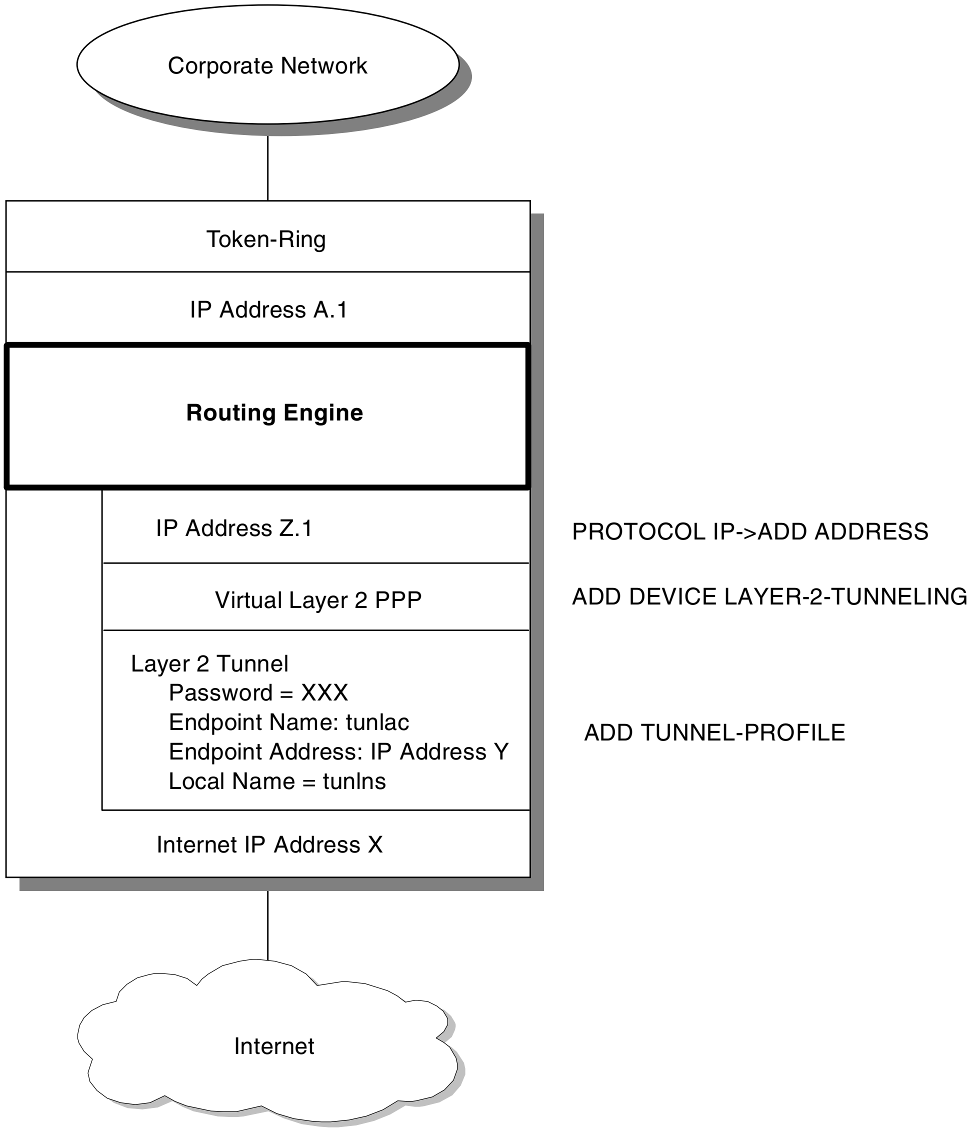


Figure 325. IBM router implementation of LNS

The end result is that from the corporate gateway (LNS) point of view it thinks that all its PPP dial-in circuits are locally attached and the user's point of view is that it is directly dialing in to the corporate router per the reference diagram (Figure 323 on page 318). In reality they are split in half and the joining point is the virtual PPP interface at the LNS and LAC (see Figure 331 on page 326). Compare this diagram with Figure 326 on page 321 which shows the IBM router implementation with a PPP dial-in user.

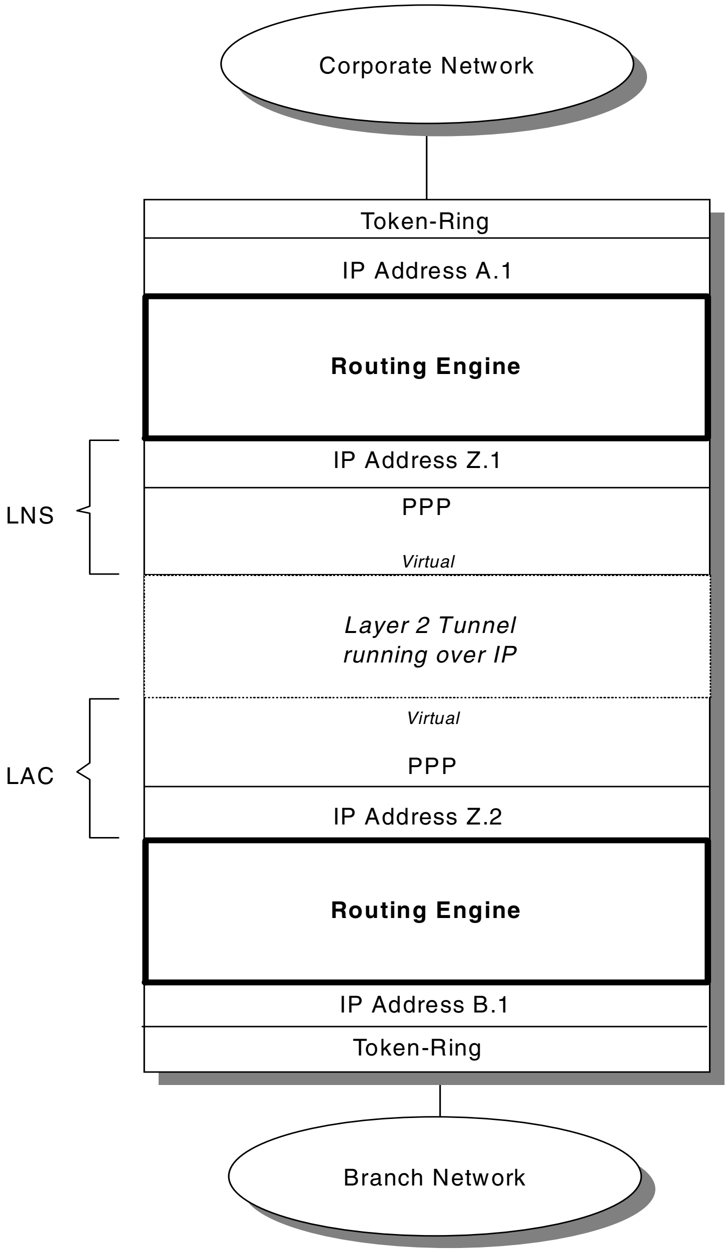


Figure 326. Consolidated layer-2 tunnel structure

17.1.2 Emulating dial-up PPP

This configuration will most likely be used by a workstation that will perform a virtual PPP dial-up to the LNS over the layer-2 tunnel. It will be allocated a dynamic IP address on one of the subnets that the LNS controls. It can, however, be used by a router as well.

Again it is important to remember that all layer-2 technologies eventually form a network structure where the network sees the layer-2 tunnel as a PPP link, in this case a dial-up PPP link. Therefore, when the LAC builds the tunnel to the LNS, as far as the corporate network is concerned it looks just like a standard PPP dial-up PPP connection to the corporate gateway. Therefore, when the LAC builds the tunnel to the LNS, as far as the corporate network is concerned it looks just like users who directly dial in to the corporate gateway using PPP. We will use this as our reference point when showing how the IBM routers fit into the layer-2 framework (see Figure 327).

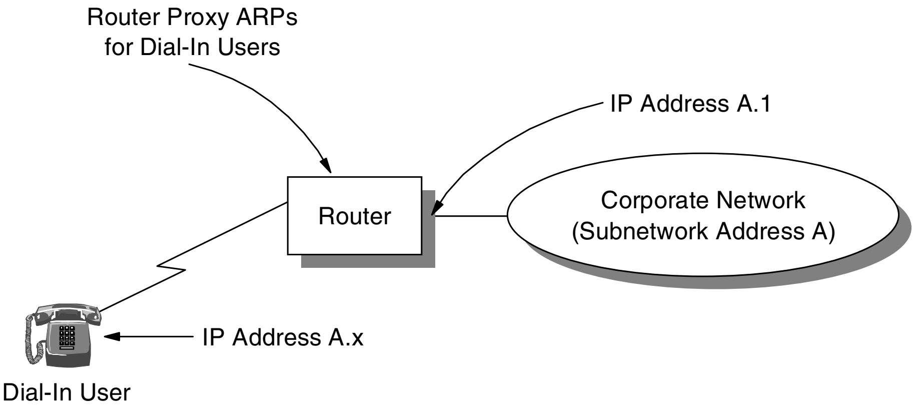


Figure 327. Dial-in PPP reference diagram

Since the layer-2 tunneling structure tries to emulate a simple dial-up PPP infrastructure we should initially examine how an IBM 221x router implements its components to support such a user.

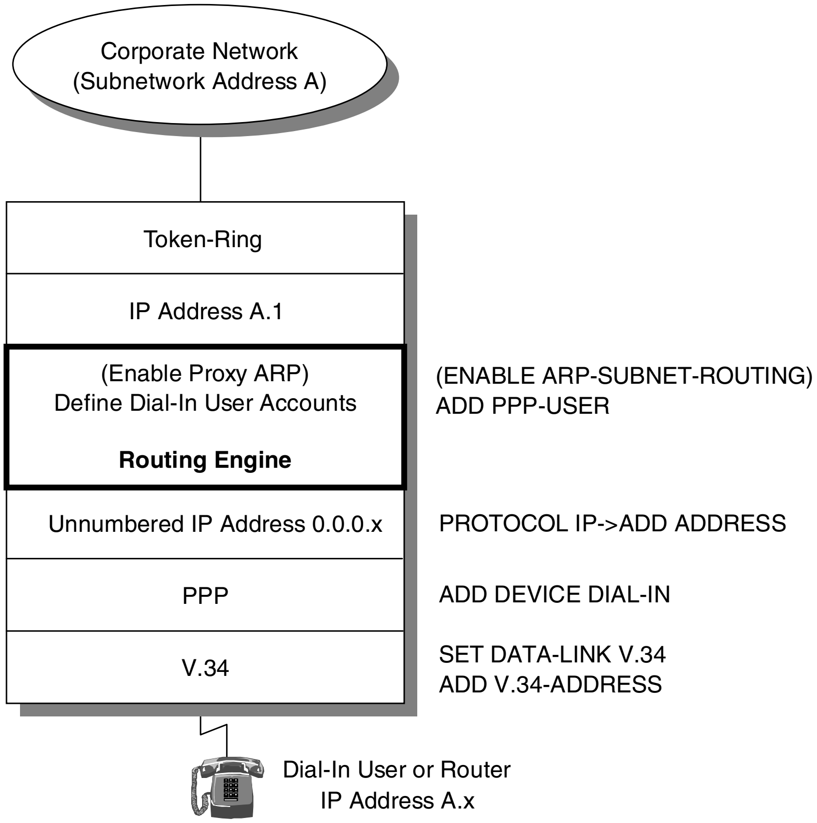


Figure 328. IBM router implementation with PPP dial-in user

In a standard PPP dial-in scenario the remote device has an IP address on the corporate network, as if it were attached locally to the corporate LAN. To support dial-in devices in this way the router must perform a proxy ARP function on behalf of the remote device, since the dial-in device is not physically on the corporate network to respond to ARP requests itself. When the router receives a packet for a dial-in device it has to forward it through the dial-in interface. The unnumbered IP address gives the router an IP address to do this. The unnumbered IP address is not a real IP address in that it is only used by the router to know to which interface to forward a packet, that is, one-way traffic to the dial-in device. The dial-in device on the other hand thinks it has a real IP address on the corporate network.

Note on proxy-ARP

If the dial-in client was given an IP address out of a subnet that was not used on the corporate LAN, proxy-ARP would not be required, but all systems on the corporate LAN would have to know that they can reach the dial-in systems via the LNS. This can be achieved by having the LNS advertise the dial-in subnet(s) to the corporate LAN using IP routing protocols.

The dial-in device is performed by the LAC with layer-2 tunneling. Let us first examine the dial-in device and the steps required on this device to set up the dial-in connection:

1. Define the physical interface.
2. Define PPP.
3. Define the IP components.

The layer-2 tunnel must perform the same steps described above. Part of step 1 is achieved through IP connectivity. With voluntary tunneling the LAC assumes that there is already IP connectivity to the LNS. This can be achieved by any method including permanent connections like Ethernet or even temporary dial-up connections as described in Figure 19 on page 387. A workstation running Windows would achieve this by dialing in to the ISP, the dial-up networking features of Windows.

The rest of step 1 is done by building a layer-2 tunnel which can then carry the PPP stream over a layer-3 IP network to the LNS. This layer-2 tunnel is generated by the command `ADD TUNNEL-PROFILE` in an IBM router. In this step you configure the IP address of the tunnel endpoint, the name of the tunnel (which is the local name of the tunnel at the LNS) and the local name of the tunnel. In addition you have to configure a secret password. These parameters will authenticate the tunnel. Once authenticated the PPP circuit can go through the tunnel.

In voluntary tunneling mode you do not have to authenticate the tunnel. This is because the authentication will be done again on the simulated dial-up PPP; the layer-2 tunnel is simply a mechanism for the PPP circuit to get to the LNS over an IP network. In fact, in some client implementations you do not have the choice of being able to authenticate the actual tunnel.

The LAC must now simulate the PPP dial-in to the LNS (step 2). The problem is that a PPP interface does not exist, therefore, the IBM router must put in place a virtual layer-2 interface with the command `ADD DEVICE LAYER-2 TUNNELING`.

If the LAC is a workstation, step 2 and the second part of step 1 would all be done by the layer-2 client code.

If the router is going to have a dynamically assigned IP address, step 3 requires that an unnumbered IP address is also added here so that the router has an interface to forward packets out. This is only required on the IBM router as it is an implementation requirement. LACs implemented on workstations would not need the unnumbered IP address.

The steps described above for the IBM router are shown diagrammatically in Figure 329:

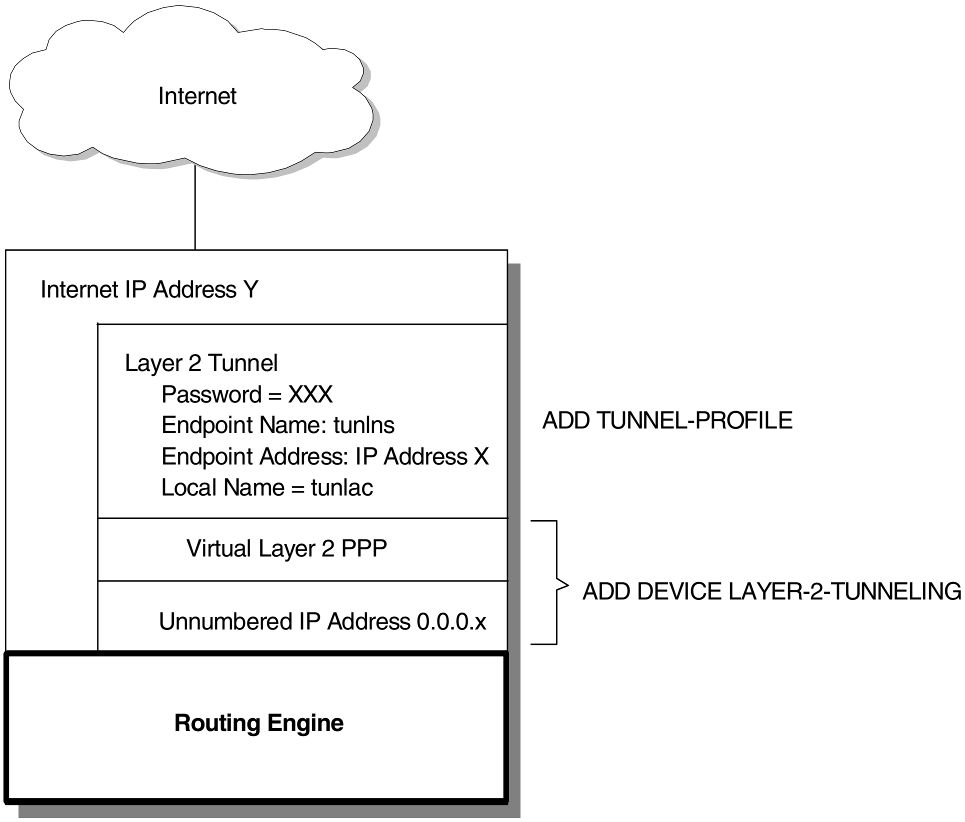


Figure 329. IBM router implementation of LAC

The next step is to examine what needs to be configured at the LNS. For an IBM router to support a standard PPP dial-in scenario the following must be configured (see Figure 328 on page 322):

1. Physical dial-in circuit. This is the process where you configure the physical dial-in interface with `SET DATA-LINK V.34` and `ADD V.34-ADDRESS` commands.
2. PPP dial-in. This is where you set the interface you just configured in step 1 above to be supported as a PPP dial-in circuit with the command `ADD DEVICE DIAL-IN`.
3. Unnumbered IP address. This is where you give the dial-in interface an IP address that the router can forward out of by using the command `PROTOCOL IP->ADD ADDRESS` commands.

4. Proxy ARPing. This ensures that the router responds to ARPs for the dial-in users with the command `ENABLE ARP-SUBNET-ROUTING`. See “Note on proxy-ARP” on page 323.
5. PPP dial-in users. This process configures the accounts of the the dial-in user with the `ADD PPP-USER` command.

As in the LAC, step 1 is achieved through IP connectivity and the forming of the layer-2 tunnel. Therefore, a component needs to be built to terminate the layer-2 tunnel from the LAC, since we are assuming standard IP connectivity already exists. The same command `ADD TUNNEL-PROFILE` is used to do this.

With step 2, the IBM router also deploys a virtual layer-2 PPP interface so that the LNS router has a PPP interface that can be treated as any other locally attached PPP interface.

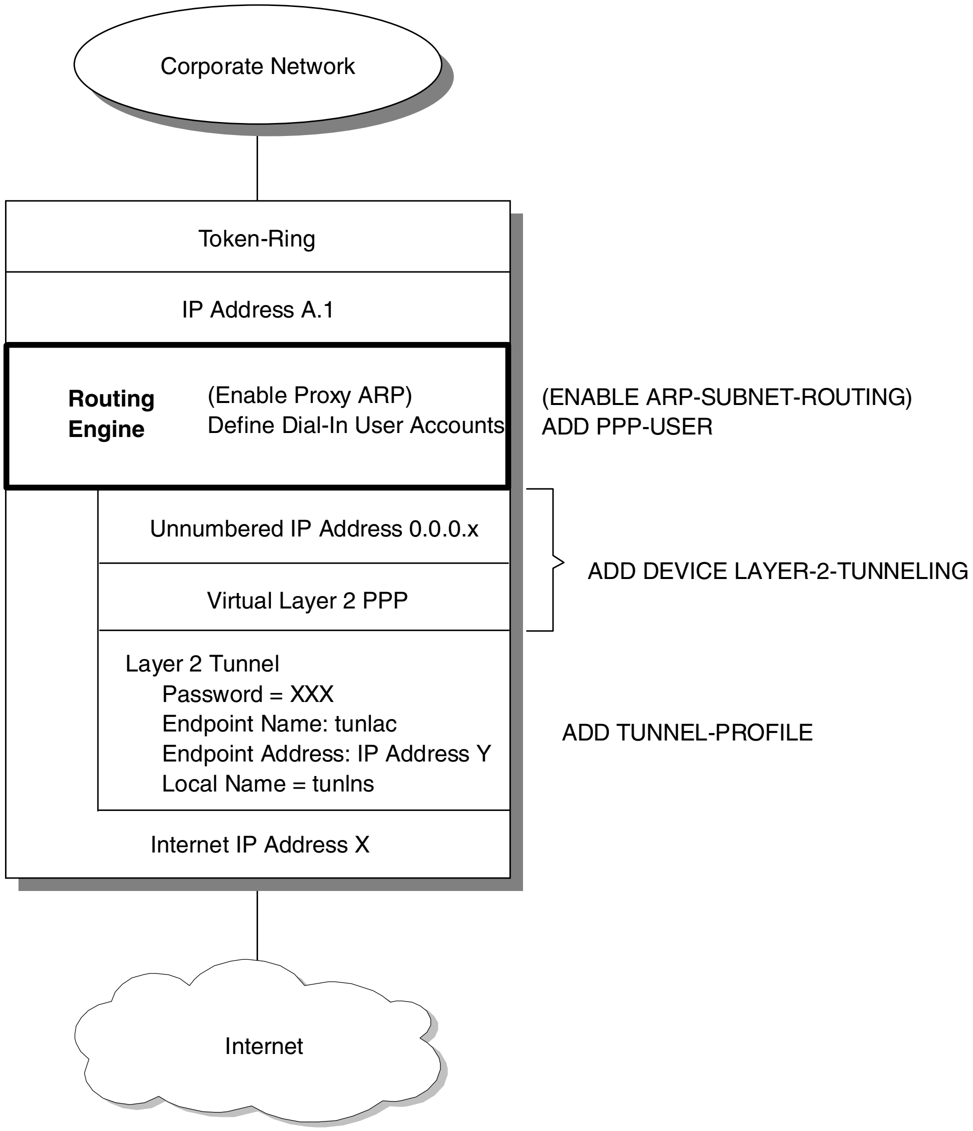


Figure 330. IBM router implementation of LNS

This virtual component is built by `ADD DEVICE LAYER-2-TUNNELING`. In addition to the virtual components, this command also automatically adds the unnumbered IP address (see Figure 330). Now all that is required is steps 3 and 4. These steps are performed in the usual manner on the LNS.

The result is that from the corporate gateway (LNS) point of view it thinks that all its PPP dial-in circuits are locally attached and the device's point of view is that it is directly dialing into the corporate router per the reference diagram (Figure 327 on page 322). In reality they are split in half and the joining point is the virtual PPP interface at the LNS and LAC (see Figure 331). Compare this diagram with Figure 328 on page 322 which shows the IBM router implementation with PPP dial-in user.

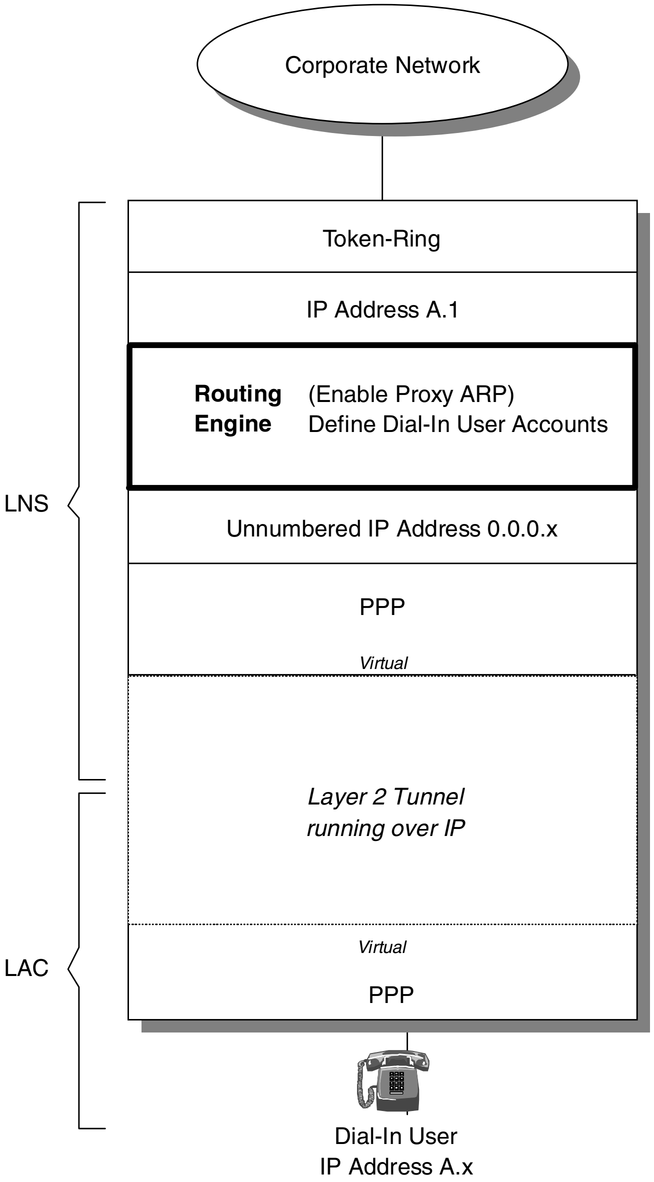


Figure 331. Consolidated layer-2 tunnel structure

17.2 Using Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) has the same aim as L2TP, which is to tunnel PPP packets across an IP network. It is a proprietary tunnel-architecture developed by Microsoft.

L2TP was developed by the IETF and is based heavily on PPTP and L2F (Cisco's equivalent). Therefore, the usage of the standardized protocol L2TP instead of proprietary protocols should be enforced.

However, there are cases where the use of these protocols is still appropriate. A typical case is, where a telecommuter is working remotely (for example, from his home office) and needs access to his home network (LAN) in the center. Therefore, he dials in to a Point-of-Presence (POP) of an Internet service provider (ISP) to access his home network.

In most cases the telecommuter will use a Microsoft Windows platform, which ships with PPTP as a tunneling protocol. At the moment Microsoft does not support L2TP - it is currently planned for Windows 2000. Therefore, to establish a tunnel with a Microsoft device, the corresponding router needs to support PPTP.

To support these cases the IBM Nways family of routers (2210, 2212, 2216), including the Network Utility, support PPTP besides L2TP and L2F as tunneling protocols.

17.2.1 Architecture and Microsoft support

We have to distinguish between the RFC and what Microsoft has actually implemented in their current products.

According to RFC 2637, PPTP is a client-server architecture with a client called the PPTP network access concentrator (PAC) and the server called the PPTP network server (PNS). According to the architecture, the PAC is typically a laptop and the PNS a server, but as we will see the Microsoft implementation differs from the RFC (see Figure 332):

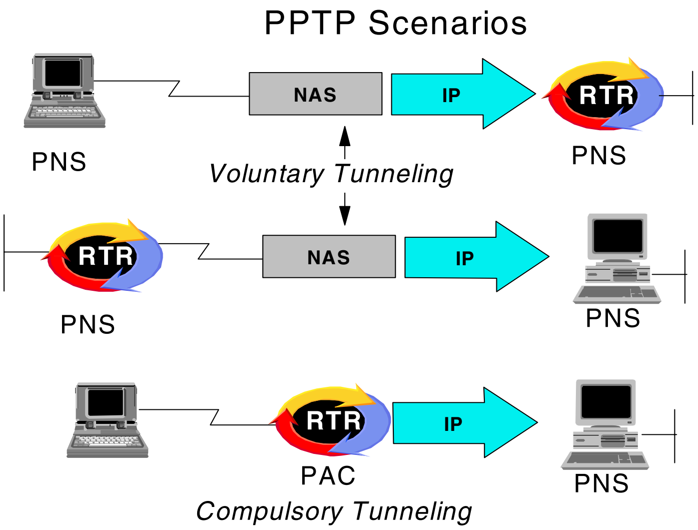


Figure 332. Types of PPTP tunneling

The diagram in Figure 332 shows the two different types of scenarios in which PPTP can be deployed:

Voluntary tunneling or client-initiated model:

The client/PAC dials in to the network access server (NAS) and establishes regular PPP network access. Next, it opens another dial-up session that establishes the PPTP tunnel. While the architecture defines that this is established by a PAC sending an incoming call request packet, Microsoft regards its devices as a PNS and actually send an outgoing call request packet. There are two scenarios in which IBM routers can be used with voluntary PPTP tunneling. The IBM router can either terminate the tunnel or initiate the tunnel. If it terminates the tunnel, the client initiating must be PPTP capable, and could be a Windows NT, Windows 98 or Windows 95 device, or any other device supporting PPTP. The other scenario is when the router establishes a tunnel back to a PPTP device, such as an NT server.

Compulsory tunneling or router-initiated model:

This is where the client has no PPTP knowledge. The client dials in to the PAC and then the PAC initiates the PPTP tunnel back to the PNS. In this case, the PAC sends an incoming call request to the PNS. Note that in this scenario, the IBM router cannot work with an NT server (or workstation) acting as the PNS. This is because Windows NT requires an inbound Link Control Protocol (LCP) configuration request to start its PPP link negotiations. Since the client has already negotiated LCP with the router, it will not send another LCP configuration request unless the PNS starts over. NT PNS will only work with PACs which are capable of ring-time tunneling - this is where PACs do not partially negotiate PPP to determine that the user wishes to be tunnelled. IBM routers will work with any other PNS that is capable of restarting the LCP connection.

Note that in both scenarios the workstation or router that is terminating the PPTP tunnel has two (physical or virtual) network adapters. One adapter is connected to the Internet and the other is connected to the private center network.

17.2.2 Description of the scenario

The configuration that we used for this scenario is shown in Figure 333 on page 329:

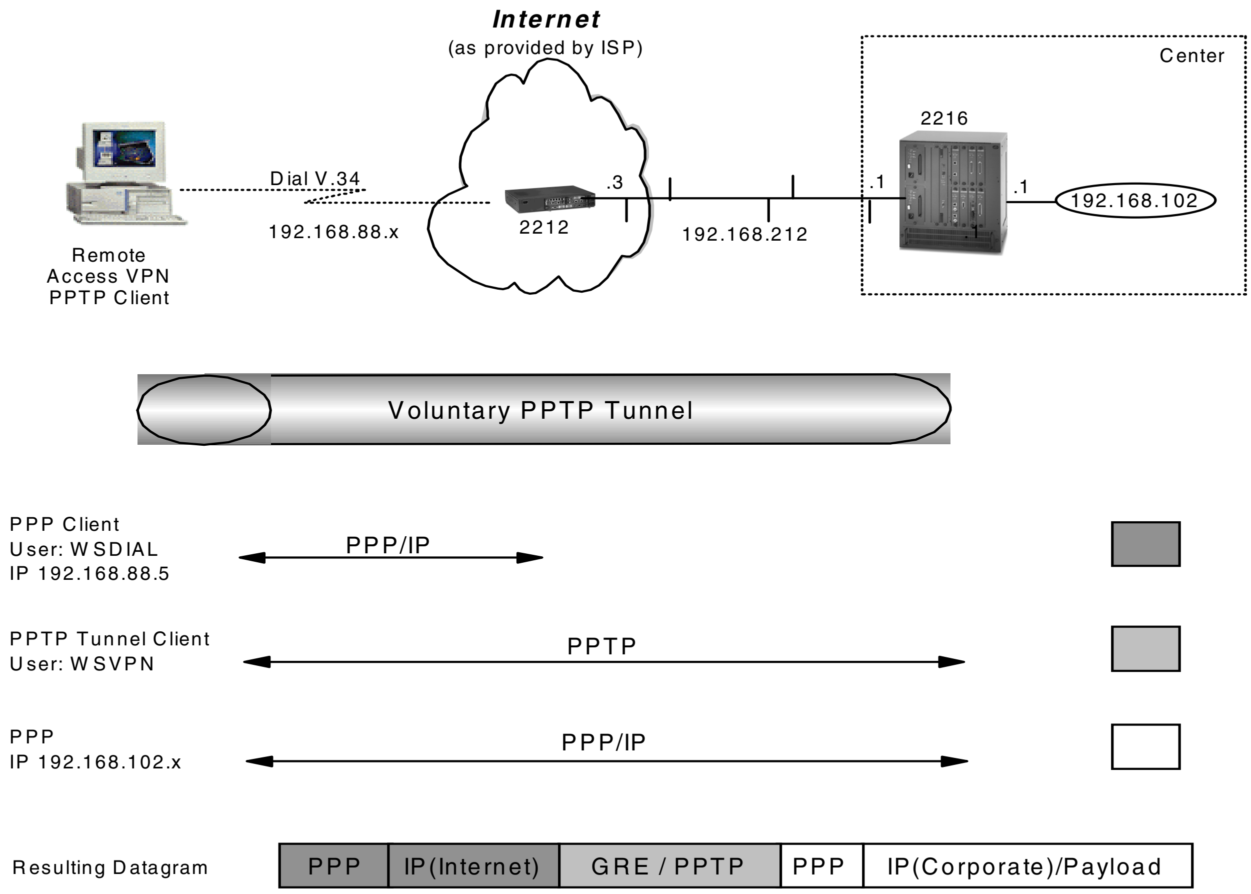


Figure 333. Creating a PPP connection with PPTP virtual tunnel

In this scenario a workstation dials in to an ISP and creates a PPTP tunnel to an IBM router on the center network.

This is an example of a remote access VPN using PPTP voluntary tunneling. The IBM router will be configured as the endpoint of a PPTP tunnel. The client, a Windows 95/98/NT Dial-Up Networking (DUN) client will dial in to the ISP router. The client will establish a PPP connection and be given an IP address on the 192.168.88.0 subnet. At this point the client has IP connectivity to anywhere in the Internet IP cloud including the WAN interface of the center Internet router. The client will then establish a tunnel to 192.168.102.1, which is the IP address of the center Internet router. The PPTP client is assigned an IP address by the center router. Once the tunnel is established, connectivity is the same as you would have if you dialed directly in to a Remote Access Server on the center LAN.

We used a workstation with DUN 1.2 or higher (Microsoft's Dial-Up Networking), a router configured as the ISP, and a center router. ARP subnet routing must be enabled on the center router.

We used a 2212 as the ISP router, as the 2212 is especially well suited to be used in the ISP environment. We use a 2216 as the center router as this is a typical router in a medium or large enterprise.

The ISP router does not require any knowledge of the PPTP tunnel. It needs to be configured for the user to dial in and get an IP address, as well as have an IP route to the tunnel endpoint IP address.

The center router needs to have PPTP enabled, have an L2-Net configured for the PPTP tunnel, and have a PPP user created for the VPN connection.

17.2.3 Definition of the ISP router

For this example we used a 2212 as the ISP router.

For the configuration of the 2212 we have to perform the following steps:

- Preparation
- Add PPP user for the dial-in workstation
- Add IP address
- Activate the definition

Note that in our case the ISP router does not establish the PPTP tunnel. Therefore, we do not need to add a tunnel definition. This differs from L2F and L2TP as PPTP does not do tunnel authentication.

17.2.3.1 Preparation

Perform the following steps to prepare the router for PPP dial-in.

Define and configure a V.34 interface for the user dial-in

Net 0 is used as the V.34 dial-in interface. Net 5 is assigned by the router as a virtual dial circuit interface. The virtual dial interface must be mapped to the physical V.34 interface (Figure 334):

Configure the V.35 WAN physical interface. The cable type and clocking may be different depending on your environment (`set hdlc cable v35 ..., set hdlc clocking..., set hdlc speed`). These commands are not shown here.

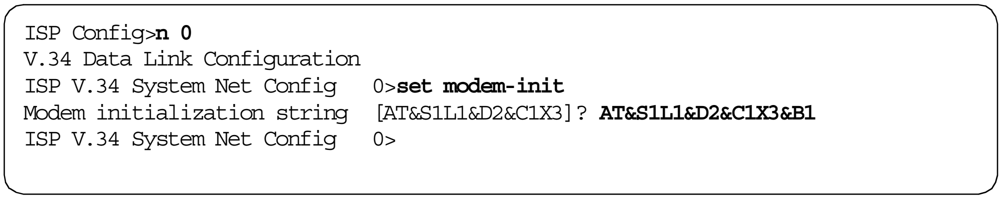
```
ISP Config>
ISP Config>set data-link v34
Interface Number [0]? 0
ISP Config>
ISP Config>add device dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]?
Adding device as interface 5
Defaulting data-link protocol to PPP
Base net for this circuit [0]? 0
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.
Add more dial circuit interface(s)?(Yes or [No]):
Use "set data-link" command to change the data-link protocol
Use "net <intf #>" command to configure dial circuit parameters
ISP Config><
```

Figure 334. Configuring the dial-in interface

Set the modem initialization string

You can also set the modem initialization string and speed.

Note: We used a *3Com-US Robotics* modem. Therefore, it was necessary to add `&B1` to the end of the default modem initialization string.The resulting string is `AT&S1L1&D2&C1X3&B1` (see Figure 335):

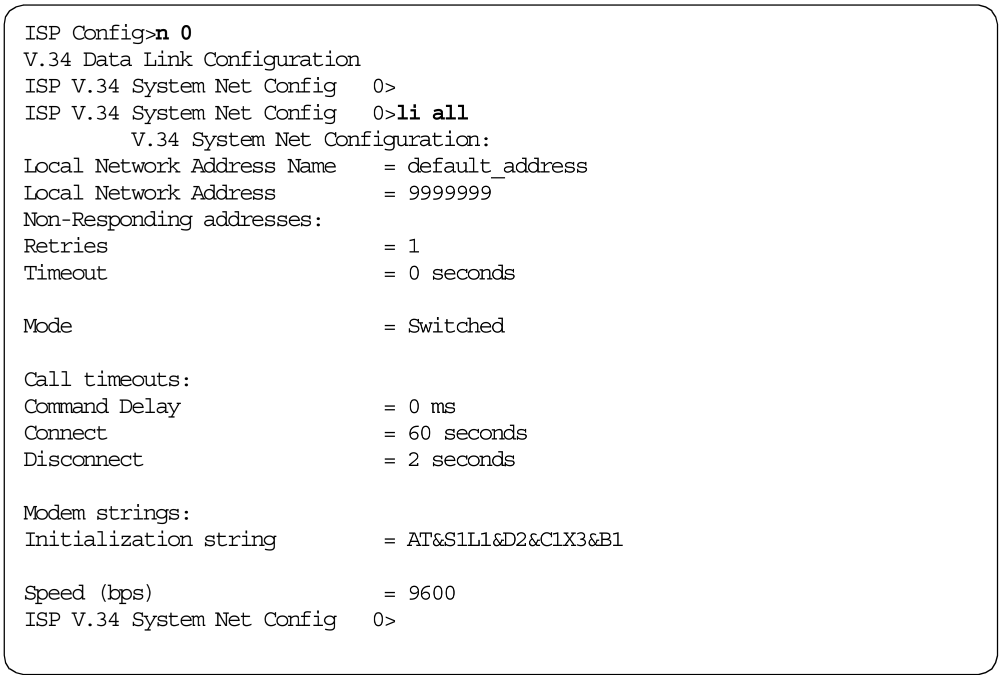


```
ISP Config>n 0
V.34 Data Link Configuration
ISP V.34 System Net Config   0>set modem-init
Modem initialization string  [AT&S1L1&D2&C1X3]? AT&S1L1&D2&C1X3&B1
ISP V.34 System Net Config   0>
```

Figure 335. Set modem initialization string

17.2.3.2 List configuration

You can check the parameters that you configured with the `list all` command (Figure 336):



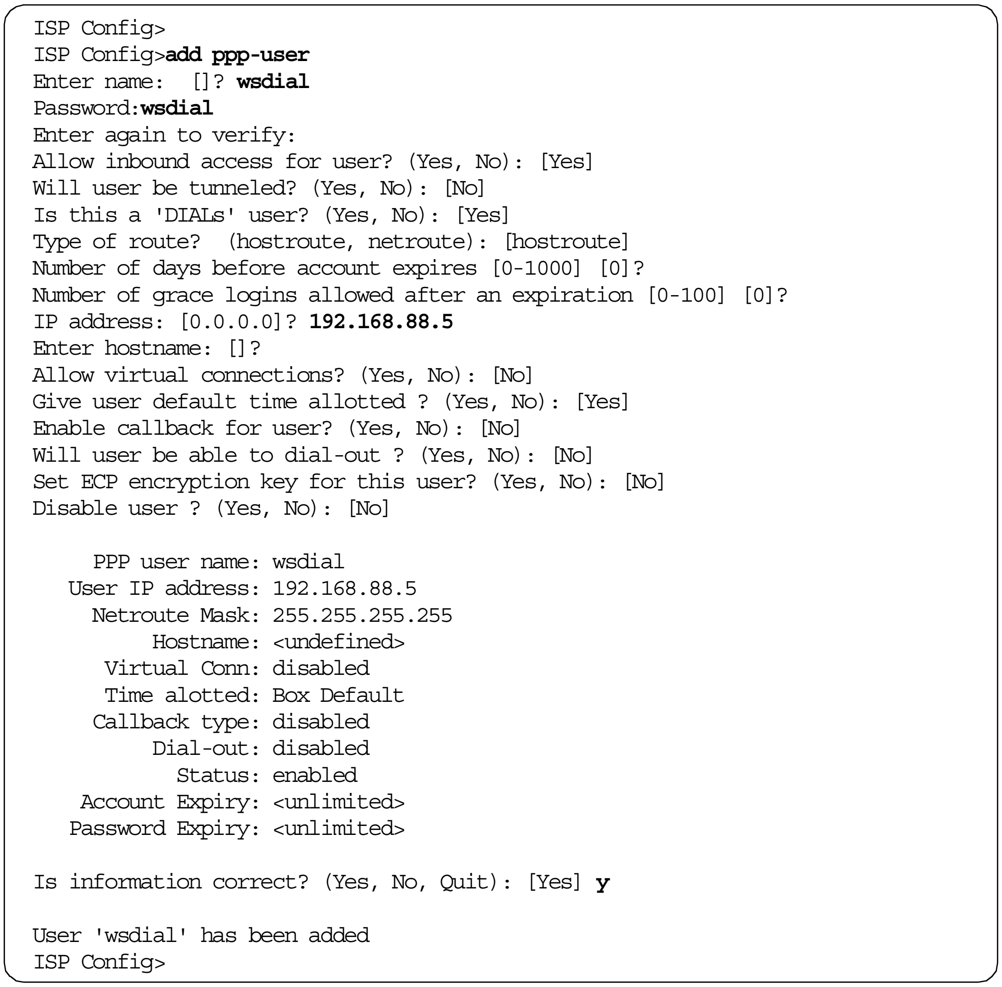
```
ISP Config>n 0
V.34 Data Link Configuration
ISP V.34 System Net Config   0>
ISP V.34 System Net Config   0>li all
         V.34 System Net Configuration:
Local Network Address Name    = default_address
Local Network Address         = 9999999
Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Mode                          = Switched

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         = AT&S1L1&D2&C1X3&B1

Speed (bps)                   = 9600
ISP V.34 System Net Config   0>
```

Figure 336. Command list all on the V.34 interface

17.2.3.3 Add PPP user for the dial-in workstation

Add the PPP user definition for the dial-in workstation. Assign it an IP address or create an IP pool; the IP address will change once the PPTP tunnel is established (see Figure 337 on page 332).

Note: The password does not show when typed but has been shown for illustration.

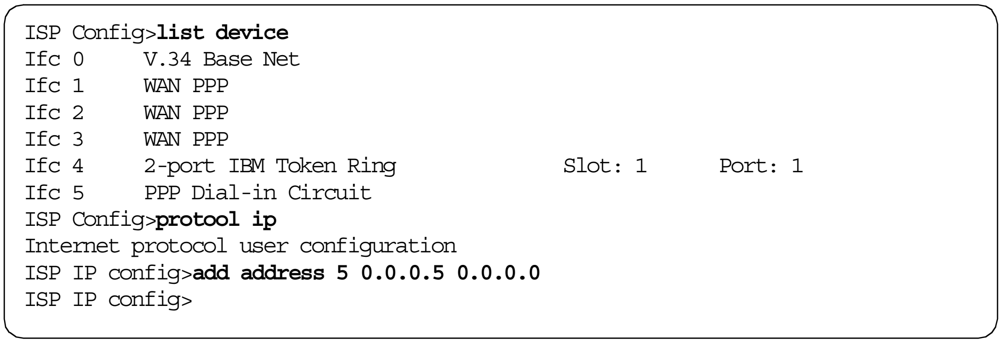


```
ISP Config>
ISP Config>add ppp-user
Enter name:  []? wsdial
Password:wsdial
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 192.168.88.5
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

     PPP user name: wsdial
   User IP address: 192.168.88.5
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
            Status: enabled
    Account Expiry: <unlimited>
   Password Expiry: <unlimited>

Is information correct? (Yes, No, Quit): [Yes] y

User 'wsdial' has been added
ISP Config>
```

Figure 337. Command add PPP user

17.2.3.4 Add IP address

To route IP through the V.34 interface, an IP address must be assigned to the interface. The router adds a static route to the V.34 virtual interface when the client dials in. You can assign a real IP address or use as we have, IP unnumbered. For IP unnumbered the format of the address is 0.0.0.n where n is the interface number.



```
ISP Config>list device
Ifc 0     V.34 Base Net
Ifc 1     WAN PPP
Ifc 2     WAN PPP
Ifc 3     WAN PPP
Ifc 4     2-port IBM Token Ring             Slot: 1      Port: 1
Ifc 5     PPP Dial-in Circuit
ISP Config>protocol ip
Internet protocol user configuration
ISP IP config>add address 5 0.0.0.5 0.0.0.0
ISP IP config>
```

Figure 338. Adding an IP address to the dial-in interface

Note: IP address is added in the format: add address x y.y.y.y z.z.z.z, where x is the interface number, y.y.y.y is the IP address of the interface and z.z.z.z is the subnet mask of the interface address.

17.2.3.5 Activate the definitions on the ISP router

You activate the definitions on the ISP with the command `restart` (see Figure 339):

```
ISP Config>
ISP *restart
Are you sure you want to restart the gateway? (Yes or [No]): y
The configuration has been changed, save it? (Yes or [No] or Abort): y
Config Save: Using bank B and config number 2
```

Figure 339. Restarting the ISP router

17.2.4 Definition of the router in the center

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation.
- Enable PPTP and add layer-2 nets.
- Enable MSCHAP and MPPE.
- Add PPP-user for the Dial-in Workstation.
- Add the default route to the Internet and enable ARP-subnet-routing.
- Activate the definitions on the center router.

17.2.4.1 Preparation

We assume that the permanent Ethernet connection to the ISP is already established. Therefore, we can concentrate on the dial-in features of this connection.

17.2.4.2 Enable PPTP and add layer-2 nets

PPTP is enabled from the layer-2 tunneling feature (as are L2F and L2TP). The next step is to create the interface that will terminate the PPTP PPP connection. This is known as L2Net. L2Nets can be added from the layer 2 tunneling feature as shown above, or from the `Config>` prompt using the `add device layer` command (Figure 340 on page 334).

Adding the L2Net creates several interfaces. An unnumbered IP address will be given automatically by way of **1** . Note that PPTP, L2TP and L2F tunneled PPP sessions will use the same pool of L2Nets.

See Figure 340 on page 334:

```
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ENABLE PPTP
Center Layer-2-Tunneling Config>
Center Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]: 1
Adding device as interface 8
Defaulting data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.
```

Figure 340. Enabling PPTP and adding L2Nets on the center router

17.2.4.3 Enable MSCHAP and MPPE

Microsoft DUN PPTP client uses MPPE to perform encryption. Therefore, MPPE needs to be enabled on the L2Net. L2Nets, which are configured as inbound from anyone (the default), take their PPP defaults from a template in the layer feature. The `encapsulator` command takes you to a prompt from where all the PPP defaults can be tuned.

To use MPPE, we must enable MS-CHAP. When you enable MPPE you are asked if MPPE is operating in mandatory or optional mode. Mandatory mode forces the router to renegotiate MPPE each time a new connection is requested, even when the sender has previously established MPPE between itself and the router. Optional mode results in the router maintaining MPPE between itself and the sender after the initial negotiation and does not renegotiate MPPE for each new connection.

You are then asked if the keys are stateful or stateless. If the keys are stateless, the key changes every time a packet is sent, whereas with stateful the key is only generated when 255 packets have been sent. Stateless is advised for lossy networks and should be used for PPTP connections. The router will know if the client is using stateless or stateful mode as part of the MPPE header indicates whether the keys have been refreshed.

MPPC is Microsoft's compression algorithm. MPPE is in fact negotiated as an MPPC option. If you wish to do compression, and you are using MPPE, you must use MPPC.

Note

Note if you are using a 2212 or 2216 you need to load the encryption package.

```
Center Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>ENABLE MSCHAP
Rechallenge Interval in seconds (0=NONE)  [0]?
Enabling MSCHAP
Center PPP-L2T Config>ENABLE MPPE
mandatory or optional [optional]?
stateful or stateless [stateless]?
Enabling encryption
** Note ** : To view the MPPE configuration, please enter a 'list ccp'
             command since MPPE is negotiated within the CCP protocol.
Center PPP-L2T Config>
```

Figure 341. Enabling MSCHAP and MPPE on the center router

17.2.4.4 Add PPP user

Configure the user name that the workstation will connect with over the PPTP tunnel (Figure 342 on page 336).

The IP address configured for the users should be on the LAN subnet to which they wish to connect. You may also assign a pool of IP addresses or use a DHCP server to allow flexibility and scalability in user management.

As we use an IP address that is in the same subnet as the LAN, ARP subnet routing must be enabled (Figure 343 on page 337).

Note: The password does not show in the real screen; we used the password wsvpn (the password has been shown for illustration).

```
Center Config>
Center Config>ADD PPP-USER
Enter name:  []? wsvpn
Password:wsvpn
Enter again to verify: wsvpn
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]? 192.168.102.11
IP address: [0.0.0.0]? 192.168.102.11
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

     PPP user name: wsvpn
   User IP address: 192.168.102.11
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Account Expiry: <unlimited>
   Password Expiry: <unlimited>

Is information correct? (Yes, No, Quit): [Yes]

User 'wsvpn' has been added
Center Config>
```

Figure 342. Adding a PPP user

17.2.4.5 Add default route and enable ARP-subnet-routing

ARP-subnet-routing must be enabled to allow the router to respond to ARPs when the next hop to the destination is over a different interface from the interface that is receiving the ARP request. In our case the PPTP client is logically on the center LAN subnet but physically on a different (V.34) interface. ARP-subnet-routing allows the router to act as a proxy for ARP requests from devices on the center LAN to reach the PPTP client. See “Note on proxy-ARP” on page 323.

```
Center *TALK 6
Center Config>PROTOCOL IP
Internet protocol user configuration
Center IP config>ADD ROUTE
IP destination []? 192.168.88.0
Address mask [255.255.255.0]?
Via gateway 1 at []? 192.168.212.3
Cost [1]?
Via gateway 2 at []?
Center IP config>
Center IP config>ENABLE ARP-SUBNET-ROUTING
Center IP config>
```

Figure 343. Add default route and enable ARP-subnet-routing

Notes:

IP Address Assignment:

IP address is added in the following format: add address x y.y.y.y z.z.z.z, where x is the interface number, y.y.y.y is the IP address of the interface, z.z.z.z is the subnet mask of the interface.

Add Route:

Add Route is in the format w.w.w.w x.x.x.x y.y.y.y z, where w.w.w.w is the route we want to reach, x.x.x.x is the subnet mask, y.y.y.y is the address of the gateway we want to use and z is the cost of the route.

17.2.4.6 Activate the definitions on the center router

You activate the definitions on the center router with the command `restart` (see Figure 344):

```
Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 344. Reloading the center router

17.2.5 Definition of the client workstation

We used an IBM Thinkpad with Windows 95 and an IBM PC 750 with Windows NT as client workstations for this scenario.

17.2.5.1 Installing and configuring PPTP on Windows 95

The workstation needs to have Dial-Up Networking 1.2 or higher. Dial-Up Networking can be found under **Start -> Programs -> Accessories** or by double-clicking the **My Computer** icon on the desktop.

To see if you have Version 1.2 or later, open a **Make New Connection** window in the Dial Up Networking folder. Check for the presence of *Microsoft VPN Adapter* in the Select a device drop-down window.

The Dial-Up Networking Client can be obtained from the Microsoft Web site at:

`http://microsoft.com/msdownload/`

Windows 98 ships with a dial-up networking version that already includes PPTP.

17.2.5.2 Installing and configuring PPTP on Windows NT

To use PPTP with Windows NT you have to add a protocol to the Network configuration. Right-click the **Network Neighborhood** icon on the desktop and select **Properties**, then select the **Protocols** tab and click **Add**. From the list of available vendors, select **Microsoft**, then select **Point-to-Point Tunneling Protocol** and click **OK**. In the following screen, select the number of PPTP connections you wish to support on this client.

> **Note**
>
> You may need your Windows NT CD-ROM to complete this step. In addition, if you already have applied a Windows NT service pack, you have to reapply it after the PPTP installation and RAS configuration have completed.

Next, select the **Services** tab and double-click **Remote Access Service**. Click **Add** to add a new device and select **Microsoft VPN Adapter**. Click **Options** and select **dial-out only**. Click **Network** and select the protocols you want to support with the PPTP connection. Only select protocols that are actually installed on your workstation. When you are done, click **OK**.

Click **Close** and select to restart your computer when prompted.

17.2.5.3 Configure the Dial-Up Networking (DUN) client

We have to add two DUN clients. One is for the PPP connection to the ISP, the second is for the (virtual) PPP connection to the central router.

Add a DUN client to the ISP

We add a DUN client to the ISP by double-clicking on **Make New Connection**. We specify user ID/password (`wsdial/wsdial`), we keep the default device of Thinkpad Data Fax Modem and click the **Next** button. We enter the telephone number and click the **Next** button.

The installation of the ISP connection is finished.

Add a DUN client for VPN

We add a DUN client to the center by double-clicking on **Make New Connection**. We specify user ID/password (`wsvpn/wsvpn`). We change the device to *Microsoft VPN Adapter*. We enter the tunnel endpoint IP address as the the telephone number.

The installation is now finished. For more information, please consult Microsoft's documentation on PPTP and your operating system's implementation thereof.

17.2.6 Building the connection

To establish a PPTP tunnel using a Microsoft platform we need to use two DUN sessions: The first one to the Internet (in our case to the ISP's router) and the second one to the center router.

17.2.6.1 Dialing to ISP router

We launch the PPP dial-up connection which establishes the Internet connection and log on with the user ID `wsdial`.

We ping the Internet interface of the center router to verify the configuration into the internet. A ping to the intranet interface of the center router does not work.

The routes on the workstation look like the following (`netstat -r`) - see Figure 345:

```
Active Routes:

  Network Address          Netmask  Gateway Address        Interface  Metric
          0.0.0.0          0.0.0.0     192.168.88.5     192.168.88.5       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
     192.168.88.0    255.255.255.0     192.168.88.5     192.168.88.5       1
     192.168.88.5  255.255.255.255        127.0.0.1        127.0.0.1       1
   192.168.88.255  255.255.255.255     192.168.88.5     192.168.88.5       1
        224.0.0.0        224.0.0.0     192.168.88.5     192.168.88.5       1
  255.255.255.255  255.255.255.255     192.168.88.5     192.168.88.5       1
```

Figure 345. Routes on the workstation after logon to the ISP

17.2.6.2 Dialing to center router through tunnel

We launch the PPTP connection to create the tunnel to the center router with the user ID `wsvpn`.

We can now also ping all hosts on the center intranet. `netstat -r` shows the updated routing table on the workstation (se Figure 346):

```
Active Routes:

  Network Address          Netmask  Gateway Address        Interface  Metric
          0.0.0.0          0.0.0.0     192.168.88.5     192.168.88.5       2
          0.0.0.0          0.0.0.0   192.168.102.11   192.168.102.11       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
     192.168.88.0    255.255.255.0     192.168.88.5     192.168.88.5       2
     192.168.88.5  255.255.255.255        127.0.0.1        127.0.0.1       1
   192.168.88.255  255.255.255.255     192.168.88.5     192.168.88.5       1
    192.168.102.0    255.255.255.0   192.168.102.11   192.168.102.11       1
   192.168.102.11  255.255.255.255        127.0.0.1        127.0.0.1       1
    192.168.212.1  255.255.255.255     192.168.88.5     192.168.88.5       1
        224.0.0.0        224.0.0.0   192.168.102.11   192.168.102.11       1
        224.0.0.0        224.0.0.0     192.168.88.5     192.168.88.5       1
  255.255.255.255  255.255.255.255     192.168.88.5     192.168.88.5       1

Route Table

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    wtr05999:1026          192.168.212.1:1723     ESTABLISHED
```

Figure 346. Routes on the workstation after building the PPTP connection

17.2.7 Testing the connection

Perform the following steps at the router to verify that the PPTP connection has been successfully established.

17.2.7.1 Checking PPTP tunnel status from the center router

The commands `TUNNEL STATE`, `TUNNEL STATISTICS`, `TUNNEL TRANSPORT` can be used to check the status of the PPTP tunnel (see Figure 347):

```
Center *TALK 5

Center +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
Center Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID | Type | Peer ID |    State    | Time Since Chg | # Calls | Flags
    14733 | PPTP |       0 | Established |     0:14: 8    |       1 |
Center Layer-2-Tunneling Console>
Center Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes |  RTT  |  ATO
    14733 | PPTP |     116 |     4202 |     174 |    10376 |    23 |     0
Center Layer-2-Tunneling Console>
Center Layer-2-Tunneling Console> TUNNEL TRANSPORT
Tunnel ID | Type | Peer IP Address | UDP Src | UDP Dest
    14733 | PPTP |    192.168.88.5 |       0 |       0
Center Layer-2-Tunneling Console>
```

Figure 347. Check PPTP tunnel information

17.2.7.2 Check layer-2 information

Layer-2 information, including PPP user information can be seen with the command `list all`. Most useful for troubleshooting is the statistics, user ID, and IP address of the connection (Figure 348 on page 341). As an overview in this redbook we show only the headers per information block:

```
Center +
Center +NETWORK 8
Point-to-Point Console
Center PPP 8>LIST ALL
Interface Statistic        In                         Out
-------------------        --                         ---
Packets:                   181                        123
Octets:                    10642                      4468

LCP Statistic              In                         Out

Version:                   1
Link phase:                Ready for network traffic (NCP)
LCP State:                 Open
Previous State:            Ack Sent
Time Since Change:         15 minutes and 46 seconds
Remote Username:           wsvpn
Last Identification Rx'd
Time Connected:            15 minutes and 46 seconds

LCP Option                 Local                      Remote
Error Type                 Count                      Last One
PAP Statistic              In                         Out
CHAP Statistic             In                         Out
MSCHAP Statistics          In                         Out
-----------------          --                         ---
Packets:                   1                          2
Octets:                    63                         42
Challenges:                0                          1
Responses:                 1                          0
Successes:                 0                          1
Failures:                  0                          0
  Restricted Hours:        0                          0
  Account Disabled:        0                          0
  Password Expired:        0                          0
  No Dialin Permission:    0                          0
  Authentication:          0                          0
  Change Password:         0                          0
Change Passwords:          0                          0
SPAP Statistic             In                         Out
MPPE Statistic             In                         Out
CCP Statistic              In                         Out
Compression Statistic      In                         Out
CBCP Statistics            In                         Out
ECP Statistic              In                         Out
Encryption Statistic       In                         Out
Spanning Tree Statistic    In                         Out
IPCP Option                Local                      Remote
-----------                -----                      ------
IP Address                 0.0.0.0                    192.168.102.11
Compression Slots          None                       None
IPCP Statistic             In                         Out
IP Statistic               In                         Out
IPv6CP Option              Local                      Remote
IPv6CP Statistic           In                         Out
IPv6 Statistic             In                         Out
DNCP Statistic             In                         Out
DN Statistic               In                         Out
Center PPP 8>
```

Figure 348. Output of list all command

17.2.7.3 Check connected PPP users

The command `list online-users ppp` lists all PPP users that are currently connected (see Figure 349):

```
Center +FEATURE AUTH
AAA Information
Center AAA Console> LIST ONLINE_USERS PPP
List  (Name, Verb, Addr, VCon, Call, Time, Encr): [Verb]
Active PPP entities:
               Net:  8
     PPP user name: wsvpn
   User IP address: 192.168.102.11
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Virtual Conn: disabled
      Time alotted: Unlimited
     TimeConnected: 00:16:57
     TimeRemaining: Unlimited
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Account Expiry: <unlimited>
   Password Expiry: <unlimited>

1 PPP record displayed.

Center AAA Console>
```

Figure 349. Check connected PPP users

17.2.7.4 Display event logging information

There is an ELS subsystem that can be used for troubleshooting (see Figure 350):

```
Center +TALK 5

Center +EVENT
Event Logging System user console
CENTER ELS>NODISPLAY SUBSYSTEM ALL ALL
Center ELS>DISPLAY SUBSYSTEM l2 all
Center ELS>
```

Figure 350. Display event logging information

17.3 Using Layer 2 Tunneling Protocol (L2TP)

L2TP is the standard protocol for remote access VPNs as declared by the IETF. It is essentially a merger between PPTP and L2F, but its endorsement by the IETF gives it the benefit of being regarded as a non-proprietary protocol. L2TP also combines all advantages of PPTP and L2F to offer the user the richest set of features of these three protocols. Several vendors of routers, access hardware and software are implementing L2TP today, and is seen by the industry as the emerging de facto standard for remote access VPNs. L2TP is defined in RFC 2661.

17.3.1 Description of the scenario

This scenario assumes that the client accesses the Internet using whatever ISP is available. The client will then build an L2TP tunnel to a corporate gateway so that it will get an IP address in the intranet. The client will use the standard dial-up networking that comes with Windows. The L2TP tunnel will be provided by TunnelBuilder, a software from Network TeleSystems, Inc. (NTS). Below is a diagram showing our test scenario:

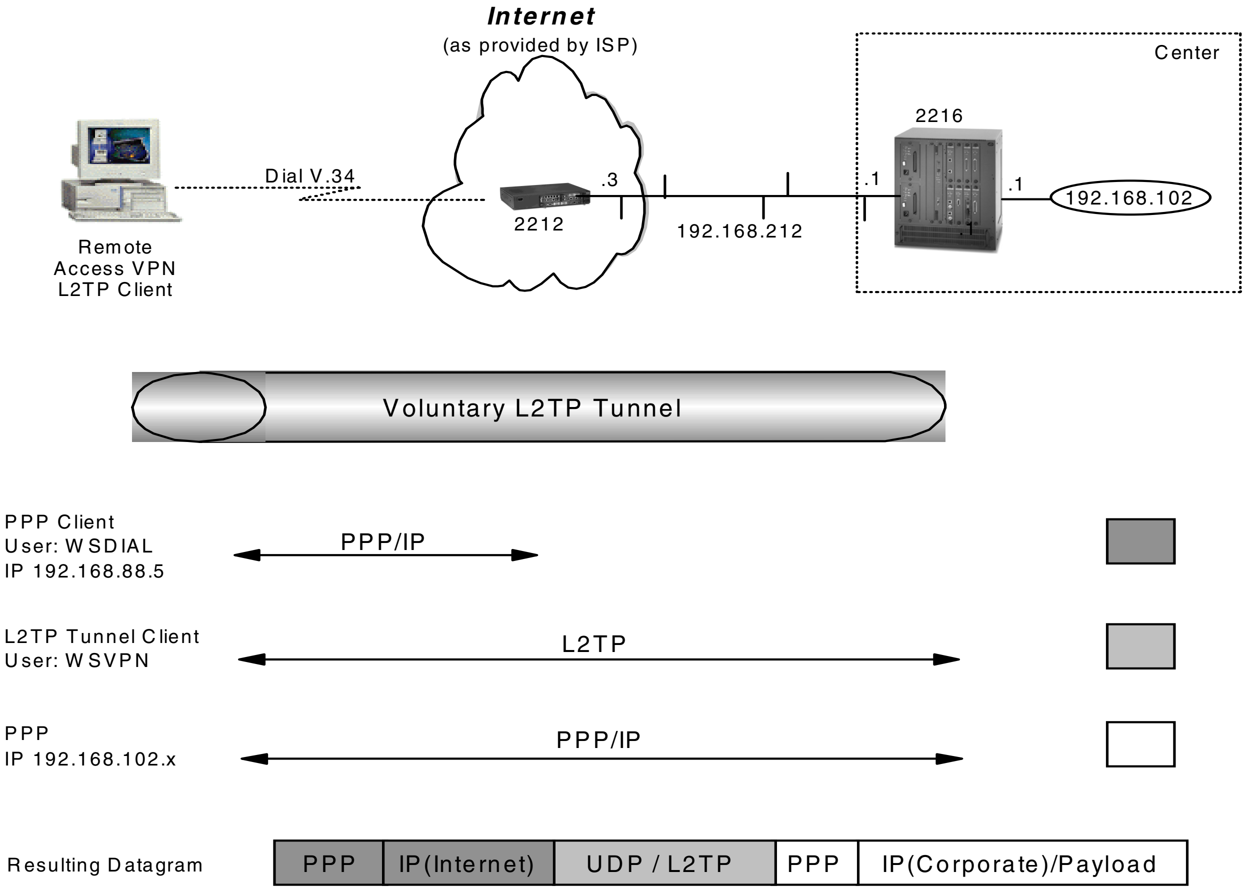


Figure 351. Creating an L2TP connection

In this scenario, the client will be assigned two IP addresses, one from the ISP and one from the corporate gateway, so the client will effectively have access to the Internet and the corporate network at the same time. This speeds up Internet access for the client but may be a security exposure to the corporate network in case the client is attacked and the L2TP tunnel is used as a backdoor by a hacker. For traveling users who need occasional access to corporate servers that cannot be accessed externally or by a Web browser but who do most of their other work over the Internet, this is certainly acceptable. For remote users who do most of their work online to corporate servers, we recommend to use PPP encryption.

17.3.2 Definition of the ISP router

The necessary steps for configuring an ISP router for this scenario are the same as described in 17.2.3, “Definition of the ISP router” on page 330.

17.3.3 Definition of the center router

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation.
- Enable L2TP and add layer-2 nets.
- Add PPP-user for the dial-in workstation.
- Add the default route to the Internet and enable ARP-subnet-routing.
- Activate the definitions on the center router.

17.3.3.1 Preparation

We assume that the permanent Ethernet connection to the ISP is already established. Therefore we can concentrate on the dial-in features of this connection.

17.3.3.2 Configure L2TP

You now have to define the layer-2 tunnel. Tunnel authentication is disabled because the client has not been enabled to do this. If it has been enabled on the client you must leave it enabled here and define the tunnel through the `ADD TUNNEL-PROFILE` command.

```
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 4
Defaulting data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.

Center Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
Center Layer-2-Tunneling Config>ENABLE FIXED-UDP-SOURCE-PORT
Center Layer-2-Tunneling Config>DISABLE TUNNEL-AUTH
Center Layer-2-Tunneling Config>LIST all
GENERAL ADMINISTRATION
------- --------------
  L2TP                              = Enabled
  PPTP                              = Disabled
  L2F                               = Disabled
  Maximum number of tunnels         = 30
  Maximum number of calls (total)   = 100
  Buffers Requested                 = 200

CONTROL CHANNEL SETTINGS
------- ------- --------
  Tunnel Auth                       = Disabled
  Tunnel Rcv Window                 = 4
  Retransmit Retries                = 6
  Local Hostname                    = IBM

DATA CHANNEL SETTINGS
---- ------- --------
  Force CHAP Challenge (extra security)= Disabled
  Hiding for PAP Attributes         = Disabled
  Hardware Error Polling Period (Sec)  = 120
  Sequencing                        = Enabled

MISCELLANEOUS
-------------
  Send Proxy-LCP                    = Enabled
  Send Proxy-AUTH                   = Enabled
  Fixed UDP source port (1701)      = Enabled
  Fixed source IP Address           = Disabled
```

Figure 352. Center router L2TP configuration

17.3.3.3 Enabling L2TP encryption

MPPE has already been enabled in 17.2.4.3, “Enable MSCHAP and MPPE” on page 334. It can be used by clients to encrypt the PPP traffic that flows through the L2TP tunnel.

17.3.3.4 Add PPP user

The next step is to define the PPP user and to reload the router. The IP address handed out to this PPP user is given out from a pool of corporate IP addresses and can also be assigned using DHCP or RADIUS. To systems inside the corporate network the remote client will thus appear to be also inside the corporate network.

```
Center Config>ADD PPP-USER
Enter name:  []? vpnclient
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 192.168.102.110
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]


     PPP user name: vpnclient
   User IP address: 192.168.102.110
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Account Expiry: <unlimited>
   Password Expiry: <unlimited>

Is information correct? (Yes, No, Quit): [Yes] y
```

Figure 353. Center router PPP user configuration for L2TP

17.3.3.5 Add default route and enable ARP-subnet-routing

These steps and the reasons for performing them are the same as described in 17.2.4.5, “Add default route and enable ARP-subnet-routing” on page 336 for the PPTP scenario.

17.3.3.6 Activate the definitions on the center router

You activate the definitions on the center router with the command `restart` (see Figure 354):

```
Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 354. Reloading the center router

17.3.4 Installing and configuring the NTS client

NTS is a company that develops software for a variety of tasks in the IP environment, including IP address and NetBIOS name management and VPN remote access. One of their products, TunnelBuilder, is a remote access VPN client that implements PPTP, L2TP and PPP over Ethernet (PPPoE) for cable modem and xDSL access. TunnelMaster is the server software for TunnelBuilder, but the client is designed to work with any VPN gateway that implements standard protocols. TunnelBuilder is available for Windows 95, Windows 98 and Windows NT. NTS also offers remote access software for Macintosh, Linux and older versions of Windows.

To find more information about TunnelBuilder and how you can purchase it, please access the URL below:

```
http://www.nts.com
```

Important

The version of TunnelBuilder that we used for this scenario was a pre-release, so the description and screenshots shown in this redbook may vary from the software you may have purchased.

17.3.4.1 NTS TunnelBuilder capabilities

In this section we briefly lists the VPN capabilities of the TunnelBuilder client:

Table 30. NTS TunnelBuilder - VPN features

Feature	
Tunnel Type	L2TP Voluntary, PPTP
Encryption	MPPE
Authentication	PAP, CHAP, MS-CHAP (V1)
Other	Logging

We used an IBM PC 750 with Windows 98 as a client workstation for this scenario.

17.3.4.2 Client installation

NTS TunnelBuilder requires Microsoft Dial-Up Networking 1.2 or higher on Windows 95. The Windows CD-ROM is also required to complete the installation on Windows 95 and Windows 98.

To install TunnelBuilder, click **Setup** in the directory where the software has been unpacked, then follow the instructions on the screen. During the installation, an NTS VPN virtual adapter will be added to your network configuration.

Windows NT note

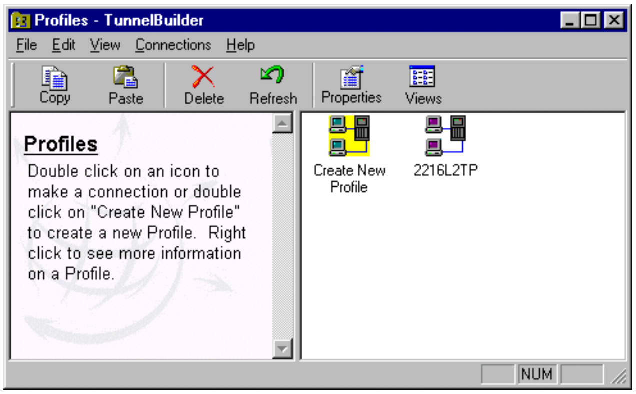
If you install TunnelBuilder on Windows NT, setup will display a Notepad window with instructions on how to install the NTS VPN adapter. You have to manually add that adapter following the steps in this window. That procedure will then invoke RAS setup so that you can add the NTS VPN adapter as a RAS port for L2TP and PPTP tunnels. Finally, select not to reboot after you finish the Networking configuration and exit the Notepad window as instructed to allow setup to finish, then let it reboot the system.

17.3.4.3 Configure a dial-up connection to the ISP

Before you can use TunnelBuilder you have to create a Dial-up Networking configuration to access your ISP. The L2TP tunnel will be established over this connection so it needs to be defined first. This step is essentially the same as described in 17.2.5.3, “Configure the Dial-Up Networking (DUN) client” on page 338 for creating a DUN entry for the ISP. The difference is that in the case of TunnelBuilder you do not have to create a second DUN entry but perform that step from the TunnelBuilder Profile window which is described in the following section.

17.3.4.4 Client configuration

Once the system has been rebooted, the TunnelBuilder client is added as an icon to the desktop. Double-click that icon to open the Profiles configuration window.



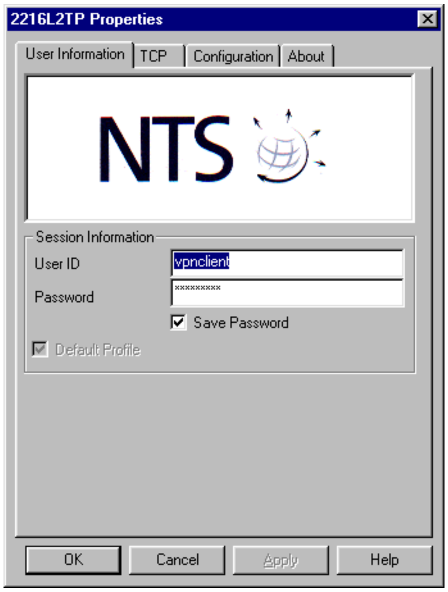
Profiles

Double click on an icon to make a connection or double click on "Create New Profile" to create a new Profile. Right click to see more information on a Profile.

Figure 355. NTS TunnelBuilder - configuration window

Create a new configuration by double-clicking the **Create New Profile** icon. Enter a name for this configuration and a user ID and password on the following screens, then click **Finish**. This is the user ID and password to connect to the corporate gateway so it has to match whatever is defined there, as described in 17.3.3.4, “Add PPP user” on page 345. An icon for the new configuration will be placed in the profile window, as shown in Figure 355.

This new profile is rather generic and requires some fine-tuning. Highlight the new configuration and click the **Properties** button to invoke the Properties window shown in Figure 356 on page 349.



Session Information

User ID: vpnclient

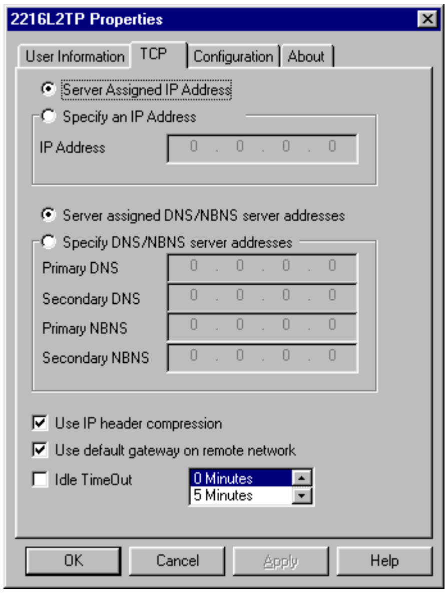
Password: *********

☑ Save Password

☑ Default Profile

Figure 356. NTS TunnelBuilder - connection properties

Check **Save Password** if you do not want to be prompted for a password every time this connection is started, then click the **TCP** tab to specify TCP/IP configuration parameters for this connection. This is shown in Figure 357.



● Server Assigned IP Address

○ Specify an IP Address

IP Address: 0 . 0 . 0 . 0

● Server assigned DNS/NBNS server addresses

○ Specify DNS/NBNS server addresses

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Primary NBNS: 0 . 0 . 0 . 0

Secondary NBNS: 0 . 0 . 0 . 0

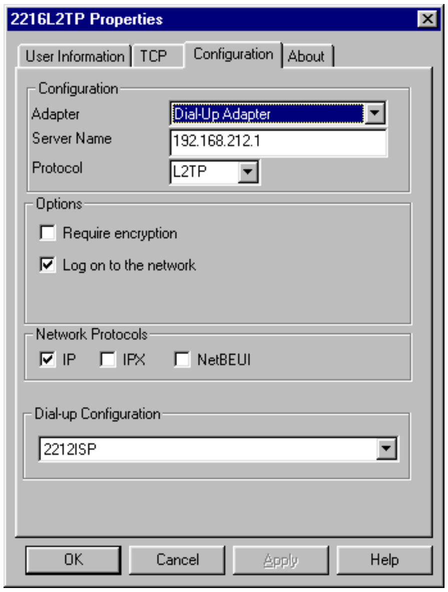
☑ Use IP header compression

☑ Use default gateway on remote network

□ Idle TimeOut: 0 Minutes / 5 Minutes

Figure 357. NTS TunnelBuilder - TCP/IP properties

Select to obtain all IP information from the server and optionally choose **Use IP header compression**. Also check **Use default gateway on remote network** to make the L2TP tunnel the default route for client traffic. Then click the **Configuration** tab to access the protocol configuration window shown in Figure 358 on page 350.



Configuration

Adapter: Dial-Up Adapter

Server Name: 192.168.212.1

Protocol: L2TP

Options

□ Require encryption

☑ Log on to the network

Network Protocols

☑ IP □ IPX □ NetBEUI

Dial-up Configuration

2212ISP

Figure 358. NTS TunnelBuilder - protocol properties

In this window you specify which tunnel protocol (L2TP, PPTP, PPPoE) you want to use over which adapter, which gateway to connect to, and which protocols to run over the tunnel.

1. In the Protocol field, select **L2TP**.

> **Note**
>
> The default is PPPoE and Ethernet Adapter if any is installed, so you have to select the protocol first in order to be able to select a dial-up adapter.

2. In the Adapter field, select **Dial-up Adapter**.
3. In the Server Name field, enter the IP address of the corporate gateway, in our case, the 2216 Center router at **192.168.212.1**.
4. You must check **Log on to the network** for the PPP connection to be established over the L2TP tunnel. Check **Require encryption** if you want to protect the traffic in the tunnel and the corporate gateway supports it. See 17.3.3.3, “Enabling L2TP encryption” on page 345 for a matching router configuration.
5. Select the network protocols you want to use over the tunnel, then, in the Dial-up Configuration window, select the dial-up connection you have previously created to access the ISP. TunnelBuilder will automatically establish that connection before starting the tunnel so you do not have to start two separate DUN sessions. Unfortunately, when you end a TunnelBuilder session it does not also take down the ISP session. This may not be viewed as a disadvantage as long as you remember to do it yourself because local telephone calls are free only in very few countries.

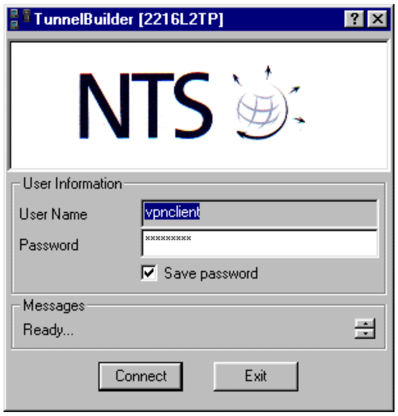
Click **OK** to finish the configuration.

17.3.5 Building the connection

To establish an L2TP tunnel using TunnelBuilder you need to use two DUN sessions: The first one to the Internet (in our case, to the ISP's router) and the second one to the center router.

17.3.5.1 Dialing to ISP router

Launch the PPP dial-up connection which establishes the Internet connection and also the L2TP tunnel by double-clicking the connection profile in the TunnelBuilder window and click **Connect**.



User Information

User Name: vpnclient

Password: *********

☑ Save password

Messages

Ready...

Figure 359. NTS TunnelBuilder - start connection

TunnelBuilder now invokes the dial-up networking entry you specified to access the ISP and places a dial-up session icon on the task bar. Next, TunnelBuilder starts the L2TP tunnel to the corporate gateway and establishes a PPP connection to it. If that is successful, another icon is placed on the task bar for the TunnelBuilder connection. Right-click on that icon to access its context menu, as shown in Figure 360.

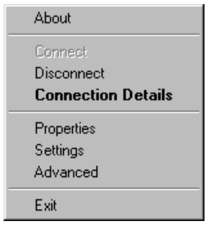
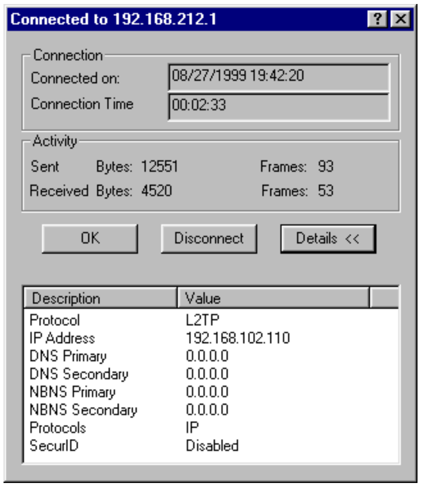


Figure 360. NTS TunnelBuilder - session context menu

Select **Connection Details** to obtain information on the L2TP tunnel, which is shown in Figure 361 on page 352.



Connection

Connected on: 08/27/1999 19:42:20

Connection Time 00:02:33

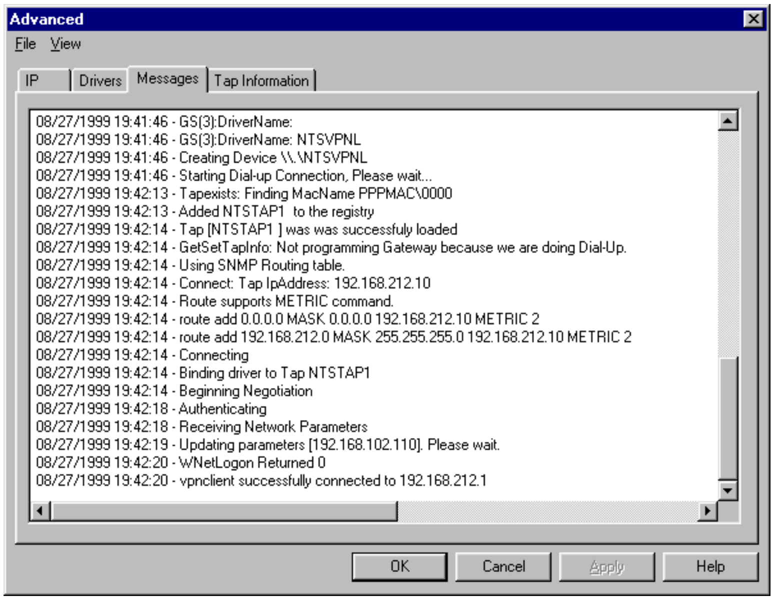
Activity

Sent	Bytes: 12551	Frames: 93
Received	Bytes: 4520	Frames: 53

Description	Value
Protocol	L2TP
IP Address	192.168.102.110
DNS Primary	0.0.0.0
DNS Secondary	0.0.0.0
NBNS Primary	0.0.0.0
NBNS Secondary	0.0.0.0
Protocols	IP
SecurID	Disabled

Figure 361. NTS TunnelBuilder - connection details

From the session context menu, select **Advanced** to obtain a full range of information on the system's present IP configuration, including interfaces, drivers and protocols as well as a message log which is shown below:



```
08/27/1999 19:41:46 - GS(3):DriverName:
08/27/1999 19:41:46 - GS(3):DriverName: NTSVPNL
08/27/1999 19:41:46 - Creating Device \\.\NTSVPNL
08/27/1999 19:41:46 - Starting Dial-up Connection, Please wait...
08/27/1999 19:42:13 - Tapexists: Finding MacName PPPMAC\0000
08/27/1999 19:42:13 - Added NTSTAP1  to the registry
08/27/1999 19:42:14 - Tap [NTSTAP1 ] was was successfuly loaded
08/27/1999 19:42:14 - GetSetTapInfo: Not programming Gateway because we are doing Dial-Up.
08/27/1999 19:42:14 - Using SNMP Routing table.
08/27/1999 19:42:14 - Connect: Tap IpAddress: 192.168.212.10
08/27/1999 19:42:14 - Route supports METRIC command.
08/27/1999 19:42:14 - route add 0.0.0.0 MASK 0.0.0.0 192.168.212.10 METRIC 2
08/27/1999 19:42:14 - route add 192.168.212.0 MASK 255.255.255.0 192.168.212.10 METRIC 2
08/27/1999 19:42:14 - Connecting
08/27/1999 19:42:14 - Binding driver to Tap NTSTAP1
08/27/1999 19:42:14 - Beginning Negotiation
08/27/1999 19:42:18 - Authenticating
08/27/1999 19:42:18 - Receiving Network Parameters
08/27/1999 19:42:19 - Updating parameters [192.168.102.110]. Please wait.
08/27/1999 19:42:20 - WNetLogon Returned 0
08/27/1999 19:42:20 - vpnclient successfully connected to 192.168.212.1
```

Figure 362. NTS TunnelBuilder - advanced connection information

You can look at the IP routing table in the Advanced information window shown above, or use the `netstat -r` command which produces the output shown in Figure 363 on page 353. The first statement shows a default route to the dial-up interface to direct all traffic over the ISP connection. The next statement shows a default route to the virtual PPP interface to direct all traffic over the L2TP tunnel to the corporate network.

Note

Our Windows 98 system has an Ethernet adapter with IP address 172.16.3.7 in addition to the dial-up adapter, so there are some routes listed in the screen above that you may not see on a dial-up only system.

```
Active Routes:

  Network Address          Netmask  Gateway Address        Interface  Metric
          0.0.0.0          0.0.0.0     192.168.88.5     192.168.88.5       2
          0.0.0.0          0.0.0.0  192.168.102.110  192.168.102.110       1
          0.0.0.0          0.0.0.0       172.16.3.2       172.16.3.7       2
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
       172.16.3.0    255.255.255.0       172.16.3.7       172.16.3.7       2
       172.16.3.7  255.255.255.255        127.0.0.1        127.0.0.1       1
   172.16.255.255  255.255.255.255       172.16.3.7       172.16.3.7       1
    192.168.102.0    255.255.255.0  192.168.102.110  192.168.102.110       1
  192.168.102.110  255.255.255.255        127.0.0.1        127.0.0.1       1
     192.168.88.0    255.255.255.0     192.168.88.5     192.168.88.5       2
     192.168.88.5  255.255.255.255        127.0.0.1        127.0.0.1       1
        224.0.0.0        224.0.0.0       172.16.3.7       172.16.3.7       1
        224.0.0.0        224.0.0.0  192.168.102.110  192.168.102.110       1
        224.0.0.0        224.0.0.0     192.168.88.5     192.168.88.5       1
  255.255.255.255  255.255.255.255     192.168.88.5     192.168.88.5       1
```

Figure 363. Routing table for L2TP connection with NTS

You can use the same router commands as described in 17.2.7, “Testing the connection” on page 340 to verify that the L2TP connection has been successfully established and that the client PPP session is active.

To verify the connection from the client, try to ping a system in the corporate network, for instance 192.168.100.3, and check the dial-up session details for increasing byte and packet counts. We have also verified this connection using Telnet and FTP between the client and a server in the corporate network, as well as using a packet sniffer in the Internet segment.

17.4 Using L2TP with IPSec

In the following section we describe how IPSec can be employed to provide strong security to L2TP tunnels in a client remote access environment. It is the way recommended by the IETF to use a combination of these two protocols for remote access VPNs.

The combination of these two protocols in a voluntary tunnel environment has the following benefits:

1. IP address assignment from the corporate address pool
2. Strong authentication and encryption for the L2TP tunnel and all traffic that flows through it
3. No cooperation required from ISPs

17.4.1 Description of the scenario

This scenario assumes that the client accesses the Internet using whatever ISP is available. The client will then build an L2TP tunnel to a corporate gateway that is protected by IPSec so that it will get an IP address in the intranet. The client will use the standard dial-up networking that comes with Windows. The IPSec-protected L2TP tunnel will be provided by iVasion WinVPN Client (`http://www.ivasion.com`), software from Wind River Systems (WRS). Below is a diagram showing our test scenario:

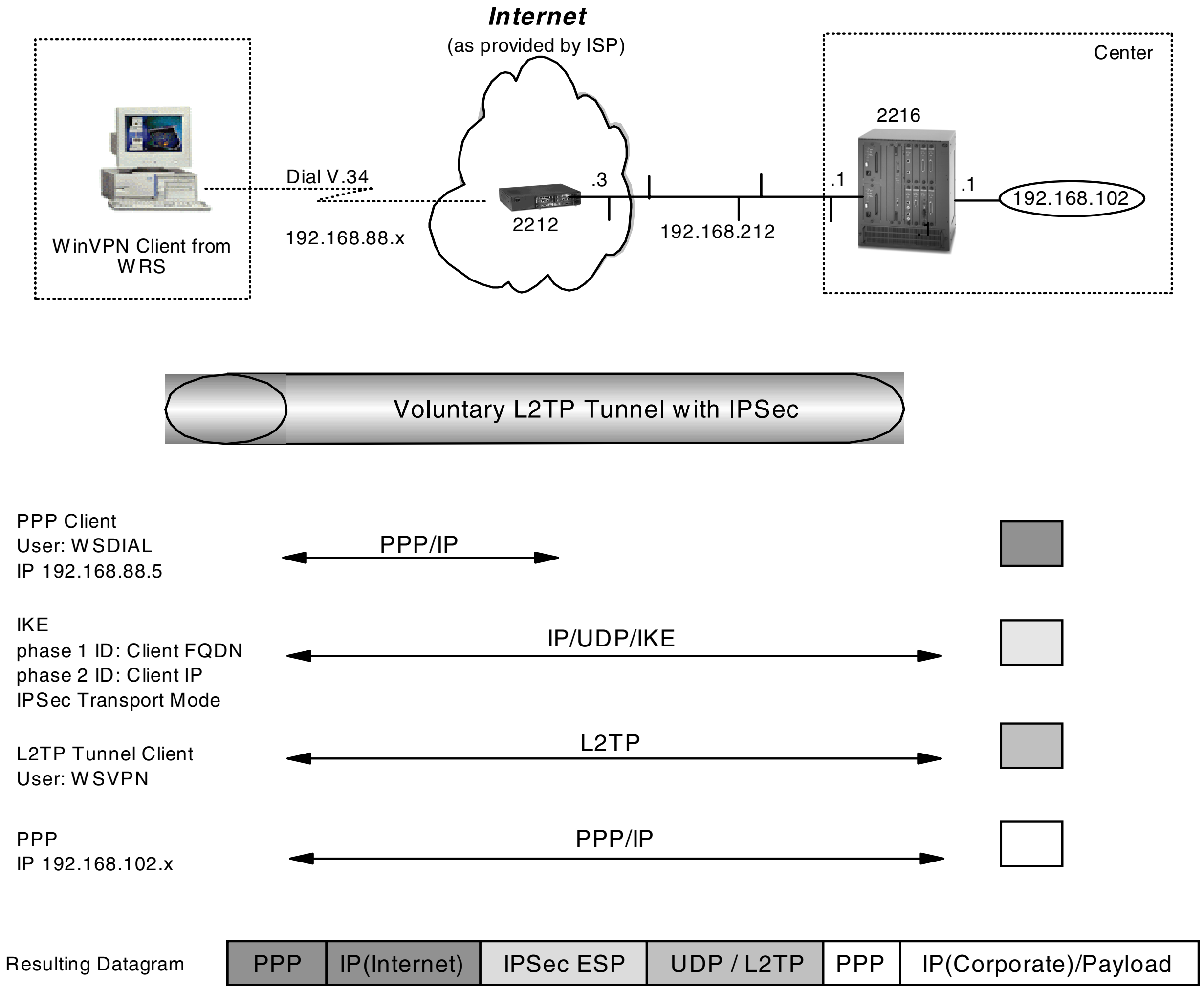


Figure 364. Remote access client using L2TP secured by IPSec

17.4.2 Definition of the ISP router

The necessary steps for configuring an ISP router for this scenario are the same as described in 17.2.3, “Definition of the ISP router” on page 330.

17.4.3 Configuring the center router

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation.

- Configure the policy and validity period for IPSec and IKE.
- Configure IPSec action and proposal.
- Configure ISAKMP action and proposal.
- Enable L2TP and add layer 2-nets.
- Add PPP-user for the dial-in workstation.
- Add the default route to the Internet and enable ARP-subnet-routing.
- Activate the definitions on the center router.

17.4.3.1 Preparation

We assume that the permanent Ethernet connection to the ISP is already established. Therefore, we can concentrate on the dial-in features of this connection.

17.4.3.2 Configure policy profile for IPSec and IKE

The first step is to configure a policy that will encapsulate L2TP traffic in an IPSec tunnel. When configuring the profile it is important that you select an address range rather than a netmask or single IP address. This is because if you use netmask the ID comparisons will fail because the netmask is of a subnet type while the ID type that will be received by the client would be an IP address type. Of course you cannot use a single IP address because you do not know what IP address the client will get from the ISP.

Additionally you also have to build the profile such that it traps UDP port 1701, which is the L2TP port.

```
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? routerware
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]?
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? routerware
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.212.1
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 2
Enter IPV4 Starting Destination Address [0.0.0.0]?
Enter IPV4 Ending Destination Address [0.0.0.0]? 255.255.255.255

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]? 2
Enter the Starting value for the Source Port [0]? 1701
Enter the Ending value for the Source Port [65535]? 1701
Enter the Starting value for the Destination Port [0]? 1701
Enter the Ending value for the Destination Port [65535]? 1701
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]: y
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]? 1
Any user within profile definition allowed access? [Yes]:
The Source and/or Destination Address information you specified
includes all addresses.  You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy.  The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]:
```

Figure 365. Center router IKE policy configuration for L2TP + IPSec

```
Here is the Profile you specified...

Profile Name    = routerware
        sAddr     =  192.168.212.1 :  sPort= 1701 : 1701
        dAddr:End =        0.0.0.0 : 255.255.255.255 dPort= 1701 : 1701
        proto     =             17 : 17
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: routerware

Enter number of the profile for this policy [1]?
```

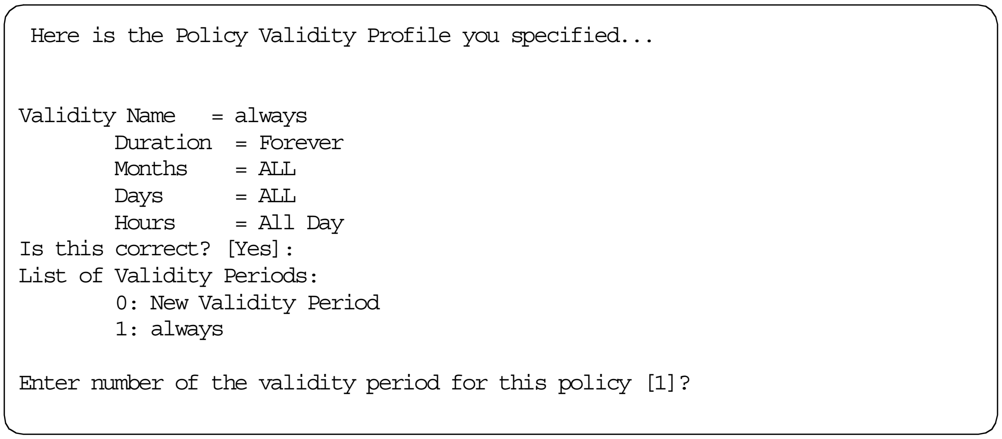
Figure 366. Center router profile configuration for L2TP + IPSec

17.4.3.3 Configure validity period

The next step is to define a validity period.

```
List of Validity Periods:
        0: New Validity Period

Enter number of the validity period for this policy [0]? 0
Enter a Name (1-29 characters) for this Policy Valid Profile []? always
Enter the lifetime of this policy. Please input the
information in the following format:
                yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?
```

Figure 367. Center router validity period configuration for L2TP + IPSec - part 1



```
 Here is the Policy Validity Profile you specified...


Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
Is this correct? [Yes]:
List of Validity Periods:
        0: New Validity Period
        1: always

Enter number of the validity period for this policy [1]?
```

Figure 368. Center router validity period configuration for L2TP + IPSec - part 2

17.4.3.4 Configure IPSec action and proposal

The next step is to define the IPSec action and proposal. You should note that you do not know the tunnel endpoint so 0.0.0.0 is entered as the destination tunnel endpoint.

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? routerware
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [192.168.102.1]? 192.168.212.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
Enter a Name (1-29 characters) for this IPsec Proposal []? routerware
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
```

Figure 369. Center router IPSec policy configuration for L2TP + IPSec - part 1

Also take note of the SA lifesize and lifetime. These are the values used by the WinVPN client which are significantly less than the default values in the router. If these are not changed the tunnel will not come up, since the router's acceptable minimum is 75% of the configured value. Of course the router's minimum tolerance percentage level could have been changed instead.

Tip

How do you find out what transforms and lifetimes a client proposes in order to match a configuration on a VPN gateway? Well, normally a client allows you to modify those settings but the WinVPN Client is different in that it allows the user very little to configure which is not a bad thing. In this case you need to run the client against a system that supports IKE and also provides extensive output for debugging. We have used IBM AIX 4.3.2 for that purpose.

```
Do you wish to enter any ESP transforms for this proposal? [No]: y
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]? 0
Enter a Name (1-29 characters) for this IPsec Transform []? routerware
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]? 2
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]?
List of ESP Cipher Algorithms:
     1)  ESP DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]?
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]? 10240
Security Association Lifetime, in seconds (120-2147483647) [3600]? 300


Here is the IPSec transform you specified...


Transform Name  = routerware
        Type =ESP   Mode =Transport  LifeSize=   10240 LifeTime=     300
        Auth =SHA   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
        0: New Transform
        1: routerware

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:

Here is the IPSec proposal you specified...

Name  = routerware
        Pfs   = N
        ESP Transforms:
                routerware
Is this correct? [Yes]:
List of IPSEC Proposals:
        0: New Proposal
        1: routerware

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:
```

Figure 370. Center router IPSec policy configuration for L2TP + IPSec - part 2

```
Here is the IPSec Action you specified...

IPSECAction Name = routerware
        Tunnel Start:End         =  192.168.212.1 : 0.0.0.0
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                routerware
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: routerware

Enter the Number of the IPSEC Action [1]?
```

Figure 371. Center router IPSec action configuration for L2TP + IPSec

17.4.3.5 Configure ISAKMP action and proposal

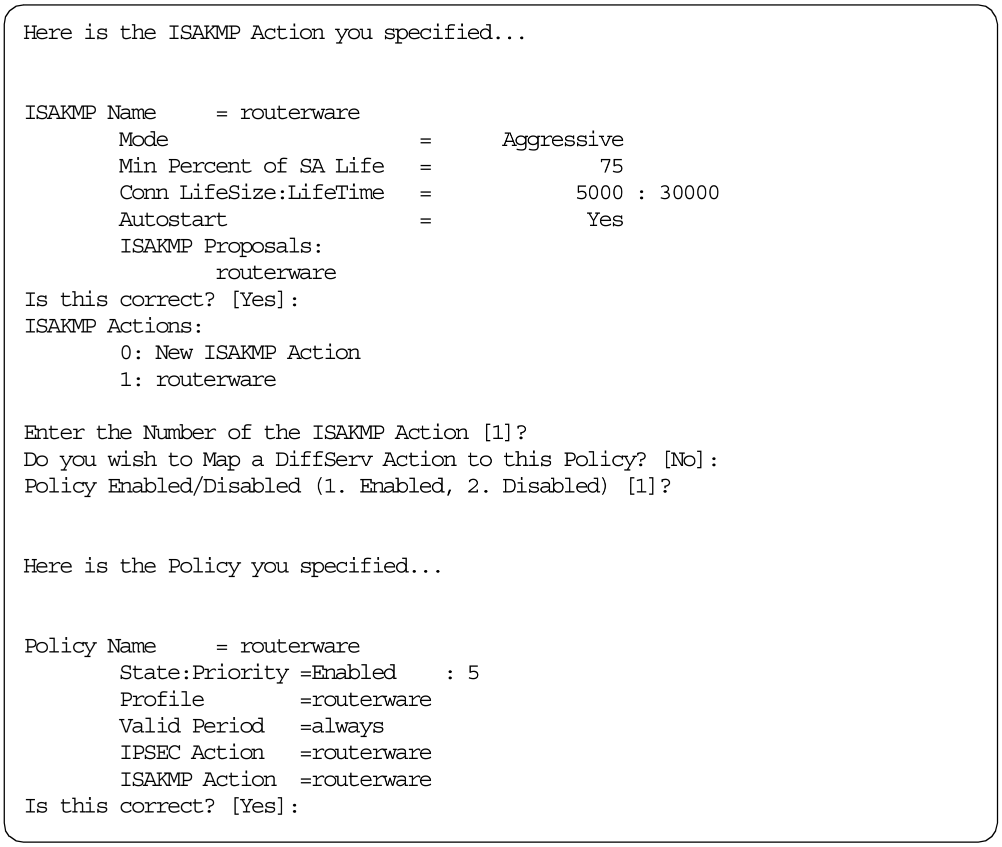
Once the IPSec action and proposal have been fully defined the next step is to define the ISAKMP action/proposal. The main point in this step is that aggressive mode must be used because the IP address of the client will not be known. In main mode the IDs are exchanged in messages 5 and 6, however, the keys must be known before then to encrypt messages 5 and 6 themselves. In aggressive mode the IDs are exchanged during the beginning of the exchange so the keys to be used can be determined at that time. In addition, encryption the last message of an aggressive mode exchange is optional.

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? routerware

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]? 2
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]:
```

Figure 372. Center router ISAKMP action configuration for L2TP + IPSec - part 1

```
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal

Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? routerware

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  Certificate (RSA SIG)

Select the authentication method (1-2) [1]?

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
     1)  DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?


Here is the ISAKMP Proposal you specified...

Name = routerware
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: routerware

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:
```

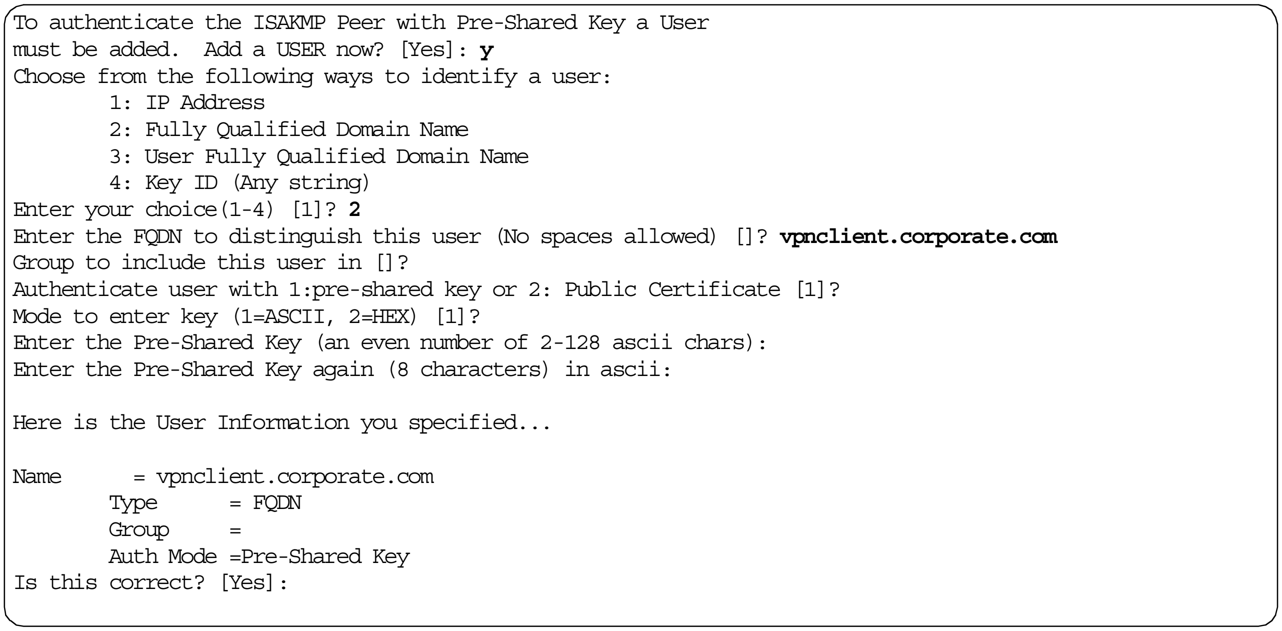
Figure 373. Center router ISAKMP action configuration for L2TP + IPSec - part 2



```
Here is the ISAKMP Action you specified...


ISAKMP Name     = routerware
        Mode                    =      Aggressive
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =             Yes
        ISAKMP Proposals:
                routerware
Is this correct? [Yes]:
ISAKMP Actions:
        0: New ISAKMP Action
        1: routerware

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?


Here is the Policy you specified...


Policy Name     = routerware
        State:Priority =Enabled    : 5
        Profile        =routerware
        Valid Period   =always
        IPSEC Action   =routerware
        ISAKMP Action  =routerware
Is this correct? [Yes]:
```

Figure 374. Center router ISAKMP action configuration for L2TP + IPSec - part 3

The last step of the policy definition is to enter the user as a fully qualified domain name (FQDN). This is the ID type that must be used because IP addresses are not known.



```
To authenticate the ISAKMP Peer with Pre-Shared Key a User
must be added.  Add a USER now? [Yes]: y
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]? 2
Enter the FQDN to distinguish this user (No spaces allowed) []? vpnclient.corporate.com
Group to include this user in []?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (8 characters) in ascii:

Here is the User Information you specified...

Name      = vpnclient.corporate.com
        Type      = FQDN
        Group     =
        Auth Mode =Pre-Shared Key
Is this correct? [Yes]:
```

Figure 375. Center router ISAKMP ID configuration for L2TP + IPSec

The FQDN configured in Figure 375 on page 363 must match the FQDN that was specified at the client as described in 17.4.4, “Installing and configuring the WinVPN client” on page 364.

17.4.3.6 Configure L2TP

These steps and the reasons for performing them are the same as described in 17.3.3.2, “Configure L2TP” on page 344 for the L2TP scenario.

17.4.3.7 Add PPP user

These steps and the reasons for performing them are the same as described in 17.3.3.4, “Add PPP user” on page 345 for the L2TP scenario.

17.4.3.8 Add default route and enable ARP-subnet-routing

These steps and the reasons for performing them are the same as described in 17.2.4.5, “Add default route and enable ARP-subnet-routing” on page 336 for the PPTP scenario.

17.4.3.9 Activate the definitions on the center router

You activate the definitions on the center router with the command `restart` (Figure 376):

```
Center Config>WRITE
Config Save: Using bank B and config number 3
Center Config>
Center *RELOAD
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 376. Reloading the Center Router

17.4.4 Installing and configuring the WinVPN client

Wind River Systems (WRS) develops OEM networking software (for other vendors to include in their products) and other commercial products through its business division Wind River Networks located at Newport Beach. This division provides Windows-based products to Internet service providers, corporations, remote offices and home users with standards-based network access solutions. The commercial products include a VPN client, VPN server and NAT gateway running on Windows 95, Windows 98 and Windows NT. These solutions support major and emerging protocol standards including NAT, PPTP, L2F, L2TP, IPSec, PPP over Ethernet and more. To find more information on WinVPN Client and how you can purchase it, please access the URL below:

`http://www.ivasion.com`

We were using Version 1.2 of the WinVPN client for the scenarios in this redbook.

> **Important**
>
> Please be aware also that the WinVPN client requires Microsoft Internet Explorer 5.0 or it will not install.

17.4.4.1 WinVPN client capabilities

In this section we briefly lists the VPN capabilities of the WinVPN client from WRS:

Table 31. WinVPN client 1.2 from WRS - VPN features

Feature	
Tunnel Type	IKE
IPSec Header Format	RFCs 24xx
IKE	
Key Management Tunnel (Phase 1)	
Negotiation Mode	Main Mode, Aggressive Mode
Encryption Algorithm	DES, 3DES
Authentication Method	Pre-Shared Key, RSA Signatures
Authentication Algorithm	HMAC-MD5, HMAC-SHA
Diffie-Hellman Group	Group 1, Group 2
Send Phase 1 Delete	No
On-demand Tunnels	No
Data Management Tunnel (Phase 2)	
Encapsulation Mode	Transport Mode
Security Protocol	ESP
AH Authentication Algorithm	HMAC-MD5, HMAC-SHA
ESP Encryption Algorithm	DES, 3DES
ESP Authentication Algorithm	HMAC-MD5, HMAC-SHA
Multiple SA Proposals	Yes
Perfect Forward Secrecy (PFS)	Yes
Other	Voluntary L2TP, Logging

We use an IBM Thinkpad with Windows 95 and an IBM PC 750 with Windows NT as client workstations for this scenario.

17.4.4.2 Client installation

The WinVPN client requires Microsoft Dial-up Networking 1.2 or higher on Windows 95. The Windows 95 CD-ROM is also required to complete the installation on Windows 95.

To install the WinVPN clint, click **Setup** in the directory where the software has been unpacked, then follow the instructions on the screen. During the installation, two iVasion VPNic virtual adapters will be added to your network configuration. The installation procedure also creates and stores in the registry a private/public key pair if you later want to use IKE with certificate-based authentication. New keys can be created at a later time. Once the setup procedure has finished, reboot your system.

Windows NT note

If you install WinVPN on Windows NT, setup will display a message that the installation could not complete because no VPN adapter could be found. You have to manually add that adapter following the steps in the Troubleshooting guide which is provided electronically with the software. That procedure will then invoke the RAS setup so that you can add the iVasion VPNic as a RAS port for L2TP tunnels.

17.4.4.3 Client configuration

Once the system has been rebooted, the WinVPN client is added as an icon to the task bar. Use the left mouse button on that icon to invoke the configuration menu as shown in Figure 377:

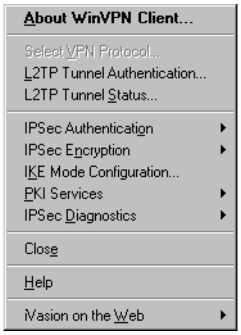


Figure 377. WinVPN client configuration menu

You have to configure the following settings to make this scenario work:

IPSec authentication

Here you can specify if you want to use pre-shared keys or certificates for IKE Phase 1 authentication. We used pre-shared keys. Certificates are supported in a copy-and-paste manner, meaning you have to manually create a certificate request, copy and paste it into a Web browser, send it to a CA, and copy and paste the certificate and the CA certificate back into the VPN client.

Important

When you switch from pre-shared key authentication to certificate-based authentication, all pre-shared key definitions will be lost.

IPSec encryption

Choose either DES or 3DES. The client will send all possible proposals for both DES and 3DES during Phase 1 and Phase 2 negotiations. This option only tells the client which transforms should be offered first. This feature is very practical in that it allows a VPN gateway to pick the appropriate proposal. It is left to the VPN gateway to enforce (that is, require) the security transform of choice. The VPN gateway may even be configured to offer or support only one transform during negotiations.

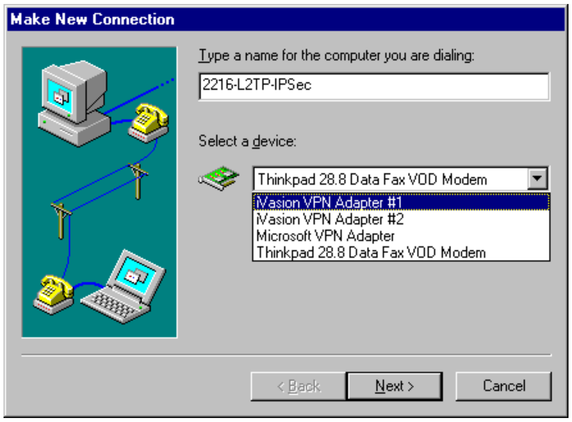
IKE mode

Select either main or aggressive mode. Because the client in our scenario is assigned a dynamic IP address from an ISP we have to use aggressive mode. As the ID we are using the fully qualified domain name (FQDN) vpnclient.corporate.com which has to be matched by the VPN gateway configuration as described in 17.4.3.5, “Configure ISAKMP action and proposal” on page 361. Main mode can be used with dynamic IP addresses and certificates.

L2TP tunnel authentication

Enter the user ID for the LNS if L2TP tunnel authentication is enabled at the server. For our scenario we did not use it because the client was already authenticated using IKE.

Next, you have to create dial-up entries for the ISP and the corporate gateway (L2TP tunnel server). This is done in the same way as described in 17.2.5.3, “Configure the Dial-Up Networking (DUN) client” on page 338 with the only difference that instead of the Microsoft VPN adapter you have to use the iVasion VPNic (#1 or #2) adapter as a device for the entry that describes the tunnel server, as shown in Figure 378 for a Windows 95 system:

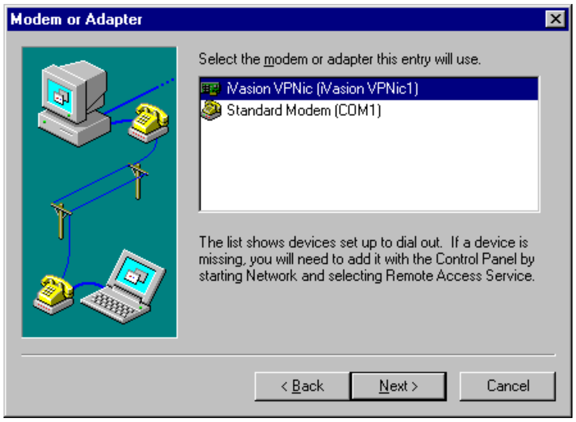


Type a name for the computer you are dialing:
2216-L2TP-IPSec

Select a device:
Thinkpad 28.8 Data Fax VOD Modem
iVasion VPN Adapter #1
iVasion VPN Adapter #2
Microsoft VPN Adapter
Thinkpad 28.8 Data Fax VOD Modem

Figure 378. Dial-up networking entry for L2TP server using WinVPN Client from WRS on Windows 95

The configuration on Windows NT is similarly performed by adding an entry for the ISP and another entry for the LNS, as shown in Figure 379 on page 368:



Modem or Adapter

Select the modem or adapter this entry will use.

iVasion VPNic (iVasion VPNic1)
Standard Modem (COM1)

The list shows devices set up to dial out. If a device is missing, you will need to add it with the Control Panel by starting Network and selecting Remote Access Service.

Figure 379. Dial-up networking entry for L2TP server using WinVPN Client from WRS on Windows NT

17.4.5 Building the connection

To establish an L2TP tunnel using the WinVPN client you need to use two DUN sessions: The first one (DUN1) to the Internet (in our case to the ISP's router) and the second one (DUN2) to the center router.

17.4.5.1 Dialing to ISP router

We launch the PPP dial-up connection which establishes the Internet connection and log on with the user ID `wsdial`.

At this time, you would assume that you have full Internet connectivity as is normally the case with PPP access. However, the WinVPN Client software hides that connectivity from the user and all applications until the L2TP tunnel is established and secured with IPSec.

17.4.5.2 Controlling traffic through the VPN tunnel

If the box, Use default gateway on remote network, located under **My Computer->Dial-Up Networking->DUN2->Properties->Server Types->TCP/IP Settings**, is checked, then all traffic from the client is forced into the DUN2 connected and hence into the tunnel to the corporate network.

If the box, Use default gateway on remote network, is unchecked, then only traffic bound to the corporate network would go through the tunnel.

WinVPN Client does not support simultaneous direct Internet access (outside the tunnel) and VPN access (through the tunnel) on the same network interface. That is, it does not support concurrent use (or sharing) of a network interface. If another network interface (say using cable or DSL) is available, direct Internet access is possible through the provider of such broadband service.

If direct access to the Internet is required (and no VPN), one only needs to do the following:

1. Disconnect from the ISP, if the dial-up connection is up.
2. Shutdown the WinVPN Client, if it is running.
3. Connect to the ISP.

At this time, direct Internet access is available.

When connection to the corporate network (VPN) is required, one needs to do the following:

1. Disconnect from the ISP if the Dial-Up connection is up.
2. Startup the WinVPN Client again by clicking **Start->Programs->StartUp->WinVPN Client**.
3. Connect to the ISP.
4. Connect to the corporate VPN gateway.

At this time, the client is logged on to the corporate intranet.

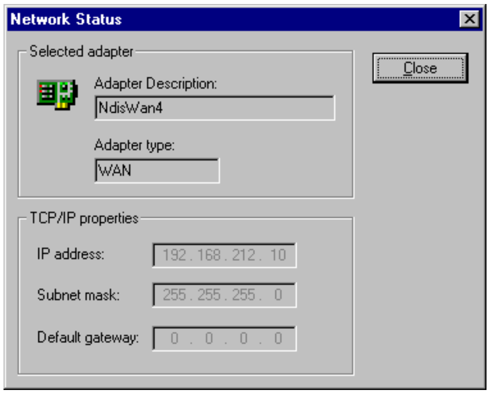
The routes on the Windows NT workstation look like the following (`netstat -r`) - see Figure 380:

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1  1
     192.168.88.5  255.255.255.255        127.0.0.1       127.0.0.1  1
   192.168.88.255  255.255.255.255     192.168.88.5    192.168.88.5  1
        224.0.0.0        224.0.0.0     192.168.88.5    192.168.88.5  1
  255.255.255.255  255.255.255.255     192.168.88.5    192.168.88.5  1
```

Figure 380. Routes on the workstation after logon to the ISP

Of course WinVPN Client has to allow IKE negotiations and the IPSec protected L2TP tunnel traffic to flow back to the corporate network, but it completely hides that from the user.

You can, however, determine your actual ISP-assigned IP configuration by selecting **IPSec Diagnostics -> Network Status** from the WinVPN context menu of the task bar icon.



Selected adapter

Adapter Description: NdisWan4

Adapter type: WAN

TCP/IP properties

IP address: 192 . 168 . 212 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 0 . 0 . 0 . 0

Figure 381. Verifying ISP connectivity with WinVPN Client

Address information for both the ISP dial-up connection and L2TP tunnel can also be obtained from the Dial-up Monitor on Windows NT.

17.4.5.3 Dialing to center router through tunnel

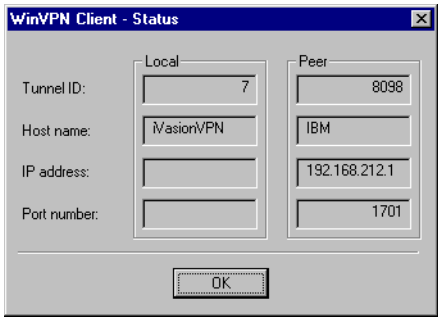
Launch the L2TP connection to create the tunnel to the center router with the user ID `wsvpn`.

This will first kick off an IKE negotiation between the WinVPN client and the router that will be used to protect the L2TP tunnel. When that is successful, the L2TP tunnel itself will be established. Once the tunnel is in place, you can ping all hosts on the center intranet. The command `netstat -r` shows the updated routing table on the workstation (see Figure 382):

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  192.168.102.110  192.168.102.110  1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1  1
    192.168.102.0    255.255.255.0  192.168.102.110  192.168.102.110  1
  192.168.102.110  255.255.255.255        127.0.0.1        127.0.0.1  1
  192.168.102.255  255.255.255.255  192.168.102.110  192.168.102.110  1
     192.168.88.5  255.255.255.255        127.0.0.1        127.0.0.1  1
   192.168.88.255  255.255.255.255     192.168.88.5     192.168.88.5  1
        224.0.0.0        224.0.0.0  192.168.102.110  192.168.102.110  1
        224.0.0.0        224.0.0.0     192.168.88.5     192.168.88.5  1
  255.255.255.255  255.255.255.255     192.168.88.5     192.168.88.5  1
```

Figure 382. Routes on the workstation after building the L2TP and IPSec connections

To display L2TP tunnel status, select that option from the WinVPN task bar icon menu:



WinVPN Client - Status

	Local	Peer
Tunnel ID:	7	8098
Host name:	iVasionVPN	IBM
IP address:		192.168.212.1
Port number:		1701

Figure 383. L2TP tunnel status for WinVPN Client

By selecting **IPSec Diagnostics -> View Log** from the WinVPN task bar icon menu, you can access the client log file where information about successfully established IKE and L2TP sessions is displayed. Under Windows 95 this is a flat file, under Windows NT these messages are logged to the application log of the Windows NT Event Log.

Chapter 18. Connecting remote users with compulsory tunneling

Compulsory tunneling is where a client PPP connection is extended using a tunnel by an LAC back to an LNS. A PPP link from the client to the LAC and IP infrastructure between the LAC and LNS is required. IP connectivity between LAC and LNS could be achieved through a temporary connection or through a permanent connection like a LAN interface. As far as compulsory tunneling is concerned, client IP connectivity will not be available until the layer-2 tunnel has been established and the PPP connection successfully established with the LNS. As result you have to establish a trust relationship (service level agreement) with the ISP to act as LAC for any layer-2 tunnels you want to establish between a remote client and a central site.

18.1 Compulsory tunneling with IBM 221x routers

IBM 221x routers support compulsory tunneling using Cisco's L2F, L2TP and Microsoft's PPTP. All three methods are implemented in the same manner. The following will describe how the components of the IBM routers fit into a compulsory layer-2 tunneling framework.

It is important to remember that all layer-2 technologies eventually form a network structure where dial-in users use PPP to access a network using a corporate gateway. So even if you have a dial-in client accessing the LAC, which builds the tunnel to the LNS, as far as the corporate network is concerned they look just like users who directly dial into the corporate gateway using PPP. We shall use this as our reference point when showing how the IBM routers fit into the layer-2 framework (see Figure 384):

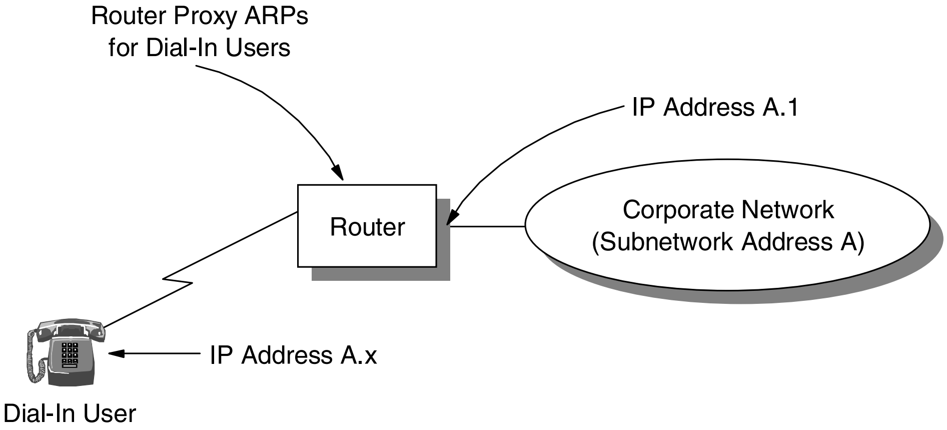


Figure 384. Dial-in PPP reference diagram

Since the layer-2 tunneling structure tries to emulate a simple PPP dial-in infrastructure we should initially examine how an IBM 221x router implements its components to support such a user.

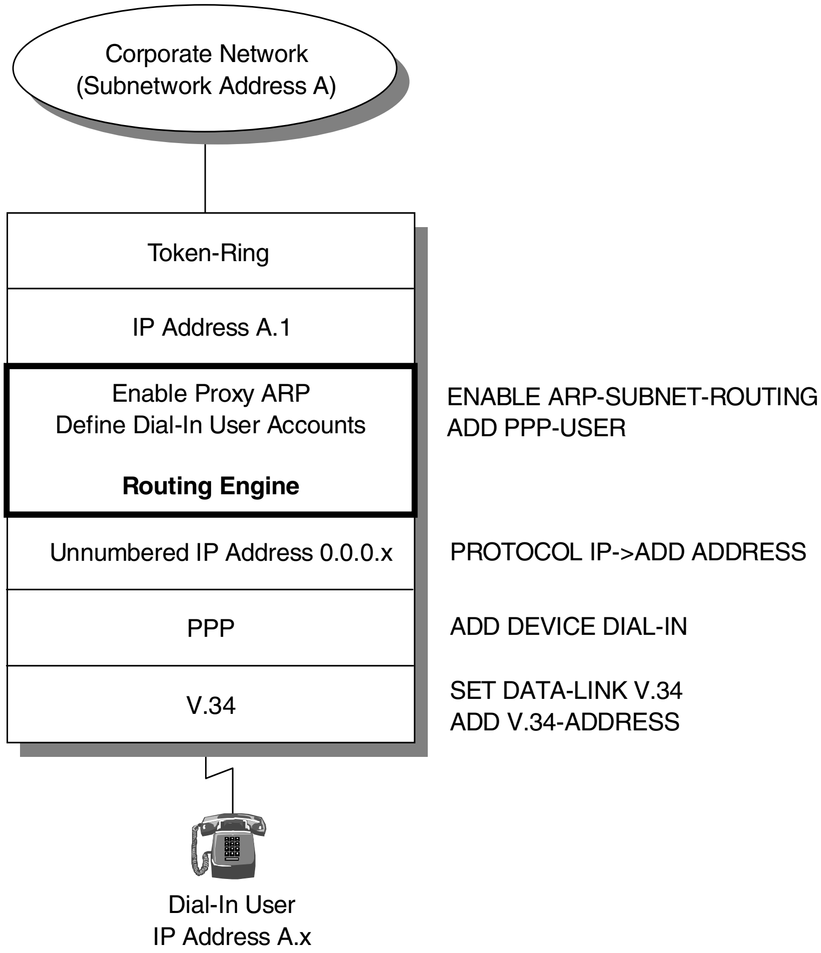


Figure 385. IBM router implementation with PPP dial-in user

In a standard PPP dial-in scenario the remote users have IP addresses on the corporate network, as if they were locally attached to the corporate LAN. To support dial-in users in this way the router must perform a proxy ARP function on behalf of the remote users, since the dial-in users are not physically on the corporate network to respond to ARPs themselves. When the router receives a packet for a dial-in user it has to forward through the dial-in interface. The unnumbered IP address gives the router an IP address to do this. The unnumbered IP address is not a real IP address in that it is only used by the router to know to which interface to forward a packet, that is, one-way traffic to the dial-in user. The dial-in user on the other hand thinks he has a real IP address on a corporate network.

For an IBM router to support a standard PPP dial-in scenario the following must be configured:

1. Physical dial-in circuit. This is the process where you configure the physical dial-in interface with the `SET DATA-LINK V.34` and `ADD V.34-ADDRESS` commands.
2. PPP dial-in. This is where you set the interface you just configured in step 1 above to be supported as a PPP dial-in circuit with the command `ADD DEVICE DIAL-IN.`.

3. Unnumbered IP Address. This is where you give the dial-in interface an IP address that the router can forward out of by using the PROTOCOL IP and ADD ADDRESS commands.
4. Proxy ARPing. This ensures that the router responds to ARPs for the dial-in users with the command ENABLE ARP-SUBNET-ROUTING.
5. PPP Dial-in Users. This process configures the accounts of the the dial-in user with the ADD PPP-USER command.

When building a compulsory layer-2 infrastructure exactly the same operations are performed except they are split over two routers, the LAC and LNS, and have a few extra steps to join them together.

Let us first examine what is configured in the LAC.

The LAC is where the remote dial-in user actually dials so it has to be configured with all the physical components necessary to support the physical interface, that is, steps 1 and part of step 2. The other steps (other parts of steps 2, 3 and 4) will be done in the LNS. So now there must be a mechanism to join the LAC and LNS. This is where the layer-2 tunnel comes in. It is this tunnel that extends the PPP all the way into the LNS. This layer-2 tunnel is generated by the command ADD TUNNEL-PROFILE. In this profile you configure the IP address of the tunnel endpoint.

The next item that needs to be configured is the name of the tunnel endpoint. The router uses this name to determine which users have to go over the tunnel. For example, if the tunnel endpoint's name is tunlns, then any user with a user ID in the form of xxx@tunlns will go through the tunnel. The name must match the LNS's local name. You also have to configure a local name in the LAC that matches with the LNS's tunnel endpoint name. With a secret password it is these two parameters that authenticate the tunnel between the LNS and LAC. The layer-2 tunnel interface is then placed on a real IP packet so that it can traverse the network to the LNS (see Figure 386 on page 374).

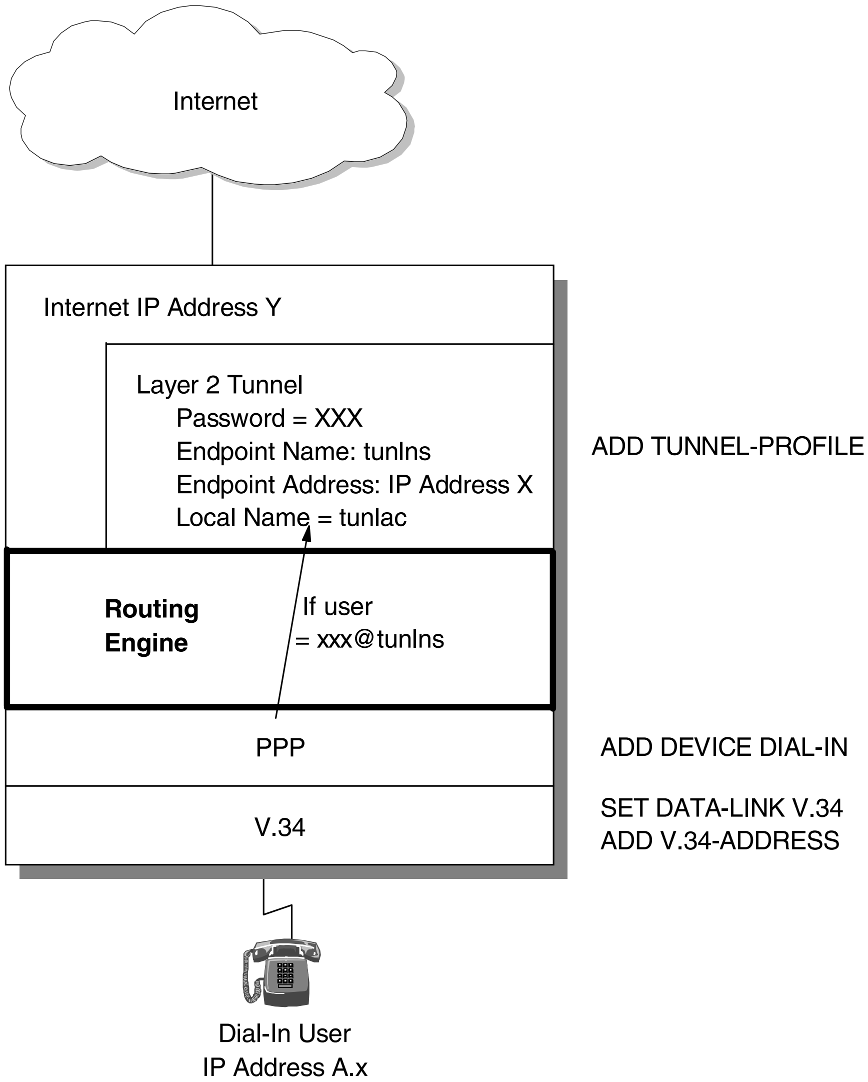


Figure 386. IBM router implementation of LAC

Note

You may have noticed that on the LAC an unnumbered IP address was not configured because it was not needed. This is because the PPP circuit will be forwarded onto the tunnel. In practical implementations you would normally do this so that the dial-in interface can support standard dial-in PPP users as well as those that will be tunneled.

As mentioned earlier the LNS must perform other parts of steps 2, 3 and 4. Before it can do this it must build a component to terminate the layer-2 tunnel from the LAC. The same command `ADD TUNNEL-PROFILE` is used to doing this. The problem now is that the router has no mechanism to handle the PPP circuit since the physical layer-2 interface is in the LAC. To overcome this the IBM routers deploy a virtual layer-2 PPP interface so that the LNS router has a PPP interface that can be treated as any other locally attached PPP interface.

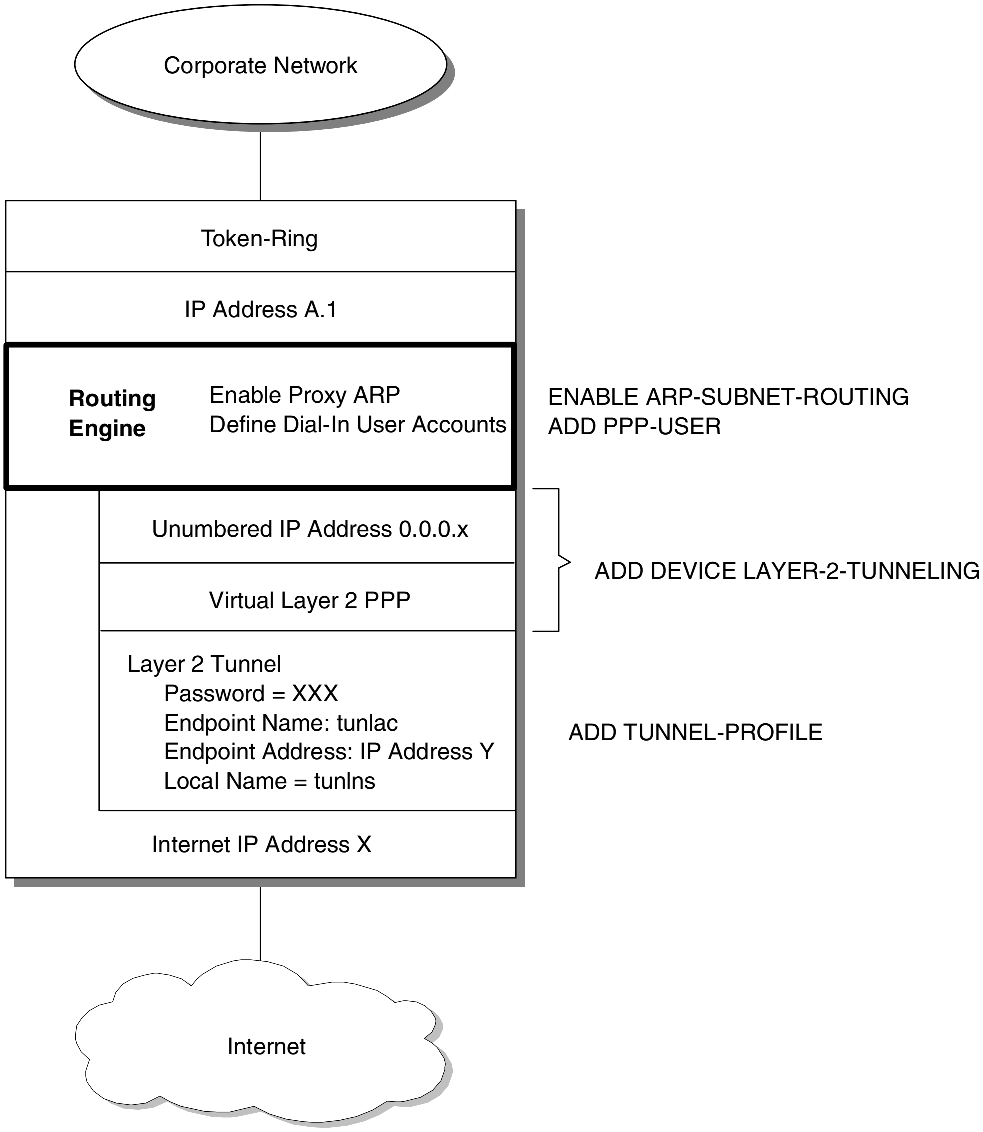


Figure 387. IBM router implementation of LNS

This virtual component is built by ADD DEVICE LAYER-2-TUNNELING. In addition to the virtual component this command also automatically adds the unnumbered IP address (see Figure 387). Now all that is required is steps 3 and 4. These steps are performed in the usual manner on the LNS.

The end result is that from the corporate gateway (LNS) point of view it thinks that all their PPP dial-in circuits are locally attached and the user's point of view is that it is directly dialing into the corporate router per the reference diagram (Figure 384 on page 371). In reality they are split in half and the joining point is the virtual PPP interface at the LNS and the real PPP interface in the LAC (see Figure 388 on page 376). Compare this diagram with Figure 385 on page 372, which shows the IBM router implementation with the PPP dial-in user.

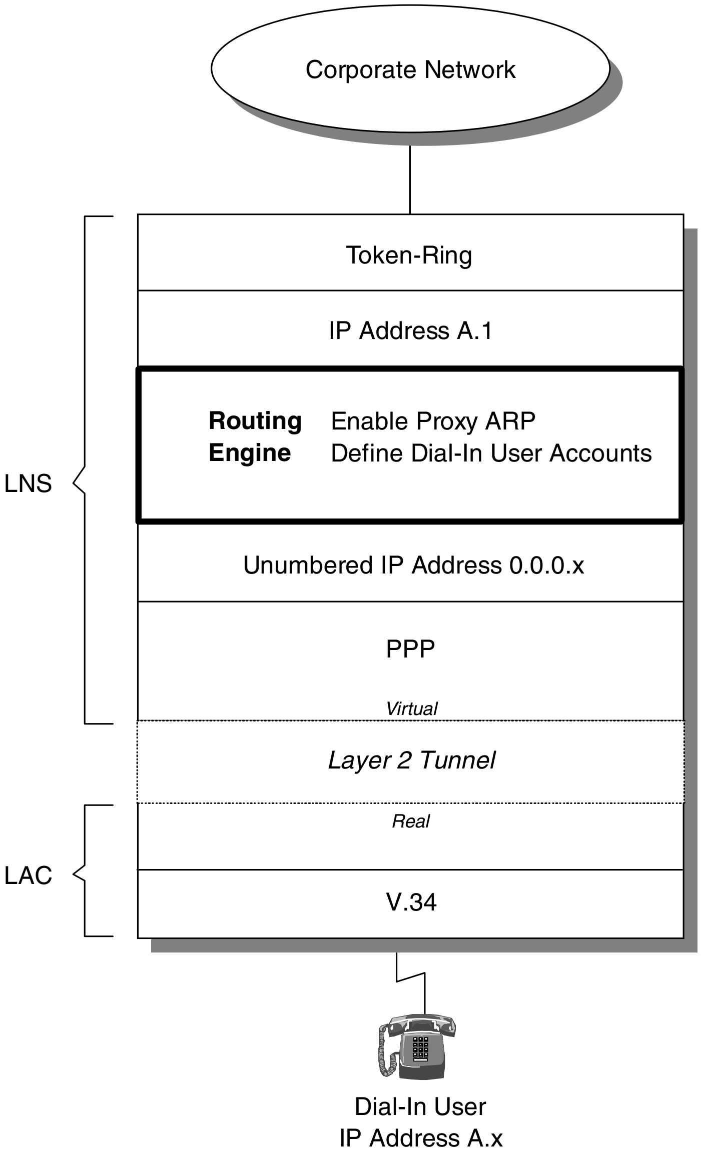


Figure 388. Consolidated layer-2 tunnel structure

18.2 Using Layer 2 Forwarding (L2F)

Layer 2 Forwarding (L2F) is Cisco’s proprietary method of of implementing layer-2 tunnels. It can only support a compulsory tunnel configuration and therefore must always involve cooperation with the ISP.

L2F is recommended when needing to connect with Cisco routers, however, it is not recommended for the connection of two IBM routers. Where possible, proprietary implementations should be avoided so with IBM-IBM scenarios L2TP is recommended.

18.2.1 Architecture

L2F is a compulsory tunneling method. Like all layer-2 tunnels it delivers a PPP interface that is tunneled to the corporate gateway which makes the client appear as if it dialed directly in to that corporate gateway.

L2F terminology refers to the router that the client dials in to (normally an ISP controlled device) as the Network Access Server (NAS). With L2F the NAS initiates the tunnel to the corporate router which is controlled by the enterprise. This corporate router is called the home gateway.

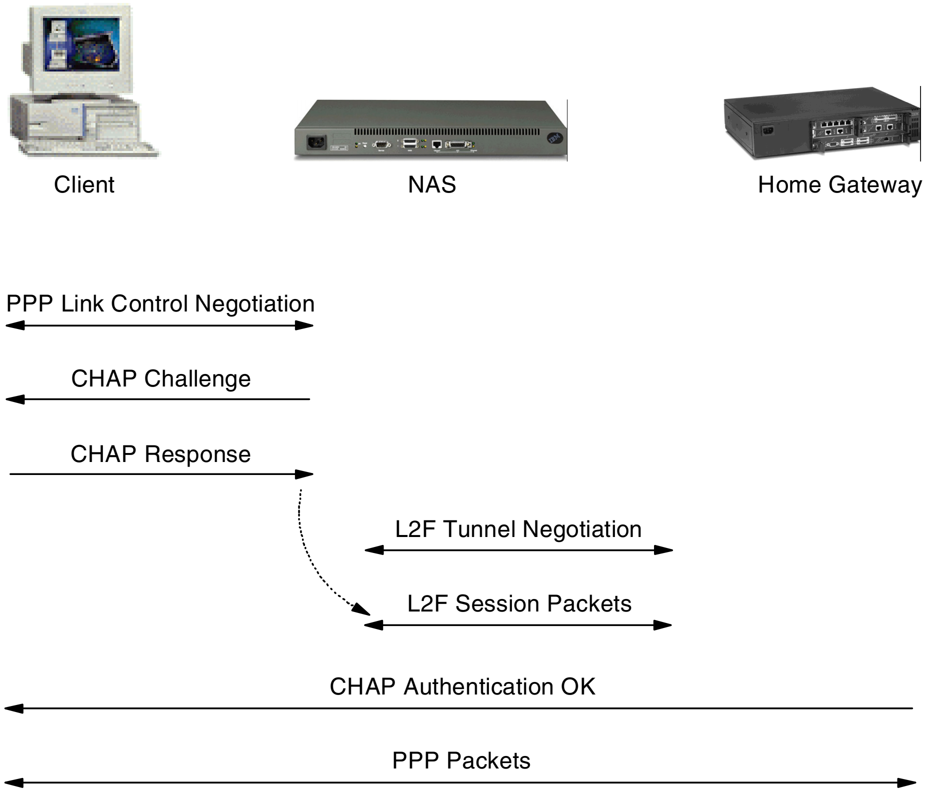


Figure 389. Basic L2F flows

When a client dials in to the NAS, standard PPP LCP negotiation occurs. Once this has completed the NAS sends a CHAP challenge to the client. The client then responds with its CHAP response. It is at this point that the NAS recognizes that it needs to make a tunnel to the home gateway. So the NAS then initiates the creation and opening of the L2F tunnel to the home gateway. Once the tunnel is open the NAS and home gateway exchange L2F session packets which include the forwarding of the CHAP response to the home gateway. If successful the home gateway responds to the client indicating that the CHAP authentication process was OK and then PPP packets can flow between the client and home gateway.

The IBM router can perform the role of an NAS or home gateway.

18.2.2 Description of the scenario

In the following example an IBM 2212 will be used to represent the ISP infrastructure and will perform the role of the NAS. A Cisco router will be used to represent the enterprise router and will be configured as the home gateway (see Figure 390):

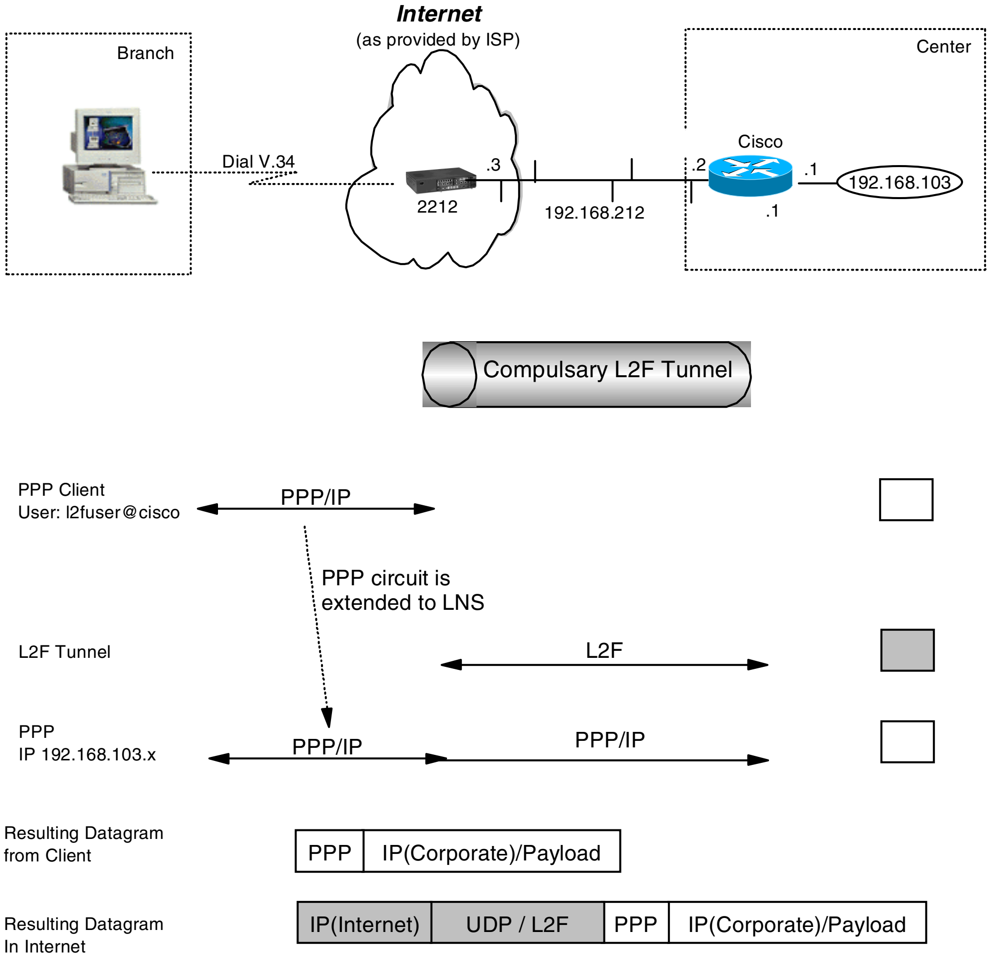


Figure 390. L2F scenario

In a compulsory tunneling scenario the dial-up client is unaware of the existence of any layer-2 tunnel. This means that the dial-in client is configured as a standard PPP dial-in client. The important part is the user name because it is that user name that determines whether the dial-in client goes into the tunnel. The user name has to be in the form of xxx@tunnel_end_point_name. In our scenario the tunnel endpoint will be called cisco and the user l2f. Therefore, the user name entered in to the dial-in client has to be l2f@cisco.

What has to occur next is to define the two routers involved in the tunnel: an IBM 2212 acting as the NAS and a Cisco router as the home gateway.

18.2.3 Definition of the ISP router

The ISP router in this scenario is the NAS since it will be receiving the dial-in users and will extend their PPP connection to the LNS. If we examine how an IBM router implements the NAS (see Figure 386 on page 374) we see that we have to perform three tasks:

1. Configuration of the physical dial-in interface
2. Configuration of a dial-in PPP circuit on that line

3. Build the layer-2 tunnel

Steps 1 and 2 have already been described in previous chapters. The configuration is not different here, except that no unnumbered IP address or proxy ARPing needs to be configured as the PPP circuit will be extended over the tunnel (see Figure 386 on page 374). For this exercise the configuration steps shown in the following sections are identical:

- 17.2.3.1, “Preparation” on page 330
- 17.2.3.2, “List configuration” on page 331
- 17.2.3.3, “Add PPP user for the dial-in workstation” on page 331

What we need to do now is to build the layer-2 tunnel. The fist step is to enable L2F and to restart/reload the router.

```
ISP *TALK 6

ISP Config>FEATURE Layer-2-Tunneling
ISP Layer-2-Tunneling Config>ENABLE L2F

 Restart system for changes to take effect.
ISP Layer-2-Tunneling Config>
ISP *RESTART
Are you sure you want to restart the gateway? (Yes or [No]): y
The configuration has been changed, save it? (Yes or [No] or Abort): y
Config Save: Using bank B and config number 3
Writing config 512K bytes
The configuration has been saved.
```

Figure 391. Enable L2F

Next is to define the layer-2 tunnel. This is achieved with the `ADD TUNNEL-PROFILE` command. Here it is important that the name of the tunnel matches the local name of the home gateway.

```
ISP Config>ADD TUNNEL-PROFILE
Enter name:  []? cisco
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP] l2f
Enter local hostname: []? 2212
Set NAS secret? (Yes, No): [No] y
NAS secret for tunnel authentication:
Enter again to verify:
Set Gateway secret? (Yes, No): [No] y
Gateway secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.212.2

       Tunnel name: cisco
          TunnType: L2F
          Endpoint: 192.168.212.2
    Local Hostname: 2212

Tunnel 'cisco' has been added
```

Figure 392. L2F tunnel profile

When a user dials in to the router with a user ID, if the form xxx@cisco is used it will recognize that the PPP dial-in circuit must go over the tunnel since the tunnel name matches the second part of the user's name (the component after the @).

This is essentially all that is required in the LNS, however, we have to configure the authentication protocol used on the PPP circuit to interoperate with the Cisco router. This is because the Cisco router uses CHAP while the IBM defaults to SPAP.

During step 2 a PPP dial-in circuit was defined with the command `ADD DEVICE DIAL-IN`. This resulted in interface 5 being generated to represent the PPP dial-in circuit (see Figure 393 on page 381). It is here we configure the authentication protocol of the dial-in PPP circuit.

```
ISP Config>NETWORK 5
Circuit configuration
ISP Dial-in Circuit config:   5>ENCAPSULATOR
Point-to-Point user configuration
SP PPP 5 Config>LIST LCP

LCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:                    10
Terminate Tries:                    10   Retry Timer:                       3000

LCP Options
-----------
Max Receive Unit:                 1522   Magic Number:                       Yes
Peer to Local (RX) ACCM:         A0000
Protocol Field Comp(PFC):           No   Addr/Cntl Field Comp(ACFC):          No


Authentication Options
----------------------
Authenticate remote using:   SPAP or CHAP or PAP   [Listed in priority order] 1
CHAP Rechallenge Interval:   0
Identify self as:            ibm
ISP PPP 5 Config>DISABLE SPAP
SPAP disabled
ISP PPP 5 Config>LIST LCP

LCP Parameters
--------------
Config Request Tries:               20   Config Nak Tries:                    10
Terminate Tries:                    10   Retry Timer:                       3000

LCP Options
-----------
Max Receive Unit:                 1522   Magic Number:                       Yes
Peer to Local (RX) ACCM:         A0000
Protocol Field Comp(PFC):           No   Addr/Cntl Field Comp(ACFC):          No


Authentication Options
----------------------
Authenticate remote using:   CHAP or PAP   [Listed in priority order] 2
CHAP Rechallenge Interval:   0
Identify self as:            ibm
ISP PPP 5 Config>
ISP *RESTART
Are you sure you want to restart the gateway? (Yes or [No]): y
The configuration has been changed, save it? (Yes or [No] or Abort): y
Config Save: Using bank B and config number 4
Writing config 512K bytes
The configuration has been saved.
```

Figure 393. Configure dial-up authentication

1 SPAP is the authentication protocol that will be used first since it has the highest priority.

2 CHAP now has the highest priority after SPAP has been disabled.

18.2.4 Definition of the central Cisco router

Complete documentation on how to configure the Cisco router can be found at the Cisco Web site http://www.cisco.com. The following will briefly describe the steps that were used to configure the Cisco router:

```
User Access Verification

Username: cisco
Password:

cisco>en
Password:
cisco#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
cisco(config)#vpdn enable 1
cisco(config)#vpdn-group 1 2
cisco(config-vpdn)#accept dialin l2f virtual-template 1 remote 2212 3
cisco(config-vpdn)#local name cisco 4
cisco(config-vpdn)#interface virtual-template 1 5
cisco(config-if)#ip unnumbered tokenring0/0 6
cisco(config-if)#ppp authentication chap 7
cisco(config-if)#peer default ip address pool default 8
cisco(config-if)#encapsulation ppp 9
cisco(config)#ip local pool default 192.168.103.50 192.168.103.100 10
cisco(config)#aaa new-model 11
cisco(config)#aaa authentication login default local 12
cisco(config)#aaa authentication ppp default local 13
cisco(config)#aaa authorization network default local 14
cisco(config)#username l2fuser@cisco password secret 15
cisco(config)#username cisco password secret 16
cisco(config)#username 2212 password secret 17
cisco(config)#^Z
```

Figure 394. Cisco L2F and dial-up configuration

The configuration steps above have the equivalent operations on the IBM routers. The explanation of the commands above will refer to the equivalent IBM router commands and Figure 387 on page 375, which describes the IBM router's implementation of the home gateway.

The commands which define the layer-2 tunnel and are equivalent to the IBM router's ADD TUNNEL-PROFILE are:

1 Enable the VPN features of the router.

2, 3 Define the VPN tunnel to allow termination from the IBM 2212.

4 Define the local name.

16, 17 Define the passwords to authenticate the tunnel.

The commands that define the virtual interface and are equivalent to the IBM router's command ADD DEVICE LAYER-2-TUNNELING are:

5 Create a virtual PPP interface.

6 Define an unnumbered IP address on the virtual interface and define it to use the token-ring interface.

7 Set the authentication protocol.

8 Define that the IP address for the client will be allocated from the default pool.

9 Define that it will be an encapsulated virtual interface.

The command at 15 defines the PPP user and is equivalent to the IBM router's command ADD PPP-USER.

Note that the PPP user is getting its IP address from a default pool as defined in 10. This is done on the IBM router by the FEATURE DIALs command. Notice also that proxy ARP is not explicitly configured; rather it is automatically done through the definition of the virtual PPP interface.

Commands 11, 12, 13 and 14 ensure that the local database is used for authentication.

Use the command show running to confirm your configuration.

Note

The screen output below does not show the full display of the show running command. Rather it only shows those sections that are relevant to this example.

```
cisco#show running
Building configuration...

Current configuration:
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authorization network default local
enable secret 5 $1$q8fW$b9EG9vl7HpMkZKXp7zucG/
enable password telnet
!
username wsvpn@2212 password 0 wsvpn
username 2212 password 0 secret
username cisco password 0 secret
username l2fuser@cisco password 0 secret
memory-size iomem 20
ip subnet-zero
!
vpdn enable
!
vpdn-group 1
 accept dialin l2f virtual-template 1 remote 2212
 local name cisco
 l2f ignore-mid-sequence
!
vpdn-group 2
 accept dialin l2f virtual-template 0
!
!
!
interface TokenRing0/0
 ip address 192.168.103.1 255.255.255.0
 no ip directed-broadcast
 ring-speed 16
!
interface Virtual-Template1
 ip unnumbered TokenRing0/0
 no ip directed-broadcast
 peer default ip address pool default
 ppp authentication chap
!
ip local pool default 192.168.103.40 192.168.103.45
ip local pool default 192.168.103.50 192.168.103.100
ip default-gateway 192.168.212.1
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.212.1
ip route 192.168.88.0 255.255.255.0 192.168.103.2
ip http server
!
end
```

Figure 395. Display Cisco configuration

18.2.5 Connecting the workstation

There are no special requirements for the definition of the workstation. It simply connects to the ISP router (in this example, the IBM 2212) using a standard PPP dial-up configuration. The user simply needs to use a user ID in the form of xxx@cisco. In our example, the user is defined as l2fuser@cisco. When the user logs in with the user ID, the IBM 2212 will start the authentication process with a CHAP challenge. The user will respond and the IBM 2212 will then make a tunnel to the Cisco router and forward the CHAP response to it to be authenticated. The Cisco router will send back a CHAP success or failure to the user.

If successful, the user will then be allocated an IP address on the corporate network from the pool of available IP addresses.

18.3 Using Layer 2 Tunneling Protocol (L2TP)

L2TP has not changed from MRS/MAS Versions 3.1/3.2. Refer to Chapter 30, “Connecting dial-in remote users” on page 541 on how to configure L2TP.

Chapter 19. Connecting dial-up routers with L2TP

As the other VPN remote access solution, IBM router supports initiating an L2TP tunnel that is terminated at a remote peer. Additionally IBM router supports a dynamic IP address for a router interface in CC5. By using these features, in this chapter we describe the scenario for the small branch offices that do not have a leased line Internet connection but have a requirement to communicate with a company's central site for several hours a day. The company might support several LAN users to connect central site's resources with one dial user ID from ISP while keeping its costs low.

19.1 Scenario descriptions

In this scenario, we demonstrate how to use the IBM Nways routers as LAC and LNS for a voluntary L2TP tunnel to secure the traffic from LAN users in the branch who want to connect to the corporate network by way of the Internet without a leased line connection. Figure 396 shows the network diagram for this scenario. We assume Ethernet between ISP's NAS 2212 and 2216 center as an Internet-leased line connection.

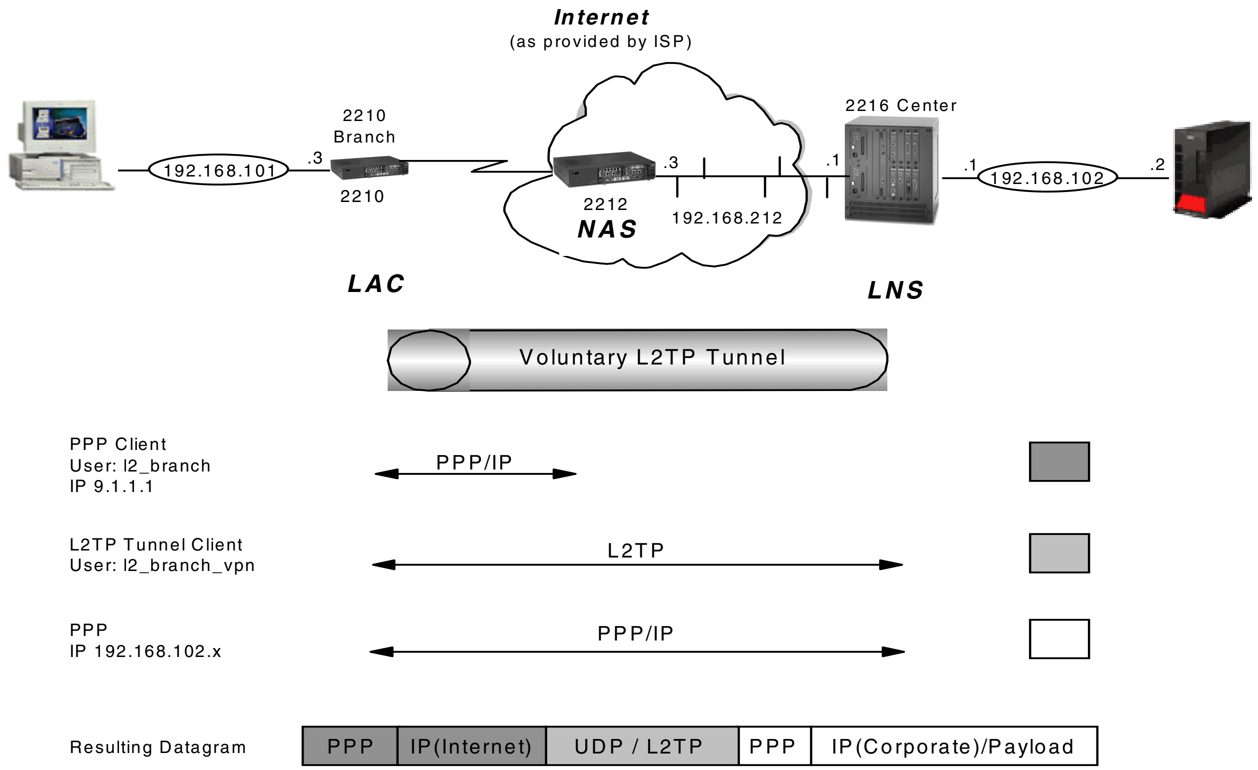


Figure 396. Sample network for L2TP connection

In this scenario we use 2210 for the branch router, 2212 for ISP's router and 2216 for the central site router. Branch router 2210 makes a first call to 2212 ISP's router when the IP host in the branch (subnetwork 192.168.103.0) sends IP packets to the WAN. An L2TP tunnel would be established using a second virtual call only if a device on the 192.168.103.0 branch network had data to send to the home LAN of 192.168.102.0. The router will be configured with a static route that says any traffic for the network 192.168.102.0 should be routed through the virtual interface. When data is received on the interface, the router will establish an L2TP tunnel. The router looks at the L2Net and tunnel definition to locate the IP address of the L2TP peer, namely 192.168.212.1. The router will establish a TCP connection to this address using the NAS. After the 2216 center router has accepted the L2TP connection, the branch router will negotiate the PPP parameters for its L2Net. The 2216 center router will return an IP address from a pool of addresses configured for that L2TP interface. The IP address has to be in the same subnet as the LAN interface of the 2216 center router. The L2Net must be configured to receive its IP address using IPCP - a new feature in V3.3 of the router code. Since IP address 9.1.1.1 from ISP is changed whenever you log on to ISP, we create a tunnel by using a token-ring interface (that is an interface to a branch LAN) IP address of the 2210 router in the branch as a tunnel endpoint.

Once an L2TP tunnel is established, the Internet is transparent to the users at the branch and central site. Therefore, it appears as if the 192.168.102.0 and 192.168.103.0 are directly attached to the L2Net as shown in Figure 397:

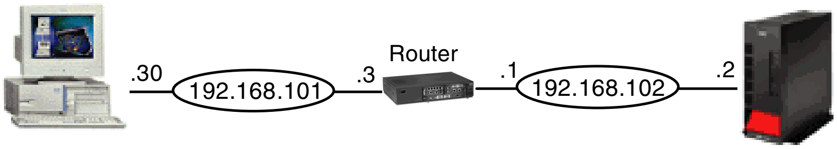


Figure 397. Appearance of network to branch and central site users

19.2 Configuring dial-up router

In this part, we configure both an ISP (2212) and client (2210) router without considering L2TP. The PPP interface can obtain its IP address by IPCP from the ISP router. We will configure L2TP over this dial-up connection in the next section. In the next part of this scenario, we extend router dial-up sessions to the corporate central site over an IP network such as the Internet by using L2TP to tunnel the PPP session from the branch office 2210 to the central site 2216.

19.2.1 Configuring a branch router as an ISP dial-up client

We start by adding a configuration to the 2210 that allows 2210 to be a dial-up client using a V.34 dial-up modem for branch LAN users.

Note: In our scenario, we demonstrate the use of V.34 for the remote access to ISP. However, the 2210 supports V.34, ISDN BRI and V.25bis. V.34 is supported using external modems connected to WAN ports or using the 4- or 8-port dial access adapters that provide integrated V.34 modems.

For the configuration of the 2210 branch router we perform the following steps:

- Preparation.
- Add a dial circuit interface.
- Enable IP on a dial circuit interface.
- Set call destination.
- Set IPCP.

19.2.1.1 Preparation

Configuring the router physical interface and IP address of the token-ring interface is required.

19.2.1.2 Adding dial circuit interface

First we add the dial circuit for the V.34 WAN interface as shown in Figure 398:

```
l2_branch Config>ADD DEVICE DIAL-CIRCUIT
Base net for the circuit(s) [0]? 1
Enter the number of PPP Dial Circuit interfaces [1]?
Adding device as interface 7
Defaulting Data-link protocol to PPP
Add more dial circuit interface(s)?(Yes or [No]):
Use "net <intf #>" command to configure circuit parameters
```

Figure 398. Adding device dial circuit

19.2.1.3 Configuring IP

In the IP configuration, you should configure an unnumbered IP address on the dial interface. Unnumbered addresses always have the format 0.0.0.x where x is the interface number.

The next step is to enable a dynamic address and the router asks you for the IP address. When the real IP address is retrieved, all references to 0.0.0.6 will be updated with the real IP address.

We also need the `Enable ARP-subnet-routing` command. ARP subnet routing must be enabled to allow the router to respond to ARPs when the next hop to the destination is over a different interface from the interface that is receiving the ARP request. In our case the router interface is logically on the corporate LAN subnet but physically on a different (V.34) interface.

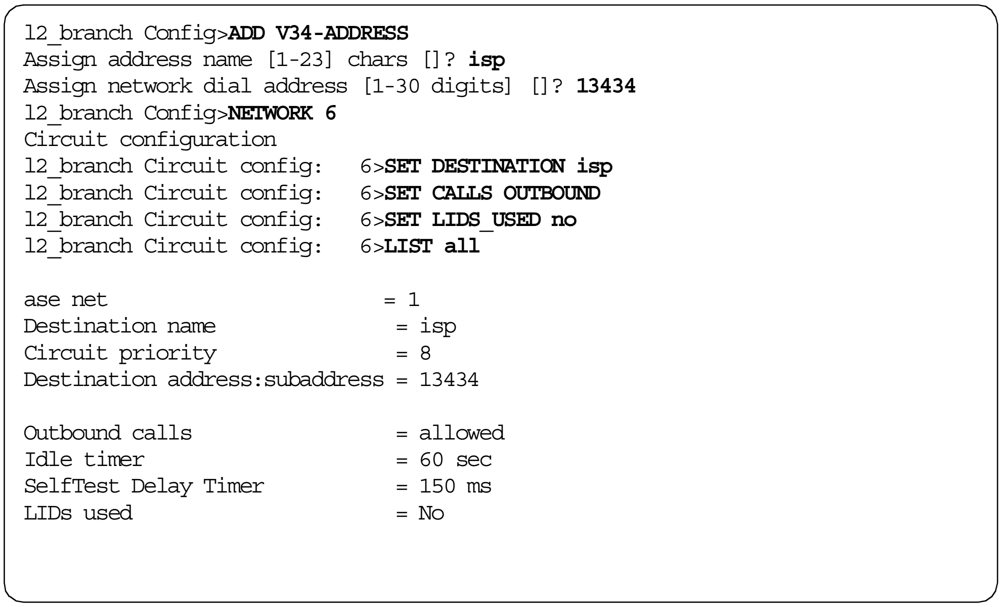
Finally, define the unnumbered dial interface 0.0.0.6 as a default route. Figure 399 shows the commands for IP configuration explained above.

```
l2_branch IP config>ADD ADDRESS 6 0.0.0.6 255.255.255.255
l2_branch IP config>ENABLE DYNAMIC-ADDRESS
Interface address []? 0.0.0.6
l2_branch IP config>ENABLE ARP-SUBNET-ROUTING
l2_branch IP config>ADD ROUTE 0.0.0.0 0.0.0.0 0.0.0.6
Cost [1]?
```

Figure 399. Configuring IP on dial interface

19.2.1.4 Setting call destination

The next step is configuring an ISP phone number and call characteristics as shown in Figure 400.



```
l2_branch Config>ADD V34-ADDRESS
Assign address name [1-23] chars []? isp
Assign network dial address [1-30 digits] []? 13434
l2_branch Config>NETWORK 6
Circuit configuration
l2_branch Circuit config:   6>SET DESTINATION isp
l2_branch Circuit config:   6>SET CALLS OUTBOUND
l2_branch Circuit config:   6>SET LIDS_USED no
l2_branch Circuit config:   6>LIST all

ase net                     = 1
Destination name             = isp
Circuit priority             = 8
Destination address:subaddress = 13434

Outbound calls               = allowed
Idle timer                   = 60 sec
SelfTest Delay Timer         = 150 ms
LIDs used                    = No
```

Figure 400. Setting call destination

Assign the remote NAS name and phone number as isp and 13434. Set the call direction as outbound so that 2210 makes an outbound call to ISP NAS. Configure the line ID not to be used since we are configuring only one circuit.

Note

When more than one circuit is configured between two routers (parallel circuits), then there needs to be a way to unambiguously know which dial circuit connects between them. For this purpose, a line ID is sent from the router at one end (the caller). At the receiving end the other router configures the same string as the inbound destination name.

19.2.1.5 Setting IPCP

Figure 401 shows that the PPP interface has been configured to request its peer for an IP address. We added dial circuit interface 6 for the V.34 WAN interface 1 in 19.2.1.2, “Adding dial circuit interface” on page 389. We should configure IPCP for this dial circuit interface 6 to get the IP address from ISP. IPCP is configured with the `set IPCP` command in Network 6, Encapsulator. 2210 in branch could receive an address through setting "yes" for question **1** in Figure 401. Next we define the local name l2_branch and password which will be authenticated by ISP NAS. Finally, set the MTU size on the PPP link through the `set LCP options` command.

```
l2_branch Config>NETWORK 6
l2_branch Circuit config:   6>ENCAPSULATOR
Point-to-Point user configuration
l2_branch PPP 6 Config>SET IPCP
IP COMPRESSION [no]:
Request an IP address [no]: y 1
Interface remote IP address to offer if requested (0.0.0.0 for none)
[0.0.0.0]?
l2_branch PPP 6 Config>SET NAME
Enter Local Name:  []? l2_branch
Password:
Enter password again:
PPP Local Name = l2_branch
l2_branch PPP 6 Config>SET LCP OPTIONS
Maximum Receive Unit (bytes) [2044]? 1500
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000]?
Protocol Field Compression(PFC) [no]:
Addr/Cntl Field Compression(ACFC) [no]:
l2_branch PPP 6 Config>EXIT
l2_branch Circuit config:   6>EXIT
l2_branch Config>res
```

Figure 401. Setting IPCP

19.2.2 Configuring ISP’s router as an NAS

Now we configure the NAS 2212 to accept the call from the 2210, give the 2210 the IP address and route the IP traffic.

For the configuration of the 2210 branch router we perform the following steps:

- Preparation.
- Enable IP on dial circuit interface.
- Add PPP-user.
- Set IPCP.

19.2.2.1 Preparation

Configuring a router physical interface and IP address of the Internet side interface is required. Since we use the same 2212 router from Chapter 17, “Connecting remote users with voluntary tunneling” on page 317 to Chapter 19, “Connecting dial-up routers with L2TP” on page 387, refer to 17.2.3.1, “Preparation” on page 330 for configuring the V.34 interface and adding dial-in interface.

19.2.2.2 Configuring IP

Next we configure the IP protocol for a dial-in interface. This step is also the same in 17.2.3.4, “Add IP address” on page 332.

19.2.2.3 Adding PPP user

Now we configure the PPP user for the 2210 branch router as shown in Figure 402. Since we will give the IP address 2210 branch router through IPCP, we set the IP address in 1 as 0.0.0.0.

```
ISP Config>add ppp-user
Enter name:  []? l2_branch
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 1
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

   PPP user name: l2_branch
   User IP address: Interface Default
   Netroute Mask: 255.255.255.255
   Hostname: <undefined>
   Virtual Conn: disabled
   Time alotted: Box Default
   Callback type: disabled
   Dial-out: disabled
   Encryption: disabled
   Status: enabled
   Account Expiry: <unlimited>
   Password Expiry: <unlimited>

Is information correct? (Yes, No, Quit): [Yes]
```

Figure 402. Adding PPP user for 2210

19.2.2.4 Setting IPCP

Finally, we set the IPCP to give the IP address to the 2210 branch router as shown in Figure 403. Network 5 is a dial-in interface as shown from `the list device` command. Assign it an IP address or create an IP pool. In this part we assign the IP address in IPCP directly and we will assign an IP address from the IP pool when we assign the IP address after establishing L2TP in 19.3.2.5, “Adding IP-pool” on page 398.

```
ISP Config>list dev
Ifc 0     V.34 Base Net
Ifc 1     WAN PPP
(Disabled)
Ifc 2     WAN PPP
Ifc 3     WAN PPP
Ifc 4     2-port IBM Token Ring             Slot: 1      Port: 1
Ifc 5     PPP Dial-in Circuit
Ifc 6     2-port 10/100 Ethernet            Slot: 2      Port: 1
ISP Config>net 5
Circuit configuration
ISP Dial-in Circuit config:   5>enc
Point-to-Point user configuration
ISP PPP 5 Config>set ipcp
IP COMPRESSION [no]:
Request an IP address [no]:
Send our IP address [no]: y
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0.0.0.0 for none)
[0.0.0.0]? 9.1.1.1
ISP PPP 5 Config>exit
ISP Dial-in Circuit config:   5>exit
```

Figure 403. Setting IPCP

19.3 Configuring L2TP

Until now we have defined a dial-on-demand router to get a switched connection to the Internet that is active only when it is needed. After connection with ISP we receive 9.1.1.1 public address from ISP. Therefore, the user in the branch could ping to the 192.168.212.0 network which is the Internet side interface of the 2216 in the center. But the user in the branch could not reach the central site network 192.168.102.0 before the L2TP connection. After checking the PPP connection working correctly, we configure L2TP in this part.

19.3.1 Configuring a branch router as an L2TP LAC

The 2210 in the branch will be configured as a LAC for initiating the L2TP voluntary tunnel in this part. This L2TP tunnel is only up when there is a request to send IP packets on the host in a central site network through the 2210.

For the configuration of the 2210 in the branch we have to perform the following steps:

- Enable L2TP.
- Add L2TP tunnel.
- Add L2Net as a VPN virtual interface.
- Configure the virtual interface.
- Configure the IP route entry.

19.3.1.1 Enabling L2TP

First of all we enable the L2TP in feature layer-2 tunneling as shown in Figure 404.

```
l2_branch Config>FEATURE Layer-2-Tunneling
l2_branch Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
```

Figure 404. Enabling L2TP

19.3.1.2 Adding L2TP tunnel

The next step is to define the L2TP tunnel endpoint. The `add tunnel` command in feature layer-2 tunneling is used to define the tunnel. The name we are prompted for in **1** is the name of the remote L2TP - this name should be matched with what is configured on the 2216 in the central site as a local name. You are asked for the tunnel server endpoint address - this is in the address of the 2216 in the central site which is reachable using the IP cloud. After the definition we view the tunnel created now by using the `list tunnel-profiles` command.

```
l2_branch Config>ADD TUNNEL-PROFILE
Enter name:  []? center 1
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? l2_branch
set shared secret? (Yes, No): [No] y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.212.1

       Tunnel name: center
          TunnType: L2TP
          Endpoint: 192.168.212.1
    Local Hostname: l2_branch

Tunnel 'center' has been added
l2_branch Config>LIST TUNNEL-PROFILES
TunnType  Endpoint         Tunnel name                    Hostname
L2TP      192.168.212.1    center                       l2_branch
1 TUNNEL record displayed.
```

Figure 405. Adding L2TP tunnel

19.3.1.3 Adding L2Net to initiate voluntary layer-2 tunnel

The next step is to create the interface that will initiate the L2TP voluntary connection. This is known as L2Net. L2Nets can be added from the layer-2-tunneling feature as shown below in Figure 406, or from the `Config>` prompt using the `add device layer` command.

Adding the L2Net creates several interfaces. An unnumbered IP address will be given automatically by way of **1** Note that PPTP, L2TP and L2F tunneled PPP sessions will use the same pool of L2Nets.

```
l2_branch Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]: 1
Adding device as interface 7
Defaulting Data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
```

Figure 406. Adding L2Net as a VPN virtual interface

Note

L2Net should be added in the following cases:

- Initiating voluntary tunnel in LAC
- Terminating voluntary and compulsory tunnel in LNS

Therefore, the compulsory tunnel does not use L2Net in LAC.

19.3.1.4 Configure virtual interface

The next step is to tie our virtual interface to the peer called *center*. By default all L2Nets are inbound from any device. This must be changed to outbound and then you are prompted for the name of the remote device. This means that when traffic is routed to our virtual interface, interface 7, it will know that it has to establish a tunnel to a peer called *center*. It looks at the *center* tunnel definition and discovers that it is an L2TP tunnel to 192.168.212.1. The router will look in its routing table to determine how to get to that address - which in this example will be by way of 0.0.0.6. Clearly the router needs to be configured, either by way of static routing or a dynamic routing protocol to know how to get to 192.168.212.1. We achieve this through configuring the default gateway in 19.2.1.3, “Configuring IP” on page 389.

The 2216 in central site will probably wish to authenticate the remote router, so a user ID and password need to be configured on the L2Net. When an L2Net is changed from inbound to outbound, you can configure the PPP defaults on that L2Net. You can get to the PPP configuration prompt by using the `encapsulator` command. The router is configured to send *l2_branch_vpn* when prompted. We want this L2Net to receive its IP address from the 2216 in central site. This will be sent during the IPCP negotiations and we need to configure the router to ask the 2216 for its IP address. This is done using the `set ipcp` command and answering *yes* to request an IP address.

```
l2_branch Config>NETWORK 7
Session configuration
l2_branch L2T config:   7>SET CONNECTION-DIRECTION OUTBOUND
Enter remote tunnel hostname:  []? center
l2_branch L2T config:   7>ENCAPSULATOR
Point-to-Point user configuration
l2_branch PPP 7 Config>SET NAME
Enter Local Name:  []? l2_branch_vpn
Password:
Enter password again:
PPP Local Name = l2_branch
l2_branch PPP 7 Config>SET IPCP
IP COMPRESSION [no]:
Request an IP address [no]: yes
Interface remote IP address to offer if requested (0.0.0.0 for none)
[0.0.0.0]?
```

Figure 407. Configuring virtual interface

19.3.1.5 Configuring IP route

Finally the branch network needs to know how to route to the home network 192.168.102.0, so a routing entry using the L2Net 0.0.0.7 has been added.This routing entry indicates the packets to 192.168.102.0 should use L2TP tunnel.

```
l2_branch Config>PROTOCOL IP
l2_branch IP config>ADD ROUTE
IP destination []? 192.168.102.0
Address mask [255.255.255.0]?
Via gateway 1 at []? 0.0.0.7
Cost [1]?
Via gateway 2 at []?
l2_branch IP config>EXIT
```

Figure 408. Configuring IP

19.3.2 Configuring center router as an L2TP LNS

The 2216 in central site will be configured as an LNS in this part.

For the configuration of the 2210 in the branch we have to perform the following steps:

- Enable L2TP.
- Add the L2TP tunnel.
- Add L2Net to terminate the VPN tunnel.
- Configure the virtual interface.
- Configure the IP route to the branch.
- Add the PPP-user for the 2210 branch router’s L2TP dial-in.

19.3.2.1 Enabling L2TP

First of all we enable the L2TP in feature layer-2-tunneling as shown in Figure 409.

```
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
```

Figure 409. Enabling L2TP

19.3.2.2 Adding L2TP tunnel

The next step is to define the L2TP tunnel endpoint. The `add tunnel` command in feature layer-2 tunneling is used to define the tunnel. The name we are prompted for in **1** is the name of the remote L2TP - this name should be matched with what is configured on the 2210 in the branch as a local name. We are asked for the tunnel server endpoint address. This is in the address of the 2210 LAN interface in central site which is the fixed IP address given by corporate.

Note: We recommend not to use the dial interface IP address to the Internet as a tunnel endpoint because it is always changing. If the branch office uses a private IP address you should implement NAT in your branch router to hide the private IP address.

```
Center Config>ADD TUNNEL-PROFILE
Enter name:  []? l2_branch 1
l2_branch is already configured as a PPP profile.
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? center
set shared secret? (Yes, No): [No] y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.103.3
    Tunnel name: l2_branch
    TunnType: L2TP
    Endpoint: 192.168.103.3
    Local Hostname: center
Tunnel 'l2_branch' has been added
```

Figure 410. Adding L2TP tunnel

19.3.2.3 Add L2Net to terminate VPN tunnel in LNS

The next step is to create the interface that will terminate the L2TP voluntary connection. Adding the L2Net creates several interfaces. An unnumbered IP address will be given automatically using **1** as a 0.0.0.10.

```
Center Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]: 1
Adding device as interface 10
Defaulting data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.
Restart router for changes to take affect.
Center Layer-2-Tunneling Config>EXIT
```

Figure 411. Adding L2Net for VPN virtual interface

19.3.2.4 Configure the virtual interface

The next step is configuring L2Net interface 10 as shown in Figure 412. We set the connection direction as an inbound to receive the VPN call. Now we set IPCP to give the IP address to the 2210 in the branch. At this time, we set the 0.0.0.0 IP address for 1 since we use the IP pool which will be defined in 19.3.2.5, “Adding IP-pool” on page 398.

```
Center Config>NETWORK 10
Session configuration
Center L2T config:  10>SET CONNECTION-DIRECTION INBOUND
Point-to-Point user configuration
Center L2T config:   7>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>SET IPCP
IP COMPRESSION [no]:
Request an IP address [no]:
Send our IP address [yes]:
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0.0.0.0 for none)
[0.0.0.0]? 1
Center PPP-L2T Config>EXIT
```

Figure 412. Configuring the virtual interface

When you want to define IPCP or other parameters in encapsulator for all L2Nets as the same value, set the value from the following prompt:

```
Center Config>FEATURE Layer-2-Tunneling
Center Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>SET IPCP
```

Figure 413. IPCP definition for all L2Nets

In another case, define IPCP or other encapsulator parameters for individual L2Net as a specific value, and set the value from the following prompt:

```
Center Config>NETWORK 10
Session configuration
Center L2T config:   7>ENCAPSULATOR
Point-to-Point user configuration
Center PPP-L2T Config>SET IPCP
```

Figure 414. IPCP definition for specific L2Net

19.3.2.5 Adding IP-pool

Now we add the IP-pool for IPCP IP address requestors in Figure 415, therefore, 2210 in the branch will receive one of the IP addresses between 192.168.102.11 and 192.168.102.14 in the IP-pool. The IP address should be on the same LAN subnet of the router interface to which it wishes to connect.

```
Center Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Center DIALs config>ADD IP-POOL
Base address []? 192.168.102.11
Number of addresses [1]? 4
Center DIALs config>EXIT
```

Figure 415. Adding IP-pool

19.3.2.6 Configuring IP route to branch

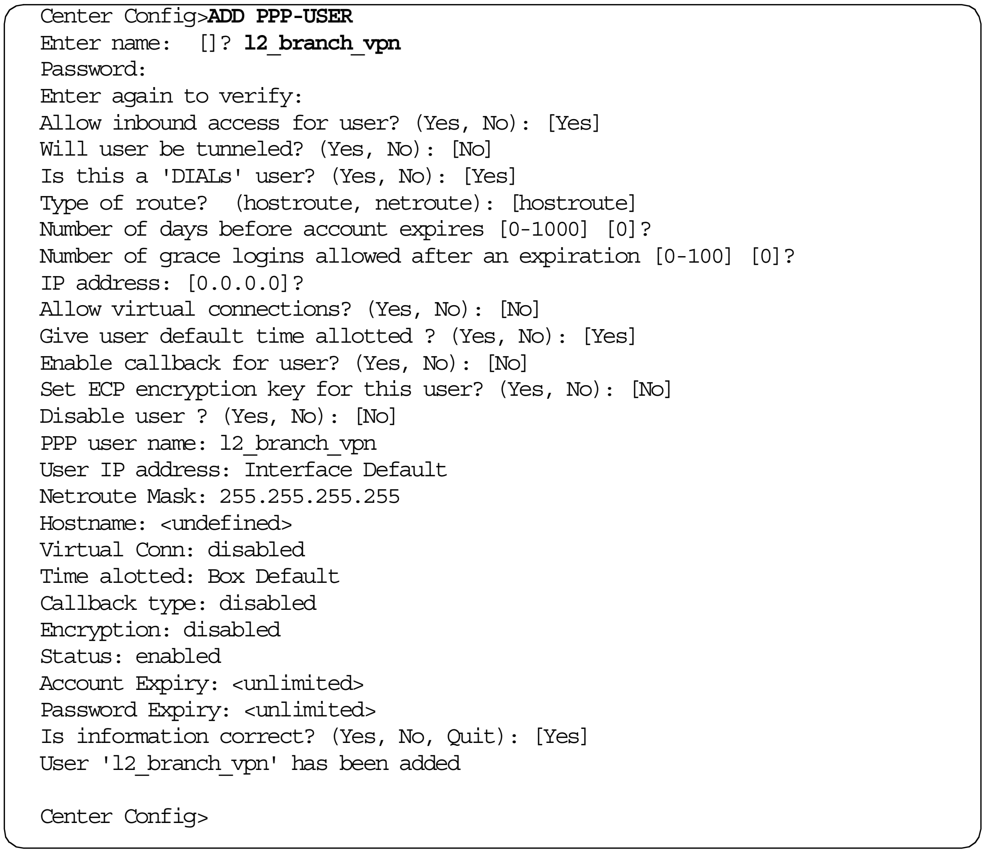
Now we define the routing entry to reach branch network 192.168.103.0 through L2Net virtual interface 0.0.0.10.

```
Center IP config>ADD ROUTE
IP destination []? 192.168.103.0
Address mask [255.255.255.0]? 255.255.255.0
Via gateway 1 at []? 0.0.0.10
Cost [1]?
Via gateway 2 at []?
```

Figure 416. Configuring IP on virtual interface

19.3.2.7 Adding PPP user for 2210 branch router’s L2TP dial-in

Configure the user name as l2_branch_vpn that was defined in the 2210 branch router to identify itself with the `set name` command in 19.3.1.4, “Configure virtual interface” on page 395.

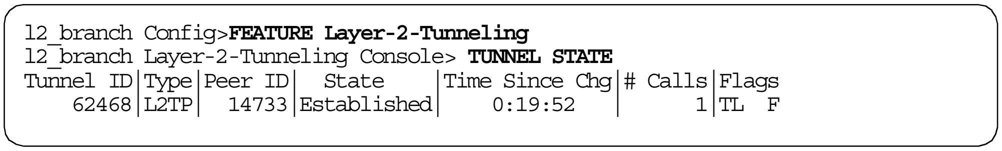


```
Center Config>ADD PPP-USER
Enter name:  []? l2_branch_vpn
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]
PPP user name: l2_branch_vpn
User IP address: Interface Default
Netroute Mask: 255.255.255.255
Hostname: <undefined>
Virtual Conn: disabled
Time alotted: Box Default
Callback type: disabled
Encryption: disabled
Status: enabled
Account Expiry: <unlimited>
Password Expiry: <unlimited>
Is information correct? (Yes, No, Quit): [Yes]
User 'l2_branch_vpn' has been added

Center Config>
```

Figure 417. Adding PPP user

19.4 Monitoring L2TP tunnel

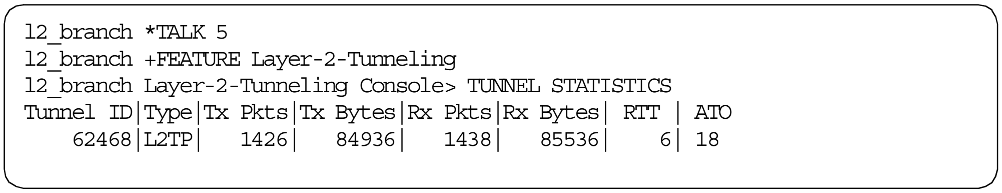
We check the tunnel status from talk 6, feature layer-2-tunneling.



```
l2_branch Config>FEATURE Layer-2-Tunneling
l2_branch Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID|Type|Peer ID|  State     |Time Since Chg|# Calls|Flags
    62468|L2TP|  14733|Established|    0:19:52    |      1|TL  F
```

Figure 418. Viewing tunnel state

We could check how much traffic went through the layer-2 tunnel using the `talk 5, feature layer-2-tunneling, tunnel statistics` commands as shown in Figure 419:



```
l2_branch *TALK 5
l2_branch +FEATURE Layer-2-Tunneling
l2_branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID|Type|Tx Pkts|Tx Bytes|Rx Pkts|Rx Bytes| RTT | ATO
    62468|L2TP|   1426|   84936|   1438|   85536|    6| 18
```

Figure 419. Viewing tunnel statistics

To monitor Event Logging System (ELS) messages you can enable event logging either under talk 5 (for dynamic viewing) or under talk 6 (for permanent viewing). If using talk 6, Event, you must restart the Router to take effect. Monitor the L2F Tunnel from talk 2 ELS using display subsystem 12 all. A sample talk 2 session from the 221x GW is shown in Figure 420:

```
13:30:19   L2.014: Start Tunnel/Call from net 7
13:30:19   L2.052: Tunnel 10158/0 has 15 seconds to establish itself
13:30:19   L2.073: Rhelm Originate Tunnel to peer tocenter
13:30:19   L2.074: Upcall from AAA subsystem, request SUCCESS
13:30:19   L2.054: Assigning tunnel peer 192.168.212.1, tid=10158/0
13:30:19   L2.050: EVENT Open-Request,tid=10158/0,state=Idle
13:30:19   L2.049: SEND SCCRQ, tid=10158/0
13:30:19   L2.035: Tunnel Auth Create Challenge, Tid=10158/0, Len=16
13:30:19   L2.044: Allocating UDP port 1026 for tunnelid=10158
13:30:19   L2.041: SND L2TP:F=C802,L=101,Tid=0,Cid=0,NS=0,NR=0,O=0
13:30:19   L2.047: Tunnel 10158/0 State Changed Idle -> Wait-ctl-rep
13:30:19   L2.040: RCV L2TP:F=C800,L=122,Tid=10158,Cid=0,NS=0,NR=1,O=0
13:30:19   L2.050: EVENT Rx-SCCRP,tid=10158/0,state=Wait-ctl-rep
13:30:19   L2.048: RCV l2tpGetHostname, tid=10158/0
13:30:19   L2.058: Peer TunnelID = 23272
13:30:19   L2.060: Peer Hostname = tocenter
13:30:19   L2.047: Tunnel 10158/23272 State Changed Wait-ctl-rep -> Authorizing
13:30:19   L2.074: Upcall from AAA subsystem, request SUCCESS
13:30:19   L2.050: EVENT Continue-SCCRP,tid=10158/23272,state=Authorizing
13:30:19   L2.048: RCV SCCRP, tid=10158/23272
13:30:19   L2.059: Peer Framing Capabilities = 3
13:30:19   L2.059: Peer Bearer Capabilities = 3
13:30:19   L2.058: Peer TunnelID = 23272
13:30:19   L2.058: Peer Rcv Window = 4
13:30:19   L2.060: Peer Hostname = tocenter
13:30:19   L2.057: Processing Challenge Response from Peer 4.8.3.3
13:30:19   L2.039: NOTE:SCCRP: Tunnel Authenticated
13:30:19   L2.049: SEND SCCCN, tid=10158/23272
13:30:19   L2.035: Tunnel Auth Create Challenge Response, Tid=10158/23272, Len=16
13:30:19   L2.041: SND L2TP:F=C802,L=42,Tid=23272,Cid=0,NS=1,NR=1,O=0
13:30:19   L2.047: Tunnel 10158/23272 State Changed Authorizing -> Established
13:30:19   L2.010: Start Call LAC net 7,speed=0,btype=1,frame=1,auth=4
13:30:19   L2.008: Call Make Msg Type AVP,attr=0,val=A,len=8,flag=8000
13:30:19   L2.008: Call Make Call Id AVP,attr=14,val=68A7,len=8,flag=8000
13:30:19   L2.008: Call Make Call SN AVP,attr=15,val=0,len=10,flag=8000
13:30:19   L2.008: Call Make Bearer Type AVP,attr=18,val=1,len=10,flag=8000
13:30:19   L2.021: SEND Inbound-Call-Request, callid=26791, net=7
13:30:19   L2.041: SND L2TP:F=C802,L=48,Tid=23272,Cid=0,NS=2,NR=1,O=0
13:30:19   L2.013: L2TP Call 26791 State Changed Idle -> Wait Reply
13:30:19   L2.040: RCV L2TP:F=C800,L=12,Tid=10158,Cid=0,NS=1,NR=2,O=0
13:30:19   L2.043: RCV CTRL Zero Len Body (ZLB), tid=10158,cid=0
13:30:19   L2.040: RCV L2TP:F=C800,L=36,Tid=10158,Cid=26791,NS=1,NR=3,O=0
13:30:19   L2.020: RCV Inbound-Call-Reply, callid=26791, net=7
13:30:19   L2.009: Call Rcv Call Id AVP,attr=14,val=5A13,len=8,flag=8008
13:30:19   L2.009: Call Rcv Pkt Proc Delay AVP,attr=20,val=5,len=8,flag=8008
13:30:19   L2.008: Call Make Msg Type AVP,attr=0,val=C,len=8,flag=8000
13:30:19   L2.008: Call Make Framimg Type AVP,attr=19,val=1,len=10,flag=8000
13:30:19   L2.008: Call Make Pkt Proc. Delay AVP,attr=20,val=0,len=8,flag=8000
13:30:19   L2.008: Call Make Connect Speed AVP,attr=24,val=0,len=10,flag=8000
13:30:19   L2.008: Call Make Proxy-Auth-Type AVP,attr=29,val=4,len=8,flag=8000
13:30:19   L2.008: Call Make SEQUENCING_REQUIRED AVP,attr=39,val=0,len=6,flag=8000
```

Figure 420. ELS log message 1/2

```
13:30:19   L2.021: SEND Inbound-Call-Connected, callid=26791, net=7
13:30:19   L2.041: SND L2TP:F=C802,L=62,Tid=23272,Cid=23059,NS=3,NR=2,O=0
13:30:19   L2.013: L2TP Call 26791 State Changed Wait Reply -> Established
13:30:19   L2.002: WARNING:Peer did not pass its Pkt Processing Delay!
13:30:19   L2.015: Call Established-LNS,net=7,speed=0,flags=4802
13:30:19   L2.006: LCP start net 7 cause=no proxy-LCP
13:30:19   L2.024: L2TP PAYLOAD SEND 18 bytes, net=7, callid=26791
13:30:19   L2.039: NOTE:CALL - no outbound queueing necessary
13:30:19   L2.041: SND L2TP:F=4902,L=30,Tid=23272,Cid=23059,NS=0,NR=0,O=0
13:30:19   L2.040: RCV L2TP:F=4900,L=30,Tid=10158,Cid=26791,NS=0,NR=0,O=0
13:30:19   L2.022: L2TP PAYLOAD RCVD 18 bytes, net 7, callid=26791
13:30:19   L2.024: L2TP PAYLOAD SEND 18 bytes, net=7, callid=26791
13:30:19   L2.039: NOTE:CALL - no outbound queueing necessary
13:30:19   L2.041: SND L2TP:F=4902,L=30,Tid=23272,Cid=23059,NS=1,NR=1,O=0
13:30:19   L2.040: RCV L2TP:F=C800,L=12,Tid=10158,Cid=0,NS=2,NR=4,O=0
13:30:19   L2.043: RCV CTRL Zero Len Body (ZLB), tid=10158,cid=0
13:30:19   L2.040: RCV L2TP:F=4900,L=30,Tid=10158,Cid=26791,NS=1,NR=1,O=0
13:30:19   L2.022: L2TP PAYLOAD RCVD 18 bytes, net 7, callid=26791
13:30:19   L2.024: L2TP PAYLOAD SEND 26 bytes, net=7, callid=26791
13:30:19   L2.039: NOTE:CALL - no outbound queueing necessary
13:30:19   L2.041: SND L2TP:F=4902,L=38,Tid=23272,Cid=23059,NS=2,NR=2,O=0
13:30:19   L2.040: RCV L2TP:F=4900,L=20,Tid=10158,Cid=26791,NS=2,NR=2,O=0
13:30:19   L2.022: L2TP PAYLOAD RCVD 8 bytes, net 7, callid=26791
13:30:19   L2.024: L2TP PAYLOAD SEND 8 bytes, net=7, callid=26791
```

Figure 421. ELS log message 2/2

Chapter 20. Connecting remote users with IPSec dial-up

In previous chapters we described how remote access VPNs can be established using various kinds of layer-2 tunneling protocols, some of which have been secured using IPSec. It is, of course, also possible to facilitate remote access VPNs based entirely on traditional PPP dial-up combined with IPSec tunnels and IKE authentication.

There are, however, significant differences between this scenario and using layer-2 tunneling:

1. IPSec dial-up does not support multiprotocol traffic.
2. The remote client has access to the Internet and the corporate network at the same time, which can pose a security exposure.
3. IPSec dial-up allows packets with external IP addresses on the corporate network. It depends on the placement of the VPN gateway relative to the corporate firewall as to how the security policy must be defined in order to allow this.
4. Because the remote client in this case is using an ISP-assigned IP address, return routes from the corporate network to the client may or may not be available depending on how many exit paths exist from the corporate network back to the Internet.

As an option to overcome issues 3 and 4 described above, a remote access client could employ a virtual IP address assigned from within the corporate network address range and emulate a branch office.

20.1 Description of the scenario

To implement remote access with IPSec, you need a client that supports PPP dial-up and IPSec as well as IKE. Because in most cases the client will get a different IP address from an ISP each time it connects, the IP address cannot be used as the IKE peer identity. Therefore, IKE must either be used in aggressive mode (if pre-shared key authentication has to be used) or with certificate-based authentication (then main mode or aggressive mode can be used). Our environment is based on a VPN client from IRE dialing in to an IBM 2212 router acting as the ISP and then establishing IKE negotiation and IPSec tunnels to an IBM 2216 router acting as the corporate VPN gateway.

Important

We used a pre-release of the IRE SafeNet VPN client. Therefore, any screenshots and features described in this chapter may be different from any version of IRE SafeNet that you may have purchased.

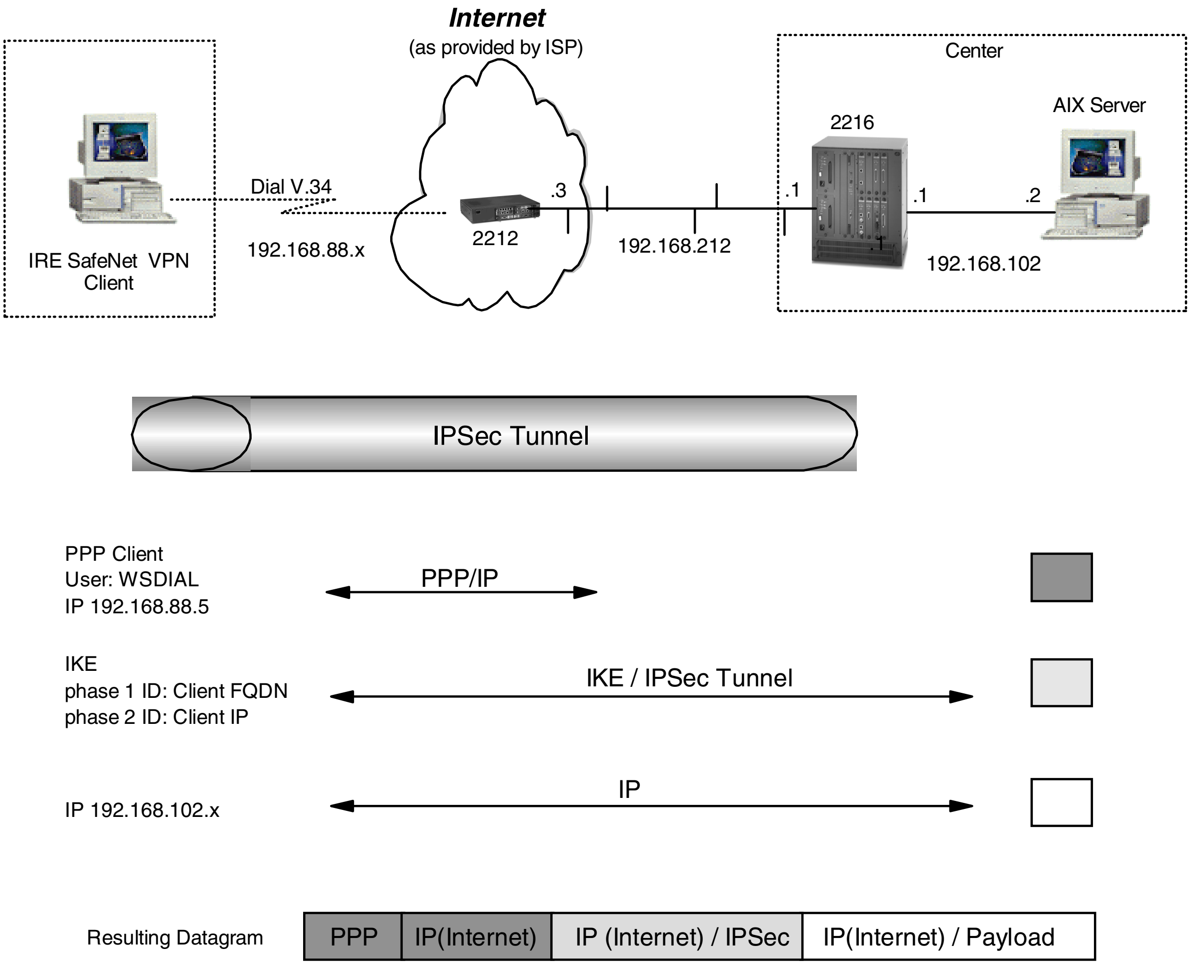


Figure 422. Sample network for IPSec dial-up

In this scenario, the remote client is accessing the secure network with an external IP address. To limit this type of packet on the internal network, we are restricting the client in this scenario to access only one specific server or firewall. In general, access to the whole internal network can be given to a client in this case but it depends on where the VPN gateway is placed relative to the corporate firewall in order to determine how the firewall is to handle this kind of traffic.

Because all client packets arrive via a secure tunnel there is no exposure associated with them other than the general tunnel fear that the client could have been attacked by a cracker and what arrives through the tunnel is malevolent traffic. This is no different from other remote access VPN scenarios.

20.2 Configuration of the ISP router

The necessary steps for configuring an ISP router for this scenario are the same as described in 17.2.3, “Definition of the ISP router” on page 330.

20.3 Configuration of the VPN gateway (center 2216 router)

For the configuration of the 2216 in the center we have to perform the following steps:

- Preparation.
- Configure the policy and validity period for IPSec and IKE.
- Configure IPSec action and proposal.
- Configure ISAKMP action and proposal.
- Activate the definitions on the center router.

20.3.1 Preparation

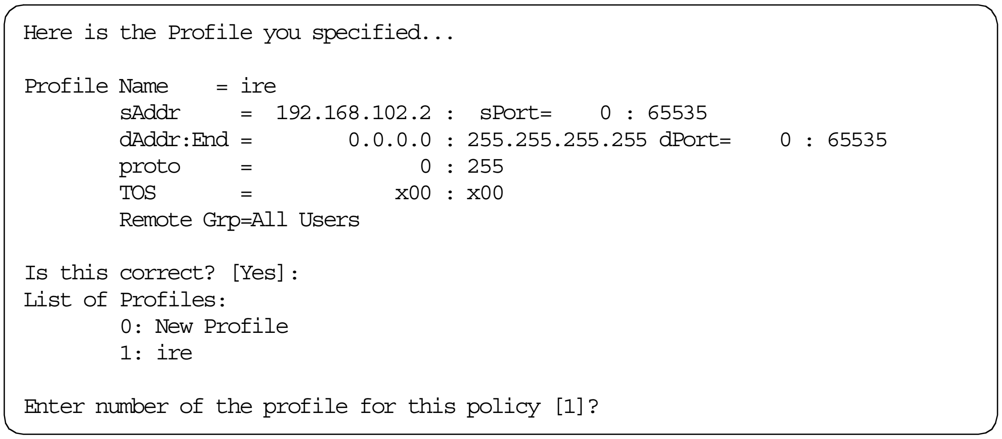
We assume that the permanent Ethernet connection to the ISP is already established. Therefore, we can concentrate on the dial-in features of this connection.

20.3.2 Configure policy profile for IPSec and IKE

The first step is to configure a policy that will encapsulate client traffic in an IPSec tunnel. When configuring the profile it is important that you select an address range rather than a netmask or single IP address. This is because if you use netmask the ID comparisons will fail because the netmask is of a subnet type while the ID type that will be received by the client would be an IP address type. Of course you cannot use a single IP address because you do not know what IP address the client will get from the ISP.

```
Center Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ire
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]?
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? ire
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]? 192.168.102.2
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 2
Enter IPV4 Starting Destination Address [0.0.0.0]?
Enter IPV4 Ending Destination Address [0.0.0.0]? 255.255.255.255

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]: y
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]? 1
Any user within profile definition allowed access? [Yes]:
The Source and/or Destination Address information you specified
includes all addresses.  You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy.  The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]:
```

Figure 423. Center router IKE policy configuration for IPSec dial-up



```
Here is the Profile you specified...

Profile Name    = ire
        sAddr     =  192.168.102.2 :  sPort=    0 : 65535
        dAddr:End =        0.0.0.0 : 255.255.255.255 dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users

Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: ire

Enter number of the profile for this policy [1]?
```

Figure 424. Center router profile configuration for IPSec dial-up

20.3.3 Configure validity period

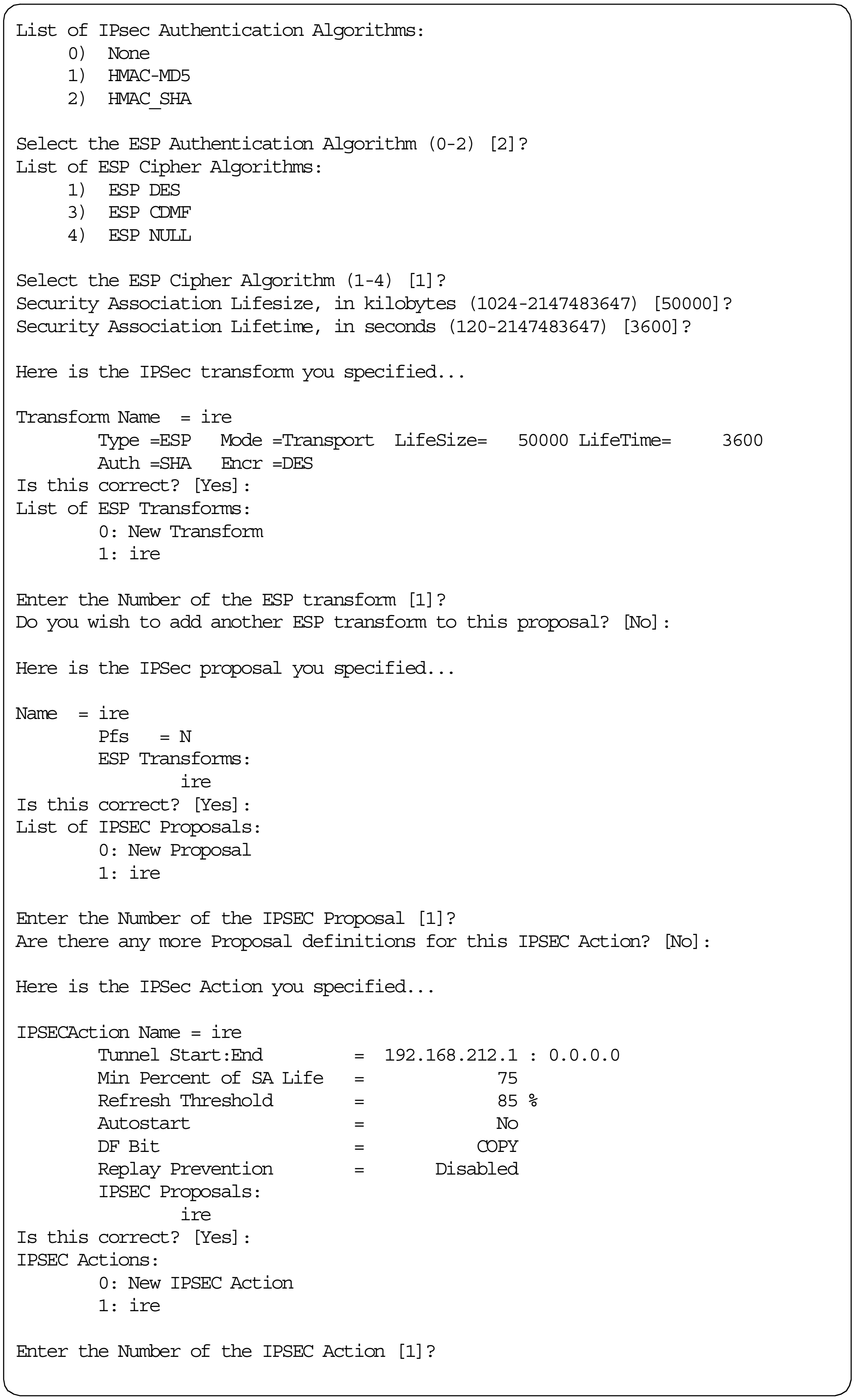
This step is the same as described in 17.4.3.3, “Configure validity period” on page 357.

20.3.4 Configure IPSec action and proposal

The next step is to define the IPSec action and proposal. You should note that you do not know the tunnel endpoint so 0.0.0.0 is entered as the destination tunnel endpoint.

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? ire
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [192.168.102.1]? 192.168.212.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
Enter a Name (1-29 characters) for this IPsec Proposal []? ire
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: y
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]? 0
Enter a Name (1-29 characters) for this IPsec Transform []? ire
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]? 2
```

Figure 425. Center router IPSec policy configuration for IPSec dial-up - part 1



```
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]?
List of ESP Cipher Algorithms:
     1)  ESP DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]?
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]?
Security Association Lifetime, in seconds (120-2147483647) [3600]?

Here is the IPSec transform you specified...

Transform Name  = ire
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=     3600
        Auth =SHA   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
        0: New Transform
        1: ire

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:

Here is the IPSec proposal you specified...

Name  = ire
        Pfs   = N
        ESP Transforms:
                ire
Is this correct? [Yes]:
List of IPSEC Proposals:
        0: New Proposal
        1: ire

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

IPSECAction Name = ire
        Tunnel Start:End         =  192.168.212.1 : 0.0.0.0
        Min Percent of SA Life   =            75
        Refresh Threshold        =            85 %
        Autostart                =            No
        DF Bit                   =          COPY
        Replay Prevention        =      Disabled
        IPSEC Proposals:
                ire
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: ire

Enter the Number of the IPSEC Action [1]?
```

Figure 426. Center router IPSec policy configuration for IPSec dial-up - part 2

20.3.5 Configure ISAKMP action and proposal

Once the IPSec action and proposal has been fully defined the next step is to define the ISAKMP action/proposal. The main point in this step is that aggressive mode must be used because the IP address of the client will not be known. In main mode the IDs are exchanged in messages 5 and 6, however the keys must be known before then to encrypt messages 5 and 6 itself. In aggressive mode the IDs are exchanged during the beginning of the exchange so the keys to be used can be determined at that time. In addition, encryption the last message of an aggressive mode exchange is optional.

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? ire

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]? 2
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]:

You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal

Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? ire

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  Certificate (RSA SIG)

Select the authentication method (1-2) [1]?

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
     1)  DES

Select the Cipher Algorithm (1-2) [1]?
```

Figure 427. Center router ISAKMP action configuration for IPSec dial-up - part 1

```
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

Here is the ISAKMP Proposal you specified...

Name = ire
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: ire

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...


ISAKMP Name     = ire
        Mode                    =      Aggressive
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =             Yes
        ISAKMP Proposals:
                ire
Is this correct? [Yes]:
ISAKMP Actions:
        0: New ISAKMP Action
        1: ire

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?


Here is the Policy you specified...


Policy Name     = ire
        State:Priority =Enabled    : 5
        Profile        =ire
        Valid Period   =always
        IPSEC Action   =ire
        ISAKMP Action  =ire
Is this correct? [Yes]:
```

Figure 428. Center router ISAKMP action configuration for IPSec dial-up - part 2

The last step of the policy definition is to enter the user as a fully qualified domain name (FQDN). This is the ID type that must be used because IP addresses are not known.

```
To authenticate the ISAKMP Peer with Pre-Shared Key a User
must be added.  Add a USER now? [Yes]: y
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]? 2
Enter the FQDN to distinguish this user (No spaces allowed) []? wtr05999.itso.ral.ibm.com
Group to include this user in []?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (8 characters) in ascii:

Here is the User Information you specified...

Name      = wtr05999.itso.ral.ibm.com
        Type      = FQDN
        Group     =
        Auth Mode =Pre-Shared Key
Is this correct? [Yes]:
```

Figure 429. Center router ISAKMP ID configuration for IPSec dial-up

The FQDN configured in Figure 429 must match the FQDN that was specified at the client as described in 20.4.2, “VPN client configuration” on page 414.

20.3.6 Add default route

These steps and the reasons for performing them are the same as described in 17.4.3.8, “Add default route and enable ARP-subnet-routing” on page 364.

20.4 Configuration of the IRE SafeNet VPN client

Information Resource Engineering, Inc. (IRE) is a company that develops software for other vendors to include in their products. Cisco Systems, Inc., for example, have licensed SafeNet as their client solution for VPNs. IRE also distributes some of their products commercially. The generally available version of the IRE VPN client is called SafeNet. We used Version 2.0.7, build 18, of SafeNet for our interoperability scenarios. To find more information about SafeNet and how you can purchase it, please access the URL below:

http://www.ire.com

20.4.1 SafeNet VPN client capabilities

The IRE VPN client offers one of the richest sets of VPN features available in the market today, ranging from manual IPSec tunnels to IKE support with digital certificates and online CA support to remote access capability with a private IP address. We have therefore chosen this client this scenario.

Important

The IRE SafeNet VPN client does not, at the time of writing, support token-ring. In fact, if you are using the client on a system that has a token-ring adapter installed, chances are that the system may crash as soon as you enable an IPSec policy. Unfortunately, this is true for many other VPN client products we have tested with the exception of Windows 2000 (which is not yet released, however).

This section briefly lists the VPN capabilities of the IRE VPN client:

Table 32. SafeNet VPN client 2.0.7 - VPN features

Feature	
Tunnel Type	IKE, manual
IPSec Header Format	RFCs 24xx
Operating Systems Supported	Windows NT, Windows 98, Windows 95
Interfaces Supported	Ethernet, Dial-up
IKE	
Key Management Tunnel (Phase 1)	
Negotiation Mode	Main Mode, Aggressive Mode
Encryption Algorithm	DES, 3DES
Authentication Method	Pre-Shared Key, RSA Signatures
Authentication Algorithm	HMAC-MD5, HMAC-SHA
Diffie-Hellman Group	Group 1, Group 2
Send Phase 1 Delete	Yes
On-demand Tunnels	Yes
Data Management Tunnel (Phase 2)	
Encapsulation Mode	Tunnel Mode, Transport Mode
Security Protocol	AH, ESP (not both in beta version)
AH Authentication Algorithm	HMAC-MD5, HMAC-SHA
ESP Encryption Algorithm	DES, 3DES
ESP Authentication Algorithm	HMAC-MD5, HMAC-SHA
Multiple SA Proposals	Yes
Perfect Forward Secrecy (PFS)	Yes
Other	Logging, Certificates, Private (Virtual) IP Address

We used an IBM PC 750 with Windows 98 as a client workstation for this scenario.

20.4.2 VPN client configuration

For remote access VPNs, SafeNet VPN Client requires Microsoft Dial-Up Networking 1.2 or higher on Windows 95.

To install SafeNet, click **Setup** in the directory where the software has been unpacked to, then follow the instructions on the screen. Once the setup procedure has finished, reboot your system.

Details on how to configure the IRE client for a LAN VPN connection and how to use digital certificates with the IRE client can be found in the redbook *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*, SG24-5309.

For a dial-up connection, you have to perform the client configuration and also create a dial-up networking entry to connect to your ISP.

20.4.2.1 Configure a dial-up connection to the ISP

Before you can use the SecureWay VPN client in this scenario, you have to create a dial-up networking configuration to access your ISP. The IPSec tunnel will be established over this connection so it needs to be defined first. This step is essentially the same as described in 17.2.5.3, “Configure the Dial-Up Networking (DUN) client” on page 338 for creating a DUN entry for the ISP. The difference is that in this case, you do not have to create a second DUN entry.

Add a DUN Client to the ISP by double-clicking **Make New Connection**. Specify user ID/password (`wsdial/wsdial`), keep the default device for your modem and click the **Next** button. Enter the telephone number and click the **Next** button. The installation of the ISP connection is finished.

20.4.2.2 Configure the SafeNet VPN client

Table 33 shows the parameters that will be configured on the client. Unless otherwise stated, other values that are not covered in the table will remain as default:

Table 33. IRE SafeNet VPN client - host-to-gateway VPN connection IPSec parameters

IPSec parameters and some pertinent information on the other party	
Local	
IP Address	unknown (ISP-assigned)
Role	Initiator
Remote	
IP Address	192.168.212.1
Role	Responder
Key Management Tunnel (Phase 1)	
Mode	Aggressive
Encryption	DES
Authentication Algorithm	SHA
Key Exchange Group	1

<table>
<tr><th colspan="2">IPSec parameters and some pertinent information on the other party</th></tr>
<tr><td>Key Lifetime</td><td>86400 sec (default)</td></tr>
<tr><td>Negotiation ID</td><td>Domain name</td></tr>
<tr><td>Pre-Shared Key</td><td>1234567890</td></tr>
<tr><td colspan="2"><b>Data Management Tunnel (Phase 2)</b></td></tr>
<tr><td>Remote Host IP Address</td><td>192.168.102.2</td></tr>
<tr><td>Remote Host Subnet Mask</td><td>255.255.255.255</td></tr>
<tr><td>Port</td><td>* (all protocols/ports)</td></tr>
<tr><td colspan="2">Security Protocols
<table>
<tr><td></td><td>AH (Authentication)</td><td></td></tr>
<tr><td>✓</td><td>ESP (Encryption)</td><td>DES</td></tr>
<tr><td>✓</td><td>ESP (Authentication)</td><td>SHA</td></tr>
</table></td></tr>
<tr><td>Encapsulation Mode</td><td>Tunnel</td></tr>
<tr><td>Perfect Forward Secrecy (PFS)</td><td>No</td></tr>
<tr><td>SA Lifetime</td><td>28800 sec (default)</td></tr>
</table>

After the system has been rebooted, SafeNet starts automatically and minimizes itself to the task bar.

1. Right mouse click the task bar icon and select **Security Policy Editor** from the context menu.

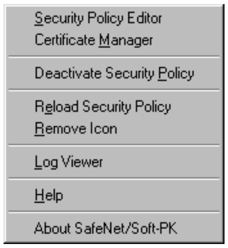
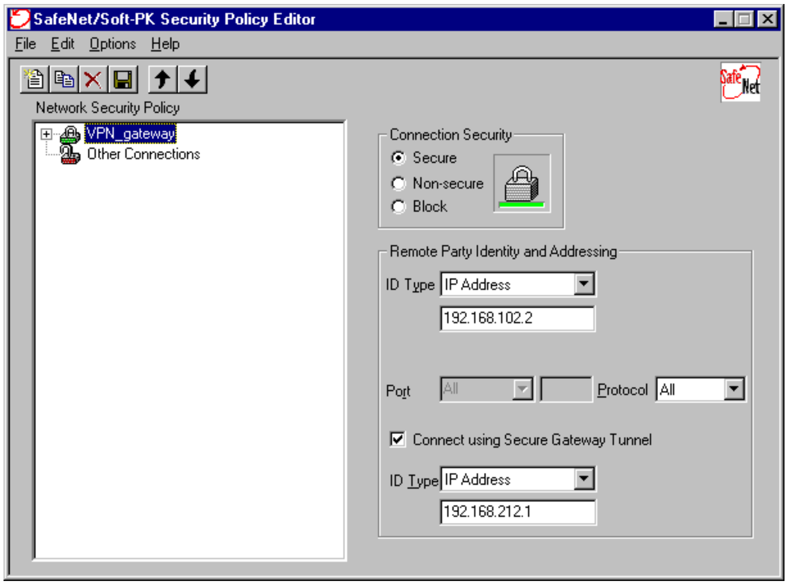


Figure 430. IRE SafeNet - task bar Icon context menu

1. Create a new connection by clicking **File -> New Connection**.



SafeNet/Soft-PK Security Policy Editor

File Edit Options Help

Network Security Policy

- VPN_gateway
- Other Connections

Connection Security

● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing

ID Type: IP Address

192.168.102.2

Port: All | Protocol: All

☑ Connect using Secure Gateway Tunnel

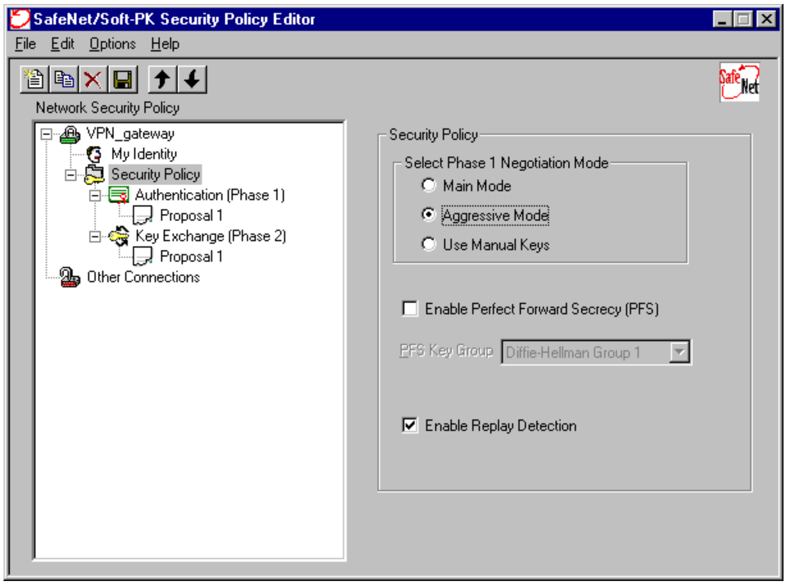
ID Type: IP Address

192.168.212.1

Figure 431. IRE SafeNet - new connection

2. Check **Secure** to protect this connection with IPSec. Enter the remote parties IP address which in our case is a single server behind the corporate VPN gateway. Check connect via security gateway and enter the appropriate IP address for that gateway. This means that the client is using IPSec tunnel mode to the VPN gateway and all traffic to the server in the corporate network flows through that tunnel across the Internet and in the clear inside the corporate network.

3. Expand all objects in the connection tree by clicking the **(+)** signs next to them, then click **Security Policy** and select **Aggressive Mode**. This triggers a wider choice of selections for the IKE Phase 1 identity.



SafeNet/Soft-PK Security Policy Editor

File Edit Options Help

Network Security Policy

- VPN_gateway
  - My Identity
  - Security Policy
    - Authentication (Phase 1)
      - Proposal 1
    - Key Exchange (Phase 2)
      - Proposal 1
- Other Connections

Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode
● Aggressive Mode
○ Use Manual Keys

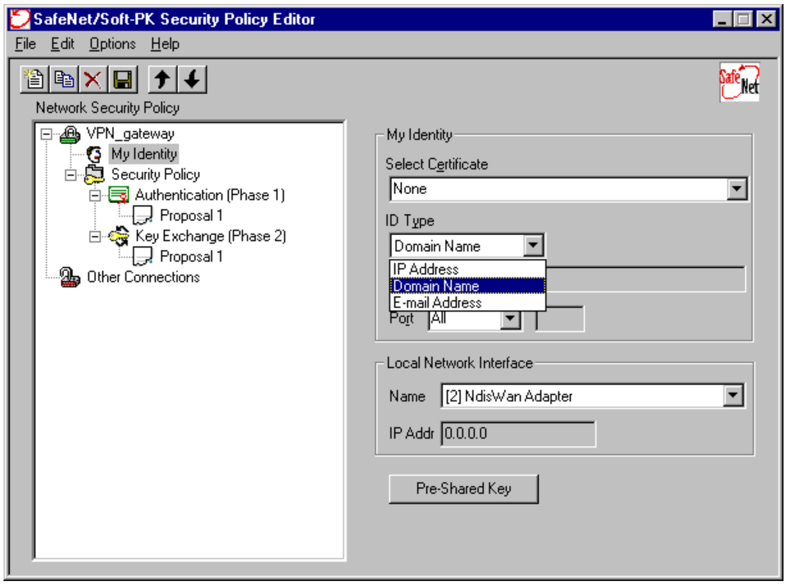
□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

Figure 432. IRE SafeNet - security policy

4. Next, click **My Identity** and select **Domain Name**. The client then pulls the configured host and domain name from the Windows Networking TCP/IP properties and inserts them into the configuration. You cannot change that field.



My Identity

Select Certificate: None

ID Type: Domain Name

Port: All

Local Network Interface

Name: [2] NdisWan Adapter

IP Addr: 0.0.0.0

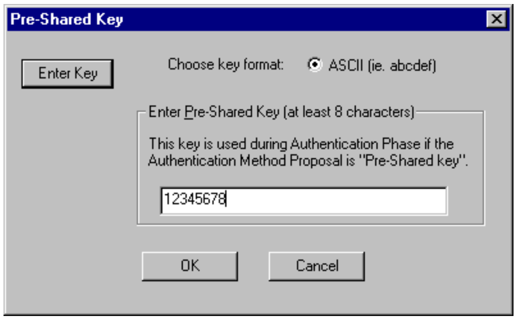
Figure 433. IRE SafeNet - set client identity

Reminder

IKE Phase 1 with pre-shared key authentication only allows an IP address as the peer ID. Since you are using pre-shared keys in this scenario but do not know your IP address in advance as it will be provided by the ISP, you must use aggressive mode and an ID different from the IP address. Because SafeNet can use certificates where the ID for Phase 1 will be whatever the certificate says, you first have to tell the client that you want to use aggressive mode or it will not let you choose anything other than IP address for My ID.

5. Select a dial-up interface or leave the selection as any. On Windows NT, you must have a dial-up connection established before it will appear in this list.

6. Enter the value for the pre-shared key.



Choose key format: ● ASCII (ie. abcdef)

Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

12345678

Figure 434. IRE SafeNet - pre-shared key

7. Enter the transforms for the Phase 1 Proposal. You can add multiple proposals if you wish.
8. Enter the transforms for the Phase 2 Proposal. You can add multiple proposals if you wish.
9. Save the policy and then select **Reload Policy** from the task bar icon context menu.

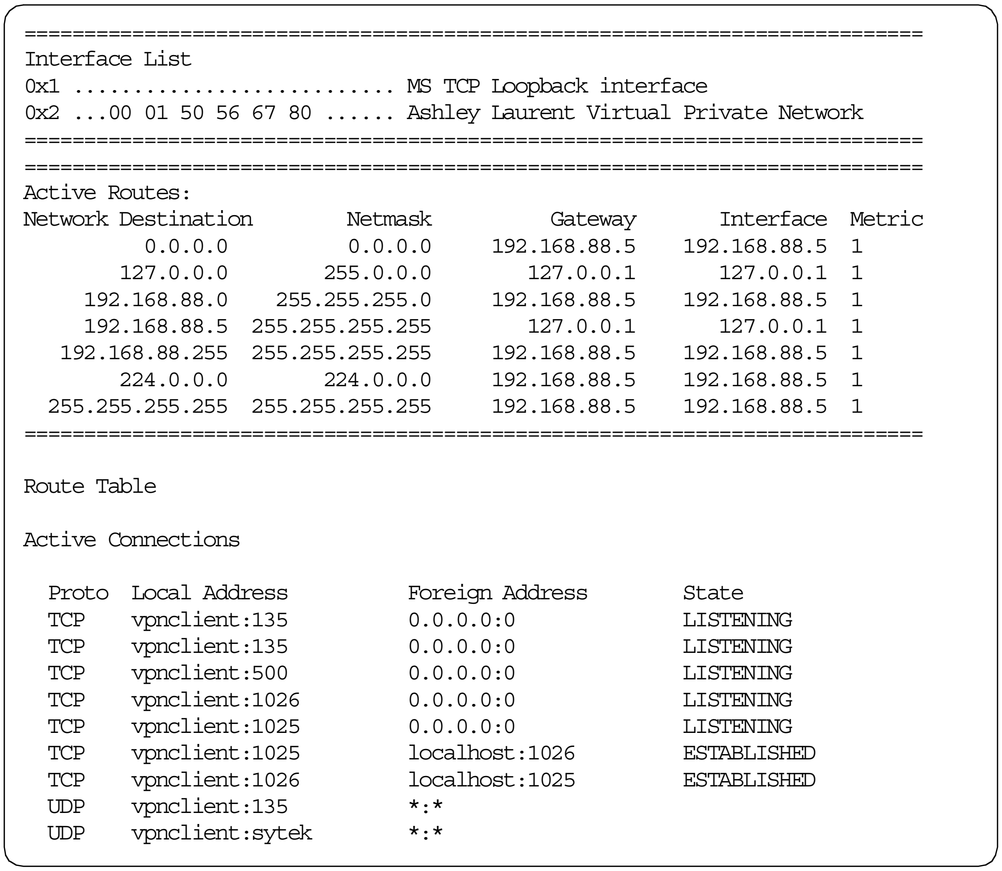
20.4.3 Testing and verifying the connection

To establish an IPSec tunnel using the IRE SafeNet VPN client, you need to use one DUN session to connect to the Internet (in our case to the ISP's router).

20.4.3.1 Dialing to ISP

We launch the PPP dial-up connection which establishes the Internet connection and logon with the user ID `wsdial`. Remember to stop the VPN client until the dial-up link is active.

The screen below shows the output from the `netstat -ra` command which lists the IP routing table after dialing the ISP, and it also lists the active ports at the client showing UDP port 500 (sytek) active which means IKE is ready.



```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 01 50 56 67 80 ...... Ashley Laurent Virtual Private Network
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.88.5    192.168.88.5  1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1  1
     192.168.88.0    255.255.255.0     192.168.88.5    192.168.88.5  1
     192.168.88.5  255.255.255.255        127.0.0.1       127.0.0.1  1
   192.168.88.255  255.255.255.255     192.168.88.5    192.168.88.5  1
        224.0.0.0        224.0.0.0     192.168.88.5    192.168.88.5  1
  255.255.255.255  255.255.255.255     192.168.88.5    192.168.88.5  1
===========================================================================

Route Table

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    vpnclient:135          0.0.0.0:0              LISTENING
  TCP    vpnclient:135          0.0.0.0:0              LISTENING
  TCP    vpnclient:500          0.0.0.0:0              LISTENING
  TCP    vpnclient:1026         0.0.0.0:0              LISTENING
  TCP    vpnclient:1025         0.0.0.0:0              LISTENING
  TCP    vpnclient:1025         localhost:1026         ESTABLISHED
  TCP    vpnclient:1026         localhost:1025         ESTABLISHED
  UDP    vpnclient:135          *:*
  UDP    vpnclient:sytek        *:*
```

Figure 435. IRE SafeNet VPN client - list routes and active connections

20.4.3.2 Starting negotiation

Once the policy has been reloaded, the SafeNet VPN client is checking any outgoing packet to see if it matches a secure traffic profile. If it does, than IKE negotiations are started as defined in the security policy. If successful, matching traffic will be secured with IPSec as defined in the security policy.

Likewise, any incoming packet is checked to see if it matches a secure traffic profile. If it does, IPSec will be used as defined in the security policy, or, in case of IKE packets, appropriate IKE response messages will be sent to negotiate new SAs for that traffic. If successful, matching traffic will be secured with IPSec as defined in the security policy.

This resembles exactly the behavior described in 3.3.1, “Outbound IPSec processing for host systems” on page 57.

From the context menu, select **Log Viewer** to determine if everything goes as it should. To initiate IKE negotiations, simply access AIXSRV2 for which a security policy has been defined. Provided the partner is ready to respond, you see in the log that IKE main mode and quick mode are completed successfully and SAs are established to protect traffic with IPSec.

Chapter 21. Connecting dial-up routers with L2TP and IPSec

Layer-2 tunneling gives an organization benefits in creating VPNs that will allow it to deploy infrastructures that require a layer-2 interface. However, the strength of the security in these tunnels is relatively weak when compared to technologies like IPSec. IPSec, on the other hand, only delivers a layer-3 interface which may not meet an organization’s requirement. The IETF has proposed to properly secure layer-2 tunnels, and IPSec should be used.

The following scenario describes the process of securing layer-2 tunnels with IPSec in a dial-up router environment. The same principle can be used to secure L2TP tunnels from remote access clients which we have already described in 17.4, “Using L2TP with IPSec” on page 353.

21.1 Scenario description

In this example, we will take an existing scenario described in Chapter 19, “Connecting dial-up routers with L2TP” on page 387. In that chapter we used exactly the same scenario but secured the tunnel with IPSec.

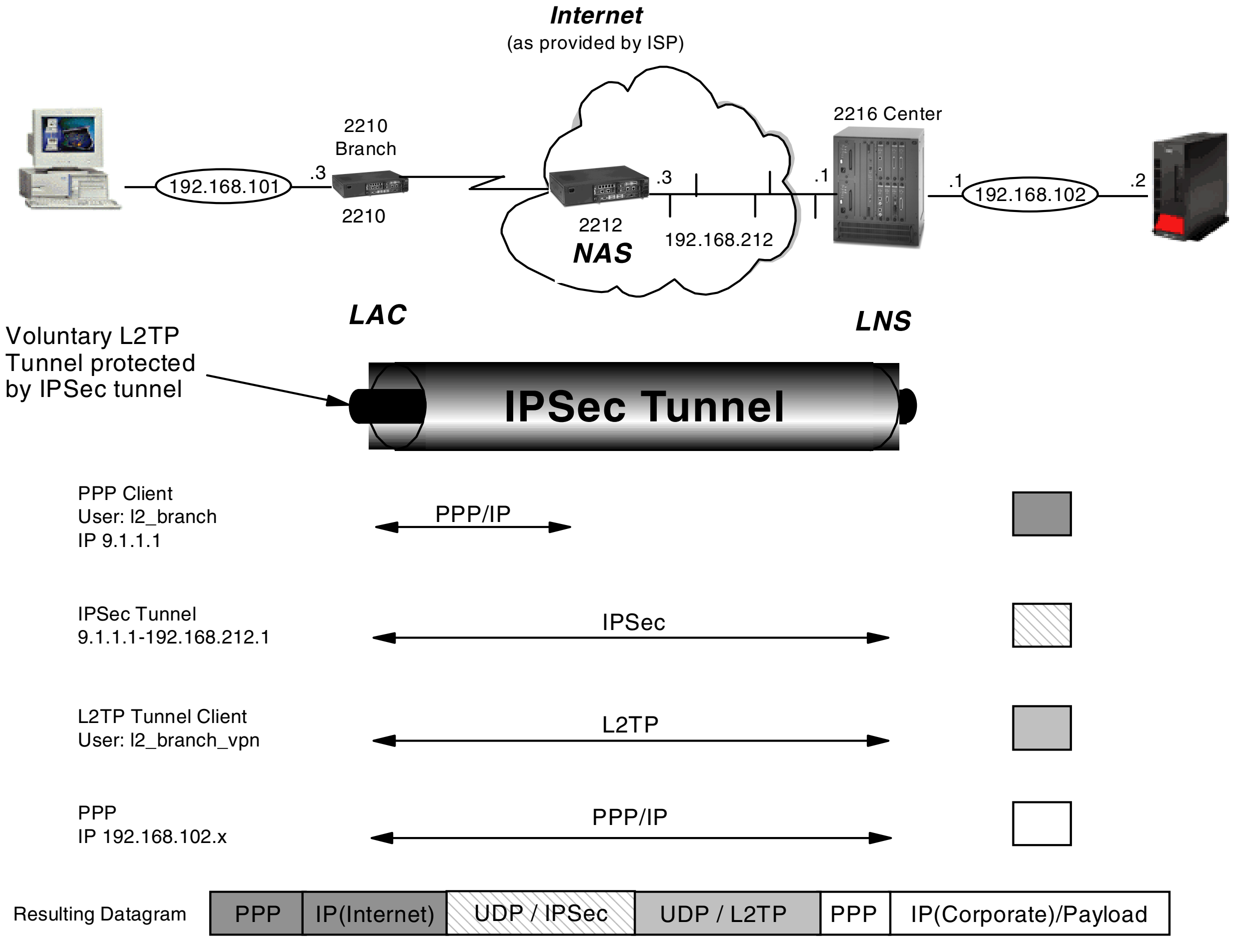


Figure 436. Scenario for securing L2TP tunnel with IPSec

When defining an IPSec tunnel you use tunnel mode if at least one end of the tunnel is not the final destination of a packet. This is the case with the scenario shown in Figure 436 on page 421 where the source and destination packets come from 192.168.102.0 and 192.168.101.0 subnets. However, the IPSec tunnel will be securing the L2TP tunnel, so as far as IPSec is concerned all the packets will be coming to and from 9.1.1.1 and 192.168.212.1, exactly the same endpoints of the IPSec tunnel. Therefore, in this scenario a transport mode tunnel should be used.

In the scenario described in Chapter 19, “Connecting dial-up routers with L2TP” on page 387 the following steps occur when IP packets need to get to the corporate network (assuming connection to the ISP has not yet occurred):

1. Packet to corporate network is passed to the branch router.
2. The branch router passes the packet to the next hop over a virtual layer-2 interface.
3. The virtual layer-2 interface sees that the tunnel has not yet been set up so it tries to open an L2TP tunnel to its endpoint 192.168.212.1.
4. This causes the packet to be forwarded over the dial-up PPP interface.
5. Since the dial-up interface has data to send it initiates a call to the ISP to establish a dial-up PPP connection to the Internet.
6. The L2TP tunnel initiated in step 3 can now be completed since the branch router now has a path to the L2TP tunnel endpoint over the Internet.
7. The packet forwarding attempted in step 2 can now be completed since the tunnel using the virtual layer-2 interface now exists.
8. The corporate router receives the packet and forwards it to the corporate network.

When we want to secure the tunnel with IPSec we need to modify steps 3 through 6 to trap all LT2P traffic and to put it over an IPSec tunnel:

3. The virtual layer-2 interface sees that the tunnel has not yet been set up so it tries to open an L2TP tunnel to its endpoint 192.168.212.1.

3a.The router detects that L2TP traffic is being sent and intercepts it and tries to initiate an IPSec tunnel to its endpoint 192.168.212.1.

4. This causes the packet to be forwarded over the dial-up PPP interface.
5. Since the dial-up interface has data to send it initiates a call to the ISP to establish a dial-up PPP connection to the Internet.

5a.The IPSec tunnel initiated in step 3a can now be completed since the branch router now has a path to its IPSec tunnel endpoint over the Internet.

6. The L2TP tunnel initiated in step 3 can now be completed since the branch router now has a path to the L2TP tunnel endpoint through the IPSec tunnel.

Note

In reality what will happen is that the branch router will drop the packets until the PPP dial-up session is activated and the tunnels have been established. It is important to configure the idle timer properly on the PPP dial-up interface. Too short a timer will mean that users will have to continually retry communications to the corporate network since the dial-up circuit and tunnels would have to be recreated. Too long a timer will mean that the corporate will incur ISP access charges even though the link is not being used.

21.1.1 Modification to the L2TP setup

Since we will be using the example shown in Chapter 19, “Connecting dial-up routers with L2TP” on page 387 as the basis for this scenario we will assume that all steps have been performed. There are, however, a number of modifications that must occur.

When L2TP negotiates the formation of a tunnel it initially uses UDP port 1701, but as part of the negotiation another UDP port can be negotiated to support the traffic flow. We have to ensure that this does not occur; otherwise, building the IPSec traffic policy will be extremely difficult. This is achieved through the ENABLE FIXED-UDP-SOURCE-PORT command.

```
l2_branch Config>FEATURE Layer-2-Tunneling
l2_branch Layer-2-Tunneling Config>ENABLE FIXED-UDP-SOURCE-PORT
```

Figure 437. L2TP fixed UDP source port

The above command must be performed on both the branch office router and the central corporate router.

The current release of the router code must specifically define the IP address IPSec tunnel start point. It is this IP address that the responding endpoint uses to to communicate back to the initiator. As a result the IPSec tunnel start point must be a real Internet IP address. The implication for a dial-up router scenario as we have here is that the ISP must provide a fixed IP address. In our scenario this will be 9.1.1.1.

Since we now have a fixed IP address from the ISP the following configuration changes need to occur with the branch office router:

1. Define a fixed IP address to the dial-up interface instead of an unnumbered IP address.
2. Redefine the static route statement to point to the fixed IP address.

```
l2_branch Config>PROTOCOL IP
Internet protocol user configuration
l2_branch IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0  192.168.103.3    255.255.255.0    Local wire broadcast, fill 1
   intf     1                                    IP disabled on this interface
   intf     2                                    IP disabled on this interface
   intf     3                                    IP disabled on this interface
   intf     4                                    IP disabled on this interface
   intf     5                                    IP disabled on this interface
   intf     6  0.0.0.6          255.255.255.255  Local wire broadcast, fill 1
                                                 DYNAMIC-ADDRESS Enabled
   intf     7  0.0.0.7          0.0.0.0          Local wire broadcast, fill 1
Internal IP address: 192.168.101.3
l2_branch IP config>DELETE ADDRESS 0.0.0.6
l2_branch IP config>ADD ADDRESS
Which net is this address for [0]? 6
New address []? 9.1.1.1
Address mask [255.0.0.0]? 255.255.255.255
l2_branch IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0  192.168.103.3    255.255.255.0    Local wire broadcast, fill 1
   intf     1                                    IP disabled on this interface
   intf     2                                    IP disabled on this interface
   intf     3                                    IP disabled on this interface
   intf     4                                    IP disabled on this interface
   intf     5                                    IP disabled on this interface
   intf     6  9.1.1.1          255.255.255.255  Local wire broadcast, fill 1
   intf     7  0.0.0.7          0.0.0.0          Local wire broadcast, fill 1
Internal IP address: 192.168.101.3
l2_branch IP config>LIST ROUTES

route to 0.0.0.0        ,0.0.0.0         via 0.0.0.6         cost 1
route to 192.168.102.0  ,255.255.255.0   via 0.0.0.7         cost 1

l2_branch IP config>CHANGE ROUTE
IP destination []? 0.0.0.0
Address mask [255.0.0.0]? 0.0.0.0
Via gateway 1 at [0.0.0.6]? 9.1.1.1
Cost [1]?
Via gateway 2 at []?
l2_branch IP config>LIST ROUTES

route to 0.0.0.0        ,0.0.0.0         via 9.1.1.1         cost 1
route to 192.168.102.0  ,255.255.255.0   via 0.0.0.7         cost 1

l2_branch IP config>
```

Figure 438. Static routes configuration

The next step is to define the policy which will trap all L2TP packets (UDP Port 1701) and to put them over an IPSec tunnel. In this example we will be using an IPSec tunnel using IKE and pre-shared keys. The definition in this example will be very similar to that described in 6.2.2, “Configuring IKE with pre-shared keys” on page 104.

The first step in defining the profile is to capture all the L2TP traffic into that profile.

```
l2_branch *TALK 6
Gateway user configuration
l2_branch Config>FEATURE Policy
IP Network Policy configuration
l2_branch Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? l2tp_in_ipsec
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]? 0
Profile Configuration questions.  Note for Security Policies, the Source
Address and Port Configuration parameters refer to the Local Client Proxy
and the Destination Address and Port Configuration parameters refer to the
Remote Client Proxy
Enter a Name (1-29 characters) for this Profile []? l2tp_in_ipsec
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Source Address [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]? 3
Enter IPV4 Destination Address [0.0.0.0]? 192.168.212.1

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]? 2
Enter the Starting value for the Source Port [0]? 1701
Enter the Ending value for the Source Port [65535]? 1701
Enter the Starting value for the Destination Port [0]? 1701
Enter the Ending value for the Destination Port [65535]? 1701
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]: yes
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)

Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:


Here is the Profile you specified...


Profile Name    = l2tp_in_ipsec
        sAddr     =        0.0.0.0 : 0.0.0.0         sPort= 1701 : 1701
        dAddr     =  192.168.212.1 :  dPort= 1701 : 1701
        proto     =             17 : 17
        TOS       =            x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:
```

Figure 439. Profile for L2TP with IPSec

The definition for the central router is the same except the destination address is 9.1.1.1.

Once the new profile is defined it is selected and the validity period is then configured. The definition is the same for the central router.

```
List of Profiles:
        0: New Profile
        1: l2tp_in_ipsec

Enter number of the profile for this policy [1]?
List of Validity Periods:
        0: New Validity Period

Enter number of the validity period for this policy [0]? 0
Enter a Name (1-29 characters) for this Policy Valid Profile []? always
Enter the lifetime of this policy. Please input the
information in the following format:
                yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?


Here is the Policy Validity Profile you specified...


Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
Is this correct? [Yes]:
List of Validity Periods:
        0: New Validity Period
        1: always

Enter number of the validity period for this policy [1]?
```

Figure 440. Define validity period

Next the IPSec action is defined. The definition is identical in the central router except that the tunnel start and endpoints are reversed.

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? l2tp_in_ipsec
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [192.168.101.3]? 9.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 192.168.212.1
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
```

Figure 441. IPSec action for L2TP

Next the IPSec proposal is defined. Again the definition in the central router is identical.

```
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [1]? 0
Enter a Name (1-29 characters) for this IPsec Proposal []? l2tp_in_ipsec
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: y
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [1]? 0
Enter a Name (1-29 characters) for this IPsec Transform []? l2tp_in_ipsec
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]? 2
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]? 1
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 1
Security Association Lifesize, in kilobytes (1024-2147483647) [50000]?
Security Association Lifetime, in seconds (120-2147483647) [3600]?

Here is the IPSec transform you specified...

Transform Name  = test
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES
Is this correct? [Yes]:
List of ESP Transforms:
        0: New Transform
        1: l2tp_in_ipsec

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [No]:

Here is the IPSec proposal you specified...

Name  = l2tp_in_ipsec
        Pfs   = N
        ESP Transforms:
                l2tp_in_ipsec
Is this correct? [Yes]:
Are there any more Proposal definitions for this IPSEC Action? [No]:
```

Figure 442. IPSec proposal for L2TP

Next the IPSec action that has just been defined is confirmed:

```
Here is the IPSec Action you specified...


IPSECAction Name = l2tp_in_ipsec
        Tunnel Start:End        =        9.1.1.1 : 192.168.212.1
        Tunnel In Tunnel        =             No
        Min Percent of SA Life  =             75
        Refresh Threshold       =             85 %
        Autostart               =            No
        DF Bit                  =           COPY
        Replay Prevention       =       Disabled
        IPSEC Proposals:
                   l2tp_in_ipsec
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: l2tp_in_ipsec

Enter the Number of the IPSEC Action [1]? 1
```

Figure 443. Confirm IPSec action

The ISAKMP action needs to be defined next. Again the definition in the central router is the same

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Action []? l2tp_in_ipsec

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?
ISAKMP Connection Lifesize, in kilobytes (100-2147483647) [5000]?
ISAKMP Connection Lifetime, in seconds (120-2147483647) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]: n
```

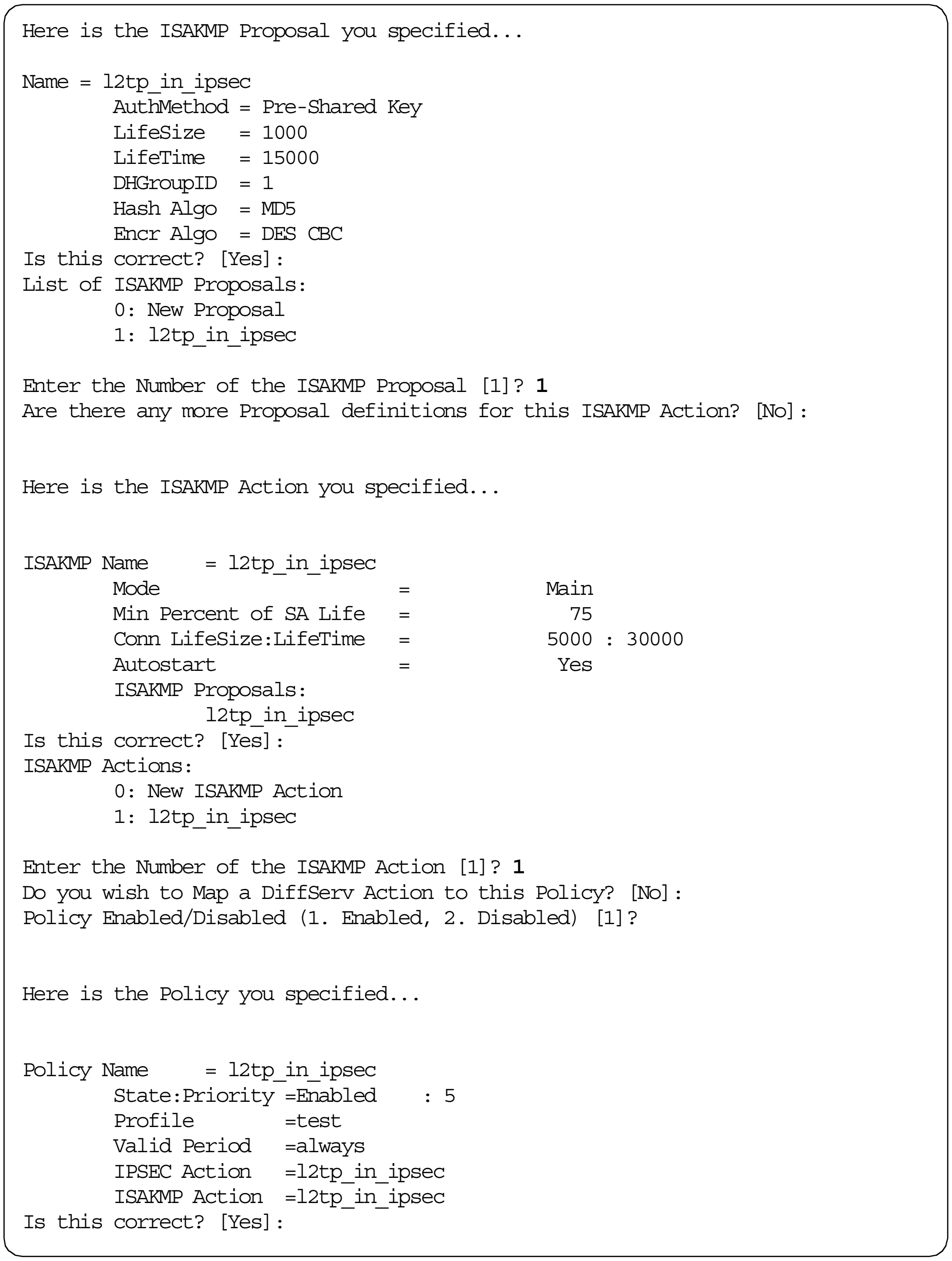
Figure 444. ISAKMP action for L2TP

The ISAKMP proposal for the action also has to be defined. Again the definition in the central router is identical.

```
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal

Enter the Number of the ISAKMP Proposal [1]? 0
Enter a Name (1-29 characters) for this ISAKMP Proposal []? l2tp_in_ipsec

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  Certificate (RSA SIG)

Select the authentication method (1-2) [1]?

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]?

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]?
Security Association Lifesize, in kilobytes (100-2147483647) [1000]?
Security Association Lifetime, in seconds (120-2147483647) [15000]?

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?


Here is the ISAKMP Proposal you specified...

Name = l2tp_in_ipsec
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
```

Figure 445. ISAKMP proposal for L2TP

Next the recently defined ISAKMP proposal and actions have to be confirmed. Also now that the policy has been fully defined it also needs to be confirmed and enabled. Again, the definition in the central router is identical.



```
Here is the ISAKMP Proposal you specified...

Name = l2tp_in_ipsec
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: l2tp_in_ipsec

Enter the Number of the ISAKMP Proposal [1]? 1
Are there any more Proposal definitions for this ISAKMP Action? [No]:


Here is the ISAKMP Action you specified...


ISAKMP Name     = l2tp_in_ipsec
        Mode                     =            Main
        Min Percent of SA Life   =              75
        Conn LifeSize:LifeTime   =            5000 : 30000
        Autostart                =             Yes
        ISAKMP Proposals:
                l2tp_in_ipsec
Is this correct? [Yes]:
ISAKMP Actions:
        0: New ISAKMP Action
        1: l2tp_in_ipsec

Enter the Number of the ISAKMP Action [1]? 1
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?


Here is the Policy you specified...


Policy Name     = l2tp_in_ipsec
        State:Priority =Enabled    : 5
        Profile        =test
        Valid Period   =always
        IPSEC Action   =l2tp_in_ipsec
        ISAKMP Action  =l2tp_in_ipsec
Is this correct? [Yes]:
```

Figure 446. Confirm ISAKMP action

Chapter 22. IPSec performance on 2212

General 2210, 2216, and 2212 performance capacity to process routing is shown in Figure 447:

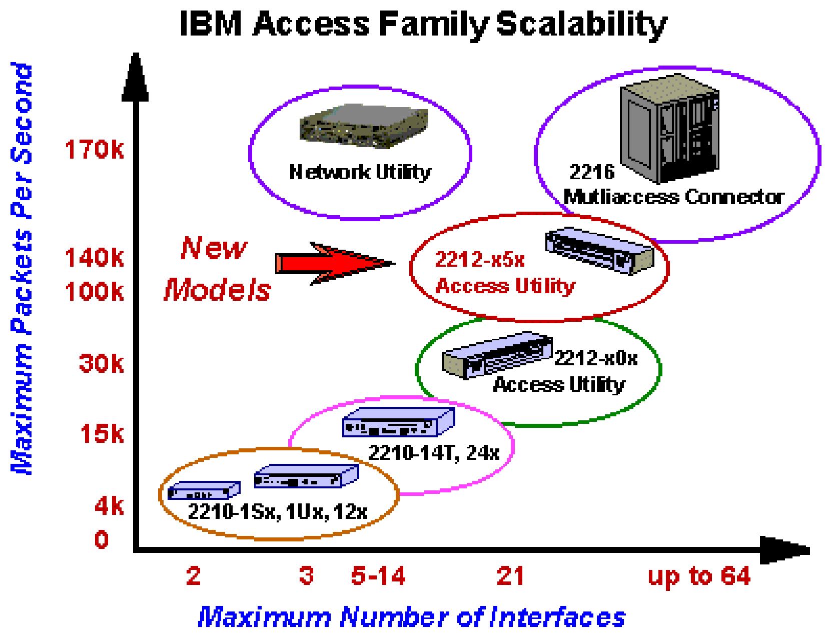


Figure 447. IBM Nways router performance capacity

Data encryption and compression usually make a significant effect in router performance since they require very intensive processing. As a solution for performance decreasing due to encryption, the new hardware Compression/Encryption Adapter (CEA) significantly increases the compression/encryption capacity of your 2212 while also reducing the burden that software compression/encryption places on the router's CPU and thereby freeing up your router to handle other networking tasks.

- With only encryption and IP enabled, With only encryption and IP enabled, the 2212 Model x0x can support a maximum of 52 PPP 64-Kbps WAN circuits running DES compression at 95% router CPU utilization. For frame relay, 14 64-Kbps WAN circuits can be supported. Adding the new CEA adapter increases the maximum PPP 64-Kbps circuits over threefold to 168.
- The new 2212 Model x5x can support a maximum of 558 PPP 64-Kbps WAN circuits. For Frame Relay CDMF, 336 64-Kbps WAN circuits can be supported. Adding the CEA adapter increases the maximum supported PPP 64-Kbps circuits to 640.

Test results are shown in Figure 448.

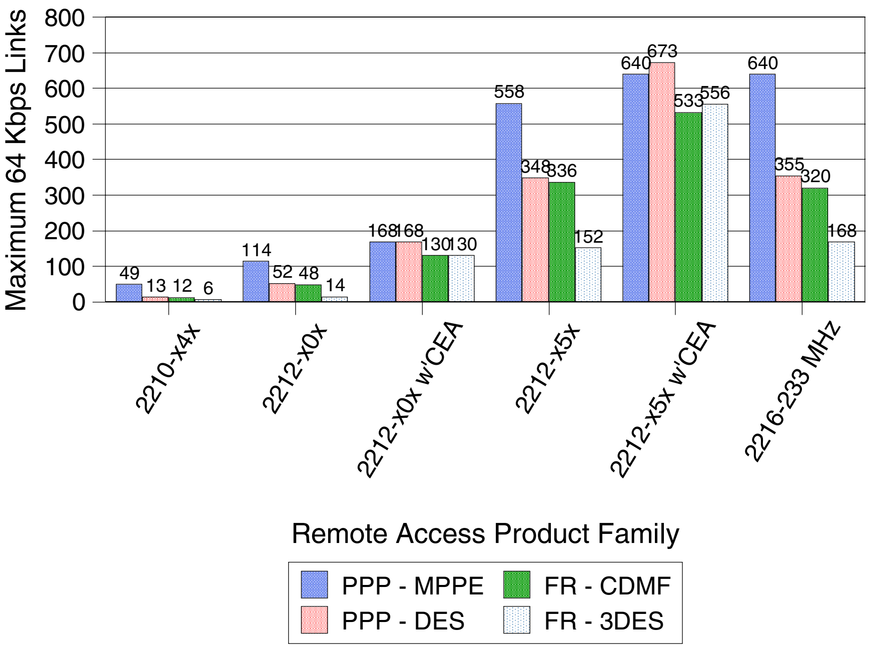


Figure 448. Encryption capacity in 221X

As one of the encryption applications IPSec provides a choice of authentication protocols (HMAC with MD5 or HMAC-SHA-1) and encryption protocols (DES with CBC, CDMF, or 3DES). Using these encryption protocols provides secure data transmission with the cost of the added CPU utilization. Test results to know how much IPSec affects performance and how much could be decreased using CEA are shown in Figure 449 and Figure 450.

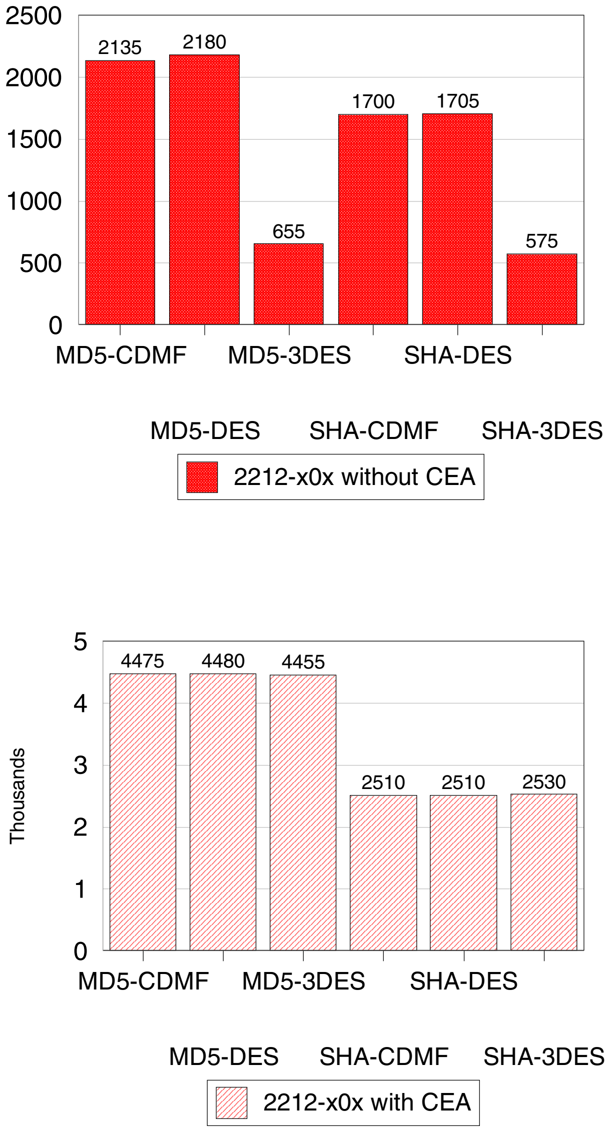


Figure 449. 2212-x0x IPSec capacity

The 2212 Model x0x can support a maximum of 2180 Kbps of WAN throughput at 95% CPU utilization when using MD5 with DES. Adding the new CEA adapter more than doubles maximum throughput to 4480 Kbps.

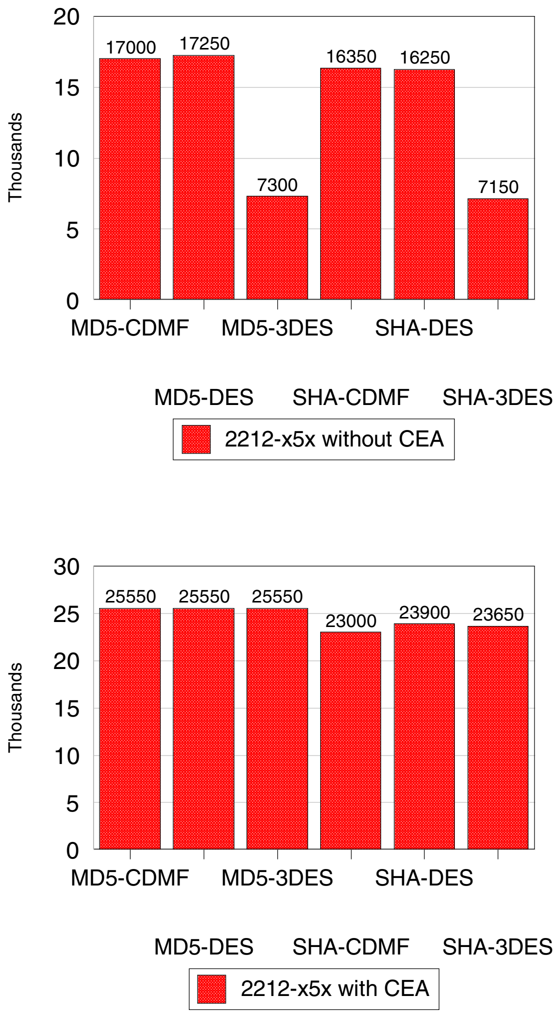


Figure 450. 2212-x5x IPSec capacity

The new 2212 Model x5x can support a maximum of 17250 Kbps of WAN throughput at 95% CPU utilization when using MD5 with DES. Adding the new CEA adapter increases the maximum throughput to 25550 Kbps.

Note

Testing was done in the IBM Network Hardware Division Performance Lab using commonly available traffic generating and measuring tools to simulate customer client/server configurations. Your real-world performance results may vary from the data in this report due to performance characteristics of the client/server devices and/or LAN/WAN networks. For more information related to 2212 performance, refer to `http://www.networking.ibm.com/2212/2212perf.html`. This Web page also includes IBM Nways router performance data related to DLSw, APPN,

Part 3. VPN scenarios based on MRS/MAS Versions 3.1 and 3.2

Chapter 23. Configuring IPSec with IBM Nways routers

This chapter explains how to manually configure IPSec tunnels using Nways Multiprotocol Routing Services (MRS) and Nways Multiprotocol Access Services (MAS) V3.1 and V3.2. It also shows the relationship between IP filters and the IPSec feature and explains how IP filters are used by IPSec to direct traffic to and from IPSec tunnels. The chapter concludes with a brief discussion of adding default gateways and static routes to an IPSec configuration.

23.1 Manual IPSec tunnel configuration

The following steps are recommended when configuring a manual IPSec tunnel. However, depending on your current router configuration, some of these steps may be omitted. These steps are:

1. Define the router interfaces, the IP addresses and masks.
2. Add packet filters for the router interfaces that will serve as tunnel endpoints.
3. Enable the packet filters.
4. Create an IPSec tunnel endpoint at a router interface.
5. Enable the tunnel.
6. Save the configuration.
7. Restart the router.

Each of these steps is explained in the following sections. As an aid in understanding the different parameters used, we reference the sample network in Figure 451. The examples are based on configuring Router A in the network.

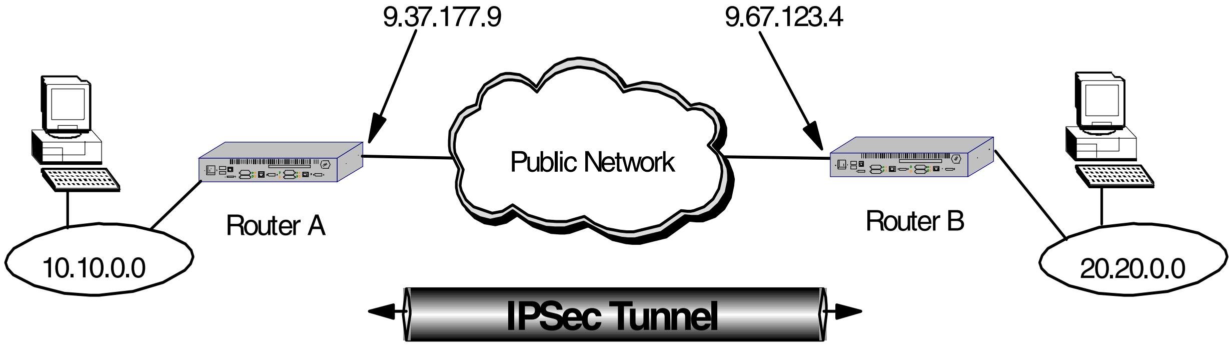


Figure 451. Sample network used in IPSec tunnel definition

23.1.1 Defining the router interfaces

The prerequisite for defining an IPsec tunnel is to configure your hardware interfaces, IP addresses and masks on each router interface that will serve as an IPSec tunnel endpoint. There are multiple ways to accomplish this using both the Config tool and the command line interface from the router console. These methods are not discussed in this redbook. However, Chapter 32, “Basic configuration with MRS/MAS V.3.1 and 3.2” on page 571 shows one way to do it using the Quick Config command dialog from the router console.

23.1.2 Packet filters and IPSec

A packet filter is a list of rules (called access controls) used by the router to control the processing of individual packets on an interface. You can define one packet filter for the inbound direction and one for the outbound direction for each interface on the router.

Two new types of access controls were added in MRS/MAS V3.1. Beginning with this version of code, there are now four types of access controls that can be specified in a packet filter. These are:

I - inclusive An access control of type I means that it is an inclusive filter. In this case, any matched packets will be allowed to proceed through the interface (either in or out depending on the direction of the filter defined.)

E - exclusive An access control of type E means that it is an exclusive filter. In this case, any matched packets will be dropped from the interface.

S - inclusive This is one of the two new access controls defined in MRS/MAS V3.1. When a match is encountered on an S filter, the packet is passed to the IPSec engine for processing by the AH and ESP protocols.

N - inclusive This is the other new access control defined in MRS/MAS V3.1. When a match is encountered on an N filter, the packet is passed to the network address translation (NAT) function for processing.

You can specify multiple access controls on each packet filter. The order of the controls in the access control list is very important because the first access control that is matched is the one that is acted on. In the case of IPSec, this is especially important for transport mode tunnels. (See , “Adding access controls” on page 442 for more information.)

23.1.2.1 How IPSec uses packet filters

The IPSec architecture defines a Security Policy Database (SPD) that is used to determine which packets should be processed by IPsec. The IPSec implementation in the IBM Nways routers uses the packet filter function as the key element of the SPD. IPSec uses packet filters to *funnel* the packets into and out of the IPSec engine. Both inbound and outbound packet filters are used for this purpose although they work slightly differently in each direction. Figure 452 on page 441 shows conceptually how this process works for IP packets in the outbound direction.

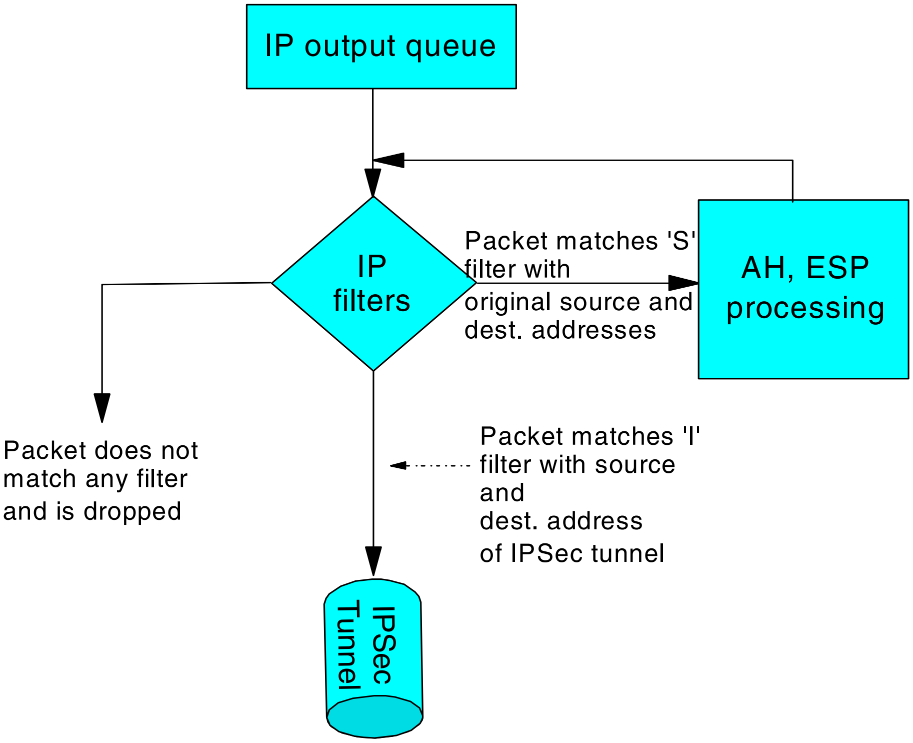

IP output queue
IP filters
Packet matches 'S' filter with original source and dest. addresses
AH, ESP processing
Packet does not match any filter and is dropped
Packet matches 'I' filter with source and dest. address of IPSec tunnel
IPSec Tunnel

Figure 452. IP Filters and IPSec - outbound traffic

As depicted in Figure 452, just before the outbound IP packets leave the router interface, they are tested by the packet filter for that interface. The packet is compared to each access control in the access control list (ACL) for the packet filter one by one. If a match is found on an S type access control, the packet is passed to the IPSec engine for AH/ESP processing.

After IPSec has processed the packet, it puts the packet back through the filters again. This time, the packet must match an inclusive access control (type I) in order for the router to send the packet out on the interface.

Note: As shown in the diagram, if a packet does not match any access control in the list, then the packet is dropped from the interface. This is the primary reason that the second access control is needed in the outbound direction.

23.1.2.2 Defining the packet filters

Defining a packet filter is a two-step process. First, you create the packet filter and give it a name. Then, you add access controls to the access control list for that packet filter.

A suggested naming convention for the packet filters is PF_DIR_IFNUM where:

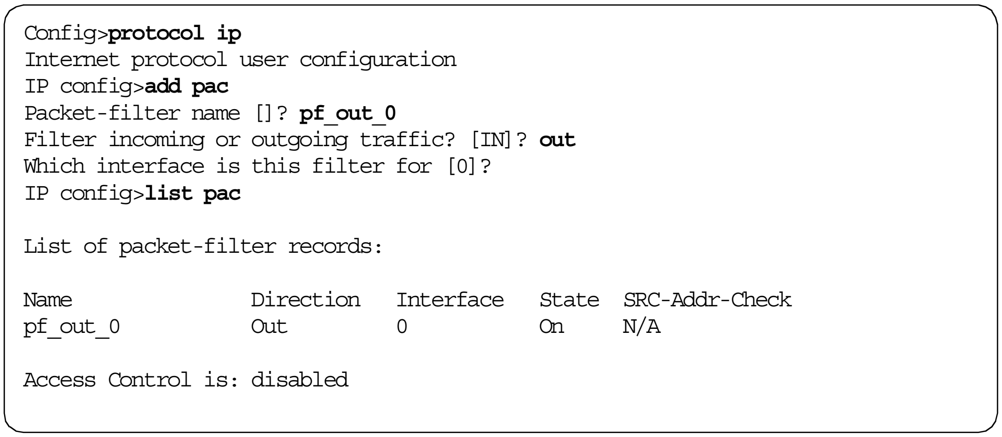
- PF stands for packet filter.
- DIR indicates the direction, either in or out.
- IFNUM is the interface number in the router.

For example, using this convention, a packet filter named PF_IN_0 would indicate an inbound filter on interface 0.

Creating the filters

You need to define a packet filter for each direction (inbound and outbound) for each interface that will serve as an IPSec tunnel endpoint. Figure 453 on page 442 shows the `Talk 6` command to create a packet filter as well as the command to list the defined packet filters. Note that these commands are issued from within the IP configuration prompt.

> **Note**
>
> The screens in this example show the prompts for configuring packet filters based on a pre-GA version of MRS V3.1. The prompts changed slightly before the the product shipped and they changed again for V3.2. Therefore, depending on the level of code that you are running, your command prompts may look slightly different than the ones shown here. However, the intent of the questions remain consistent with the prompts shown in this example.



```
Config>protocol ip
Internet protocol user configuration
IP config>add pac
Packet-filter name []? pf_out_0
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]?
IP config>list pac

List of packet-filter records:

Name              Direction   Interface   State  SRC-Addr-Check
pf_out_0          Out         0           On     N/A

Access Control is: disabled
```

Figure 453. Creating a filter

Notes:

1. In MRS/MAS Version 3.1, a new feature of packet filters was added called Source Address Verification. If enabled, this feature checks to see if the source IP address of the packet matches the subnet for the router interface that the packet is arriving on. If not, the packet is discarded. This helps to block hacking attempts. It is only valid for inbound filters and that is why you see the N/A (not applicable) under the column marked SRC-Addr-Check.
2. Note that when the packet filter is first created, it is *not* enabled. It only becomes active after you enable access control on the router and enable the individual packet filter. (See 23.1.4, “Enabling packet filters” on page 448.)
3. You cannot change the name of the filter without losing the details of the access control list. Therefore, be careful when choosing your names for the packet filters.

Adding access controls

Once the packet filters have been created, you add access controls to the access control list of the packet filter. Each filter needs two access controls in the list:

- For a tunnel mode IPSec tunnel, one of the controls specifies the source and destination IP addresses of the tunnel endpoints as well as the IPsec protocols (50 for ESP and 51 for AH). It is a type I (inclusive) control. When this access control is matched on an outbound packet, the packet is allowed to exit the router interface.

- The other access control specifies the network or host IP address(es) that are "funneled" into/out of the tunnel. Its type is S for IPSec. When this access control is matched on an outbound filter, the packet gets sent to the IPSec engine for processing of the AH and ESP protocols.

As stated previously, the order of the controls in the list is important - especially for transport mode tunnels. For example, as can be seen in Figure 452, for outbound packets, the first access control that you want the packet to encounter is the type S control. This is necessary so that the packet can be processed by IPSec and the appropriate headers added to the packet before it exits the router.

With transport-mode tunnels, the original IP packet header is used and source and destination IP addresses of the packet, as it traverses the tunnel, are those of the end systems and not the IPSec tunnel endpoints. Therefore, the I access control specifies the same source and destination IP addresses as the S control. In this situation, the only way to distinguish packets that have been through IPSec processing is by using the protocol field which will either be 50 or 51, depending on whether you are doing ESP or AH, respectively.

Figure 454 on page 443 shows the creation of the first of two required access controls. In order to add an access control, the update packet-filter command is issued first and then the add access-control command is used to create the individual access controls for that packet filter. In this case, this access control specifies the tunnel endpoints as source and destination IP addresses for the filter and the IPSec protocols 50 and 51. (See Figure 451.) This access control is used to allow IPSec packets to exit the router after they have been processed by IPSec and encapsulated (tunnel mode tunnels) with the new IP header.

```
IP config>update pac
Packet-filter name []? pf_out_0
Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 9.37.177.9
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 9.67.123.4
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging?(Yes or [No]):
Packet-filter 'pf_out_0' Config>
```

Figure 454. Adding an access control to a packet filter

Figure 455 on page 444 shows the addition of the second IPSec required access control to the outbound filter. This control specifies the network or host IP address(es) that will be *funneled* into the IPSec tunnel. Referring to Figure 451, these subnetwork addresses are the token-ring segments that are attached to each router and represent the private intranet segments that we are trying to connect using our VPN. When this access control is matched, the outbound packets are directed to the IPSec engine for AH and ESP processing. Note that for this access control, the protocol field and the port numbers are not specified because we want *all* protocols to be processed by IPSec and sent through the tunnel.

The tunnel ID specified needs to match the ID that will be specified during the creation of the IPSec tunnel. (See 23.1.5, “Defining the IPSec tunnel” on page 449.)

```
Packet-filter 'pf_out_0' Config>add access-control
Enter type [I]? S
Internet source [0.0.0.0]? 10.10.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 20.20.0.0
Destination mask [255.255.255.255]? 255.255.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 100
Enable Logging(Yes or [No]):
Packet-filter 'pf_out_0' Config>
```

Figure 455. Adding the second access control to the packet filter

This completes the definition of the outbound packet filter and the two IPSec required access controls.

23.1.3 Defining the inbound packet filter

In addition to the outbound filter, you must also define a packet filter for the inbound direction. Like the outbound filter, the inbound filter needs two access controls. However, the purpose of the access filters is slightly different for the inbound direction. Figure 456 on page 445 shows conceptually how this process works for IP packets in the inbound direction.

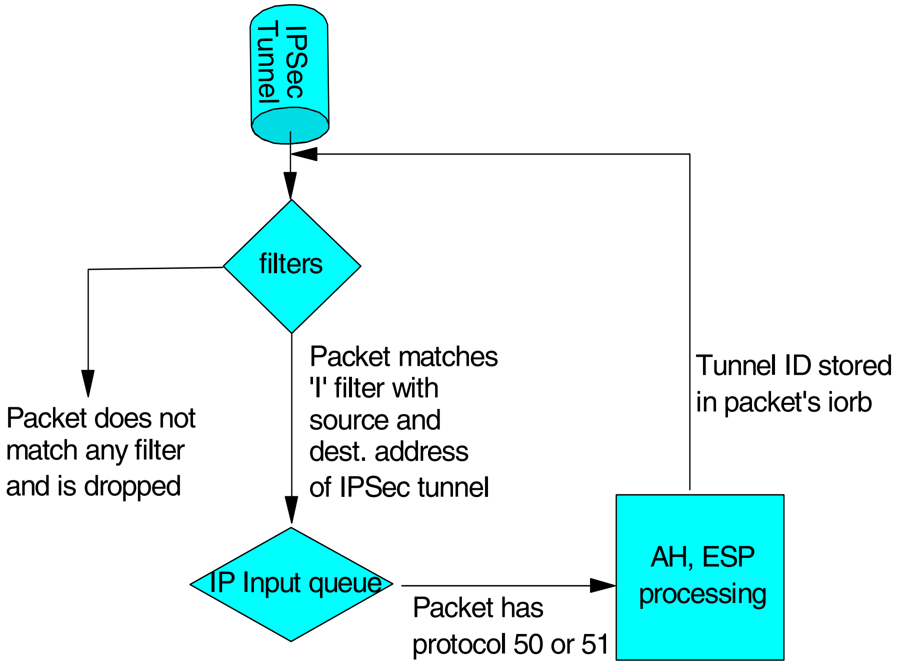

IPSec Tunnel
filters
Packet does not match any filter and is dropped
Packet matches 'I' filter with source and dest. address of IPSec tunnel
Tunnel ID stored in packet's iorb
IP Input queue
Packet has protocol 50 or 51
AH, ESP processing

Figure 456. IP filters and IPSec - inbound traffic

As packets come into the interface, the process that was used in the outbound direction at the ingress of the IPSec tunnel needs to be reversed. As can be seen in the figure, we want the packet to first match an access control of type I with source and destination addresses of the IPSec tunnel endpoints. (Remember that when using IPSec in tunnel mode, the packets get encapsulated with a new IP header. The source and destination addresses that get put into this new header are the tunnel starting and ending points.)

This control also specifies IPSec protocols 50 and 51, but for the purpose of checking to make sure they are really IPSec packets - not so that they can be routed to the IPSec engine. The packets get routed to IPSec by the protocol demux logic when that function sees that they have a protocol field of 50 or 51. This works exactly the same way as a TCP or UDP packet gets routed to the TCP or UDP code.

When the packet is passed to IPSec, the AH and ESP headers are processed, the packet is authenticated and/or decrypted and the tunnel ID is stored in the packet's iorb. The packet is then sent back through the filters - the same as it works for the outbound direction. Figure 457 on page 446 shows conceptually how the packet is processed the second time through the filters.

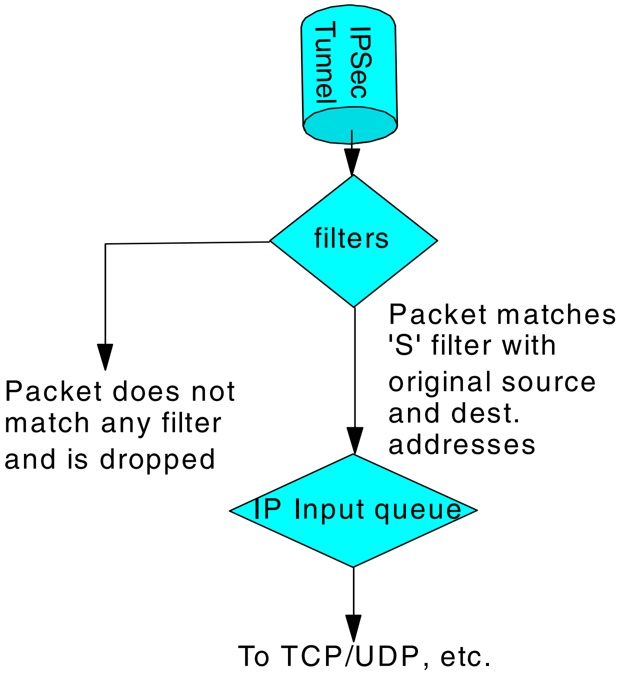

IPSec Tunnel
filters
Packet does not match any filter and is dropped
Packet matches 'S' filter with original source and dest. addresses
IP Input queue
To TCP/UDP, etc.

Figure 457. The second time through the inbound packet filter

This time, the packet needs to match a control of type S. When this occurs, the filter checks the tunnel ID that was received with the IPSec packet against the ID that was configured in the access control. These two tunnel IDs have to match or the packet is dropped. If they match, the packet is allowed to proceed to either the local IP queue (if the decapsulated packet is for local services such as TCP) or is routed to another interface (if the packet is not for local services).

23.1.3.1 Changing access controls in a packet filter

There are several other useful commands that can be used to modify a packet filter once it has been created. One gives you the ability to modify the data on the access control. Another command gives you the ability to change the order of the controls in the access control list. Finally, there is a command to delete an access control from the list. These commands are described in the following sections.

Modifying the data

To modify the data in an access control, first issue the update command for the packet filter, then issue the change command. This is illustrated in Figure 458 on page 447, Figure 459 on page 447, and Figure 460 on page 448. First the update command is issued followed by the list command to see the current access controls that are in the list.

```
IP config>update pac
Packet-filter name []? pf_out_0
Packet-filter 'pf_out_0' Config>list acc
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=9.37.177.9       Dest=9.67.123.4       Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535      Log=No

2   Type=I     Source=10.10.0.0        Dest=10.20.0.0        Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
               ACK0=N  T/C= **/**      Log=No
```

Figure 458. Listing access controls on a packet filter

Then the change command is issued to change one of the controls. Here, we change the type from an ordinary inclusive control to an IPSec control. Note that one of the parameters for an S control is the IPSec tunnel ID. This parameter is not necessary for an ordinary inclusive control.

```
Packet-filter 'pf_out_0' Config>change acc
Enter index of access control to be changed [1]? 2
Enter type [I]? S
Internet source [10.10.0.0]?
Source mask [255.255.255.255]?
Internet destination [10.20.0.0]?
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter Secured Tunnel ID [0]? 100
Enable Logging?(Yes or [No]):
Packet-filter 'pf_out_0' Config>
```

Figure 459. Changing an access control

Finally, the access control list (ACL) is redisplayed to make sure the change took effect. You can see that the type for control number two was changed from I to S.

```
Packet-filter 'pf_out_0' Config>list acc
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=9.37.177.9       Dest=9.67.123.4       Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=SI    Source=10.10.0.0        Dest=10.20.0.0       Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=100
                                       Log=No

Packet-filter 'pf_out_0' Config>
```

Figure 460. Verifying the change

Changing the order of access controls

You can use the `move access-control` command to change positions of the controls in the ACL. Figure 461 on page 448 gives an example of using this command.

```
2210 Packet-filter 'pf_out_0' Config>move access-control 4 1
About to move:

4   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
to be after:

1   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
Are you sure this is what you want to do(Yes or [No]): yes
2210 Packet-filter 'pf_out_0' Config>exit
```

Figure 461. Changing the order of the access controls in the ACL

Deleting an access control

To delete an access control, use the `delete access-control` command from within the `update-packet-filter` command.

23.1.4 Enabling packet filters

In order for the packet filter to be active, the access control function has to be enabled at the box level and each packet filter must be enabled by name. Figure 462 on page 449 shows an example of both of these commands which are self explanatory. Note that these commands are both issued from the Talk 6 IP config prompt.

```
IP config>set access-control on
IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_out_0
IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_in_0
```

Figure 462. Enabling access control and individual packet filters

It is a good idea to check to make sure that the filters are enabled. One way to verify that the filter is enabled is to use the update command for a packet filter and then list the access controls. This will tell you whether the access control is enabled for that packet filter. An example of this is shown in Figure 463:

```
IP config>update pac
Packet-filter name []? pf_out_0
Packet-filter 'pf_out_0' Config>list acc
Access Control is: enabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=9.37.177.9       Dest=9.67.123.4       Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=10.10.0.0        Dest=10.20.0.0        Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=100
                                       Log=No

Packet-filter 'pf_out_0' Config>
```

Figure 463. Checking that the packet filter is enabled

After making changes to the access controls, you need to reset IP to make the changes effective and also to clear the access control cache. However, in this example, we wait until the IPSec tunnel has been defined and then we perform a restart of the router. This activates both the changes to the filters and IPSec at the same time.

23.1.5 Defining the IPSec tunnel

This section describes the procedure to create the IPSec tunnel between two routers for a VPN over the public network.

Important note

This section assumes a working knowledge of the IPSec architecture. A basic explanation is given for each of the required parameters. However, if you are not familiar with the IPSec architecture, it is strongly recommended that you reference the companion redbook in this series entitled *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201 for more information.

IPSec tunnel configuration is performed from the IPSec feature menus under talk 6. For each IPSec tunnel, you give it a name, define the tunnel characteristics, and then enable the tunnel. While the dialog to add a tunnel is initiated with just one command, we have broken up the dialog into several pieces to provide some explanation at key points in the dialog.

The first part of the dialog defines the tunnel name, ID, tunnel lifetime, encapsulation mode, and tunnel policy.

```
RTR-A IPsec config>add tun
Tunnel ID (1-65535) [1]? 100
Tunnel Name (optional) []? ah_test
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH_ESP,ESP_AH) [AH_ESP]? AH
```

Figure 464. Defining the tunnel

Notes:

1. When you define the tunnel, you are defining two IPSec Security Associations (SAs), one in each direction. (Remember that an IPSec tunnel consists of two uni-directional security associations between the tunnel endpoints.)
2. The tunnel ID here must be the same as specified when the access control was created. (See Figure 455.)
3. Once created, the tunnel name cannot be changed.
4. The tunnel lifetime defaults to 46080 minutes which converts to 32 days. The maximum is 525600 minutes which is one year.
5. The tunnel encapsulation mode can be set to either tunnel mode or transport mode per the IPSec architecture. Tunnel mode is the normal case between routers that are using the public network to create a VPN. Transport mode is used to create a tunnel between two end stations.

   The difference between the two modes is that with tunnel mode, the entire original IP packet is encapsulated within a new IP packet. This new packet has IP source and destination addresses of the tunnel endpoints. With transport mode, the original IP header is used with the original source and destination IP addresses.
6. From Figure 464, you can see that there are four choices for the tunnel policy:

   AH This is the choice if you want to perform only authentication (the IPSec AH protocol) on packets going over this tunnel.

ESP This is the choice if you want to perform encryption (the IPSec ESP protocol) on packets going over this tunnel. Note that if you make this selection, you can also do authentication on the packets since the ESP protocol has an optional authentication feature.

AH_ESP This is the choice if you want to perform encryption and authorization using both the IPSec ESP and AH protocols. This selection indicates that for packets in the outbound direction, the packets will be encrypted first using the ESP protocol, then the AH algorithms will be run on the encrypted payload.

ESP_AH tunnel, defined This choice also allows you to do both encryption and authorization using both the IPSec ESP and AH protocols. However, the order is reversed. With this selection, packets in the outbound direction will go through the AH algorithms first, then they will be encrypted using the ESP protocol.

Take note

If you are ever trying to configure a tunnel policy and the only choice is AH, then you either don't have a code load with encryption or you are working on a 2216 where the `load add package encryption` command has not yet been specified. (Encryption is supplied as a separate load module for MAS and the `load add package encryption` command specifies that this module should be loaded as part of the normal IPL process.) This command only needs to be issued once.

At this point, the basic tunnel has been defined. Since we specified that this tunnel will use AH, the dialog now prompts us for the parameters that the AH algorithms will use. Figure 465 shows an example of these prompts.

```
Local IP Address [192.168.182.1]? 9.37.177.9
Local Authentication SPI (1-65535) [666]? 333
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
```

Figure 465. Defining AH parameters - local end of the tunnel

Notes:

1. This first series of prompts are for the AH parameters at the local end of the tunnel (the router you are configuring which is Router A in Figure 451 in this example). The parameters in local authentication must be the same as the parameters in remote authentication of the router at the other side of tunnel. For example, if you choose the HMAC-MD5 algorithm for the local authentication algorithm, then you must configure HMAC-MD5 as the other router's *remote* AH algorithm. In effect, you are defining parameters for two uni-directional security associations (SAs) and each tunnel endpoint must agree on the parameters used for each SA. (Remember that two SAs exist for each IPSec tunnel: one in each direction.)

2. You can use different parameters for the SAs in each direction. However, the parameters specified for each SA have to match at each end of the IPSec tunnel. For example:

   - The local key entered in router A must match the remote key entered in router B.
   - The remote key entered in router A must match the local key entered in router B.

   The same principle holds true for the SPI and the AH algorithm specified.

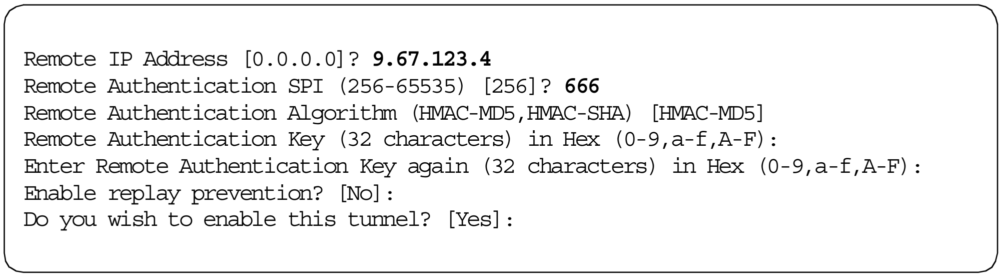
   With this said, however, we recommend that you use the same parameters for both SAs unless you have a good reason to do otherwise.

3. SPI is the security parameter index. You can think of this as an index into the database where the parameters for this tunnel will be stored.
4. In this version of MRS/MAS, we are using manual key configuration. This means that we manually enter the keys that will be used for the AH and ESP algorithms. We use simple keys in this example. In future versions of MRS/MAS, we will have the capability to use ISAKMP/Oakley, the automated key management protocols that will set the keys and refresh them periodically. The IPSec architecture specifies ISAKMP/Oakley as the protocols to use for its Integrated Key Exchange (IKE) framework.
5. In total, you have to enter four keys when configuring AH:

   - Local key in router A
   - Remote key in router A
   - Local key in router B
   - Remote key in router B

6. Also remember that each of the above keys must be typed twice to prevent mistakes. At the time of this writing, any typing mistakes will terminate the add tunnel command and you must start over.

After these parameters have been entered, the prompts switch to questions about the AH parameters for the remote end of the tunnel. As you might expect, the parameters entered for remote authentication must match parameters entered for local authentication of the router at the other side of the tunnel. For example, if you specify at the far end that outgoing packets should use the HMAC-MD5 algorithm to generate the Integrity Check Value (ICV), then you need to specify that incoming packets here at this end of the tunnel will be authenticated using the same HMAC-MD5 algorithm (and the same key). This is the idea behind configuring the parameters used at the remote end here at the local end of the tunnel. Figure 466 shows an example of these prompts:



```
Remote IP Address [0.0.0.0]? 9.67.123.4
Remote Authentication SPI (256-65535) [256]? 666
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
```

Figure 466. Defining AH parameters - remote end of the tunnel

The IPSec architecture defines a technique for ensuring that a hacker cannot intercept a datagram and play it back at some later time without being detected. This is called anti-replay or replay prevention support. As per the architecture, MRS/MAS implements this support using a sequence number that is included in the AH header of every packet. If enabled, the receiving side of the SA checks all sequence numbers on incoming packets to make sure that they fall within a window and have not been received previously. The sequence number is a 32-bit field in the header and is initialized to zero at the inception of the SA.

For manual IPSec implementations such as MRS/MAS V3.1 and V3.2, it is not recommended to enable anti-replay support. This is due to the fact that the architecture stipulates that the sequence number cannot wrap when it reaches the highest number in the range (2^{32}=4.29 billion packets). This means that if you enable anti-replay support, you have to ensure that the SA is re-established every 4.29 billion packets. When MRS/MAS implement ISAKMP/Oakley, there will be automated ways to refresh the SAs and hence this will not be a restriction.

After the tunnel definition is completed, you can list the definition back out to check for errors such as incorrectly typed IP addresses. Figure 467 shows an example of this command.

```
IPsec config>list tunnel all

   ID        Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
    100  ah_test          9.37.177.9       9.67.123.4       TUNN   Enabled
```

Figure 467. Listing a tunnel definition

23.1.6 Enabling IPSec on the router

IPSec must be enabled in order for the tunnel to become active. Figure 468 on page 453 shows an example of this command which is performed from the Talk 6 IPSec feature prompt. As the figure shows, you can check the status of IPSec and the status of each tunnel with the list all command.

```
IPsec config>enable ipsec
IPsec config>list all

IPsec is ENABLED

   ID        Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
    100  ah_test          9.37.177.9       9.67.123.4       TUNN   Enabled
```

Figure 468. Listing the IPSec status

Whenever you make a change to an IPSec tunnel (or add a new definition), you need to reset the IPSec feature to make the changes effective. However, in this example, we restart the router in the next step which both resets IPSec and also activates the changes to the access controls that we made in 23.1.3, “Defining the inbound packet filter” on page 444.

23.1.7 Saving the configuration

Now that the tunnel has been created, you need to save the changes to the configuration and reload (2216) or restart (2210) the router. This will activate both the changes to the access controls and to the IPSec feature.

The procedure to do this is slightly different for the 2210 and the 2216.

If you are using a 2210, the configuration is automatically written to the CONFIG area in Flash memory as you make the configuration changes. Therefore, you do not have to explicitly perform a save operation.

If you are using a 2216, you need to write the configuration to the hard disk to save it. An example of this operation is shown in Figure 469 on page 454.

```
Config>write
Config Save: Using bank A and config number 2
```

Figure 469. Saving the Configuration on a 2216

23.1.8 Restarting the router

Next, restart the router to make the configuration changes active. On a 2216, use the reload command as shown in Figure 470:

```
Config>reload
Are you sure you want to reload the gateway? (Yes or [No]): y
```

Figure 470. Restarting the 2216

On the 2210, use the restart command as shown in Figure 471. Note that this command is performed from the main router prompt. (Press <CNTRL><P> to get to this prompt.)

```
*restart
Are you sure you want to restart the gateway? (Yes or [No]): y

Copyright Notices:

Licensed Materials - Property of IBM
Multiprotocol Routing Services
(C) Copyright IBM Corp. 1996
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.

MOS Operator Control

*
```

Figure 471. Restarting the router (2210)

23.1.9 Defining an IPSec tunnel using encryption (ESP)

The procedure for configuring a tunnel that uses ESP is very similar to that for creating a tunnel with the AH protocol. However, instead of defining parameters that relate to the AH protocol, you define parameters for the ESP protocol, for example, the encryption algorithm.

Important note

Encryption is an optional feature in MRS/MAS. If your software load does not include encryption, you will not see encryption related parameters when configuring the IPSec feature.

Also, on the 2216, the encryption load module must be specified to be loaded during the IPL of the router. You specify this using the `load add package encryption` command.

We illustrate the configuration of an ESP tunnel below by changing the tunnel configuration that we created in 23.1.5, “Defining the IPSec tunnel” on page 449 to specify ESP instead of AH. We use the "change tunnel" command to make these changes to the existing tunnel configuration. As in the AH example, we break up the dialog into several figures to provide some explanation of the parameters. Figure 472 on page 455 shows an example of these prompts.

```
RTR-A IPsec config>chan tun
Tunnel ID or Tunnel Name []? 100
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH]? esp
```

Figure 472. Changing an IPSec tunnel definition

Like AH, ESP configuration requires parameters for the local and remote ends of the tunnel. First, you are prompted for the parameters for the local end. Also like AH, the parameters for the local end must be the same as the parameters in the other router's remote parameters.

Like AH, there are four keys to configure. However, as mentioned previously, the IPSec ESP protocol does allow you to do authentication as part of ESP processing. If you specify to do authentication as part of ESP, then you will have to configure additional keys for the authentication. (See the last question in the dialog below.) Figure 473 on page 455 shows an example of these prompts.

```
Local IP Address [9.37.177.9]?
Local Encryption SPI (256-65535) [256]? 444
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

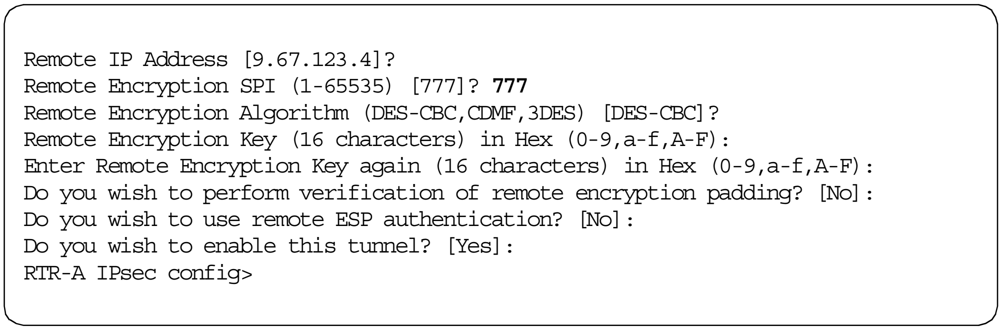
Figure 473. Defining the local ESP parameters

Depending on the country you are in, you may not have all the options shown above for the encryption algorithms. IBM is restricted by the U.S. Government in exporting Triple DES (3DES) and not all countries allow DES-CBC to be imported. For these reasons, there are different MRS/MAS loads with different encryption algorithms embedded that are used for export.

The additional padding feature can be used to extend the size of the ESP payload in order to help prevent a hacker from knowing the true size of the data being encrypted. You can specify up to 120 bytes of additional padding for each packet.

As mentioned previously, you can also specify to perform authentication as part of ESP processing. When you do authentication in ESP instead of AH, the coverage on the part of the packet that is authenticated is not quite as good as it is on packets that are authenticated with the AH protocol. When using ESP authentication, only the part of the packet from the ESP header to the ESP trailer gets authenticated. With AH authentication, the entire IP packet is authenticated. (Please see *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201 for more information.)

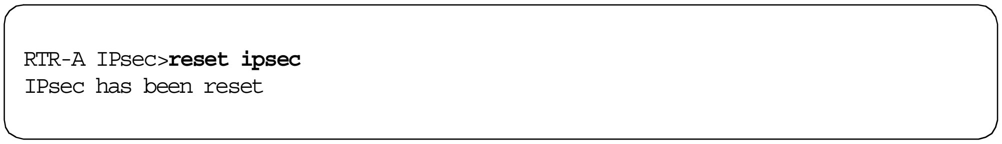
Next, you will define the parameters for the remote end of the tunnel. Again, the parameters entered here for the remote side must be the same as the parameters entered at the other router for its local encryption. Figure 474 shows an example of these prompts:



```
Remote IP Address [9.67.123.4]?
Remote Encryption SPI (1-65535) [777]? 777
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Do you wish to enable this tunnel? [Yes]:
RTR-A IPsec config>
```

Figure 474. Defining the remote ESP parameters

Now we need to reset the IPSec feature to activate the changes in the existing tunnel. This is performed from the Talk 5 IPSec menus. You do not have to reload or restart the router. Figure 475 shows how to do this.



```
RTR-A IPsec>reset ipsec
IPsec has been reset
```

Figure 475. Resetting the IPSec feature to activate changes

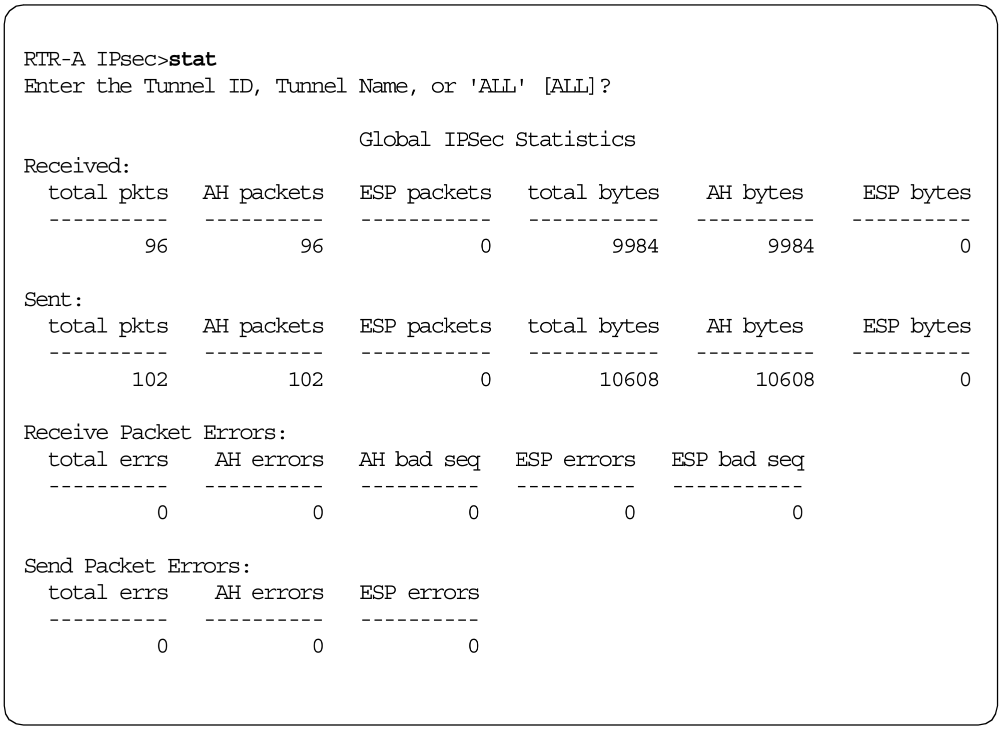
23.1.10 Monitoring status

You can monitor the status of the IPSec from the talk 5 menus. The `list tunnel active` command shows the information of active IPSec tunnels. You can specify to see a specific tunnel or you can see the information for all active tunnels. An example is shown in Figure 476 on page 457 for tunnel number 1. Note that this example shows the AH tunnel configured in 23.1.5, “Defining the IPSec tunnel” on page 449.

```
RTR-A >f ipsec
RTR-A IPsec>list tunnel active 1
Tunnel       Name        Mode   Policy   Life   Replay       Tunnel
  ID                                             Prev      Expiration
------  ---------------  -----  ------  ------  ------  ------------------
   100  ah_test          TUNN   AH       46080    No    15:40  Jul  6 1998

Local Information:
      IP Address: 9.37.177.9
  Authentication:  SPI:   333    Algorithm: HMAC-MD5
      Encryption:  SPI: -----    Encryption Algorithm: --------
                                 Extra Pad: ---
                                 ESP Authentication Algorithm: ----------
Remote Information:
      IP Address: 9.67.123.4
  Authentication:  SPI:   666    Algorithm: HMAC-MD5
      Encryption:  SPI: -----    Encryption Algorithm: --------
                                 Verify Pad?: ---
                                 ESP Authentication Algorithm: ----------
```

Figure 476. Listing tunnel information from talk 5

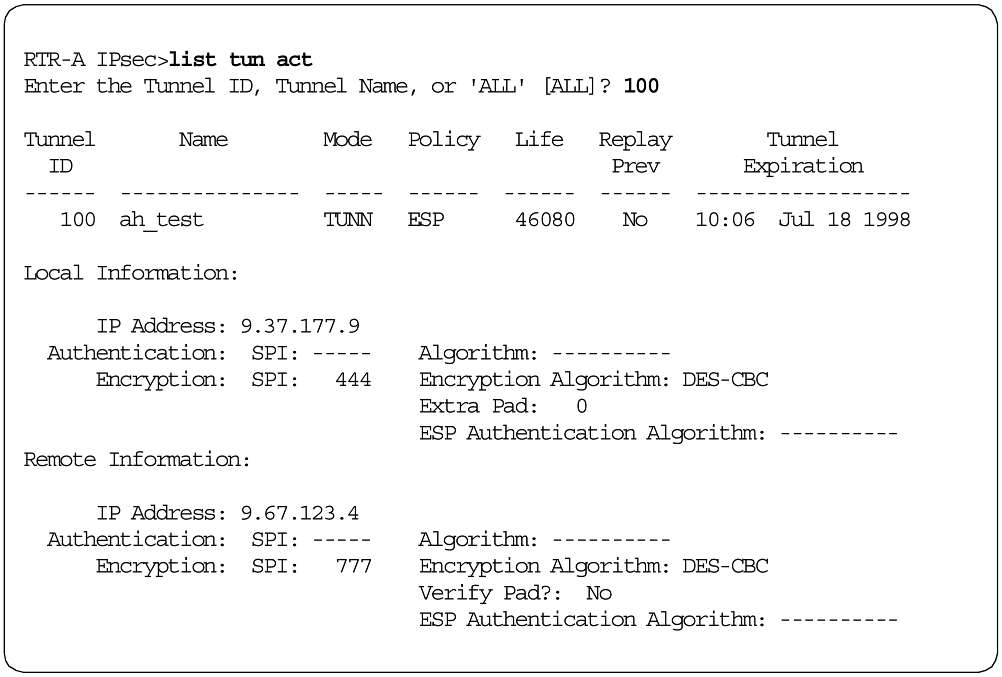
The `stat` command shows you the number of packets sent and received through IPSec. You can specify a tunnel name or number to see statistics for just one tunnel or you can get the global statistics for all the IPSec tunnels currently active in the router. Figure 477 on page 458 shows an example of listing the global statistics. In this case, there is only one tunnel defined - the same AH tunnel that was defined above.



```
RTR-A IPsec>stat
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          96           96             0          9984         9984            0

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         102          102             0         10608        10608            0

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0
```

Figure 477. Listing tunnel statistics

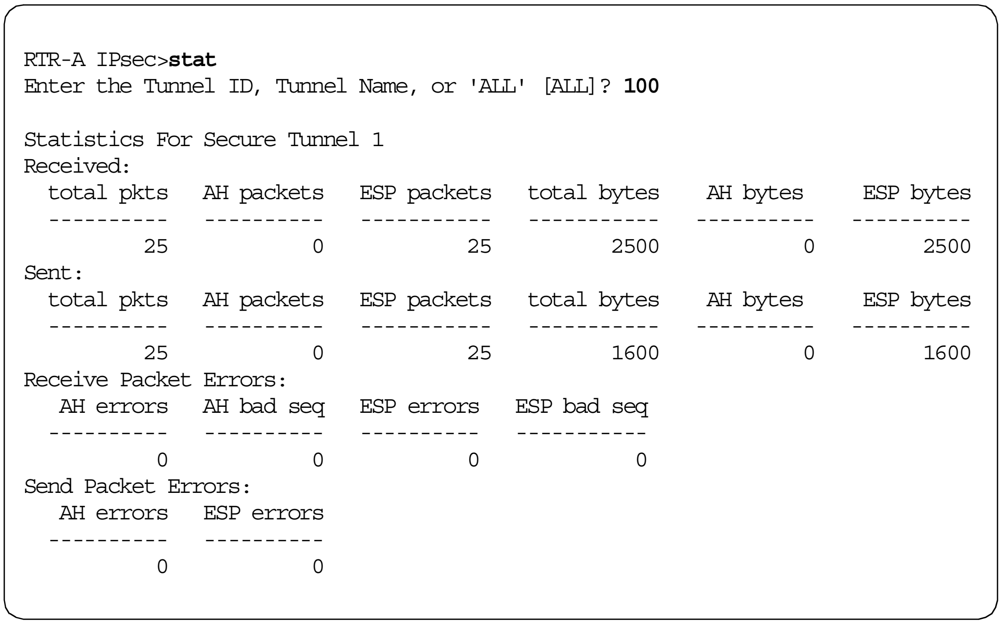
Figure 478 on page 458 shows an example of the `list tunnel active` command for an ESP tunnel.



```
RTR-A IPsec>list tun act
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 100

Tunnel       Name        Mode   Policy   Life   Replay        Tunnel
  ID                                             Prev       Expiration
------  ---------------  -----  ------  ------  ------  ------------------
   100  ah_test          TUNN   ESP      46080    No    10:06  Jul 18 1998

Local Information:

      IP Address: 9.37.177.9
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:   444    Encryption Algorithm: DES-CBC
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 9.67.123.4
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:   777    Encryption Algorithm: DES-CBC
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: ----------
```

Figure 478. Listing tunnel information from talk 5

Figure 479 on page 459 shows an example of the `stat` command for the same ESP tunnel in the previous figure. Note that in this case, tunnel 1 is an ESP tunnel and so there are statistics for ESP packets while there are no occurrences of AH packets reported.



```
RTR-A IPsec>stat
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 100

Statistics For Secure Tunnel 1
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          25            0           25          2500            0         2500
Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          25            0           25          1600            0         1600
Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0
Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0
```

Figure 479. Listing tunnel information from talk 5

Another important method of monitoring an IPSec tunnel is to check the packet filters at the tunnel endpoints to see how many times they have been invoked. The `packet-filter` command is used for this and is issued from the talk 5 IP prompt as shown in Figure 480 on page 460 for an example packet filter named pf_in_0.

Note: Figure 480 on page 460 is just an example screen and does not relate to the example IPSec tunnel defined in this chapter.

```
RTR-A IP>packet-filter pf_in_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_in_0           In   0     On     Off           3

Access Control currently enabled
Access Control facility: USER

Access Control run 1687 times, 9335 cache hits

List of access control records:

1   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=4
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=2
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=2
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
```

Figure 480. Displaying the number of invocations of an access control

The `Use=x` shows how many times each access control has been matched. If your filters are defined correctly, you should see these numbers increasing as traffic is being sent through the tunnel.

These counters are reset every time the router is IPLed or the IP protocol is reset.

23.2 IP routing considerations

When using a public network such as the Internet to create a VPN as illustrated in Figure 451, you will not be able to run a dynamic routing protocol between the routers at the endpoints of the IPSec tunnel.

Without setting any explicit routing, the routing code will route to any subnet that it is aware of based on the IP address and subnet mask specified at the physical interfaces. This means that the router knows how to route to IP addresses located within the subnets associated with its interfaces with no explicit configuration.

If the ultimate IP destination is not on one of the subnets on the router's interfaces then the router must obtain a route to the next-hop router. Since we cannot run RIP or OSPF over a public network, we have to either set a default gateway (all IP traffic that does not belong in an attached subnet is sent to the default gateway) or set static (explicit) routes.

If the router is the start of a tunnel, the next-hop router is either the IP address of the start of the tunnel, that is, an IP address on that router, or the IP address of the next router. Both approaches appear to work. However, it is recommended that the IP address of the next router be used.

23.2.1 Setting a default gateway

The router will send all traffic that is not destined to a subnet that is attached directly to the router to the default gateway. Figure 481 on page 461 shows an example of defining a default gateway.

```
Config>protocol ip
Internet protocol user configuration
IP config>set default network-gateway
Default gateway []? 2.2.2.2
gateway's cost [1]?
IP config>
```

Figure 481. Setting the default gateway

23.2.2 Setting static routes

The static route is the address of the next router (next hop) that a packet with a given IP address or a packet belonging to a particular subnet should be routed to. In the following example, all packets destined for network 4.4.4.X will be sent to the router whose address is 2.2.2.2. The router, knowing its own interface addresses and the subnets associated with each interface address, will determine which physical port to route the packet to. Figure 482 on page 461 shows an example of defining a default gateway.

```
IP config>add route
IP destination []? 4.4.4.0
Address mask [255.0.0.0]? 255.255.255.0
Via gateway 1 at []? 2.2.2.2
Cost [1]?
Via gateway 2 at []?
IP config>
```

Figure 482. Adding a static route

Now, to list the static routes that have been defined, use the `list` command as shown in Figure 483:

```
IP config>list routes

route to  4.4.4.0      ,255.255.255.0     via  2.2.2.2       cost 1

IP config>
```

Figure 483. Listing the static routes

Chapter 24. Connecting the data center to the branch office

As discussed in 1.5, “Common VPN scenarios” on page 15, one application of VPNs is in connecting branch office intranets to a central site (perhaps a mainframe data center) using a nonsecure public network such as the Internet. In this section of the redbook, we provide step-by-step procedures for implementing such a scenario using the IPSec feature of the IBM Nways 2210/2216 routers.

In this chapter, we configure a secure tunnel to establish basic TCP/IP connectivity between the branch office intranet and the central intranet located in the corporate data center.

Then, in subsequent chapters, we extend the configuration of the routers so that more protocols and features make use of the secure connection between the intranet sites. The following protocols and features are demonstrated:

1. DLSw for NetBIOS and SNA
2. Bridging tunnel for LAN-to-LAN bridging over TCP/IP
3. HPR over IP
4. APPN DLUR function
5. TN3270E server function

24.1 Description of the environment

Figure 484 on page 463 shows our configuration used to implement the scenario. As can be seen in the figure, the main intranet site consists of two Ethernet LAN segments, one token-ring, as well as a channel-attached S/390. The main site is connected to the Internet with an IBM 2216. The branch office intranet consists of a token-ring LAN and is connected to the Internet with an IBM 2210.

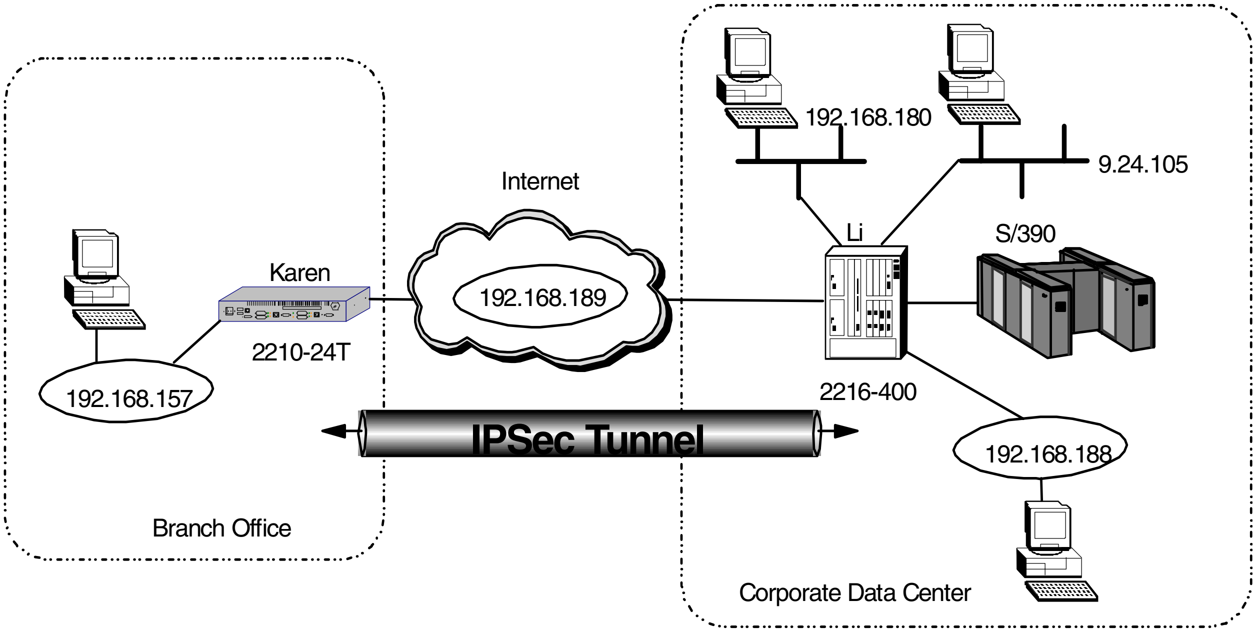


Figure 484. Branch office connection with a VPN

Note: In our laboratory environment we used a token-ring LAN as our nonsecure network. Hereafter, we refer to this nonsecure network as the "Internet" and to the interfaces of the 2210 and 2216 connected to this network as the "public interfaces". Most probably, your routers will be connected to the Internet using serial PPP or frame relay connections. This, however, does not change the basic steps to configure the IPSec tunnel between the routers. The routers just need IP connectivity for the tunnels.

The 2216 and 2210 have been named "Li" and "Karen" respectively. These host names are visible in the configuration screens so that you can easily distinguish which commands are for the 2216 and which for the 2210.

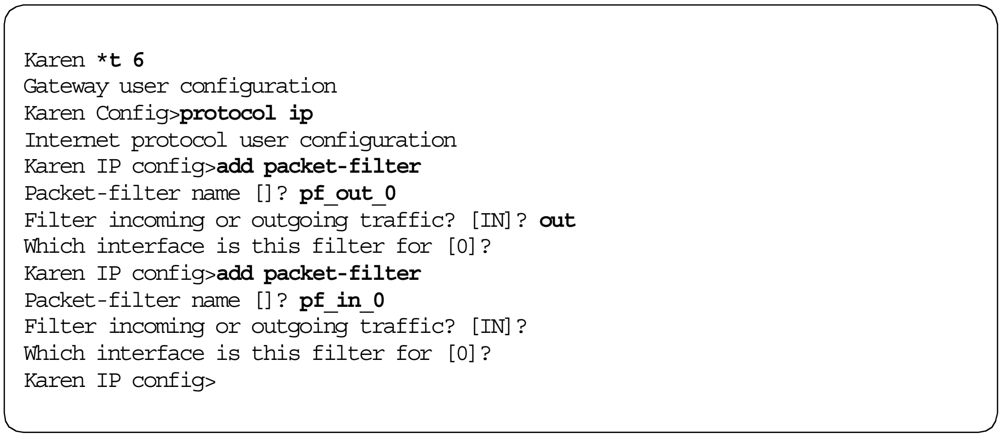
For testing purposes, we placed different kinds of clients and servers (FTP, telnet, HTTP, IPX and NetBIOS), APPN (HPR) network nodes, 3270 clients and an OS/390 host in both our intranet and Internet. The OS/390 host was connected to a channel adapter in the 2216 on the main site. In the scenario where we start using the host-connectivity a short example of the configuration of this connection is provided.

As discussed in 23.1.1, “Defining the router interfaces” on page 439, the prerequisite for defining an IPSec tunnel is to configure your hardware interfaces, IP addresses and masks on each router interface that will serve as an IPSec tunnel endpoint. Chapter 32, “Basic configuration with MRS/MAS V.3.1 and 3.2” on page 571 shows the quick config screens from when we configured the routers for the scenarios in this redbook.

24.1.1 Configuring the branch office router

In this section, we provide the configuration of the router in the branch office. The configuration of the router in the corporate site is discussed in 24.1.2, “Configuring IPSec at the data center” on page 476.

The first step is to create the packet filters on the interface that connects to the Internet (the public interface). This interface will be the endpoint of our IPSec tunnel at the branch office. We need to define two filters: one for out-bound traffic and one for in-bound traffic. We give each filter a name that corresponds to the function of the filter. For example, `pf_in_0` is the packet filter for the inbound traffic on interface 0 of the router. Figure 485 shows the `add packet-filter` commands used to create these filters for our scenario.



```
Karen *t 6
Gateway user configuration
Karen Config>protocol ip
Internet protocol user configuration
Karen IP config>add packet-filter
Packet-filter name []? pf_out_0
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]?
Karen IP config>add packet-filter
Packet-filter name []? pf_in_0
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]?
Karen IP config>
```

Figure 485. Creating the packet filter on the public interface (0)

Now, we have packet filters created, but we have not specified what criteria will be used to accept or reject packets. These *access controls* are added to the these newly-created packet filters using the `update` command followed by the `add access-control` command.

As discussed in 23.1.2, “Packet filters and IPSec” on page 440, the IPSec access control is used slightly differently between outbound and inbound packet filters. For outbound packet filters, a packet that matches an IPSec (type S) control is indeed sent to the IPSec engine, while for an inbound packet filter, the type S control is used after a packet leaves the IPSec engine and is used to verify the tunnel number.

The access controls in a packet filter will be evaluated on the packets in the order which they are listed. The first control that matches the packet will be executed. Thus, the packet will be accepted if it matches an inclusive control, dropped if it matches an exclusive control or sent to IPSec if it matches an S control. If no access control in the list matches the packet, it is dropped.

The order of the controls in the list is therefore very important. For example, if you add a new access control for a specific host in the Internet to communicate using a tunnel with your site and this access control is in the list after one that excludes any communication for all Internet hosts, then the new access control will never be used. You can use the `move access-control` command to change positions of the controls in the list and `delete access-control` to remove a control.

Figure 486 on page 465 shows the commands to add the first filter criteria for the outbound traffic (the traffic leaving our branch over the IPSec tunnel). This first control is an *IPSec* access control that specifies to funnel all packets with the following criteria to the IPSec engine for further processing:

- Source address of the 192.168.157 subnet in the branch office
- Destination address of the 192.168.180 subnet in the corporate site
- Any IP protocol

```
Karen IP config>update packet-filter pf_out_0
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.180.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>
```

Figure 486. Configuring the outbound packet filter on the branch router

The specification of tunnel number one in the access control says that all such traffic will be sent over IPSec tunnel number one. We will configure the tunnel later in this section after the configuration of the packet filters.

It is important to remember that we use a tunnel-mode IPSec tunnel for traffic coming from/going to one of our private subnets. Tunnel mode will hide these addresses from anyone on the Internet who might be trying to eavesdrop on the communication. Using tunnel mode means that the IPSec engine will encapsulate the original packet in a new IP packet with the IP addresses of the two routers.

After the packet has been processed by IPSec, it is passed back through the IP filters. It will now have an IP protocol number of 50 or 51 (for ESP and AH respectively). Thus we need to configure another access control in the outbound filter with the following criteria:

- A source address of the local side of the IPSec tunnel
- A destination address of the remote side of the IPSec tunnel
- An IP protocol field that indicates it is an IPSec packet (protocol 50-51)

Figure 487 shows the command used to define this control for our scenario.

```
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>
```

Figure 487. Configuring the outbound packet filter on the branch router

Later in our scenario, we create several configurations that involve router-to-router traffic that we also need to secure using IPSec. These include:

- Data Link Switching (DLSw)
- An IP bridging tunnel
- Enterprise Extender (HPR over IP)

With these types of traffic, you could either use tunnel-mode or transport-mode tunnels. Technically, with these types of traffic, the routers act as IP hosts. It is common practice to use transport-mode tunnels for host-to-host traffic because there is no need to camouflage the IP addresses in the original IP headers as is done with tunnel mode.

However, it is not required to use a transport-mode tunnel for router-to-router communication. We could use the same tunnel-mode tunnel that we use for communication between the intranet LANs.

There are trade-offs either way. If you use the existing tunnel-mode tunnel, you will create larger IP packets than is strictly necessary, since you add an IP header and trailer. On the other hand you keep your tunnel database smaller, thus reducing processing by the router. So you have to make a trade off between more overhead in your traffic (you will use more bandwidth) or more processing in your router (you will consume slightly more DRAM and processing power).

In our scenario, we chose a separate transport-mode tunnel for the router-to-router communication, since we only have two sites to connect to each other. Therefore, the next step is to add another access control of type S (IPSec) that is used to funnel the router-to-router traffic to IPSec for processing. The control will have the following criteria:

- Source address of the local router's internal address
- Destination address of the remote router's internal address
- All IP protocols are allowed

Figure 488 shows the commands used to define this control for our scenario.

```
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>
```

Figure 488. Configuring the outbound packet filter on the branch router

Since we chose to use a transport-mode tunnel, this is a different tunnel than the one we use to send the intranet traffic and so we specify a new tunnel ID (tunnel number 2) for this traffic. This tunnel is defined later in this scenario in 24.1.1.4, “Defining the IPSec tunnels” on page 472.

Next, we list the access controls for this packet filter. Figure 489 on page 467 shows this listing for our scenario.

```
Karen Packet-filter 'pf_out_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

3   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Karen Packet-filter 'pf_out_0' Config>exit
Karen IP config>
```

Figure 489. Listing the access controls

> **Important note**
>
> The position of the access controls is very critical here, especially the controls that specify the router-to-router IP addresses (controls 2 and 3). We have placed the most specific control (protocols 50-51) in front of the more generic control (all protocols). It has to be this way or the tunnel-mode IPSec packets will never leave the box.
>
> The transport-mode packets (HPR/IP packets for example) will not match access control number 2 but will match control number 3. They will get passed to IPSec for processing and then passed back through the filters where they will match control number 2 since they will then have a protocol field of 50 or 51.

This completes the definition of the packet filter for the outbound traffic.

24.1.1.1 Defining the inbound packet filters

Next, we need to add the access controls for the inbound traffic. Now that we have configured the outbound packet filter we understand what kinds of packets we can expect on the inbound traffic using the public interface. To start with, we will receive IPSec traffic from the other router; thus the first control is an *inclusive* control that specifies to accept all packets with the following criteria:

- A source address of the remote side of the IPSec tunnel
- A destination address of the local side of the IPSec tunnel
- An IP protocol field that indicates it is an IPSec packet (protocol 50-51)

Figure 490 on page 468 shows the commands to add this access control.

```
Karen IP config>update packet-filter pf_in_0
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>
```

Figure 490. Configuring the inbound packet filter on the branch router

Any packet that matches the criteria in the first filter gets passed to the IPSec engine in the router since this engine takes care of all traffic that is sent to the router with IP protocol 50 or 51.

Next, we add the access control that will accept traffic from the intranet segment(s) located at the central site. In this case, we specify that any packet from the 192.168.180 subnetwork that is destined for the 192.168.157 subnetwork should be allowed into our router. Thus the control has the following criteria:

- The source is the 192.168.180 subnet in the corporate site.
- The destination is the 192.168.157 subnet in the branch office.
- All IP protocols are allowed.

This is an S type control and we specify to use tunnel number 1 for this traffic. Figure 491 shows the commands used for our scenario.

```
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.180.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>
```

Figure 491. Configuring the inbound packet filter on the branch router

The next access control that we need for in-bound traffic for this interface is for the router-to-router traffic using the transport-mode tunnel. The control for this traffic has the following criteria:

- An S type control using tunnel number 2.
- The source address is the remote router's internal address.
- The destination address is the local router's internal address.
- All IP protocols are allowed.

Figure 492 shows the commands used to add this access control.

```
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>
```

Figure 492. Configuring the inbound packet filter on the branch router

Next, we list the access controls for this packet filter. Figure 493 shows the listing for our scenario:

```
Karen Packet-filter 'pf_in_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Karen Packet-filter 'pf_in_0' Config>exit
Karen IP config>
```

Figure 493. Listing access controls on the inbound packet filter

This completes the definition of the packet filters for the inbound traffic from the 192.168.180 subnet pictured in Figure 484.

24.1.1.2 Configuring additional subnets

To permit more subnets or hosts to use our tunnel-mode tunnel, we just need to add access controls of type S for the other combinations of source and destination hosts or subnets that need communication across the IPSec tunnel. Remember that we need an additional access control on both the inbound and outbound filters similar to those depicted in Figure 486 and Figure 491.

In this section, we add additional access controls in the inbound and outbound packet filters for communication between the other Ethernet LAN (the 9.24.105 subnet) in the corporate site and the token-ring LAN in the branch office. Figure 494 on page 471 and Figure 495 on page 471 show the commands to add the controls and to move them just after the other access controls for communication between the intranet LANs.

```
Karen IP config>update packet-filter pf_out_0
Karen Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 9.24.105.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_out_0' Config>move access-control 4 1
About to move:

4   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
to be after:

1   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
Are you sure this is what you want to do(Yes or [No]): yes
Karen Packet-filter 'pf_out_0' Config>exit
Karen IP config>
```

Figure 494. Adding and moving an access control for the outbound packet filter

```
Karen IP config>update packet-filter pf_in_0
Karen Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 9.24.105.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Karen Packet-filter 'pf_in_0' Config>move access-control 4 2
About to move:

4   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
to be after:

2   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No
Are you sure this is what you want to do(Yes or [No]): yes
Karen Packet-filter 'pf_in_0' Config>exit
Karen IP config>
```

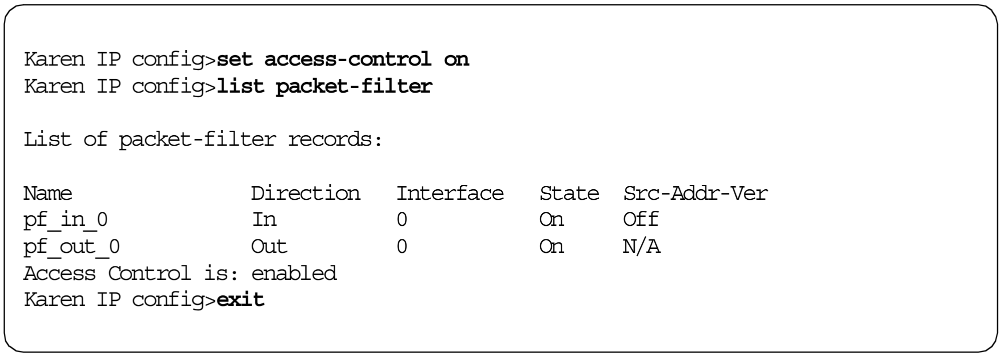
Figure 495. Adding and moving an access control for the inbound packet filter

24.1.1.3 Enabling access control and the packet filters

At this point, the packet filters and their corresponding access controls have been defined. However, they are not active until we globally enable access control on the router.

Figure 496 shows the command to enable access control at the box level. The list command is used to verify that access control has been enabled for the router.

Note: In addition to enabling access control at the box level, you can also enable/disable each packet filter individually. (The default state at creation time is enabled.) The list command also shows the state of each packet filter.



```
Karen IP config>set access-control on
Karen IP config>list packet-filter

List of packet-filter records:

Name             Direction   Interface   State  Src-Addr-Ver
pf_in_0          In          0           On     Off
pf_out_0         Out         0           On     N/A
Access Control is: enabled
Karen IP config>exit
```

Figure 496. Enabling access controls

24.1.1.4 Defining the IPSec tunnels

At this point, we have the correct packet filters and access controls defined and enabled but we have not yet defined the IPSec tunnels. The next few figures show the definition of the first tunnel.

Figure 497 on page 473 shows that a tunnel is defined from within the IPSec feature of the Talk 6 menus. The `add tunnel` command is used to create the tunnel and after this command you are prompted for all variables you need to set.

The first tunnel we create will be a tunnel-mode tunnel with id=1 and we have chosen to use AH-ESP as tunnel policy. As discussed in 23.1.5, “Defining the IPSec tunnel” on page 449, AH_ESP is the choice if you want to perform encryption and authorization using both the IPSec ESP and AH protocols. This selection indicates that for packets in the outbound direction, the packets will be encrypted first using the ESP protocol, then the AH algorithms will be run on the encrypted payload. We have chosen to use AH_ESP because we want both authentication and encryption to run. Also, we want the more complete authentication provided by the AH protocol which authenticates the complete packet, including the ESP and IP headers.

```
Karen Config>feature ipsec
IP Security feature user configuration
Karen IPsec config>add tunnel
Tunnel ID (1-65535) [1]?
Tunnel Name (optional) []? ESP&AH1
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 497. Defining the tunnel-mode IPSec tunnel on the branch router

Next, we are prompted to define the *local end* of the Security Association (SA). Figure 498 on page 473 shows the required parameters. The local algorithms are used on the outbound packets and the remote algorithms are used on the inbound packets. We input all SPIs to a value of 256, the AH algorithm is HMAC-MD5 and the Encryption algorithm is DES-CBC.

The local SPIs are the SPIs expected in inbound packets, and the remote SPIs are placed in the outbound packets. To prevent problems with remote and local SPIs and algorithms we advise you to use the same SPIs and algorithms on both sides.

It cannot be stressed enough that since your routers are connected to the Internet you have to take all measures within your ability to make them secure. Use strict rules which the keys must satisfy just as you probably have for passwords in your systems and networks. For example, change them periodically, use alphanumeric characters, and do not use a convention for creating your passwords (like using the IP address and/or host name in the key).

```
Local IP Address [192.168.189.59]?
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 498. Defining the tunnel-mode IPSec tunnel on the branch router

Note: The keys are not displayed while typed.

Next, we are prompted to define the *remote end* of the SA. Figure 499 shows the required parameters:

```
Remote IP Address [0.0.0.0]? 192.168.189.1
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Karen IPsec config>
```

Figure 499. Defining the tunnel-mode IPSec tunnel on the branch router

The next tunnel we create is the transport-mode tunnel for the router-to-router traffic. We specify an ID of 2 for this tunnel and we use AH-ESP again as the tunnel policy. The value of 257 is used for the SPIs, the AH algorithm is HMAC-MD5, and the 3DES algorithm is used for encryption. Figure 500, Figure 501 on page 474, and Figure 502 on page 475 show the configuration of this transport-mode tunnel.

```
Karen IPsec config>add tunnel
Tunnel ID (1-65535) [1]? 2
Tunnel Name (optional) []? TRANS-ESP&AH
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]? TRANS
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 500. Defining the transport-mode IPSec tunnel on the branch router

Next, we are prompted to define the local end of the SA.

```
Local IP Address [192.168.189.59]?
Local Authentication SPI (256-65535) [256]? 257
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [257]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]? 3DES
First Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 501. Defining the transport-mode IPSec tunnel on the branch router

Next, we are prompted to define the remote end of the SA.

```
Remote IP Address [0.0.0.0]? 192.168.189.1
Remote Authentication SPI (1-65535) [257]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [257]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [3DES]?
First Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Karen IPsec config>
```

Figure 502. Defining the transport-mode IPSec tunnel on the branch router

Next, we list the tunnels that we have created. Figure 503 on page 475 shows the command and output.

```
Karen IPsec config>list tunnel all

   ID        Name          Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      2  TRANS-ESP&AH     192.168.189.59   192.168.189.1    TRANS  Enabled
      1  ESPAH            192.168.189.59   192.168.189.1    TUNN   Enabled
Karen IPsec config>
```

Figure 503. Listing defined tunnels on the branch router

The last step is to enable IPSec on the router. Figure 504 on page 475 shows this command.

```
Karen IPsec config>enable ipsec
Restarting the router is required for IPsec to be active.
Karen IPsec config>exit
Karen Config>
```

Figure 504. Enabling IPSec

As the message from the router indicates, we need to restart the router so that the newly created IPSec tunnel will be activated.

```
Karen Config> <CTRL>+<P>
Karen *restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 505. Restarting the router

24.1.2 Configuring IPSec at the data center

Now we need to perform the same steps to configure the router Li at the corporate data center. The only differences are:

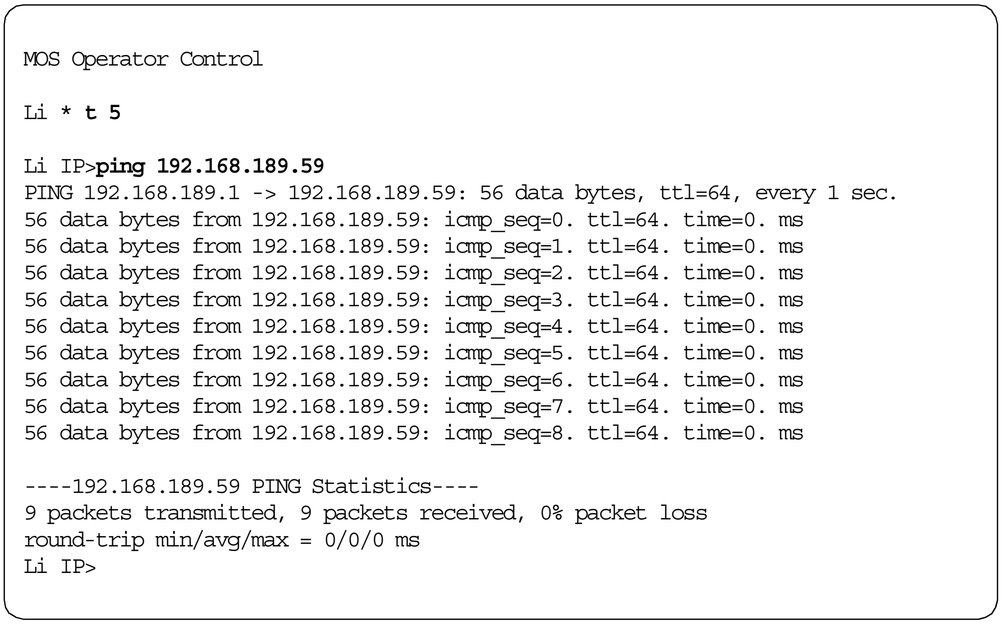
- The IP addresses in the filters and the tunnels will be swapped from those that we used for the branch router configuration.
- The parameters in the tunnel definitions will also be swapped. The values used for the remote end at the branch router are now the ones used for the local end at the data center router and vice versa. (However, for the most part, we used the same values for both the remote and the local end, so this is not a very big issue.)

For completeness, these screens are documented in Chapter 33, “Configuring IPSec with MRS/MAS V3.1/3.2” on page 585.

24.2 Monitoring and troubleshooting

In this section, we show a couple of useful commands to display statistics about the state and the use of tunnels and the packet filters. We only show the commands on the 2216 in our scenario. However, the commands and outputs on an IBM 2210 are exactly the same.

The first thing to check after the routers have been restarted with the new IPSec configuration is to make sure that you still have IP connectivity to the other side of the tunnel. In Figure 506 on page 477, you can see a ping command from the IP prompt in Talk 5 where nine pings from router Li to router Karen were sent.



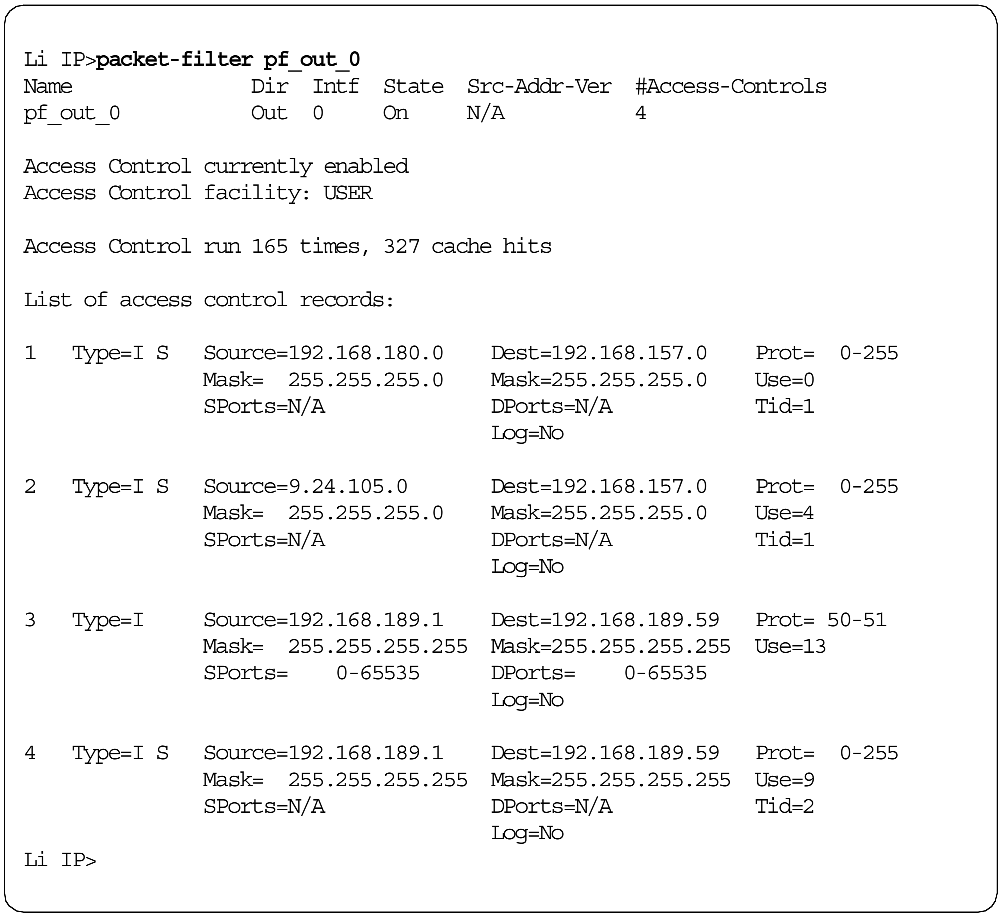
```
MOS Operator Control

Li * t 5

Li IP>ping 192.168.189.59
PING 192.168.189.1 -> 192.168.189.59: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.168.189.59: icmp_seq=0. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=1. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=2. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=3. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=4. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=5. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=6. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=7. ttl=64. time=0. ms
56 data bytes from 192.168.189.59: icmp_seq=8. ttl=64. time=0. ms

----192.168.189.59 PING Statistics----
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
Li IP>
```

Figure 506. Pinging the other side of the tunnel

In addition, we issued four pings from a station in the 9.24.105 subnet on the corporate site to a station in the 192.168.157 subnet in the branch office (not shown) to check end-to-end connectivity between the branch and the data center.

These pings not only check the connectivity through our tunnel, but they also generate some traffic that we can use to check our access controls to see how many packets matched each control. We look at the number for "use" in the last column of the output which tells us the number of times that the access control has been matched.

Figure 507 on page 478 shows the command and output for the outbound packet filter and you can see that access control number 2 was matched four times, which correlates to the four pings between the two intranet LANs. Control number 4 was matched nine times, which correlates to the nine pings between the routers. And since all pings are sent through an IPSec tunnel, we also see 13 matches for control number 3 for IPSec packets that are sent to the other router.



```
Li IP>packet-filter pf_out_0
Name               Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0           Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 165 times, 327 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=4
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=13
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=9
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 507. Showing the outbound packet filter

Figure 508 on page 479 shows the command for displaying the statistics of the inbound packet filter. Here we see similar statistics that have resulted from the packets that were echoed from the other router.

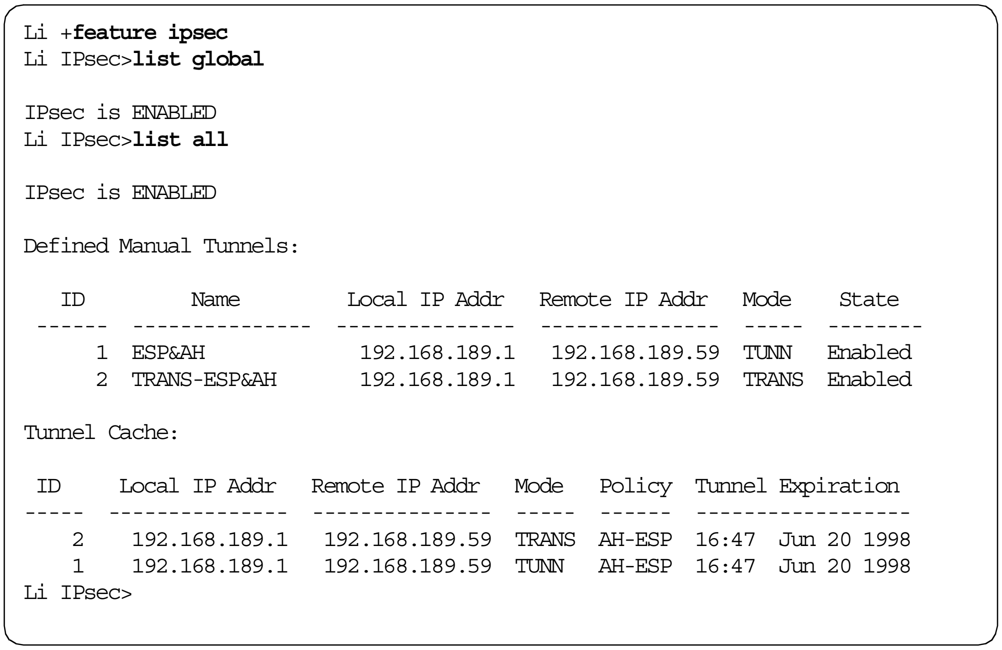
Note that access control number 1 is matched twice for each IPSec packet that enters the router from our ping command. This is a result of the way in which packets flow in the router. Tunnel-mode IPSec packets are matched twice because the access controls are checked just after the packet enters the interface and again after the destination is determined to be for the local queue (the router itself is the destination). Finally, in the case of the router-to-router pings, after the packet is decapsulated in the IPSec engine, it is passed through the filters again where it matches access control number 4. See 23.1.2, “Packet filters and IPSec” on page 440 for more information about the internal packet flow in the router.

```
Li IP>packet-filter pf_in_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_in_0           In   0     On     Off           4

Access Control currently enabled
Access Control facility: USER

Access Control run 507 times, 875 cache hits

List of access control records:

1   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=26
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=4
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

4   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=9
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>exit
Li +
```

Figure 508. Showing the inbound packet filter

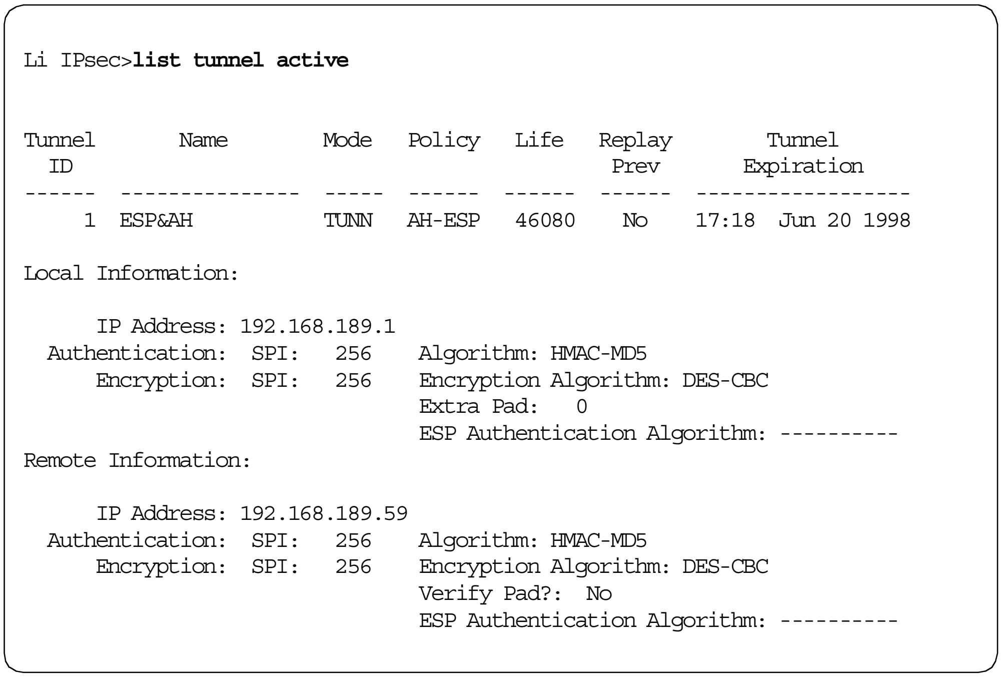
Other useful information regarding the IPSec tunnels can be obtained from the IPSec prompt in Talk 5. In Figure 509 on page 480, Figure 510 on page 480, and Figure 511 on page 481 we show several variations of the `list` command:

- `List global` displays the state of IPSec (enabled/disabled).
- `List all` displays the defined and active tunnels with details.
- `List tunnel active` and `list tunnel defined` display more details about active and defined tunnels.



```
Li +feature ipsec
Li IPsec>list global

IPsec is ENABLED
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID        Name        Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  ESP&AH            192.168.189.1   192.168.189.59  TUNN   Enabled
      2  TRANS-ESP&AH      192.168.189.1   192.168.189.59  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  AH-ESP  16:47  Jun 20 1998
    1    192.168.189.1   192.168.189.59  TUNN   AH-ESP  16:47  Jun 20 1998
Li IPsec>
```

Figure 509. Listing IPSec information



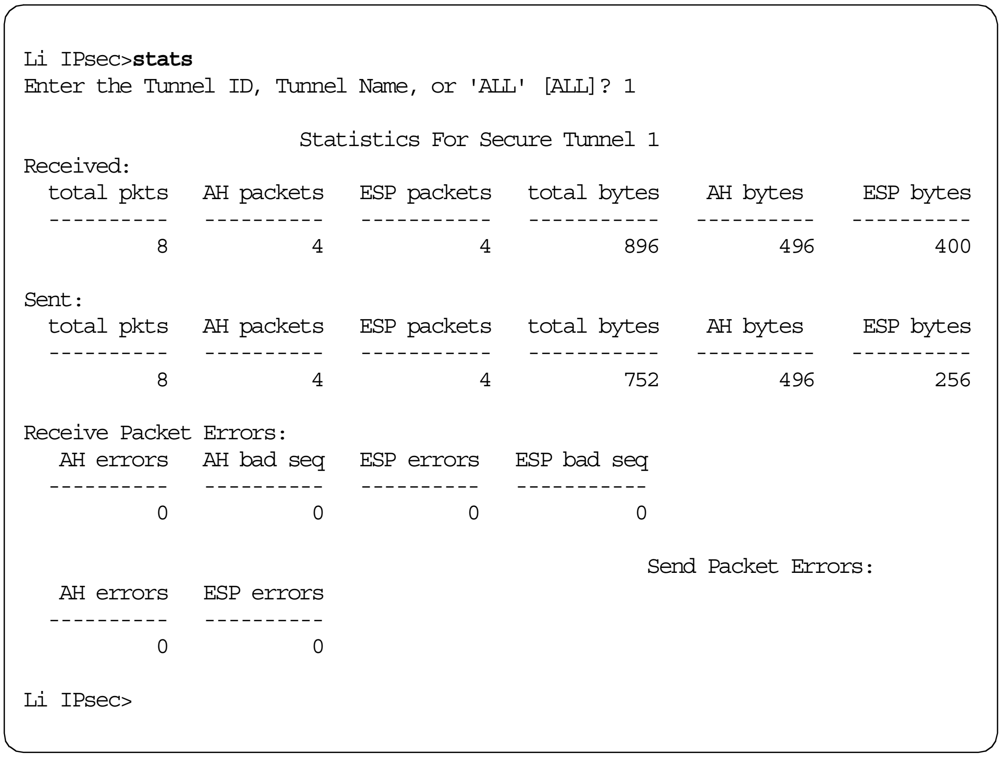
```
Li IPsec>list tunnel active


Tunnel       Name        Mode   Policy   Life   Replay       Tunnel
  ID                                             Prev      Expiration
------  ---------------  -----  ------  ------  ------  -----------------
     1  ESP&AH           TUNN   AH-ESP   46080    No    17:18  Jun 20 1998

Local Information:

      IP Address: 192.168.189.1
  Authentication:  SPI:   256    Algorithm: HMAC-MD5
      Encryption:  SPI:   256    Encryption Algorithm: DES-CBC
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 192.168.189.59
  Authentication:  SPI:   256    Algorithm: HMAC-MD5
      Encryption:  SPI:   256    Encryption Algorithm: DES-CBC
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: ----------
```

Figure 510. Listing active tunnels

```
Li IPsec>list tunnel defined
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

Tunnel        Name         Mode    Policy    Life    Replay    State
  ID                                                  Prev
------   ---------------   -----   ------   ------   ------   --------
     2   TRANS-ESP&AH      TRANS   AH-ESP    46080     No     Enabled

Local Information:

      IP Address: 192.168.189.1
  Authentication:  SPI:   257    Algorithm: HMAC-MD5
      Encryption:  SPI:   257    Encryption Algorithm: 3DES
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: ----------
Remote Information:

      IP Address: 192.168.189.59
  Authentication:  SPI:   257    Algorithm: HMAC-MD5
      Encryption:  SPI:   257    Encryption Algorithm: 3DES
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: ----------
Li IPsec>
```

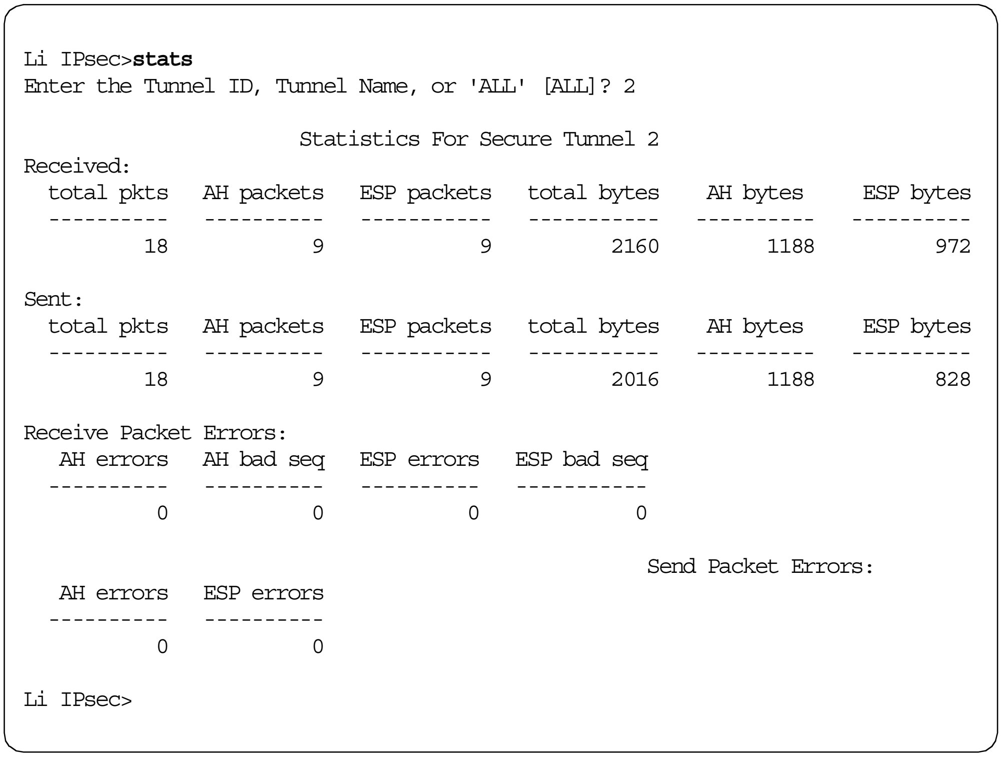
Figure 511. Listing defined tunnels

Another useful command from the IPSec prompt in Talk 5 is the `stats` command. This command gives some statistics about the packets handled by IPSec. Figure 512 on page 482 and Figure 513 on page 482 give the statistics for tunnel 1 and tunnel 2 respectively. In these, you can also see the four pings between the two intranet LANs over tunnel 1 and the nine pings between the routers over tunnel 2.



```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

                       Statistics For Secure Tunnel 1
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           8            4             4           896          496          400

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           8            4             4           752          496          256

Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

                                                    Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0

Li IPsec>
```

Figure 512. Showing IPSec statistics for tunnel 1



```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                       Statistics For Secure Tunnel 2
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          18            9             9          2160         1188          972

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          18            9             9          2016         1188          828

Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

                                                    Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0

Li IPsec>
```

Figure 513. Showing IPSec statistics for tunnel 2

Chapter 25. Data link switching over IPSec

Now that the IPSec tunnel is in place between the branch and the data center, we have the capability to securely route IP traffic between these two locations over our virtual private network. However, most enterprise environments today are not IP only networks. Therefore, to get the maximum utility of the tunnel, we need to add support for other protocols like SNA and NetBIOS.

DLSw is an IBM-invented standard technology for transporting connection-oriented protocols, mainly SNA and NetBIOS, across IP backbone networks. DLSw routers on the edges of an IP network process link establishment requests from native SNA and NetBIOS end stations, search among peer DLSw routers for one serving the target end station, then set up a path and relay application data between the end stations through the peer router.

With an IPSec tunnel defined between the routers, we can easily define a DLSw connection that uses this tunnel. This chapter describes the procedures for implementing a DLSw connection in a VPN environment using the IBM Nways 2210/2216 routers.

Note

This chapter assumes you are already familiar with DLSw. For more information on using DLSw, please see *IBM 2210 Nways Multiprotocol Router IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume II*, SG24-4956.

25.1 Configuring DLSw in an IPSec environment

We use the same configuration here as in Chapter 24, “Connecting the data center to the branch office” on page 463. We simply build on it to add the DLSw capability. Figure 514 on page 484 shows the network along with the DLSw related parameters.

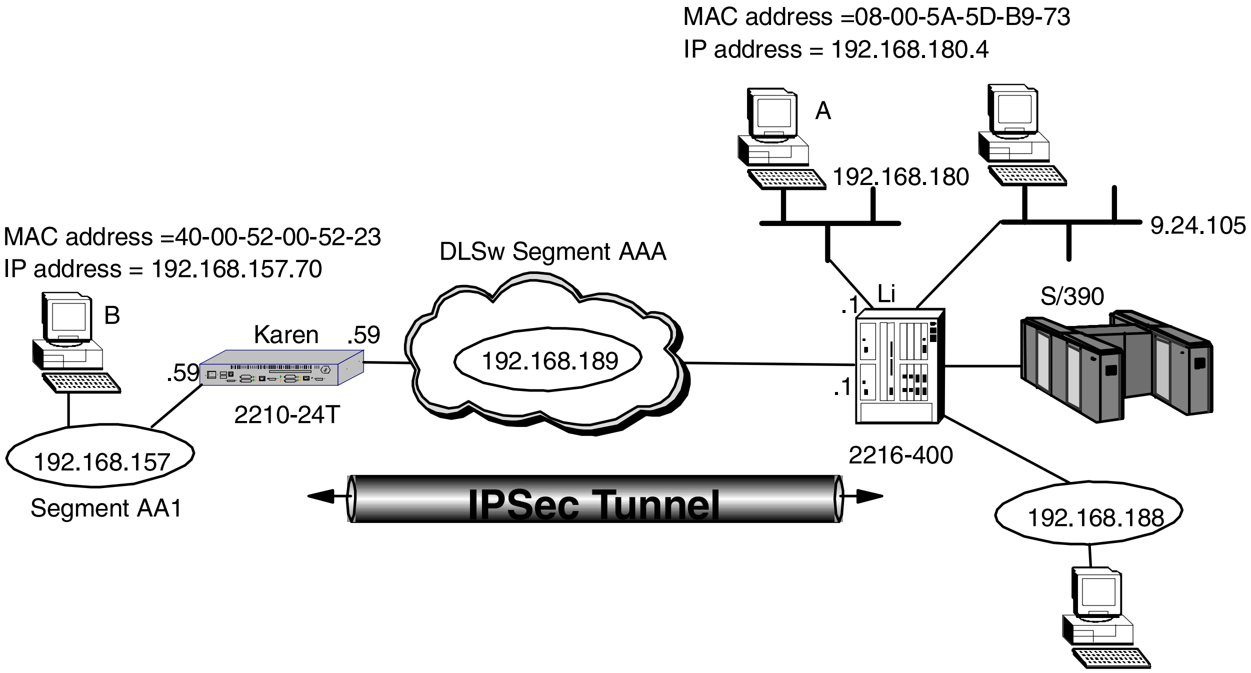


Figure 514. Data link switching through an IPSec tunnel

To configure DLSw in the VPN environment, we perform the following procedures:

1. Disable access control.
2. Disable IPSec.
3. Configure bridging.
4. Configure DLSw.
5. Enable access control.
6. Enable IPSec.

Each of these steps is explained in detail in the following sections.

25.1.1 Configuring the data center router

As a first step in adding DLSw to our configuration, we temporarily disable IPSec and access control. This allows us to define and test the DLSw configuration independently of any IPSec functions. After the DLSw configuration is working, we re-enable access control and IPSec.

Note: We recommend that you do this first in order to facilitate any problem determination that may be necessary while bringing up DLSw. Otherwise, if you do experience problems, it will be difficult for you to determine if the problem is in the DLSw configuration or if there is an IPSec problem such as a filter definition.

Figure 515 on page 485 shows the command used to disable access control. As can be seen from the figure, this command is executed from within the IP configuration in the talk 6 process.

Note: Figure 515 on page 485 also illustrates that after you disable access control, you must reset IP in order to make this change effective.

```
Li *t 6
Li Config>p ip
Internet protocol user configuration

Li IP config>set access-control off
Li IP config>exit
Li Config>
Li *t 5
Li +p ip
Li IP>reset ip
Li IP>exit
```

Figure 515. Temporarily disabling access control

Figure 516 shows the command to temporarily disable IPSec on the router. As shown in the figure, this is performed from within the IPSec feature configuration under talk 6.

Note: You can also disable IPSec from the talk 5 process, but like other changes made from talk 5, if you reload the router, this change will be lost and the IPSec function will be enabled when the router comes back up.

```
Li *t 6
Li Config>feature ip
IP Security feature user configuration
Li IPsec config>disable ipsec pass
Li IPsec config>exit
Li Config>
Li *
```

Figure 516. Temporarily disabling IPSec

Now we configure the bridging function. Here we disable the ports that we are not using in this configuration. For more information on configuring bridging, please see *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I*, SG24-4446.

```
Li Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Li ASRT config>ena bridge
Li ASRT config>ena dls
Li ASRT config>disa trans 1
Li ASRT config>disa trans 2
Li ASRT config>disa trans 3
```

Figure 517. Configuring ASRT on the data center router

Now we list the bridge configuration back out to verify that we made the correct changes. This is shown in Figure 518 on page 486.

```
Li ASRT config>list bridge
           Source Routing Transparent Bridge Configuration
           ===============================================
Bridge:                  Enabled                 Bridge Behavior: STB
+---------+-----------| SOURCE ROUTING INFORMATION |-----------+---------+
Bridge Number:           N/A                     Segments:          0
Max ARE Hop Cnt:         00                      Max STE Hop cnt:   00
1 : N SRB:               Not Active              Internal Segment:  0x000
LF-bit interpret:        Extended
+---------+----------------| SR-TB INFORMATION |---------------+---------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0
+---------+-------| SPANNING TREE PROTOCOL INFORMATION |----------+------+
Bridge Address:          Default               Bridge Priority:   32768/0x8000
STP Participation:       IEEE802.1d
+---------+-----------| TRANSLATION INFORMATION |-------------+---------+
FA<=>GA Conversion:      Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:      Enabled
+---------+---------------| PORT INFORMATION |----------------+---------+
Number of ports added: 4
Port: 1      Interface: 0      Behavior: No Bridging   STP:  Enabled
Port: 2      Interface: 1      Behavior: No Bridging   STP:  Enabled
Port: 3      Interface: 2      Behavior: No Bridging   STP:  Enabled
Port: 4      Interface: 3      Behavior:    STB Only   STP:  Enabled
```

Figure 518. Configuring ASRT on the data center router

Now we configure DLSw. This involves enabling it at the box level and also opening SAPs for the traffic that you want to carry across the DLSw connection. These steps are illustrated in Figure 519:

```
Li Config>p dls
DLSw protocol user configuration
Li DLSw config>enable dls
Data Link Switching is now enabled
Li DLSw config>set srb aaa
DLSw segment number has been set.
Li DLSw config>open-sap
Enter Interface number [0]? 3
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? sna
SAP(s)  0  4  8  C opened on interface 3
Li DLSw config>open-sap
Enter Interface number [0]? 3
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? nb
SAP(s) F0 opened on interface 3
Li DLSw config>list open
Interface SAP(s)
    3      0  4  8  C F0
```

Figure 519. Configuring DLSw on the data center router

Now we add the DLSw neighbor (the other end of the DLSw pipe). The neighbor DLSw IP address added here must be the internal IP address of the peer DLSw router. In our case, this is the router at the other end of the IPSec tunnel although it could be any router in the branch office that has a valid IP connection.

In our example, the internal address has been set to the interface address of the public network (our IPSec tunnel endpoint). This has an implication regarding the configuration of the packet filters for IPSec. DLSw packets have source and destination IP addresses of the TCP connection endpoints which are the internal addresses of the two routers at the endpoints. Our packet filters need to have access controls that enable these DLSw packets to get through the tunnel.

```
Li DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 192.168.189.59
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]? e
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been added
Li DLSw config>exit
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 4
```

Figure 520. Configuring TCP neighbors on the data center router

This completes the configuration of the data center router. As shown in Figure 520, you need to restart or reload the router before the new DLSw configuration changes will become active.

25.1.2 Configuring the branch router

The configuration of the branch router will be the same as the data center router except that in the branch office, we have a token-ring segment instead of an Ethernet segment. So, we need to use source route bridging instead of transparent bridging.

The first step is to disable access control as shown in Figure 521:

```
Karen *t 6
Karen Config>p ip
Internet protocol user configuration

Karen IP config>set access-control off
Karen IP config>exit
Karen Config>
Karen *t 5
Karen +p ip
Karen IP>reset ip
Karen IP>exit
```

Figure 521. Temporarily disabling access control on the branch router

The next step is to disable IPSec as shown in Figure 522 on page 488.

```
Karen *t 6
Karen Config>feature ip
IP Security feature user configuration
Karen IPsec config>disable ipsec stop
Karen IPsec config>exit
Karen Config>
Karen *
```

Figure 522. Temporarily disabling IPSec on the branch router

The next step is to configure the bridging function as shown in Figure 523:

```
Karen Config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Karen ASRT config>ena bridge
Karen ASRT config>ena dls
```

Figure 523. Configuring ASRT on the branch router

Next, we list it back out to verify the changes as shown in Figure 524:

```
Karen ASRT config>list bridge

           Source Routing Transparent Bridge Configuration
           ==============================================
Bridge:                 Enabled                 Bridge Behavior: STB
+---------+-----------| SOURCE ROUTING INFORMATION |-----------+---------+
Bridge Number:          N/A                     Segments:          0
Max ARE Hop Cnt:        00                      Max STE Hop cnt:   00
1 : N SRB:              Not Active              Internal Segment:  0x000
LF-bit interpret:       Extended
+---------+----------------| SR-TB INFORMATION |---------------+---------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
+---------+-------| SPANNING TREE PROTOCOL INFORMATION |----------+------+
Bridge Address:         Default               Bridge Priority:   32768/0x8000
STP Participation:      IEEE802.1d
+---------+-----------| TRANSLATION INFORMATION |-------------+---------+
FA<=>GA Conversion:     Enabled              UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
+---------+---------------| PORT INFORMATION |----------------+---------+
Number of ports added: 2
Port: 1      Interface: 0      Behavior:    STB Only   STP:  Enabled
Port: 2      Interface: 5      Behavior:    STB Only   STP:  Enabled
```

Figure 524. Configuring ASRT on the branch router

Next, we disable bridging in the interfaces not being used for this configuration. We then configure interface 5 (bridge port number 2) for Source Route Bridging (SRB) and give it a segment number. This is illustrated in Figure 525 on page 489.

```
Karen ASRT config>disa trans
Port Number [1]? 1
Karen ASRT config>disa trans
Port Number [1]? 2
Karen ASRT config>ena source
Port Number [1]? 2
Segment Number for the port in hex(1 - FFF) [001]? aa1
Bridge number in hex (0 - 9, A - F) [0]? 1
```

Figure 525. Configuring ASRT on the branch router

Now we configure DLSw. This is illustrated in Figure 526:

```
Karen Config>p dls
DLSw protocol user configuration
Karen DLSw config>ena dls
Data Link Switching is now enabled
Karen DLSw config>set srb aaa
DLSw segment number has been set.
Karen DLSw config>open-sap
Enter Interface number [0]? 5
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? sna
One or more SAPs already opened on interface 5
Karen DLSw config>open
Enter Interface number [0]? 5
Enter SAP in hex (range 0-FE), 'SNA', 'NB' or 'LNM'  [4]? nb
SAP F0 already opened on interface 5
Karen DLSw config>list open
Interface SAP(s)
    5      0  4  8  C F0
```

Figure 526. Configuring DLSw on the branch router

Add the DLSw neighbor (the other end of the pipe). This is the internal IP address of the 2210 in the branch. This is shown in Figure 527:

```
Karen DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 192.168.189.1
Connectivity Setup Type (a/p) [p]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]? e
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been added
Karen *r
Are you sure you want to restart the gateway? (Yes or [No]): y
```

Figure 527. Configuring TCP neighbors on the branch router

This completes the steps necessary for adding DLSw to our VPN configuration. As shown in Figure 527, you need to restart the router to make the DLSw changes active.

25.1.3 Testing DLSw

At this point, you would stop and test the DLSw configuration and make sure that it is working like you intended. You can see if the connection between the TCP neighbors is established and also if there is a DLS session. In Figure 528 on page 490, you can see that a NetBIOS session has been established between PC B and PC A in our test network. This is indicated by the F0 Service Access Point (SAP) in the MAC address/SAP pairs for the DLS session.

```
Li *t 5
Li +p dls
Data Link Switching Console

Li DLSw>list tcp sess all
Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
--------------- --------------- -------------- --- -------- ------ ----------
1               192.168.189.59  ESTABLISHED     a  AIW V2R0   1            1

Li DLSw>list dls sess all
    Source         Destination       State     Flags    Dest IP Addr    Id
---------------  ---------------  ---------  -------  --------------  ----
1 08005A5DB973 F0 400052005123 F0 CONNECTED           192.168.189.59    0

Li DLSw>exit
```

Figure 528. Testing DLSw

25.1.4 Re-enabling access control and IPSec

After we are satisfied that DLSw is working correctly, it is time to re-enable access control and IPSec.

Here we show how to do these steps for the router in the data center (the 2216 named Li). It is the same for the 2210 except that in the 2210, you use the restart command instead of the reload command as on the 2216. Figure 529 shows the command to re-enable access control:

```
Li *t 6
Li Config>p ip
Internet protocol user configuration
Li IP config>set access on
Li IP config>exit
Li Config>
```

Figure 529. Re-enabling access control

Figure 530 on page 491 shows the command to re-enable IPSec.

```
Li *t 6
Li Config>f ip
IP Security feature user configuration
Li IPsec config>enable ipsec
Restarting the router is required for IPsec to be active.
Li IPsec config>
```

Figure 530. Re-enabling IPSec

After enabling IPSec, you must restart the router in order to make the changes effective. When the router comes back up, IPSec and access control are enabled. Figure 531 shows the reload command for the router Li (2216).

```
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
```

Figure 531. Reloading the 2216

25.1.5 Testing DLSw with IPSec enabled

After restarting the router, we check to verify that IPSec and our tunnels are enabled. As shown in Figure 532, you can use the `list all` command at the IPSec prompt.

From the figure, we can see that IPSec is enabled and both tunnels are enabled also. Tunnel number 2 is the important one for DLSw as that is the one that all our DLSw traffic will go through. Remember that tunnel 2 is a transport-mode tunnel and all packets that originate in the routers will go through this tunnel.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  10:21  Jun 20 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  10:21  Jun 20 199
Li IPsec>exit
```

Figure 532. Testing DLSw with IPSec enabled

Next, we verify that DLSw is still working with IPSec enabled. Figure 533 shows that the TCP and DLSw sessions are still active with IPSec enabled.

```
Li *t 5
Li +p dls
Data Link Switching Console

Li DLSw>list tcp sess all
Group/Mcast@    IP Address      Conn State     CST Version  ActSes SesCreates
--------------- --------------- -------------- --- -------- ------ ----------
1               192.168.189.59  ESTABLISHED     a  AIW V2R0   1            1

Li DLSw>list dls sess all
    Source         Destination      State     Flags    Dest IP Addr    Id
---------------  ---------------  ---------  -------  -------------  ----
1 08005A5DB973 F0 400052005123 F0 CONNECTED           192.168.189.59    0

Li DLSw>exit
```

Figure 533. Testing DLSw with IPSec enabled

To make sure that the DLSw traffic is actually going through the IPSec tunnel, we check the IPSec statistics and see if the counters are increasing. Figure 534 shows the statistics for tunnel number 2, the tunnel that handles the traffic originated by the routers that includes our DLSw traffic.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      109788       109788        109788      22627872     12631392      9996480

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
          30           30            30          5456         3328         2128

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 534. Checking the IPSec statistics

Another way to check the number of packets that are going through the IPSec tunnel is to check the packet filter statistics and see how many times this filter was matched. Figure 535 shows a listing of the outbound filter, but you can also check the inbound filter and see similar information.

In this case we are interested in access control numbers 3 and 4. The figure shows that these have been matched 597 times (Use=597). Remember that control number 4 is the control that funnels the DLSw traffic to the IPSec engine and control number 3 is the control that lets the IPSec packets out of the router after they have been through the IPSec code.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 1208 times, 3570 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=597
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=597
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 535. Checking the packet filters

Chapter 26. IP bridging through an IPSec tunnel

Another way to enable multiple protocols through our IPSec tunnel is to use the Bridging Tunnel feature of the IBM Nways 2210/2216 routers. The bridging tunnel (encapsulation) is another feature of the ASRT bridge software. By encapsulating packets in industry-standard TCP/IP packets, the bridging router can dynamically route these packets through large IP internetworks to the destination end stations.

End stations see the IP path (the tunnel) as a single hop, regardless of the network complexity. This helps overcome the usual 7-hop distance limit encountered in source routing configurations. It also lets you connect source-routing end stations across non-source-routing media like Ethernet networks.

Since the IP bridging tunnel uses IP packets, we can secure them using IPSec. This chapter shows you how to configure IP bridging over our VPN by using our IPSec tunnel defined in Chapter 24, “Connecting the data center to the branch office” on page 463.

26.1 Configuring IP bridge tunnel in an IPSec environment

Figure 536 shows our sample network again with some additional MAC addresses that we use in this scenario.

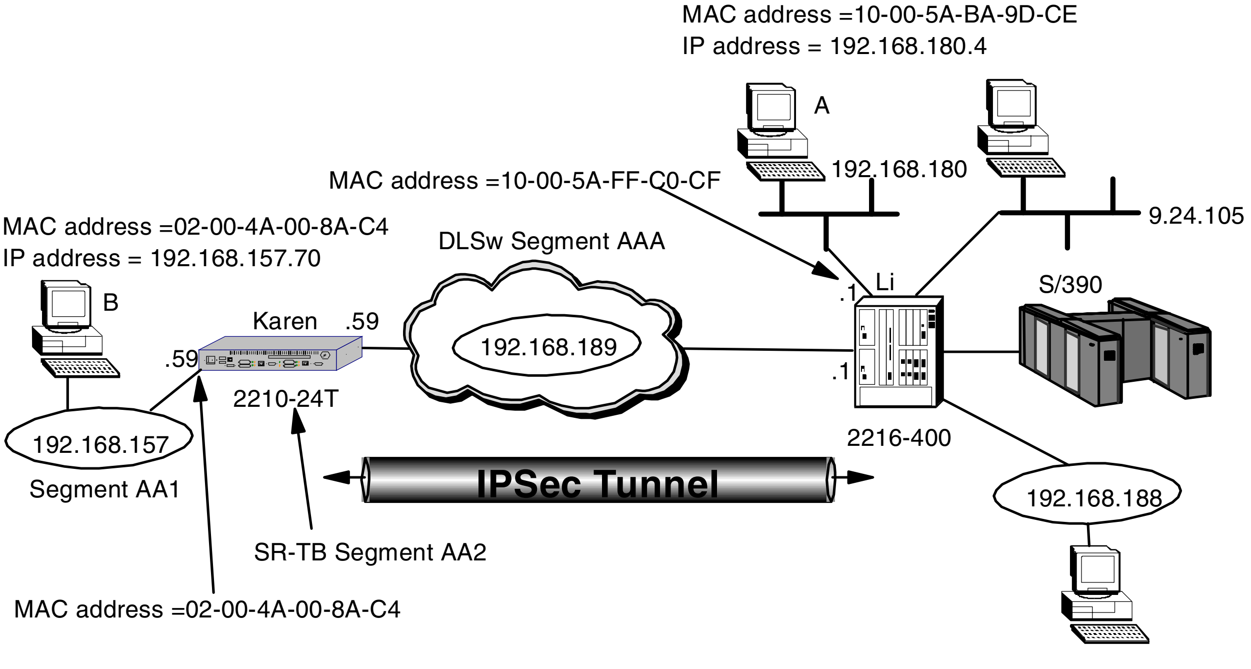

MAC address =10-00-5A-BA-9D-CE
IP address = 192.168.180.4
A
192.168.180
MAC address =10-00-5A-FF-C0-CF
9.24.105
MAC address =02-00-4A-00-8A-C4
IP address = 192.168.157.70
DLSw Segment AAA
.1
Li
S/390
B
Karen
.59
.59
192.168.189
.1
2210-24T
192.168.157
2216-400
Segment AA1
IPSec Tunnel
192.168.188
SR-TB Segment AA2
MAC address =02-00-4A-00-8A-C4

Figure 536. IP bridging tunnel through an IPSec tunnel

For this scenario, we want the 2210 to be configured as a source route-translational bridge (SR-TB) with source route bridging (SRB) on token-ring interface 5 (secure network side) and transparent bridging (STB) through an IP tunnel on token-ring 0 (nonsecure network).

We want the 2210 token-ring interface 0 to route IP. It has an IP address of 192.168.189.59 with a subnet mask of 255.255.255.0.

We want the 2216 to be a pure transparent bridge (STB) with STB enabled on the Ethernet interface and the token-ring interface 0 through our IP bridged tunnel.

We also want the 2216 token-ring interface 0 to route IP. It has an IP address of 192.168.189.1 with a subnet mask of 255.255.255.0.

We have an IPSec tunnel configured between the addresses 192.168.189.1 and 192.168.189.59 and we only allow packets from or to those addresses to go through the tunnel.

We have a PC configured with NetBIOS in the data center which is labeled PC A. Another PC, labeled PC B, is located in the branch office and is also configured with NetBIOS. From PC A we access a remote disk on PC B using the IP bridging tunnel which is passed through the IPSec tunnel.

As discussed in Chapter 25, “Data link switching over IPSec” on page 483, we recommend that you make these configuration additions and test them first with the IP packet filters and IPSec feature disabled. This will help you with problem determination if you experience any problems in setting up the bridged tunnel.

26.1.1 Configuring the 2210 branch router

The first step is to enable the Adaptive Source Route Transparent (ASRT) bridge function of the router. This command is shown in Figure 537 on page 497 along with the command to list the ASRT bridge characteristics.

Note: Listing the bridge configuration is an easy way to get the bridge port numbers that we need to set the port characteristics.

As can be seen from the figure, the ASRT bridge behavior defaults to transparent bridging (STB) while source route translational bridging (SR-TB) is disabled. Token-ring interface 0 is bridge port 1 while token-ring interface 5 is bridge port 2.

```
Karen config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Karen ASRT config>enable bridge
Karen ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                ===============================================
Bridge:                  Enabled                 Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:           N/A                     Segments:          0
Max ARE Hop Cnt:         00                      Max STE Hop cnt:   00
1 : N SRB:               Not Active              Internal Segment:  0x000
LF-bit interpret:        Extended
+----------+----------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address :         Default                 Bridge Priority: 32768/0x8000
STP Participation :      IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:      Enabled             UB-Encapsulation:  Disabled
DLS for the bridge:      Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+
Number of ports added: 2
Port:   1      Interface:    0      Behavior:    STB Only   STP:  Enabled
Port:   2      Interface:    5      Behavior:    STB Only   STP:  Enabled
```

Figure 537. Enabling the bridge

Next, we need to disable the STB function since we do not use it on either of the token-ring ports (ports 1 and 2). We then enable SRB on port 2 and define the segment number attaching to this token-ring port to be AA1 and the 2210 bridge number to be 1. This is shown in Figure 538 on page 497.

```
Karen ASRT config>disa transparent 1
Karen ASRT config>disa transparent 2
Karen ASRT config>enable source 2 AA1
Bridge number in hex (0 - 9, A - F) [0]? 1
```

Figure 538. Configuring bridge ports

As we have STB and SRB, we need to use Source Route-Translational Bridge (SR-TB) to translate a source route bridge frame into a transparent bridge frame and vice versa. SR-TB is enabled at the box level which is illustrated in Figure 539 on page 497. The transparent bridge domain is seen as LAN segment number AA2 from the source route bridge domain.

```
Karen ASRT config>ena sr-tb
TB-Domain Segment Number in hex(1 - FFF) [1] ? aa2
TB-Domain's MTU1470
Bridge Virtual Segment Number in hex(1 - FFF) [1] ?
```

Figure 539. Configuring translational bridging

At this point, we define the IP bridging tunnel. This is done simply with the `add tunnel` command as shown in Figure 540. As a result, a new bridge port is added with a default behavior of transparent bridging (STB).

```
Karen ASRT config>add tunnel
Port Number [3]? 3

                Source Routing Transparent Bridge Configuration
                ===============================================
Bridge:                 Enabled                 Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:          N/A                     Segments:         0
Max ARE Hop Cnt:        00                      Max STE Hop cnt:   00
1 : N SRB:             Not Active             Internal Segment:  0x000
LF-bit interpret:       Extended
+----------+----------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:       Disabled
TB-Virtual Segment:     0x000                   MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address:         Default                 Bridge Priority:  32768/0x8000
STP Participation:      IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:     Enabled             UB-Encapsulation:  Disabled
DLS for the bridge:     Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+

Number of ports added: 2
Port: 1    Interface:      0      Behavior: No Bridging   STP:  Enabled
Port: 2    Interface:      5      Behavior:    SRB Only   STP:  Enabled
Port: 3    Interface: Tunnel      Behavior:    STB Only   STP:  Enabled
```

Figure 540. Adding a bridging tunnel

We also need to specify the destination IP address of the other end of the IP bridging tunnel. This is shown in Figure 541 on page 499. The IP address of the other end of the IP bridging tunnel is the interface address and also the internal IP address of the router.

Note: It is very important to add the necessary access controls to the inbound and outbound packet filters for this router-to-router traffic so that the packets can be processed by IPSec. This was performed in 24.1.1, “Configuring the branch office router” on page 464 and 24.1.1.1, “Defining the inbound packet filters” on page 468 for the 2210.

```
Karen ASRT config>tunnel
Tunnel interface configuration

Karen TNL config>add address
Enter the address to be added [0.0.0.0]? 192.168.189.1
Karen TNL config>list all
IP Tunnel Addresses

     192.168.189.1

Karen TNL config>exit
Karen ASRT config>exit
```

Figure 541. Configuring a bridging tunnel

Finally, we restart the router to activate this configuration. This is illustrated in Figure 542.

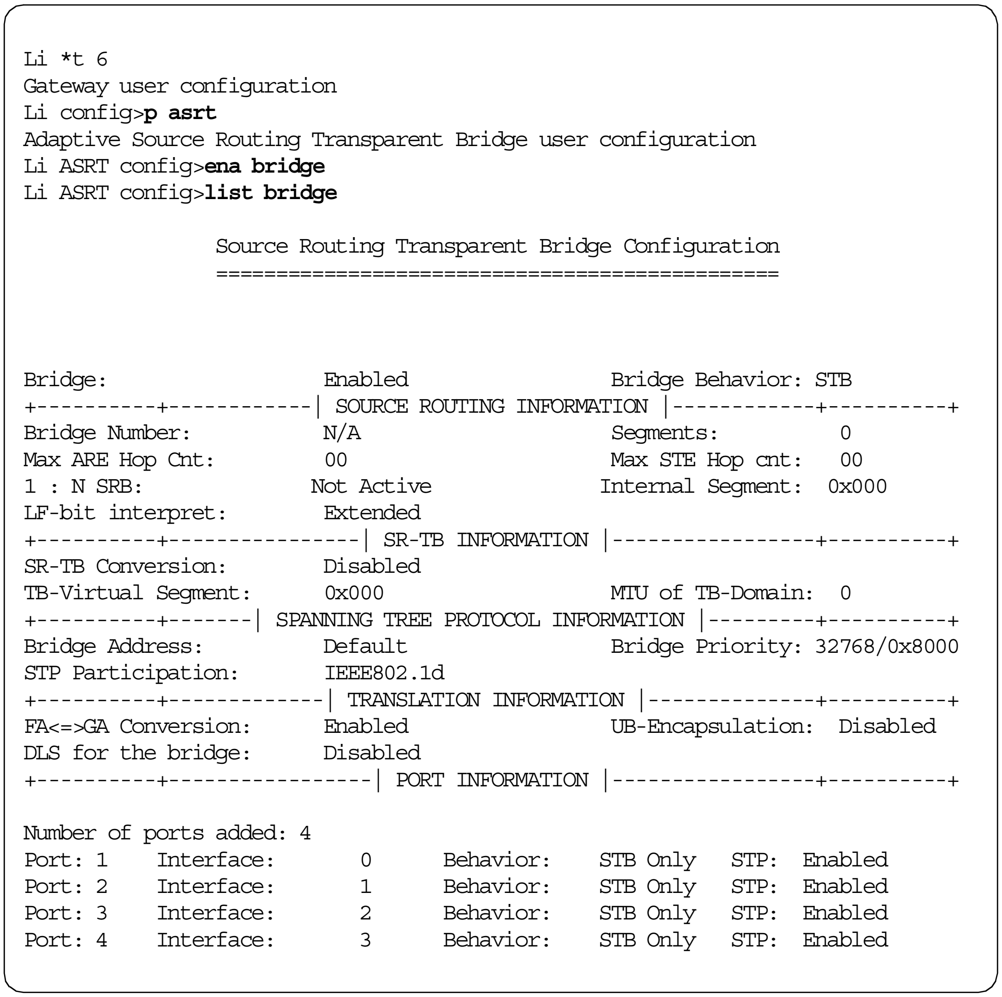
```
Karen config>
*restart
Are you sure you want to restart the gateway? (Yes or [No]): Yes
```

Figure 542. Restarting the router

26.1.2 Configuring the data center router

We need to do the same steps almost exactly to configure the 2216 in the data center for our bridging tunnel. This section takes you step by step through this process.

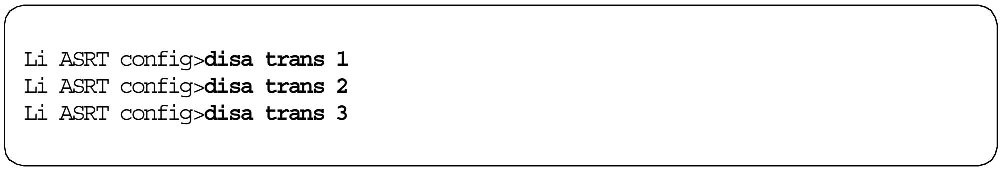
Again, the first step is to enable the bridge and list the configuration so that we can see the port numbers that have been defined. This is illustrated in Figure 543 on page 500.



```
Li *t 6
Gateway user configuration
Li config>p asrt
Adaptive Source Routing Transparent Bridge user configuration
Li ASRT config>ena bridge
Li ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                ===============================================



Bridge:                   Enabled                 Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:            N/A                     Segments:          0
Max ARE Hop Cnt:          00                      Max STE Hop cnt:   00
1 : N SRB:               Not Active              Internal Segment:  0x000
LF-bit interpret:         Extended
+----------+----------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:         Disabled
TB-Virtual Segment:       0x000                   MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address:           Default                 Bridge Priority: 32768/0x8000
STP Participation:        IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:       Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:       Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+

Number of ports added: 4
Port: 1    Interface:      0      Behavior:    STB Only   STP:  Enabled
Port: 2    Interface:      1      Behavior:    STB Only   STP:  Enabled
Port: 3    Interface:      2      Behavior:    STB Only   STP:  Enabled
Port: 4    Interface:      3      Behavior:    STB Only   STP:  Enabled
```

Figure 543. Enabling the bridge

Again, we disable the default STB behavior (in this example on all the interfaces except port 4 which is our Ethernet segment where we use transparent bridging). This is illustrated in Figure 544:



```
Li ASRT config>disa trans 1
Li ASRT config>disa trans 2
Li ASRT config>disa trans 3
```

Figure 544. Configuring bridge ports

Next, we add the IP bridging tunnel port. This is illustrated in Figure 545 on page 501. Note that the tunnel port is STB by default.

```
Li ASRT config>add tunnel
Port Number [5]? 5
Li ASRT config>list bridge

                Source Routing Transparent Bridge Configuration
                ===============================================

Bridge:                  Enabled                 Bridge Behavior: STB
+----------+------------| SOURCE ROUTING INFORMATION |------------+----------+
Bridge Number:           N/A                     Segments:          0
Max ARE Hop Cnt:         00                      Max STE Hop cnt:   00
1 : N SRB:              Not Active              Internal Segment:  0x000
LF-bit interpret:        Extended
+----------+----------------| SR-TB INFORMATION |-----------------+----------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                   MTU of TB-Domain:  0
+----------+-------| SPANNING TREE PROTOCOL INFORMATION |---------+----------+
Bridge Address:          Default                 Bridge Priority: 32768/0x8000
STP Participation:       IEEE802.1d
+----------+-------------| TRANSLATION INFORMATION |--------------+----------+
FA<=>GA Conversion:      Enabled                 UB-Encapsulation:  Disabled
DLS for the bridge:      Disabled
+----------+-----------------| PORT INFORMATION |-----------------+----------+

Number of ports added: 5
Port: 1    Interface:      0      Behavior: No Bridging   STP:  Enabled
Port: 2    Interface:      1      Behavior: No Bridging   STP:  Enabled
Port: 3    Interface:      2      Behavior: No Bridging   STP:  Enabled
Port: 4    Interface:      3      Behavior:    STB Only   STP:  Enabled
Port: 5    Interface:  Tunnel     Behavior:    STB Only   STP:  Enabled
```

Figure 545. Adding a bridge tunnel port

Next, we add the destination IP address of the other side of the tunnel. This is illustrated in Figure 546:

```
Li ASRT config>tunnel
Tunnel interface configuration

Li TNL config>add address 192.168.189.59
Li TNL config>list all
IP Tunnel Addresses

     192.168.189.59

Li TNL config>exit
Li ASRT config>exit
Li config>
```

Figure 546. Configuring a bridging tunnel

Finally, we reload the router to activate the configuration.

```
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
```

Figure 547. Reloading the router

26.1.3 Testing the IP bridging tunnel (IPSec disabled)

Now, we test the IP bridging tunnel configuration to make sure that it is working like we intended. After sending some NetBIOS traffic between PC A and PC B, we issue the `list database` command from talk 5 to see if our MAC addresses are dynamically registered to use the IP bridging tunnel. From the listing in Figure 548 on page 502, you can see:

- **Address 00-20-35-45-D3-95 :** This is the address for interface 5 of the router Karen, *the 2210 in the branch office*. This physical MAC address is dynamically registered *through the IP tunnel*.
- **Address 02-00-4A-00-8A-C4 :** This is the address for PC B that is attached to the SRB segment. As you can see, it is also dynamically registered.
- **Address 10-00-5A-BA-9D-CE :** This is the address for PC A that is connected to the STB segment. Here you see that this address is also dynamically registered on the Ethernet interface.
- **Address 10-00-5A-FF-C0-CF :** This is the address for the local Ethernet interface (bridge port 4) on the 2216. It does not use the IP bridge tunnel itself because it is a local interface.

```
Li ASRT>list database all
MAC Address    MC*  Entry Type       Age  Port(s)

00-20-35-45-D3-95   Dynamic           300  5 (IP Tunnel) @192.168.189.59
01-80-C2-00-00-00*  Registered            4-5
01-80-C2-00-00-01*  Reserved              All
01-80-C2-00-00-02*  Reserved              All
01-80-C2-00-00-03*  Reserved              All
01-80-C2-00-00-04*  Reserved              All
01-80-C2-00-00-05*  Reserved              All
01-80-C2-00-00-06*  Reserved              All
01-80-C2-00-00-07*  Reserved              All
01-80-C2-00-00-08*  Reserved              All
01-80-C2-00-00-09*  Reserved              All
01-80-C2-00-00-0A*  Reserved              All
01-80-C2-00-00-0B*  Reserved              All
01-80-C2-00-00-0C*  Reserved              All
01-80-C2-00-00-0D*  Reserved              All
01-80-C2-00-00-0E*  Reserved              All
01-80-C2-00-00-0F*  Reserved              All
02-00-4A-00-8A-C4   Dynamic          295  5 (IP Tunnel) @192.168.189.59
03-00-00-00-80-00*  Reserved              All
03-00-00-20-00-00*  Registered            1-2
10-00-5A-BA-9D-CE   Dynamic          295  4 (Eth /1         )
10-00-5A-FF-C0-CF   Registered            4 (Eth /1         )
```

Figure 548. Testing the IP bridging tunnel

26.1.4 Testing the IP bridging tunnel with IPSec enabled

Now we re-enable access control, reset IP, then re-enable IPSec and reset the IPSec feature.

Next, we check the IPSec status as shown in Figure 549 to make sure that IPSec has been re-enabled:

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH             192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH       192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  15:32  Jun 21 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  15:32  Jun 21 199
Li IPsec>exit
```

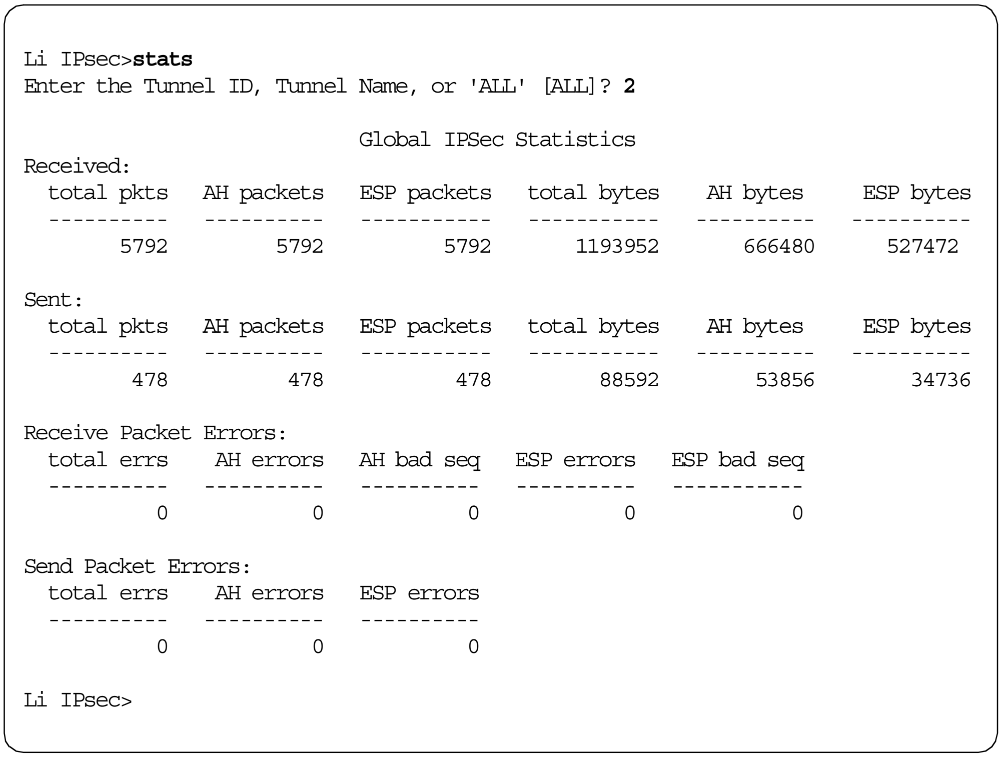
Figure 549. IPSec status

Next, we check the IP bridging tunnel again to make sure that the tunnel is still working with IPSec enabled. As can be seen in Figure 550 on page 504, the MAC addresses are still registered.

```
Li ASRT>list database all

MAC Address    MC*  Entry Type       Age  Port(s)

00-20-35-45-D3-95   Dynamic          250  5 (IP Tunnel) @192.168.189.59
01-80-C2-00-00-00*  Registered            4-5
01-80-C2-00-00-01*  Reserved              All
01-80-C2-00-00-02*  Reserved              All
01-80-C2-00-00-03*  Reserved              All
01-80-C2-00-00-04*  Reserved              All
01-80-C2-00-00-05*  Reserved              All
01-80-C2-00-00-06*  Reserved              All
01-80-C2-00-00-07*  Reserved              All
01-80-C2-00-00-08*  Reserved              All
01-80-C2-00-00-09*  Reserved              All
01-80-C2-00-00-0A*  Reserved              All
01-80-C2-00-00-0B*  Reserved              All
01-80-C2-00-00-0C*  Reserved              All
01-80-C2-00-00-0D*  Reserved              All
01-80-C2-00-00-0E*  Reserved              All
01-80-C2-00-00-0F*  Reserved              All
02-00-4A-00-8A-C4   Dynamic          245  5 (IP Tunnel) @192.168.189.59
03-00-00-00-80-00*  Reserved              All
03-00-00-20-00-00*  Registered            1-2
10-00-5A-BA-9D-CE   Dynamic          245  4 (Eth /1         )
10-00-5A-FF-C0-CF   Registered            4 (Eth /1         )
```

Figure 550. Testing IP bridging with IPSec enabled

Finally, in order to be sure that the IP bridging traffic is going through the IPSec tunnel, we list the IPSec statistics and check to see that the counters are increasing. This is shown in Figure 551 on page 505. Note that tunnel number 2 is the one that we defined to carry the router-to-router traffic. As we send more traffic through the IP bridging tunnel, the counters for IPSec tunnel number 2 increase.



```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
        5792         5792          5792       1193952       666480      527472

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         478          478           478         88592        53856        34736

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 551. Checking the IPSec statistics

Next, we check the number of times that the access controls on our IP packet filter have been matched. You can see in Figure 552 on page 506 that access control number 4 has been matched 434 times (use=434). This is the IPSec control for the router-to-router traffic (including our IP bridging traffic). Our traffic is first *caught* by this control and passed to IPSec for encapsulation after which it is sent through the filters again. The second time through the filters, access control number 3 is matched. This is because the traffic now has a protocol field that indicates that it is IPSec traffic (Protocol=50-51). Access control number 3 is an inclusive control that tells the router to let these packets out of the interface.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 893 times, 8770 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=434
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=434
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 552. Checking the packet filter statistics

Chapter 27. APPN through an IPSec tunnel

Advanced Peer-to-Peer Networking (APPN) is another very important protocol to transport across our virtual private network. Fortunately, the Enterprise Extender feature of MRS/MAS allows us to transport our APPN High Performance Routing (HPR) traffic over an IP backbone, in this case, the Internet. Since Enterprise Extender (also called HPR over IP) uses IP encapsulation, we can use IPSec to protect these packets as they traverse the public network.

In our scenario, (see Figure 553) we have an APPN end node (EN) in the branch office that needs to communicate with another EN in the data center. In the figure, these devices are labeled VPNOS2A and VPNWNTA, respectively. The 2210 router (named Karen) in the branch is configured as an APPN network node (NN) and is providing APPN directory services for device VPNOS2A. The 2216 (named Li) is also configured as a NN and is providing directory services for device VPNWNTA.

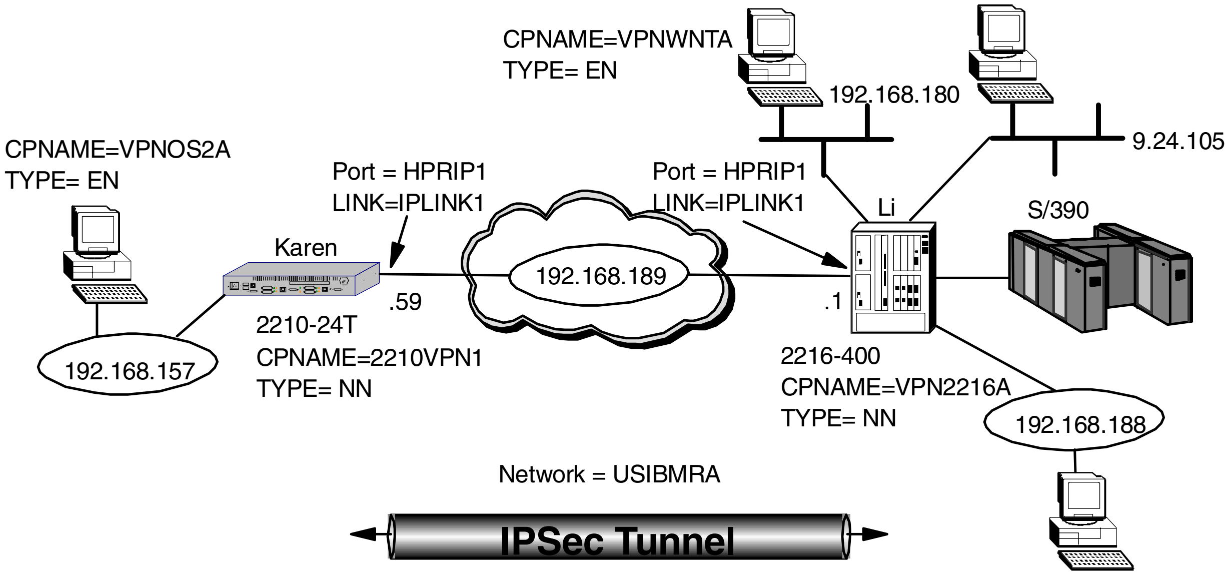


Figure 553. APPN through an IPSec tunnel

The APPN traffic comes into the branch router as an LLC frame over the token-ring interface (which is also defined as an APPN port). The branch router, acting as an APPN network node, decides to route the traffic to its destination over the HPR over IP port. The HPR over IP engine in the router encapsulates the APPN LLC frame into an IP packet (using UDP) and then passes it to the IP routing element. IP then sends the packet to the other token-ring interface (our interface to the public network).

At this point, the outbound packet filter that we define on the token-ring interface redirects the packet to the IPSec engine where it is processed for AH and ESP headers before being sent out on the physical interface.

A similar process occurs in the reverse direction. As the IP packet reaches the end of the tunnel, it gets decapsulated and decrypted by the IPSec engine, then passed to the IP stack where it is determined that it must be directed to the HPR over IP port in the router. The HPR over IP function strips off the IP and UDP headers and passes the APPN LLC frame to APPN. The APPN network node routes the frame to its destination.

As discussed in Chapter 24, “Connecting the data center to the branch office” on page 463, we could use either an IPSec tunnel-mode tunnel or a transport-mode tunnel. One reason a company would use tunnel mode versus transport mode is to hide internal IP addresses used in the network.[1] When packets use tunnel mode, they are encapsulated with a new IP header and the original source and destination addresses are no longer visible.

However, in the case of HPR over IP packets, the IP traffic originates in the router where the APPN traffic is encapsulated and terminates in the router where it is decapsulated. In our scenario, the routers where the APPN traffic is encapsulated are the same routers used as our IPSec tunnel endpoints. In other words, only the Internet addresses of these two routers will appear in the HPR over IP packets. Using tunnel mode in this situation does not offer any advantages over transport mode in terms of hiding the source and destination IP addresses of the sender and receiver.

For our scenario, we chose to implement a transport-mode tunnel to carry our APPN traffic (as well as all the other router-to-router traffic). This tunnel was defined in Figure 500 on page 474.

27.0.1 Configuring the 2216 in the data center

Before we can configure APPN on the 2216, we first have to load the APPN package. This is shown in Figure 554 on page 508. Once this command has been issued, the APPN module will be loaded during each subsequent IPL of the router.

Note: You must have an MAS software load that contains the APPN.LD file in order for this work.

```
Li *t 6

Li Config>load add package appn
appn package configured successfully
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3
The configuration has been saved.
```

Figure 554. Configuring the necessary 2216 code elements

After the router comes back up, we go to the talk 6 APPN protocol menus and set the APPN node characteristics. This is done using the `set node` command as shown in Figure 555 on page 509.

[1] Another reason is to use unregistered IP addresses.

```
Li Config>protocol appn
Li APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [ ]? usibmra
Control point name (Max 8 characters) [ ]? vpn2216a
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 555. Defining the APPN node on the 2216

As you can see, the only parameters that are absolutely necessary are the APPN CP name and the Network ID. The other parameters can be left at their default values.

The next step is to add the APPN ports that will be used to carry our APPN traffic. In Figure 556 on page 509, we add an HPR over IP port.

```
Li APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        Enable IP Precedence: (Y)es (N)o [N]? Y
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 556. Adding an APPN port for HPR over IP

Again, we use the defaults for most of the parameters. The critical one is the port type (I for HPR over IP). Note that you do not need to specify an interface number because there is only one HPR over IP port per router. We also give it a port name that we can easily recognize on the monitoring console.

Note: One new question on this screen in MAS/MRS V3.1 deals with the IPv4 precedence bits. If you respond yes to this question to enable setting of the precedence bits, then the 3 precedence bits in the TOS field of the IPv4 header will be set based on the HPR priority of the traffic. This allows you to preserve your SNA priorities using the Bandwidth Reservation System (BRS) feature even on encrypted packets. Please see *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

Next, we add a link station on the newly defined HPR over IP port. This is shown in Figure 557.

```
Li APPN config>add link
APPN Station
Port name for the link station [ ]? HPRIP1
Station name (Max 8 characters) [ ]? IPLINK1
        Activate link automatically (Y)es (N)o [Y]?
        IP address of adjacent node  [192.168.189.59]?
        Adjacent node type: 0 = APPN network node,
        1 = APPN end node or Unknown node type  [0]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
        Remote SAP(04-EC) [4]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 557. Adding a link station for the HPR over IP link

By specifying the port name for this link station, the router knows that it is an HPR over IP port. Therefore, it knows to prompt you for an IP address as opposed to a MAC address that it would need if we were defining a link station for a LAN port.

The IP address that we specify is the *internal address* of the 2210 in the branch office. This is the endpoint of our HPR over IP network. The other end of the HPR over IP link is always at the router that will decapsulate the packets and *not* the next hop router in the path. Intermediate routers, if any, merely perform IP routing on the encapsulated packets.

Note: The router internal address is configured from the talk 6 `protocol ip` prompt.

Next we add a port on the Ethernet LAN interface 3 so that stations on that LAN can set up link stations to the 2216. This is shown in Figure 558 on page 511.

```
Li APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? e
Interface number(Default 0): [0]? 3
Port name (Max 8 characters) [E00003]? TOWNTA
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-1496) [1289]?
        Maximum number of link stations (1-976) [512]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Li APPN config>
```

Figure 558. Adding the APPN port for the 2216 Ethernet interface

We do not need to define any link stations on this port as the workstations (APPN end nodes) will create implicit links when they initialize with their network node (in this case, the 2216 itself).

This completes the configuration of the 2216 in the data center. To activate the changes, we reload the router as shown in Figure 559:

```
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3
The configuration has been saved.
```

Figure 559. Reloading the 2216 in the data center

27.0.2 Configuring the 2210 in the branch office

This section takes you step-by-step through the APPN configuration of the 2210 in the branch office. (Please refer back to Figure 553 to see the network diagram.) The steps are almost identical to the ones for configuring the 2216 in the data center.

First we set the APPN node characteristics. This is shown in Figure 560 on page 512.

```
Karen Config>p appn
Karen APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? vpn2210a
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
Karen APPN config>
```

Figure 560. Setting the APPN node characteristics for the branch router

Note: The network ID must match at both ends of the HPR over IP link.

Next, we add an HPR over IP port. This is shown in Figure 561.

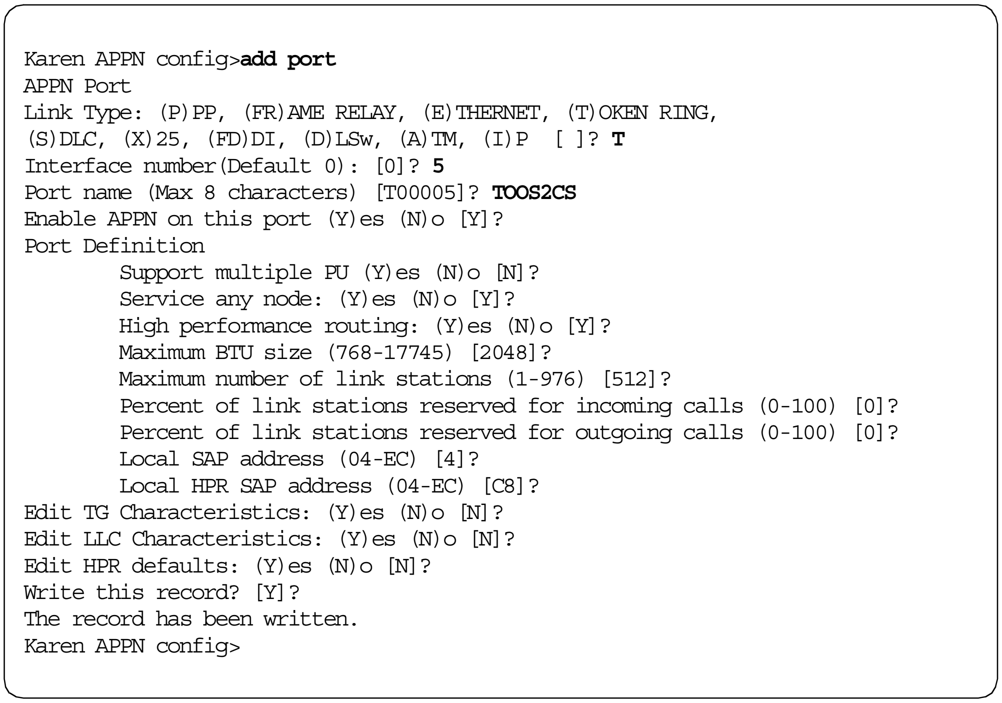
```
Karen APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? I
Port name (Max 8 characters) [IP65535]? HPRIP1
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Service any node: (Y)es (N)o [Y]?
        Maximum BTU size (768-2048) [1469]?
        UDP port number for XID exchange (1024-65535) [12000]?
        UDP port number for low priority traffic (1024-65535) [12004]?
        UDP port number for medium priority traffic (1024-65535) [12003]?
        UDP port number for high priority traffic (1024-65535) [12002]?
        UDP port number for network priority traffic (1024-65535) [12001]?
        IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]? 1
        Enable IP Precedence: (Y)es (N)o [N]? Y
        Local SAP address (04-EC) [4]?
        LDLC Retry Count(1-255) [3]?
        LDLC Timer Period(1-255 seconds) [15]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y]?
Karen APPN config>
```

Figure 561. Adding the HPR over IP port for the branch router

Note that we use the same port name as we used for the 2216. This is just for our convenience as the port name is only used at the router where it is defined and has no correlation to any other port names on any other routers.

Now that we have the port defined, the next step would normally be to define a link station to the next hop APPN node. However, in this case, it is not necessary because an implicit link will be created when the 2216 in the data center establishes a connection with this router in the branch office.

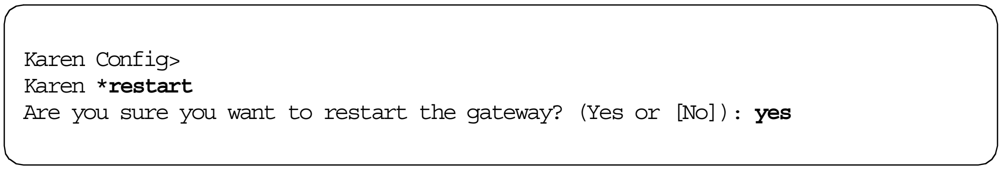
Next, we add a token-ring APPN port for LAN connected end nodes to connect to the 2210 as their NN server. This is shown in Figure 562:



```
Karen APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? T
Interface number(Default 0): [0]? 5
Port name (Max 8 characters) [T00005]? TOOS2CS
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [Y]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-976) [512]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
Karen APPN config>
```

Figure 562. Adding an APPN port for the LAN interface on the branch router

This completes the APPN definition on the branch router. We restart the gateway to activate APPN as shown in Figure 563:



```
Karen Config>
Karen *restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 563. Restarting the router

27.0.3 Testing the APPN configuration

To test the APPN setup, we go to the talk 5 APPN GWCON on the branch router and list the active links. This is shown in Figure 564 on page 514.

```
Karen *t 5


CGW Operator Console

Karen +p appn
APPN GWCON
Karen APPN >list link
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
======================================================================
 IPLINK1      HPRIP1     7   USIBMRA.VPN2216A   NN    ACTIVE     ACT_LS
     @@0     TOOS2CS     5   USIBMRA.VPNOS2A    EN    ACTIVE     ACT_LS
```

Figure 564. Listing the status of the APPN links on the branch router

From the figure, one thing that you can see is that an end node (USIBMRA.VPNOS2A) is connected over the token-ring port (TOOS2CS) through an implicit link (@@0).

However, more important to our VPN discussion is that the HPR over IP link to the 2216 in the data center (USIBMRA.VPN2216A) is active. We know that this traffic is going over the IPSec tunnel because we are using the same IPSec configuration and IP filters that we used in all previous scenarios. This configuration stipulates that all router-to-router traffic will be sent through transport mode over IPSec tunnel number 2. (Please see Chapter 24, “Connecting the data center to the branch office” on page 463 for a description of the transport-mode tunnel definition.)

Note: If the HPR over IP link does not become active, first re-check your configuration. If the configuration looks correct, try and ping each router's internal address: first from the router to its own internal address, then to the other router's internal address. Repeat this test from the other router. The internal address of each router must be reachable in order for the HPR over IP link to function.

Chapter 28. Adding dependent LU requester

The dependent LU requester (DLUR) feature available in both MRS and MAS allows you to connect PU Type 2.0 or T2.1 devices containing dependent LUs to your SNA host using APPN. The DLUR function in the router works in conjunction with a dependent LU server (DLUS) located in VTAM. The router can either be configured as an APPN network node or an APPN end node.

In our VPN scenario (see Figure 565 on page 515), we have some T2.0 devices (and their associated dependent LUs) in the branch that we want to connect back to the data center. We put the DLUR function in the branch router, then use APPN transport between the DLUR and VTAM. Then, we use HPR over IP to carry the APPN traffic over the IP backbone (the Internet in this case) and hence, IPSec to protect these packets.

Further, with the new support for setting the IP precedence bits that became available in MRS/MAS Version 3.1, you can map the SNA priority (for example, HPR) of these connections into the IP packets.

Note: This priority is preserved even if you are using IPSec tunnel mode, where the original packet is completely encapsulated in another one.

28.1 Configuring DLUR in an IPSec environment

Figure 565 shows the configuration that we used in this scenario.

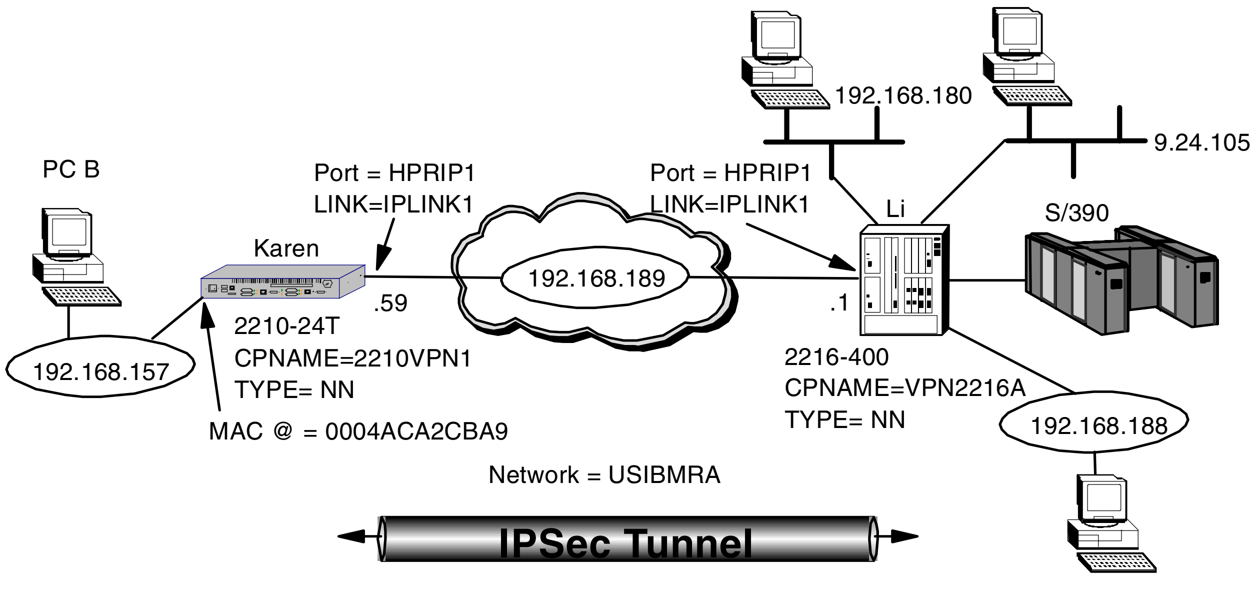


Figure 565. DLUR using HPR over IP through an IPSec tunnel

For our scenario, we use a PC with Personal Communications for OS/2 (PCOMM) as our PU T2.0 with a dependent LU. This machine is labeled PC B in the diagram. We configure PC B to access the host using the DLUR in the 2210 by simply providing the MAC address of the token-ring interface on the 2210 as the LAN destination MAC address for the 3270 gateway. The MAC address of the 2210 interface is 0004ACA2CBA9.

As for the 2210 configuration, we use the same environment that we used in Chapter 27, “APPN through an IPSec tunnel” on page 507, except that we enable DLUR support in the router.

In the 2216, we use an MPC+ connection over the ESCON channel to VTAM.[1] This is a very high performance connection and will generally provide the highest data throughout. Additionally, the required APPN support for DLUR is available over MPC+. Not shown in the figure is an IBM 9032 ESCON Director (ESCD) between the 2216 and the S/390.

To configure it, we simply define the MPC+ connection and then add an APPN port for this new connection to the existing APPN configuration that we used in Chapter 27, “APPN through an IPSec tunnel” on page 507. Also as in that scenario, we use HPR over IP between the routers and send that traffic through the IPSec tunnel already configured between them.

28.1.1 VTAM definitions

In this section, we present the basic VTAM definitions we used for our scenario. This is not meant to be a complete reference on the subject. For more information on configuring VTAM, refer to *CS OS/390 Resource Definition Reference*, SC31-8565.

DLUS support requires that VTAM be configured as an APPN network node. This requires certain parameters to be specified in the VTAM startup parameters to specify the use of APPN and HPR. These are shown in Figure 566 on page 517. Set the CONNTYPE to APPN and the NODETYPE to a Network Node (NN).

[1] Multi-Path Channel (MPC) is a protocol layer which allows multiple read and write subchannels to be treated as a single transmission group between the host and channel-attached devices. This interface is used by VTAM for APPN data transport. For more information about MPC+, refer to *IBM 2216 Multiaccess Connector ESCON Solutions*, SG24-2137.

```
ASYDE=TERM,IOPURGE=5M,
CONFIG=I0,
CONNTYPE=APPN,
CPCP=YES,
CSALIMIT=0,
DYNADJCP=YES,
ENCRYPTN=NO,
GWSSCP=YES,
HOSTPU=ISTPUS18,
HOSTSA=18,
HPR=RTP,
NETID=USIBMRA,
NODETYPE=NN,
NOTRACE,TYPE=VTAM,IOINT=0
PPOLOG=YES
SORDER=APPN,
SSCPDYN=YES,
SSCPID=18,
SSCPNAME=RAI,
SSCPORD=PRIORITY,
SUPP=NOSUP,
TNSTAT,CNSL,
VRTG=YES
OSITOPO=LLINES,
OSIMGMT=YES
XNETALS=YES
```

Figure 566. VTAM startup parameters

28.1.2 VTAM definitions for an MPC+ connection

An MPC+ connection requires entries in two VTAM control blocks:

- The Local major node
- The Transport Resource List (TRL) major node

Figure 567 on page 517 shows a sample definition for a local SNA major node for a 2216 MPC+ connection. This is the local PU that resides in VTAM that supports the channel connection defined in the TRL. The connection type must be APPN and you also need to enable HPR.

```
LOCNETU VBUILD TYPE=LOCAL
LNETU   PU     TRLE=LNETU,
               XID=YES,
               CONNTYPE=APPN,
               CPCP=YES,
               HPR=YES
```

Figure 567. VTAM local major node definition

Notes:

1. TYPE must equal LOCAL on the VBUILD statement.
2. TRLE identifies the TRL being used. The name must match the name of an existing TRL.

3. XID indicates whether XIDs will be exchanged. It must be XID=YES.
4. CONNTYPE must be set to CONNTYPE=APPN since APPN is the only protocol that VTAM uses with an MPC+ connection.
5. CPCP specifies that CP-CP connections with APPN can be established over this MPC+ connection. This could be either set to YES or NO, depending upon your APPN topology.
6. HPR specifies that APPN HPR traffic can flow over this MPC+ connection. HPR is normally used by default, but setting this value to YES ensures it. This is important because an MPC+ connection requires RTP (and HPR).

Next, you need a transport resource list for the MPC+ connection from the 2216. An example definition is shown in Figure 568.

```
      VBUILD TYPE=TRL
LNETU TRLE   LNCTL=MPC,
             MAXBFRU=9,
             READ=280,
             WRITE=281,
             MPCLEVEL=HPDT,
             REPLYTO=3.0
```

Figure 568. VTAM Transport Resource List (TRL) definition

Notes:

1. TYPE must be TRL.
2. LNETU is the name that identifies the TRL. It must match what is specified in the TRLE= field in the local major node definition. (See Figure 567.)
3. LNCTL identifies the connection type. It must be LCNTL=MPC.
4. MAXBFRU is the number of 4K pages per read subchannel.
5. READ/WRITE specifies the subchannels in the MPC+ group, and indicates their direction. The subchannel numbers must be in the range of addresses specified in the IODEVICE statement in the IOCP definition. There can be multiple READ and WRITE parameters in the TRLE statement but there must be at least one of each.

   Note: The designations READ and WRITE here are from the HOST perspective. In the 2216 MPC+ definition, the designations are from the 2216 perspective. Therefore, subchannels designated as READ on the host *must* be designated as WRITE on the 2216, and vice versa.
6. REPLYTO is the reply timeout value in seconds.

28.1.3 Configuring the 2216 for MPC+

In this section, we show the steps necessary to:

1. Configure the 2216 for an ESCON MPC+ connection to the host
2. Add an APPN port for this connection

In order to connect the 2216 to the host using the ESCON adapter, you first need to add an ESCON interface for the router and configure it. Figure 569 on page 519 shows this step. As can be seen from the figure, if you list the devices after adding the ESCON adapter, it will appear at the bottom of the list. You should check that the slot number is correct. Also remember that the interface numbers are dependent on the order in which you added the devices to the configuration.

```
Li *t 6
Gateway user configuration
Li Config>add device escon
Device Slot #(1-8) [1]? 3
Adding ESCON Channel device in slot 3  port 1 as interface #6
Use "net 6" to configure ESCON Channel parameters
Li Config>list dev
Ifc 0     Token Ring                          Slot: 1   Port: 1
Ifc 1     Token Ring                          Slot: 1   Port: 2
Ifc 2     Ethernet                            Slot: 5   Port: 1
Ifc 3     Ethernet                            Slot: 5   Port: 2
Ifc 4     V.35/V.36 PPP                       Slot: 6   Port: 0
Ifc 5     V.35/V.36 Frame Relay               Slot: 6   Port: 1
Ifc 6     ESCON Channel                       Slot: 3   Port: 1
```

Figure 569. Adding the ESCON adapter

Now that we have the ESCON interface defined we need to add the MPC+ virtual interface. This MPC *virtual net handler* will perform all the MPC protocol functions for our connection to the host. Figure 570 on page 519 shows this step.

```
Li Config>net 6
Li ESCON Config>add mpc
```

Figure 570. Adding the MPC+ virtual interface

As can be seen from Figure 571, the prompt will change to the `ESCON Add Virtual>` prompt. From here you define the read and write subchannels that will be used for this connection.

```
Li ESCON Add Virtual>sub addr
Li ESCON Add MPC+ Read Subchannel>device
Device address (range 0x00-0xFF): [0]? 1
Li ESCON Add MPC+ Read Subchannel>link
Link address (ESCD Port) (range 0x01-0xFE): [1]? cc
Li ESCON Add MPC+ Read Subchannel>cu
Control Unit Logical Address (range 0x0-0xF): [0]? 0
Li ESCON Add MPC+ Read Subchannel>lpar
LPAR number (range 0x0-0xf): [0]? 1
Li ESCON Add MPC+ Read Subchannel>exit
```

Figure 571. Adding a read subchannel

You will need to provide the appropriate values for the following parameters:

Device address The unit address transmitted on the channel path to select the 2216 over another device on the channel. It is also referred to as subchannel number in S/370 I/O architecture. It is a two-digit hexadecimal value that may range from 00-FF. This value is defined in the host Input/Output Configuration Program (IOCP) by the UNITADD statement on the CNTLUNIT macro instruction for the real device. The value entered here will relate to the entry made in the TRL major node in VTAM for the *write* subchannel address. Remember that the write subchannel defined to VTAM will be your read subchannel for the 2216 and vice versa. (See Figure 572.)

Link address The ESCON Director (ESCD) port number which is attached to the *host*. Note that this is *not* the ESCD port number on which the 2216 is attached. If you are using EMIF and not an ESCD, then the link address must be set to 1 and the LPAR parameter is used to select the logical partition.

CU address The control unit address defined in the host for the 2216. This must match the entry defined in the host IOCP CUADD parameter in the CNTLUNIT macro.

LPAR number Allows multiple partitions in a logically partitioned (LPAR) host to share one ESCON fiber. If you are using EMIF on the host, the value entered here must be the logical partition number for this connection. If you are using an ESCD, then it must be set to 1.

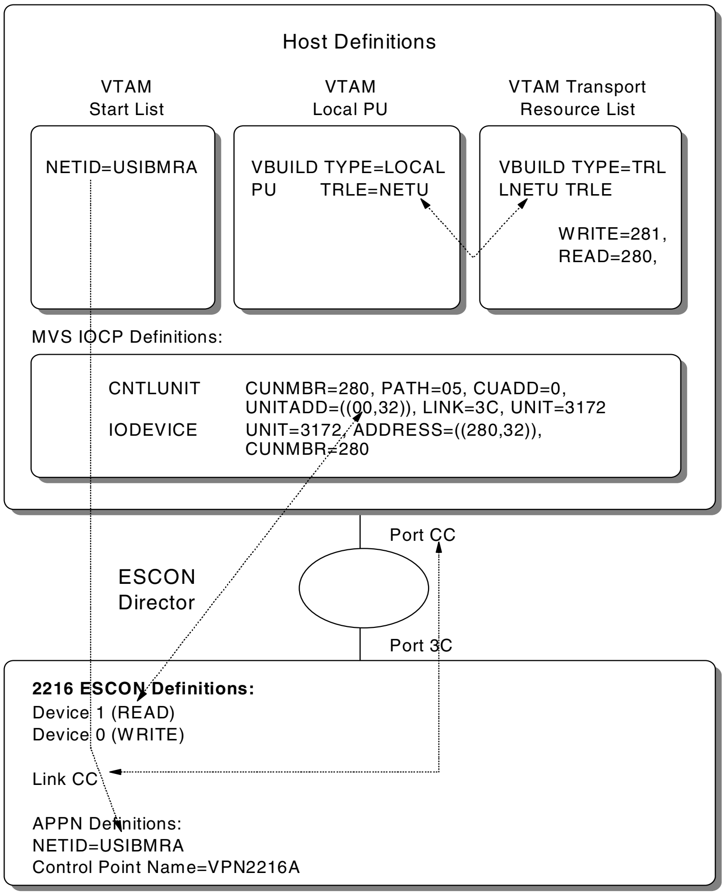


Figure 572. Host/2216 parameter relationships - MPC+

Notes:

1. The device addresses specified in the 2216 MPC+ interface definition must be within the range specified in the UNITADD parameter in the CNTLUNIT macro from the IOCP. For example, the UNITADD parameter in Figure 572 shows that 32 (decimal) device addresses starting at 00 (hex) are being reserved for the 2216 definition. Device addresses 00 and 01 have been specified for the 2216 MPC+ interface. Since 00 and 01 are in the range between 00 and 1F hex, this is OK as long as no other device (or interface on this 2216) tries to use these same subchannels.
2. The values specified in the VTAM TRL major node definition must be within the range specified in the ADDRESS parameter in the IODEVICE macro from the IOCP. For example, the TRL major node definition in Figure 572 specifies 280 and 281 which are in the range between 280 and 29F that the ADDRESS parameter in the IODEVICE statement specifies.
3. The values specified for the ADDRESS parameter in the IODEVICE macro and the UNITADD parameter in the CNTLUNIT macro are related *by convention only*. When defining device addresses on the 2216 MPC+ definition, use the UNITADD parameter and not the ADDRESS parameter to determine the valid range of values.

Because MPC+ operates with at least one subchannel for each direction you need to add a write subchannel address next. This step, shown in Figure 573, is very similar to adding a read subchannel.

```
Li ESCON Add Virtual>sub addw
Li ESCON Add MPC+ Write Subchannel>device
Device address (range 0x00-0xFF): [2]? 0
Li ESCON Add MPC+ Write Subchannel>link
Link address (ESCD Port) (range 0x01-0xFE): [CC]? cc
Li ESCON Add MPC+ Write Subchannel>cu
Control Unit Logical Address (range 0x0-0xF): [0]? 0
Li ESCON Add MPC+ Write Subchannel>lpar
LPAR number (range 0x0-0xf): [1]? 1
Li ESCON Add MPC+ Write Subchannel>exit
```

Figure 573. Adding a write subchannel

Next, we list the subchannels that we just defined to check that we have entered the parameters correctly. This is shown in Figure 574.

```
Li ESCON Add Virtual>sub list
          Read Subchannels:
          Sub  0   Device address   :  1   LPAR number        : 1
                   Link address     : CC   CU Logical Address : 0
          Write Subchannels:
          Sub  1   Device address   :  0   LPAR number        : 1
                   Link address     : CC   CU Logical Address : 0
Li ESCON Add Virtual>exit
```

Figure 574. Listing the configured subchannels

Finally, we list all the interface parameters for our ESCON interface as shown in Figure 575. This shows the listing of the ESCON interface (for which we accepted the defaults) as well as the newly-defined read and write subchannels.

```
Li ESCON Config>list all
Net : 7   Protocol: MPC+   LAN type: MPC+           LAN number:  0
          Maxdata: 2048
          Reply TO : 45000   Sequencing Interval Timer: 3000
          Outbound protocol data blocking is enabled
          Block Timer:    5 ms   ACK length:   10 bytes
          Read Subchannels:
          Sub  0   Dev addr:  1  LPAR: 1  Link addr: CC  CU addr: 0
          Write Subchannels:
          Sub  1   Dev addr:  0  LPAR: 1  Link addr: CC  CU addr: 0
```

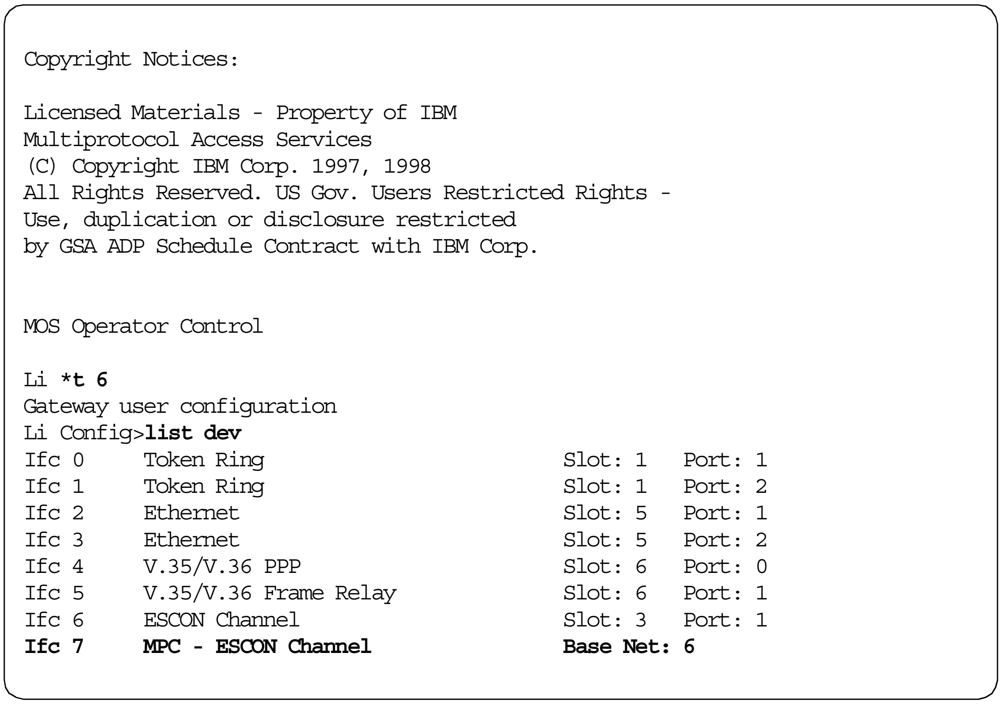
Figure 575. Listing the ESCON interface

This completes the steps necessary to add the ESCON adapter and the MPC+ virtual interface. When you exit the ESCON configuration you will be prompted if you want to keep the changes. You must answer yes. Also, before continuing with the configuration, you need to reload the router. Figure 576 on page 522 shows these steps.

```
Li ESCON Config>exit
ESCON configuration has been changed.
Do you wish to keep the changes? [Yes]: y
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or No orAbort):yes
Config Save: Using bank A and config number 2
The configuration has been saved.
```

Figure 576. Reloading the router

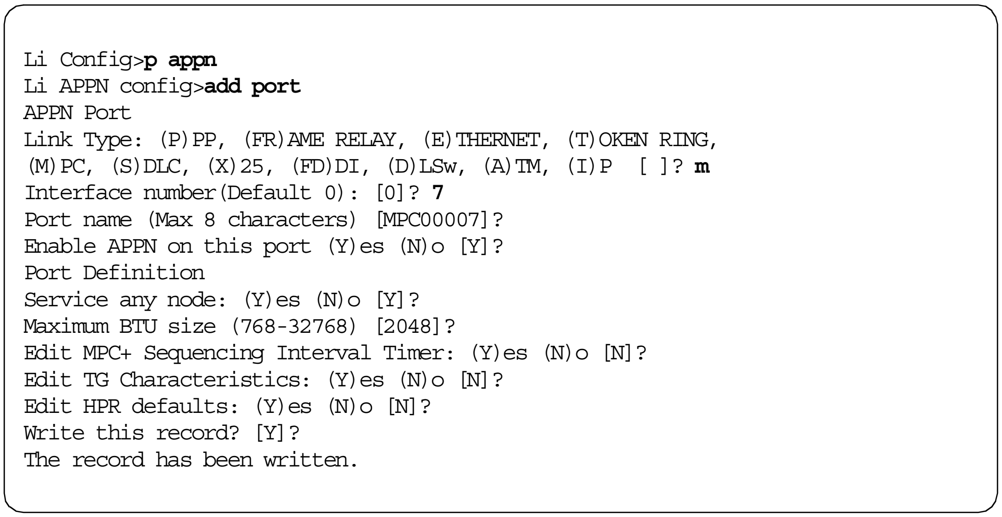
After the router comes back up, use the `list device` command to see the MPC virtual interface that was added in the last step. Figure 577 on page 523 shows that a new MPC+ interface (interface 7) was added to our configuration.



```
Copyright Notices:

Licensed Materials - Property of IBM
Multiprotocol Access Services
(C) Copyright IBM Corp. 1997, 1998
All Rights Reserved. US Gov. Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.


MOS Operator Control

Li *t 6
Gateway user configuration
Li Config>list dev
Ifc 0     Token Ring                        Slot: 1   Port: 1
Ifc 1     Token Ring                        Slot: 1   Port: 2
Ifc 2     Ethernet                          Slot: 5   Port: 1
Ifc 3     Ethernet                          Slot: 5   Port: 2
Ifc 4     V.35/V.36 PPP                     Slot: 6   Port: 0
Ifc 5     V.35/V.36 Frame Relay             Slot: 6   Port: 1
Ifc 6     ESCON Channel                     Slot: 3   Port: 1
Ifc 7     MPC - ESCON Channel               Base Net: 6
```

Figure 577. Checking for the MPC+ interface

The next step is to add an APPN port for our new MPC+ interface. This is done from the APPN protocol menu as shown in Figure 578.



```
Li Config>p appn
Li APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? m
Interface number(Default 0): [0]? 7
Port name (Max 8 characters) [MPC00007]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
Maximum BTU size (768-32768) [2048]?
Edit MPC+ Sequencing Interval Timer: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 578. Adding an APPN port to the MPC+ interface

Note: You might notice that the menus do not prompt you whether to enable High Performance Routing (HPR) on this port. This is because MPC+ supports HPR only. It does not support APPN Intermediate Session Routing (ISR).

Next, we add a link station to the host. This is shown in Figure 579 on page 524. The port name specified is the name of the APPN port that we created in the last step. The adjacent node type is 0 because we defined VTAM as a network node in the VTAM startup parameters.

```
Li APPN config>add link
APPN Station
Port name for the link station [ ]? mpc00007
Station name (Max 8 characters) [ ]? tovtam
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type [0]? 0
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

Figure 579. Adding a link to VTAM

Now we list the complete APPN configuration as shown in Figure 580 on page 525. Note that DLUR is not enabled for this node. DLUR support is not needed on the 2216. In this configuration, the 2216 is merely providing automatic network routing (ANR) services as an intermediate APPN node.

Note: DLUR is needed on the 2210 as it is that router that is providing the DLUR support for the downstream PUs in the branch. We configure DLUR for the 2210 in the next step.

From the port section in the listing, it can be seen that our new MPC+ port has been added and is enabled. In this configuration, we only make use of this port (MPC00007) and the Enterprise Extender port (HPRIP1). The other ports, ETH0IF2 and TOWNTA, are not used in this scenario.

In the link station list, our new link station (TOVTAM) appears. This is the MPC+ connection between the 2216 and the host over the ESCON channel.

```
Li APPN config>list all
NODE :
NETWORK ID: USIBMRA
CONTROL POINT NAME: VPN2216A
XID: 00000
APPN ENABLED: YES
BREX OR BORDER NODE: NEITHER
MAX SHARED MEMORY: 5108
MAX CACHED: 4000
DLUR :
DLUR ENABLED: NO
PRIMARY DLUS NAME:
TN3270 :
TN3270E enabled: NO
TN3270E IP Address: 0.0.0.0
TN3270E Port Number: 23
CONNECTION NETWORK:
      CN NAME       LINK TYPE  PORT INTERFACES
-------------------------------------------------------------
COS :
COS NAME
--------
  #BATCH
#BATCHSC
#CONNECT
  #INTER
#INTERSC
 CPSVCMG
SNASVCMG
MODE:
 MODE NAME  COS NAME
---------------------
PORT ::
  INTF     PORT      LINK      HPR    SERVICE   PORT
 NUMBER    NAME      TYPE    ENABLED    ANY    ENABLED
------------------------------------------------------
     3    TOWNTA   ETHERAND    YES      YES      YES
 65535    HPRIP1     HPR_IP    YES      YES      YES
     2   ETH0IF2   ETHERAND    YES      YES      YES
     7  MPC00007       MPC+    YES      YES      YES
STATION :
 STATION    PORT       DESTINATION      HPR    ALLOW  ADJ NODE
  NAME      NAME         ADDRESS      ENABLED  CP-CP    TYPE
------------------------------------------------------------
 IPLINK1   HPRIP1    192.168.189.59     YES     YES       0
  TOVTAM MPC00007      000000000000     YES     YES       0
LU NAME :
      LU NAME         STATION NAME           CP NAME
------------------------------------------------------------

Li APPN config>
```

Figure 580. Listing the APPN configuration

It is not necessary to restart the router at this point. To activate the changes to the APPN configuration, we simply issue the `activate` command from the `APPN Config>` prompt. This is illustrated in Figure 581 on page 526.

```
Li APPN config>activate
```

Figure 581. Activating the new APPN configuration

This completes the steps necessary to configure the 2216 for this scenario.

28.1.4 Configuring the branch router for DLUR

In Chapter 27, “APPN through an IPSec tunnel” on page 507, we added APPN support on the branch router specifying it as a network node and using HPR over IP to communicate to the 2216 in the data center. For this scenario, the only change necessary to the 2210 configuration is to add the DLUR support to this existing APPN configuration.

Adding DLUR support is quite simple. From the APPN configuration, we specify to enable DLUR. Then, we provide the CP name of the primary DLUS (VTAM). Finally, we activate the DLUR configuration in the router. These steps are shown in Figure 582.

```
Karen *t 6
Gateway user configuration
Karen Config>p appn
Karen APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
Karen APPN config>activate
```

Figure 582. Enabling DLUR in the branch router

Note: For more information about DLUR configuration, refer to *Nways Multiprotocol Routing Services V3.3 Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3865.

This completes the steps necessary to configure the 2210 for DLUR support in this scenario.

28.1.5 Testing DLUR (IPSec disabled)

At this point, the configuration of both routers and the host is complete and IPSec and the IP filters have been temporarily disabled. Now, we need to test the DLUR function before re-enabling IPSec and the packet filters.

In our scenario, we use a PC with PCOMM for OS/2 connected to the token-ring segment on the 2210. This device is configured with one 3270 session back to the host in the data center.

We first check the status of the APPN ports on the 2216. Figure 583 shows that both ports 7 and 8 are in the active (ACT_PORT) state. Remember these are the ports defined for the MPC+ connection and the HPR over IP port respectively.

```
Li *t 5

Li APPN >li port
  Intf        Name       DLC Type        HPR          State
===========================================================
    8       HPRIP1         HPR_IP       TRUE       ACT_PORT
    2      ETH0IF2       ETHERAND       TRUE       ACT_PORT
    3       TOWNTA       ETHERAND       TRUE       ACT_PORT
    7     MPC00007           MPC+       TRUE       ACT_PORT
```

Figure 583. Checking the MPC+ port status

Next, we verify the status of the link stations on the routers. This is shown in Figure 584 on page 527 for the 2216. From the figure, you can see that the MPC+ and HPR over IP links are in the active (ACT_LS) state. (Remember that IPLINK1 is our link station between the routers and TOVTAM is the link station for the MPC+ connection to the host.)

```
Li APPN >li link
    Name   Port Name  Intf       Adj CP Name  Type       HPR      State
=======================================================================
 IPLINK1      HPRIP1     8  USIBMRA.VPN2210A    NN    ACTIVE     ACT_LS
  TOVTAM    MPC00007     7                      NN   ENABLED     ACT_LS
```

Figure 584. Checking the status of the link to VTAM

Finally, we verify that there is an APPC session between the branch router and VTAM. This is done from talk 5 by listing the active APPC sessions as shown in Figure 585. (Remember VTAM is USIBMRA.RA03M.)

```
Karen APPN config>
Karen *t 5
Karen APPN >li appc
LU Name            Mode  Type  FSM
======================================
USIBMRA.RA03M     CPSVRMGR Pri  ACT
USIBMRA.RA03M     CPSVRMGR Sec  ACT
USIBMRA.VPN2216A  CPSVCMG  Pri  ACT
USIBMRA.VPN2216A  CPSVCMG  Sec  ACT
```

Figure 585. Listing the APPC sessions

Note: The CPSVRMGR sessions will not come up until the downstream link to PC B comes up. This triggers the DLUR to activate its DLUR-DLUS session to VTAM.

28.1.6 Retesting DLUR with IPSec enabled

At this point, we can re-enable IPSec and the packet filters to make certain that our configuration works through our VPN tunnel. To re-enable IPSec and access control, we use the same procedures that we used in 25.1.4, “Re-enabling access control and IPSec” on page 490.

After these steps have been performed, we first check the status of the defined tunnels to make sure that they are in fact enabled. This is shown in Figure 586 on page 528 where you can see that our two previously defined tunnels have been re-enabled.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH            192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH      192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  11:05  Jun 20 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  11:05  Jun 20 199
```

Figure 586. Checking IPSec status

Next, we check to see that the APPC sessions are still active on the 2216. This is shown in Figure 587.

```
Karen APPN config>
Karen *t 5
Karen APPN >li appc
LU Name            Mode  Type  FSM
======================================
USIBMRA.RA03M     CPSVRMGR Pri  ACT
USIBMRA.RA03M     CPSVRMGR Sec  ACT
USIBMRA.VPN2216A  CPSVCMG  Pri  ACT
USIBMRA.VPN2216A  CPSVCMG  Sec  ACT
```

Figure 587. Listing the active APPC sessions

Now, to make sure that the APPN traffic is actually going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 588 on page 529. Remember that in this case, tunnel 2 is used since that is the tunnel that HPR over IP traffic is funneled into.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      114414       114414        114414      23581152     13163544     10417608

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         338          338           338         59968        36744        23224

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 588. Checking the IPSec statistics

You can also check the counters on the packet filters as a way to verify that the APPN traffic is going through the IPSec tunnel. Figure 589 on page 530 shows the outbound packet filter for the 2216. Tunnel 2 uses filters 3 and 4.

```
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 692 times, 348 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=346
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=346
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 589. Checking the packet filters

This completes the section for configuration and testing of DLUR through an IPSec tunnel.

Chapter 29. Adding TN3270E server

The TN3270E server function available in both MRS and MAS provides a gateway function for Telnet 3270 clients that are downstream of a SNA host. These clients connect to the gateway using a TCP connection that is mapped to a SNA dependent LU-LU session that the gateway maintains with the SNA host. Thus, the TN3270E server handles the conversion between the TN3270 data stream and a SNA 3270 data stream.

Figure 590 shows the configuration used to produce our TN3270E scenario.

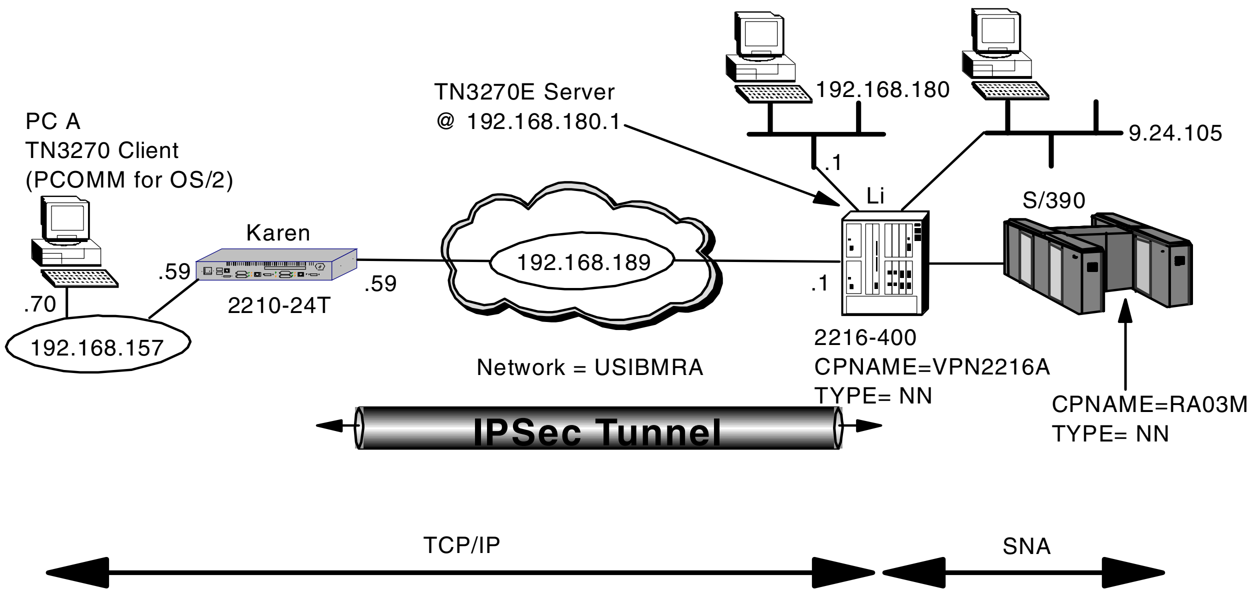


Figure 590. TN3270E through an IPSec tunnel

In our scenario, the TN3270 clients in the branch office connect to the TN3270E server located in the 2216 at the corporate data center. As these connections are TCP based, we use our IPSec tunnel once again to protect them.

Note: We could also configure the 2210 router in the branch as a TN3270E server (instead of putting it in the 2216). The TN3270E server support in MRS/MAS is very flexible and allows you to make the decision to centralize or distribute this function based on your company's requirements. If we had chosen to distribute the TN3270E server function out to the branch, the DLUR configuration would be the same as in Chapter 28, “Adding dependent LU requester” on page 515. The TN3270E server would use the DLUR function configured in the branch router to communicate with the DLUS in VTAM. We would use HPR/IP through our IPSec tunnel between the two routers.

To test our configuration, we placed a PC on the branch token-ring running telnet 3270 (in PCOMM for OS/2). This PC is labeled PC A in the diagram. PC A connects to the TN3270E server in the 2216 located in the corporate data center at IP address 192.168.180.1.

29.1 Configuring TN3270E server in an IPSec environment

The configuration of the 2210 router remains unchanged from that used in the basic IPSec tunnel scenario. (See Chapter 24, “Connecting the data center to the branch office” on page 463.)

For the 2216 in the data center, we start with the APPN configuration used in Chapter 27, “APPN through an IPSec tunnel” on page 507 and we add a TN3270E server and DLUR configuration.

An MRS/MAS TN3270E server can connect to an SNA host either by APPN or by a subarea connection (V3.1 or later). In this case, we chose to use the APPN over MPC+ connection that we defined in Chapter 28, “Adding dependent LU requester” on page 515.

For this configuration, the 2210 in the branch will act as a normal IP router. All TN3270 traffic between the two routers will go through the IPSec tunnel that we have configured. For example, PC A will telnet to the TN3270E server address of 192.168.180.1. (This is an interface address on the 2216.) This TCP/IP traffic will be funneled through the IPSec tunnel 1 previously configured in Chapter 24, “Connecting the data center to the branch office” on page 463 via the inclusive access control that allows traffic from subnet 192.168.157.0 to reach subnet 192.168.180.0.

Note

This scenario was built using MRS and MAS V3.1. The talk 6 prompts for TN3270E server changed slightly for V3.2. If you are using V3.2, the screens in this scenario will not match exactly what you see when you configure this function.

29.1.1 VTAM definitions

As we chose APPN DLUR for the TN3270E server to communicate with the host, we can use the same VTAM definitions that we made in Chapter 28, “Adding dependent LU requester” on page 515. However, we need to make additional VTAM definitions for the PUs used by the TN3270E server. We need to make a definition for each PU in the TN3270E server. For example, each PU in the TN3270E server can support up to 253 LUs. If you need 500 3270 sessions, then you will need two PUs in the router and two PU definitions in VTAM.

Figure 591 on page 533 shows the host VTAM switched major node definition for the TN3270E server PU for our scenario.

```
LOC2216  VBUILD TYPE=SWNET
M2216A  PU     ADDR=01,ISTATUS=ACTIVE,VPACING=0,                     *
               DISCNT=NO,PUTYPE=2,SSCPFM=USSSCS,USSTAB=US327X,       *
               IDBLK=077,IDNUM=02216,IRETRY=YES,MAXDATA=521,         *
               MAXOUT=7,MAXPATH=8,PASSLIM=7,PACING=0,ANS=CONTINUE
*******************************************************************
P2216A   PATH  PID=1,DLCADDR=(1,C,INTPU),DLCADDR=(2,X,07702216),     *
               DLURNAME=M2216A
*******************************************************************
JC7LU2   LU    LOCADDR=2
JC7LU3   LU    LOCADDR=3
JC7LU4   LU    LOCADDR=4
```

Figure 591. VTAM definitions for the TN3270E server configuration

29.1.2 Configuring the 2216 in the data center

As discussed in 25.1.1, “Configuring the data center router” on page 484, we make these configuration additions and test them first with the IPSec feature and IP packet filters disabled. This helps with problem determination if we experience any problems in setting up the TN3270E server.

As a first step to configure the TN3270E server function on the 2216, we need to add the TN3270E server package to the router's IPL sequence. This is shown in Figure 592 on page 533. Once this command has been issued, the TN3270E server module will be loaded during each subsequent IPL of the router.

Important notes

You must have an MAS software load that contains the TN3270E.LD *and* the APPN.LD files in order for this work. Both APPN and subarea connectivity options for the TN3270E server require APPN support to be installed on the router. This is true even though a pure subarea configuration does not use the APPN function. This is an implementation statement as the TN3270E server function uses the APPN SNA stack for both subarea and APPN connections to the host.

```
Li *t 6

Li Config>load add package tn3270e
tn3270e package configured successfully
Li Config>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 3
The configuration has been saved.
```

Figure 592. Configuring the necessary 2216 code modules

Note: The APPN package was already loaded. (See Figure 554 on page 508.)

After the router reloads, we go to the talk 6 APPN protocol menus and we enable DLUR and configure the primary CP name of the DLUS in VTAM. This is shown in Figure 593:

```
Li APPN config>set dlur
Enable DLUR (Y)es (N)o [N]? y
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds) [120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y]?
The record has been written.
```

Figure 593. Enabling DLUR on the 2216

Next, we add a local PU on the 2216. This Local PU will be used by the TN3270E server to establish a CP-CP session to VTAM. Note that the Local Node ID that we configure in Figure 594 is the IDNUM of the switched major node configured on VTAM. (See Figure 591 on page 533.)

```
Li APPN config>add local
Local PU information
Station name (Max 8 characters) []? M2216A
Fully-qualified CP name of primary DLUS []? USIBMRA.RA03M
Fully-qualified CP name of a backup DLUS []?
Local Node ID (5 hex digits) [00000]? 02216
Autoactivate (y/n) [Y]?
Write this record? [Y]?
The record has been written.
```

Figure 594. Configuring a local PU

Note: Each PU can handle 253 LUs, so if we needed more than 253 LUs, we would have to define another local PU that corresponds to another VTAM switched major node with a different IDNUM value.

Next, we enable and configure the TN3270E server. The TN3270E server is configured from within the APPN configuration process. This is shown in Figure 595 on page 535.

```
Li APPN config>set tn3270
TN3270E Server Parameters
Enable TN3270E Server (Y/N) [N]? y
TN3270E Server IP Address []? 192.168.180.1
Port Number [23]?
Keepalive type:
 0 = none,
 1 = Timing Mark,
 2 = NOP [2]?
Frequency ( 1 - 65535 seconds) [60]?
Automatic Logoff (Y/N) [Y]?
 Time (1 - 65535 minutes)  [30]?
Enable IP Precedence (Y/N) [N]?
Write this record? [Y]?
The record has been written.
```

Figure 595. Enabling TN3270E server

Please keep in mind the following notes when configuring the TN3270E server:

IP Address The address that will be used by the TN3270 clients to reach the server. This address can be any interface address or the internal IP address of the router. However, keep in mind that whatever address you use for the TN3270E server will be unavailable to use as a normal telnet to the router unless you change the port number on which the TN3270E server listens.

Reminder

You must configure an IP filter that allows the TN3270E clients to access the IP address that you have defined for the TN3270E server. In this case, from the 192.168.157.0 subnet to the 192.168.180.0 subnet. (See access control number 1 in Figure 489 on page 467.) This access control funnels the TN3270 traffic (and all other IP traffic to/from these subnets) through the IPSec tunnel.

Port Number The port number on which the TN3270E server will listen.

Keepalive Type Whether and how the server polls clients to see if they are still active. Possible values are:

- **None** Server does not poll clients, and will only discover client absence when trying to send data.
- **NOP** Server polls clients at the TCP level. Client software need not have capability to respond.
- **Timing Mark** Server polls clients at the TN3270 level, and client software must respond within a certain time window.

Automatic Logoff Whether or not the server disconnects clients after a period of inactivity (with no data flowing in either direction).

IP Precedence This would be used, for example, if we had put the TN3270E server function on the branch router instead of the data center. It is used when the SNA traffic from/to the TN3270E server is encapsulated in IP packets. If enabled, then the 3 precedence bits in the TOS field of the IPv4 header will be set to a value of

'011'B for all packets between the TN3270E server and the host. This allows you to preserve your SNA priorities when using BRS even on encrypted packets. Please see the *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885 for more information.

Next, we define our downstream LU resources that the clients will access. The downstream LUs can be defined either as explicit or implicit:

- Use explicit definitions when you need to ensure that the device will always use the same LU name. (For example, printers would normally use explicit definitions.)
- Use implicit definitions when you have a large group of devices that can use a common pool of available LUs and do not need to use the same LU name every time.

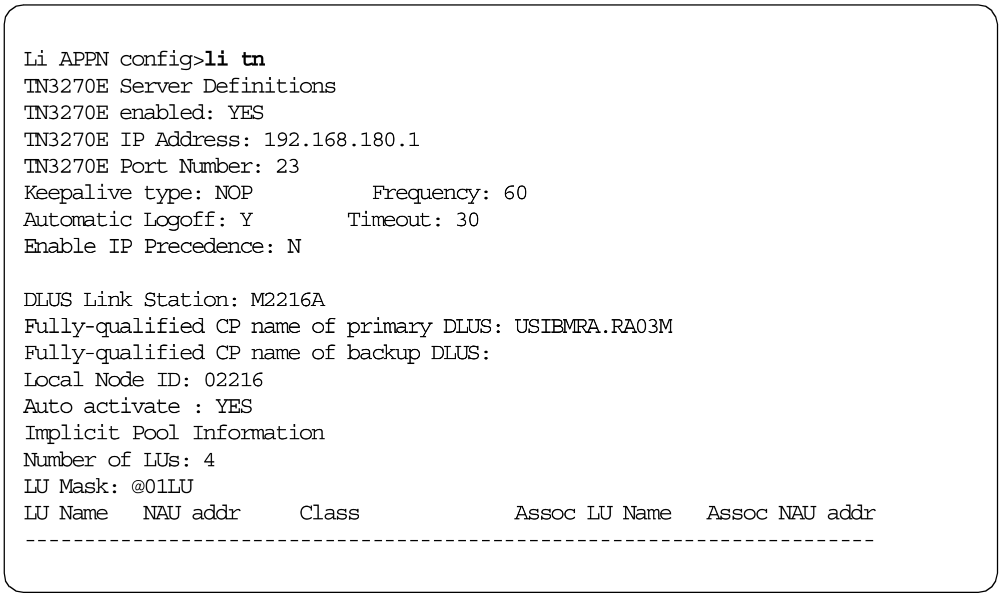
In Figure 596 on page 536, we define an implicit pool of LUs for our TN3270E server. We specify the station name (local PU) from which the LUs will be allocated and specify the number of LUs available in this pool.

```
Li APPN config>add tn imp
TN3270E Server LU Implicit Pool
Station name (Max 8 characters) []? m2216a
LU Name Mask (Max 5 characters) [@01LU]?
Number of Implicit LUs in Pool(1-253) [1]? 4
Write this record? [Y]?
The record has been written.
```

Figure 596. Enabling TN3270E server

The @01LU is a template that will be used to create the actual LU names in the pool. In this example, with 4 LUs in the pool, the LU names generated are 01LU2, 01LU3, 01LU4, and 01LU5, which correspond to LOCADDRs 2-5 for the PU defined in VTAM.

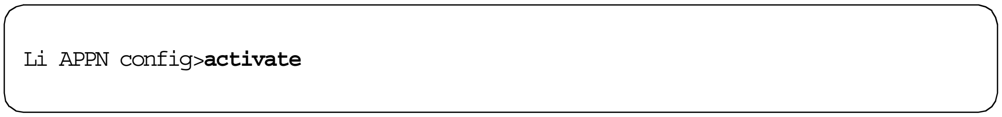
Next, we list our TN3270E server configuration as shown in Figure 597 on page 537 so that we can check our work.



```
Li APPN config>li tn
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 192.168.180.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: Y        Timeout: 30
Enable IP Precedence: N

DLUS Link Station: M2216A
Fully-qualified CP name of primary DLUS: USIBMRA.RA03M
Fully-qualified CP name of backup DLUS:
Local Node ID: 02216
Auto activate : YES
Implicit Pool Information
Number of LUs: 4
LU Mask: @01LU
LU Name   NAU addr     Class            Assoc LU Name   Assoc NAU addr
-----------------------------------------------------------------------
```

Figure 597. Listing TN3270E server configuration

Finally, we activate our changes to the configuration as shown in Figure 598. Note that since we have already enabled APPN previously, we can just issue the `activate` command instead of having to reload the router.



```
Li APPN config>activate
```

Figure 598. Activating the TN3270E server configuration

29.1.3 Testing TN3270E server

Now, it is time to test if the configuration is working as we intended. For this we see if there is an SSCP-LU session between the TN3270E server and client. (We also check our TN3270 client and see if it has an active connection to the host.) From talk 5, in the APPN monitor, we issue the `list tn3270` command as shown in Figure 599 on page 538. As you can see, we have one LU that is in the active state. Since no user is logged on however, the LU is in the SSCP-LU state and not the LU-LU state.

```
Li APPN config>
Li *t 5
Li +p appn
APPN GWCON
Li APPN >li tn3270
TN3270E Server Status Summary

TN3270E IP Address: 192.168.180.1       TN3270E Port Number: 23
  Keepalive type: NOP          Frequency: 60
  Automatic Logoff: Y        Timeout: 30 minutes
  Number of connections: 1
  Number of connections in SSCP-LU state: 1
  Number of connections in LU-LU state: 0
```

Figure 599. Checking the TN3270E server for LU status

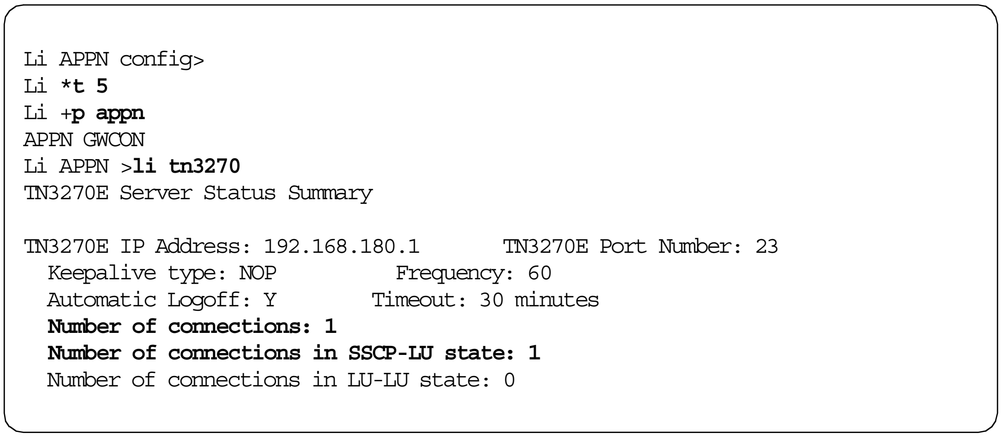
29.1.4 Testing TN3270E server with IPSec enabled

Next, we re-enable access controls and IPSec. Then, check if the TN3270E server is still working. In Figure 600, we check the IPSec status. We see that both our tunnels as well as the IPSec feature are enabled.

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID        Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  ------
      1  ESP&AH            192.168.189.1   192.168.189.59  TUNN   Enable
      2  TRANS-ESP&AH      192.168.189.1   192.168.189.59  TRANS  Enable

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  11:32  Jun 23 199
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  11:32  Jun 23 199
Li IPsec>exit
```

Figure 600. Testing TN3270E server with IPSec enabled

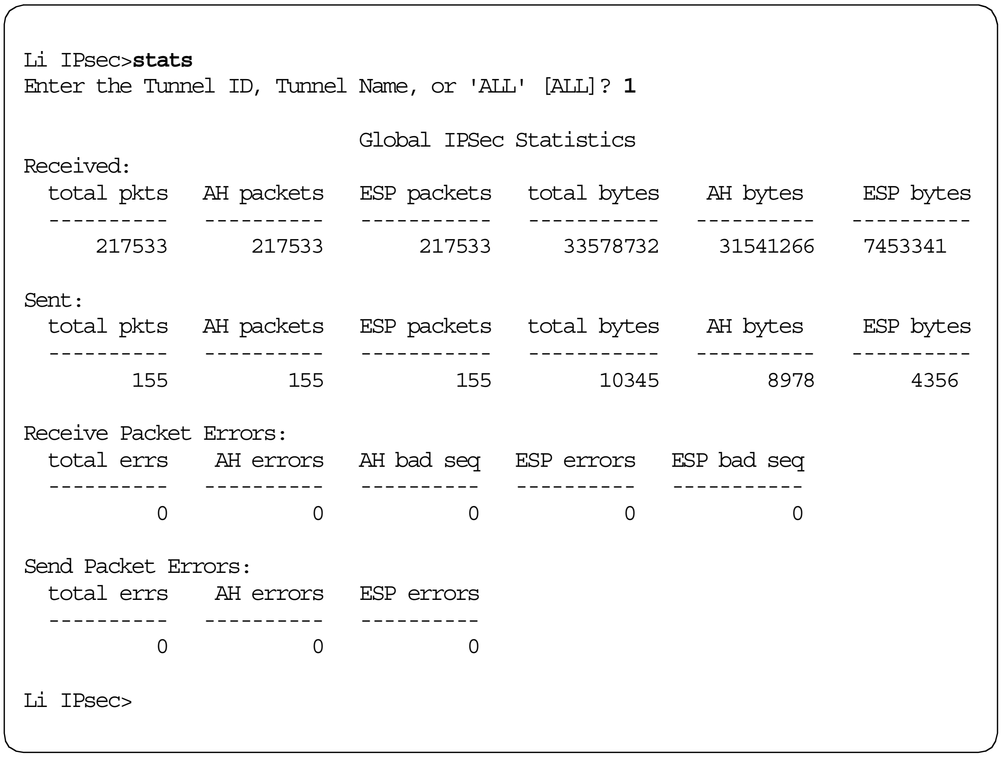
Next, we check to make sure our TN3270E server is still working as shown in Figure 601 on page 539.



```
Li APPN config>
Li *t 5
Li +p appn
APPN GWCON
Li APPN >li tn3270
TN3270E Server Status Summary

TN3270E IP Address: 192.168.180.1      TN3270E Port Number: 23
  Keepalive type: NOP          Frequency: 60
  Automatic Logoff: Y        Timeout: 30 minutes
  Number of connections: 1
  Number of connections in SSCP-LU state: 1
  Number of connections in LU-LU state: 0
```

Figure 601. Checking the status of the TN3270E server

As a double check to make sure that the TN3270 client traffic is going through the IPSec tunnel, we check the IPSec statistics to see if the counters are increasing. This is shown in Figure 602. We check tunnel number 1 this time because that is the tunnel that we specified for all traffic between the 192.168.157.0 subnet and the 192.168.180.0 subnet.



```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

                            Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      217533       217533        217533      33578732     31541266    7453341

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
         155          155           155         10345         8978       4356

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0

Li IPsec>
```

Figure 602. Checking IPSec statistics

Finally, we check the IP packet filter counters to see if they are increasing as shown in Figure 603 on page 540.

```
Li IP>pac pf_out_0
Name             Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0         Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER

Access Control run 308 times, 450 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=150
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=150
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=0
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li IP>
```

Figure 603. Checking the statistics for the packet filters

Remember that the traffic is being generated by the PC on subnet 192.168.157.0, and the TN3270E server is at 192.168.180.1. Therefore we need to check access controls 1 and 3. Number 1 is the access control that funnels the TN3270 traffic to IPSec (traffic between subnets 192.168.157.0 and 192.168.180.0). Number 3 is the access control that allows IPSec-encrypted packets out of the router.

This completes the configuration and testing of the TN3270E server scenario.

Chapter 30. Connecting dial-in remote users

Another application of VPNs is in connecting remote dial-in users to a central site over a public IP network like the Internet. The remote access server can be administrated by an Internet Service Provider (ISP) or by the user's company itself.

In this scenario, we demonstrate how to use the IBM Nways 2210/2216 routers as Remote LAN Access (RLAN) servers using the Layer 2 Tunneling Protocol (L2TP) and Dial In Access to LANs (DIALs) features of the IBM Nways 2210/2216 routers.

The configuration that we used for this scenario is shown in Figure 604:

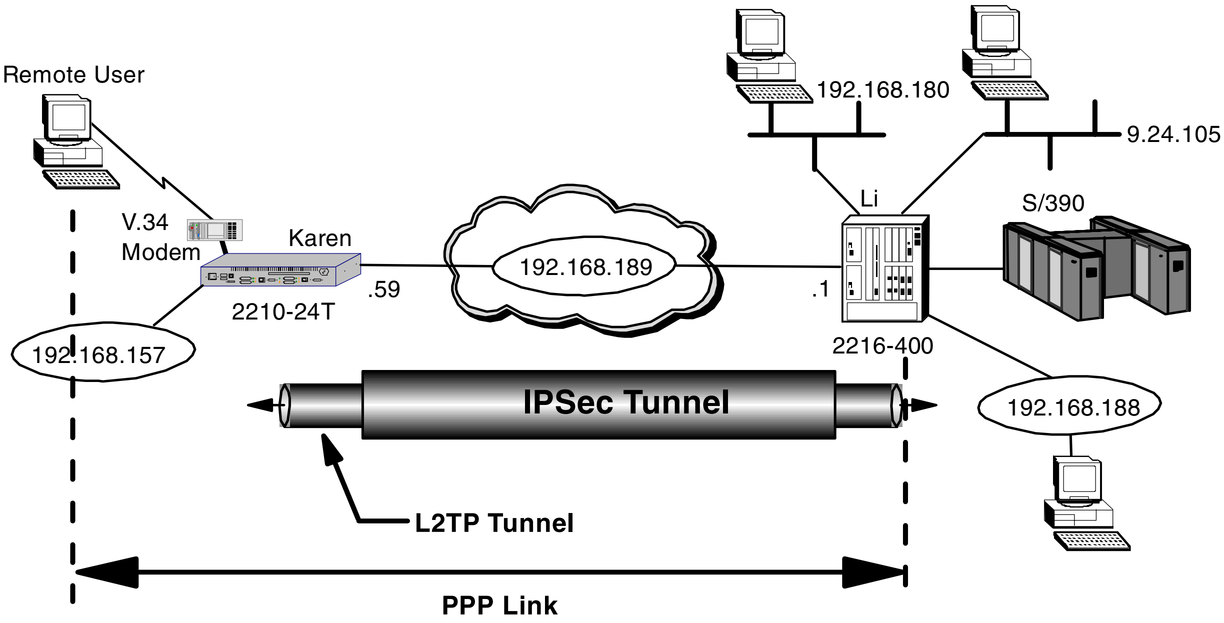


Figure 604. Tunneling an L2TP connection through an IPSec tunnel

For this scenario we use the same hardware configuration that we used for the previous scenarios. However, now the 2210 in the branch will also provide an RLAN server for the remote dial-in users. Also we set up a L2TP tunnel between the branch router and the 2216 in the data center so that the remote users can use the RLAN function in the 2216 to access resources on the corporate intranet.

Since the L2TP connection is IP based, we send this traffic through the IPSec tunnel configured previously between the two routers.

30.1 Configuring the branch router as an RLAN server

We start by adding a configuration to the 2210 that allows a remote user to access the LAN at his local branch using a V.34 dial-up modem.

Note: In our scenario, we demonstrate the use of V.34 for the remote user access. However, the 2210 supports V.34, ISDN BRI, and V.25bis. V.34 is supported using external modems connected to WAN ports or using the 4- or 8-port dial access adapters that provide integrated V.34 modems.

In the next part of this scenario (30.3, “Configuring L2TP in the branch router” on page 551), we extend the remote users' sessions to the corporate data center location over an IP network such as the Internet by using L2TP to tunnel the PPP session from the branch-office 2210 to the central-site 2216.

Note: The IP network could be any IP-based network such as the Internet or a public frame relay network. In our scenario, the IP network is represented by an Ethernet LAN segment.

The first step in the RLAN configuration is to add a V.34 address. This is shown in Figure 605. We give it a logical name and assign a telephone number (based here on the US 10-digit numbering plan). Next, we set the data link control (DLC) protocol for WAN interface number 1 to V.34.

```
Karen *t 6
Gateway user configuration
Karen Config>add v34
Assign address name [1-23] chars []? ifv34_1
Assign network dial address [1-30 digits] []? 9193016666
Karen Config>set data v34
Interface Number [0]? 1
Karen Config>list dev
Ifc 0     Token Ring                  CSR 6000000, vector 95
Ifc 1     V.34 Base Net               CSR  81600, CSR2  80C00, vector 94
Ifc 2     WAN PPP                     CSR  81620, CSR2  80D00, vector 93
Ifc 3     WAN PPP                     CSR  81640, CSR2  80E00, vector 92
Ifc 4     WAN PPP                     CSR  81660, CSR2  80F00, vector 91
Ifc 5     Token Ring                  CSR 6000100, vector 90
Ifc 6     NULL Device                 CSR       0, vector 0
```

Figure 605. Adding a V.34 address and setting the WAN interface to V.34

As can be seen from the figure, when we list the devices, we see that WAN interface number 1 has been changed from the default DLC of PPP to V.34.

The next step is to configure the V.34 interface. This is shown in Figure 606:

```
Karen Config>net 1
V.34 Data Link Configuration
Karen V.34 System Net Config   1>set local
Local network address name   []? ifv34_1
Karen V.34 System Net Config   1>set speed
Line speed (2400 to 460800) [57600]? 57600
```

Figure 606. Configuring the V.34 interface

All that is really necessary here is to map the V.34 port to the V.34 address created in Figure 605 and set up the baud rate of the connection. You can also set the modem initialization string, but in this environment we use the default parameters.

You can check the parameters that you configured with the `list all` command as shown in Figure 607:

```
Karen V.34 System Net Config   1>list all

         V.34 System Net Configuration:

Local Network Address Name    = ifv34_1
Local Network Address         = 9193016666

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         = AT&S1L1&D2&C1X3

Speed (bps)                   = 57600

Karen V.34 System Net Config   1>exit
```

Figure 607. Listing the configuration of the V.34 port

The next step is to create the virtual interfaces used for dial-in connections. RLAN users use a special kind of dial circuit called a *dial-in* circuit (as opposed to the normal dial circuit that a router uses to dial another router). For this scenario we create one virtual interface for our single RLAN test user.

Note: Though we only use one V.34 interface we could create many more. The practical limit is the number of async ports available on the router. We would do precisely the same steps for each V.34 interface available.

The dial-in interfaces are added from the talk 6 `Config>` prompt as shown in Figure 608:

```
Karen Config>add dev dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]? 1
Adding device as interface 7
Base net for this circuit [0]? 1
Defaulting Data-link protocol to PPP
Use "net <intf #>" command to configure circuit parameters

Karen Config>list dev
Ifc 0     Token Ring                   CSR 6000000, vector 95
Ifc 1     V.34 Base Net                CSR  81600, CSR2  80C00, vector 94
Ifc 2     WAN PPP                      CSR  81620, CSR2  80D00, vector 93
Ifc 3     WAN PPP                      CSR  81640, CSR2  80E00, vector 92
Ifc 4     WAN PPP                      CSR  81660, CSR2  80F00, vector 91
Ifc 5     Token Ring                   CSR 6000100, vector 90
Ifc 6     NULL Device                  CSR      0, vector 0
Ifc 7     PPP Dial-in Circuit
```

Figure 608. Creating the virtual dial-in interfaces

Note: Only PPP is supported over V.34. However, with DIALs, we can support multiple protocols (IP, IPX, NetBIOS, 802.2, and LLC) over the PPP connection.

As you can see from the `list devices` command above, the software assigns an interface number to each virtual device. We use this interface number to configure the interface.

The next step is to configure the virtual interfaces. For each dial-in circuit, there are a number of parameters which can be configured; however, these can generally be left at their default values. You can list the default parameters with the `list all` command from the configuration prompt for the interface. An example is shown in Figure 609 for the virtual interface number 7.

```
Karen Config>n 7
Circuit configuration
Karen Circuit config:   7>list all

Base net                       = 1
Destination name               = default_address
Circuit priority               = 8
Destination address:subaddress = 9999999

Inbound dst name               = * ANY *
Outbound calls                 = allowed
Inbound calls                  = allowed
Idle timer                     = 0 (standard circuit)
SelfTest Delay Timer           = 150 ms
LIDs used                      = No

Karen Circuit config:   7>
```

Figure 609. Listing the virtual dial-in interface parameters

The following is a description of these parameters:

- Idle timer

  This parameter generally has no meaning as the inactivity timeout is defined globally, not per interface.

- Inbound calls

  This means that any PPP user is allowed to call. (We could reserve this circuit for a specific user, if required.)

- Outbound calls

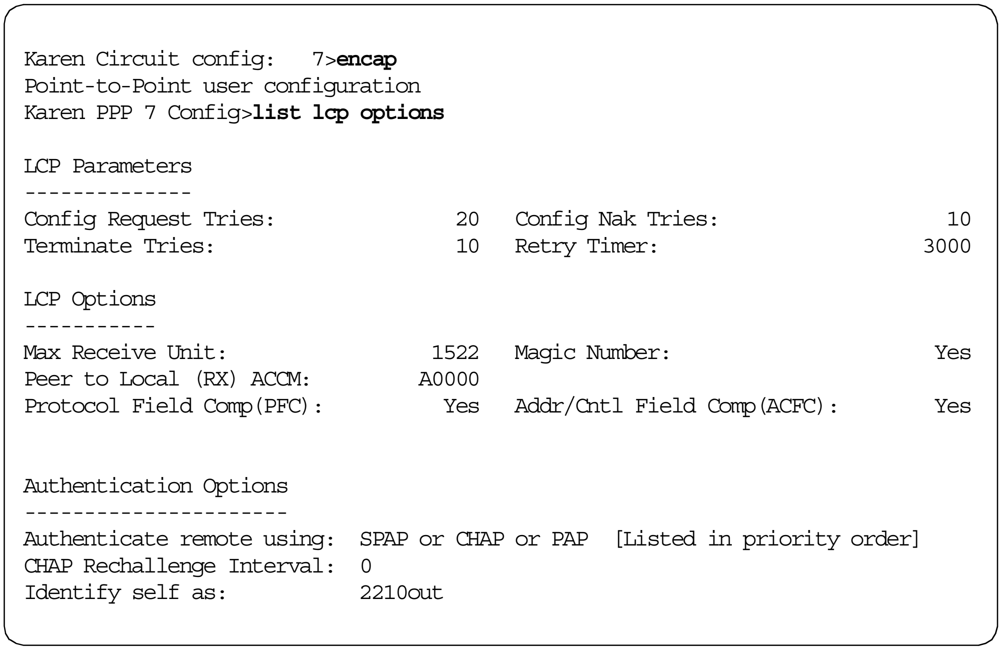
  This does not mean that dial-in circuits can be used for dial-out. This allows a client to be called back, or when connecting using ISDN, allows PPP multilink to form a bundle of multilink channels between the dial-in client and the router.

- Default destination address.

  A default destination address of "default-address" is set up when the dial-in circuit is created. Because these circuits service inbound calls only, and the only outbound calls will be the result of either a callback or a multilink PPP exchange, the destination address is meaningless in this instance. However, the address is required by the software to define the circuit parameters. Do not delete this address or the circuits will come up disabled.

In addition to the parameters for the virtual interface itself, you can also configure the parameters used for the PPP encapsulator for that interface. This is done so that the parameters used at the router will match those used by the dial-in clients. While most of these parameters can be negotiated between the two ends of the PPP link at link activation time, the less negotiation that is necessary, the faster the link will come up.

The prompt for configuring the encapsulator is a sub-menu of the dial-in interface configuration prompt. In Figure 610, we show the default options for the encapsulator using the `list lcp options` command from the encapsulator sub prompt.



```
Karen Circuit config:   7>encap
Point-to-Point user configuration
Karen PPP 7 Config>list lcp options

LCP Parameters
--------------
Config Request Tries:             20   Config Nak Tries:                10
Terminate Tries:                  10   Retry Timer:                   3000

LCP Options
-----------
Max Receive Unit:               1522   Magic Number:                   Yes
Peer to Local (RX) ACCM:       A0000
Protocol Field Comp(PFC):        Yes   Addr/Cntl Field Comp(ACFC):     Yes


Authentication Options
----------------------
Authenticate remote using:  SPAP or CHAP or PAP  [Listed in priority order]
CHAP Rechallenge Interval:  0
Identify self as:           2210out
```

Figure 610. Listing the PPP LCP options

The MRU size can be negotiated by the router with the client. The setting in the router must be at least as large as that on the client. An MRU size of 1522 is needed for the Windows 3.1, OS/2 and DOS versions of the IBM DIALs client. Do not change the default value if one of these clients is being used.

The following notes pertain to the LCP authentication options configured for RLAN:

- SPAP, CHAP and PAP are enabled by default. The router will negotiate with the client in the order that they are listed.
- You must have at least one authentication method enabled on the interface and the client must be configured to use a method that you have enabled on the router.
- The Shiva Password Authentication Protocol (SPAP) allows the clients to change their own password in the router's local authentication database. If you overwrite the router's configuration (for example using the MRS graphical configuration tool), then these password changes will be lost. You can avoid this by reading the router configuration into the router before making the changes and writing the new configuration back to the router.

The next step is to define a PPP user on the 2210 so that we can test it as an RLAN server. The user will be authenticated at the 2210 when he or she dials in. This is shown in Figure 611:

```
Karen Config>add ppp
Enter name:  []? kacir
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]? 192.168.157.40
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user?(Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]


     PPP user name: kacir
            Expiry: <unlimited>
   User IP address: 192.168.157.40
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0

Is information correct? (Yes, No, Quit): [Yes]

User 'kacir' has been added
```

Figure 611. Creating a PPP user continuation

The following notes pertain to adding PPP users for the DIALs function:

Notes:

1. For the first part of this scenario, the user is not tunneled. It is just a straight DIALs scenario at this point. In the next part, we specify that the user is tunneled which is the indication to the router to start an L2TP tunnel to the 2216.
2. The client's IP address is on the same subnet as the destination LAN to which he wishes to connect.
3. Configuring an IP address here means that the IP address will be provided by the user ID to the client. If you leave the IP address at 0.0.0.0, the IP address can be provided by the interface, client or DHCP server.
4. If you enable callback for the user you will be prompted to choose what type of callback you want to use.

Note

For our scenario, we first configure the RLAN function in the branch router so that we can test the dial-in client connecting to the branch office LAN. If you are configuring only the L2TP function so that your clients will tunnel through the branch router and never use the RLAN functions in that router, then the remaining steps are not required on the branch router.

The next step is to define which method we want to use for the clients to obtain an IP address. Remote users dialing into the DIALs server (2210) need to be assigned an IP address that is on the same subnet as the LAN interface to which they wish to connect. There are five methods available:

- Client

  The IP address is configured on the client.

- User ID

  The IP address is configured as part of the User ID definition on the router and sent to the client when it is authenticated. In this case the IP address is associated with a specific user.

- Interface

  The IP address is configured in the interface and sent to the client. Here, the IP address is associated with the interface instead of the User ID.

- DHCP proxy

  The IP address will be provided by a DHCP server and the router acts as a DHCP proxy for the client.

- IP Pool

  MRS/MAS V3.2 introduces a new method called IP pooling that allows you to set up a block of IP addresses that are stored in a pool. When a client connects and requests an IP address, the router retrieves an address from the pool. The command to configure an IP pool is `add ip-pool` and it is issued from the `DIALs config>` prompt.

The methods are configured from the global DIALs menu as shown in Figure 612 on page 548. In our scenario, we use the default settings of the client, user ID and interface methods enabled. The router will attempt to use the first method that is enabled (in the order that is listed).

```
Karen Config>f dial
Dial-in Access to LANs global configuration
Karen DIALs config>li ip
DIALs client IP address specification:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
Karen DIALs config>exit
Karen Config>
```

Figure 612. Listing methods to obtain IP addresses

You can also define primary and secondary domain name servers whose addresses are passed to the client during the IPCP negotiations.

In order to route IP through the V.34 interface, an IP address must be assigned to the interface. When the client dials in, the router automatically adds a static route to its routing table that says the next hop for the remote user is the IP address of the V.34 virtual interface.

The address must be on a different subnet from the destination LAN segment. You can use a real IP address or use unnumbered IP. For unnumbered IP, the format of the address is 0.0.0.n where n is the interface number (for example, for interface 7, the unnumbered IP address would be 0.0.0.7). Figure 613 shows the dialog used for our scenario. Interface 7 is our virtual interface for our test dial-in user.

```
Karen Config>p ip
Internet protocol user configuration
Karen IP config>list add
IP addresses for each interface:
   intf     0   192.168.189.59   255.255.255.0    Local wire broadcast, fill 1
   intf     1                                     IP disabled on this interface
   intf     2                                     IP disabled on this interface
   intf     3                                     IP disabled on this interface
   intf     4                                     IP disabled on this interface
   intf     5   192.168.157.59   255.255.255.0    Local wire broadcast, fill 1
   intf     6                                     IP disabled on this interface
   intf     7                                     IP disabled on this interface
Internal IP address: 192.168.189.59

Karen IP config>add address
Which net is this address for [0]? 7
New address []? 0.0.0.7
Address mask [0.0.0.0]? 255.255.255.0
```

Figure 613. Configuring IP addresses on the virtual interfaces

ARP-subnet routing must be enabled in order to allow the router to respond to ARPs when the next hop to the destination is over a different interface from the interface that is receiving the ARP request. This is the case with RLAN where the client IP address is on the same subnet as the router's LAN interface but the next hop (the V.34 interface) is on a different subnet. ARP-subnet routing is enabled as shown in Figure 614 where we also list our IP addresses to double-check our latest addition.

```
Karen IP config>en arp
Karen IP config>list add
IP addresses for each interface:
   intf     0   192.168.189.59   255.255.255.0    Local wire broadcast, fill 1
   intf     1                                     IP disabled on this interface
   intf     2                                     IP disabled on this interface
   intf     3                                     IP disabled on this interface
   intf     4                                     IP disabled on this interface
   intf     5   192.168.157.59   255.255.255.0    Local wire broadcast, fill 1
   intf     6                                     IP disabled on this interface
   intf     7   0.0.0.7          255.255.255.0    Local wire broadcast, fill 1
Internal IP address: 192.168.189.59
Karen IP config>exit
```

Figure 614. Enabling ARP-subnet-routing

This completes the configuration of the branch router for the basic DIALs function. We restart the router to activate the changes as shown in Figure 615:

```
Karen Config>
Karen *r
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 615. Restarting the router

30.2 Testing RLAN on the branch router

RLAN operation can be confirmed by dialing in from a remote user (using DIALs Client software on a PC) via a V.34 modem. The user should be able to test IP connectivity by pinging the target LAN interface and connecting to any device on that LAN. As this is a multiprotocol connection, other protocols (SNA, NetBIOS) can also be tested.

While there is no specific subsystem in ELS to monitor RLAN connections, there are a number of ways in which correct operation can be confirmed. One way is to monitor inbound calls from ELS (V.34) as shown in Figure 616 on page 550.

```
*t 5
>ev
ELS>nodisp sub all all
ELS>disp sub ip all
ELS>disp sub v34
ELS>
*flush 2
*talk 2

18:54:59   GW.021: Nt up nt 7 int PPP/3
18:55:00   IP.025: add nt 192.168.157.40 rt via 0.0.0.7 nt 7 int PPP/3
18:55:00   IP.068: routing cache cleared
```

Figure 616. Monitoring V.34 inbound calls

From the message `GW.021`, we see when the user dials in and we also see that interface 7 has been allocated to this call.

From the message `IP.025`, we can see the router adding the static route to the client IP address using the unnumbered address that we assigned to interface 7.

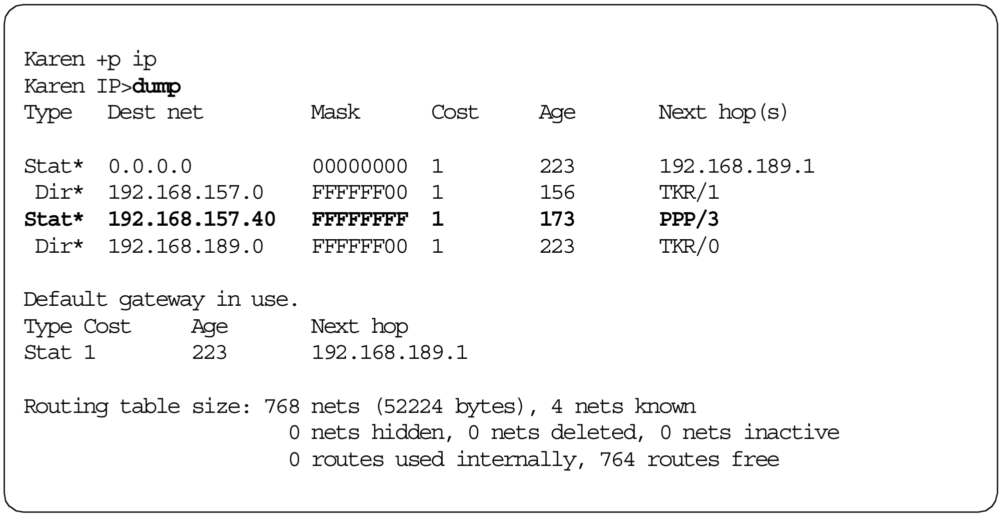
We can also check the state of the PPP link using the `list connection lcp` command under talk 5 for the dial-in interface. From here, we can see the LCP state, the remote user name, the time connected and the LCP options being used by both the local and remote ends of the link. This is shown in Figure 617:

```
Karen +n 7
Point-to-Point Console
Karen PPP 7>li con lcp

Version:                   1
Link phase:                Ready for network traffic (NCP)
LCP State:                 Open
Previous State:            Ack Sent
Time Since Change:         2 minutes and 29 seconds
Remote Username:           kacir
Last Identification Rx'd
Time Connected:            2 minutes and 29 seconds

LCP Option                 Local                       Remote
----------                 -----                       ------
Max Receive Unit:          1500                        1500
Async Char Mask:           A0000                       A0000
Authentication:            C223 (CHAP)                 None
Magic Number:              C6504AB8                    2795AB71
Protocol Field Comp:       Yes                         Yes
Addr/Cntl Field Comp:      Yes                         Yes
32-Bit Checksum:           No                          No
Endpoint Discriminator:    No                          No
Rcv Short Sequence Nums:   -                           -
Link Discriminator:        0                           0
MRRU:                      0                           0
Karen PPP 7>exit
```

Figure 617. Monitoring the dial-in interface

Note: This command can be very useful when you want to compare the LCP options being used at each end during the startup of a new connection.

We can also check the IP route table to see whether the router dynamically created a static route to the client for the virtual PPP interface. This is shown in Figure 618:



```
Karen +p ip
Karen IP>dump
Type  Dest net         Mask      Cost     Age       Next hop(s)

Stat*  0.0.0.0         00000000  1        223       192.168.189.1
 Dir*  192.168.157.0   FFFFFF00  1        156       TKR/1
Stat*  192.168.157.40  FFFFFFFF  1        173       PPP/3
 Dir*  192.168.189.0   FFFFFF00  1        223       TKR/0

Default gateway in use.
Type Cost     Age       Next hop
Stat 1        223       192.168.189.1

Routing table size: 768 nets (52224 bytes), 4 nets known
                      0 nets hidden, 0 nets deleted, 0 nets inactive
                      0 routes used internally, 764 routes free
```

Figure 618. Monitoring the IP route table

From the routing table, we see that the static route has been added to our dial-in client on PPP interface 3 which is the fourth PPP interface on the box and correlates to net 7 (see Figure 608).

30.3 Configuring L2TP in the branch router

Now that we have tested the DIALs function in the local branch router, we extend the dial-in user's PPP connection by setting up an L2TP tunnel between the 2210 in the branch location and 2216 in the data center. The end user should then be able to use the RLAN function in the 2216 to connect to resources in the data center. Since L2TP tunnels PPP over UDP, we can secure these packets with IPSec.

L2TP is a mechanism that involves a tunnel between an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS). In our scenario, the 2210 in the branch will be configured as the LAC and the 2216 will be configured as the LNS.

The first step is to create a tunnel in the LAC. This is shown in Figure 619 on page 552.

```
Karen Config>add tunnel
Enter name:  []? lns.org
Enter hostname to use when connecting to this peer: []? lac.org
set shared secret? (Yes, No): [No] yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.189.1

       Tunnel name: lns.org
          Endpoint: 192.168.189.1
          Hostname: lac.org

User 'lns.org' has been added
```

Figure 619. Creating a tunnel in the LAC

The following notes pertain to the LAC tunnel configuration:

Notes:

1. Tunnel name

   This name should match the hostname which is configured on the LNS (2216).

2. Hostname

   This is the hostname of the LAC.

3. Tunnel-Server endpoint

   The IP address of the endpoint of the tunnel. This address has to be reachable from the LAC. It can be any interface address or an internal IP address on the 2216. Here we use the address of the interface which is the endpoint of the tunnel.

   Remember that in this case, the IP traffic is generated by the router. So we need to have packet filters configured to allow packets to and from the IPSec tunnel endpoints. We already configured the tunnel and the access controls for our router-to-router traffic in our previous configuration (see 24.1.1, “Configuring the branch office router” on page 464).

4. Shared secret

   This parameter must be set if authentication is to be used on the tunnel and the value here must match the value configured in the LNS. L2TP tunnel authentication is enabled by default.

Next, we enable L2TP. This is shown in Figure 620 on page 553. Also, we restart the router in order to activate these changes.

```
Karen Config>f layer
Karen Layer-2-Tunneling Config>en l2tp

 Restart system for changes to take effect.
Karen Layer-2-Tunneling Config>exit
Karen Config>
Karen *r
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

Figure 620. Enabling L2TP in the LAC (branch router)

30.4 Configuring L2TP in the 2216

Now we configure the 2216 as an L2TP Network Server (LNS). We first create the tunnel in the LNS, pointing to the IP address and the name of the LAC. This is shown in Figure 621.

```
Li *t 6
Gateway user configuration
Li Config>add tunnel
Enter name:  []? lac.org
Enter hostname to use when connecting to this peer: []? lns.org
set shared secret? (Yes, No): [No] yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.189.59

       Tunnel name: lac.org
          Endpoint: 192.168.189.59
          Hostname: lns.org

User 'lac.org' has been added
```

Figure 621. Creating a tunnel in the LNS

Note: If you are using shared secrets, the key here must match the one configured in the LAC.

You can modify the PPP parameters for the L2TP tunnel. However, these parameters will be negotiated between the LAC and the LNS. The LAC acts as a proxy for the client PC in the PPP negotiation. Note that an authentication protocol must be enabled for the L2TP tunnel. Figure 622 on page 554 shows a listing of the default PPP parameters on the LNS. None of these parameters needs to be changed for our scenario.

```
Li Layer-2-Tunneling Config>encap
Point-to-Point user configuration
Li PPP-L2TP Config>list all

Disabled as a Multilink PPP Link


LCP Parameters
--------------
Config Request Tries:              20   Config Nak Tries:                   10
Terminate Tries:                   10   Retry Timer:                      3000

LCP Options
-----------
Max Receive Unit:                2048   Magic Number:                      Yes
Peer to Local (RX) ACCM:        A0000
Protocol Field Comp(PFC):          No   Addr/Cntl Field Comp(ACFC):         No

Authentication Options
----------------------
Authenticate remote using:  SPAP or CHAP or PAP  [Listed in priority order]
CHAP Rechallenge Interval:  0
Identify self as:           ibm


NCP Parameters
Config Request Tries:              20   Config Nak Tries:                   10
Terminate Tries:                   10   Retry Timer:                      3000


Dial-in Access to LANs ENABLED




CCP Options
-----------
Data Compression disabled
Algorithm list: none
STAC histories: 1
STAC check_mode: SEQ


ECP Options
-----------
Data Encryption disabled
Algorithm list: DES
DESE (Data Encryption Standard Encryption Protocol)

BCP Options
-----------
Tinygram Compression:         Disabled


IPCP Options
------------
IPCP Compression:                None
Send Our IP Address:               No
Remote IP Address to Offer if Requested: None
Li PPP-L2TP Config>
```

Figure 622. Listing PPP parameters for L2TP connections

Next, we enable L2TP in the LNS as shown in Figure 623 on page 555.

```
Li Config>f layer
Li Layer-2-Tunneling Config>en l2tp

 Restart system for changes to take effect.
```

Figure 623. Enabling L2TP in the LNS

Next, we add the virtual interfaces over which the PPP connections will be terminated. These are analogous to the dial-in interface that we added in the branch router when we configured it for the DIALs function. Except in this case, the users are coming in through an L2TP tunnel instead of a V.34 interface.

In the LNS, these are added from the L2TP feature configuration prompt. (In the LAC, they were added from the talk 6 main prompt.) This is shown in Figure 624 on page 555.

```
Li Layer-2-Tunneling Config>add l2
Additional L2 nets:  [0]? 3
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 8
Defaulting data-link protocol to PPP
Adding device as interface 9
Defaulting data-link protocol to PPP
Adding device as interface 10
Defaulting data-link protocol to PPP
Enable IPX on L2TP interfaces?(Yes or [No]):
Enable transparent bridging on L2TP interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
Li Layer-2-Tunneling Config>exit
Li Config>
```

Figure 624. Adding the virtual interfaces

In order to route IP through the L2 nets, an IP address must be assigned to the interface. When the client establishes the PPP connection through the L2TP tunnel, the router automatically adds a static route to its routing table that says that the next hop for the remote user is the IP address of the L2TP virtual interface. The address must be on a different subnet from the destination LAN segment.

The IP addresses for these interfaces are added when you create the interfaces. By default, they are unnumbered IP addresses. The format of the address is 0.0.0.n where n is the interface number (for example, for interface 8, the unnumbered IP address would be 0.0.0.8).

Note: If you need to change the default IP address associated with an L2TP net, you can do so using the IP config prompt in talk 6. However, unnumbered IP addressing works very well for RLAN because users connect to an L2TP net arbitrarily and the particular IP address associated with an L2TP net is not very critical.

ARP-subnet routing must be enabled in order to allow the router to respond to ARPs when the next hop to the destination is over a different interface from the interface that is receiving the ARP request. This is the case with RLAN where the client IP address is on the same subnet as the router's LAN interface, but the next hop (the L2TP virtual interface) is on a different subnet. ARP-subnet-routing is enabled as shown in Figure 625:

```
Li config>p ip
Li IP config>en arp
Li IP config>exit
Li config>
```

Figure 625. Enabling ARP-subnet-routing

The next step is to define which method we want to use for the clients to obtain an IP address. In this regard, the DIALs server in the 2216 needs to be configured just as if the users were dialing in using ISDN or V.34 rather than tunneling in through an L2TP tunnel. The steps that are necessary are identical to the ones that we performed for the branch router.

DIALs users need to be assigned an IP address that is on the same subnet as the LAN interface to which they wish to connect. There are five methods available:

- Client

  The IP address is configured on the client.

- User ID

  The IP address is configured as part of the User ID definition on the router and sent to the client when it is authenticated. In this case the IP address is associated with a specific user.

- Interface

  The IP address is configured in the interface and sent to the client. Here, the IP address is associated with the interface instead of the User ID.

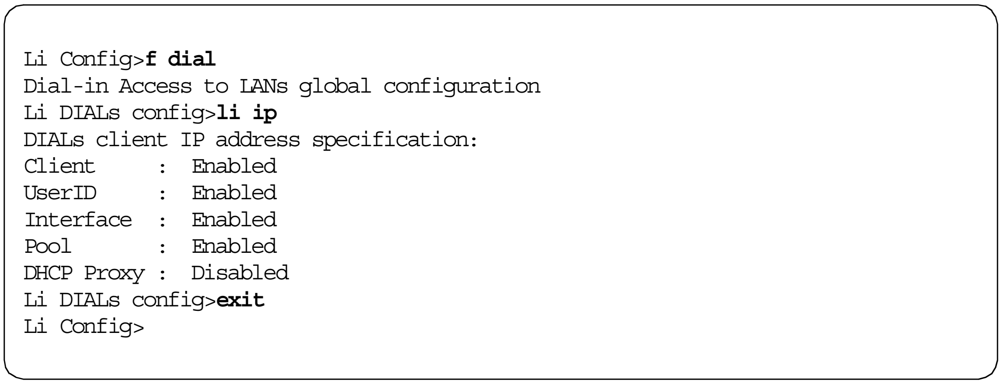
- DHCP Proxy

  The IP address will be provided by a DHCP server and the router acts as a DHCP proxy for the client.

- IP Pool

  MRS/MAS V3.2 introduces a new method called IP pooling that allows you to set up a block of IP addresses that are stored in a pool. When a client connects and requests an IP address, the router retrieves an address from the pool. The command to configure an IP pool is `add ip-pool` and it is issued from the `DIALs config>` prompt.

The methods are configured from the global DIALs menu as shown in Figure 626 on page 557. In our scenario, we use the default settings of the client, user ID and interface methods enabled. The router will attempt to use the first method that is enabled (in the order that is listed).



```
Li Config>f dial
Dial-in Access to LANs global configuration
Li DIALs config>li ip
DIALs client IP address specification:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
Li DIALs config>exit
Li Config>
```

Figure 626. Listing methods to obtain IP addresses

You can also define primary and secondary domain name servers whose addresses are passed to the client during the IPCP negotiations.

At this point we have the tunnel configured in both the LNS and LAC and the DIALs feature has been configured in the LNS.

Note: The DIALs feature is also configured in the LAC, but this was because we wanted to use the branch router as an RLAN server also. If we had just wanted to use it to tunnel users over to the LNS, then configuring the DIALs function in the branch router would not have been necessary.

Now we configure the PPP users that will tunnel to the LNS. There are two ways to configure the PPP users to be tunneled:

- Rhelm-based tunneling

  Using this method, you only need to define the user at the LNS. You must use the format username@domain where domain is the hostname of the LNS. When the client dials into the LAC using the username@domain format (for example, Steven@lns.org), the LAC will create a tunnel to the specified domain (lns.org) and the PPP connection will be tunneled to the desired destination. With this method, all users with the same domain name are tunneled to the same destination.

- User-based tunneling

  With this method, the user's profile has to be configured at both the LAC and the LNS, and does not use the username@domain format. In the LAC you specify, in the user's profile, where the end destination is. In the LNS, you configure a normal dial-up user.

Figure 627 on page 558 shows the definition of a Rhelm-based user on the 2216 in the data center.

```
Li Config>add ppp
Enter name:  []? steven@lns.org
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]


     PPP user name: steven@lns.org
            Expiry: <unlimited>
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname: <undefined>
      Time alotted: Box Default
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0

Is information correct? (Yes, No, Quit): [Yes]

User 'steven@lns.org' has been added
```

Figure 627. Adding a Rhelm-based L2TP user

For user-based tunneling, we define the ID in both the LAC and LNS. Figure 628 shows the definition of a user-based ID on the 2210 in the branch office.

```
Karen Config>add ppp
Enter name:  []? garth
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connecting to this peer: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.189.1

     PPP user name: garth
          Endpoint: 192.168.189.1
          Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes]

User 'garth' has been added
```

Figure 628. Adding a user-based tunneling user in the 2210 (LAC)

We define this user to be tunneled which is the router's notification to set up the L2TP tunnel when this user dials in. We then specify the destination IP address of the other tunnel endpoint as well as the hostname of the 2210 to use when creating the tunnel.

Note: As soon as we specify that this user will be tunneled, the router knows enough not to ask us about whether we want the DIALs function enabled for this user, what the IP address of the client should be, or any of the other parameters that you are prompted for when defining a DIALs user. This is because the DIALs function for this user is being provided by the 2216. The 2210 is merely providing a gateway service to the 2216.

Figure 629 shows the definition of the same user-based ID on the 2216 in the data center. Here, we define a normal DIALs user. This user is not a tunneled user because by the time he is authenticated by the DIALs function, the L2TP headers have all been stripped off and the packets are just normal PPP packets.

```
Li Config>add ppp
Enter name:  []? garth
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No] no
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]
           PPP user name: garth
              Expiry: <unlimited>
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname:
     Time allotted: Box Default
     Callback type: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0

Is information correct? (Yes, No, Quit): [Yes]

User 'garth' has been added
```

Figure 629. Adding a user-based tunneling user in the 2216 (LNS)

This completes the configuration of the LNS. We need to reload the 2216 in order to activate these changes. This is shown in Figure 630 on page 560.

```
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
The configuration has been saved.
```

Figure 630. Reloading the 2216 (LNS)

30.5 Testing L2TP (IPSec disabled)

Now that we have the configuration in place, we test the L2TP and RLAN configuration. We can test L2TP by dialing in from the remote PC, first with the Rhelm-based user ID, and then with the User-based ID. We can test IP connectivity using PING from the PC client to the 2216.

We can monitor L2TP from ELS using `disp sub l2 all`. A sample talk 2 session from the 2216 LNS is shown in Figure 631:

```
Li *t 2
00:00:42   GW.001:

Copyright 1984 Massachusetts Institute of Technology,
Copyright 1989 The Regents of the University of California

00:12:12   L2.024: PAYLOAD SEND 38 bytes, net=10, callid=17957
00:12:12   L2.041: SND F=4902,L=50,Tid=58577,Cid=31030,NS=56,NR=54,O=0
00:12:12   L2.040: RCV F=4800,L=12,Tid=30892,Cid=17957,NS=54,NR=57,O=0
00:12:12   L2.043: RCV PAYLOAD Zero Len Body (ZLB), tid=30892,cid=17957
00:12:12   L2.040: RCV F=4900,L=50,Tid=30892,Cid=17957,NS=54,NR=57,O=0
00:12:12   L2.022: PAYLOAD RCVD 38 bytes, net 10, callid=17957
00:12:12   L2.023: Send PAYLOAD Zero Len Body (ZLB), tid=58577,cid=0
00:12:12   L2.041: SND F=4802,L=12,Tid=58577,Cid=31030,NS=57,NR=55,O=0
```

Figure 631. Monitoring L2TP from ELS

We can also check the L2TP tunnel state from talk 5 as shown in Figure 632:

```
Li Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID |    State    | Time Since Chg | # Calls | Flags
    30892 | L2TP |   58577 | Established |     0: 4:31    |       1 |  TL  F

Li Layer-2-Tunneling Console>exit
```

Figure 632. Monitoring L2TP from talk 5

30.6 Testing L2TP with IPSec enabled

Now it is time to re-enable IPSec and verify that L2TP is still working.

After IPSec is re-enabled, we first check the IPSec tunnel's status with the `list all` command as shown in Figure 633:

```
Li +f ip
Li IPsec>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID        Name        Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  ESP&AH            192.168.189.1   192.168.189.59  TUNN   Enabled
      2  TRANS-ESP&AH      192.168.189.1   192.168.189.59  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  --------------  --------------  -----  ------  -----------------
    2    192.168.189.1   192.168.189.59  TRANS  ESP-AH  17:01  Jun 25 1998
    1    192.168.189.1   192.168.189.59  TUNN   ESP-AH  17:01  Jun 25 1998
Li IPsec>exit
Karen +
```

Figure 633. Verifying the IPSec tunnels are enabled

We then verify that the L2TP tunnel is still working.

```
Li Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID |    State    | Time Since Chg | # Calls | Flags
    30892 | L2TP |   58577 | Established |     0: 5:29    |       1 |  TL  F

Li Layer-2-Tunneling Console>exit
```

Figure 634. Monitoring L2TP with IPSec enabled

To be sure that IPSec tunnel number 2 is being used for the L2TP traffic, we check the IPSec statistics and see if the send and receive counts are increasing. This is shown in Figure 635 on page 562.

```
Li IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 2

                       Statistics For Secure Tunnel 2
Received:
  total pkts   AH packets   ESP packets   total bytes   AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
      357842       178921        178921      36722368     20508236     16214132

Sent:
  total pkts   AH packets   ESP packets   total bytes   AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
       80058        40029         40029       8401232      5001196      3400036

Receive Packet Errors:
   AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   -----------
           0            0            0             0

Send Packet Errors:
   AH errors   ESP errors
  ----------   ----------
           0            0
```

Figure 635. Checking the IPSec statistics

We also check the IP packet filters to see how many times the filters were hit. This is shown in Figure 636 on page 563.

```
Li +p ip
Li IP>pac pf_out_0
Name              Dir  Intf  State  Src-Addr-Ver  #Access-Controls
pf_out_0          Out  0     On     N/A           4

Access Control currently enabled
Access Control facility: USER


Access Control run 808   times, 0 cache hits

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=4
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0    Use=0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=400
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255  Use=400
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
```

Figure 636. Checking the packet filters

Note: Remember that in this case, the router is generating the traffic, so we need to look at access controls number 3 and 4. We see that they have been matched 400 times (Use=400).

This completes the configuration and testing of L2TP over an IPSec tunnel.

Part 4. Basic router configuration

Chapter 31. Basic router configuration with MRS/AIS/MAS V.3.3

Before an IPSec tunnel can be defined, you need to have a valid IP configuration in the router. This consists of defining the hardware interfaces (2216) and adding IP interface addresses and subnetmasks. There are several ways to accomplish this task:

- Config Only mode (2216)
- EasyStart (2210)
- Explicit Talk 6 commands
- The Configuration program
- Quick config process

Since there is no significant change for this process from CC4, we show only the CC5 `qcongif` command for the 2216 at the branch in this appendix.

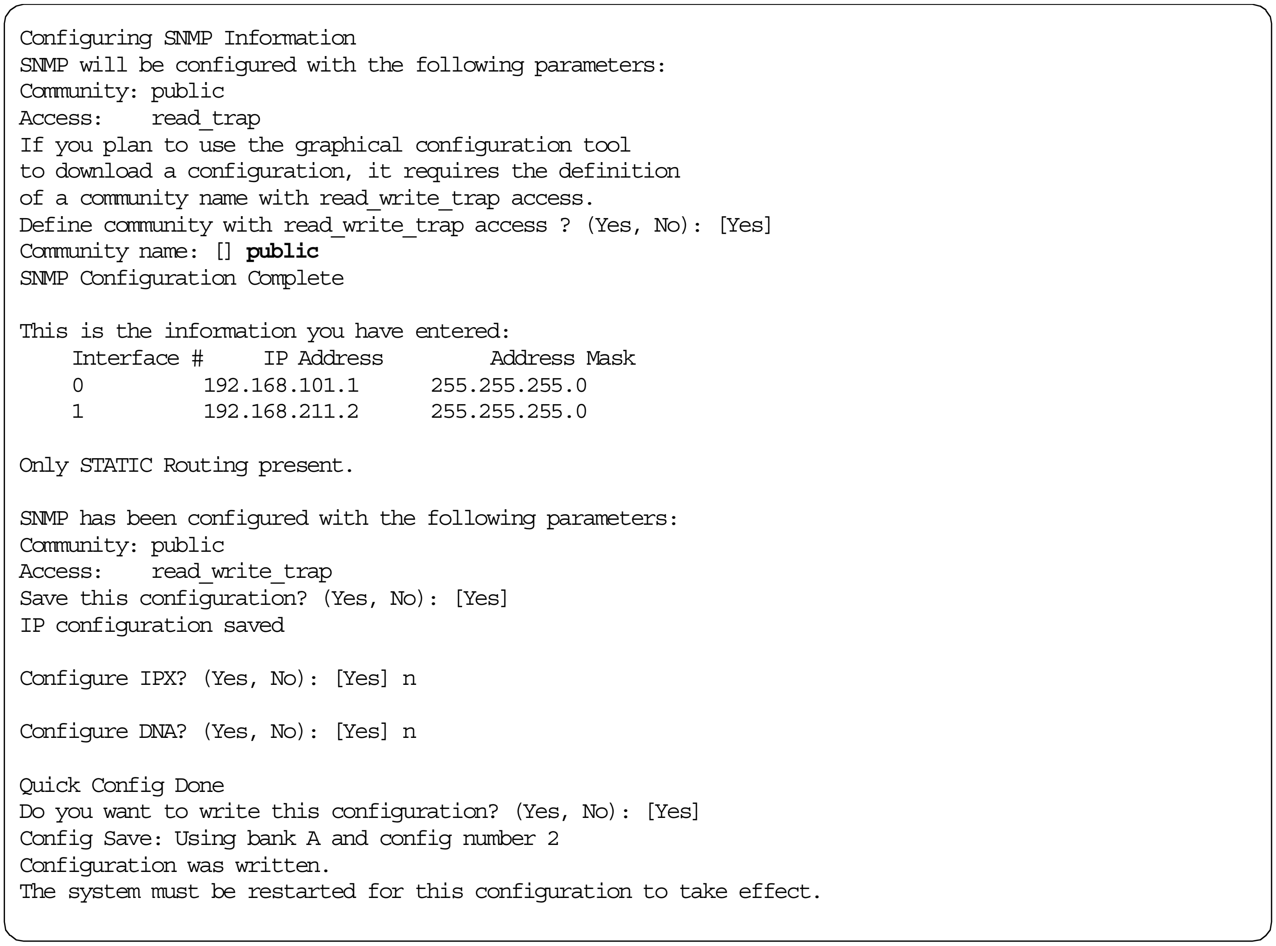
The `qconfig` command can be used to configure most of the functions of the router. Here, we just use it to define the physical interfaces and the IP addresses on these interfaces to get a valid IP configuration installed on the router.

For more information on configuring the 2210 or the 2216, please see *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I*, SG24-4446 or *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*, SG24-4957, respectively.

The sections below take you step-by-step through the `qconfig` command dialogs from the `talk 6` command prompt on the 2216 that we used in our scenarios. Our purpose was to obtain a valid IP configuration so that it could be used as a base configuration for IPSec tunnel definitions. Figure 638 shows these configuration screens.

```
Config>set hostname Branch
Host name updated successfully
Branch Config>QCONFIG
Router Quick Configuration for the following:
    No   Bridging
    Spanning Tree Bridge (STB)
    Source Routing Bridge (SRB)
    Source Routing/Transparent Bridge (SR/TB)

    No   Protocols
    IP (including OSPF, RIP and SNMP)
    IPX
    DNA (DECnet)

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
**********************************************************
Bridging Configuration
**********************************************************
Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config
Configure Bridging? (Yes, No, Quit): [Yes] n
**********************************************************
Protocol Configuration
**********************************************************
Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config
Configure Protocols? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Protocol Configuration
Configure IP? (Yes, No): [Yes]
Type 'r' any time at this level to restart IP Configuration
IP Configuration is already present
Configure IP anyway? (Yes, No): [No] y
Configuring Per-Interface IP Information
Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [172.16.220.253] 192.168.101.1
Address Mask: [255.255.255.0]
Configuring Interface 1 (EIA-232E/V.24 PPP)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [192.168.141.56] 192.168.211.2
Address Mask: [255.255.255.0]
Configuring Interface 2 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes] n
Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes] n
Only Static Routing Enabled
Routing Configuration Complete
```

Figure 637. Quick configuration (QCONFIG) of the 2216



```
Configuring SNMP Information
SNMP will be configured with the following parameters:
Community: public
Access:    read_trap
If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.
Define community with read_write_trap access ? (Yes, No): [Yes]
Community name: [] public
SNMP Configuration Complete

This is the information you have entered:
    Interface #     IP Address         Address Mask
    0          192.168.101.1      255.255.255.0
    1          192.168.211.2      255.255.255.0

Only STATIC Routing present.

SNMP has been configured with the following parameters:
Community: public
Access:    read_write_trap
Save this configuration? (Yes, No): [Yes]
IP configuration saved

Configure IPX? (Yes, No): [Yes] n

Configure DNA? (Yes, No): [Yes] n

Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
Config Save: Using bank A and config number 2
Configuration was written.
The system must be restarted for this configuration to take effect.
```

Figure 638. Quick configuration (QCONFIG) of the 2216 (continued)

Chapter 32. Basic configuration with MRS/MAS V.3.1 and 3.2

Before an IPSec tunnel can be defined, you need to have a valid IP configuration in the router. This consists of defining the hardware interfaces (2216) and adding IP interface addresses and submasks. There are several ways to accomplish this task.

- Config Only mode (2216)
- EasyStart (2210)
- Explicit Talk 6 commands
- The configuration program
- Quick config process

In this appendix, we show you the quick config process that we used to build the network shown in Figure 484 on page 463. The *qconfig* process can be used to configure most of the functions of the router. Here, we just use it to define the physical interfaces and the IP addresses on these interfaces to get a valid IP configuration installed on the router.

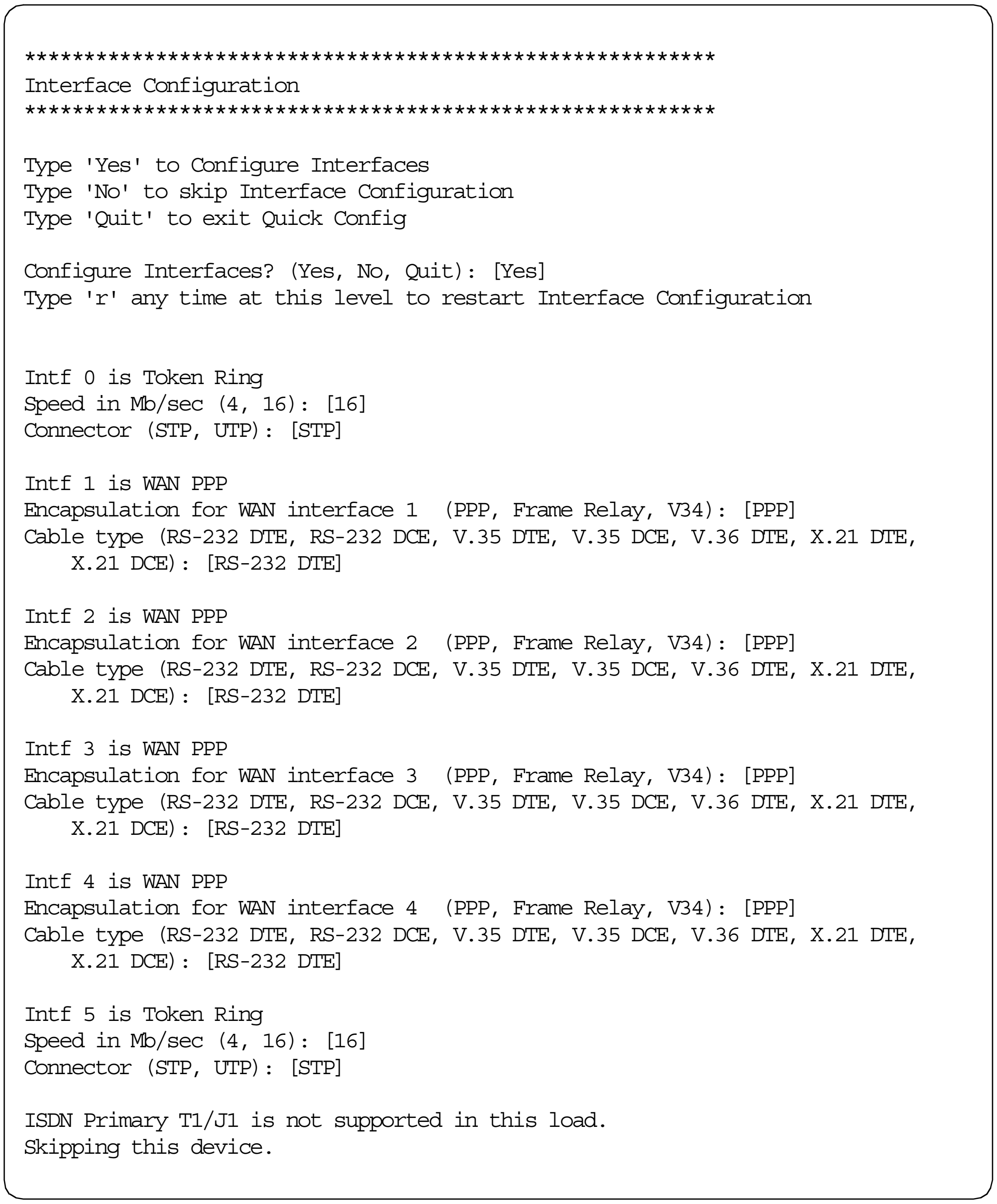
For more information on configuring the 2210 or the 2216, please see *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios Volume I*, SG24-4446 or *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*, SG24-4957, respectively.

32.1 Quick config of the 2210 in the branch office

The sections below take you step by step through the qconfig command dialogs from the talk 6 command prompt on the 2210-24T that we used in our scenarios. Our purpose was to obtain a valid IP configuration so that it could be used as a base configuration for IPSec tunnel definitions. Figure 639 on page 572 through Figure 644 on page 577 show these configuration screens.

```
*t 6
Config>set hostname Karen
Host name updated successfully
Karen Config>qconfig

Router Quick Configuration for the following:
o   Interfaces
o   Multilink PPP (w/o DIALs)
o   Dial Circuits (w/o DIALs)
o   Dial-in Access to LANs (DIALs)
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP and SNMP)
        IPX
        DNA (DECnet)
o   Booting
o   Service Port

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

Figure 639. Quick configuration (QCONFIG) of the 2210



```
**********************************************************
Interface Configuration
**********************************************************

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit Quick Config

Configure Interfaces? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Interface Configuration


Intf 0 is Token Ring
Speed in Mb/sec (4, 16): [16]
Connector (STP, UTP): [STP]

Intf 1 is WAN PPP
Encapsulation for WAN interface 1  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 2 is WAN PPP
Encapsulation for WAN interface 2  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 3 is WAN PPP
Encapsulation for WAN interface 3  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 4 is WAN PPP
Encapsulation for WAN interface 4  (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
    X.21 DCE): [RS-232 DTE]

Intf 5 is Token Ring
Speed in Mb/sec (4, 16): [16]
Connector (STP, UTP): [STP]

ISDN Primary T1/J1 is not supported in this load.
Skipping this device.
```

Figure 640. Quick configuration (QCONFIG) of the 2210

```
This is all configured device information:

Intf 0 is Token Ring, Speed 16 Mb/sec, Connector UTP
Intf 1 is WAN PPP, RS-232 DTE cable
Intf 2 is WAN PPP, RS-232 DTE cable
Intf 3 is WAN PPP, RS-232 DTE cable
Intf 4 is WAN PPP, RS-232 DTE cable
Intf 5 is Token Ring, Speed 16 Mb/sec, Connector UTP
Intf 6 is ISDN Primary T1/J1

Save this configuration? (Yes, No): [Yes]

Device  configuration saved

**********************************************************
Multilink PPP Configuration (w/o DIALs)
**********************************************************

Type 'Yes' to Configure Multilink PPP
Type 'No' to skip Multilink PPP Configuration
Type 'Quit' to exit Quick Config

Configure Multilink PPP? (Yes, No, Quit): [Yes] no

**********************************************************
Dial Circuit Configuration (w/o DIALs)
**********************************************************

Type 'Yes' to Configure Dial Circuits
Type 'No' to skip Dial Circuits Configuration
Type 'Quit' to exit Quick Config

Configure Dial Circuits? (Yes, No, Quit): [Yes] no

**********************************************************
Dial-in Access to LANs (DIALs) Configuration
**********************************************************

Type 'Yes' to Configure DIALs Configuration
Type 'No' to skip DIALs Configuration Configuration
Type 'Quit' to exit Quick Config

Configure DIALs Interfaces? (Yes, No, Quit): [Yes] no

Configure DIALs Server? (Yes, No, Quit): [Yes] no
```

Figure 641. Quick configuration (QCONFIG) of the 2210

```
**********************************************************
Bridging Configuration
**********************************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes] no

**********************************************************
Protocol Configuration
**********************************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Protocol Configuration

Configure IP? (Yes, No): [Yes]
Type 'r' any time at this level to restart IP Configuration

Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.189.59
Address Mask: [255.255.255.0]

Configuring Interface 1 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 2 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 3 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 4 (WAN PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 5 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.157.59
Address Mask: [255.255.255.0]
```

Figure 642. Quick configuration (QCONFIG) of the 2210

```
Configuring Interface 6 (ISDN Primary T1/J1)
IP cannot be configured directly on this interface

Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes] no

Only Static Routing Enabled

Routing Configuration Complete

Configuring SNMP Information

SNMP will be configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No): [Yes] no

SNMP Configuration Complete

This is the information you have entered:

     Interface #     IP Address         Address Mask
          0          192.168.189.59     255.255.255.0
          5          192.168.157.59     255.255.255.0

Only STATIC Routing present.

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool to
download a configuration, you will need to use the SNMP configuration
environment to define a community name with read_write_trap access.


Save this configuration? (Yes, No): [Yes]

IP configuration saved
```

Figure 643. Quick configuration (QCONFIG) of the 2210

```
Configure IPX? (Yes, No): [Yes] no

Configure DNA? (Yes, No): [Yes] no

**********************************************************
Booting Configuration
**********************************************************

Type 'Yes' to Configure Booting
Type 'No' to skip Booting Configuration
Type 'Quit' to exit Quick Config

Configure Booting? (Yes, No, Quit): [Yes] no

**********************************************************
Service Port Configuration
**********************************************************

Type 'Yes' to Configure Service Ports
Type 'No' to skip Service Ports Configuration
Type 'Quit' to exit Quick Config

Configure service port? (Yes, No, Quit): [Yes] no

Quick Config Done
Restart the router for this configuration to take effect.

Restart the router? (Yes, No): [Yes]

RESTARTING THE ROUTER........
```

Figure 644. Quick configuration (QCONFIG) of the 2210

This completes the quick config of the 2210 in the branch office.

32.2 Quick config of the 2216 in the data center

On a 2210, in the case of the LAN and WAN ports, the hardware interfaces are a fixed configuration and no additional steps are required to add interfaces.

Note: You do have to add interfaces in the case of dial circuits.

On the 2216, you need to first add the devices to the configuration before they can be configured.

32.2.1 Adding the interfaces

Before we run the quick config process on the 2216, we must first configure the interfaces. In Figure 645 on page 578, we show you how we added the devices for our scenarios. These include two token-ring interfaces, two Ethernet interfaces, a V35/V36 PPP interface and a V35/V36 frame relay interface. These are added using the `add device` command from the talk 6 prompt.

The order of adding the interfaces is arbitrary. However, the network numbers for your interfaces will be different depending upon the order that you added them to the configuration.

Note: Your 2216 will probably have a different hardware configuration with different adapters in different slots. Look carefully at which devices are in which slots of your 2216.

```
*t 6
Config>set hostname Li
Host name updated successfully
Li Config>add dev token-ring
Device Slot #(1-8) [1]?
Device Port #(1-2) [1]?
Adding Token Ring device in slot 1  port 1 as interface #0
Use "net 0" to configure Token Ring parameters
Li Config>add dev token-ring
Device Slot #(1-8) [1]?
Device Port #(1-2) [2]?
Adding Token Ring device in slot 1  port 2 as interface #1
Use "net 1" to configure Token Ring parameters
Li Config>add dev ethernet
Device Slot #(1-8) [1]? 5
Device Port #(1-2) [1]?
Adding Ethernet device in slot 5  port 1 as interface #2
Use "net 2" to configure Ethernet parameters
Li Config>add dev ethernet
Device Slot #(1-8) [1]? 5
Device Port #(1-2) [2]?
Adding Ethernet device in slot 5  port 2 as interface #3
Use "net 3" to configure Ethernet parameters
Li Config>add dev V35/V36
Device Slot #(1-8) [1]? 6
Device Port #(0-5) [0]?
Defaulting Data-link protocol to PPP
Adding V.35/V.36 PPP device in slot 6  port 0 as interface #4
Use "set data-link" command to change the data-link protocol
Use "net 4" to configure V.35/V.36 PPP parameters
Li Config>add dev V35/V36
Device Slot #(1-8) [1]? 6
Device Port #(0-5) [0]? 1
Defaulting Data-link protocol to PPP
Adding V.35/V.36 PPP device in slot 6  port 1 as interface #5
Use "set data-link" command to change the data-link protocol
Use "net 5" to configure V.35/V.36 PPP parameters
Li Config>set data-link frame-relay
Interface Number [0]? 5
Li Config>list dev
Ifc 0     Token Ring                        Slot: 1   Port: 1
Ifc 1     Token Ring                        Slot: 1   Port: 2
Ifc 2     Ethernet                          Slot: 5   Port: 1
Ifc 3     Ethernet                          Slot: 5   Port: 2
Ifc 4     V.35/V.36 PPP                     Slot: 6   Port: 0
Ifc 5     V.35/V.36 Frame Relay             Slot: 6   Port: 1
Li Config>
```

Figure 645. Adding devices to the 2216

For more information on adding devices to a 2216 configuration, please see *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume I*, SG24-4957.

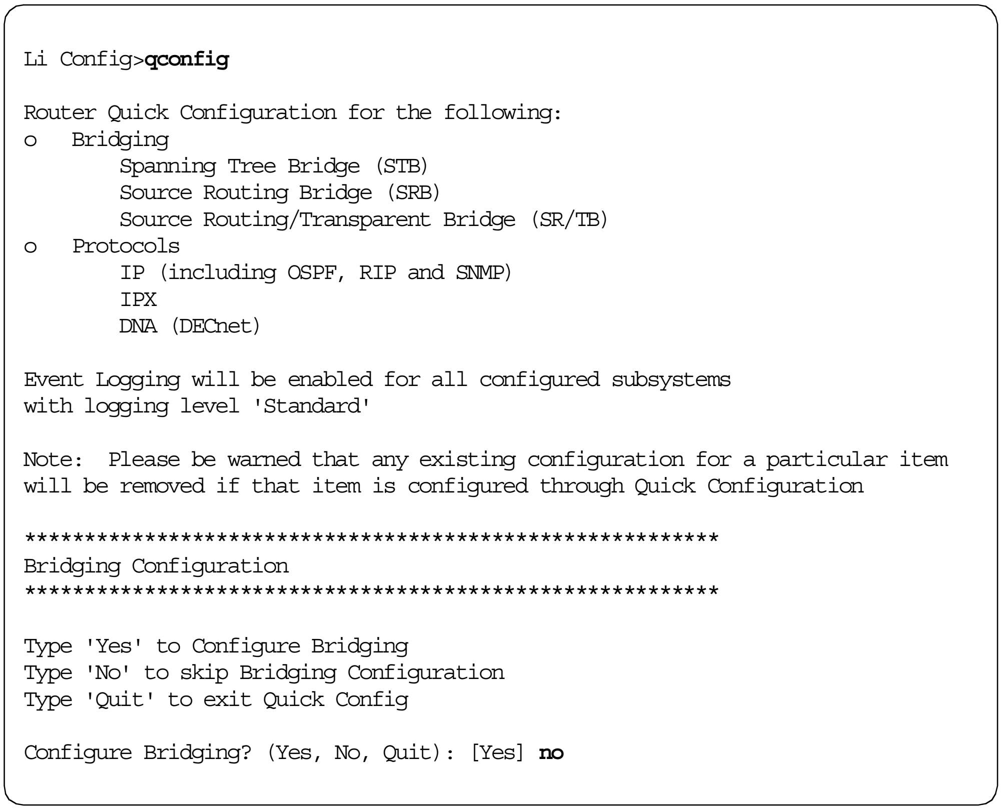
After we add the hardware interfaces, we need to configure the parameters for these interfaces. We use the `net <ifc#>` command to configure these parameters. For our scenarios, we set the ring speed of the token-ring interfaces to 16 Mbps and the media type to shielded twisted pair. For the Ethernet interfaces, we set the connector type to RJ45 (10Base-T).

```
Li Config>net 0
Token-Ring interface configuration
Li TKR config>speed 16
Li TKR config>media shielded
Li TKR config>exit
Li Config>net 1
Token-Ring interface configuration
Li TKR config>speed 16
Li TKR config>media shielded
Li TKR config>exit
Li Config>net 2
Ethernet interface configuration
Li ETH config>connector-type rj45
Li ETH config>exit
Li Config>net 3
Ethernet interface configuration
Li ETH config>connector-type rj45
Li ETH config>exit
Li Config>
```

Figure 646. Setting interface parameters on the 2216

32.2.2 Running quick configuration

Now, we are ready to do the IP protocol configuration of the 2216. In this example, we use the `qconfig` command although we could also use direct configuration commands from the IP configuration submenu of talk 6.

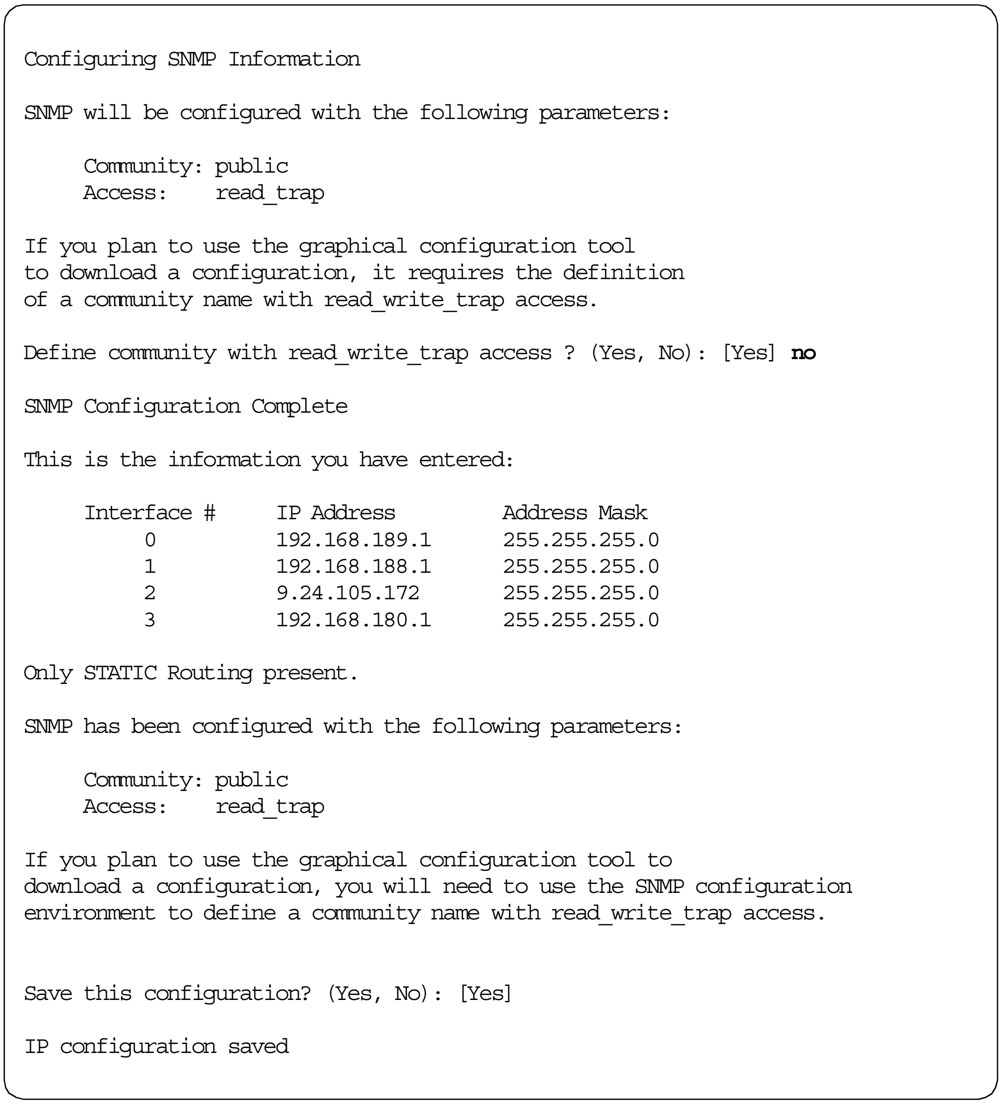


```
Li Config>qconfig

Router Quick Configuration for the following:
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
o   Protocols
        IP (including OSPF, RIP and SNMP)
        IPX
        DNA (DECnet)

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note:  Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration

**********************************************************
Bridging Configuration
**********************************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes] no
```

Figure 647. Quick configuration (QCONFIG) of the 2216

```
**********************************************************
Protocol Configuration
**********************************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
Type 'r' any time at this level to restart Protocol Configuration

Configure IP? (Yes, No): [Yes]
Type 'r' any time at this level to restart IP Configuration

Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.189.1
Address Mask: [255.255.255.0]

Configuring Interface 1 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.188.1
Address Mask: [255.255.255.0]

Configuring Interface 2 (Ethernet)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 9.24.105.172
Address Mask: [255.0.0.0] 255.255.255.0

Configuring Interface 3 (Ethernet)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [] 192.168.180.1
Address Mask: [255.255.255.0]

Configuring Interface 4 (V.35/V.36 PPP)
Configure IP on this interface? (Yes, No): [Yes] no

Configuring Interface 5 (V.35/V.36 Frame Relay)
Configure IP on this interface? (Yes, No): [Yes] no

Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing? (Yes, No): [Yes] no

Only Static Routing Enabled

Routing Configuration Complete
```

Figure 648. Quick configuration (QCONFIG) of the 2216



```
Configuring SNMP Information

SNMP will be configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No): [Yes] no

SNMP Configuration Complete

This is the information you have entered:

     Interface #     IP Address         Address Mask
          0         192.168.189.1      255.255.255.0
          1         192.168.188.1      255.255.255.0
          2         9.24.105.172       255.255.255.0
          3         192.168.180.1      255.255.255.0

Only STATIC Routing present.

SNMP has been configured with the following parameters:

     Community: public
     Access:    read_trap

If you plan to use the graphical configuration tool to
download a configuration, you will need to use the SNMP configuration
environment to define a community name with read_write_trap access.


Save this configuration? (Yes, No): [Yes]

IP configuration saved
```

Figure 649. Quick configuration (QCONFIG) of the 2216

```
Configure IPX? (Yes, No): [Yes] no

Configure DNA? (Yes, No): [Yes] no

Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
Config Save: Using bank A and config number 1

Configuration was written.
The system must be restarted for this configuration to take effect.
Li Config> <CTRL>+<P>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or ,No„ or Abort): yes
Config Save: Using bank A and config number 1
The configuration has been saved.
```

Figure 650. Quick configuration (QCONFIG) of the 2216

This completes the quick config of the 2216 in the data center.

Chapter 33. Configuring IPSec with MRS/MAS V3.1/3.2

In this chapter we provide the screens that we used in configuring the IPSec tunnels and the packet filters for the IBM 2216 Nways Multiaccess Connector in the data center for the scenario described in Chapter 24, “Connecting the data center to the branch office” on page 463.

We start by creating the packet filters as shown in Figure 651.

```
Li *t 6
Gateway user configuration
Li Config>protocol ip
Internet protocol user configuration
Li IP config>add packet-filter
Packet-filter name []? pf_out_0
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]?
Li IP config>add packet-filter
Packet-filter name []? pf_in_0
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]?
Li IP config>
```

Figure 651. Creating packet filters on the public interface (0)

Then we update the outbound packet filter. We first add an access control for communication between the two intranet LANs at the corporate site and the intranet LAN at the branch office using tunnel 1. See Figure 652 on page 585 for these commands.

```
Li IP config>update packet-filter pf_out_0
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.180.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 9.24.105.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.157.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>
```

Figure 652. Configuring the outbound packet filter

Next we add an access control for the IPSec packets that are sent by router Li to router Karen. See Figure 653 on page 586 for the command.

```
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>
```

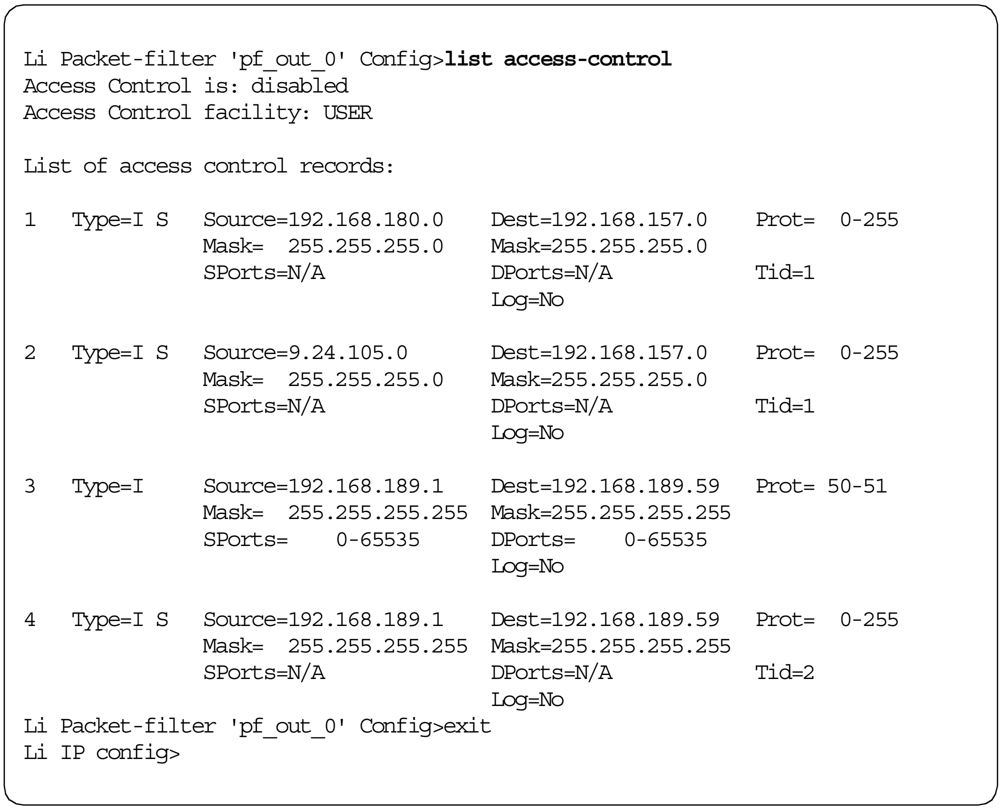
Figure 653. Configuring the outbound packet filter

Finally, we add the access control for all non-IPSec traffic between the two routers. This traffic is sent through tunnel 2. See Figure 654 for the command.

```
Li Packet-filter 'pf_out_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.1
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.59
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_out_0' Config>
```

Figure 654. Configuring the outbound packet filter

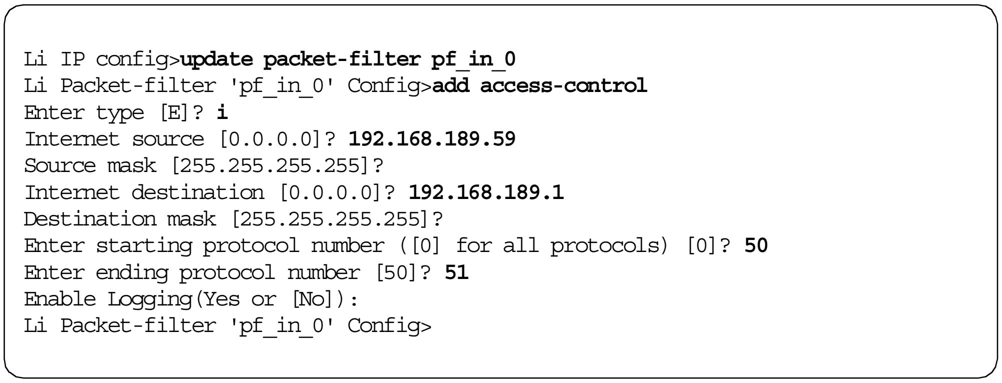
Next we list the access controls in the outbound packet filter.



```
Li Packet-filter 'pf_out_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I S   Source=192.168.180.0    Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

2   Type=I S   Source=9.24.105.0       Dest=192.168.157.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I     Source=192.168.189.1    Dest=192.168.189.59   Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

4   Type=I S   Source=192.168.189.1    Dest=192.168.189.59   Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li Packet-filter 'pf_out_0' Config>exit
Li IP config>
```

Figure 655. Listing access controls

Then we add access controls to the inbound packet filter. We start with the access control for IPSec packets coming in from router Karen.



```
Li IP config>update packet-filter pf_in_0
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>
```

Figure 656. Configuring the inbound packet filter

Then we add the access control for communication between the intranet LANs using tunnel 1.

```
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 192.168.180.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.157.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]? 9.24.105.0
Destination mask [255.255.255.255]? 255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>
```

Figure 657. Configuring the inbound packet filter

Finally, we add the access control for router-to-router traffic using tunnel 2.

```
Li Packet-filter 'pf_in_0' Config>add access-control
Enter type [E]? s
Internet source [0.0.0.0]? 192.168.189.59
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 192.168.189.1
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]? 2
Enable Logging(Yes or [No]):
Li Packet-filter 'pf_in_0' Config>
```

Figure 658. Configuring the inbound packet filter

Here is the list of access controls in the inbound packet filter.

```
Li Packet-filter 'pf_in_0' Config>list access-control
Access Control is: disabled
Access Control facility: USER

List of access control records:

1   Type=I     Source=192.168.189.59   Dest=192.168.189.1    Prot= 50-51
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=    0-65535      DPorts=    0-65535
                                       Log=No

2   Type=I S   Source=192.168.157.0    Dest=192.168.180.0    Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

3   Type=I S   Source=192.168.157.0    Dest=9.24.105.0       Prot=  0-255
               Mask=  255.255.255.0    Mask=255.255.255.0
               SPorts=N/A              DPorts=N/A            Tid=1
                                       Log=No

4   Type=I S   Source=192.168.189.59   Dest=192.168.189.1    Prot=  0-255
               Mask=  255.255.255.255  Mask=255.255.255.255
               SPorts=N/A              DPorts=N/A            Tid=2
                                       Log=No
Li Packet-filter 'pf_in_0' Config>exit
Li IP config>
```

Figure 659. Listing the access controls

Next we enable the packet filters and set access control on. The listing of the packet filters shows that access control is on and that the state of the packet filters is on.

```
Li IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_in_0
Li IP config>enable packet-filter
Enter packet-filter name to be enabled []? pf_out_0
Li IP config>set access-control on
Li IP config>list packet-filter

List of packet-filter records:

Name               Direction   Interface   State  Src-Addr-Ver
pf_in_0            In          0           On     Off
pf_out_0           Out         0           On     N/A
Access Control is: enabled
Li IP config>exit
```

Figure 660. Enabling access control

Next we go into the IPSec feature configuration to add tunnel 1.

```
Li Config>feature ipsec
IP Security feature user configuration
Li IPsec config>add tunnel
Tunnel ID (1-65535) [1]?
Tunnel Name (optional) []? ESP&AH1
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 661. Defining the tunnel-mode IPSec tunnel

Next, we are prompted to define the local end of the SA. Figure 662 shows the required parameters.

```
Local IP Address [192.168.189.1]?
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 662. defining the tunnel-mode IPSec tunnel

Note that the keys are not displayed while typed.

Next, we are prompted to define the remote end of the SA. Figure 663 shows the required parameters.

```
Remote IP Address [0.0.0.0]? 192.168.189.59
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]?
Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Li IPsec config>
```

Figure 663. Defining the tunnel-mode IPSec tunnel

The next tunnel we create is the transport-mode tunnel with id=2 and we have chosen to use AH-ESP again as the tunnel policy, the value of 257 for all SPIs, AH protocol using HMAC-MD5 and 3DES encryption algorithm.

Figure 664 shows the configuration of the transport-mode tunnel.

```
Li IPsec config>add tunnel
Tunnel ID (1-65535) [1]? 2
Tunnel Name (optional) []? TRANS-ESP&AH
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]? TRANS
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]?
```

Figure 664. Defining the transport-mode IPSec tunnel

Next, we are prompted to define the local end of the SA. Figure 665 shows the required parameters.

```
Local IP Address [192.168.189.1]?
Local Authentication SPI (256-65535) [256]? 257
Local Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Local Encryption SPI (256-65535) [257]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES) [DES-CBC]? 3DES
First Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Local Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Local Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [No]:
```

Figure 665. Defining the transport-mode IPSec tunnel

Next, we are prompted to define the remote end of the SA. Figure 666 shows the required parameters.

```
Remote IP Address [0.0.0.0]? 192.168.189.59
Remote Authentication SPI (1-65535) [257]?
Remote Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote Encryption SPI (1-65535) [257]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES) [3DES]?
First Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter First Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Second Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Second Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Third Remote Encryption Key (16 characters) in Hex (0-9,a-f,A-F):
Enter Third Remote Encryption Key again (16 characters) in Hex (0-9,a-f,A-F):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Li IPsec config>
```

Figure 666. Defining the transport-mode IPSec tunnel

Next, we list the tunnels that we have created. Figure 667 shows the command and output:

```
Li IPsec config>list tunnel all

   ID        Name        Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      2  TRANS-ESP&AH     192.168.189.1    192.168.189.59   TRANS  Enabled
      1  ESP&AH1          192.168.189.1    192.168.189.59   TUNN   Enabled
Li IPsec config>
```

Figure 667. Listing defined tunnels

The last step is to enable IPSec on the router. Figure 668 shows this command.

```
Li IPsec config>enable ipsec
Restarting the router is required for IPSec to be active.
Li IPsec config>exit
Li Config>
```

Figure 668. Enabling IPSec

Next, we have to reload the 2216 so that the newly created IPSec tunnel will be activated.

```
Li Config> <CTRL>+<P>
Li *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort): yes
Config Save: Using bank A and config number 2
The configuration has been saved.
```

Figure 669. Reloading the router

This completes the configuration of the IPSec tunnels and the packet filters for the data center router.

Appendix A. Special notices

This publication is intended to help networking professionals quickly understand the functions of Nways Multiprotocol Access Services, Nways Multiprotocol Routing Services and Nways AIS. The information in this publication is not intended as the specification of any programming interfaces that are provided by Nways Multiprotocol Access Services or Nways Multiprotocol Routing Services. See the PUBLICATIONS section of the IBM Programming Announcement for Nways Multiprotocol Access Services and Nways Multiprotocol Routing Services for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

This document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

Advanced Peer-to-Peer Networking
Application System/400
AS/400
CUA
eNetwork
FAA
IBM
MVS/ESA
NetView
Operating System/2
OS/390
RACF
S/370
SP
VTAM
AIX
APPN
CICS
DB2
ESCON
IBM Global Network
IMS
Netfinity
Nways
OS/2
OS/400
RISC System/600
SecureWay
System/390

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

SET and the SET logo are trademarks owned by SET Secure Electronic Transaction LLC.

Appendix B. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 International Technical Support Organization publications

For information on ordering these ITSO publications see “How to get IBM Redbooks” on page 603.

VPN

- *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201
- *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management,* SG24-5309
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks*, SG24-5404
- *SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements*, SG24-5631

Nways routers

- *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume I*, SG24-4957
- *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios - Volume I*, SG24-4446
- *IBM 2210 Nways Multiprotocol Router IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios - Volume II*, SG24-4956
- *IBM 2216 Multiaccess Connector ESCON Solutions*, SG24-2137

IP and SNA

- *Inside APPN - The Essential Guide to the Next-Generation SNA*, SG24-3669
- *TCP/IP Tutorial and Technical Overview*, GG24-3376
- *IP Network Design Guide*, SG24-2580

LDAP

- *Understanding LDAP*, SG24-4986
- *LDAP Implementation Cookbook,* SG24-5110

B.2 Redbooks on CD-ROMs

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at `http://www.redbooks.ibm.com/` for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	**Collection Kit Number**
System/390 Redbooks Collection	SK2T-2177
Networking and Systems Management Redbooks Collection	SK2T-6022

CD-ROM Title	Collection Kit Number
Transaction Processing and Data Management Redbooks Collection	SK2T-8038
Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
AS/400 Redbooks Collection	SK2T-2849
Netfinity Hardware and Software Redbooks Collection	SK2T-8046
RS/6000 Redbooks Collection (BkMgr Format)	SK2T-8040
RS/6000 Redbooks Collection (PDF Format)	SK2T-8043
Application Development Redbooks Collection	SK2T-8037
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

B.3 Other publications

These publications are also relevant as further information sources:

B.3.1 IBM documentation

2210 and MRS

Available through the IBM networking page:
`http://www.networking.ibm.com/support/docs.nsf/2210docs?OpenView`

- *Nways Multiprotocol Routing Services V3.3 Software User's Guide*, SC30-3681
- *Nways Multiprotocol Routing Services V3.3 Protocol Configuration and Monitoring Reference, Volume 1*, SC30-3680
- *Nways Multiprotocol Routing Services V3.3 Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3865
- *Nways Multiprotocol Routing Services V3.3 Using and Configuring Features*, SC30-3992

2212 and AIS

Available through the IBM networking page:
`http://www.networking.ibm.com/support/docs.nsf/2212docs?OpenView`

- *2212 Installation and Initial Configuration Guide*, GA27-4216
- *2212 Introduction and Planning Guide*, GA27-4215
- *2212 Hardware Quick Reference Card*, GX27-4048
- *2212 Service and Maintenance Manual*, GY27-0362
- *Nways Access Integration Services V3.3 Protocol Configuration and Monitoring Reference Volume 1*, SC30-3990
- *Nways Access Integration Services V3.3 Protocol Configuration and Monitoring Reference Volume 2*, SC30-3991
- *Nways Access Integration Services V3.3 Software User's Guide*, SC30-3988
- *Nways Access Integration Services V3.3 Using and Configuring Features*, SC30-3989
- *Release Notes: Configuring the 4-Port Analog 56K Modem CPCI Adapter*
- *Release Notes: Hardware*

Network Utility, 2216 and MAS

Available via the IBM networking page:
`http://www.networking.ibm.com/support/docs.nsf/2216docs?OpenView`

- *Nways Multiprotocol Access Services V3.3 Software User's Guide*, SC30-3886
- *Nways Multiprotocol Access Services V3.3 Protocol Configuration and Monitoring Reference, Volume 1*, SC30-3884
- *Nways Multiprotocol Access Services Protocol Configuration and Monitoring Reference, Volume 2*, SC30-3885
- *Nways Multiprotocol Access Services V3.3 Using and Configuring Features*, SC30-3993
- *2216/Network Utility Channel-Attach Examples*, G224-4599
- *Network Utility Installation, Getting Started, and User's Guide*, GA27-4167

2210 / 2212 / 2216 - MRS / AIS / MAS

- *Nways Event Logging System Messages Guide*, SC30-3682-01
- *Configuration Program User's Guide for Nways Multiprotocol Access Services and Multiprotocol Routing Services*, GC30-3830

SNA / VTAM

- *SNA APPN Architecture Reference*, SC30-3422
- *VTAM Network Implementation Guide V4R4 for MVS/ESA*, SC31-8370
- *VTAM Resource Definition Reference V4R4 for MVS/ESA*, SC31-8377
- *OS/390 SecureWay Communications Server: SNA Resource Definition Reference*, SC31-8565

B.3.2 Internet standards and drafts

IPSec

- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: IP Authentication Header
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2411: IP Security Document Roadmap
- RFC 2412: The OAKLEY Key Determination Protocol
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- draft-ietf-ipsec-pki-req-03.txt: PKI Requirements for IP Security

L2TP

- RFC 2661: Layer Two Tunneling Protocol "L2TP"
- draft-ietf-pppext-l2tp-security-04.txt: Securing L2TP using IPSEC

PPTP

- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)

L2F

- RFC 2341: Cisco Layer Two Forwarding (Protocol) "L2F"

LDAP

- RFC 1777: Lightweight Directory Access Protocol
- RFC 2251: Lightweight Directory Access Protocol (v3)
- RFC 2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- draft-rajan-policy-qosschema : Schema for Differentiated Services and Integrated Services in Networks
- draft-good-ldap-ldif: The LDAP Data Interchange Format (LDIF) - Technical Specification

RADIUS

- RFC 2138: Remote Authentication Dial In User Service (RADIUS)
- RFC 2139: RADIUS Accounting

Public key infrastructure

- RFC 2437: PKCS #1: RSA Cryptography Specifications Version 2.0
- RFC 2315: PKCS #7: Cryptographic Message Syntax Version 1.5
- RFC 2314: PKCS #10: Certification Request Syntax Version 1.5
- RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 2510: Internet X.509 Public Key Infrastructure Certificate Management Protocols
- RFC 2511: Internet X.509 Certificate Request Message Format
- RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 2528: Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
- RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
- RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- RFC 2585: Internet X.509 Public Key Infrastructure Operational Protocols - FTP and HTTP
- RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema

B.3.3 Further reading

Security and VPN

- *Applied Cryptography*, Second Edition, John Wiley & Sons, Inc., 1996, by Bruce Schneier; ISBN 0-471-11709-9
- *Network Security: Private Communication in a Public World*, PTR Prentice Hall, 1995, by Charlie Kaufman, Radia Perlman, and Mike Speciner; ISBN 0-13-061466-1
- *Designing Network Security*, Cisco Press, 1999, by Merike Kaeo; ISBN 1-57870-043-4
- *Enhanced IP Services for Cisco Networks*, Cisco Press, 1999, by Donald C. Lee; ISBN 1-57870-106-6
- *IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks*, PTR Prentice Hall, 1999, by Naganand Doraswamy and Dan Harkins; ISBN 0-13-011898-2
- *L2TP: Implementation and Operation,* Addison-Wesley, 1999, by Richard Shea; ISBN 0-201-60448-5
- *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*, Second Edition, Sam's Publishing, 1998, by anonymous; ISBN 0-67231-341-3
- *Intrusion Detection: Network Security Beyond the Firewall*, John Wiley & Sons, Inc., 1998, by Terry Escamilla; ISBN: 0-47129-000-9

B.3.4 Web site references

Internet standards and drafts

- `http://www.ietf.org`

Public key infrastructure

- `http://www.rsa.com`

IBM VPN solutions

- `http://www.networking.ibm.com/vpn/vpnprod.html`

IBM Security

- `http://www.ibm.com/security`

IBM 2212 VPN performance

- `http://www.networking.ibm.com/2212/2212perf.html`

Cisco Systems, Inc.

- `http://www.cisco.com`

Microsoft Windows 2000

- `http://www.microsoft.com/windows/professional/`
- `http://www.microsoft.com/windows/server/`

IRE SafeNet VPN client

- `http://www.ire.com/Products/VPN/soft_pk.htm`

Network TeleSystems TunnelBuilder VPN client

- `http://www.nts.com/products/prod_client.html`

Wind River Networks WinVPN Client

- http://www.ivasion.com/winvpn_client/vpnclient_overview.htm

RADIUS

- http://www.livingston.com

Other referenced Web sites

- http://www.ivasion.com
- http://www.ire.com
- http://www.networking.ibm.com/support/docs.nsf/2212docs?OpenView
- http://www.networking.ibm.com/support/docs.nsf/2210docs?OpenView
- http://www.networking.ibm.com/support/docs.nsf/2216docs?OpenView
- http://www.networking.ibm.com/vpn/vpnprod.html
- http://w3.itso.ibm.com
- http://w3.ibm.com
- http://www.elink.ibmlink.ibm.com/pbl/pbl

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web site** `http://www.redbooks.ibm.com/`

  Search for, view, download, or order hardcopy/CD-ROM redbooks from the redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this redbooks site.

  Redpieces are redbooks in progress; not all redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail orders**

  Send orders by e-mail including information from the redbooks fax order form to:

	e-mail address
In United States	usib6fpl@ibmmail.com
Outside North America	Contact information is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

- **Fax orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: `http://www.elink.ibmlink.ibm.com/pbl/pbl/`

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the redbooks Web site.

IBM intranet for employees

IBM employees may register for information on workshops, residencies, and redbooks by accessing the IBM Intranet Web site at `http://w3.itso.ibm.com/` and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access `MyNews` at `http://w3.ibm.com/` for redbook, residency, and workshop announcements.

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

□ Invoice to customer number

□ Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

List of abbreviations

AAA	Authentication, Authorization and Accounting
AAL	ATM Adaptation Layer
AFS	Andrews File System
AH	Authentication Header
AIX	Advanced Interactive Executive Operating System
API	Application Programming Interface
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
AS/400	Application System/400
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
BNF	Backus-Naur Form
BRI	Basic Rate Interface
BSD	Berkeley Software Distribution
CA	Certification Authority
CBC	Cipher Block Chaining
CCITT	Comité Consultatif International Télégraphique et Téléphonique (now ITU-T)
CDMF	Commercial Data Masking Facility
CERN	Conseil Européen pour la Recherche Nucléaire
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CICS	Customer Information Control System
CIDR	Classless Inter-Domain Routing
CIX	Commercial Internet Exchange
CLNP	Connectionless Network Protocol
CORBA	Common Object Request Broker Architecture
COS	Class of Service
CPCS	Common Part Convergence Sublayer
CPU	central processing unit
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DARPA	Defense Advanced Research Projects Agency
DCE	Distributed Computing Environment
DCE	Data Circuit-terminating Equipment
DDN	Defense Data Network
DDNS	Dynamic Domain Name System
DEN	Directory-Enabled Networking
DES	Digital Encryption Standard
DFS	Distributed File Service
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLCI	Data Link Connection Identifier
DLL	Dynamic Link Library
DLSw	Data Link Switching

DLUR	dependent LU requester
DLUS	dependent LU server
DME	Distributed Management Environment
DMI	Desktop Management Interface
DMTF	Desktop Management Task Force
DMZ	demilitarized zone
DNS	Domain Name System
DOD	U.S. Department of Defense
DOI	Domain of Interpretation
DOS	Disk Operating System
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DTP	Data Transfer Process
DVMRP	Distance Vector Multicast Routing Protocol
EBCDIC	Extended Binary Communication Data Interchange Code
EGP	Exterior Gateway Protocol
ESCON	Enterprise Systems Connection
ESP	Encapsulating Security Payload
FDDI	Fiber Distributed Data Interface
FQDN	Fully Qualified Domain Name
FR	frame relay
FTP	File Transfer Protocol
GGP	Gateway-to-Gateway Protocol
GMT	Greenwich Mean Time
GSM	Group Special Mobile
GUI	Graphical User Interface
HDLC	High-level Data Link Control
HMAC	Hashed Message Authentication Code
HPR	High Performance Routing
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAB	Internet Activities Board
IAC	Interpret As Command
IANA	Internet Assigned Numbers Authority
IBM	International Business Machines Corporation
ICMP	Internet Control Message Protocol
ICSS	Internet Connection Secure Server
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IDLC	Integrated Data Link Control
IDRP	Inter-Domain Routing Protocol
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGN	IBM Global Network
IGP	Interior Gateway Protocol
IIOP	Internet Inter-ORB Protocol
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IMS	Information Management System

IP	Internet Protocol
IPC	Interprocess Communication
IPSec	IP Security Architecture
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange
IRFT	Internet Research Task Force
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet service provider
ITSO	International Technical Support Organization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector (was CCITT)
IV	Initialization Vector
JDBC	Java Database Connectivity
JDK	Java Development Toolkit
JES	Job Entry System
JIT	Java Just-in-Time Compiler
JMAPI	Java Management API
JVM	Java Virtual Machine
JPEG	Joint Photographic Experts Group
LAC	L2TP Access Concentrator
LAN	local area network
LAPB	Link Access Protocol Balanced
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LE	LAN Emulation (ATM)
LLC	Logical Link Layer
LNS	L2TP Network Server
LPD	Line Printer Daemon
LPR	Line Printer Requester
LSAP	Link Service Access Point
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
MAC	Message Authentication Code
MAC	Medium Access Control
MD2	RSA Message Digest 2 Algorithm
MD5	RSA Message Digest 5 Algorithm
MIB	Management Information Base
MILNET	Military Network
MIME	Multipurpose Internet Mail Extensions
MLD	Multicast Listener Discovery
MOSPF	Multicast Open Shortest Path First
MPC	Multi-Path Channel
MPEG	Moving Pictures Experts Group
MPLS	Multiprotocol Label Switching
MPOA	Multiprotocol over ATM
MPTN	Multiprotocol Transport Network
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTA	Message Transfer Agent
MTU	Maximum Transmission Unit
MVS	Multiple Virtual Storage Operating System
NAS	network access server

NAT	network address translation
NBDD	NetBIOS Datagram Distributor
NBNS	NetBIOS Name Server
NCF	Network Computing Framework
NCP	Network Control Protocol
NCSA	National Computer Security Association
NDIS	Network Drivers Interface Specification
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	Network Information Center
NIS	Network Information Systems
NIST	National Institute of Standards and Technology
NMS	Network Management Station
NNTP	Network News Transfer Protocol
NRZ	Non-Return-to-Zero
NRZI	Non-Return-to-Zero Inverted
NSA	National Security Agency
NSAP	Network Service Access Point
NSF	National Science Foundation
NTP	Network Time Protocol
NVT	Network Virtual Terminal
ODBC	Open Database Connectivity
ODI	Open Datalink Interface
OEM	Original Equipment Manufacturer
ONC	Open Network Computing
ORB	Object Request Broker
OSA	Open Systems Adapter
OSI	Open Systems Interconnect
OSF	Open Software Foundation
OSPF	Open Shortest Path First
OS/2	Operating System/2
OS/390	Operating System for the System/390 platform
OS/400	Operating System for the AS/400 platform
PAD	Packet Assembler/Disassembler
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PI	Protocol Interpreter
PIM	Protocol Independent Multicast
PKCS	Public Key Cryptosystem
PKI	public key infrastructure
PNNI	Private Network-to-Network Interface
POP	Post Office Protocol
POP	Point-of-Presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSDN	Packet Switching Data Network
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QLLC	Qualified Logical Link Control
QOS	Quality of Service
RACF	Resource Access Control Facility
RADIUS	Remote Authentication Dial-In User Service
RAM	random access memory

RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RC2	RSA Rivest Cipher 2 Algorithm
RC4	RSA Rivest Cipher 4 Algorithm
REXEC	Remote Execution Command Protocol
RFC	Request for Comments
RIP	Routing Information Protocol
RIPE	Réseaux IP Européens
RISC	Reduced Instruction-Set Computer
ROM	Read-only Memory
RPC	Remote Procedure Call
RSH	Remote Shell
RSVP	Resource Reservation Protocol
RS/6000	IBM RISC System/6000
RTCP	Realtime Control Protocol
RTP	Realtime Protocol
SA	security association
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SET	Secure Electronic Transaction
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transfer Protocol
SLA	service level agreement
SLIP	Serial Line Internet Protocol
SMI	Structure of Management Information
S-MIME	Secure Multipurpose Internet Mail Extension
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNAP	Subnetwork Access Protocol
SNG	Secured Network Gateway (former product name of the IBM eNetwork Firewall)
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SONET	Synchronous Optical Network
SOCKS	SOCK-et-S (An internal NEC development name that remained after release)
SPI	Security Parameter Index
SSL	Secure Sockets Layer
SSAP	Source Service Access Point
SSP	Switch-to-Switch Protocol
SSRC	Synchronization Source
SVC	Switched Virtual Circuit
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TLPB	Transport-Layer Protocol Boundary
TLS	Transport Layer Security
TOS	Type of Service
TRD	Transit Routing Domain
TTL	time to live
UDP	User Datagram Protocol
UID	Unique Identifier

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UT	Universal Time
VC	Virtual Circuit
VM	Virtual Machine Operating System
VPN	virtual private network
VRML	Virtual Reality Modeling Language
VRRP	Virtual Router Redundancy Protocol
VTAM	Virtual Telecommunications Access Method
WAN	wide area network
WWW	World Wide Web
XDR	External Data Representation
XML	Extensible Markup Language
X11	X Window System Version 11
X.25	CCITT Packet Switching Standard
X.400	CCITT and ISO Message-handling Service Standard
X.500	ITU and ISO Directory Service Standard
X.509	ITU and ISO Digital Certificate Standard
3DES	Triple Digital Encryption Standard

Index

ITSO Redbook evaluation

A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions
SG24-5234-01

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at `http://www.redbooks.ibm.com/`
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to `redbook@us.ibm.com`

Which of the following best describes you?
_ Customer   _ Business Partner   _ Solution Developer   _ IBM employee
_ None of the above

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction __________

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

____

____

____

____

What other redbooks would you like to see published?

____

____

____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

____

____

____

____

____

SG24-5234-01

Printed in the U.S.A.

A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions

SG24-5234-01