IBM

IBM @server iSeries Universal Connection

for Electronic Support and Services

Explains the supported functions with Universal Connection

Shows how to install, tailor, and configure Universal Connection

Helps you determine communications problems

Masahiko Hamada
Michael S Alexander
Makoto Kikuchi

Redbooks

ibm.com/redbooks

International Technical Support Organization

SG24-6224-00

iSeries Universal Connection for Electronic Support and Services

August 2001

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 209.

First Edition (August 2001)

This edition applies to Version 5 Release 1 of OS/400.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

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

Introducing IBM @server iSeries Universal Connection! Now you have more options in OS/400 V5R1 and V4R5 for Electronic Customer Support (ECS) and Electronic Service Agent connectivity. Universal Connection offers dial-up support over TCP/IP via AT&T Global Network Services. It supports an Internet connection using a virtual private network (VPN) for more secure connections over the Internet. You can have a direct Internet connection through an integrated modem (9771) with an Internet Service Provider (ISP) of your choice. Or you can have higher speed direct Internet connections (T1, T2, Ethernet-attached cable, or DSL modems).

This IBM Redbook explains how to use the variety of ESP support tools that report inventories of software and hardware on your machine to IBM so you can get personalized electronic support, based on your system data. This helps streamline your support process so that you can spend more time running your business rather than maintaining your systems. You control the transmission of data to IBM (what is sent and when it is sent). Then IBM helps secure your customer data and use that data to appropriately provide you IBM's world-class, personalized support. This book also shows you how to install, tailor, and configure the new Universal Connection Wizard for your environment.

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 Rochester Center.

Masahiko Hamada is an Advisory International Technical Support Specialist for the iSeries and AS/400e servers at the International Technical Support Organization, Rochester Center. He writes extensively and teaches IBM classes worldwide on all areas of iSeries e-business. Before joining the ITSO in 2000, he worked in the AS/400 Field Support Center in Japan as an AS/400 System Specialist.

Michael S Alexander works in the IBM iSeries Support Center in Rochester, Minnesota. He is currently a member of the Client Access Emulation and Connectivity, Telnet, and Operations Console teams. He was involved in the Universal Connection Wizard initial testing at OS/400 V4R5M0 and is also a contributor to the *iSeries Magazine*. Michael began his career at IBM in 1999 after graduating with a BSCpE in Computer Engineering from the University of Central Florida.

Makoto Kikuchi is an Advisory ITAP System Services Specialist for OS/400 networking with IBM Global Services in Japan. He has been with IBM for 14 years. He has experience in handling various network problems in Enterprise systems, client/server systems, TCP/IP Internet-related problems, and OS/400 networking problems.

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

Carol Egan
Christopher Gloe
IBM Rochester

Hanif Dandia
Alen Gnezda
Franklin Gruber
Warren Grunbok II
Pat Sullivan
IBM Endicott

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 "IBM Redbooks review" on page 221 to the fax number shown on the form.
- Use the online evaluation form found at **ibm.com**/redbooks
- Send your comments in an Internet note to redbook@us.ibm.com

Chapter 1. Extreme Support Personalized (ESP)

Extreme Support Personalized (ESP) is the IBM comprehensive technical service and support initiative exclusively for AS/400 and iSeries servers. ESP offers total solutions support that is personalized for you in the form you need it. ESP includes Internet support, voice and on-site support, and support that is integrated into the product.

This chapter is written mainly for CEOs or business decision makers from a customer perspective. It explains:

- What ESP is
- The applications that are available
- Connectivity options
- Connectivity tools for iSeries

1.1 Introduction to ESP

The iSeries server delivers personalized service and electronic support that is designed to help you keep your business running at peak performance. You can take advantage of customized, automated support; online service tracking; and proactive maintenance for your unique system environment. Such options include a product offering that lets you know when it's time to upgrade and a new voice integration feature that allows for electronically scheduled callbacks.

1.1.1 Customer Care Advantage

IBM has more than 100,000 dedicated technical support people delivering superior Customer Care to customers around the globe, around the clock. IBM has been the leader and innovator in electronic technical support for more than 25 years. That support is made even stronger by using and expanding the Web to make it easier for IBM customers to access the information needed to run their businesses. Customer Care Advantage focuses on support across the new IBM @server product lines (Figure 1).

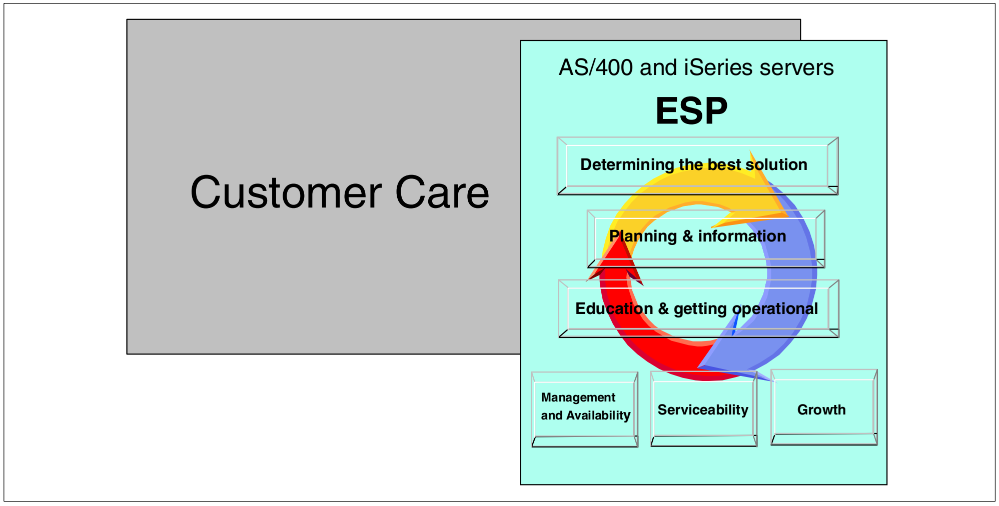

Customer Care
AS/400 and iSeries servers
ESP
Determining the best solution
Planning & information
Education & getting operational
Management and Availability
Serviceability
Growth

Figure 1. Customer Care and ESP

To learn more about Customer Care Advantage, see:

`http://www-1.ibm.com/servers/eserver/introducing/customercare.html`

1.1.1.1 Remote service and support capability

Remote service and support for IBM @server provides a new level of peace of mind and an easier way to maintain your systems. Proactive care capabilities are offered for each IBM @server to help ensure that your server can deliver maximum availability and to make it easier for you to maintain and control your systems. These functions are joined with other personalized, proactive “down the wire” functions to make the support for your IBM @server even stronger. For iSeries servers, IBM provides the following services:

- Service Agent Inventory
- Electronic Customer Support
- Service Agent Reporting
- Internet PTF
- Workload Estimator
- Remote Service
- Physical Device Placement Assistance
- Hardware Updates via Business Partners and IBM
- Performance Management for AS/400e (PM/400e)
- Software Upgrade Assistance (U.S.A., Europe (late second quarter in 2001))

1.1.1.2 Technical support portal

Customers can quickly and easily access technical information needed by means of the IBM @server Technical support portal (`http://techsupport.services.ibm.com/eserver/support`). This portal also makes it possible for customers to order software enhancements to existing operating systems. Given that we live in a heterogeneous world, with most IT infrastructures featuring multiple platforms, the IBM Web site features pointers to technical support for the entire IBM @server brand of servers instead of just individual servers. IBM also gives customers access to a customer experience knowledge base to test their plans against the experiences of others. For iSeries servers, IBM provides the following services:

- Information (Web page)

  Online information access via the Web:

  - Task based articles (information Center)
  - Database Technical Support information
  - Redbook, Technical Studio

- My iSeries (Web page)

  Personalized Web site

1.1.1.3 Learning Services

IBM is making it possible to link to all world-class Learning Services courses (`http://www.ibm.com/services/learning/`) from the IBM Technical Support Web site. This makes it much easier to shop IBM’s rich educational offerings. IBM Learning Services provides world-class education and training to support all IBM servers and associated technologies. Customers can take advantage of training in a variety of flexible delivery formats, including Web-based pages, CD-ROM, and the traditional classroom. For iSeries servers, IBM provides the iSeries University, which offers consolidated education.

1.1.2 ESP approach

ESP focuses on comprehensive support specifically for the AS/400 and iSeries servers. This section highlights the new IBM support offerings. For more information, see the Web site at: `http://www.as400service.ibm.com/`

Electronic support over TCP/IP

Simplify your support process with new and flexible options for electronic support over Transmission Control Protocol/Internet Protocol (TCP/IP). Use the power of the V4R5 integrated high-speed V.90 modem to obtain fixes, report problems, and dial-up for remote support. In V5R1, the connectivity options were expanded to include VPN connections.

This function eliminates the need for the additional external modem that had been required for electronic support. It gives you an option to move to TCP/IP-based electronic support. Feature 9771 ships with every iSeries server as part of the base machine.

PDF quick references for technical support

These handy “spec sheets” in PDF format highlight important aspects of Extreme Support Personalized (ESP) such as *What's New* and *Tools on the Web*.

New technical support Web portal

This new portal gives you easier access to IBM Technical Service and Support for IBM servers on the Web, including the IBM product line, RS/6000, 390, Netfinity, and Numa-q.

Simplified installation of I/O features

Physical Device Placement Assistant (PDPA) makes it easier to add PCI features to existing AS/400 and iSeries servers.

Flexible system monitoring

With Management Central: Pervasive, you can remotely monitor system performance and status using a Web phone, a Personal Digital Assistant (PDA) with a wireless modem, or a Web browser on a PC or Network Station. Network administrators have more flexibility to access Management Central information and monitor the servers they support.

Easy Internet connection

The Internet setup wizard simplifies the process of connecting your server to the Internet.

New services for business-to-business (B2B)

These new services will help you assess your B2B opportunity and define a B2B solution.

Easier upgrade sizing capabilities using tools on the Web

PM/400e has been integrated with the IBM Workload Estimator for iSeries. The Workload Estimator provides sizing recommendations for an iSeries or an AS/400e server that runs one or more workloads associated with e-business or collaboration.

Simplified software upgrade ordering process

A customer installable feature (CIF) with the easy-to-use Physical Device Placement Assistant offers a handy Web-based tool. This saves you time by quickly identifying where you can install the CIF as you add it to the system. This tool works by retrieving information from your system via a secure Internet connection, analyzing it, and then advising you of open and occupied card slots.

PM/400e, Service Agent, and inventory consolidation with Management Central via TCP/IP

Management Central Extreme Support (V5R1) is the result of merging technologies. It involves Management Central's inventory collection support, PM/400e data, and the IBM Electronic Services infrastructure. This merger enables customers to perform the necessary configuration and setup to connect to IBM, send collected data, and receive IBM fixes for multiple systems and groups from the Management Central "central" system. This precludes requiring customers sending data and receiving IBM fixes from each individual system as the process is today.

The IBM @server iSeries family of servers includes an integrated modem to facilitate electronic support as shown in Figure 2.

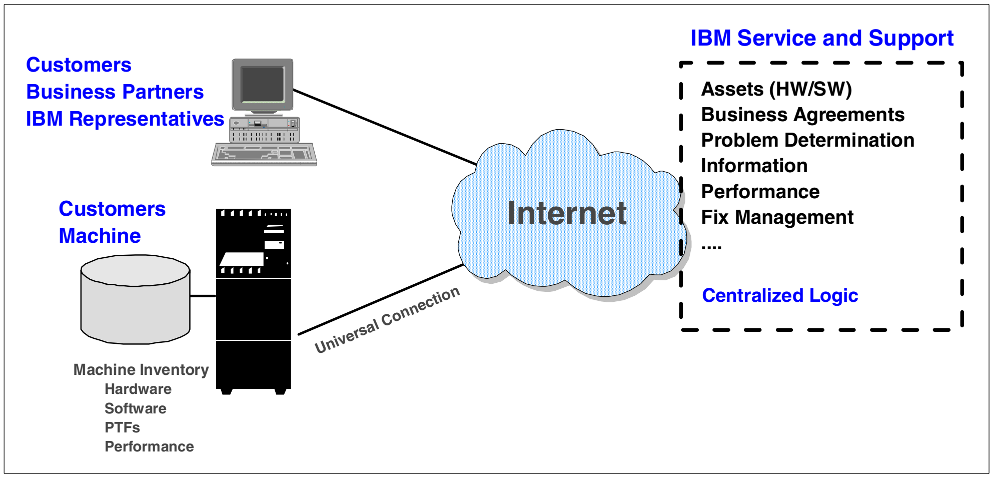


Figure 2. Electronic support overview

1.1.3 Benefits for customers

If you do not have a connection to IBM and have problems on your system, you have to call IBM to report the problems. When you call IBM, you must provide your system information (hardware and software configurations, PTF lists, system values, and so on) via telephone or e-mail to the IBM Support Center (Figure 3).

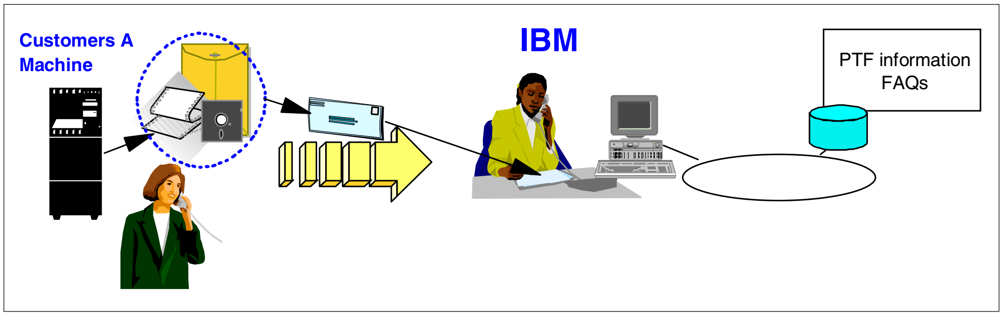


Figure 3. Support via telephone

You should establish an electronic relationship between IBM, your machine, and you. This way, you don't have to repeatedly provide IBM with the same basic information. Then, the information you receive is always available to help IBM quickly resolve problems or answer questions. You simply send your system inventory to the IBM Support Center and an operator retrieves your latest system information from a database (Figure 4).

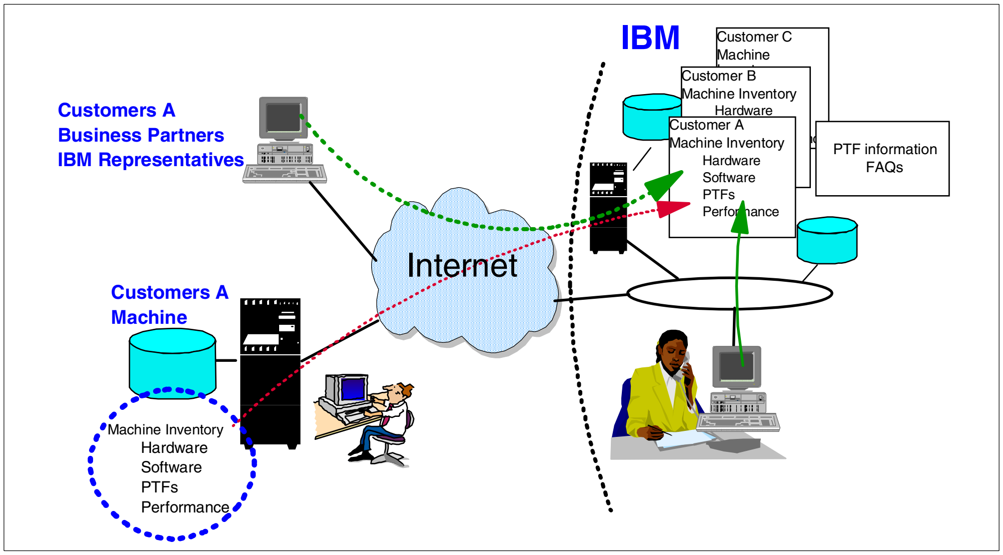


Figure 4. Support using ESP

The IBM Electronic Services for AS/400 and iSeries servers provides this service, which provides the following additional benefits:

- **Increased control**: Advanced knowledge management technology, together with access to more data than before, guarantees a far greater degree of control. You can obtain solutions to problems when you need them. And, you can manage your service by moving to the next level for unsurpassed continuity of support.
- **Increased capability**: Proactive analysis of information received from an iSeries Service Agent can prevent potential outages before they occur. You can access a store of knowledge of problems for installations similar to yours and take advantage of product engineering advanced failure analysis.

1.2 Available applications in electronic support

ESP provides many functions on the Web and through a connection to the IBM site. This section explains some services that are provided through the connection into the IBM site. The connection configuration to these services are created with the Universal Connection Wizard, which is available through Operations Navigator. You can learn more about the wizard in 3.1, "Universal Connection Wizard" on page 37.

1.2.1 Electronic Customer Support (ECS) connection

Simplify your support process with new, flexible options for electronic support over TCP/IP. You can use the power of the V4R5 integrated high-speed V.90 modem to obtain fixes, report problems, and dial up for remote support.

1.2.2 Service Agent

In the past, AS/400 Service Director, a Licensed Product Offering (LPO), was responsible for the hardware problem reporting function, and AS/400 Service Agent, distributed as a PTF to the AS/400 Service Director product, was responsible for system inventory collection and transmission. Now, these two functions are packaged as IBM Electronic Services for iSeries and AS/400. This is a Licensed Product Offering (LPO) that operates on an IBM AS/400 system with OS/400 V4R5.

Service Agent provides two functions:

- **Hardware and software problem reporting**: Predicts and prevents hardware errors by early detection of potential problems, downloads fixes, and automatically calls IBM Service when necessary.

  Note: The hardware problem reporting function of Service Agent can only be activated if your iSeries server is under warranty or if you have purchased an IBM Maintenance Services Agreement.

- **System inventory collection and transmission**: Collects and electronically sends system information based on the following list to IBM to be used as input for problem analysis and problem prevention functions. It also assists IBM in providing improved service. You control what is collected and sent:
  - System values
  - Services attributes
  - Network attributes
  - Software resources
  - Hardware resources
  - PTF information
  - PM/400 performance data

1.2.3 Consolidated inventory collection using Management Central

Management Central is a suite of systems management functions that began to appear with OS/400 V4R3. It provides management capabilities built into the base OS/400 and integrated into the AS/400 graphical interface interface (Operations Navigator) at no additional cost. The latest release, Management Central V5R1, has powerful management extensions. Management Central offers long running, batch, scheduled, or unattended operations distributed to multiple remote systems.

Management Central Extreme Support (V5R1) is a merging technology that involves Management Central's inventory collection support, PM/400e data, and the IBM Electronic Services infrastructure. This merger enables customers to perform the necessary configuration and set up to get a connection to IBM, send collected data, and receive IBM fixes for multiple systems and groups from the Management Central central system. This precludes requiring customers to send data and receive IBM fixes from each individual system as the process is today. For more information, refer 1.4.1, "Extreme Support configuration wizard" on page 11.

1.2.4 Electronic Services for iSeries and AS/400 servers

IBM Electronic Services for iSeries and AS/400 is an exclusive service capability offered to customers that contract for services with IBM. Each iSeries and AS/400 server supported by IBM Electronic Services for iSeries and AS/400 is provided with a Service Agent that monitors system parameters, error conditions, and system and software configuration. This information, which is key to providing the best possible service, is electronically forwarded to the IBM Electronic Services servers.

IBM Electronic Services for iSeries and AS/400 provides a single entry point to comprehensive, customized support, information, and tools. This is the IBM premium World Wide Web location to help you manage your software and hardware computing environment according to your needs, and with applications that share a common registration and user identification process.

IBM Electronic Services for iSeries and AS/400 collects the information from your Service Agent and automatically processes this information to provide reports back to you. Or, it can initiate service activity based on an error condition or a specific request from you.

Customers with existing support contracts for software services or maintenance services are eligible to install the AS/400 Service Agent and to connect to IBM Electronic Services for AS/400 without an additional charge. To take advantage of the key functions of IBM Electronic Services for iSeries and AS/400, you must have one or more of the IBM Service contracts listed here. You can only use the services for which you are entitled (for example, an Alert contract is required to view your Alert reports):

- IBM Warranty
- IBM Maintenance Services for Hardware
- Support Line
- AS/400 System Alert
- PM/400e

Notes

- For a “free” PM/400e, you need a warranty and maintenance contract. For a “fee” PM/400e, you need a PM/400e contract.
- “Alert” type information requires an AS/400 System Alert contract. Please note PM/400e does not function properly with “alert” information.

With this e-business service solution, you have direct access, 24 hours-a-day, to IBM Technical Support from any PC connected to the Internet.

This service offers:

- Enhanced problem prevention and resolution capabilities with a new e-business technical support solution
- A no-charge enhancement to your existing iSeries service contracts
- Enhanced abilities of IBM hardware and software support services that are integrated them into this new IBM electronic support infrastructure
- Monitoring of your AS/400 systems, 24 hours per day, enabling solutions tailored to your system and environment

- Convenient, secure Web access from any PC connected to the Internet, 24 hours-a-day
- No-hassle, cost effective, and efficient electronic technical support

Note: The IBM Electronic Services for iSeries and AS/400 function is available in the United States, France, Germany, Italy, United Kingdom, Norway, Belgium, Luxembourg, Australia, New Zealand, Finland, Sweden, Denmark, and Switzerland. For the latest information, refer to the Web site:

`https://www.ibm.com/services/electronic/`

1.2.5 Performance Management/400e

Behind many successful businesses, you can bet that there's an Information Technology system hard at work (one that's scalable, operating at its peak efficiencies, and offering effective capacity planning and performance analysis).

Unfortunately, the typical capacity planning and performance analysis processes are time consuming and expensive to purchase. As a result, most customers fail to implement any process. The repercussions that businesses face are poorly performing systems or capacities that are lacking.

1.2.5.1 The solution

Performance Management/400e is a dynamic tool shipped with OS/400. It automates many of the functions associated with capacity planning and performance analysis automatically. Because it's simple, there's nothing that you need to do other than activate the function and periodically check whether the data is being collected and transmitted to IBM.

1.2.5.2 The result

Capacity planning and performance analysis reports and graphs provide a crisp picture of your current system operating efficiencies. If you qualify, you could receive this service for free. Based on current trends, these reports let you know when you should consider rectifying an approaching capacity planning problem.

Ultimately, PM/400e puts you in control, instead of your system being in control of you.

1.2.5.3 How PM/400e works

PM/400e is an integrated function with OS/400 that automates many of the steps required in capacity planning and performance analysis. When you activate PM/400e, OS/400 Collection Services automatically collects system utilization information. This information can include CPU utilization and disk capacity, response time, throughput, application, and user usage.

Note: The information collected is limited to non-proprietary system utilization data coming from Collection Services.

1.2.5.4 Information whenever and wherever you need it

The data is summarized and sent to IBM for analysis. Reports and graphs that show a snapshot of weekly happenings, as well as your server’s utilization and growth trends, are returned periodically to you.

1.3 Connectivity options

As mentioned earlier, you should build an electronic relationship with IBM. Figure 5 shows the connectivity options that IBM provides. With the Electronic Customer Service (ECS) connections that IBM started providing in 1989 (with the V1R2 release of OS/400), customers used an SNA connection via an IBM 5853 modem. However, currently, many customers connect via the Internet. With the release of V4R5, IBM started providing TCP/IP connectivity since the Internet's standard protocol is TCP/IP.

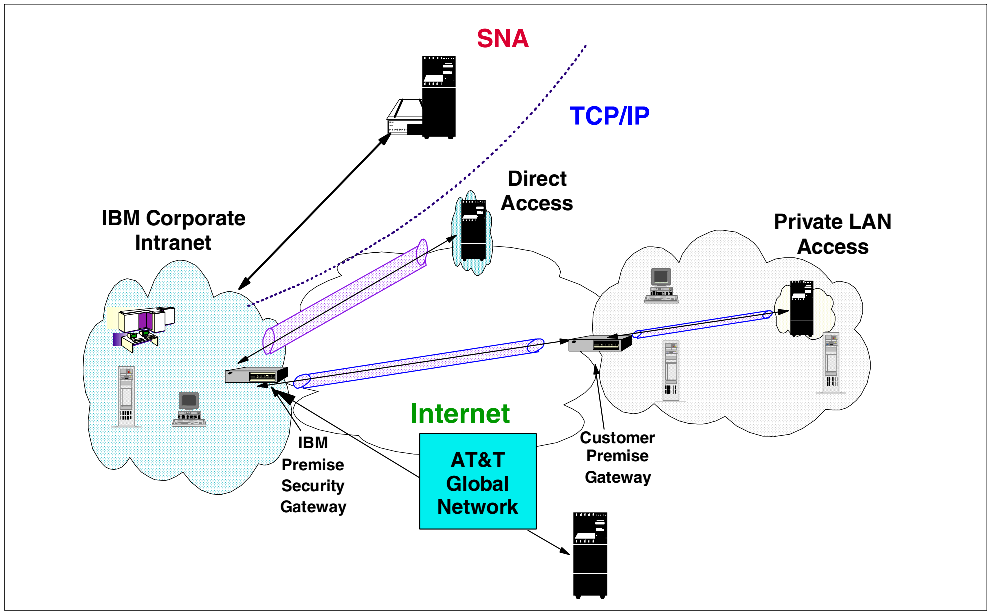


Figure 5. Connectivity options to IBM

There are four options for TCP/IP connections:

- **Dial-up connection using AT&T Global Network Service**: This connection is made across the AT&T Global Network Service (AGNS), which provides a secure connection between the customer and IBM. Authentication occurs when a connection is made to AGNS. At that time, AGNS assigns an IP address to the customer's Point-to-Point Protocol (PPP) client.
- **Dial-up connection using an ISP**: If you have an existing dial-up or leased line connection to an ISP and want to use it to connect to IBM, this option is available starting with the release of V5R1. This connection uses a virtual private network (VPN) connection over the Internet to IBM. This scenario requires your system to connect using PPP to IBM. If you want know about a VPN, see *AS/400 Internet Security Scenarios: A Practical Approach,* SG24-5954.
- **Direct access**: Use this option if your iSeries server has direct access to the Internet, such as a LAN across the Internet to IBM. This scenario also uses a VPN connection to IBM by using your existing direct connection to the Internet. This connection scenario requires your system to have a globally routable IP address.
- **Private LAN access (a multi-hop connection to the Internet)**: Use this option if you plan to use a private LAN access connection, such as a LAN

across the Internet to IBM. This connection uses a VPN secure gateway connection (tunnel mode) to IBM by using your existing direct connection to the Internet. This connection scenario requires you to have a globally routable IP address in a customer premise border gateway box such as a firewall.

Table 1 lists the application you can use for each connectivity option. You can use the ECS and legacy services on SNA and TCP/IP connection, but you can only use new services on TCP/IP connections.

Table 1. Connection options for Electronic Services and Electronic Support

Function	**Fee/Free**	**SNA/SDLC**	**TCP/IP (PPP or AGNS)**	**TCP/IP (any ISP with VPN)**
Existing IBM Electronic Service Agent inventory collection	Base (Free)	No	V4R5	V5R1
Consolidated IBM Electronic Service Agent inventory collection using Management Central	Base (Free)	No	Umbrella PTF: 5798-RZG SF64660[2]	V5R1
IBM Electronic Service Agent problem reporting	Warranty or Maintenance	#9771 or #4745 with modem[1]	V4R5 (with PTF SF64124)	V5R1
PM/400e	Warranty or Maintenance	#9771 or #4745 with modem[1]	Umbrella PTF: 5798-RZG SF64660[2]	V5R1
ECS - Send PTF order - Send Service Request - Query Problem Status - Order Support PTFs	Base (Free)	#9771 or #4745 with modem[1]	V4R5 (with PTF SF64124)	V5R1
Remote Support	Support line	#9771 or #4745 with modem [1]	V4R5 (with PTF SF64123) not for AGNS	No

1. The IBM 7852-400 can be attached to the second port on the 9771 adapter on the Model 250, 270, and 8xx systems. It provides an option for earlier participation for both new system installations (if you choose to order the modem and cable) or migrations to new hardware (if you have an existing cable and modem). Once the cable and modem are attached to the 9771 RVX port, you must manually configure for specific functions. For more information, go to:
   `http://www.as400.ibm.com/tstudio/planning/esa/esa.htm`
2. This umbrella PTF includes:
   - PM/400: 5769-PM1 PTFs: SF64316 and SF64352
   - 5769-SS1 PTFs: SF64343, SF64337, SF64369, and SF64367
   - Service Agent 5798-RZG - SF64519

   For more information, see the cover letter for SF64660.

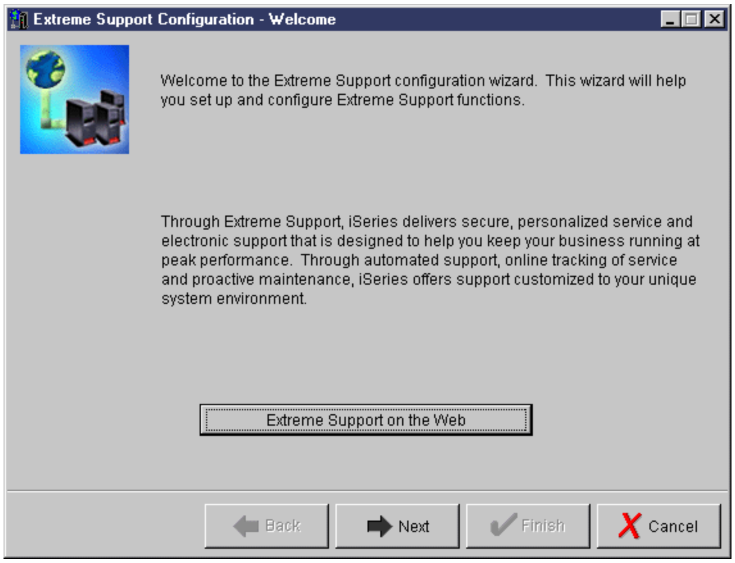
1.4 Connectivity tools for iSeries

An iSeries server provides many connection wizards to configure a connection to IBM for ESP. This section briefly explains the connection wizards that are provided by Operations Navigator.

1.4.1 Extreme Support configuration wizard

Through Extreme Support configuration wizard, the iSeries server creates the configuration for delivering secure, personalized service and electronic support that is designed to help you keep your business running at peak performance. Through automated support, online tracking of service, and proactive maintenance, the iSeries server offers support customized to your unique system environment.

To access the Extreme Support configuration wizard, expand Management Central in the Operations Navigator window. Right-click **Extreme Support** and select **Configuration...** from the pop-up menu. This wizard is also available via EZ-Setup. The Extreme Support Configuration wizard - Welcome dialog appears (Figure 6).


Extreme Support Configuration - Welcome

Welcome to the Extreme Support configuration wizard. This wizard will help you set up and configure Extreme Support functions.

Through Extreme Support, iSeries delivers secure, personalized service and electronic support that is designed to help you keep your business running at peak performance. Through automated support, online tracking of service and proactive maintenance, iSeries offers support customized to your unique system environment.

Figure 6. Extreme Support Configuration wizard - Welcome

The wizard guides you through the configuration and setup. This process involves:

- Choosing the functions or services you want to configure:
  - Send collected data to IBM for service and support
  - Receive fixes from IBM and report problems to IBM
- If a connection does not exist, prompting you to create a new connection using the Universal Connection Wizard. Some of the information required includes:
  - Contact information
  - Type of connection: ECS or IBM Electronic Service Agent for AS/400
  - Interface, hardware resource, and line information

  - Configuring what information and systems or system groups you want to collect
  - Scheduling the collection
  - Receiving fixes

After you select which services to configure, the Electronic Service Agent welcome window appears, which provides additional information about the services provided. If you choose the Send collected data function and select Next, the license agreement appears. Then, you have two choices:

- Accept the agreement (if accepted, any collected and sent data is covered by this agreement).
- Do not accept the agreement (if *not* accepted, the wizard ends and the Send Collected Data feature is not configured).

You then configure Send Collected Data and setup Receiving Fixes.

You may review the Electronic Service Agent History at any time. The history details the information being sent to IBM from the Agents Object in MC.

In V4R5, you only had the ability to collect and send data to IBM. The process involved:

- Agreeing to license and data usage agreements
- Configuring your connection to IBM with the Universal Connection Wizard
- Scheduling a collection and sending data using Management Central
- Registering systems on the Web

With V5R1, the Management Central Extreme support automates all these processes, enables customizing of information that is sent, and includes the ability to receive IBM fixes into one wizard.

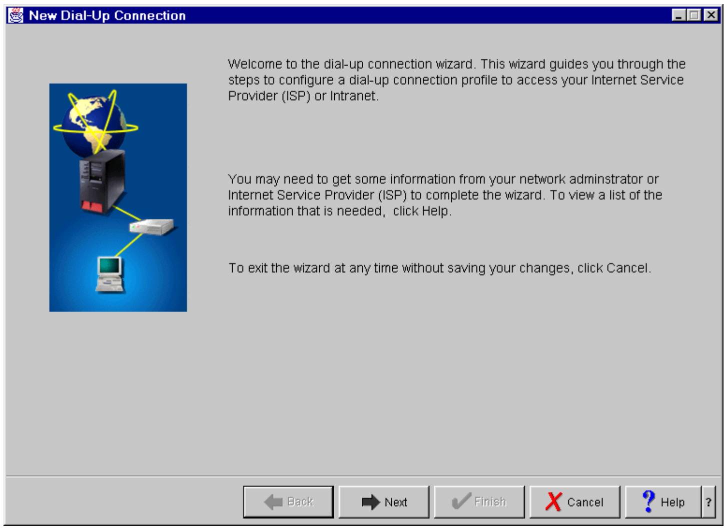
1.4.2 Universal Connection Wizard (UVC)

Currently, the iSeries server contains a number of customer-to-IBM applications that use different connection mechanisms to provide an electronic exchange of system and customer information between the customer and IBM. UVC provides a means for consolidating the connection methods for ECS, PM/400e, service agent, and management central inventory. This redbook explains how to use the wizard later in this redbook.

1.4.3 Dial-up connection wizards

Your iSeries server connects to the Internet through a dial-up (modem) connection to an Internet Service Provider (ISP). You may choose this wizard if you are working in a branch office of a company that has a private network that uses dial-up connections (Figure 7).

The wizard helps you configure a dial-up (modem) connection to your ISP or private network. We explain how to use the dial-up connection wizard later in this book. For more detail, refer to 3.3.3.1, “New Dial Connection Wizard: Creating a dial-up connection profile” on page 62.



Welcome to the dial-up connection wizard. This wizard guides you through the steps to configure a dial-up connection profile to access your Internet Service Provider (ISP) or Intranet.

You may need to get some information from your network adminstrator or Internet Service Provider (ISP) to complete the wizard. To view a list of the information that is needed, click Help.

To exit the wizard at any time without saving your changes, click Cancel.

Figure 7. New Dial-up Connection welcome dialog

Chapter 2. Network security concepts and overview

This chapter describes the goals of network security, the threats against those goals, and the technologies that have been developed to counteract those threats.

Disclaimer

This chapter is *not* intended to provide comprehensive information on network security. It is merely an introduction to the topic and a reference to other relevant sources of information.

You should *not* take network security lightly. To the very minimum, you should become aware of the risks and decide with which ones you can live and from which ones you must protect your network. This chapter does *not* include a complete list of risks and measures to counteract them. Use it only as a staring point to either perform serious research on the topic or to hire consulting services to do it for you.

2.1 Designing network security

Network security design, as part of a total security plan within an organization, can be an overwhelming and complex subject. You can break down the process into the following major steps:

1. Identify and decide *what* you need to protect (your assets).
2. Know your enemy. Determine from whom or what are you protecting your network (the threats).
3. Create a comprehensive security policy and implementation plan.
4. Implement the security policies.
5. Continually monitor to detect any deviation from your policies and take actions if needed.
6. Periodically review your processes and policies to update them and improve them.

2.1.1 Goals of network security

Network security should be implemented to protect two objects: the data that is transmitted on the network and the computers that are connected to the network. Network security cannot replace physical site security, host security on the connected systems, application security, and user security education. It can only act as a first layer of defense.

Figure 8 shows that you should always implement security in layers. That is to assume that if an error or an attack in one layer opens a hole, there is a second layer of defense that protects the heart of your assets.

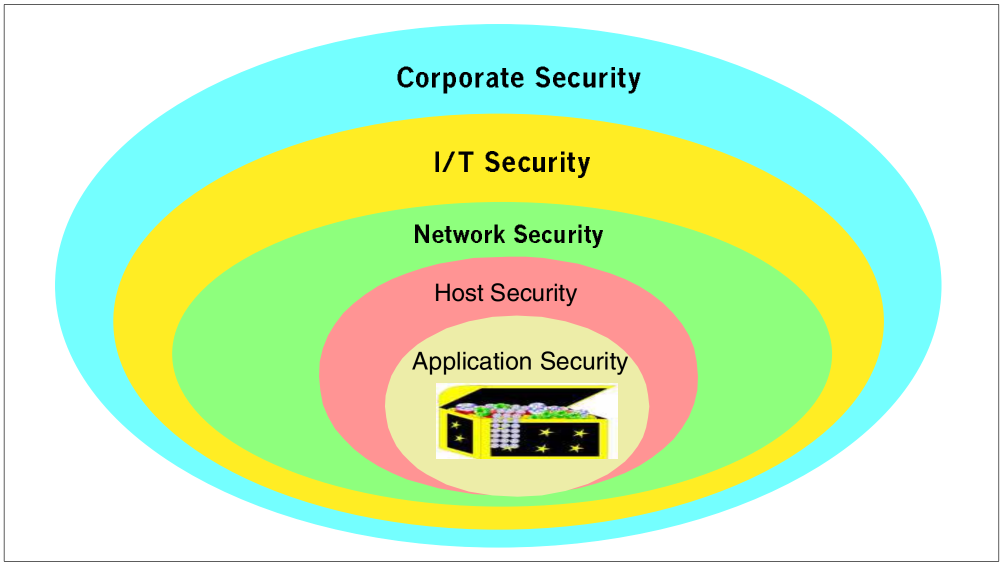


Figure 8. Implementing security in layers

Important

Security is only as strong as the weakest link in the chain.

The goals and basic concepts of network security are similar to other aspects of security in computer systems. The main difference is that network security often deals with data that is transmitted, parties that are remote, and networks that are public and more vulnerable to attacks. Also, the myriad of devices of different characteristics in a network makes network security particularly challenging.

First, we must describe two central concepts of security:

- **Authentication**: Determine that the users are who they claim to be. The most common technique to authenticate is by user ID and password.
- **Authorization**: Permit a user to access resources and perform actions on them. An example of authorization is the permissions on OS/400 objects.

These concepts are necessary to achieve the three primary goals in all types of security:

- **Confidentiality**: Only authorized users can view the data. For data that is transmitted through a network, there are two ways to achieve this goal:
  - Make sure that only authorized persons can access the network.
  - Encrypt the data.
- **Integrity**: Only authorized users can modify the data, and they can only modify it in approved ways. The data is not changed either by accident or maliciously. For data that is transmitted over a network, there are two ways to achieve this goal:
  - Make sure that only authorized persons can access the network (not easy to achieve in public networks such as the Internet).
  - Digitally sign the data.

- **Availability**: The resources are always available and performing at the expected level. Users can access applications and data at all approved times. The resources have no unexpected downtime as a consequence of an attack.

Network security is also often the first line of defense for securing your host systems. The network is replacing the physical gates and doors to enter your organization. Attackers from outside your organization must break through either your network or your physical security before they can attempt to break your host security.

2.1.2 Threats against network security

This section explains some common threats to the network security goals:

- **Sniffing**: Computers with access to the public network can record the traffic flowing through it. If data or commands are sent unencrypted, it is very easy for unauthorized people to passively eavesdrop. *Sniffing* is a threat to *confidentiality,* but if user IDs and passwords are sniffed, the threat becomes more serious because the attacker could then impersonate a legitimate user.
- **Impersonation**: The attacker tricks your security system passing as an authorized user. An example would be when the attacker steals valid user IDs and passwords by recording network traffic while users sign on. Another example would be if the communication is over a public network, and it is not digitally signed or signed with a weak technology. In this case, an attacker could modify or enter completely new data and commands. Impersonation can be a threat to all three goals of computer security.
- **Decryption**: If the data is sent over a public network, attackers can often easily obtain the encrypted data. If the encryption is weak, the attackers can decrypt the data in a fairly short time. Decryption is a threat to confidentiality.
- **Flooding**: If an attacker sends large amounts of data, such as connection requests to a public Web server, it could fill the network bandwidth. The network resource becomes overused, which prevents access to other users or greatly affects performance. Flooding is a threat to availability.
- **Technology or application weakness**: The TCP/IP protocol, some of its applications, and some operating systems have inherent security shortcomings. Sometimes these shortcomings are due to the objectives of their original design (openness or easy communication between computers and applications). For example, the UNIX Sendmail application used to run e-mail is famous for a long history of security problems. Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), and Syn Floods all present security holes related to the insecure structure on which TCP was designed. Known security problems for UNIX, Windows, and OS/2 are documented at the Computer Emergency Response Team (CERT) Web site at: `http://www.cert.org/`

  Likewise, company-developed applications or software purchased from vendors may have security weaknesses that attackers can exploit. The degree of the damage depends on the nature of the problem. The most common damage is to shut down a system. It could be more serious to allow the attackers access to data that they can alter or use to their advantage. Technology and application weaknesses exploited by malicious attackers are threats against all goals of network security. To protect yourself, you must keep up to date with the vendors' security updates and rely on providers with a good reputation for paying attention to security. If you develop your own applications to run on hosts that are accessed from the network, security must always be a top priority in the design goals.

Note: When considering the threats to your environment, keep in mind that the largest percentage of vulnerabilities are the result of unintentional or accidental actions by internal users.

2.1.3 Evaluating the threats

When you have identified the resources you need to protect and the threats to which they are exposed, you must evaluate your options. Answer the following questions:

- What would the damage be for us?
- What would the gain be for the attacker?
- How much will it cost the attacker to break in?
- How much will it cost us to protect against the threat?

Attack trees are a good tool for threat assessment. Figure 9 shows an example of an attack tree. You can find more information on this subject at:
`http://www.ddj.com/articles/1999/9912/9912a/9912a.htm`

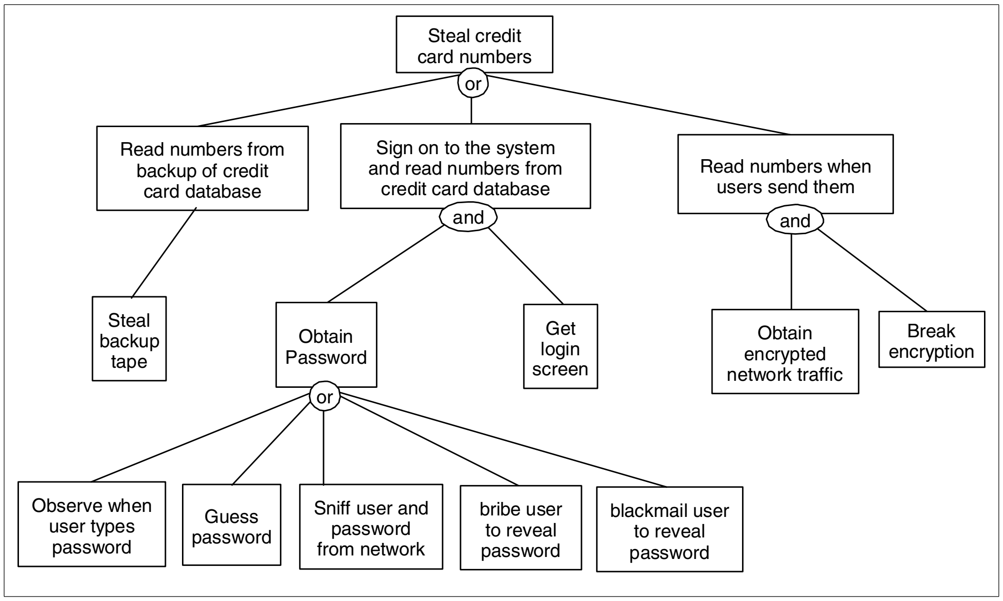

Steal credit card numbers
or
Read numbers from backup of credit card database
Sign on to the system and read numbers from credit card database
and
Read numbers when users send them
and
Steal backup tape
Obtain Password
or
Get login screen
Obtain encrypted network traffic
Break encryption
Observe when user types password
Guess password
Sniff user and password from network
bribe user to reveal password
blackmail user to reveal password

Figure 9. An example attack tree

2.1.4 Creating a security policy

When you have identified and assessed the threats, you must decide from which ones to defend your network. If the damage, both direct and indirect, is smaller than the cost of protection, it is not worth the investment to implement the protection.

Develop well-organized security policies that are easy to understand and only include relevant information. If it is too hard, or takes too much time to understand your policies, employees do not read them, and therefore, ignore them.

Developing a poorly organized or unclearly written policy would be a waste of time and money.

You must make the policies as easy to follow as possible without compromising security. Be aware that there are many organizations with extensive security policies that often ignore them because the policies make real work too hard. Top-level management must understand, agree with, and support all security policies. In general, technical specialists should not be responsible for developing security policies. They should help to identify the risks and implement them by choosing the appropriate technologies and products.

Your policy should also prepare your response to an attack or accident that compromises security. Consider these examples:

- Keep up-to-date lists of people and organizations to contact in case of a security emergency. Include the names of the persons in your organization who are expected to make those calls.
- Make a list of the most likely attacks to which your network is vulnerable, and consider what you should do when they happen, for example:
  - Should you immediately disconnect your network from the Internet?
  - How can you track the attacker? What supporting documentation is required? Who must be informed? If a journalist calls, what should you tell them?
- Have drills or rehearsals to verify that your people and organization react according to plan.

You may not be able to prevent an attack, but you can avoid being unprepared for it.

2.1.5 Security plan

Before you create a specific security policy, develop an overall security plan. It should be a set of general guidelines and a framework for the security policy. The purpose of the security plan is to make the individual components of the security policy consistent and the whole plan comprehensive.

2.1.6 Anatomy of a security policy

The network security policy is part of the entire IT security policy, which is part of the company's corporate security policy (Figure 8 on page 16). A network is not secure without securing the other layers. For example, if there is no physical security at your site, anyone can connect a sniffer to your network, and anyone can cut the power to your systems. Figure 10 illustrates one way of organizing the security policy.

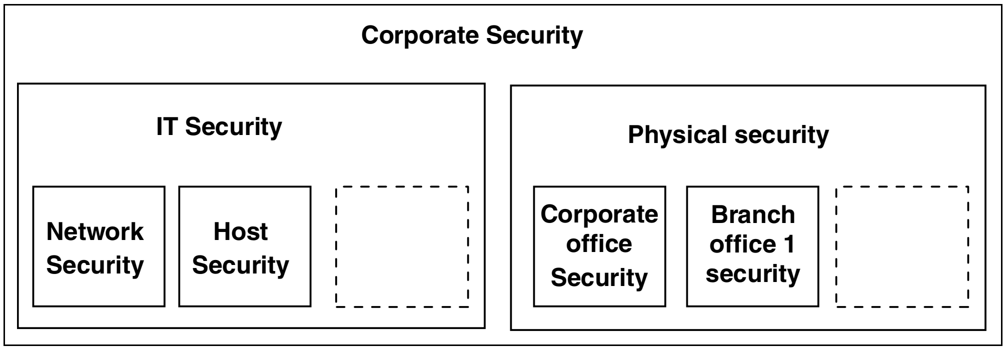


Figure 10. Some components of a security policy: Network security does not exist in a vacuum

Note: It is beyond the scope of this redbook to provide detailed information on overall security concepts, policies, and processes. An excellent starting point for this subject is *Site Security Handbook*, RFC 2196, which lists the elements of a sound security policy.

The following list outlines some examples of security policy components:

- Guidelines on required and preferred security features of new products that the company purchases
- Privacy policy dealing with electronic mail, keystroke recording, files stored on company's media, and other uses of company resources
- The messages that must be displayed, which warn users that they might be monitored and that inform them that only authorized access is permitted
- An *Acceptable Use Policy* (AUP) that clearly defines the purposes for which the company's systems and networks may be used
- Responsibilities of users, IT staff, and management, and how each of them should handle a security incident
- The messages that should be displayed, which warn users that only authorized access is permitted and that warn them when they are monitored
- The connections that are allowed to external networks and systems
- The services that are permitted from the internal network to the Internet, who is authorized to access those services, and what restrictions apply
- Same as the previous point, but from the Internet to the company network
- How the configuration of systems and networks may be changed and who may change them
- Who is allowed to access what systems, and in which ways they may access those systems
- How to authenticate users, password requirements, and local and remote user authentication guidelines
- Availability of resources (how to achieve the desired level of availability and performance and how to measure the service level; how to monitor for deviations from the normal or expected values; what to do when an availability or performance anomaly is detected)

- Who is authorized to perform maintenance of systems and networks, especially which type of remote maintenance is allowed (how authorized maintenance personnel proves their identity)
- How to report policy violations, including contact information
- How to handle queries about security incidents and requests for confidential information
- Cross references to security procedures and other documents (policies, laws, government regulations)

2.1.6.1 Sample security policy

Figure 11 and Figure 12 show a sample security policy for user IDs at Itsoroch Inc.

Computer user IDs

There are two types of user IDs: personal and system. A system user ID is used *only* for maintenance and configuration of systems. If the maintenance or configuration can be performed without the use of a special system user ID, it *must* be performed with a personal user ID. A personal user ID must be used at all other times. No user may use a user ID for which they are not authorized to use. Only the owner of a personal user ID is authorized to it. The owner of a system user ID authorizes others to it, following the security policy for the user ID's system or systems.

Personal user IDs

Each person authorized to access any of Itsoroch Inc.'s computers or networks must be assigned a unique user ID. The user ID must be recorded in both the online user database and in a paper document. The format for this record is:

```
Personal User ID
User ID:                            <user ID>
Class:                              <user class>
Owner:                              <firstname> <lastname>
Office telephone number of owner:   <tie line number>
Home telephone number of owner:     <telephone number>
Room number of owner:               <room number>
```

Figure 11. Example user ID security policy for Itsoroch Inc. (Part 1 of 2)

System user IDs

Many systems require that a special user ID is used for some or all configuration and maintenance tasks. All system user IDs must have a manager. The manager is responsible for granting access to the user ID and updating the password. The current password of all system user IDs must be stored in a password storage (refer to *password storage document*). All system user IDs must be recorded both in the on-line user database and in a paper document. The format of this record is:

```
System User ID
User ID:                  <user ID>
System:                   <system name as in systems database>
Purpose:                  <text describing the purpose of this user ID>
Manager user ID:          <Personal user ID of person managing this system
                          user ID>
Authorized users:         <a list of the personal user ID of all users
                          that are authorized to use this system user ID,
                          including the manager of this user ID>
```

How to obtain a new user ID

The owner of the new user ID must submit a registration request to one of the corporate user ID managers (refer to the *procedure document*). The request must be a complete personal or system user ID record as indicated above. Note that the intention is that the user ID database contains the same information as the request.

How to handle violations

In case of a violation to this policy, contact:

<contact information>
<description of actions that should be taken by the party that is contacted>

Objectives of user IDs

The objective of a user ID is to identify users for authorization, accounting, auditing, and responsibility.

Notes

A personal user ID does not authorize the owner to any of Itsoroch Inc.'s systems. Authorization must be obtained from the security manager of the system you need to access.

References

Reference to password storage
Reference to a list of user ID managers

Document owner

<first name> <last name>
<telephone number>
<room number>

Figure 12. Example user ID security policy for Itsoroch Inc. (Part 2 of 2)

Update and review your security policies regularly. An outdated security policy is *more* dangerous than no security policy at all because an outdated policy gives a false sense of security and a belief that everything is under control.

2.1.6.2 References for security policies and standards definitions

It is important that your implementation follow your company's security policies and security standards.

Good guidelines for developing computer security policies and procedures for sites that are connected to Internet are available in the following documents and Web sites:

- *The Site Security Handbook*, RFC 2196:
  `http://www.rfc-editor.org/rfc/rfc2196.txt` or
  `http://www.faqs.org/rfcs/rfc2196.html`
- National Institute of Standards and Technology:
  `http://cs-www.ncsl.nist.gov/policies/welcome.html`
- Center for Information Technology/Security
  `http://irm.cit.nih.gov/policy/security.html`

If your company does not have a security policy, standards, or procedures, IBM Global Services has trained security consultants that can help you to define your policies, standards, and procedures.

For more information regarding IBM Security Services, see:

- `http://www.ibm.com/security/services`
- `http://www.ibm.com/services/e-business/security`

2.2 Security characteristics of popular protocols and services

This section provides an overview of the security characteristics of the most popular protocols and services used on the Internet.

2.2.1 Internet Protocol (IP) security characteristics

Although IP has some security functions in the standard, they are not used on the Internet. The reason for not using them is that these functions do not map well to today's security requirements.

IP is responsible for transporting *datagrams*, small packets filled with data, between hosts. It does not completely solve any of the three main security goals:

- **Confidentiality and authentication**: IP does not provide data encryption. You must implement other protocols, such as Secure Sockets Layer (SSL) or IP Security (IPSec) protocol to add encryption and authentication if it is required. IP is being enhanced to include security. IPSec is optional in IP version 4 (IPv4), and standard in IPv6.
- **Integrity**: IP protects the IP header with a simple *checksum*. The checksum is intended to prevent transmission errors and defective network equipment. It is not strong enough to afford protection against malicious attacks. The checksum is easy to forge.
- **Availability**: IP provides for better availability by allowing datagrams to travel alternative paths from the source to the destination. However, IP cannot

guarantee that there *will be* an available path; only the links and routers in the network can do this.

2.2.2 Internet Control Message Protocol (ICMP) security characteristics

The ICMP includes a suite of messages intended for network diagnostics and error reporting. For example, ICMP messages report that a datagram could not reach its destination or that a router does not have enough buffer capacity to forward datagrams. Routers use ICMP redirect messages to inform a host that there is a shorter route to which it should direct traffic. PING (echo request/reply) and TRACEROUTE use ICMP messages.

There are two classes of ICMP messages: error and query. Query messages are more dangerous from a security standpoint than error messages are.

ICMP is an integral part of IP and must be implemented by every IP module. It is described in RFC 792.

2.2.2.1 How an attacker can take advantage of ICMP

Attackers can use ICMP to gather information about your network. Since ICMP is in part designed to report errors in a network, it is a good tool for reporting network information.

Attackers also use ICMP to flood networks by sending so many messages that all the network bandwidth is used up. It may be impossible to stop this kind of attack.

If an attacker manages to compromise your network and install a program on one of your internal systems, the attacker can later use ICMP to communicate with the pirate program. This communication can be done with any ICMP message. Therefore, you must carefully determine what ICMP services you need to allow and block the rest.

2.2.2.2 Why you should not block all ICMP services

If you block *all* ICMP services to your internal network, several error messages from the network cannot reach you. Your local systems are unaware that the error occurred and do not react to it. This creates problems that are difficult to debug. If you do not want to allow any ICMP to your internal network, you should not use NAT or similar techniques to allow your internal clients to access the public network directly. If you use a proxy to enable your internal clients to access the public network, you only need to allow some ICMP services to the proxy itself.

2.2.2.3 ICMP messages are less dangerous to allow

ICMP error messages are less dangerous to allow than query messages because no system replies to them. *Requirements for Internet hosts -- Communication Layers*, RFC1122, requires that no host sends a reply to ICMP error messages. The ICMP error messages report the following conditions:

- **Source quench**: A request that the host transmitting data slows down. It is not widely used.
- **Time exceeded**: All IP packets have a *Time To Live* (TTL) field. Any router that forwards a packet must decrease this field by the number of seconds during which the router stored the packet. If the packet was stored for less than one second, it must be decreased by one. If decreasing the TTL makes it zero or less, the router must discard the packet and send an ICMP time

exceeded message to the originator of the packet. Routers may have a configuration option to disable sending the ICMP time exceeded message. If the time exceeded is enabled on the router, an attacker can access as much information as it can by using ping to the router itself. See *Requirements for IP Version 4 Routers*, RFC 1812, for details. The TRACEROUTE tool uses this feature by sending packets with TTL 1, 2, 3, and so on. It listens for the time exceeded messages coming back and finds the path packets to take to the destination. Note that the *return* path may be different.

- **Parameter problem**: If a router or host finds a problem with the IP header, but the checksum is OK, it must send a parameter-problem ICMP message. Most IP packets do not have such problems, but should still be enabled.
- **Unreachable**: There are several types of unreachable messages. The most commonly unreachable is probably code 4, “fragmentation needed and DF (Don’t Fragment) set”. It is sent when the packet is too large for the router to forward, and the Don’t Fragment flag is set. The router discards the packet and sends an unreachable message with code 4 to the originator. This procedure lets the originator find the Path MTU (PMTU) to that specific destination.

2.2.3 Transmission Control Protocol (TCP) security characteristics

The TCP does not provide security functions. It has two functions, sequence numbers and port numbers, that provide weak security. These two functions were designed to protect against network errors and to identify connections. You should not rely on these TCP protocol features for security.

TCP is responsible for communication sessions. To transport data, it uses IP. TCP does not guarantee any of the main goals of security:

- **Confidentiality**: Like Internet Protocol, TCP does not provide data encryption. You must implement other protocols, such as Secure Sockets Layer (SSL) or IP Security protocol (IPSec) to add encryption and authentication if it is required. IP is being enhanced to include security. IPSec is optional in IP version 4 (IPv4), and standard in IPv6.
- **Integrity**: TCP segments include a checksum similar to the IP packet checksum. The difference is that the data is also included in the checksum. As with the IP checksum, it is trivial to forge.

  TCP packets also include a sequence number. But, if the attackers can see the communication, they can easily obtain the sequence numbers. If the attackers cannot see the sequence numbers, it can be easy or difficult to guess them. The difficulty depends on how the initial sequence numbers are chosen. Good TCP implementations choose them in a way that is almost impossible to guess.
- **Availability**: TCP provides some availability by retransmitting data that is not acknowledged by the remote system. However, TCP cannot guarantee that the network to the remote system will be available.
- **Authentication**: The only authentication TCP provides is the port number. If you trust the remote system, this can be good enough for your needs. But if the remote system is not trusted, port numbers do not provide any security.

2.2.4 Simple Mail Transfer Protocol (SMTP) security characteristics

To understand the security issues with SMTP, you need to understand the basic structure of the SMTP protocol. Figure 13 provides a high level overview of the SMTP protocol components and flow.

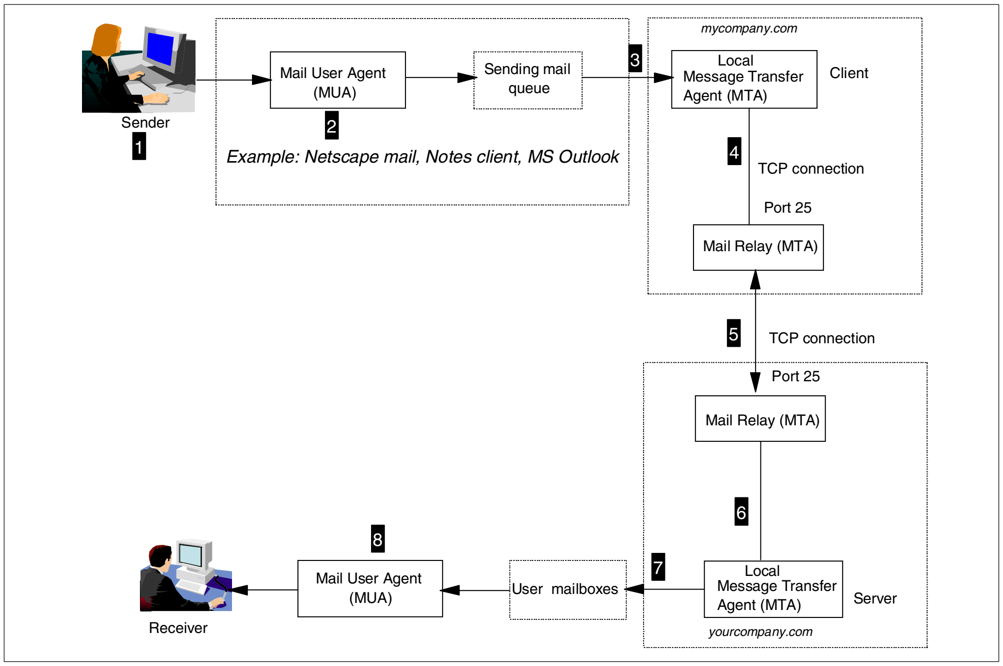


Figure 13. Simple Mail Transfer Protocol (SMTP) protocol structure overview

The following steps summarize the flow of a piece of mail from the sender to the receiver using SMTP:

1. User *marcela@mycompany.com* sends an e-mail from her PC client, using Netscape mail or Lotus Notes client, for example, to user *erik@yourcompany.com*.
2. The Mail User Agent (MUA) program in the mail application is invoked.
3. The MUA passes the mail to the Mail Delivery Agent (MDA) which, in turn, transfers it to the local Message Transfer Agent (MTA) for delivery.
4. The local MTA client (part of the SMTP application, such as OS/400 SMTP, UNIX Sendmail, Lotus Domino SMTP) in *mycompany.com,* sends the mail to the company's *mail relay* MTA.

Mail relay

A mail relay is an MTA that accepts to send mail for domains outside the local domain.

5. The mail relay in *mycompany.com* sends the mail to the mail relay MTA in *yourcompany.com*.
6. The mail relay MTA in *yourcompany.com* passes the mail to the local MTA in the SMTP server.
7. The local MTA at *yourcompany.com* delivers the mail to the receiver's mail box.

8. The MUA in the mail application at the receiver’s PC is invoked to receive the mail.

The main security problem related to SMTP is to configure an MTA as an open relay. An *open relay* is an MTA that accepts mail from all domains and sends it to any domain without restrictions, neither in the inbound or in the outbound.

Important

Never configure your SMTP server as an open relay. Configure your local and mail relay MTAs with inbound and outbound restrictions to avoid open relays. Attackers take advantage of open relays for e-mail spamming.

The most common attack against SMTP is spamming and mail bombing.

2.2.4.1 Fighting mail spamming

In an effort to fight abuse and misuse of the Internet, there are some organizations that keep track of open relays and publish an offenders list. An example of such an organization is Mail Abuse Prevention System (MAPS). Its goal is to stop the Internet's e-mail system from being abused by spammers. MAPS encourages ISPs to enforce strong terms and conditions that prohibit their customers from engaging in abusive e-mail practices.

In many instances, the ISP customers unintentionally become spammers by misconfiguring their MTA as an open relay. MAPS Realtime Blackhole List (RBL) is a list of networks used by spammers to either originate or relay spam. Organizations can use this list to configure their MTA to reject mail from networks in the RBL. For more information, visit the site at: `http://www.mail-abuse.org/rbl/`

2.2.5 Domain Name System (DNS) security

The DNS is a critical part of your internal network infrastructure. The information in your internal DNS can be very valuable to attackers. It can identify the systems attackers can target and figure out your organization. You can configure your DNS server to accept queries only from internal clients or to prevent zone transfers. A popular DNS configuration in secure networks is known as *split DNS*. Refer to 2.3.7, “Domain Name Server (DNS)” on page 34, for more information.

Domain Name System Security Extensions, RFC 2065, describes extensions to DNS to provide security mechanisms to assure data integrity or authentication.

2.2.6 Passive attacks

The objective of passive attacks is to gather information without being discovered. These types of attacks are usually difficult to detect because there are no obvious symptoms or tracks left by them. Two examples of passive attacks are:

- **Eavesdropping**: This attack is also known as *packet sniffing*. Intruders record network traffic using protocol analyzers or similar devices. The intruder analyzes the data looking for user IDs and passwords, credit card numbers, SNMP data, and other information that they can use to their advantage or to perform another attack. To counteract eavesdropping, you should have good physical security policies that prevent physical access to the network. Avoid the use of protocols or applications that are susceptible to sniffing (sending information that should remain confidential in cleartext or with weak encryption). Use strong encryption whenever it is required.

- **Port scanning**: Crackers use port scanning to create a map of your network or find holes that they can use to attack.

2.2.7 Denial of Service (DoS) attacks

DoS attacks are aimed to deny legitimate users access to your network and computer resources. They prevent authorized use of services by using up network and system resources. Examples of DoS attacks are:

- **TCP SYN attack**: To perform a SYN attack, the attacker sends thousands of invalid SYN *start connection* messages to the victim system. The victim host automatically takes these requests and waits a number of seconds for the connection to continue. This delay, combined with the large number of requests received in a short time, creates an enormous load on the victim machine, and it becomes unable to respond to legitimate requests. A SYN attack is usually done from a bogus address. A different fake address is sent with each packet, which makes it extremely difficult to trace. One way to counteract this attack is to close open connections when a configurable threshold has been reached.
- **Mail bombing**: This type of attack consists of sending a large number of e-mail messages to one or more e-mail addresses. This attack overloads network connections, fills up the disk, and uses all available CPU on the victim's mail server. This attack is very difficult to prevent because the mail is sent to a valid address. You can detect this attack by monitoring resources on the mail server and detecting deviations from normal operation conditions. For example, set a disk use threshold above what an alert is sent to the operator, and the SMTP server stops accepting mail.
- **Ping of death**: The attacker modifies the IP header indicating that there is more data in the packet than there actually is. Or it exceeds the maximum allowed packet size, which causes the victim system to crash.
- **Viruses**: These are malicious applets written in Java, JavaScript, or ActiveX programs that destroy critical files or tie up resources.

There are intrusion detection tools and features in firewalls and routers that help to detect well-known DoS attacks and either take action or report the condition. You can also detect attacks and track the intruder by keeping logs or a history of the connections (timestamp, source and destination hosts, duration, bytes transmitted).

2.2.8 Unauthorized access

Intruders can gain access to computer and network resources to which they are not authorized to use usually by sniffing valid user IDs and passwords that travel through the network or due to configuration errors. Two examples of unauthorized access are:

- **Spamming**: E-mail spamming consists of taking advantage of an open mail relay usually to send e-mail to hundreds or thousands of users through a victim's mail relay that is configured as an open relay (see 2.2.4, "Simple Mail Transfer Protocol (SMTP) security characteristics" on page 26).

To avoid open relays, configure your SMTP server to prevent someone from outside your network from using your relay to deliver mail outside your network. You should configure your local MTA (see Figure 13 on page 26) to only accept mail from internal hosts. You should configure your mail relay MTA to only accept mail destined for your local domain. If your server allows others to relay unsolicited mail, other servers might block the mail that comes from your server. See 2.2.4.1, “Fighting mail spamming” on page 27, for more information.

- **Stolen password**: Intruders steal a valid user ID and password to impersonate a valid user. To counteract this attack, use advanced security technologies, such as VPN and client authentication with digital certificates, and require periodical re-authentication.

2.2.9 Impersonation or masquerade

The intruder manipulates the TCP/IP packet to alter the IP address and pretend it comes from another network. *Spoofing* is a technique used for impersonation.

2.2.9.1 Spoofing

Spoofing means to capture, alter, and retransmit a communication stream in a way that misleads the recipient. As used by hackers, this refers especially to altering TCP/IP packet source addresses or other packet-header data to masquerade as a trusted machine. This term has become very widespread and is borderline techspeak.

2.2.9.2 The danger of spoofing

Every system that trusts the remote system based on its IP address, for example a packet filter, can be tricked by spoofing. Any system that *only* looks at the IP address is unsafe, unless other systems, such as the secure gateways we describe later in this book, prevents spoofing.

One of the greatest dangers with spoofing is the difficulty to find the real source since the address of the offending packets is not the address of the attacker. To find the source, you must trace the entire path, step by step. Very crude DoS attacks are possible that merely send large amounts of nonsense data to the victim’s system or network. The only reason such attacks are not more common is that they require as much bandwidth from the attacker as the target has (and bandwidth is expensive). To work around this problem, malicious crackers install flooding agents on third-party systems and steal bandwidth from the third-party to attack their targets. For this reason, it is very important to protect all your systems and your data and to avoid being used to attack others.

2.2.9.3 Fighting spoofing

To protect your network from spoofing, you should configure packet filters on your secure gateway to the Internet. The basic principles are:

- Deny *all* inbound traffic on the secure gateway’s public interface with an IP address of the internal network or IP addresses reserved for private networks as specified in *Address Allocation for Private Internets*, RFC 1918.
- Permit *only* internal network IP addresses in the inbound traffic on the secure gateway’s private interface. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, RFC2827, recommends that you allow only addresses from the internal network in the

inbound traffic on the internal interface of a gateway. This technique does not protect against DoS attacks, which originate from valid internal networks IP addresses. This filtering prevents attackers within the originating network from launching a DoS attack using forged source addresses that do not conform to Ingress filtering rules. An additional benefit of implementing this type of filtering is that it enables the originator to be easily traced since the attacker must use a legitimately reachable source IP address to launch the attack.

2.3 Network security technologies

This section provides a summary of the technologies you can use in any combination to implement your network security policies. It is not meant to be a comprehensive list. For more information, refer to the IBM white paper *AS/400 and Network Security Directions*, which is located on the Web at:

`http://www-1.ibm.com/servers/eserver/iseries/software/firewall/pdf/fw_whitepaper.pdf`

The book *Building Internet Firewalls*, by Chapman and Zwicky, also provides helpful information.

The network security technologies can be grouped in two general levels: application and network.

Network-level technologies are:

- IP packet filtering
- Network address translation (NAT)
- IPSec

Application level technologies are:

- Proxy servers
- SOCKS servers
- SSL and Transport Layer Security (TLS)
- Domain Name Servers
- Mail relays

2.3.1 IP packet filters

An IP packet filter discards denied traffic. Permitted traffic is not affected in any way. A packet filter can only discard traffic that is sent to it. Therefore, the device with the packet filter must either do IP routing or be the destination for the traffic.

A packet filter has a set of rules with actions. Every packet is compared against the filter rules, from top to bottom. At the first match, the action in the matching filter rule (permit or deny) is taken. Most packet filters have an implicit *deny all* rule at the bottom of the file. Most packet filters permit or deny packets based on:

- Source and destination IP addresses
- Protocol, such as TCP, UDP, or ICMP
- Source and destination ports and ICMP types and codes
- Flags in the TCP header, such as whether the packet is a connect request
- Direction (inbound or outbound)
- Which physical interface the packet is traversing

All packet filters have a common problem: The trust is based on IP addresses. As explained in 2.2.1, “Internet Protocol (IP) security characteristics” on page 23, this is not sufficient for providing good security, but it is a good complement.

Most IP packet filters are *stateless*, which means they don’t remember anything about packets they previously processed. A *stateful* packet filter can keep some information about previous traffic, which gives you the ability to configure that only replies to requests from the internal network are allowed from the Internet. Stateless packet filters are vulnerable to spoofing since the source IP address and ACK bit in the packet’s header can be easily forged by attackers.

2.3.2 Network address translation (NAT)

NAT translates internal or private IP addresses to public or globally routable IP addresses. It can also translate ports. Some advantages of NAT are:

- It saves public IP addresses. Because a client only needs a public IP address when it is communicating with the Internet, the pool of globally routable IP addresses can be shared with other clients. Therefore, you need fewer public IP addresses than the actual number of internal clients that need access to the public network if you use NAT. Most routers, firewalls, and other network address translators allow you to use the IP address assigned to their public interface as the globally routable IP address to which internal IP addresses are translated. This feature and the ability to translate both the IP address and port (NAT port mapping) make it possible, in many NAT implementations, to require only one public IP address.
- It hides the internal network’s IP addresses.
- It simplifies routing. Since internal hosts are assigned IP addresses from the internal network, other internal systems can access them without special routes or routers. The same hosts are accessed from the public network using globally routable IP addresses translated by NAT.
- It is transparent to the clients and, therefore, allows you to support a wider range of clients.
- It supports a wide range of services with a few exceptions. Any application that carries (and uses) the IP address inside the application does not work through NAT.
- It consumes fewer computing resources and is more efficient than SOCKS and proxy servers.

Some disadvantages of NAT are:

- NAT provides minimum logging services.
- IP forwarding must be enabled.
- NAT is not as adept as either the SOCKS or proxy servers in detecting attacks.
- It breaks certain applications (or as in the case of FTP, makes them more difficult to run).

NAT is described in *The IP Network Address Translator (NAT)*, RFC 1631, which is available on the Web at: `http://ietf.org/rfc/rfc1631.txt`

2.3.3 Virtual private network (VPN) and IPSec

Initially, companies used the Internet chiefly to promote their images, products, and services by providing World Wide Web access to corporate Web sites. Today, however, the focus has shifted to e-business. Companies are leveraging the global reach of the Internet (due to its ease and inexpensive access) to cost-effectively extend their private networks. By using the Internet for intra-company and inter-company communications, you save on communication costs and on outsourcing the management and operation of the network to an Internet Service Provider (ISP).

In this environment, security becomes a prime concern. The Internet makes the connection relatively inexpensive, but VPN makes it more secure.

VPN is an extension of a company's private intranet across a public network infrastructure such as the Internet. It is based on creating *virtual* secure tunnels between hosts connected to the public network. To participate in a secure tunnel or VPN connection, the VPN partners or tunnel endpoints must implement a compatible suite of VPN protocols.

2.3.3.1 VPN and IPSec

VPN implementations differ from vendor to vendor. But in the last year, the IP Security architecture (IPSec) has become the industry standard upon which most new VPN implementations are based. The IPSec protocols are aimed to provide the following Internet security functions:

- **Data origin authentication**: Verifies that each datagram was originated by the claimed sender.
- **Data integrity**: Verifies that the contents of a datagram were not changed in transit, either deliberately or due to random errors.
- **Data confidentiality**: Conceals the clear text of a message by using encryption.
- **Replay protection**: Ensures that an attacker cannot intercept a datagram (containing, for example, an encrypted user ID and password) and play it back at some other time.
- **Key management**: Ensures that your VPN policy can be implemented throughout the extended network with little or no manual configuration.

The IPSec protocols are:

- **Authentication Header (AH)**: Provides data origin authentication data integrity and replay protection.
- **Encapsulating Security Payload (ESP)**: Provides data confidentiality, data origin authentication, data integrity, and replay protection.
- **Internet Key Exchange (IKE)**: Provides a method for automatic key management. Authentication, encryption, and integrity algorithms heavily depend on secret keys that the VPN partners share. IKE provides the support needed by AH and ESP to generate and refresh the secret keys.

2.3.4 Proxy server

Application proxies connect a client to a target server. The client sends requests to the proxy. The proxy forwards or "proxies" the request to the server. The server sends the reply to the proxy, which, in turn, sends the reply back to the originating client. Because a proxy server is application specific, it has a good understanding of the protocol. Some characteristics of a proxy server are:

- Breaks the TCP/IP connection between a client and server; IP forwarding is not required
- Hides the internal client IP addresses; only the public IP address of the proxy server is visible from the external network
- Logs access with a great detail of information
- Authenticates users
- Caches information

The most common type of proxy is the HTTP proxy. Most HTTP proxies also handle Secure HTTP (HTTPS) and file transfer protocol (FTP). The SMTP mail relay is also an application proxy.

The main drawback of proxy servers is that they must support the application for which they are performing the proxy function. Many TCP/IP applications are not supported by proxy servers.

2.3.5 SOCKS server

A SOCKS server is another TCP/IP application that resends requests and responses between clients and servers. The SOCKS server is like a multi-talented proxy. Instead of just handling one type of application protocol, it handles them all (HTTP, Telnet, FTP, and so on). The purpose of the SOCKS server is the same as a proxy; it breaks the TCP/IP connection and hides internal network information. However, to use a SOCKS server the client must be SOCKS-enabled. That is, it must support the SOCKS protocol. Some applications (such as popular Web browsers) support SOCKS. There are products, such as Hummingbird SOCKS, that SOCKSify the Microsoft TCP/IP stack on a Windows NT or Windows 95 or 98 operating systems.

There are also some systems (such as OS/400) that support a SOCKS client in their TCP/IP protocol stack (versatile clients) so that all client applications can use a SOCKS server. The client configuration gives the name of the SOCKS server to use and rules for when it should be used.

Socks servers have no knowledge of the application protocol that they are using. They don't distinguish Telnet from HTTP. As a result, they can be written in a more efficient manner than a proxy. The downside is that they can't do things like caching or log URLs that are accessed.

2.3.6 Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

The objective of the TLS protocol and its predecessor SSL is to provide privacy over the Internet. TCP/IP client and server applications that are SSL-enabled can communicate in a way designed to prevent eavesdropping, tampering, or message forgery. These protocols provide, encryption, integrity, and authentication. SSL was originally developed by Netscape. TLS is based on SSL V3.0 and is published in *The TLS Protocol Version 1.0*, RFC 2246.

TLS is an evolutionary upgrade of the SSL Version 3.0 protocol. TLS Version 1 and SSL Version 3 share the same basic record construction and line flows. TLS provides the same function as SSL and is compatible with SSL. But it includes some new features and clarifications of protocol flows for areas that are ill-defined by the SSL protocol definition. The major goal of TLS was to standardize the SSL definition and implementations, to make the SSL protocol more secure, and to make the specification of the protocol more concise and complete.

The SSL/TLS protocol consists of two separate protocols: the record protocol and the handshake protocol. The *handshake protocol* is encapsulated within the *record protocol*. The SSL handshake is used to establish an SSL session on the TCP/IP connection between a client and a server application. The SSL handshake usually occurs immediately after the TCP connection is established. During the handshake, the client and server agree on the encryption algorithms and the encryption keys that they use for that session. In all SSL handshakes, the client authenticates and verifies the identity of the server. The server can optionally authenticate and verify the identity of the client. After the SSL handshake has successfully completed, information exchanged between the client and server is encrypted using the negotiated keys. An important advantage of SSL is its ability to negotiate unique encryption keys for each SSL session between a client and a server even if they have not previously communicated with each other.

During the SSL handshake, the server sends a digital certificate to the client. If client authentication is used, the server requires the client to also send a client certificate. Digital certificates provide identifying information that enable the client and server to identify each other. Digital certificates are issued by trusted third-parties called *certificate authorities*. An SSL client must trust the certificate authority that issued the server's certificate in order for the SSL handshake to complete successfully.

2.3.7 Domain Name Server (DNS)

A Domain Name Server is another technology that is often employed when building a secure network. You may recognize Domain Name Services as the application that enables client to determine the IP address associated with host name. For example, a DNS server can translate a host name such as www.as400.ibm.com to 208.222.150.11.

Because it is User Datagram Protocol (UDP)-based, DNS replies are relatively easy to fake. Another problem with DNS is that it could be used by an attacker on the Internet to find out the internal clients names and IP addresses in your organization. Domain name trees typically reflect the organizational structure of a company. All this information should be regarded as confidential. Access to the domain name records for the secure network is of great assistance to crackers, since it gives them a list of hosts to attack.

To limit the exposure when connecting to a public network, such as the Internet, configure two name servers in a configuration known as *split DNS*. This technique uses two Domain Name Servers: the internal DNS for secure and *private* host names, and the external one for *public* names. The external DNS is the only one visible from the Internet. Only some hosts need to be known by Internet systems: the e-mail relay, the public WWW server or servers, the external name server itself, and any other public server in the demilitarized zone (DMZ).

The internal name server forwards queries to resolve Internet host names to the external DNS server. You only need a public DNS server to advertise your public servers. If you don't have public servers or you only need to advertise a mail exchanger, you may consider using the ISP as the primary public DNS and mail exchanger for your company.

In summary, the objectives of the split DNS function are to:

- Provide access to non-secure network domain name and address resolution for users in the secure network.
- Hide the secure network names and addresses from users outside the secure network.
- Provide name and addresses resolution for resources that you want to reveal (usually servers and gateways in the DMZ).

The standard DNS configuration for a private network connected to the Internet assumes at least three Domain Name Servers:

- The internal or private DNS server located in the secure network
- The external or public DNS server located on the DMZ
- The Internet DNS server located at the ISP or directly on the Internet root servers

The Domain Name System protocol is described in the following RFCs:

- *Domain Names - Concepts and Facilities*, RFC 1034 :
  `http://www.rfc-editor.org/rfc/rfc1034.txt`
- *Domain Names - Implementation and Specification*, RFC 1035:
  `http://www.rfc-editor.org/rfc/rfc1035.txt`

For more information, refer to *DNS and BIND* by Paul Albitz and Cricket Liu.

2.3.8 Comparing network security functions

Table 2 summarizes the characteristics of some of the security solutions mentioned before and compares them to each other. This should help anyone who needs to devise a security strategy to determine what combination of solutions would achieve a desired level of protection.

Table 2. Security solution implementations: Comparison

	Access control	**Encryption**	**Authentication**	**Integrity checking**	**Address concealment**
IP filtering	Y	N	N	N	N
NAT	Y	N	N	N	Y
IPSec	Y	Y (packet)	Y (packet)	Y (packet)	Y
SOCKS	Y	N	Y (client/user)	N	Y
SSL	Y	Y (data)	Y (system/user)	Y	N
Application proxy	Y	Normally no	Y (user)	Y	Y

2.4 Monitoring: Auditing and logging

The ability to constantly prove that your security strategy is working and your security policies are not being violated is as important as the initial setup. Most security products provide some form of logging or auditing of security events.

Monitoring and early detection of DoS attacks and other intrusions is also very important.

Most security devices, including OS/400, provide a wide range of tools and functions for auditing and logging. There are also products on the market that integrate DoS attack analysis, monitoring, and intrusion detection by automatically collecting and analyzing the output from other network devices.

For example, Tivoli Risk Manager is a centralized risk management solution that enables organizations to centrally manage attacks, threats, and exposures by correlating security information from firewalls, intrusion detectors, vulnerability scanning tools, and other security checkpoints. For more information about this product, visit: `http://www.tivoli.com/products/index/secureway_risk_mgr/`

Note: Some consulting companies and ISPs also provide intrusion detection services.

2.5 Universal Connection security

In light of all the security issues that have been discussed so far, the Universal Connection has also implemented many security features to make sure its connection is as secure as possible. These include authentication, encryption, and IP packet filtering. VPN security and PPP dial-up security implementations are further described in Chapter 3, “Point-to-Point Protocol (PPP) connection examples” on page 37, and in Chapter 4, “Direct connection examples” on page 107.

Chapter 3. Point-to-Point Protocol (PPP) connection examples

This chapter explains how to configure the dial-up and dedicated PPP connections on the iSeries server using the Universal Connection Wizard (UVC). Three separate types of dial-up and dedicated PPP scenarios are discussed:

- PPP dial-up to AT&T Global Network Services (AGNS)
- PPP dial-up to any ISP
- PPP dedicated FT1/T1

3.1 Universal Connection Wizard

Currently the iSeries server contains a number of customer-to-IBM applications that use different connection mechanisms to provide an electronic exchange of system and customer information between the customer and IBM. Universal Connection Wizard provides a means for consolidating the connection methods for ECS, PM/400e, service agent, and Management Central inventory. All of the applications will move toward using a TCP/IP connection that will be configured through UVC.

The first application enabled for UVC was Electronic Customer Support (ECS). With the release of V4R5, the PTFs to enable this became available on 17 November 2000. The following commands can be used:

- Send PTF Order (SNDPTFORD)
- Send Service Request (SNDSRVRQS)
- Query Problem Status (QRYPRBSTS)
- Order Supported PTFs (ORDSPTPTF)

In addition, if automatic problem reporting has been enabled by using the RPTPRBAUTO parameter of the Change Services Attribute (CHGSRVA) command, and a Report value of *IBMSRV is specified, notification of any problems will be enabled over this Universal Connection.

As mentioned earlier, there are three dial-up or dedicated PPP scenarios that can be configured using the Universal Connection Wizard. These are listed and summarized here:

- **PPP dial-up to AGNS**

  The dial-up to the AGNS connection was the first to be introduced and was available starting with the release of V4R5 of OS/400. It provides a private link to the IBM Service system using an AT&T network as its mode of transport. It uses both the internal 56 Kbps modem (9771 adapter card) that was first shipped with new V4R5M0 systems and standard external modems, such as the 7852-400.

- **PPP dial-up to any ISP**

  The dial-up to an ISP connection is only available for release V5R1M0 and later of OS/400. It allows a connection to IBM Electronic Support systems using an ISP of your choice. First, the iSeries server is connected to the ISP, and a VPN tunnel is created over the Internet that then connects to the IBM service system. Both the internal 56 Kbps and external modems can be used for this connection. In the Universal Connection Wizard, you are asked to specify an existing dial-up PPP connection profile name.

- **PPP dedicated FT1/T1**

  The leased line PPP connection profile must be connected to the Internet through your ISP. Your ISP needs to support the VPN-encrypted connection to route the traffic to IBM Electronic Support. In the Universal Connection Wizard, you are asked to specify an existing leased PPP connection profile name.

> **Note**
>
> The SDLC QESLINE description can still be used as a backup in the event that a connection using the UVC cannot be established. Howeverm, this cannot be done over the 2771 internal modem only with external modems such as the 7852-400.
>
> If this is desired, ensure that the QESLINE description specifies a valid resource name. This can be done by using the Display Line Description (DSPLIND) command. If the Universal Connection fails, the system attempts to use the QESLINE description. In addition, the SNA information must be correct since it was used prior to the internal modem, such as CALL QESPHONE, etc.

3.2 PPP dial-up to AGNS

Universal Connection is a consolidation of multiple IBM connection mechanisms into a common TCP/IP based mechanism. One of these mechanisms uses the PPP protocol to make a connection to IBM. This connection is made across AGNS, which provides a secure connection between the customer and IBM by implementing authentication and encryption when making a connection. AGNS then assigns an IP address to the customer's PPP client. Figure 14 shows a diagram of the connection to IBM.

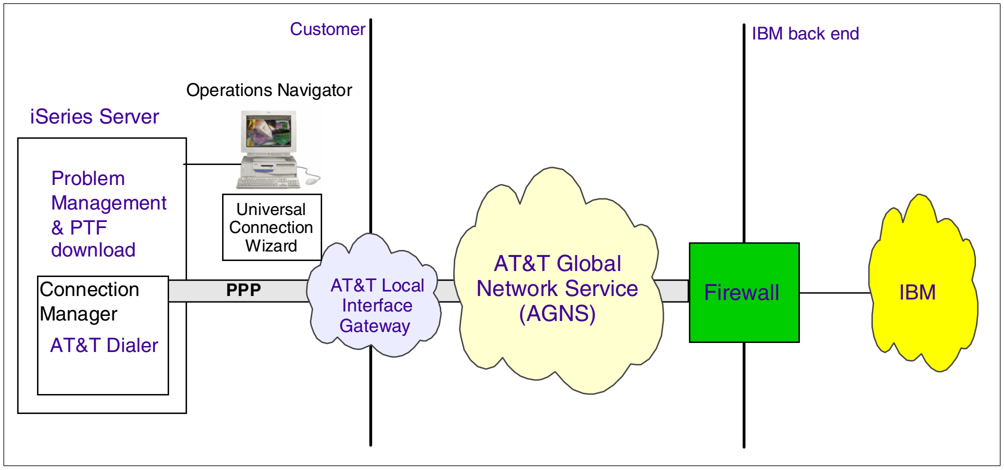

Customer
IBM back end
Operations Navigator
iSeries Server
Problem Management & PTF download
Universal Connection Wizard
Connection Manager
AT&T Dialer
PPP
AT&T Local Interface Gateway
AT&T Global Network Service (AGNS)
Firewall
IBM

Figure 14. ECS using PPP connection to IBM

3.2.1 Prerequisites

The prerequisites for enabling ECS over an AGNS connection include:

- At V4R5M0 of OS/400, SF64122 and SF64124 for product 5769SS1 need to be installed. You must also install SF64123, which is also included under the umbrella SF64124 PTF allows for remote support by IBM support personnel. These are all non-IPL PTFs. V5R1M0 of OS/400 includes all these functions as part of the base code.

- You must install TCP/IP Connectivity Utilities (5769-TC1).
- Client Access Express V4R5M0 with Service Pack SF64217 (or later) or Client Access Express V5R1M0 with Service Pack SI01037 is required to obtain the wizard.
- Ensure the QRETSVRSEC system value is set to `1`. This can be done by issuing the Display System Value (DSPSYSVAL) command. If it is not set to "1", run the Change System Value (CHGSYSVAL) command.
- If the user is using an internal modem such as the 56 Kbps provided with the 9771 adapter card, ensure that network attribute MDMCNTRYID is set appropriately. The Display Network Attributes (DSPNETA) command display the current value. The Change Network Attributes (CHGNETA) command allows changes to be made.
- TCP/IP needs to be active. You can start it with the Start TCP/IP (STRTCP) command.
- The user configuring the wizard requires *ALLOBJ and *IOSYSCFG authority as part of their iSeries server user profile.

3.2.2 Planning worksheet for PPP dial-up to AGNS

Complete the iSeries server planning worksheet as shown in Table 3. It allows you to gather the necessary information to implement the AGNS connection.

Table 3. PPP AGNS connection information

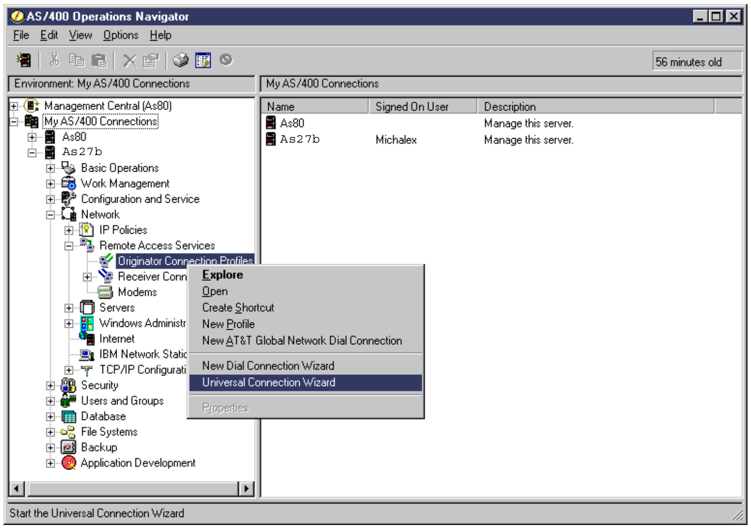
Possible wizard questions	Example answers
Service information: - Company - Contact name - Phone number - Alternate phone number - Fax number	 IBM Mike Alexander 111-111-1111 222-222-2222 333-333-3333
Company address: - Street address - City/state - Country - ZIP code - National language version - Media for PTFs	 Hwy 52 and 37th St NW Rochester/Minnesota United States 55901 English (2924) Automatic Selection
Location: - Country - State or province	 United States Minnesota
Country (if not located in list): - Country code - Country name - State or province code - State or province name - Hemisphere	Only if needed
Application selection	Electronic Customer Support

Possible wizard questions	Example answers
Connection type	A dial-up connection using AT&T Global Network Services
Hardware resource	CMN08
Choose line	QESPPLIN (or other line description)
Modem type (if external modem is used)	IBM 7852-400

3.2.3 Configuring a PPP connection using AGNS

The Universal Connection Wizard is configured through Operations Navigator, which is a component that is shipped with Client Access Express. Complete the following steps to configure a PPP connection to AGNS:

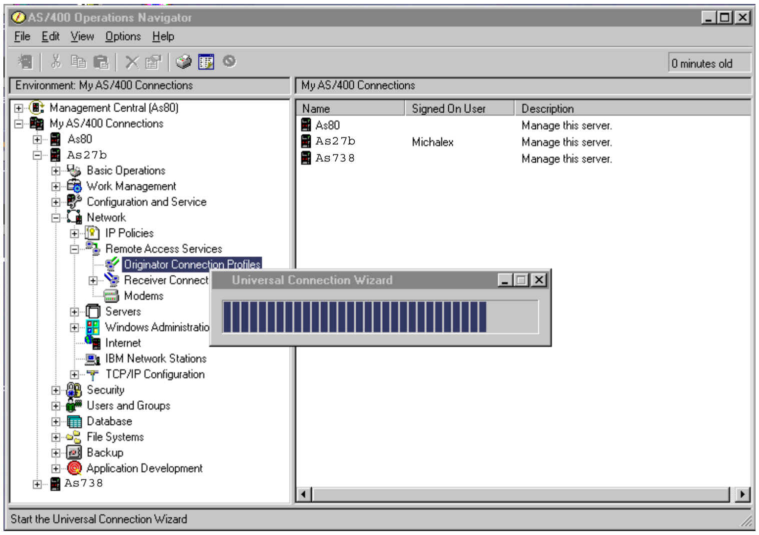
1. Start Operations Navigator.
2. Expand the iSeries server under **My AS400 connections**, in our example AS27B. Sign on with a valid iSeries user ID and password if prompted.
3. Expand the **Network** component.
4. Expand **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. From the pull-down menu, choose **Universal Connection Wizard** as shown in Figure 15.



Name	Signed On User	Description
As80		Manage this server.
As27b	Michalex	Manage this server.

Figure 15. Universal Connection Wizard selection

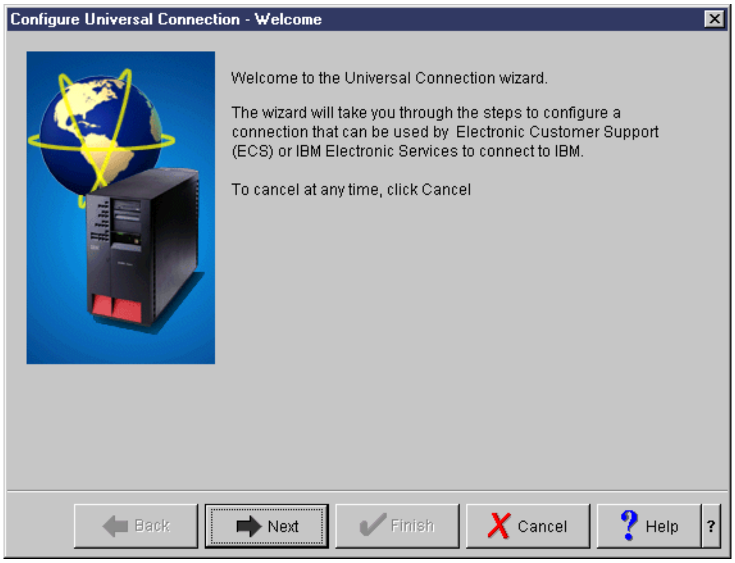
A progress bar appears as shown in Figure 16. This indicates that the application is in processing mode. This feature was implemented to facilitate the continuity of the configuration process, while allowing the Java code to load the wizard.



Name	Signed On User	Description
As80		Manage this server.
As27b	Michalex	Manage this server.
As738		Manage this server.

Figure 16. Progress bar showing that the wizard is being loaded

6. The Welcome display for the wizard appears first as shown in Figure 17. It is available in English only for V4R5M0 of Client Access Express. It is translated to other languages in V5R1M0. Help text is available for all fields.



Welcome to the Universal Connection wizard.

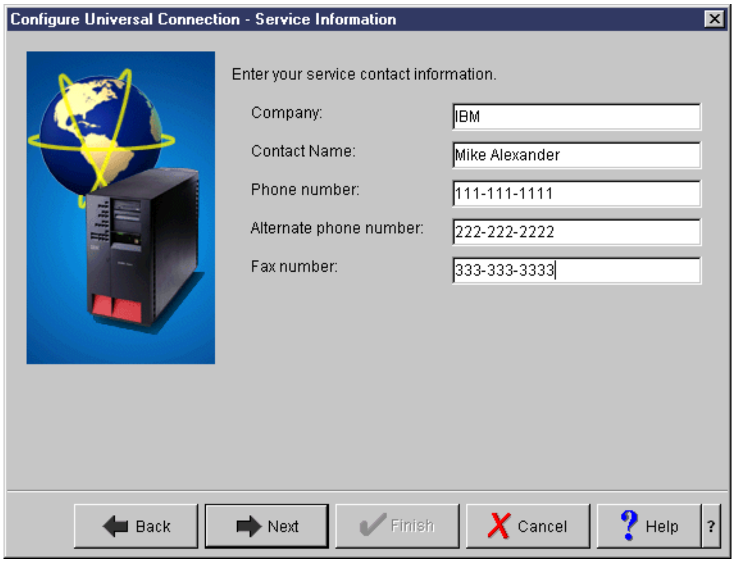
The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 17. Welcome display

Click **Next** to continue.

7. The Service Information display shown in Figure 18 allows you to enter service contact information.



Configure Universal Connection - Service Information

Enter your service contact information.

Company: IBM

Contact Name: Mike Alexander

Phone number: 111-111-1111

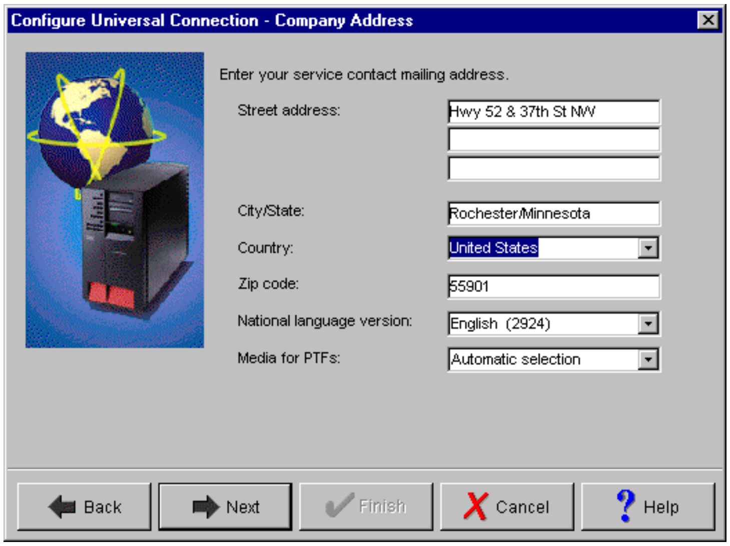
Alternate phone number: 222-222-2222

Fax number: 333-333-3333

Figure 18. Service contact information

You are required to complete the first three fields. This display updates the same information as the Work with contact information (WRKCNTINF) option 2 on a 5250 emulation screen. If that information was entered on the system, these parameters are pre-filled. Click **Next** to continue.

8. On the next display (Figure 19), enter the address where the iSeries server machine service contact is located. There are pull-down options for Country, National language version, and Media for PTFs. The Media for PTFs field allows you to choose *Automatic selection* or *CD-ROM*. Click **Next** to continue.



Configure Universal Connection - Company Address

Enter your service contact mailing address.

Street address: Hwy 52 & 37th St NW

City/State: Rochester/Minnesota

Country: United States

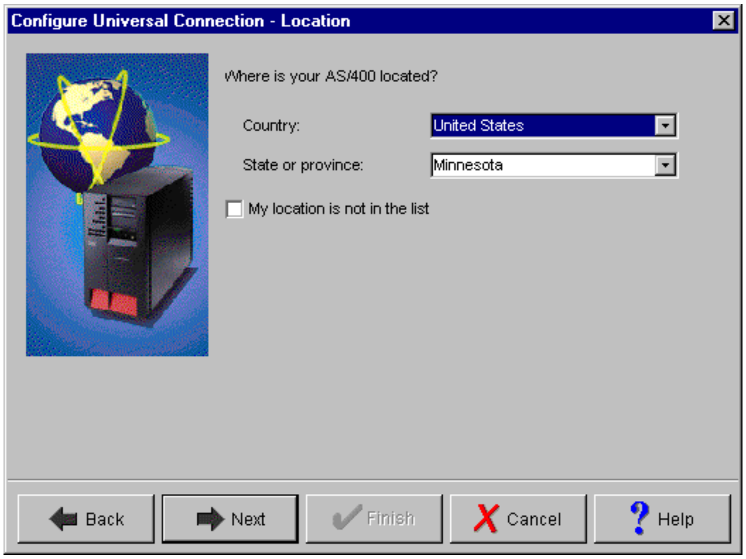
Zip code: 55901

National language version: English (2924)

Media for PTFs: Automatic selection

Figure 19. Company address

9. On the Location display shown in Figure 20, select the country and state or province. The My location is not in the list check box is only selected if a country is not listed. Click **Next** to continue.



Configure Universal Connection - Location

Where is your AS/400 located?

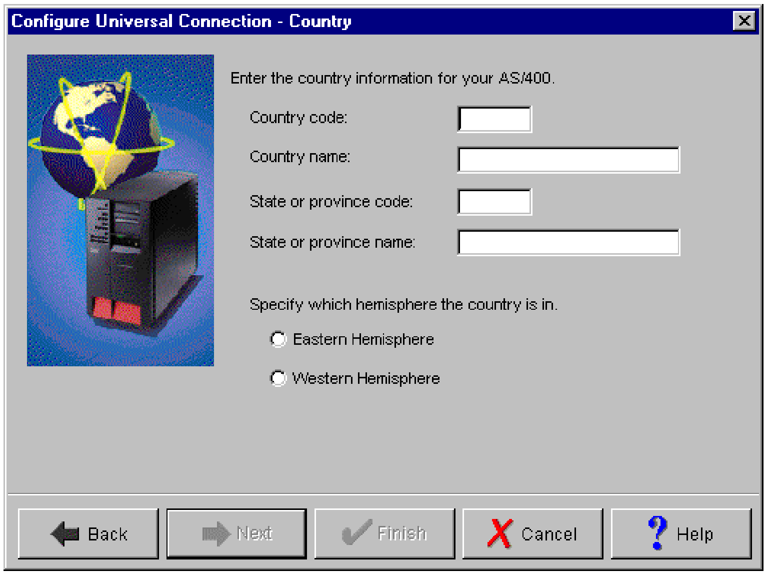
Country: United States

State or province: Minnesota

□ My location is not in the list

Figure 20. Location information

The display in Figure 21 appears if the My location is not in the list check box is selected. The hemisphere specification is used to look up default nodes for the application. Click **Next** to move on to the next display.



Configure Universal Connection - Country

Enter the country information for your AS/400.

Country code:

Country name:

State or province code:

State or province name:

Specify which hemisphere the country is in.

○ Eastern Hemisphere

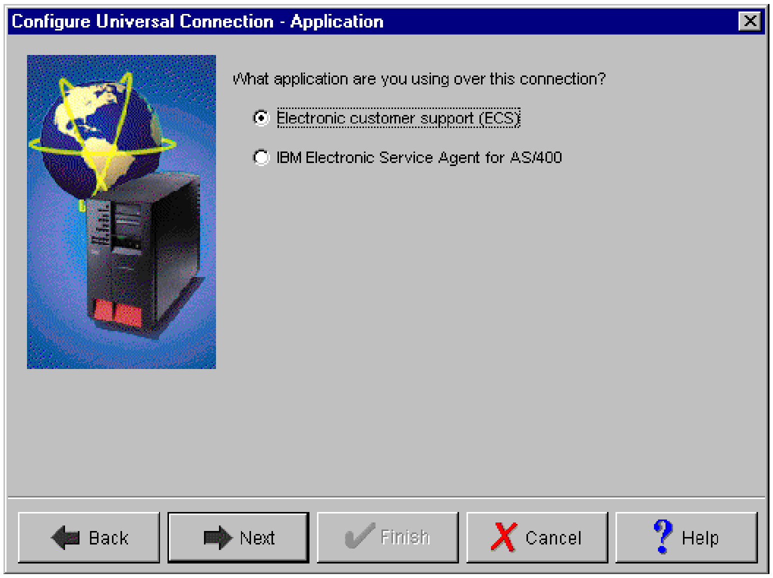
○ Western Hemisphere

Figure 21. Country information

10.On the Application selection display that appears next (Figure 22), you see two applications listed: ECS and Electronic Service Agent. ECS is part of OS/400. Electronic Service Agent requires product 5798RZG. If the 5798RZG product is installed, you can select the **Electronic Service Agent** radio button. For more information on Electronic Service Agent, see:

`http://publib.boulder.ibm.com/as400_sd/sdsadoc.html`

Click **Next** to continue.



Configure Universal Connection - Application

What application are you using over this connection?

● Electronic customer support (ECS)

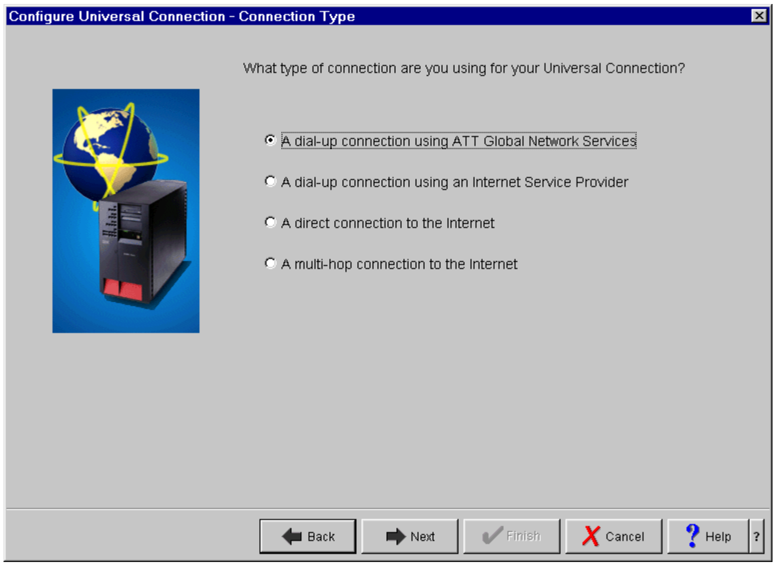
○ IBM Electronic Service Agent for AS/400

Figure 22. Application selection

11.The next display (Figure 23) prompts for the connection type. There are four options:

- A dial-up connection using AT&T Global Network Services
- A dial-up connection using an Internet Service Provider
- A direct connection to the Internet
- A multi-hop connection to the Internet

Choose the **Dial-up connection using AT&T Global Network Services** option, and click **Next** to continue.



Configure Universal Connection - Connection Type

What type of connection are you using for your Universal Connection?

● A dial-up connection using ATT Global Network Services

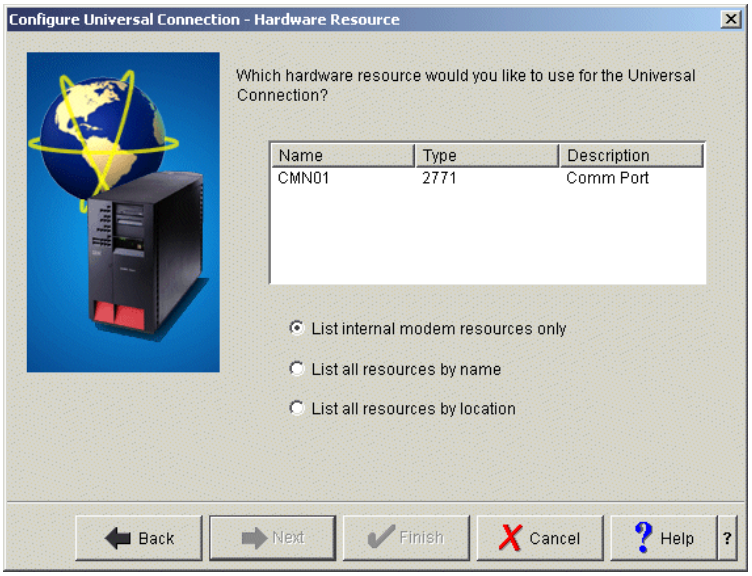
○ A dial-up connection using an Internet Service Provider

○ A direct connection to the Internet

○ A multi-hop connection to the Internet

Figure 23. Connection Type

12.The next display (Figure 24) allows you to select a hardware resource. You can choose from one of three radio buttons that offer different resource views. Select the resource that is used for the AGNS connection. You can select either a resource with an internal modem or one that has an external modem attached. Click **Next** to continue.



Configure Universal Connection - Hardware Resource

Which hardware resource would you like to use for the Universal Connection?

Name	Type	Description
CMN01	2771	Comm Port

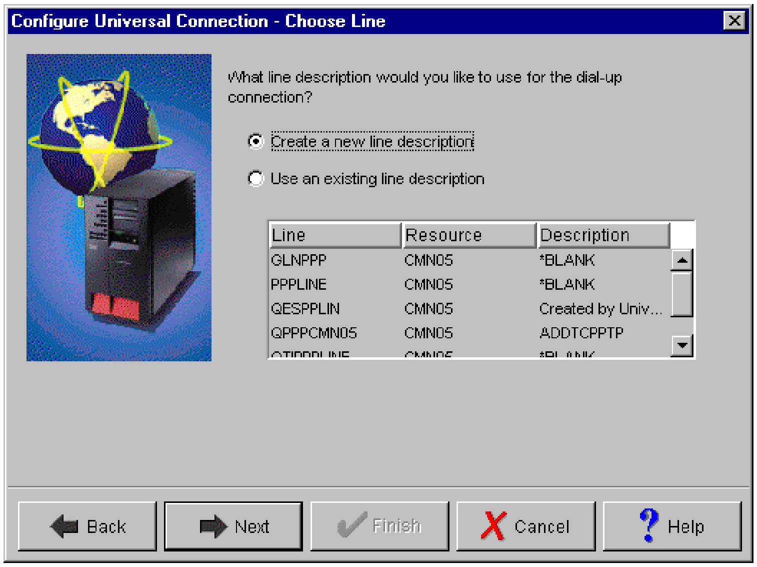
● List internal modem resources only

○ List all resources by name

○ List all resources by location

Figure 24. Hardware resource selection

13.After you select a resource, you must provide a line description as shown in the display in Figure 25. If multiple PPP lines exist for the resource that was selected, you can choose between using an existing line or creating a new one. If only one line exists for the selected resource, that line is used. Then you can choose to select an option or to create a line description.



Configure Universal Connection - Choose Line

What line description would you like to use for the dial-up connection?

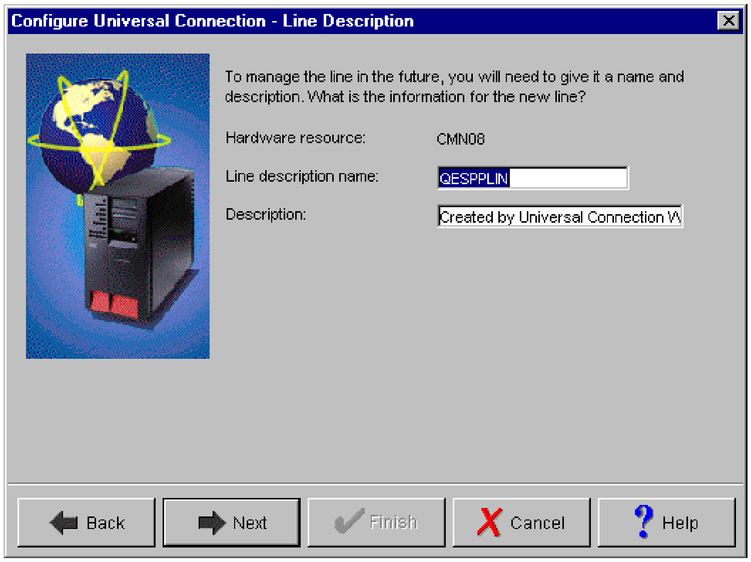
● Create a new line description

○ Use an existing line description

Line	Resource	Description
GLNPPP	CMN05	*BLANK
PPPLINE	CMN05	*BLANK
QESPPLIN	CMN05	Created by Univ...
QPPPCMN05	CMN05	ADDTCPPTP

Figure 25. Line description selection

If no line descriptions exist for the resource selected, the display shown in Figure 26 appears. It prompts you to create a new line. The default line name is QESPPLIN. You can use a different name if you prefer. Click **Next** to continue.



Configure Universal Connection - Line Description

To manage the line in the future, you will need to give it a name and description. What is the information for the new line?

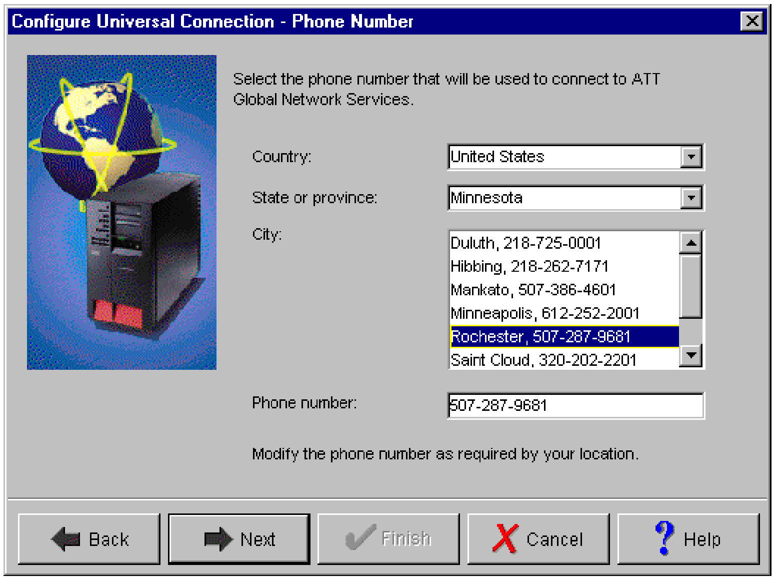
Hardware resource: CMN08

Line description name: QESPPLIN

Description: Created by Universal Connection W

Figure 26. Creating a line description

14.On the next display (Figure 27), you select the primary phone number that is used for the connection to IBM. The country and state or province fields are pre-filled with the values that were specified earlier. If the fields are not correct, change them to what they should be. If there are special dial prefixes that must be used, enter these at this time as suggested by the instructions at the bottom of the display.



Configure Universal Connection - Phone Number

Select the phone number that will be used to connect to ATT Global Network Services.

Country: United States

State or province: Minnesota

City:
Duluth, 218-725-0001
Hibbing, 218-262-7171
Mankato, 507-386-4601
Minneapolis, 612-252-2001
Rochester, 507-287-9681
Saint Cloud, 320-202-2201

Phone number: 507-287-9681

Modify the phone number as required by your location.

Figure 27. Phone number selection

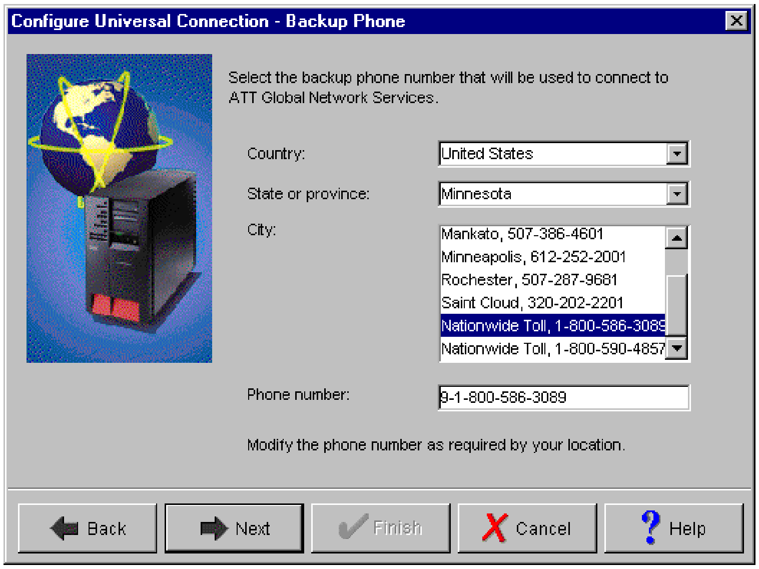
15.Every 30 days (or whenever Universal Connection is used after that 30-day period), an updated AT&T telephone list is downloaded by the system. This ensures that the telephone numbers available for Universal Connection remain current.

When this download occurs, a message is posted to the system operator's message queue. To view these messages, display the QSYSOPR message queue (use the `DSPMSG QSYSOPR` command)

If the Universal Connection Profile being used contains a telephone number that is no longer in the current AT&T telephone list, a diagnostic message is issued. The purpose of this message is to notify you to re-run the wizard to update the telephone numbers. When you re-run the wizard, updated telephone numbers become available for you to choose. To view the very latest telephone numbers, visit the AT&T Web site at:

`http://www.attbusiness.net`

16. The Backup Phone number display (Figure 28) prompts you to select a backup phone number for contacting IBM. It is important to do this to ensure that you are connected. You may select 800 numbers, but if at all possible, do not use them for the primary number. Click **Next** to continue.



Configure Universal Connection - Backup Phone

Select the backup phone number that will be used to connect to ATT Global Network Services.

Country: United States

State or province: Minnesota

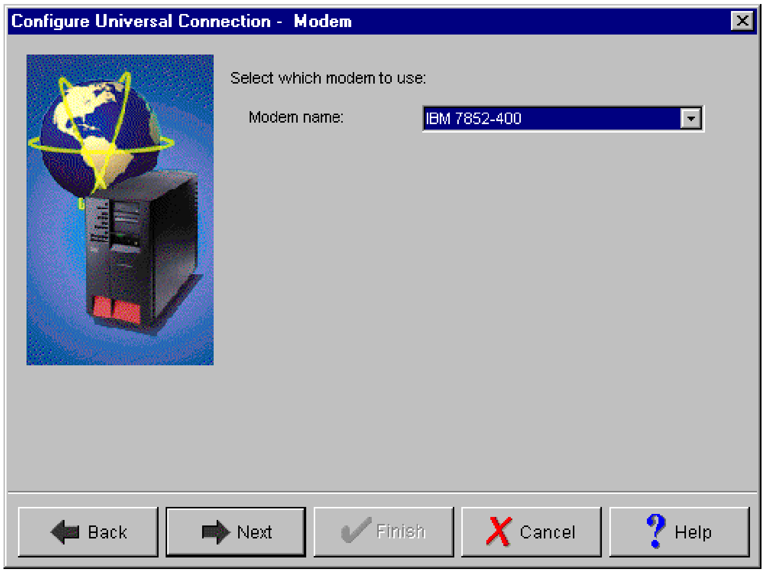
City:
Mankato, 507-386-4601
Minneapolis, 612-252-2001
Rochester, 507-287-9681
Saint Cloud, 320-202-2201
Nationwide Toll, 1-800-586-3089
Nationwide Toll, 1-800-590-4857

Phone number: 9-1-800-586-3089

Modify the phone number as required by your location.

Figure 28. Backup phone number

17. On the display shown in Figure 29, you are prompted for a modem name if the resource selected does not contain an internal modem. There is a pull-down menu for the modem selection. If the desired modem is not listed, you may create a new modem definition. You can do this through Operations Navigator by right-clicking the modem folder that is listed under Remote Access Services. If 7852-400 is selected, the line is created with the Set modem to ASYNC command parameter set to END. This causes a modem that is set to *synchronous* mode to switch to *asynchronous* when it is activated by the PPP line description.



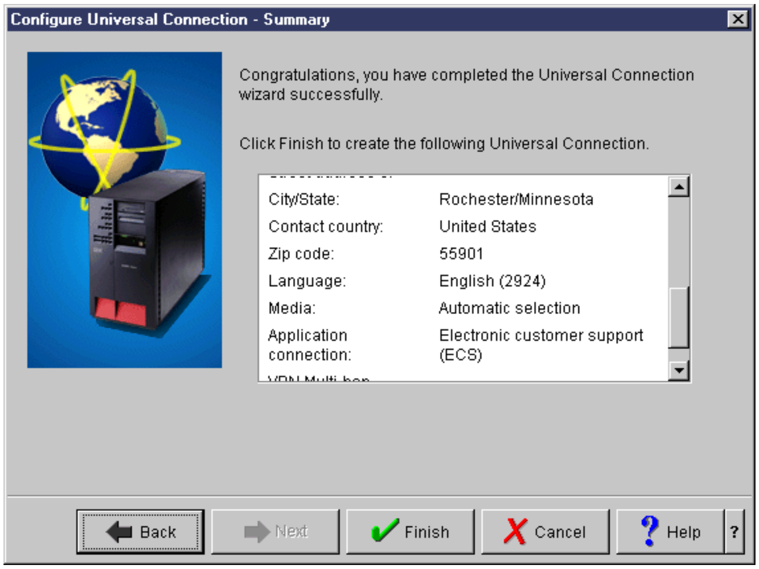
Configure Universal Connection - Modem

Select which modem to use:

Modem name: IBM 7852-400

Figure 29. Modem selection

18. After you complete all of the displays for the configuration, a summary display appears (Figure 30). The panel lists the choices that you've made. Click **Finish**. The contact information is updated, and the PPP profile and associated PPP line are created.



Configure Universal Connection - Summary

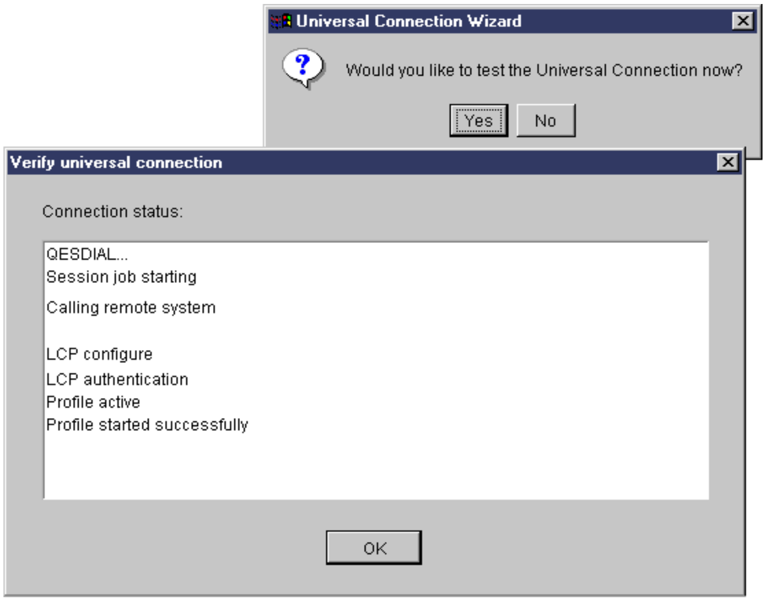
Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

City/State:	Rochester/Minnesota
Contact country:	United States
Zip code:	55901
Language:	English (2924)
Media:	Automatic selection
Application connection:	Electronic customer support (ECS)

Figure 30. Summary of selections

19. After you click Finish, the pop-up window shown in Figure 31 appears. It asks whether you want to test the Universal Connection now. Selecting Yes causes Universal Connection to start the PPP profile for testing purposes. No information is exchanged. Then, a connection status window appears showing whether it was successful.


Universal Connection Wizard

Would you like to test the Universal Connection now?

Verify universal connection

Connection status:

```
QESDIAL...
Session job starting
Calling remote system

LCP configure
LCP authentication
Profile active
Profile started successfully
```

Figure 31. Verifying Universal Connection

3.2.4 Objects created by the wizard for AGNS connections

This section gives a brief description of the objects that are created by the Universal Connection Wizard for the AGNS connection. Table 4 outlines these objects and provides some details about their use.

Table 4. List and description of AGNS created objects

Objects created by wizard	Object details
QESDIAL	PPP profile - Connection type - Mode type - Remote phone numbers - Line description - Authentication
QESPPLIN (or any other line associated with modem resource)	Line description - Resource name - Physical interface - Line speed

3.2.4.1 PPP profile (QESDIAL)

QESDIAL is the PPP profile that is used to make the connection to AGNS for the Universal Connection to use. It contains connection and authentication information that is used to eventually sign on to the IBM system for PTF ordering, etc.

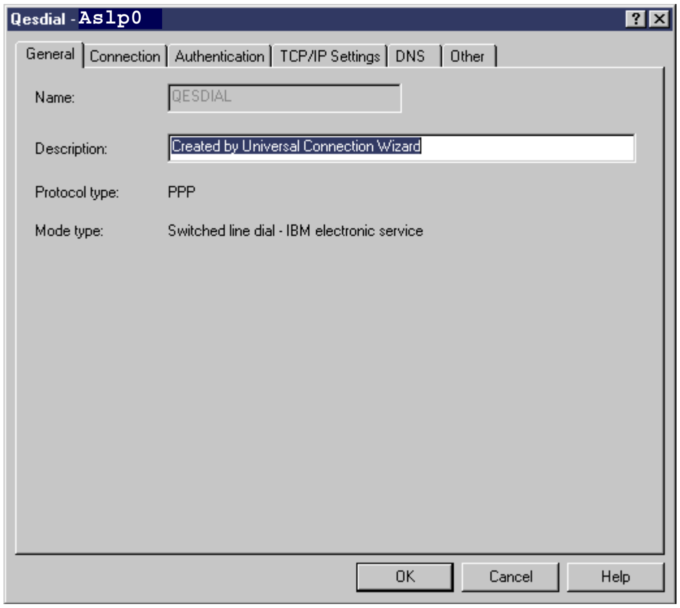
You can access the QESDIAL profile in two ways:

- Operations Navigator
- 5250 emulation

Operations Navigator access

Access through Operations Navigator allows a user to view existing data and make changes if necessary so it is covered first. The following steps outline how to do this:

1. Start Operations Navigator.
2. Expand the iSeries server under My AS400 Connections. Sign on with a valid iSeries user ID and password if prompted.
3. Expand **Network**.
4. Expand **Remote Access Services**.
5. Click **Originator Connection Profiles**.
6. A list of PPP profiles appears in the right-hand section of the Operations Navigator display. Locate and right-click the **QESDIAL** profile. Select **Properties**. The Properties display should look like the example in Figure 32.



Name: QESDIAL

Description: Created by Universal Connection Wizard

Protocol type: PPP

Mode type: Switched line dial - IBM electronic service

Figure 32. Properties of the QESDIAL PPP profile

There are six tabs on this display:

- **General tab**: Gives a description of the PPP profile, its name, and for what application it is being used. In this case, it is associated with the IBM Electronic Service or ECS function.
- **Connection tab**: Gives the name of the line description associated with the profile and the primary and backup phone numbers that are used to connect to the AGNS system. Here, you can make changes to both parameters, such as specifying a different line description or a different phone number. However, we recommend that, to correctly make these changes, rerun the Universal Connection Wizard.
- **Authentication tab**: Provides the Local System Identification parameters, such as the unencrypted PAP user ID and password.

Important

Do not make any changes to the Authentication section at any time since they may disable the PPP profile's ability to successfully sign on to the remote IBM system.

- **TCP/IP Settings tab**: Does not provide much information since all TCP/IP address allocation is handled by the remote system.
- **DNS tab**: Is not used for the AGNS connection and does not provide any relevant information.
- **Other tab**: Specifies the subsystem in which the PPP connection job runs and also the location of the Connection script that is used for the AGNS connection. Do *not* change these parameters.

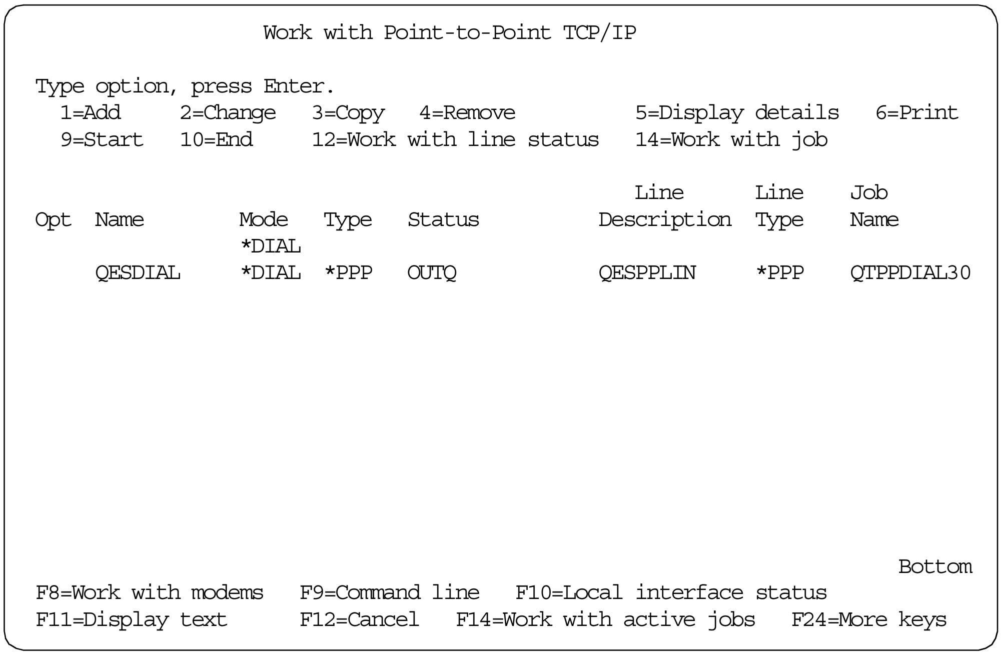
5250 emulation access

As mentioned before, 5250 emulation access to the PPP profile only allows the user to view the properties. No changes can be made. This is prevents anyone who has 5250 emulation access from making inadvertent changes to the profile.

To view the QESDIAL profile from a 5250 emulation screen, follow these steps:

1. Start the 5250 emulation session.
2. From a command line, type `WRKTCPPTP` and press Enter.

The QESDIAL profile should appear as shown in Figure 33.



```
                   Work with Point-to-Point TCP/IP

 Type option, press Enter.
   1=Add     2=Change   3=Copy   4=Remove         5=Display details   6=Print
   9=Start   10=End     12=Work with line status   14=Work with job

                                                    Line        Line     Job
 Opt  Name         Mode   Type   Status          Description  Type     Name
                   *DIAL
      QESDIAL      *DIAL  *PPP   OUTQ            QESPPLIN     *PPP     QTPPDIAL30









                                                                        Bottom
 F8=Work with modems   F9=Command line   F10=Local interface status
 F11=Display text      F12=Cancel   F14=Work with active jobs   F24=More keys
```

Figure 33. PC5250 description of the QESDIAL PPP profile

The mode, type, status, line description, line type, and associated job are all displayed. Not all options listed on this screen are available for use with the QESDIAL profile such as options 2, 3, and 5. These functions must all be performed in the Operations Navigator environment.

You can start and end the QESDIAL profile from this screen, and you can view the job log using option 14. This is covered in more detail in Chapter 6, “Troubleshooting tips” on page 173.

Note

The ECS and Electronic Service Agent applications automatically start and end the PPP profiles when needed. Therefore, it is *not* necessary for you to manually start these profiles for either application to function.

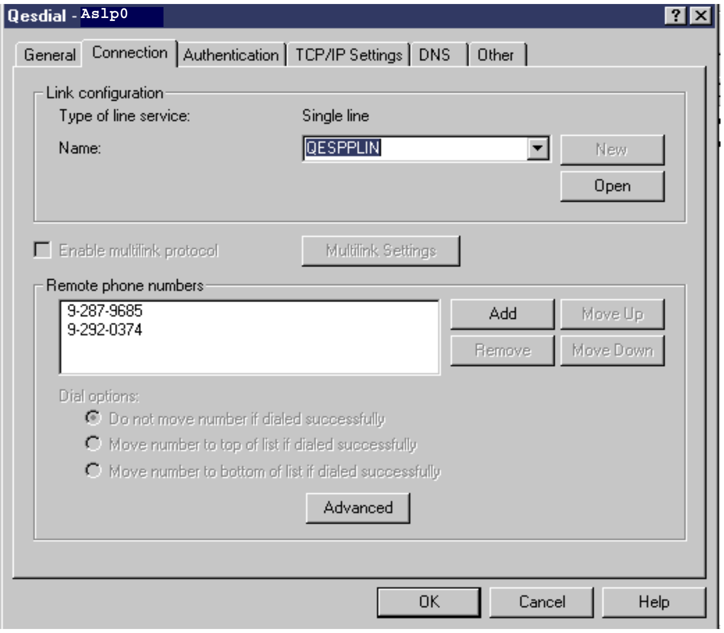
A user can also use option 12 to look at the status of the line description associated with the profile, as well as the controller and device.

3.2.4.2 QESPPLIN or other line description

The other object that is created by an AGNS connection is the line description. The default name for that line is QESPPLIN. However, as mentioned previously, any line that is associated with the modem resource can be used, regardless of its name. This line description behaves like any other TCP line description and can be accessed in the same manner (through Operations Navigator or a 5250 emulation screen).

To view and work with the PPP line description through Operations Navigator, follow these steps:

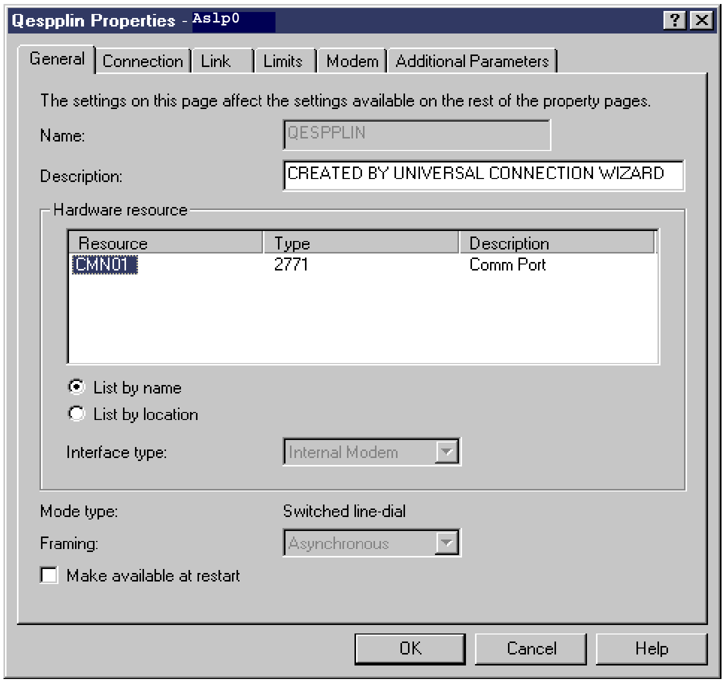
1. Start Operations Navigator.
2. Expand the iSeries server and sign on with a valid iSeries user ID and password if prompted.
3. Expand **Network**.
4. Expand **Remote Access Services**.
5. Click **Originator Connection Profiles**. Locate and double-click the **QESDIAL PPP** profile in the right pane of Operations Navigator.
6. Select the **Connection** tab. Find the **QESPPLIN** line description (or whatever line description that was used for QESDIAL), and click **Open** as shown in Figure 34.



Link configuration
Type of line service: Single line
Name: QESPPLIN
☐ Enable multilink protocol
Remote phone numbers
9-287-9685
9-292-0374
Dial options:
● Do not move number if dialed successfully
○ Move number to top of list if dialed successfully
○ Move number to bottom of list if dialed successfully

Figure 34. Working with the QESPPLIN line description

7. The display shown in Figure 35 appears and allows you to access different parameters of the line description, such as the modem and resource being used.



The settings on this page affect the settings available on the rest of the property pages.
Name: QESPPLIN
Description: CREATED BY UNIVERSAL CONNECTION WIZARD
Hardware resource

Resource	Type	Description
CMN01	2771	Comm Port

● List by name
○ List by location
Interface type: Internal Modem
Mode type: Switched line-dial
Framing: Asynchronous
☐ Make available at restart

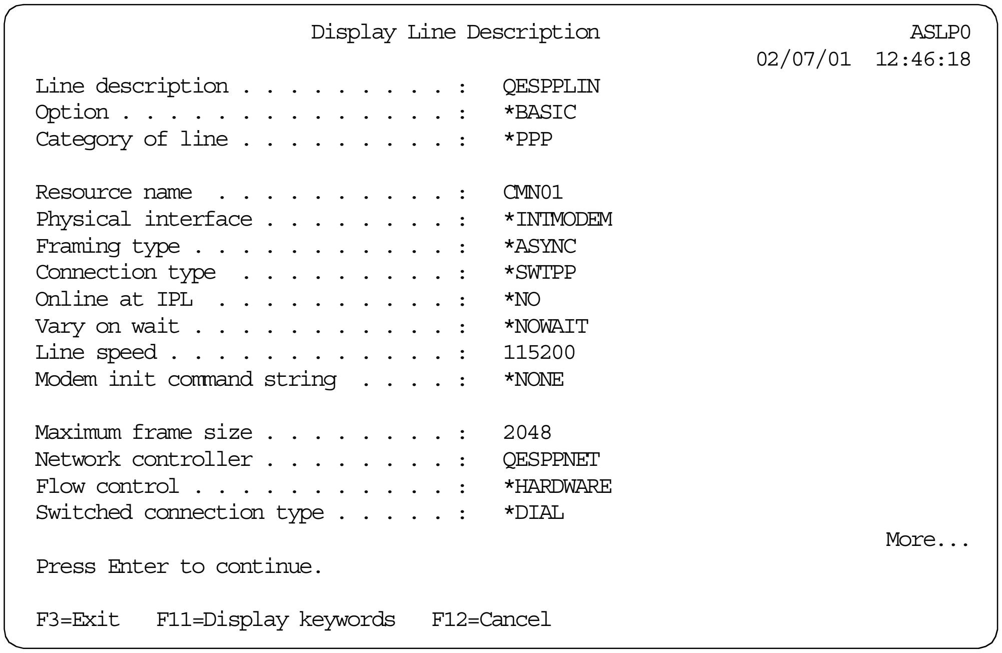
Figure 35. Properties of the QESPPLIN line description

To view and work with the PPP line description through a 5250 emulation screen, follow these steps:

1. From an OS/400 command line, type `WRKLIND QESPPLIN`, or the line name that is being used, and press Enter.

2. Select option 5 to display the details of the line description or option 8 to work with the status of the line.

Option 5 prompts the screen shown in Figure 36.



```
                      Display Line Description                      ASLP0
                                                          02/07/01  12:46:18
 Line description . . . . . . . . . :   QESPPLIN
 Option . . . . . . . . . . . . . . :   *BASIC
 Category of line . . . . . . . . . :   *PPP

 Resource name  . . . . . . . . . . :   CMN01
 Physical interface . . . . . . . . :   *INTMODEM
 Framing type . . . . . . . . . . . :   *ASYNC
 Connection type  . . . . . . . . . :   *SWTPP
 Online at IPL  . . . . . . . . . . :   *NO
 Vary on wait . . . . . . . . . . . :   *NOWAIT
 Line speed . . . . . . . . . . . . :   115200
 Modem init command string  . . . . :   *NONE

 Maximum frame size . . . . . . . . :   2048
 Network controller . . . . . . . . :   QESPPNET
 Flow control . . . . . . . . . . . :   *HARDWARE
 Switched connection type . . . . . :   *DIAL
                                                                    More...
 Press Enter to continue.

 F3=Exit   F11=Display keywords   F12=Cancel
```

Figure 36. Description of the QESPPLIN line description on a 5250 emulation

The parameters listed on this first screen are the most important ones in the AGNS connection. The Resource Name refers to the resource associated with the modem being used. The Physical interface indicates the type of modem that is associated with the line. In this case, it is *INTMODEM, which indicates an internal 56 Kbps modem. The switched connection type must be *DIAL or *BOTH for AGNS connections.

3.2.5 Using Universal Connection

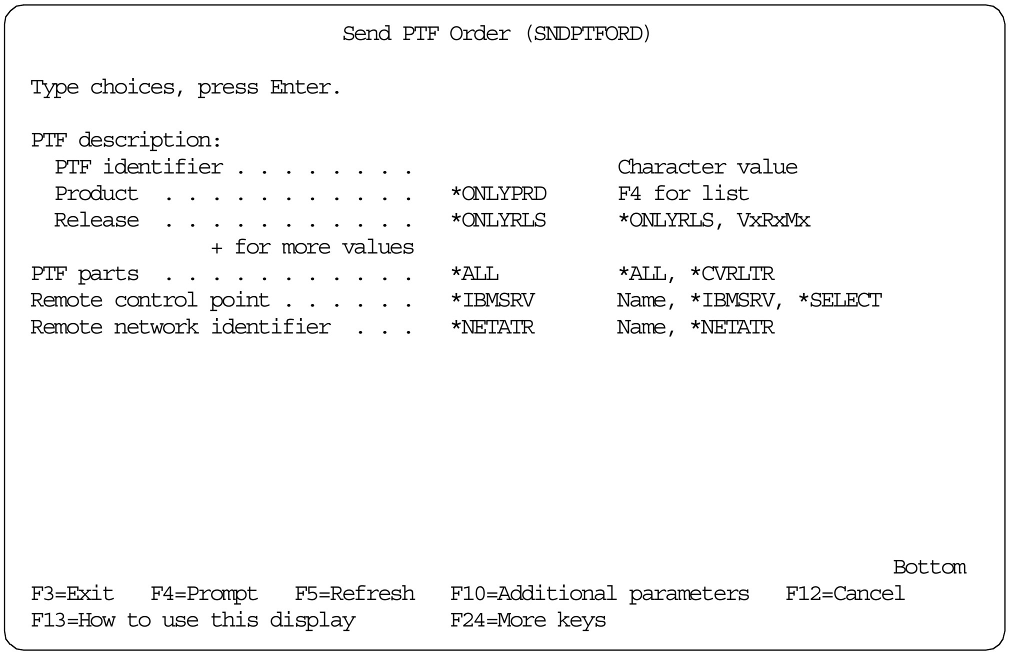
Once Universal Connection is configured and tested, the ECS commands (mentioned previously) can be used the same as before, only now they are implemented over an AGNS connection. This section outlines some of the differences in how these commands are run and displayed using this connection type.

3.2.5.1 Using the SNPTFORD command

The Send PTF Order (SNDPTFORD) command is used primarily to order and receive IBM-supplied program temporary fixes (PTFs) for the iSeries server and IBM-supplied applications. To run this command, type `SNDPTFORD` and prompt it by pressing F4. An example of the SNDPTFORD screen is shown in Figure 37.

Note

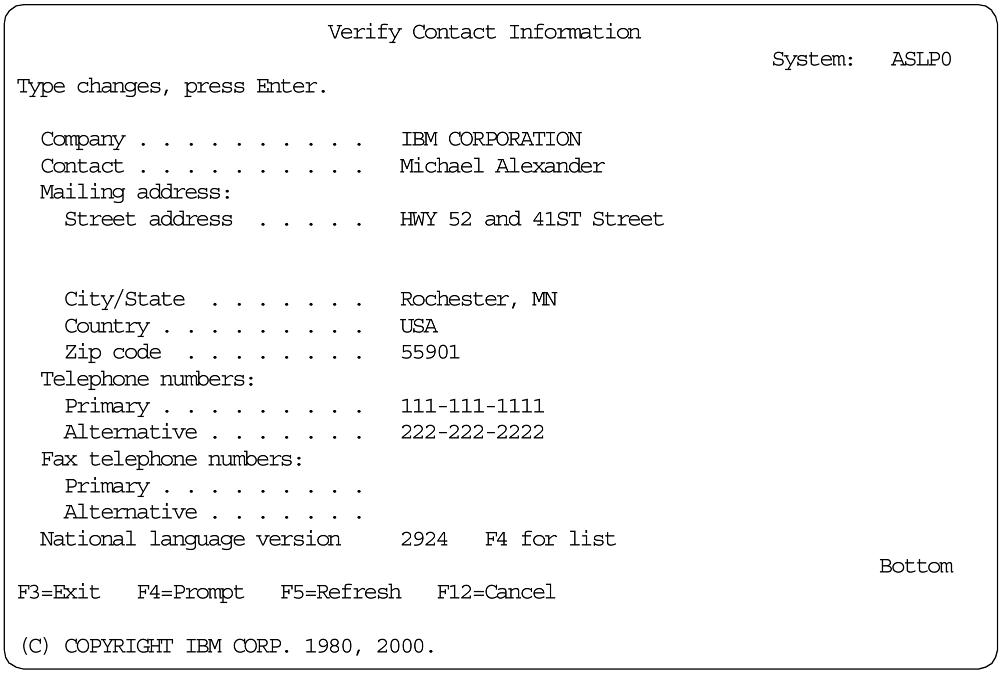
To use Universal Connection, the Remote control point parameter shown in Figure 37 must be set to `*IBMSRV`.



```
                         Send PTF Order (SNDPTFORD)

Type choices, press Enter.

PTF description:
  PTF identifier . . . . . . . .                Character value
  Product  . . . . . . . . . . .   *ONLYPRD      F4 for list
  Release  . . . . . . . . . . .   *ONLYRLS      *ONLYRLS, VxRxMx
               + for more values
PTF parts  . . . . . . . . . . .   *ALL          *ALL, *CVRLTR
Remote control point . . . . . .   *IBMSRV       Name, *IBMSRV, *SELECT
Remote network identifier  . . .   *NETATR       Name, *NETATR









                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Figure 37. SNDPTFORD screen

PTF identifier is the only required parameter for this command. This parameter refers to the PTF number, for example PTF SF98450, which is the latest cumulative package for release V4R5M0 of the OS. After this parameter and any other optional ones are entered, the screen shown in Figure 38 appears. This screen allows you to verify the contact information, such as company name, mailing address, and phone numbers.



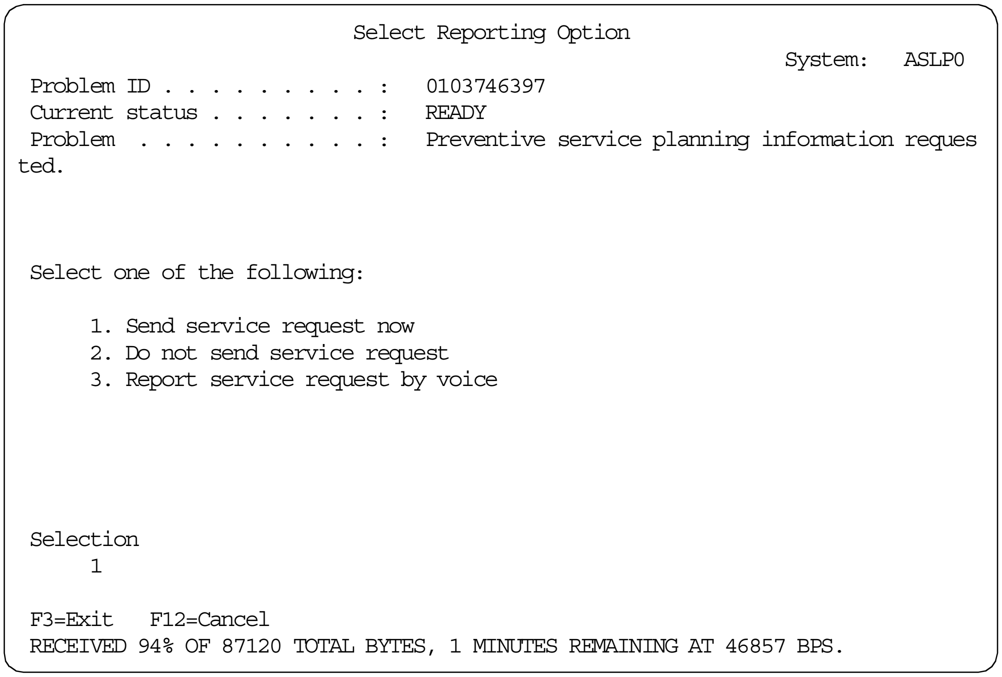
```
                          Verify Contact Information
                                                            System:   ASLP0
Type changes, press Enter.

  Company . . . . . . . . . .   IBM CORPORATION
  Contact . . . . . . . . . .   Michael Alexander
  Mailing address:
    Street address  . . . . .   HWY 52 and 41ST Street


    City/State  . . . . . . .   Rochester, MN
    Country . . . . . . . . .   USA
    Zip code  . . . . . . . .   55901
  Telephone numbers:
    Primary . . . . . . . . .   111-111-1111
    Alternative . . . . . . .   222-222-2222
  Fax telephone numbers:
    Primary . . . . . . . . .
    Alternative . . . . . . .
  National language version     2924   F4 for list
                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel

(C) COPYRIGHT IBM CORP. 1980, 2000.
```

Figure 38. Verify Contact Information screen

So far, all of these screens look the same as before, when SNA methods were used to download a PTF. From this point on, there are a few changes that have been introduced by the Universal Connection PTFs. These changes are outlined and described in the following screens.

Once the contact information is verified, select the Reporting Option and press Enter (see Figure 39). Usually, you can order a PTF immediately using option `1` (Send Service Request Now). Once you choose this option, a QTPPDIALxx job, where *xx* can be any number, is submitted to job queue QSYSNOMAX in QSYS for processing.

After the job is successfully submitted and started, the sign-on to the IBM PTF provider is made and the download takes place. Again, there is a distinct difference in the messaging. In it, there is a better indication of how much of the PTF has already been downloaded and at what speed the transfer is taking place. This is shown in Figure 39. The traditional SNA PTF download showed how many records were downloaded, but there was no way to determine the download speed or how much of the transfer had already occurred.



```
                              Select Reporting Option
                                                              System:   ASLP0
 Problem ID . . . . . . . . . :   0103746397
 Current status . . . . . . . :   READY
 Problem  . . . . . . . . . . :   Preventive service planning information reques
ted.



 Select one of the following:

      1. Send service request now
      2. Do not send service request
      3. Report service request by voice






 Selection
      1

 F3=Exit   F12=Cancel
 RECEIVED 94% OF 87120 TOTAL BYTES, 1 MINUTES REMAINING AT 46857 BPS.
```

Figure 39. Status and speed of the PTF download

Once the download is complete, a service number is provided, and the PTF is ready to be applied.

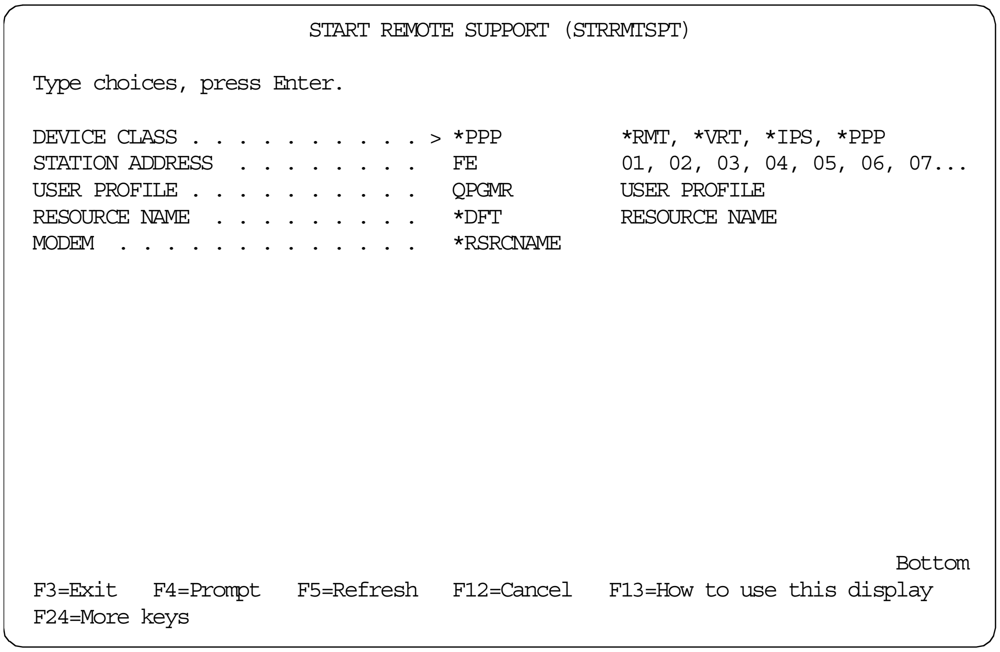
3.2.5.2 Using other ECS commands

Other commands, such as SNDSRVRQS, QRYPRBSTS, and ORDSPTPTF, are similar to the SNDPTFORD command. They all start a PPP dial job that is submitted to the QSYSNOMAX job queue, and a connection is made to the IBM service system.

Other IBM service functions, such as Service Agent, also use Universal Connection. For more information on Service Agent, refer to:
`http://publib.boulder.ibm.com/as400_sd/sdsadoc.html`

3.2.5.3 Allowing Remote Support

At some time, it may be necessary to contact IBM Support Personnel and allow them to dial in remotely to the iSeries server for further problem determination. Universal Connection also allows Remote Dial in Support just as before with the SNA pass through server. IBM personnel can assist in enabling Remote Support using the Start Remote Support (STRRMTSPT) command when it is necessary to do so. The STRRMTSPT command screen is shown in Figure 40.

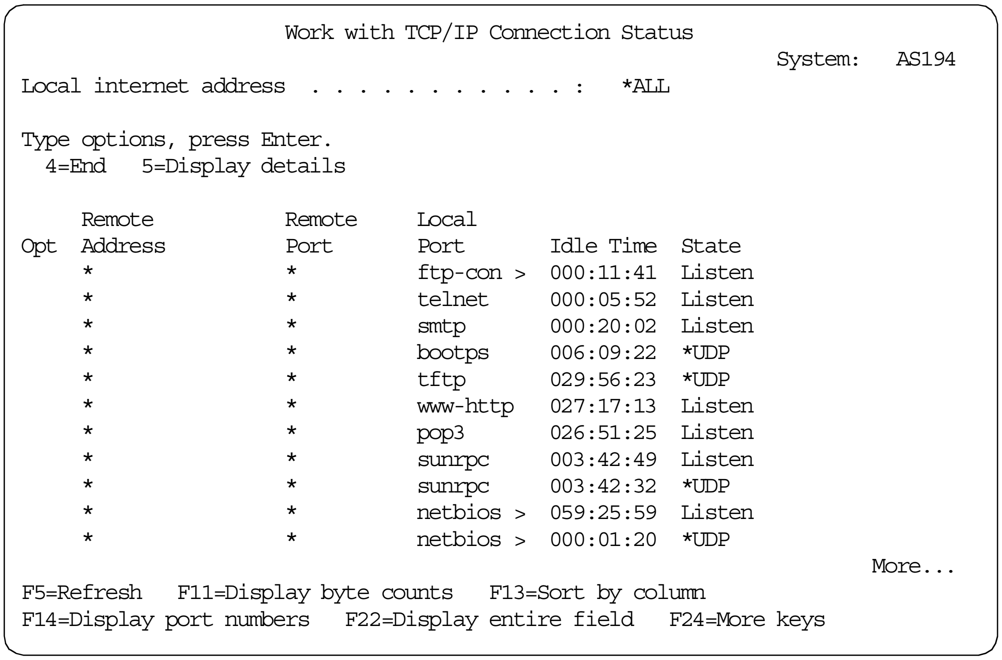


```
                      START REMOTE SUPPORT (STRRMTSPT)

Type choices, press Enter.

DEVICE CLASS . . . . . . . . . . . > *PPP         *RMT, *VRT, *IPS, *PPP
STATION ADDRESS  . . . . . . . .     FE           01, 02, 03, 04, 05, 06, 07...
USER PROFILE . . . . . . . . . .     QPGMR        USER PROFILE
RESOURCE NAME  . . . . . . . . .     *DFT         RESOURCE NAME
MODEM  . . . . . . . . . . . . .     *RSRCNAME














                                                                        Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 40. New PPP function for the STRRMTSPT command

However, it is noteworthy to mention that all the STRRMTSPT functions are included in OS/400 V4R5M0 PTF SF64123. Therefore, it is necessary to have this PTF applied to the system if Remote Support is to be enabled using the 9771 adapter internal 56 Kbps modem. This PTF provides the *PPP option, which is used for this type of connection.

The ability to gain Remote Support to the iSeries server over this connection is also based on the availability and functionality of the Telnet server. To ensure that Telnet is active on the system, run the NETSTAT command and select option `3`. If Telnet is in a listen state under the Local Port column, as shown in Figure 41, then it is active.



```
                       Work with TCP/IP Connection Status
                                                             System:   AS194
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote           Remote     Local
Opt  Address          Port       Port       Idle Time  State
     *                *          ftp-con >  000:11:41  Listen
     *                *          telnet     000:05:52  Listen
     *                *          smtp       000:20:02  Listen
     *                *          bootps     006:09:22  *UDP
     *                *          tftp       029:56:23  *UDP
     *                *          www-http   027:17:13  Listen
     *                *          pop3       026:51:25  Listen
     *                *          sunrpc     003:42:49  Listen
     *                *          sunrpc     003:42:32  *UDP
     *                *          netbios >  059:25:59  Listen
     *                *          netbios >  000:01:20  *UDP
                                                                     More...
F5=Refresh   F11=Display byte counts   F13=Sort by column
F14=Display port numbers   F22=Display entire field   F24=More keys
```

Figure 41. Telnet should be in listen state for Remote Support

Remote Support using *PPP can also allow FTP transfers, providing that FTP is also active on the system. In the future, this connection will allow the use of Operations Navigator and HTTP access to the iSeries server for more convenient Remote Support by IBM personnel.

3.2.6 Security over an AGNS connection

This section provides a brief overview of the mechanisms that are involved in maintaining a safe and secure connection using the AGNS provider. Security is essential for data integrity as well as confidentiality. The AGNS connection implements security in three separate phases:

- Authentication
- Authorization
- Transport

These three components work together to provide a secure connection from the iSeries server to the IBM system. However, you should never assume that they provide full network security. Therefore, you must also consider such measures as those mentioned in Chapter 2, “Network security concepts and overview” on page 15.

3.2.6.1 Authentication

Authentication is usually the first step of any secure connection. It answers the question “Who is trying to connect?” It validates the user who is trying to connect by prompting for a user ID and password pairing. The AGNS connection is no different in this manner. This initial level of authentication is handled by the QESDIAL PPP dial profile. Here, the Password Authentication Protocol (PAP) user ID and password are stored. This user ID and password are verified by the AGNS system. It is the first step of the secure connection.

3.2.6.2 Authorization

Authorization takes authentication a step further and asks the question “Now that this user is authorized to connect, where should it be allowed to go?” To decide this, an extended encrypted authentication takes place with the Local Interface Gateway (LIG). Successful validation at this stage allows access to the IBM service system. This completes the second stage of the connection process. Now the user can send and receive data across this secure bridge. The next step is to determine how and where the data is sent.

3.2.6.3 Transport

Transport is the final stage of the AGNS security mechanism. It answers the question “Where and how will the data be sent and received?” Once connected to the LIG, the service system assigns an IP address to the connecting node, based on a pool of IP addresses that are available. This is then configured in the TCP stack of the connecting system. The service system also assigns itself an IP address and the conversation starts using these two IP addresses. Data then flows over the AT&T Global Network from the iSeries server to IBM and back. This is particularly important because data is not being sent over the Internet. Rather, a private network is being used for transfer of information. This reduces the risk of hacking and data loss, since access is limited to a select set of users.

Once data starts transferring, consistent packet checking takes place where critical pieces of information, such as source port, source address, destination port, and destination address, are checked. If any of these change during the transfer, the packets exhibiting these changes are discarded. This ensures that data integrity is maintained and also safeguards against outside intervention by hackers, etc.

3.3 PPP dial-up to any ISP

Figure 42 shows the network configuration of PPP dial-up to any ISP. If you currently subscribe to an ISP, and you want to have a service connection with IBM, you can follow the procedure to create the PPP dial-up to any ISP configuration.

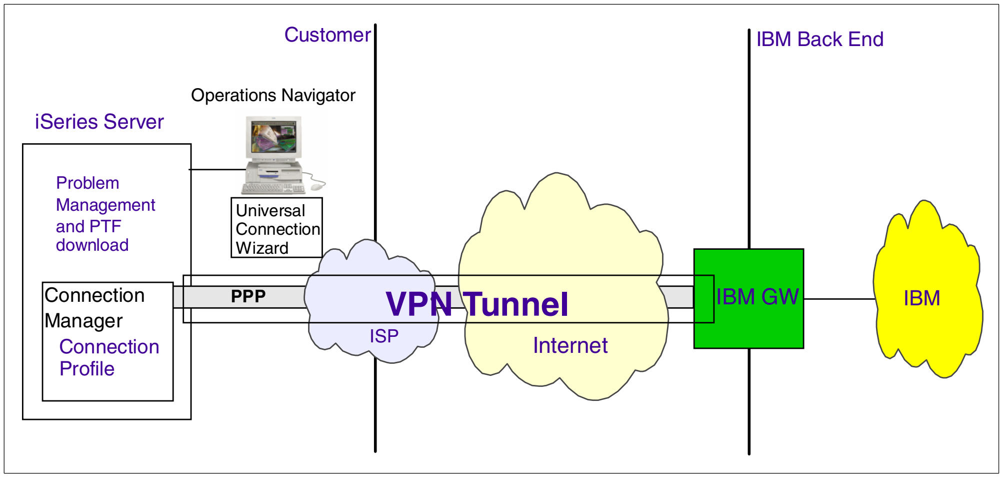


Figure 42. Network configuration of PPP dial-up to any ISP

3.3.1 Prerequisites

The prerequisites for creating a PPP dial-up to any ISP configuration using Universal Connection Wizard are:

- The level of OS/400 should be V5R1M0. The GA PTF cumulative package must be applied.
- TCP/IP Connectivity Utilities (5722-TC1) is required.
- Crypto Access Provider 128-bit/56-bit for AS/400 (5722-AC3) or Crypto Access Provider 56-bit for AS/400 (5722-AC2) is required.
- Client Access Express V5R1M0 with Service Pack SI01037 or later are required to obtain the wizard.
- Ensure the QRETSVRSEC system value is set to `1`. This can be done by issuing the Display System Value (DSPSYSVAL) command. If it is not set to "1", run the Change System Value (CHGSYSVAL) command.
- If you are using an internal modem, such as the 56 Kbps provided with the 9771 adapter card, ensure that the network attribute MDMCNTRYID is set appropriately. The Display Network Attributes (DSPNETA) command displays the current value. The Change Network Attributes (CHGNETA) command allows you to make changes.
- TCP/IP must be active. It can be started with the Start TCP/IP (STRTCP) command.
- The user configuring the wizard needs *ALLOBJ and *IOSYSCFG authority as part of their iSeries user profile.

3.3.2 Planning worksheet for PPP dial-up to any ISP

Figure 43 shows the sample network configuration in this section.

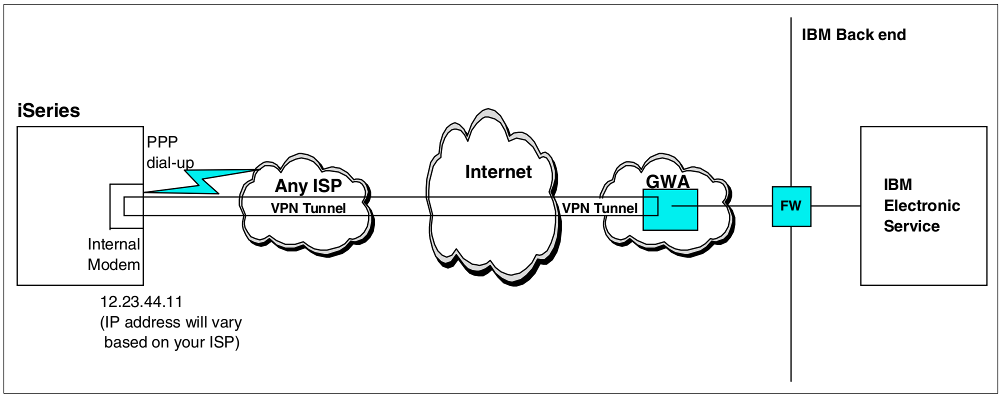


Figure 43. PPP dial-up to any ISP network configuration

Complete the iSeries server planning worksheets as shown in Table 5. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 5. AS026 PPP dial-up to any ISP configuration: Customer information

Customer information to create PPP dial-up to any ISP configuration	**Scenario answers**
What is the service contact information? - Company - Contact Name - Phone - Alternate Phone Number - Fax number	 IBM ITSO 111-111-1111 222-222-2222 333-333-3333
What is the service contact mailing address? - Street address - City/State - Country - ZIP code - National language version - Media for PTFs	 3605 Hwy52 North Rochester/Minnesota United States 55901 English (2924) Automatic selection
Where is your server located? - Country - State or province	 United States Minnesota
What application are you using over this connection? - Electronic Customer Support (ECS) or - IBM Electronic Service Agent for AS/400	Electronic Customer Support
What type of connection are you using for your Universal Connection?	A dial-up connection using an Internet Service Provider
What is the connection profile name of your ISP that you are going to use for IBM Electronic Service? - Profile name	ISPDIAL

If you do not have the PPP ISP dial-up connection profile and its line definition, create the configuration for the PPP ISP dial-up connection by using the New Dial-up Connection Wizard. Gather all the configuration data to create the ISP dial-up connection profile and its line definition before the actual implementation, as shown in Table 6.

Table 6. The customer information to create the PPP ISP dial-up connection

Customer information to create the PPP ISP dial-up connection profile and its line definition	**Scenario answers**
What is the new connection profile name? - Profile name	ISPDIAL
What hardware resource are you going to use for the PPP ISP dial-up connection profile? - Hardware resource name	CMN05(2771)
What is the new line definition name? - Line definition name	QESPPLIN

Customer information to create the PPP ISP dial-up connection profile and its line definition	**Scenario answers**
What is the phone number that will be used for making a dial-up connection with your Internet Service Provider? - Dial-up phone number	123-4567
What are the user ID and password that were supplied with your Internet Service Provider to make a dial-up connection? - UserID - password Your ISP requires the account information to be encrypted?	USER PASSWORD No

3.3.3 Configuring a PPP dial-up to any ISP connection

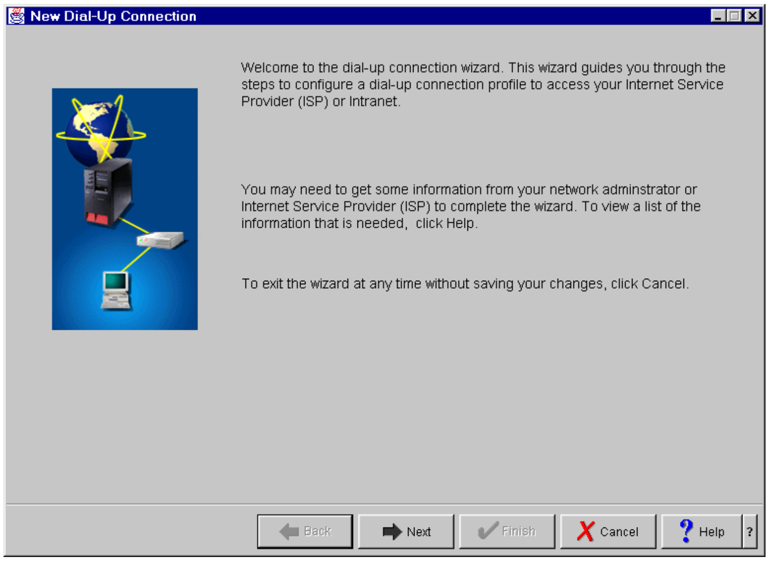
In this procedure, you perform the following steps:

1. Create the new PPP dial-up connection profile and its line definition. If you have the PPP dial-up connection profile for ISP, go to 3.3.3.2, “Creating the PPP dial-up to any ISP connection with UVC” on page 68.
2. Create a PPP dial-up to any ISP configuration using the Universal Connection Wizard. In the wizard, choose the existing PPP dial-up ISP connection profile and its line definition that is created in the previous step.
3. Test the connection.

3.3.3.1 New Dial Connection Wizard: Creating a dial-up connection profile

Perform the following steps to configure the dial-up connection profile to your ISP using the Dial Connection Wizard:

1. Start Operations Navigator.
2. Expand the iSeries server (in this case, AS026) under My Connections. Sign on when prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **New Dial Connection Wizard**.
6. Click **Next** in the Welcome dialog as shown in Figure 44.


New Dial-Up Connection

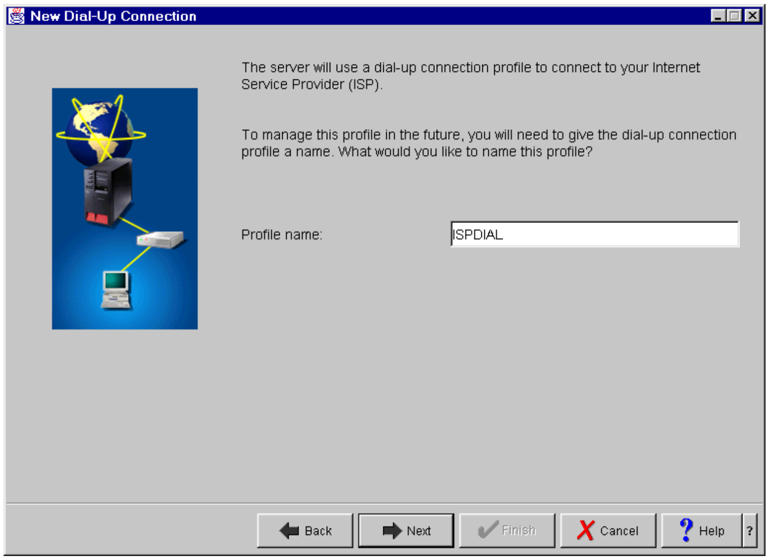
Welcome to the dial-up connection wizard. This wizard guides you through the steps to configure a dial-up connection profile to access your Internet Service Provider (ISP) or Intranet.

You may need to get some information from your network adminstrator or Internet Service Provider (ISP) to complete the wizard. To view a list of the information that is needed, click Help.

To exit the wizard at any time without saving your changes, click Cancel.

Figure 44. Configuring a new dial Connection: Welcome

7. Enter the dial-up connection profile name (refer to the planning worksheet) as shown in Figure 45. In this example, we enter `ISPDIAL`. Click **Next** to continue.


New Dial-Up Connection

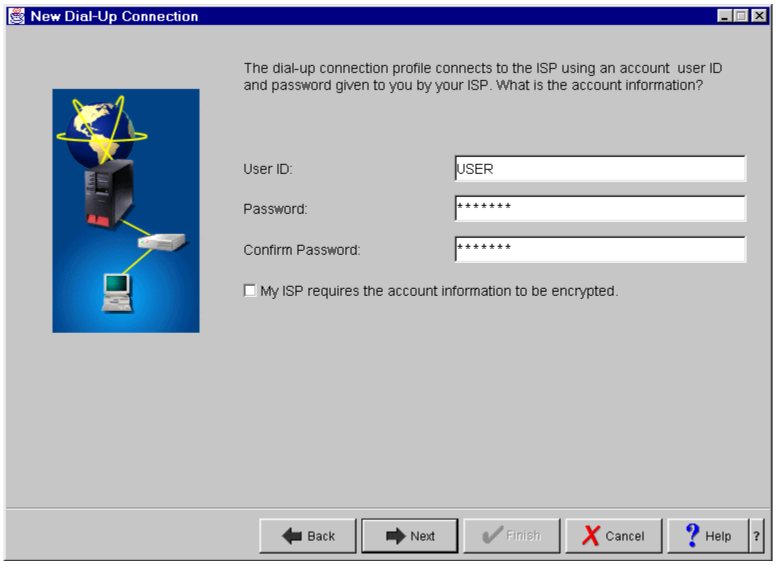
The server will use a dial-up connection profile to connect to your Internet Service Provider (ISP).

To manage this profile in the future, you will need to give the dial-up connection profile a name. What would you like to name this profile?

Profile name: ISPDIAL

Figure 45. Entering the dial-up connection profile name

8. Enter the user ID and password that was supplied with your Internet Service Provider to establish a connection as shown in Figure 46. If your ISP requires the user ID and password to be encrypted, select **My ISP requires the account information to be encrypted**. Click **Next** to continue.



New Dial-Up Connection

The dial-up connection profile connects to the ISP using an account user ID and password given to you by your ISP. What is the account information?

User ID: USER

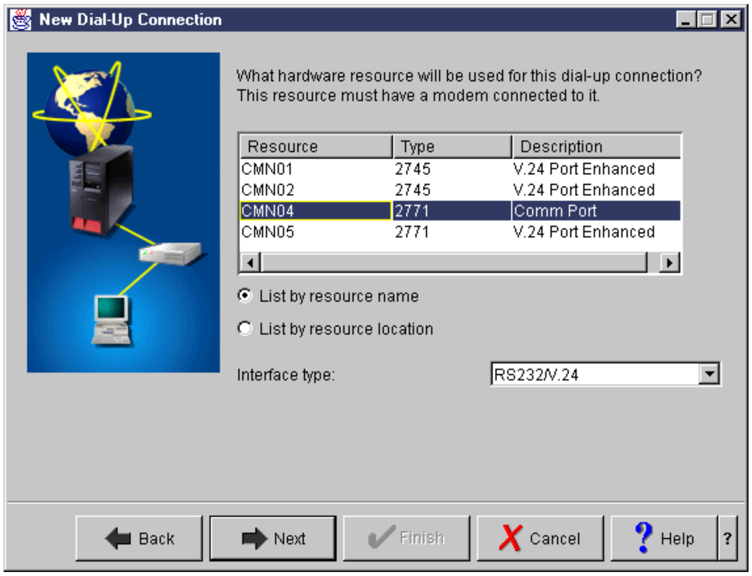
Password: *******

Confirm Password: *******

□ My ISP requires the account information to be encrypted.

Figure 46. Inputting the account information

9. Choose the hardware resource for the PPP dial-up connection (refer to the planning worksheet) as shown in Figure 47. In this example, we choose the **F/C2771** internal modem. You can also choose F/C2761 or another communication port feature that has an external modem to establish the PPP dial connection. Figure 48 shows an example where the F/C2720 communication port is chosen. You should also select the interface type. In this example, we choose **RS232/V.24** for the F/C2720 communication port. Click **Next** to continue.



New Dial-Up Connection

What hardware resource will be used for this dial-up connection? This resource must have a modem connected to it.

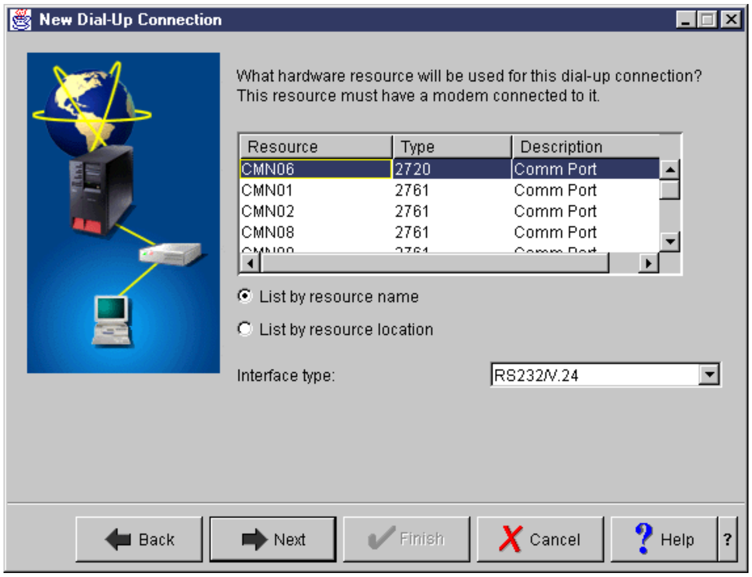
Resource	Type	Description
CMN01	2745	V.24 Port Enhanced
CMN02	2745	V.24 Port Enhanced
CMN04	2771	Comm Port
CMN05	2771	V.24 Port Enhanced

● List by resource name

○ List by resource location

Interface type: RS232/V.24

Figure 47. Selecting hardware resources: F/C2771 internal modem



New Dial-Up Connection

What hardware resource will be used for this dial-up connection? This resource must have a modem connected to it.

Resource	Type	Description
CMN06	2720	Comm Port
CMN01	2761	Comm Port
CMN02	2761	Comm Port
CMN08	2761	Comm Port

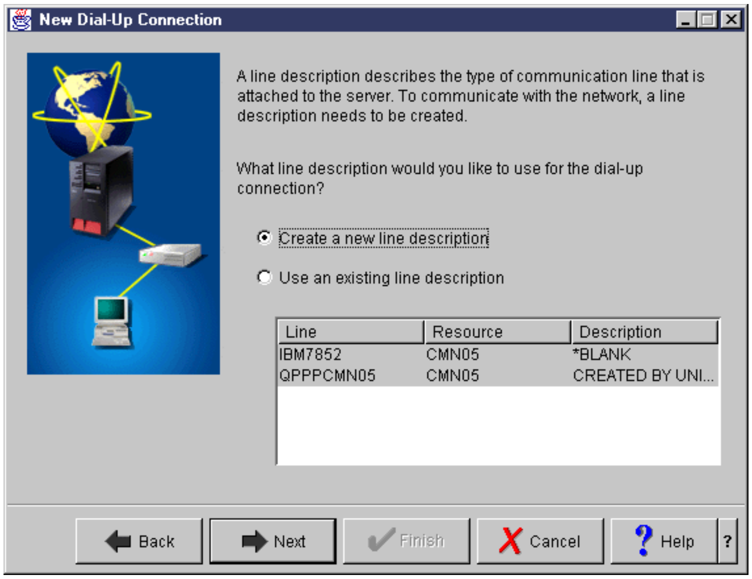
● List by resource name

○ List by resource location

Interface type: RS232/V.24

Figure 48. Selecting hardware resources: F/C2720 communication port

10.On the next display (Figure 49), select **Create a new line description**. Click **Next** to continue.



New Dial-Up Connection

A line description describes the type of communication line that is attached to the server. To communicate with the network, a line description needs to be created.

What line description would you like to use for the dial-up connection?

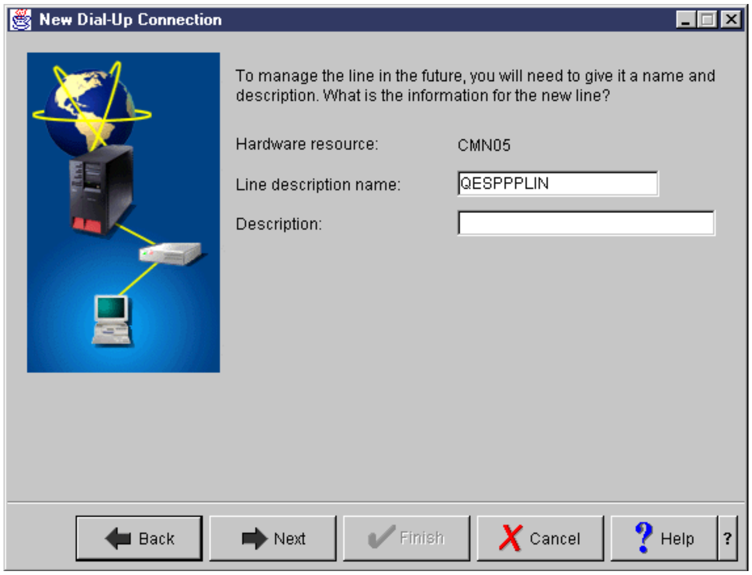
● Create a new line description

○ Use an existing line description

Line	Resource	Description
IBM7852	CMN05	*BLANK
QPPPCMN05	CMN05	CREATED BY UNI...

Figure 49. Creating a new line description

11.Enter the line description name and description as shown in Figure 50. Click **Next** to continue.



To manage the line in the future, you will need to give it a name and description. What is the information for the new line?

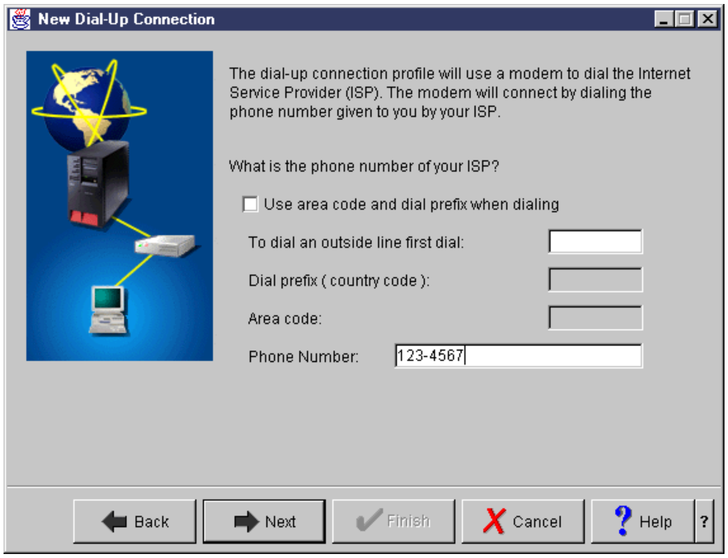
Hardware resource: CMN05

Line description name: QESPPPLIN

Description:

Figure 50. Line description

12.Enter the phone number that is used for making a dial-up connection with your Internet Service Provider as shown in Figure 51. Click **Next** to continue.



The dial-up connection profile will use a modem to dial the Internet Service Provider (ISP). The modem will connect by dialing the phone number given to you by your ISP.

What is the phone number of your ISP?

□ Use area code and dial prefix when dialing

To dial an outside line first dial:

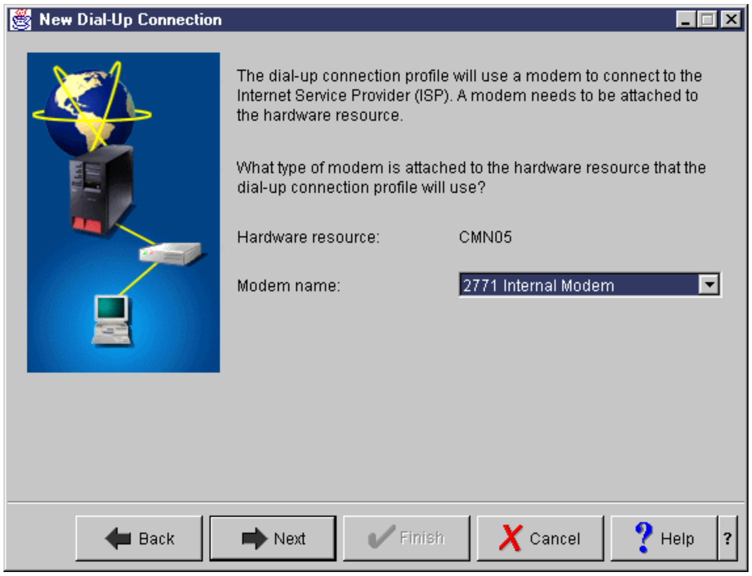
Dial prefix (country code):

Area code:

Phone Number: 123-4567

Figure 51. Phone number to connect to your service provider

13.Select the modem from the list as shown in Figure 52. In this example, choose **2771 Internal modem**. If you chose the communication port feature in step 9, select the external modem from the list. Click **Next** to continue.



The dial-up connection profile will use a modem to connect to the Internet Service Provider (ISP). A modem needs to be attached to the hardware resource.

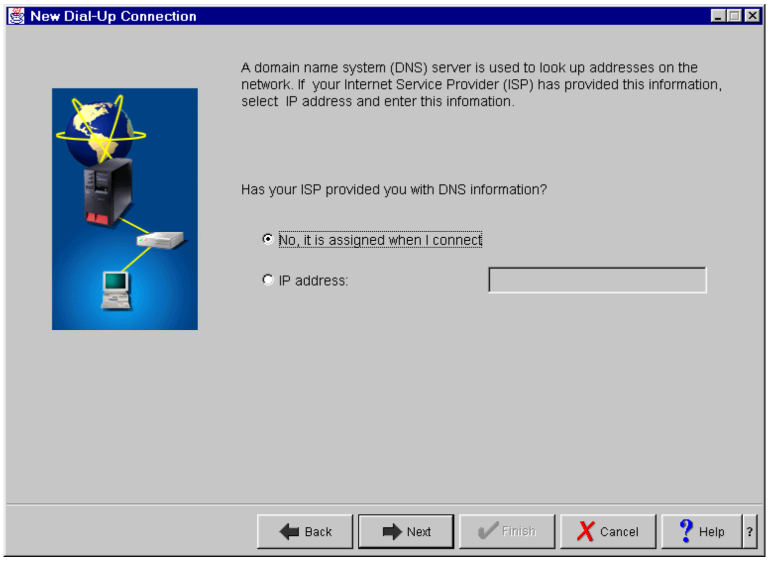
What type of modem is attached to the hardware resource that the dial-up connection profile will use?

Hardware resource: CMN05

Modem name: 2771 Internal Modem

Figure 52. Selecting the modem information

14.If your ISP requires you to specify the domain name system (DNS) server IP address, click **IP address** and enter the DNS IP address. In this example, we choose **No, it is assigned when I connect** as shown in Figure 53. Click **Next** to continue.



A domain name system (DNS) server is used to look up addresses on the network. If your Internet Service Provider (ISP) has provided this information, select IP address and enter this infomation.

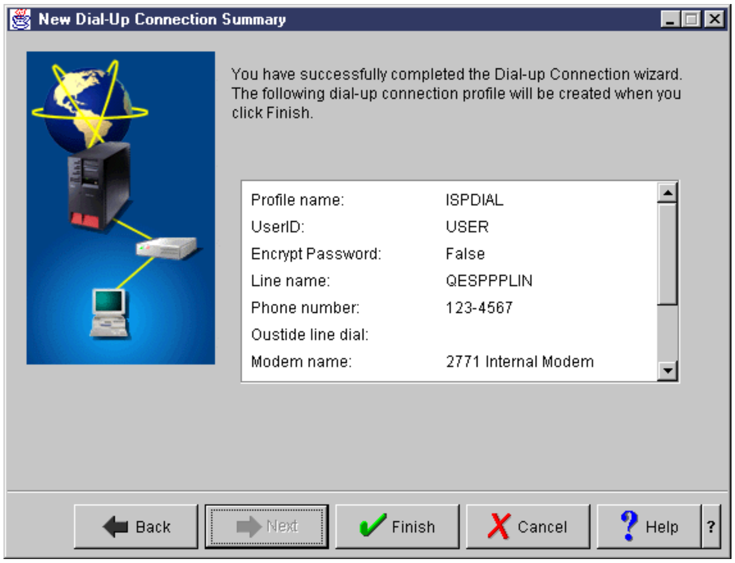
Has your ISP provided you with DNS information?

● No, it is assigned when I connect

○ IP address:

Figure 53. Selecting the DNS information

15.Click **Finish** to create the definition shown in Figure 54.



You have successfully completed the Dial-up Connection wizard. The following dial-up connection profile will be created when you click Finish.

Profile name:	ISPDIAL
UserID:	USER
Encrypt Password:	False
Line name:	QESPPPLIN
Phone number:	123-4567
Oustide line dial:	
Modem name:	2771 Internal Modem

Figure 54. Confirming the new dial-up connection profile

3.3.3.2 Creating the PPP dial-up to any ISP connection with UVC

Perform the following steps to configure a PPP dial-up any ISP connection using UVC.

> **Note**
>
> If you created your ISP profile using the new dial-up wizard, it created a default route that allows the VPN connection to be routed through your ISP connection. If you did not use the new dial-up wizard, you must ensure that either a default route was added to this profile, you added a route to allow, or you added a route to allow the connection to the IBM gateway (GWA).

1. Start Operations Navigator.
2. Expand the iSeries server (in this case, AS026) under My Connections. Sign on when prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **Universal Connection Wizard** as shown in Figure 55.

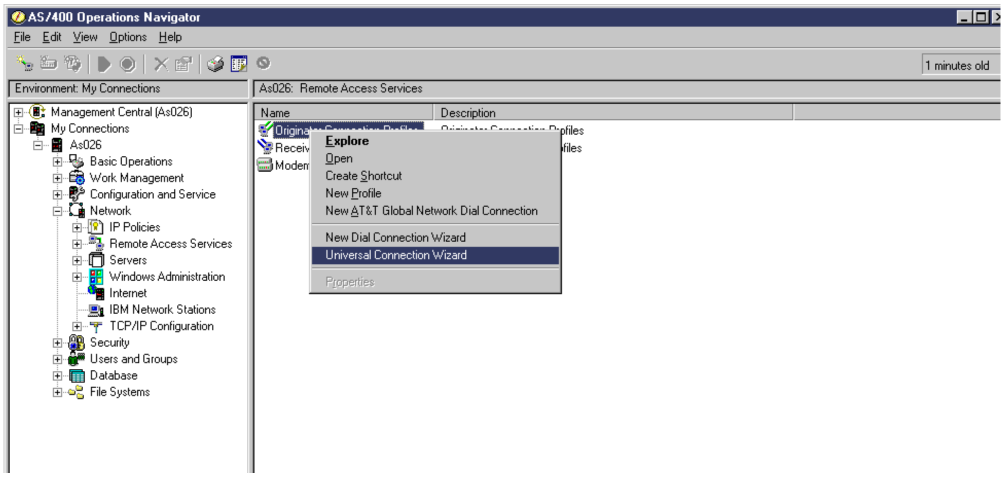
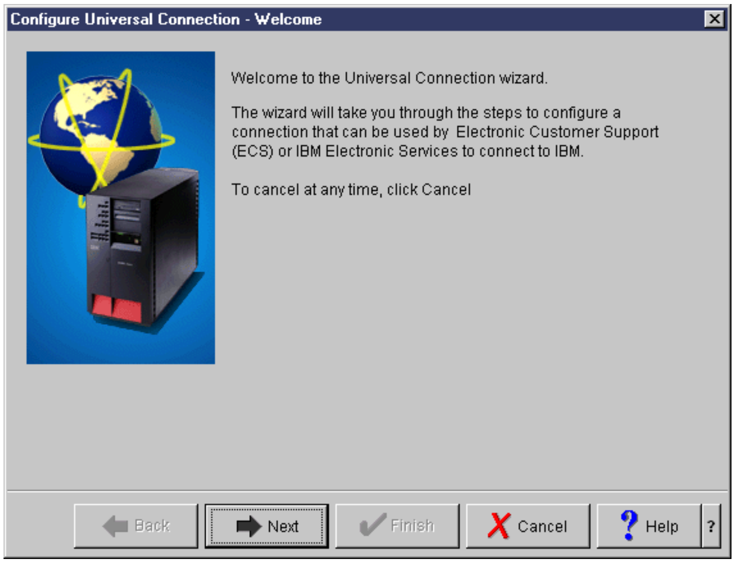


Figure 55. Selecting Universal Connection Wizard

6. Click **Next** in the Welcome dialog as shown in Figure 56.



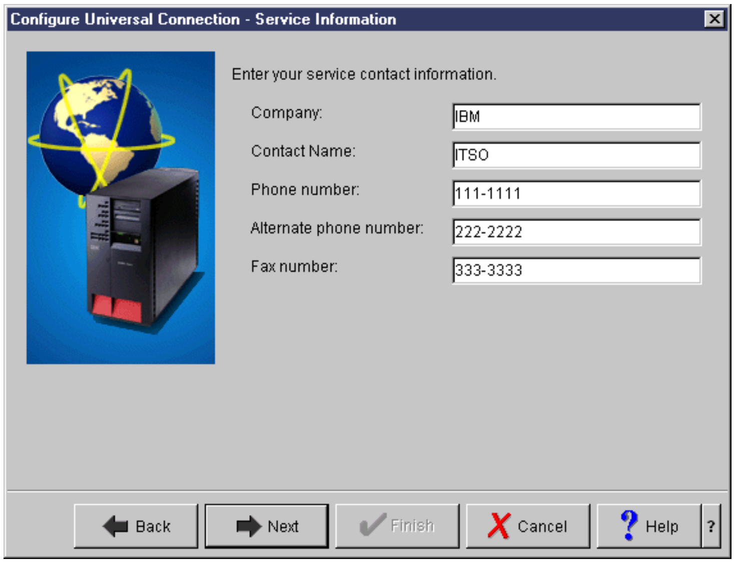
Welcome to the Universal Connection wizard.

The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 56. Configure Universal Connection - Welcome window

7. Enter the service contact information as shown in Figure 57. Click **Next** to continue.



Configure Universal Connection - Service Information

Enter your service contact information.

Company: IBM

Contact Name: ITSO

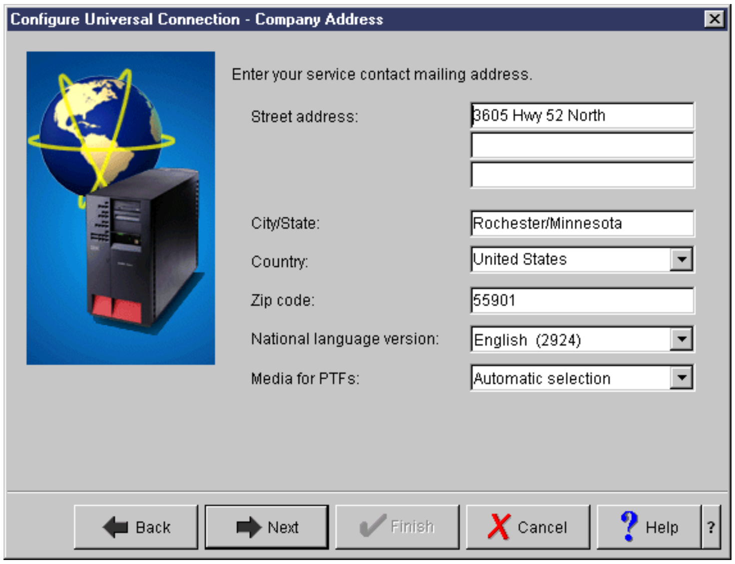
Phone number: 111-1111

Alternate phone number: 222-2222

Fax number: 333-3333

Figure 57. Service contact information

8. Enter the service contact mailing address, national language version, and media for PTFs information as shown in Figure 58. Click **Next** to continue.



Configure Universal Connection - Company Address

Enter your service contact mailing address.

Street address: 3605 Hwy 52 North

City/State: Rochester/Minnesota

Country: United States

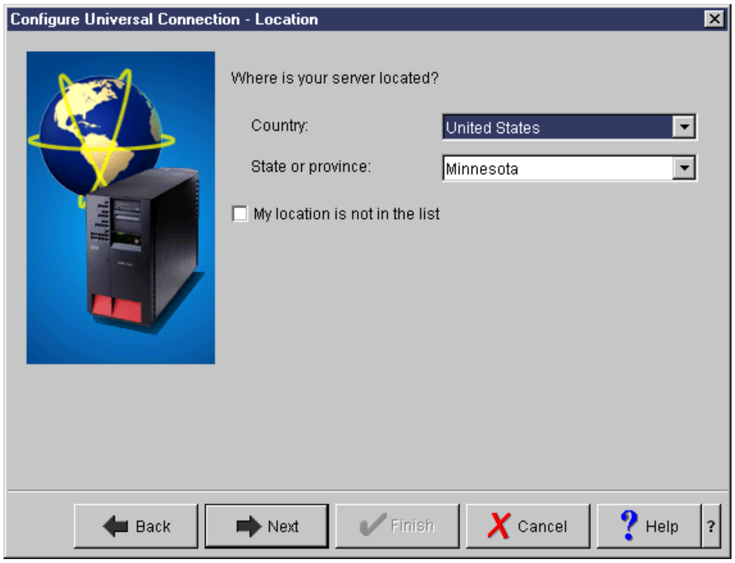
Zip code: 55901

National language version: English (2924)

Media for PTFs: Automatic selection

Figure 58. Service contact mailing address

9. Choose the country and state or province as shown in Figure 59. Click **Next** to continue.


Configure Universal Connection - Location

Where is your server located?

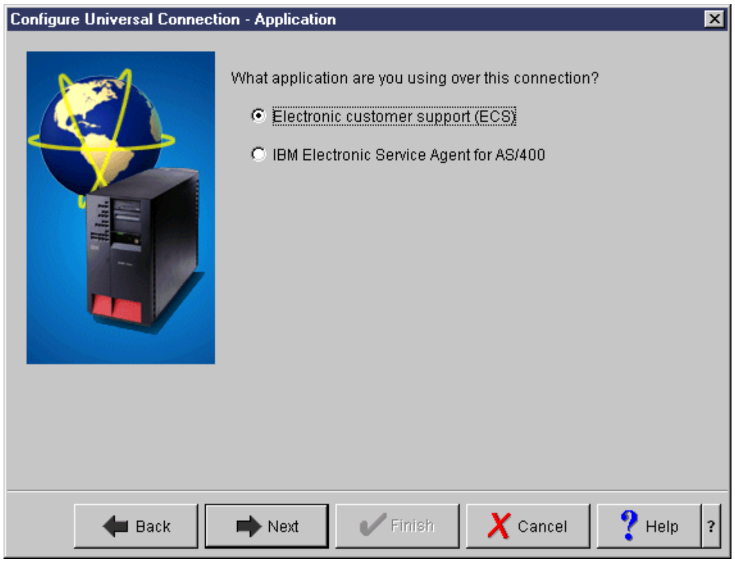
Country: United States

State or province: Minnesota

□ My location is not in the list

Figure 59. Selecting the country, state, or province

10.Select the application you want to use. In this example, select **Electronic Customer Support (ECS)** as shown in Figure 60. Click **Next** to continue.


Configure Universal Connection - Application

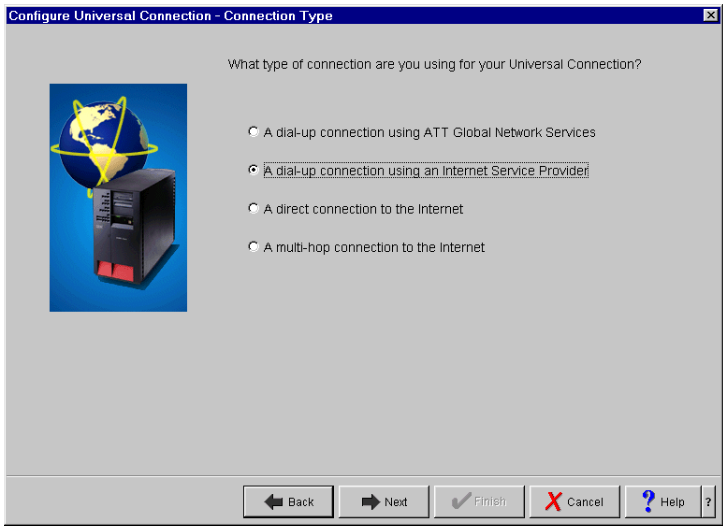
What application are you using over this connection?

● Electronic customer support (ECS)

○ IBM Electronic Service Agent for AS/400

Figure 60. Selecting an application

11.Select **A Dialup connection using an Internet Service Provider** as shown in Figure 61. Click **Next** to continue.


Configure Universal Connection - Connection Type

What type of connection are you using for your Universal Connection?

○ A dial-up connection using ATT Global Network Services

● A dial-up connection using an Internet Service Provider

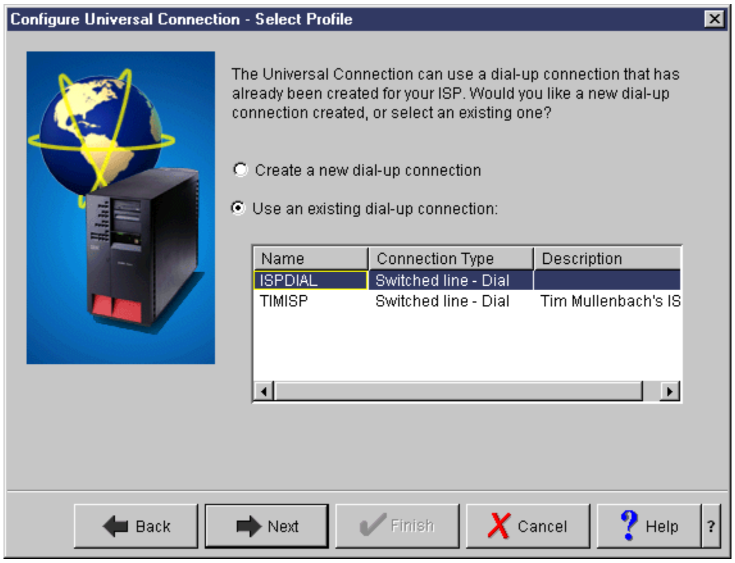
○ A direct connection to the Internet

○ A multi-hop connection to the Internet

Figure 61. Selecting the connection type

12.Select the connection profile that you want to use for IBM Electronic Service as shown in Figure 62. In this example, we select **ISPDIAL**. Click **Next** to continue.

If the PPP to any dial-up ISP connection profile and its line definition haven't been created on your iSeries server, create them by using the New Dial Connection Wizard as explained in 3.3.3.1, "New Dial Connection Wizard: Creating a dial-up connection profile" on page 62.


Configure Universal Connection - Select Profile

The Universal Connection can use a dial-up connection that has already been created for your ISP. Would you like a new dial-up connection created, or select an existing one?

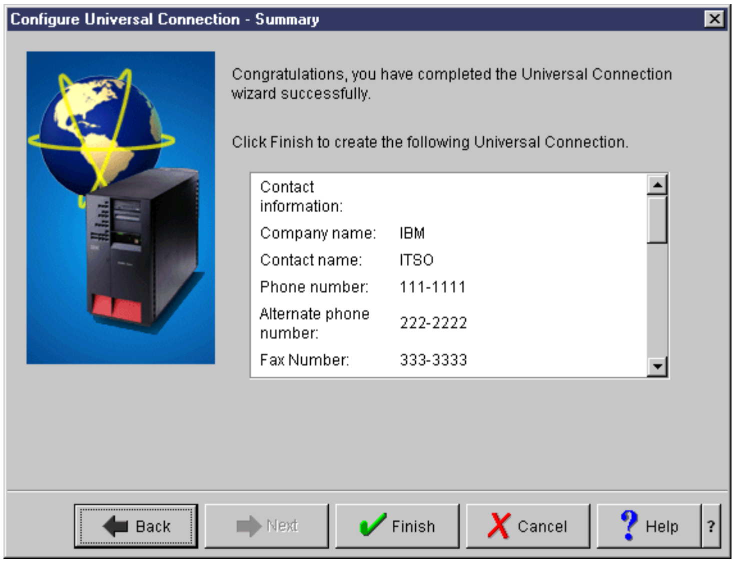
○ Create a new dial-up connection

● Use an existing dial-up connection:

Name	Connection Type	Description
ISPDIAL	Switched line - Dial	
TIMISP	Switched line - Dial	Tim Mullenbach's IS

Figure 62. Select Profile

13.Click **Finish** to create the definition shown in Figure 63.



Configure Universal Connection - Summary

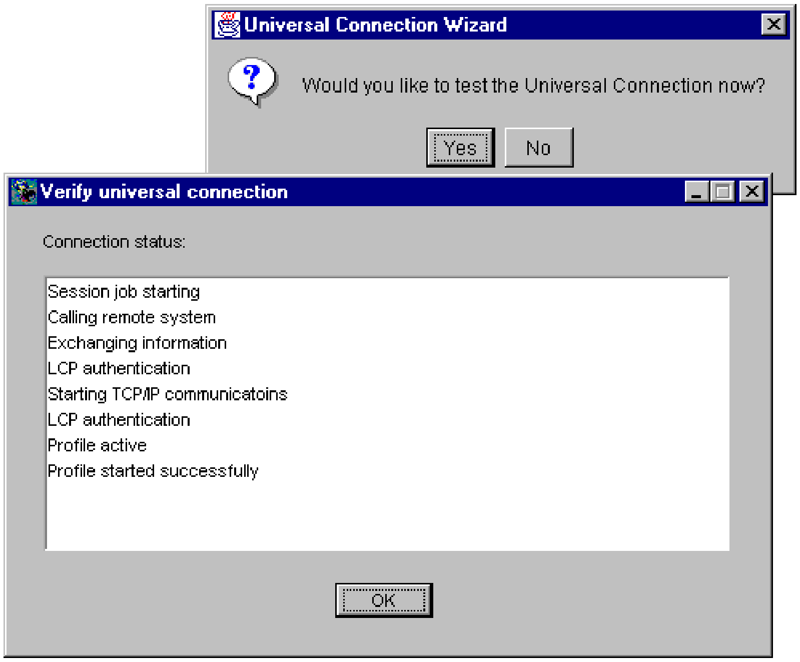
Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

Contact information:	
Company name:	IBM
Contact name:	ITSO
Phone number:	111-1111
Alternate phone number:	222-2222
Fax Number:	333-3333

Figure 63. Summary display

14.After you click Finish, the pop-up display in Figure 64 appears. It asks if you want to test the Universal Connection now. Selecting Yes causes Universal Connection to initiate a connection for testing purposes. No information is exchanged. A connection status window appears that indicates whether it was successful.



Universal Connection Wizard

Would you like to test the Universal Connection now?

Verify universal connection

Connection status:

```
Session job starting
Calling remote system
Exchanging information
LCP authentication
Starting TCP/IP communicatoins
LCP authentication
Profile active
Profile started successfully
```

Figure 64. Testing the connection

3.3.4 The definitions created in the Universal Connection Wizard

There are two groups of definitions that are created in the Universal Connection Wizard. One group is the VPN connection-related definitions. The other group is the connection profile and its line definitions for the PPP dial-up any ISP connection.

3.3.4.1 VPN connection related definitions

Table 7 shows a summary of the VPN connection-related definitions created in the Universal Connection Wizard.

Table 7. Summary of VPN connection-related definitions created in the wizard

Definition name	Definition details
IKE key policies	It specifies the Internet Key Exchange Policies (IKE) key details: - Preshared key name - Key encryption algorithm
QIBMSERVICE51 - Security Data policies	It specifies the Encapsulating Security Payload (ESP) encryption details: - ESP mode (Tunnel or Transfer) - Encryption Algorithm
QIBMSERVICE51 - Secure Connection definition	It specifies the VPN connection details: - Remote key server IP address - Local IP address - Remote IP address - Services ports and protocol
QTOCL2TP - L2TP (virtual line) initiator	It specifies the Layer-2 Tunneling Protocol (L2TP) initiator details. - VPN endpoint IP address - IPSec protection connection group name - Link definitions - Authentication PAP/CHAP-MD5, user ID and password - DNS

The details of each definition described in Table 7 are as follows:

- **IKE key policies**

  You can find the IKE definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Internet Key Exchange Policies**.

- **QIBMSERVICE51 - Security Data policies and Secure connection definition**

  There are two QIBMSERVICE51 definitions created by the wizard. One is the IP Security Data Policies definition and the other is the Secure connection definition. You can access the Security Data Policies definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Data Policies**.

The values of the QIBMSERVICE51 Security Data Policies created in the wizard are shown in Table 8.

Table 8. Values of the IBMSERVICE51 Security Data Policies created in the wizard

Parameters	Values
General - Name - Description - Use Diffie-Hellman perfect forward secrecy - Diffie-Hellman group	 QIBMSERVICE51 IBM UNIVERSAL CONNECTION Check the use Diffie-Hellman perfect forward secrecy Group 1 (768-bit MODP)
Proposals - Protocol - Encapsulation - Key expiration expire after - Key expiration expire at size limit - Authentication algorithm - Encryption algorithm	 ESP transfer mode 15 minutes No size limit MD5 DES-CBC

You can access the Secure connection definition by performing the following steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **IP Policies**.

c. Expand **Virtual Private Networking**.

d. Expand **Secure Connections**.

e. Click **All Connections**.

The values of the QIBMSERVICE51 Secure connection definition created in the wizard are shown in Table 9.

Table 9. Values of the IBMSERVICE51 Secure Connections definition created by the wizard

Parameters	Values
General - Remote key server Identifier type - IP address - Start when the VPN server starts - Start on-demand	 IP version 4 address Assigned by wizard Not selected Not selected
Local addresses - Identifier type - Identifier	 PPP profile Name ISPDIAL
Remote addresses - Identifier type - Identifier	 IP version 4 address Assigned by wizard
Services - Local port - Remote port - Protocol	 1701 1701 UDP

- **QTOCL2TP - L2TP (virtual line) initiator**

  QTOCL2TP is the L2TP (virtual line) initiator. You can access the QTOCL2TP definition by performing the following steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **Remote Access Services**.

c. Click **Originator Connection Profiles**.

The values of the QTOCL2TP definition created in the wizard are shown in Table 10.

Table 10. Values of the QTOCL2TP definition created by the wizard

Parameters	**Values**
General - Name - Description - Protocol type - Mode type	 QTOCL2TP Created by Universal Connection Wizard PPP L2TP (virtual line) - initiator
Connection - Link configuration type of line service - Virtual line name - Remote tunnel endpoint IP address - Requires IPSec protection connection group name - Line inactivity time-out	 Virtual Line (L2TP) QTOCL2TP Assigned by wizard QIBMSERVICE51 600
QTOCL2TP Link definition General - Name - Description - Mode type Link - Bandwidth reservation - Maximum frame size - Enable packet sequence numbering - Activate tunnel keep alive Limits - LCP authentication Authenticate remote peer periodically Maximum authentication attempts - LCP configuration Configuration retry timer Maximum configuration failures Maximum configuration requests Maximum termination requests - Recovery limits Count limit Maximum time-out Authentication - Local host name Remote system L2TP tunnel authentication - Require this iSeries server to verify the identity of the remote L2TP terminator system	 QTOCL2TP Created by Universal Connection Wizard L2TP (virtual line) - initiator 115200 1500 Not selected Not selected Not selected 8 5 5 10 10 2 10 as026 Not selected

Parameters	Values
Authentication Local system identification - Allow the remote system to verify the identity of this iSeries server - Authentication protocol to use - Remote system identification require this iSeries server to verify the identity of the remote system	Selected Require encrypted password (CHAP-MD5) Not selected
TCP/IP settings - Local IP address - Remote IP address - Routing - Hide addresses (full masquerading)	Assigned by remote system Assigned by remote system Define additional static routes Not selected
QTOCL2TP routing	IP addresses will vary based on the iSeries server location
DNS - Domain name server	Do not use
Other Subsystem - Enter the name of the subsystem in which to run name Connection - Use connection script - Script ASCII coded character set identifier	QSYSWRK Not selected 819

3.3.4.2 Connection profile and the line definition

Table 11 shows the definition summary of the ISPDIAL connection profile and the QESPPLIN line definition created by the wizard.

Table 11. Summary of definitions created in the wizard

Definition name	Summary
ISPDIAL	Connection profile for PPP dial-up ISP - Link name - Authentication - TCP/IP settings - DNS
QESPPLIN	Line definition for ISPDIAL - Physical resource name - Connection parameter such as RTS/CTS - Link speed - Limits timers for this line - Modem description

The details of each definition described in Table 11 are as follows:

- **ISPDIAL - PPP connection profile**

  ISPDIAL is the PPP connection profile. You can reach the ISPDIAL definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Click **Originator Connection Profiles**.

c. Double-click **ISPDIAL**.

The values of the ISPDIAL definition are shown in Table 12.

Table 12. Values of the ISPDIAL definitions

Parameters	**Values**
General - Name - Description - Protocol type - Mode type	 ISPDIAL Created by Internet Setup wizard PPP Switched line-dial
Connection - Link configuration type of line service - Name - Enable multilink protocol - Remote phone numbers	 Single line QESPPLIN Not selected 123-4567
Authentication - Local system identification allow the remote system to verify the identity of the iSeries server - Authentication protocol to use - User name - Password - Remote system identification require this iSeries server to verify the identity of the remote system	 Selected Require unencrypted password (PAP) USER PASSWORD (invisible) Not selected
TCP/IP settings - Local IP address - Remote IP address - Routing - Hide addresses (full masquerading)	 Assigned by remote system Assigned by remote system A default route added by wizard Selected
DNS - Domain Name Server	 Dynamically assign
Other - Subsystem - Connection script use connection script - Script ASCII coded character set identifier	 QSYSWRK Not selected 819

- **QESPPLIN - Line definition**

  QESPPLIN is the Line definition for ISPDIAL. You can access the QESPPLIN definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Click **Originator Connection Profiles**.

  c. Double-click **ISPDIAL**.

  d. Select the **Connection** tab.

  e. Click **Open**.

The values of the QESPPLIN definition created in the wizard are shown in Table 13.

Table 13. Values of the QESPPLIN definition created by the wizard

Parameters	**Values**
General	
- Name	QESPPLIN
- Description	Created by Internet Setup wizard
- Resource	CMN05 (2771)
- Interface type	(gray out)
- Mode type	Switched Line - Dial
- Framing	(gray out)
- Make available at restart	Not selected
Connection	
- Dial command type	AT command set
- Connections allowed	Dial
- Send V.25 command to set modem to asynchronous mode	Not selected
- Use flow control (RTS/CTS)	Selected
- CTS timeout	25 seconds
- Inactivity timeout	Not selected
Link	
- Line speed	115200
- Maximum frame size	2048
- Message queue name	Use system value
Limits	
- LCP authentication	
Authenticate remote peer periodically	Not selected
Maximum authentication attempts	8
- LCP configuration	
Configuration retry timer	5
Maximum configuration failures	5
Maximum configuration requests	10
Maximum termination requests	2
- Recovery limits	
Use system value	Not selected
Limits count limit	2
Time interval	5
Modem	56 Kbps Internal Modem (9771 adapter)
- Initialization string	AT
- Reset string	ATZ
- Dial command	ATDT
- Answer command	ATS0=2
- Additional parameters	none
Additional parameters	none

3.4 PPP dedicated FT1/T1 configuration

Figure 65 shows the network configuration of PPP dedicated FT1/T1. If you have a leased FT1/T1 line and want to have a service connection with IBM, follow the procedure to create the PPP dedicated FT1/T1 configuration.

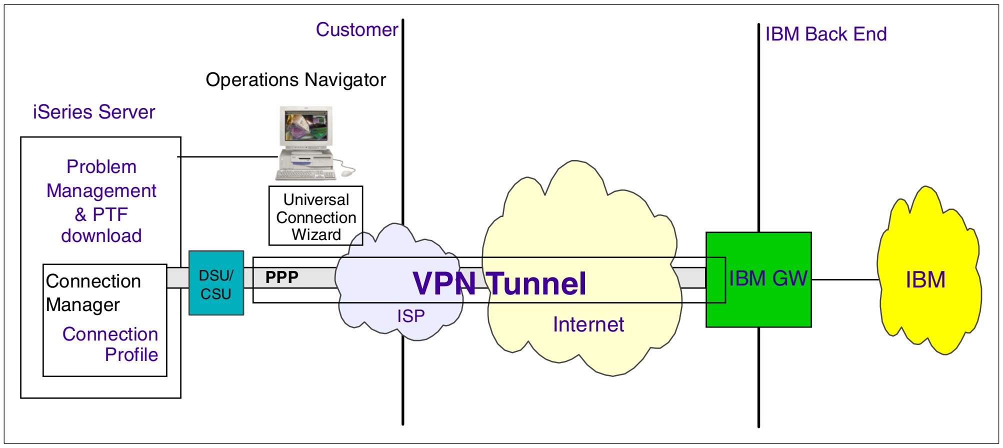


Figure 65. Network configuration of the PPP dedicated FT1/T1

3.4.1 Planning worksheet for the dedicated FT1/T1 configuration

Figure 66 shows the sample network configuration in this section.

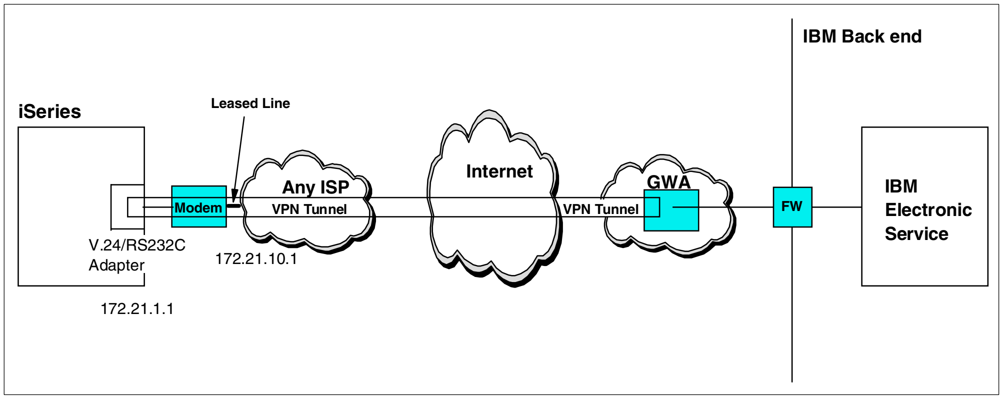


Figure 66. Dedicated FT1/T1 network configuration

Complete the iSeries server planning worksheets as shown in Table 14. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 14. AS026 Dedicated FT1/T1 configuration - Customer information

The customer information to create a dedicated FT1/T1 configuration	Scenario answers
What is the service contact information? - Company - Contact Name - Phone - Alternate Phone Number - Fax number	 IBM ITSO 111-111-1111 222-222-2222 333-333-3333
What is the service contact mailing address? - Street address - City/State - Country - ZIP code - National language version - Media for PTFs	 3605 Hwy 52 North Rochester/Minnesota United States 55901 English (2924) Automatic selection
Where is your server located? - Country - State or province	 United States Minnesota
What application are you using over this connection? - Electronic Customer Support (ECS) or - IBM Electronic Service Agent for AS/400	Electronic Customer Support
What type of connection are you using for your Universal Connection?	A dial-up connection using an Internet Service Provider
What is the connection profile name of the dedicated FT1/T1 Line that you are going to use for IBM Electronic Service? - Profile name	DEDICATED

If you haven't created the dedicated FT1/T1 connection profile and leased line definition, here are the sample configurations. DEDICATED is the sample connection profile name for the dedicated FT1/T1 connection as shown in Table 15. LEASED is the sample leased line definition as shown in Table 16. You also need information, from your ISP, to configure the DEDICATED connection profile. This chapter provides sample wizard displays for the DEDICATED and LEASED definition later.

Table 15. AS026 PPP dedicated FT1/T1 configuration: Line description

This is the customer information to create PPP dedicated FT1/T1 configuration	Scenario answers
What type of line service will you use for PPP dedicated FT1/T1 configuration? - Type of line service	Single line
What is the name of the PPP dedicated FT1/T1 configuration? - Name	DEDICATED
What is the Link name for this PPP dedicated FT1/T1 configuration? - Name	LEASED

This is the customer information to create PPP dedicated FT1/T1 configuration	**Scenario answers**
What is the hardware resource name that you are going to use for the link? - Hardware resource name	CMN06 F/C2720 V.24 Port Enhanced
Which framing do you choose for the link? - Framing name	Asynchronous (default)
What are the connection parameters? - Use flow control - CTS time-out value	Click **Use flow control** (default) 25 seconds (default)
What are the link parameters? - Line speed - Maximum frame size - Message queue name	115200 (default) 2048 (default) Use system value (default)
What are the limits parameters? - LCP authentication Maximum authentication counts - LCP configuration Configuration retry timer Maximum configuration failures Maximum configuration requests Maximum termination requests - Recovery limits Count limits Time interval	8 (default) 5 seconds (default) 5 (default) 10 (default) 2 (default) 2 (default) 5 minutes (default)
What is the modem type? - Modem name	IBM 7858
What are the security options? - Default authority to this line	QSYS new object authority
What is the optional parameter of your modem? - Additional parameter if needed	No additional parameter

Table 16. AS026 PPP dedicated FT1/T1 configuration: Information provided by your ISP

This is the information provided by your ISP to create PPP dedicated FT1/T1 configuration	**Scenario answers**
What are the local system identification parameters? - Allow the remote system to verify the identity of iSeries server - Authentication protocol to use - If you use PAP, what is the User ID and the password? - User ID - Password	Click **Allow** (default) PAP USER PASSWORD

This is the information provided by your ISP to create PPP dedicated FT1/T1 configuration	**Scenario answers**
What are the remote system identification parameters? - Require this iSeries server to verify the identity of the remote system	Not selected (default)
What are the TCP/IP settings? - Local fixed IP address - Remote fixed IP address - Routing - Hide addresses (full masquerading)	172.21.1.1 (Provided by your ISP) 172.21.10.1 (Provided by your ISP) See “Note” on page 68 Not selected (default)
What is the DNS server parameter? - IP address	172.21.8.1 (Provided by your ISP)
What are the Other parameters? - Use Connection scripts - Script ASCII coded character set identifier	Not selected (default) 819 (default)

3.4.2 Configuring a PPP dedicated FT1/T1 on AS026

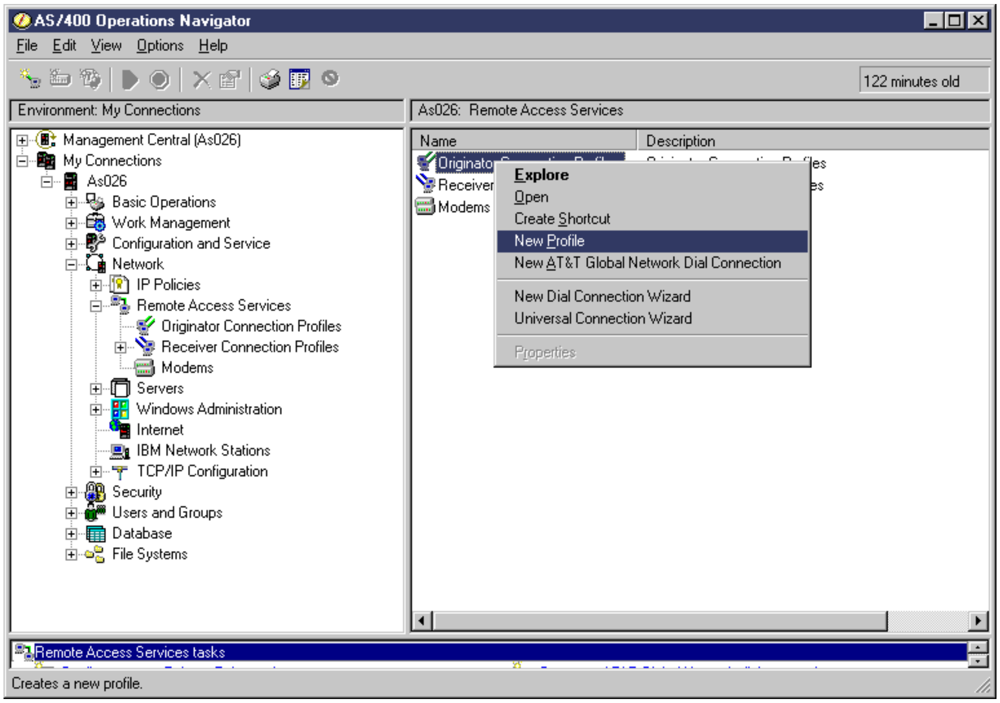
In this procedure, you perform the following tasks:

1. Create the FT1/T1 connection profile of DEDICATED and its line definition LEASED if your server doesn’t have the connection profile and its leased line definition for the IBM Electronic Support connection.
2. Create a PPP dedicated FT1/T1 ECS connection using the Universal Connection Wizard.
3. Test the connection.

3.4.2.1 Configuring the FT1/T1 connection profile and the leased line

Perform the following steps to configure the FT1/T1 connection profile DEDICATED and leased line definition LEASED. If you already have an FT1/T1 leased line definition and FT1/T1 connection profile, skip to step 20.

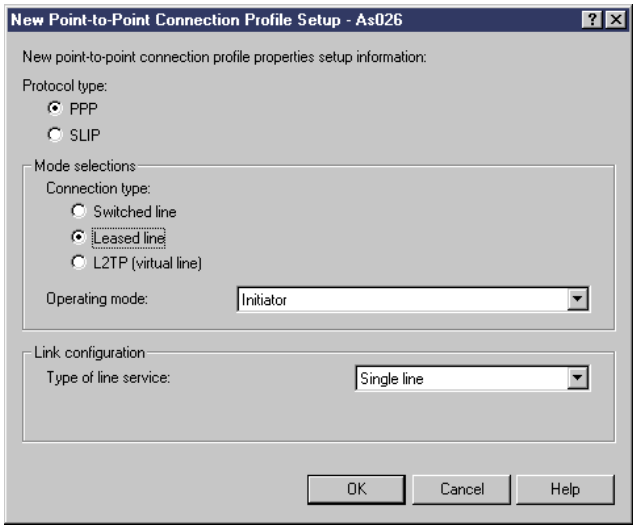
1. Start Operations Navigator from the desktop.
2. Expand the iSeries server (in this case, **AS026**). Sign on when prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **New Profile** as shown in Figure 67.


AS/400 Operations Navigator
File Edit View Options Help
122 minutes old
Environment: My Connections
Management Central (As026)
My Connections
As026
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profiles
Receiver Connection Profiles
Modems
Servers
Windows Administration
Internet
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
As026: Remote Access Services
Name
Description
Originator
Receiver
Modems
Explore
Open
Create Shortcut
New Profile
New AT&T Global Network Dial Connection
New Dial Connection Wizard
Universal Connection Wizard
Properties
Remote Access Services tasks

Creates a new profile.

Figure 67. New Profile

6. Click **PPP** for Protocol type and **Leased line** for Connection type. Choose **Single line** for Type of line service, and click **OK** as shown in Figure 68.



New point-to-point connection profile properties setup information:

Protocol type:
● PPP
○ SLIP

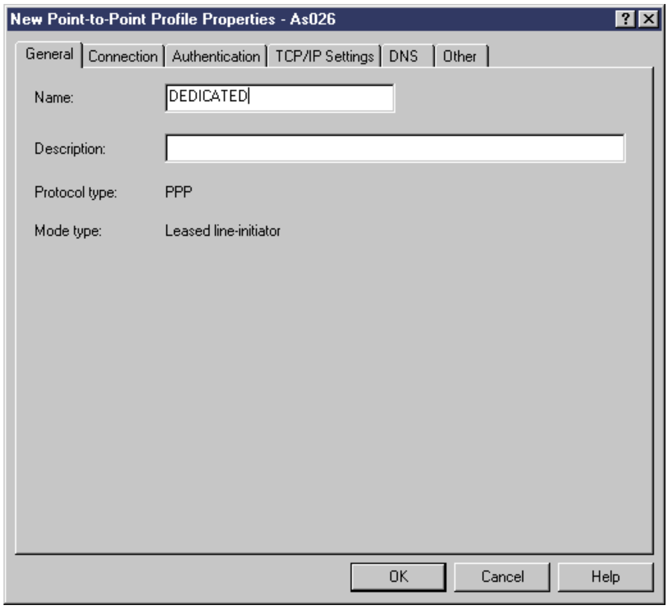
Mode selections
Connection type:
○ Switched line
● Leased line
○ L2TP (virtual line)

Operating mode: Initiator

Link configuration
Type of line service: Single line

Figure 68. New Point-to-Point Connection Profile Setup

7. On the New Point-to-Point Profile Properties display, click the **General** tab. Enter the connection name `DEDICATED` in the Name column and a description if required as shown in Figure 69.



New Point-to-Point Profile Properties - As026

Name: DEDICATED

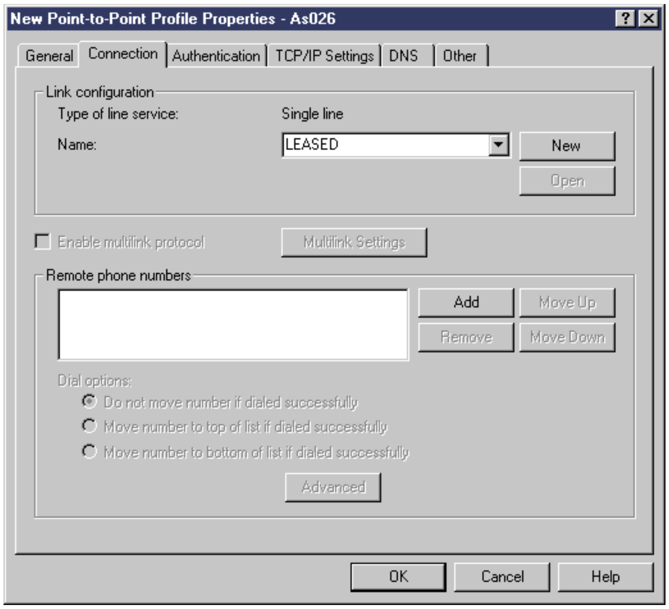
Description:

Protocol type: PPP

Mode type: Leased line-initiator

Figure 69. New Point-to-Point Profile Properties: General tab

8. Click the **Connection** tab. Enter the link name `LEASED` on the Name column as shown in Figure 70. Click **New**.



New Point-to-Point Profile Properties - As026

Link configuration

Type of line service: Single line

Name: LEASED

☐ Enable multilink protocol

Remote phone numbers

Dial options:

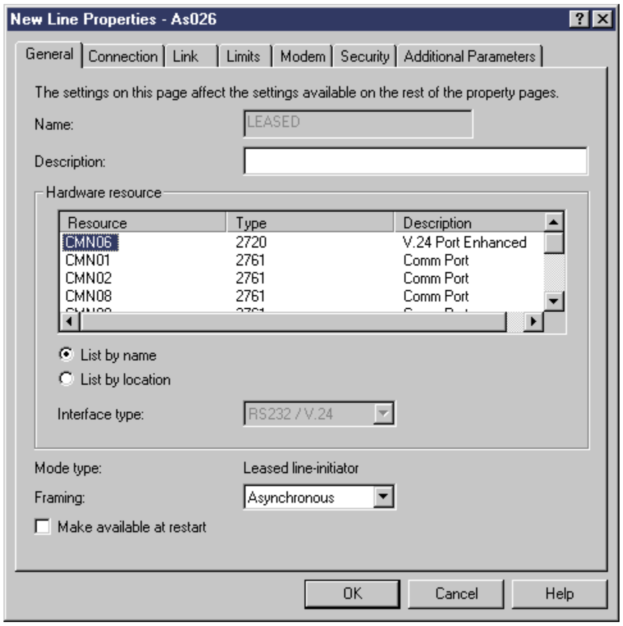
● Do not move number if dialed successfully

○ Move number to top of list if dialed successfully

○ Move number to bottom of list if dialed successfully

Figure 70. New Point-to-Point Profile Properties: Connection tab

9. Choose the physical resource for the PPP dedicated FT1/T1 connection. Choose either synchronous or asynchronous for Framing. Select **Make available at restart if required** as shown in Figure 71.



New Line Properties - As026

The settings on this page affect the settings available on the rest of the property pages.

Name: LEASED

Description:

Hardware resource

Resource	Type	Description
CMN06	2720	V.24 Port Enhanced
CMN01	2761	Comm Port
CMN02	2761	Comm Port
CMN08	2761	Comm Port

● List by name
○ List by location

Interface type: RS232 / V.24

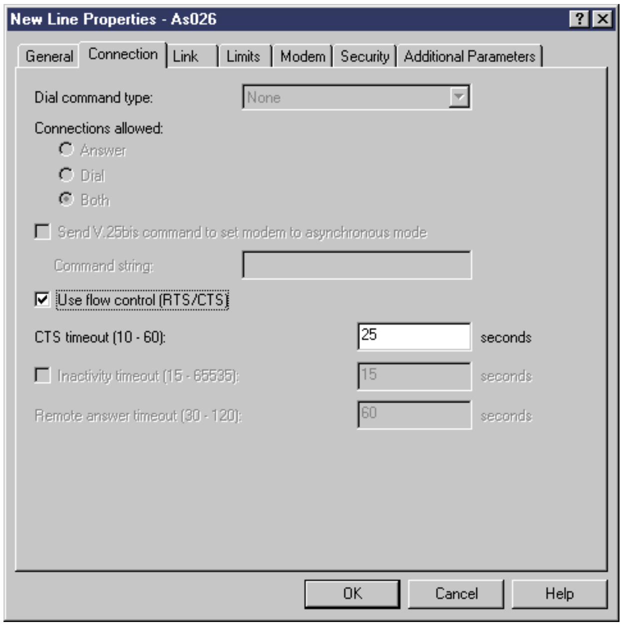
Mode type: Leased line-initiator

Framing: Asynchronous

□ Make available at restart

Figure 71. New Line Properties: General tab

10.Click the **Connection** tab. Choose the RTS/CTS control if required. Change the CTS time-out value, if required, as shown in Figure 72.



New Line Properties - As026

Dial command type: None

Connections allowed:
○ Answer
○ Dial
● Both

□ Send V.25bis command to set modem to asynchronous mode

Command string:

☑ Use flow control (RTS/CTS)

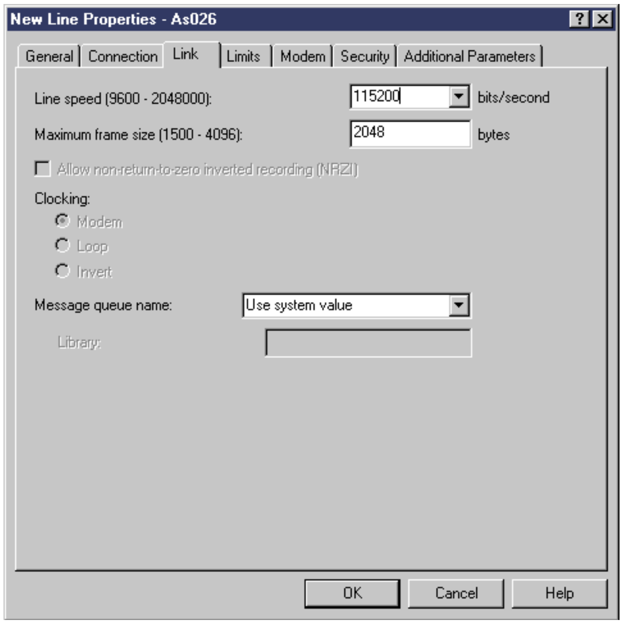
CTS timeout (10 - 60): 25 seconds

□ Inactivity timeout (15 - 65535): 15 seconds

Remote answer timeout (30 - 120): 60 seconds

Figure 72. New Line Properties: Connection tab

11.Click the **Link** tab. Choose the line speed for your provided connection speed. Enter `Maximum frame` as shown in Figure 73. If required, change the message queue name.



New Line Properties - As026

General | Connection | Link | Limits | Modem | Security | Additional Parameters

Line speed (9600 - 2048000): 115200 bits/second

Maximum frame size (1500 - 4096): 2048 bytes

□ Allow non-return-to-zero inverted recording (NRZI)

Clocking:

● Modem

○ Loop

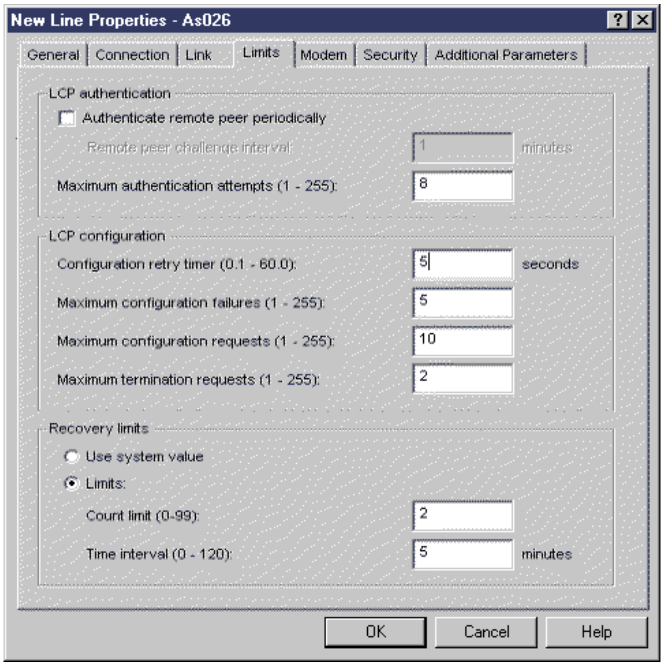
○ Invert

Message queue name: Use system value

Library:

Figure 73. New Line Properties: Link tab

12.Click the **Limits** tab. Change the default values if required as shown in Figure 74.



New Line Properties - As026

General | Connection | Link | Limits | Modem | Security | Additional Parameters

LCP authentication

□ Authenticate remote peer periodically

Remote peer challenge interval: 1 minutes

Maximum authentication attempts (1 - 255): 8

LCP configuration

Configuration retry timer (0.1 - 60.0): 5 seconds

Maximum configuration failures (1 - 255): 5

Maximum configuration requests (1 - 255): 10

Maximum termination requests (1 - 255): 2

Recovery limits

○ Use system value

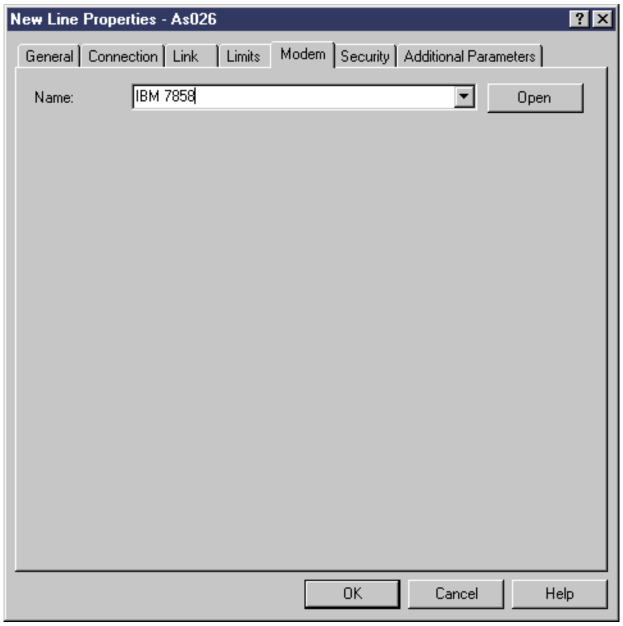
● Limits:

Count limit (0-99): 2

Time interval (0 - 120): 5 minutes

Figure 74. New Line Properties: Limits tab

13.Click the **Modem** tab. Choose the modem name as shown in Figure 75.

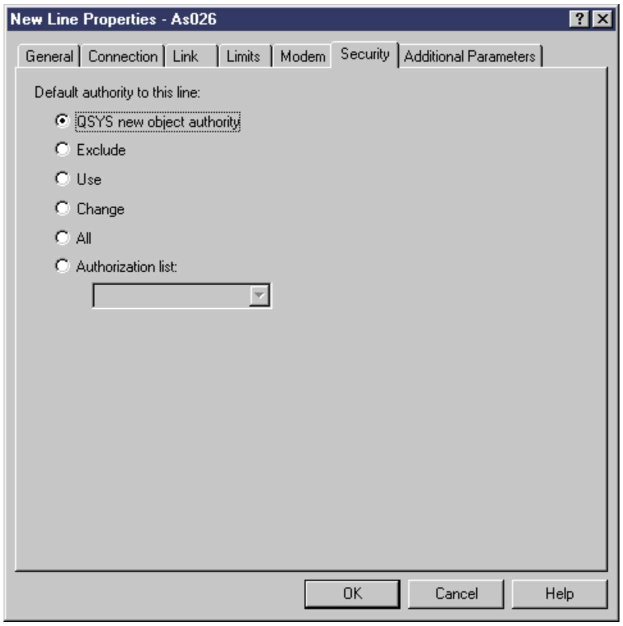


New Line Properties - As026

Name: IBM 7858

Figure 75. New Line Properties: Modem tab

14.Click the **Security** tab. Change the value for *Default authority to this line* if required as shown in Figure 76.



New Line Properties - As026

Default authority to this line:

● QSYS new object authority

○ Exclude

○ Use

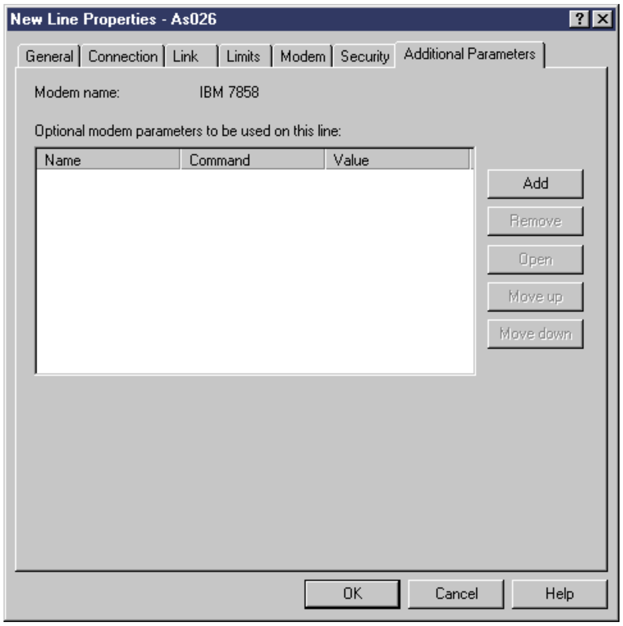
○ Change

○ All

○ Authorization list:

Figure 76. New Line Properties: Security tab

15.Click the **Additional Parameters** tab. If the modem needs optional parameters, add the parameter as shown in Figure 77.


New Line Properties - As026

Modem name: IBM 7858

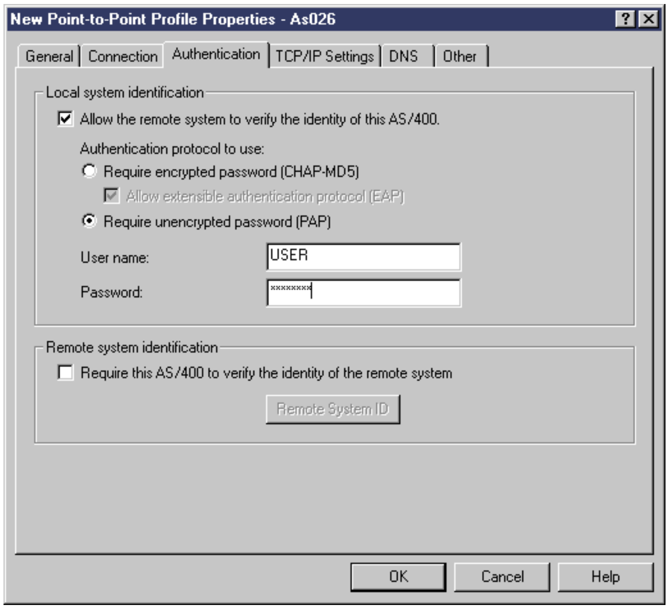
Optional modem parameters to be used on this line:

Name	Command	Value

Figure 77. New Line Properties: Additional Parameters tab

Click **OK**. You then return to the New Point-to-Point Profile Properties display.

16.Click the **Authentication** tab. Select **Allow the remote system to verify the identity of this AS/400** as shown in Figure 78. Click either **Require encrypted password (CHAP-MD5)** or **Require uncrypted password (PAP)** as required. Enter the PAP or CHAP user ID and password.


New Point-to-Point Profile Properties - As026

Local system identification

☑ Allow the remote system to verify the identity of this AS/400.

Authentication protocol to use:

○ Require encrypted password (CHAP-MD5)

☑ Allow extensible authentication protocol (EAP)

● Require unencrypted password (PAP)

User name: USER

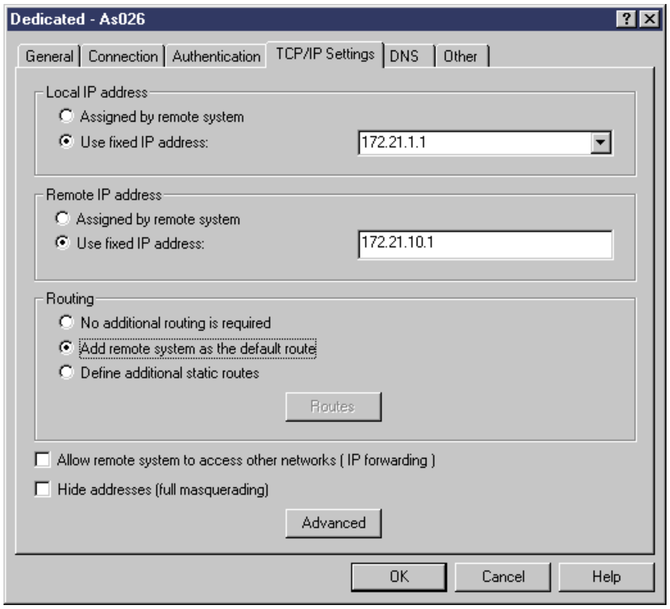
Password: ********

Remote system identification

☐ Require this AS/400 to verify the identity of the remote system

Figure 78. New Point-to-point Profile Properties: Authentication tab

17.Click the **TCP/IP Settings** tab. If prompted, enter the PAP or CHAP password again. Click **OK**. Enter the Local IP address and Remote IP address provided by your ISP as shown in Figure 79.



Local IP address

○ Assigned by remote system

● Use fixed IP address: 172.21.1.1

Remote IP address

○ Assigned by remote system

● Use fixed IP address: 172.21.10.1

Routing

○ No additional routing is required

● Add remote system as the default route

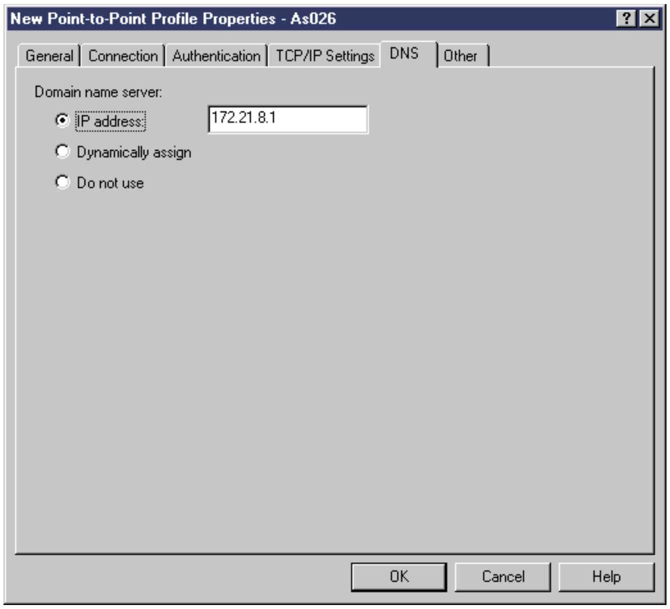
○ Define additional static routes

□ Allow remote system to access other networks (IP forwarding)

□ Hide addresses (full masquerading)

Figure 79. New Point-to-Point Profile Properties: TCP/IP Settings tab

18.Click the **DNS** tab. Select **IP address**. Enter the DNS IP address if needed as shown in Figure 80.



Domain name server:

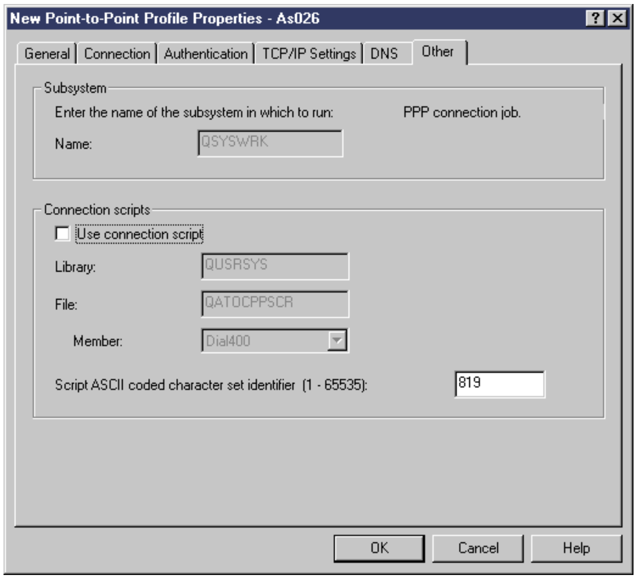
● IP address: 172.21.8.1

○ Dynamically assign

○ Do not use

Figure 80. New Point-to-Point Profile Properties: DNS tab

19.Click the **Other** tab. Change the default value for Script ASCII-coded character set identifier, if required, as shown in Figure 81. Click **OK**.



New Point-to-Point Profile Properties - As026

General | Connection | Authentication | TCP/IP Settings | DNS | Other

Subsystem

Enter the name of the subsystem in which to run: PPP connection job.

Name: QSYSWRK

Connection scripts

☐ Use connection script

Library: QUSRSYS

File: QATOCPPSCR

Member: Dial400

Script ASCII coded character set identifier (1 - 65535): 819

Figure 81. New Point-to-Point Profile Properties: Other tab

3.4.2.2 Using the Universal Connection Wizard

After creating the dedicated FT1/T1 configuration DEDICATED and leased line definition LEASED, create the ECS connection with the Universal Connection Wizard.

1. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **Universal Connection Wizard** as shown in Figure 82.

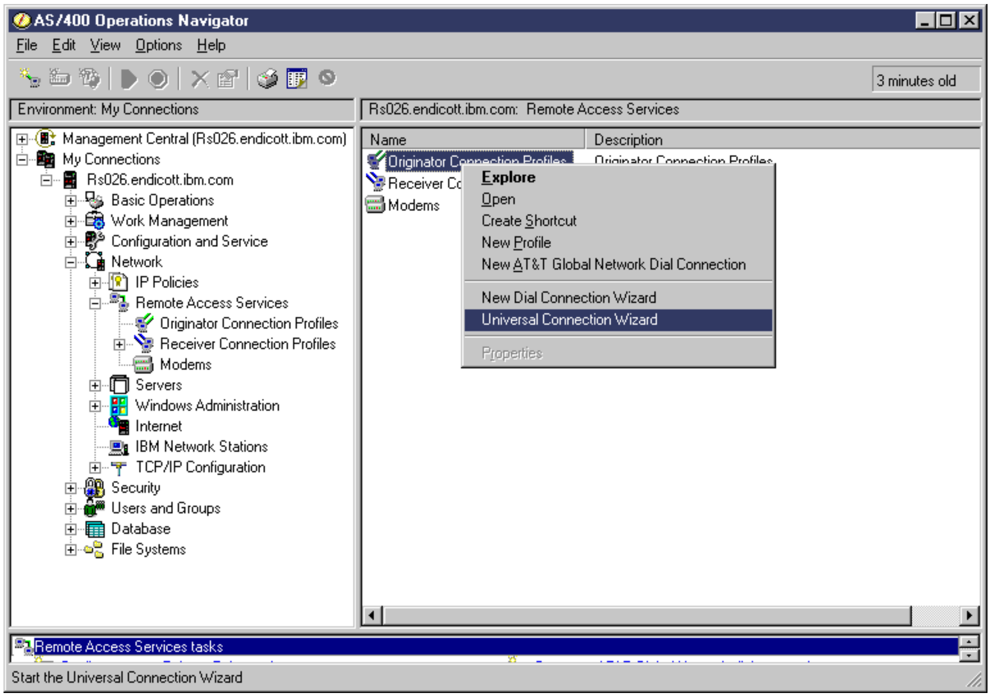
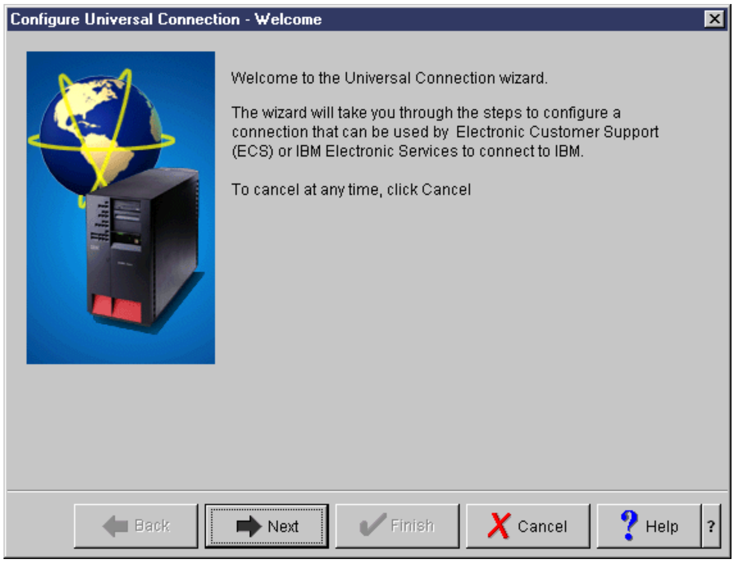

AS/400 Operations Navigator
File Edit View Options Help
3 minutes old
Environment: My Connections
Rs026.endicott.ibm.com: Remote Access Services
Management Central (Rs026.endicott.ibm.com)
My Connections
Rs026.endicott.ibm.com
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profiles
Receiver Connection Profiles
Modems
Servers
Windows Administration
Internet
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
Name
Description
Originator Connection Profiles
Receiver Co
Modems
Originator Connection Profiles
Explore
Open
Create Shortcut
New Profile
New AT&T Global Network Dial Connection
New Dial Connection Wizard
Universal Connection Wizard
Properties
Remote Access Services tasks
Start the Universal Connection Wizard

Figure 82. Universal Connection Wizard

2. Click **Next** in the Welcome dialog as shown in Figure 83.


Configure Universal Connection - Welcome

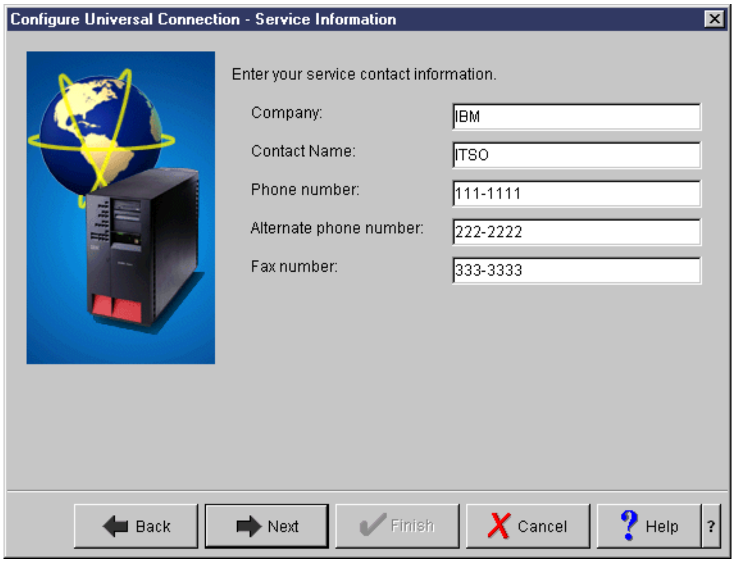
Welcome to the Universal Connection wizard.

The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 83. Configure Universal Connection - Welcome

3. Enter the service contact information as shown in Figure 84.

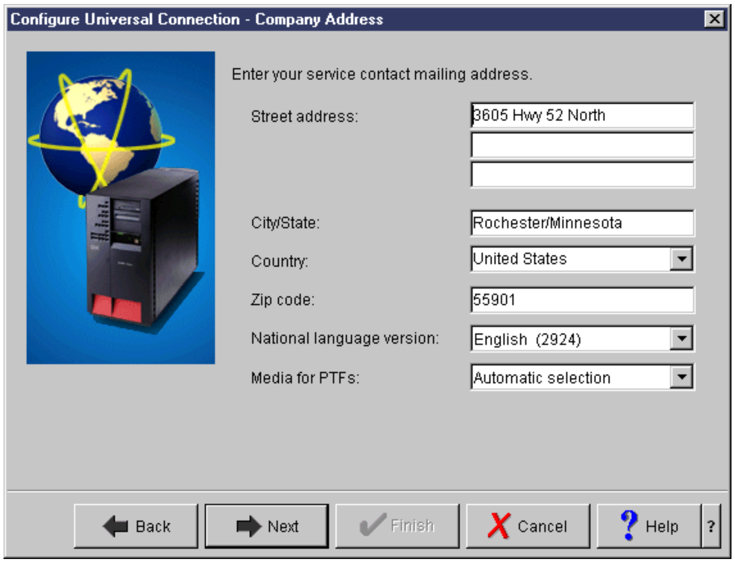

Configure Universal Connection - Service Information

Enter your service contact information.

Company:	IBM
Contact Name:	ITSO
Phone number:	111-1111
Alternate phone number:	222-2222
Fax number:	333-3333

Figure 84. Service contact information

4. Enter the service contact mailing address, national language version, and media for PTFs as shown in Figure 85.



Configure Universal Connection - Company Address

Enter your service contact mailing address.

Street address: 3605 Hwy 52 North

City/State: Rochester/Minnesota

Country: United States

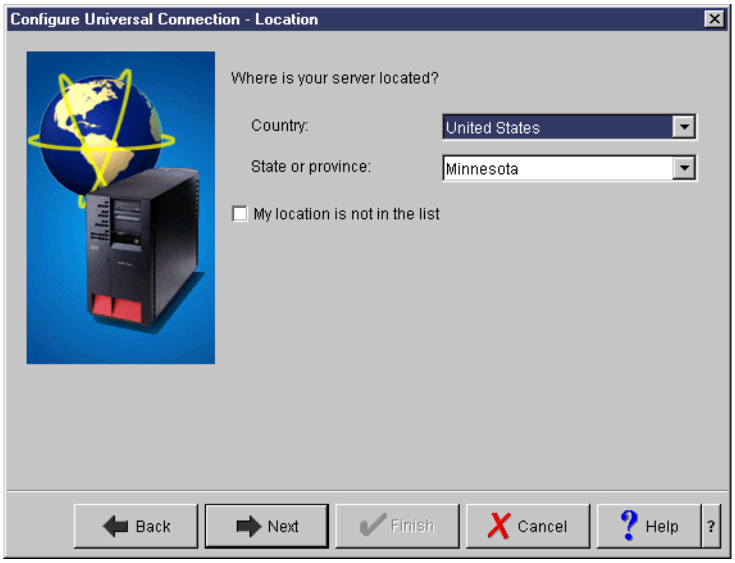
Zip code: 55901

National language version: English (2924)

Media for PTFs: Automatic selection

Figure 85. Service contact mailing address

5. Choose the country, state, or province as shown in Figure 86.



Configure Universal Connection - Location

Where is your server located?

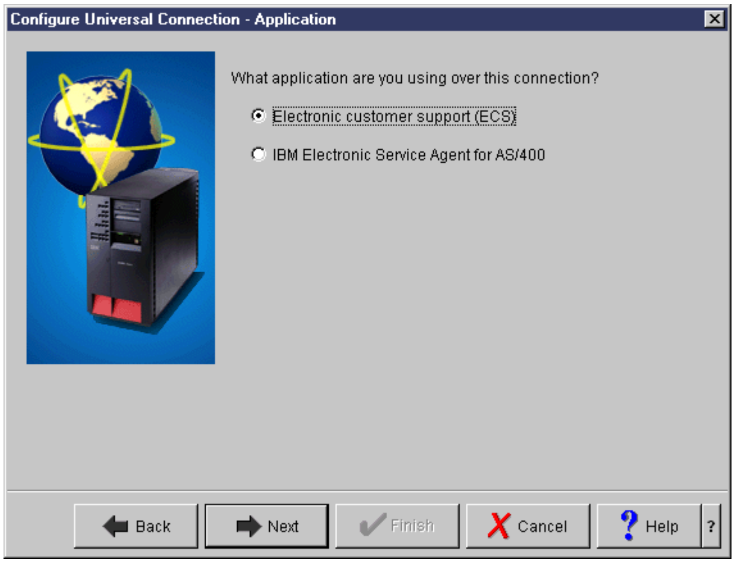
Country: United States

State or province: Minnesota

□ My location is not in the list

Figure 86. Country, state, or province

6. Select **Electronic Customer Support (ECS)** as shown in Figure 87.


Configure Universal Connection - Application

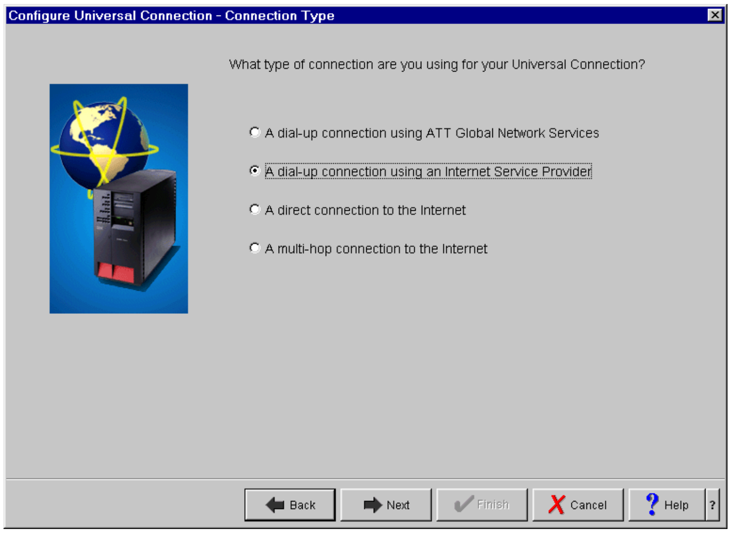
What application are you using over this connection?

● Electronic customer support (ECS)

○ IBM Electronic Service Agent for AS/400

Figure 87. Application selection

7. Select **A dial-up connection using an Internet Service Provider** as shown in Figure 88.


Configure Universal Connection - Connection Type

What type of connection are you using for your Universal Connection?

○ A dial-up connection using ATT Global Network Services

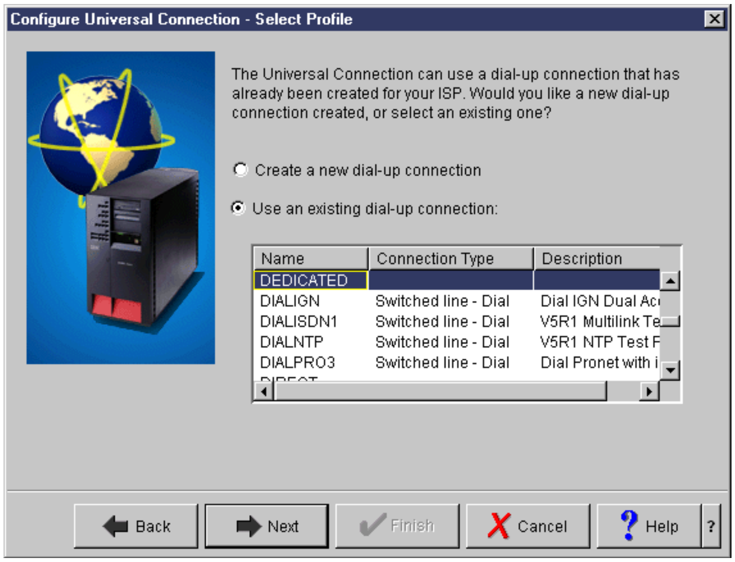
● A dial-up connection using an Internet Service Provider

○ A direct connection to the Internet

○ A multi-hop connection to the Internet

Figure 88. Connection type selection

8. Click **Use an existing dial-up connection**, and select the connection profile that you want to use for IBM Electronic Service shown in Figure 89. In this example, we choose **DEDICATED**.



Configure Universal Connection - Select Profile

The Universal Connection can use a dial-up connection that has already been created for your ISP. Would you like a new dial-up connection created, or select an existing one?

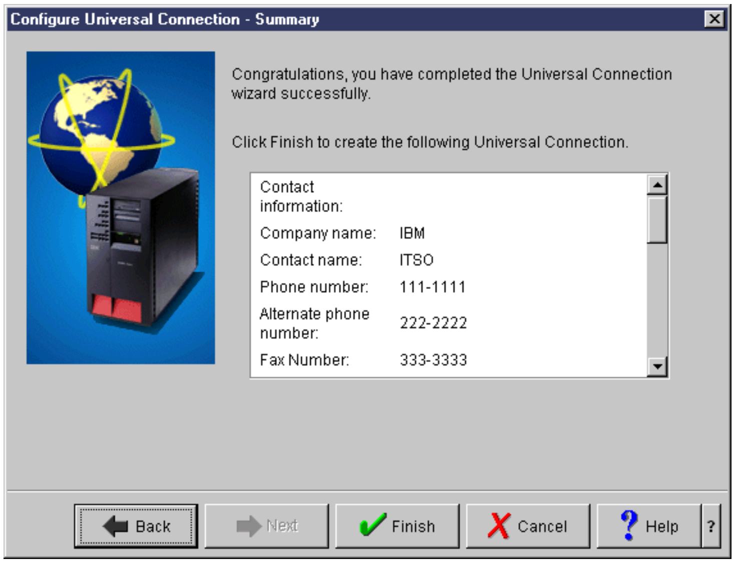
○ Create a new dial-up connection

● Use an existing dial-up connection:

Name	Connection Type	Description
DEDICATED		
DIALIGN	Switched line - Dial	Dial IGN Dual Ac
DIALISDN1	Switched line - Dial	V5R1 Multilink Te
DIALNTP	Switched line - Dial	V5R1 NTP Test F
DIALPRO3	Switched line - Dial	Dial Pronet with i
DIRECT		

Figure 89. Selecting a profile

9. Click **Finish** to create the definition shown in Figure 90.



Configure Universal Connection - Summary

Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

Contact information:

Company name:	IBM
Contact name:	ITSO
Phone number:	111-1111
Alternate phone number:	222-2222
Fax Number:	333-3333

Figure 90. Final display

10. After you click Finish, a pop-up window asks if you want to test the Universal Connection now. Selecting Yes causes Universal Connection to initiate a connection for testing purposes. No information is exchanged. A connection status window appears showing whether it was successful.

3.4.3 The definitions created in the wizard

There are two groups of definitions created in the wizard. One is a dedicated Ft1/T1 connection profile and leased line definition created by the new profile. The other is VPN connection definitions created by Universal Connection Wizard.

3.4.3.1 The definitions created in the new profile

Table 17 shows the definitions summary of FT1/T1 connection profile DEDICATED and FT1/T1 leased line definition LEASED.

Table 17. Summary of definitions created in the new profile

Definition name	Summary
DEDICATED	FT1/T1 connection profile - Link name - Authentication - TCP/IP settings - DNS
LEASED	Line definition for DEDICATED - Physical resource name - Connection parameter such as RTS/CTS - Link speed - Limits timers for this line - Modem description

The details of each definition described in Table 17 are listed here:

- **DEDICATED - FT1/T1 connection profile**

  DEDICATED is the FT1/T1 connection profile. You can reach the DEDICATED definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Click **Originator Connection Profiles**.

  The values of the DEDICATED definition created in the wizard are shown in Table 18.

Table 18. The values of the DEDICATED definition

Parameters	Values
General - Name - Protocol type - Mode type	 DEDICATED PPP Leased line -initiator
Connection - Type of the service - Name - Remote phone numbers	 Single line LEASED none
Authentication - Local system identification allow the remote system to verify the identity of iSeries system - Authentication protocol to use - User name - Password - Remote system identification require this iSeries server to verify the identity of the remote system	 Selected Require unencrypted password (PAP) USER PASSWORD Not selected
TCP/IP settings - Local IP address - Remote IP address - Routing - Hide addresses (full masquerading)	 172.21.1.1 172.21.10.1 Add remote system as the default value Not selected

Parameters	Values
DNS - Domain name server	 172.21.8.1
Other - Subsystem - Connection script Use connection script - Script ASCII coded character set identifier	 QSYSWRK Not selected 819

- **LEASED - line definition**

  LEASED is the line definition for DEDICATED. You can reach the LEASED definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Click **Originator Connection Profiles**.

  c. Double-click **DEDICATED**.

  d. Select the **Connection** tab.

  e. Click **Open**.

The values of the LEASED definition created in the wizard are shown in Table 19.

Table 19. Values of the LEASED definition

Parameters	Values
General - Name - Description - Resource - Mode type - Framing - Make available at restart	 LEASED none CMN06 (2720) Switched Line - Dial Asynchronous Not selected
Connection - Dial command type - Connections allowed - Use flow control (RTS/CTS) - CTS timeout	 none Both Selected 25
Link - Line speed - Maximum frame size - Message queue name	 115200 2048 Use system value
Limits - LCP authentication Authenticate remote peer periodically Maximum authentication attempts - LCP configuration Configuration retry timer Maximum configuration failures Maximum configuration requests Maximum termination requests - Recovery limits Use system value Limits count limit Time interval	 Not selected 8 5 5 10 2 Not selected 2 5

Parameters	Values
Modem - Name	IBM 7858
Security - Default authority to this line	QSYS new object authority
Additional parameters	none

3.4.3.2 The definitions created by the Universal Connection Wizard

Table 20 shows the summary of VPN connection definitions created in the Universal Connection Wizard.

Table 20. Summary of the definitions created in the wizard

Definition name	Definition details
IKE key policies	It specifies the Internet Key Exchange Policies (IKE) key details. - Preshared key name - Key encryption algorithm
QIBMSERVICE51 - Data policies	It specifies the Encapsulating Security Payload (ESP) encryption details: - ESP mode (Tunnel or Transfer) - Encryption algorithm
QIBMSERVICE51 - Connection definition	It specifies the virtual private network (VPN) connection details: - Remote key server IP address - Local IP address - Remote IP address - Services ports and protocol
QTOCL2TP - L2TP (virtual line) initiator	It specifies the Layer-2 Tunneling protocol (L2TP) initiator details. - VPN endpoint IP address - IPSec protection connection group name - Link definitions - Authentication PAP/CHAP-MD5, user ID and password - DNS

The details of each definition described in Table 20 are listed here:

- **IKE key policies**

  You can reach the IKE definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Internet Key Exchange Policies**.

- **QIBMSERVICE51 - Security Data policies and Secure connection definition**

  There are two QIBMSERVICE51 definitions created by the wizard. One is the IP Security Data Policies definition, and the other is the Secure connection definition. You can reach the IP Security definition by performing the following steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **IP Policies**.

c. Expand **Virtual Private Networking**.

d. Expand **IP Security Policies**.

e. Click **Data Policies**.

The values of the QIBMSERVICE51 IP Security Data Policies definition created in the wizard are shown in Table 21.

Table 21. Values of the IBMSERVICE51 Data Policies definition created in the wizard

Parameters	Values
General - Name - Description - Use Diffie-Hellman perfect forward secrecy - Diffie-Hellman group	 QIBMSERVICE51 IBM Universal Connection Check the Use Diffie-Hellman perfect forward secrecy Group 1 (768-bit MODP)
Proposals - Protocol - Encapsulation - Key expiration expire after - Key expiration expire at size limit - Algorithms authentication - Encryption algorithm	 ESP transfer mode 15 minutes No size limit MD5 DES-CBC

You can reach the Secure connection definition by performing the following steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **IP Policies**.

c. Expand **Virtual Private Networking**.

d. Expand **Secure Connections**.

e. Click **All Connections**.

The values of the QIBMSERVICE51 Secure connection definition created in the wizard are shown in Table 22.

Table 22. Values of the IBMSERVICE51 Secure Connections definition created by wizard

Parameters	Values
General - Remote key server Identifier type - IP address - Start when the VPN server starts - Start on-demand	 IP version 4 address Assigned by wizard Not selected Not selected
Local addresses - Identifier type - Identifier	 IP version 4 address 172.21.1.1 (depends on your ISP)
Remote addresses - Identifier type - Identifier	 IP version 4 address Assigned by wizard

Parameters	Values
Services - Local port - Remote port - Protocol	 1701 1701 UDP

- **QTOCL2TP - L2TP (virtual line) initiator**

  QTOCL2TP is the L2TP (virtual line) initiator. You can reach the QTOCL2TP definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **Remote Access Services**.

  c. Click **Originator Connection Profiles**.

  The values of the QTOCL2TP definition created in the wizard are shown in Table 23.

Table 23. Values of the QTOCL2TP definition created by wizard

Parameters	Values
General - Name - Description - Protocol type - Mode type	 QTOCL2TP Created by Universal Connection Wizard PPP L2TP (virtual line) - initiator
Connection - Link configuration type of line service - Virtual line name - Remote tunnel endpoint IP address - Requires IPSec protection connection group name - Line inactivity time-out	 Virtual Line (L2TP) QTOCL2TP Assigned by wizard QIBMSERVICE51 600

Parameters	Values
QTOCL2TP Link definition	
General	
- Name	QTOCL2TP
- Description	Created by Universal Connection Wizard
- Mode type	L2TP (virtual line) - initiator
Link	
- Bandwidth reservation	115200
- Maximum frame size	1500
- Enable packet sequence numbering	Not selected
- Activate tunnel keep alive	Not selected
Limits	
- LCP authentication	
Authenticate remote peer periodically	Not selected
Maximum authentication attempts	8
- LCP configuration	
Configuration retry timer	5
Maximum configuration failures	5
Maximum configuration requests	10
Maximum termination requests	10
- Recovery limits	
Count limit	2
Maximum time-out	10
Authentication	
- Local host name	as026
Remote system L2TP tunnel authentication	
- Require this iSeries server to verify the identity of the remote L2TP terminator system	Not selected
Authentication	
Local system identification	
- allow the remote system to verify the identity of this iSeries server	Selected
- Authentication protocol to use	Require encrypted password (CHAP-MD5)
- Remote system identification require this iSeries server to verify the identity of the remote system	Not selected
TCP/IP settings	
- Local IP address	Assigned by remote system
- Remote IP address	Assigned by remote system
- Routing	Define additional static routes
- Hide addresses (full masquerading)	Not selected
QTOCL2TP routing	IP address will vary based on the iSeries system location.
DNS	
- Domain name server	Do not use
Other	
Subsystem	
- Enter the name of the subsystem in which to run Name	QSYSWRK
Connection	
- Use connection script	Not selected
- Script ASCII coded character set identifier	819

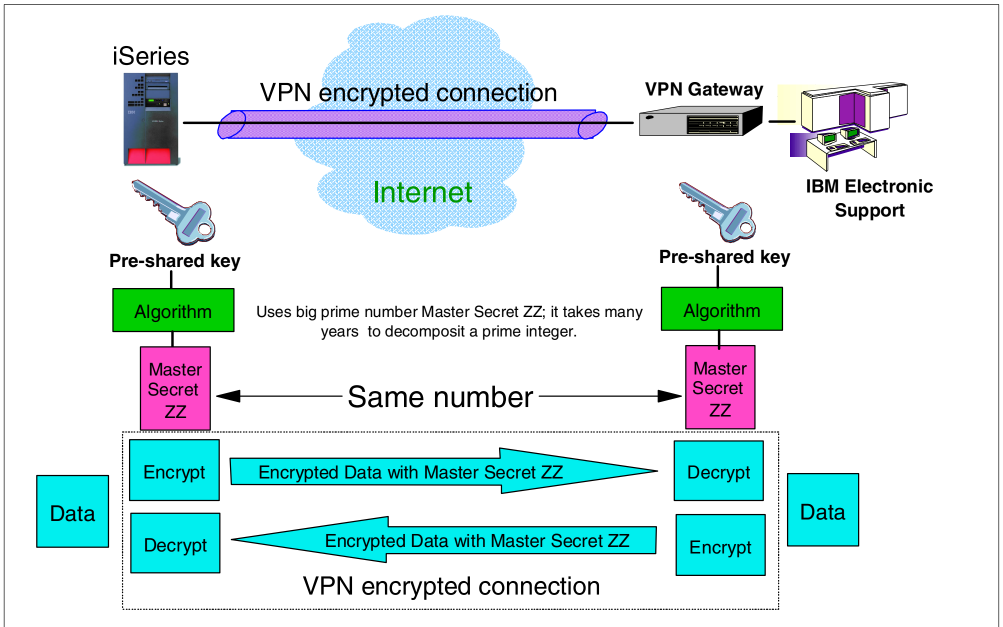
3.5 Security over a PPP dial-up to any ISP connection

The wizard creates the security-related definitions to establish encrypted safe reliable connections between your iSeries server and IBM Electronic Support. This section explains how the VPN connection works, how safe VPN connections can be established between your iSeries server and IBM Electronic Support, and how IP Packet filters work to protect your iSeries server from intrusion.

3.5.1 IBM Electronic Support connection using VPN

Figure 91 shows the overview of the IBM Electronic Support connection using a VPN-encrypted connection. The VPN uses a pre-shared key to authenticate your iSeries server and IBM Electronic Support. The pre-shared key is calculated using the same algorithm on both ends, so the calculated result is always the same. It is called *Master Secret ZZ*.

Master Secret is a big prime number. It would take many years to decompose a prime integer from the Master Secret ZZ. All data is encrypted with the Master Secret ZZ. This is the reason why the VPN connection is safe and reliable.



Using the same algorithm, Master Secret ZZ is calculated to same number on both ends.
In the VPN connection, all datas are encrypted with ZZ, and decrypted with ZZ on both ends.

Figure 91. IBM Electronic Support connection using VPN

The VPN connection is established in the sequence shown in Figure 92.

Internet Key Exchange (IKE) protocol authenticates your iSeries server with IBM Electronic Support. The IKE definition has IKE key details such as what authentication mode would be used (aggressive mode with pre-shared key authentication).

After the IKE authentication is completed, Encapsulating Security Payload (ESP) protocol provides the encrypted VPN connection between your iSeries server and the VPN gateway, which is located in the IBM site.

The QIBMSERVICE51 - Data policies definition has encryption details such as what encryption algorithm would be used and what Diffie-Hellman group would be used. The IP datagrams are encapsulated into the ESP encrypted payload, so the IP datagram information such as, source and destination IP address, protocol, port number, and data are all invisible.

The QIBMSERVICE51 - Secure connection definition has security details such as, what is the remote key server IP address and what is the local and remote address for the ESP connection. The QTOCL2TP definition has the L2TP profile such as what is the VPN endpoint IP address, what is the authentication user ID and password for CHAP-MD5 authentication, and routing IP addresses to which the encrypted IP datagrams could be routed.

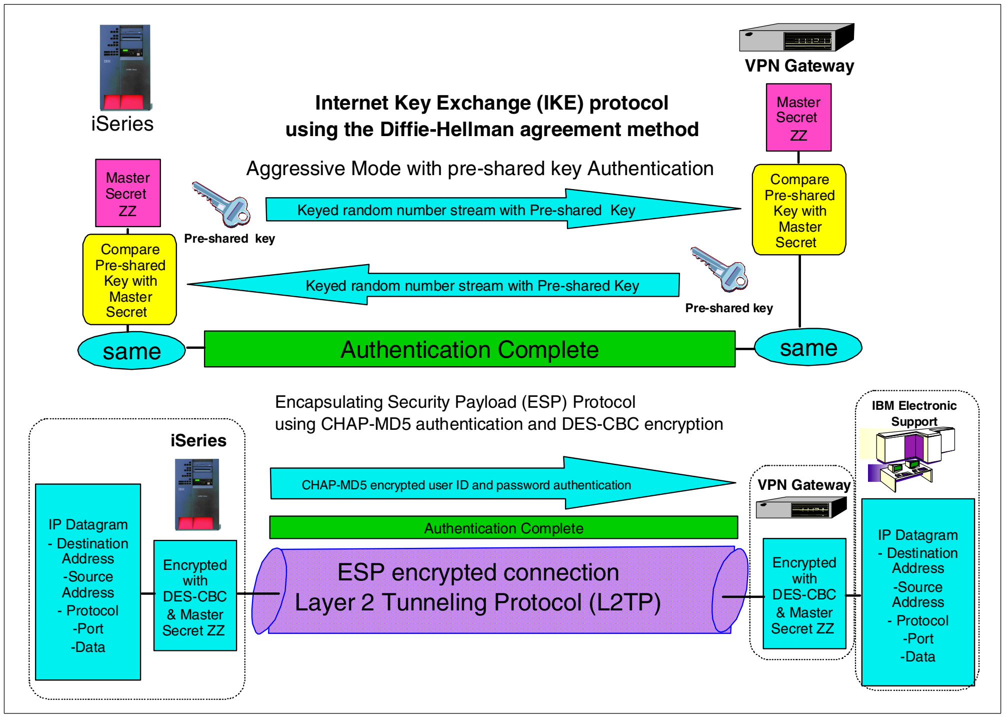
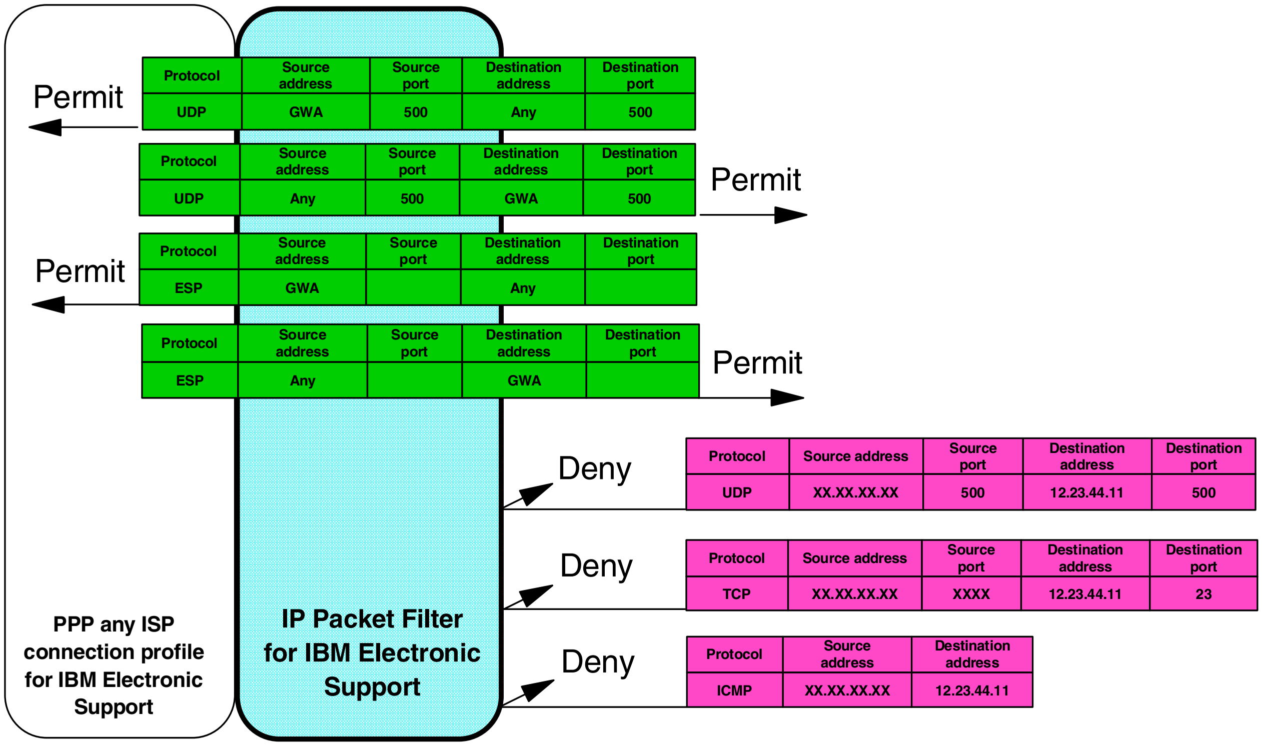

iSeries
VPN Gateway
Internet Key Exchange (IKE) protocol
using the Diffie-Hellman agreement method
Aggressive Mode with pre-shared key Authentication
Master Secret ZZ
Master Secret ZZ
Compare Pre-shared Key with Master Secret
Compare Pre-shared Key with Master Secret
Keyed random number stream with Pre-shared Key
Keyed random number stream with Pre-shared Key
Pre-shared key
Pre-shared key
same
Authentication Complete
same
Encapsulating Security Payload (ESP) Protocol
using CHAP-MD5 authentication and DES-CBC encryption
IBM Electronic Support
iSeries
VPN Gateway
CHAP-MD5 encrypted user ID and password authentication
Authentication Complete
IP Datagram - Destination Address -Source Address - Protocol -Port -Data
Encrypted with DES-CBC & Master Secret ZZ
ESP encrypted connection
Layer 2 Tunneling Protocol (L2TP)
Encrypted with DES-CBC & Master Secret ZZ
IP Datagram - Destination Address -Source Address - Protocol -Port -Data

Figure 92. VPN connection establishment sequences

3.5.2 IP packet filtering

The wizard also creates or modifies existing IP packet filter rules for the ISP dial-up connection profile. The IP packet filter watches each IP packet to see if the packet meets the condition described in the filter rules. The IP filter prevents the threat of intrusions in Active Attack cases and Denial of Service Attack cases. Figure 93 shows the IP packet filter rules.


Permit
Protocol | Source address | Source port | Destination address | Destination port
UDP | GWA | 500 | Any | 500
Protocol | Source address | Source port | Destination address | Destination port
UDP | Any | 500 | GWA | 500
Permit
Permit
Protocol | Source address | Source port | Destination address | Destination port
ESP | GWA | | Any |
Protocol | Source address | Source port | Destination address | Destination port
ESP | Any | | GWA |
Permit
Deny
Protocol | Source address | Source port | Destination address | Destination port
UDP | XX.XX.XX.XX | 500 | 12.23.44.11 | 500
Deny
Protocol | Source address | Source port | Destination address | Destination port
TCP | XX.XX.XX.XX | XXXX | 12.23.44.11 | 23
Deny
Protocol | Source address | Destination address
ICMP | XX.XX.XX.XX | 12.23.44.11
PPP any ISP connection profile for IBM Electronic Support
IP Packet Filter for IBM Electronic Support

IP Packet Filter Rules for IBM Electronic Support

Action	Direction	Protocol	Source address	Source port	Destination address	Destination port
Permit	Inbound	UDP	GWA	500	Any	500
Permit	Outbound	UDP	Any	500	GWA	500
Permit	Inbound	ESP	GWA		Any	
Permit	Outbound	ESP	Any		GWA	

Figure 93. IP Packet filter rules for IBM Electronic Support

Note

You can find the GWA IP address on the Web by going to:

`http://www.as400service.ibm.com`

Click the **Technical Databases** hyperlink. On the page that appears, click the **Registered Software Knowledge Base** hyperlink. A password is required to access this page. You must have a valid support line contract to access these articles. Once you enter your password, you can perform a search on **VPN Cisco Multi-Hop Connection Configuration** or **23300444**. This page provides the GWA IP address as an IBM gateway address.

The VPN encrypted connection and IP Packet filter work together to improve the Internet Security. To protect your server against Internet threats, we recommend you read Chapter 2, “Network security concepts and overview” on page 15, for more details about Internet security.

If a customer already defined the connection profile (for example, ISPDIAL) and the IP filter rules are already set on the connection profile, the wizard adds the required IP filter rules on the connection profile to allow the VPN connection for IBM Electronic Support to be established. If no IP filter rules existed prior to running the wizard, the rules that are generated do not deny traffic. It is your responsibility to ensure the correct denies are in place.

Chapter 4. Direct connection examples

This chapter explains how to configure the Universal Connection Wizard on the iSeries server to establish a service connection with IBM Electronic Support using a VPN-secured direct connection.

4.1 Direct connection support

Currently, an iSeries server contains a number of customer-to-IBM applications that use different connection mechanisms to provide an electronic exchange of system and customer information between the customer and IBM. Chapter 3, “Point-to-Point Protocol (PPP) connection examples” on page 37, explains the AGNS dial-up connection and any ISP dial-up/dedicated connection. These two connections need a dial-up or dedicated connection from the iSeries server to make a connection with IBM Electronic Support.

The direct connection is another way to make a connection with IBM Electronic Support. A direct connection support using a VPN secured connection was released in OS/400 V5R1. A direct connection needs either an Ethernet or a Token-Ring TCP interface before you can run the wizard to create the IBM Electronic Support connection. Your iSeries server must have a globally routable IP address. Using a wizard, customers can easily create the VPN secured direct connection definition.

This chapter describes three direct connection cases:

- **Frame relay direct connection to the Internet**

  A frame relay configuration needs a configured frame relay connection profile before you run the Universal Connection Wizard to create the IBM Electronic Support connection. The frame relay connection profile must be connected to the Internet through your frame relay network. The TCP interface of the frame relay must be active prior to running the Universal Connection Wizard. In the Universal Connection Wizard, you are asked to specify the already created TCP Interface that has the globally routable IP address for the frame relay connection.

- **Cable and DSL modems**

  Cable and DSL modems are becoming popular for delivering fast and easy-to-use Internet connections. In most cases, the IP address of the modem side would be automatically assigned by Dynamic Host Configuration Protocol (DHCP). A cable modem has a fixed IP address supplied by your ISP. A DSL modem has a fixed IP address supplied by your ISP. The TCP interface for the cable modem or DSL modem must be active prior to running the Universal Connection Wizard. You are asked to specify the TCP interface for the cable modem or the DSL modem in the Universal Connection Wizard. The Universal Connection Wizard creates all the required definitions for the IBM Electronic Support connection.

- **Router isolated access**

  If you have a router that is connected between your perimeter network and the Internet, a router isolated access configuration is a good example for you. The router has IP filter rules for both inbound and outbound IP traffic. You must configure your router to allow the inbound and outbound IP traffic for the IBM

Electronic Support connection. By simply specifying the TCP interface that you want to use for the IBM Electronic Support, the Universal Connection Wizard creates all required definitions for the IBM Electronic Support connection. The TCP interface that is connected to the router must be active prior to running the Universal Connection Wizard.

4.1.1 Prerequisites

The prerequisites for creating direct connection configurations using Universal Connection Wizard are listed here:

- The level of OS/400 should be V5R1M0. The GA PTF cumulative package must be applied.
- TCP/IP Connectivity Utilities (5722-TC1) is required.
- Crypto Access Provider 128-bit/56-bit for AS/400 (5722-AC3) or Crypto Access Provider 56-bit for AS/400 (5722-AC2) is required.
- Client Access Express V5R1M0 with Service Pack SI01037 or later is required to obtain the wizard.
- The iSeries server must have a globally routable IP address.
- Ensure the QRETSVRSEC system value is set to `1`. You can do this by issuing the Display System Value (DSPSYSVAL) command. If it is not set to “1”, issue the Change System Value (CHGSYSVAL) command.
- TCP/IP must be active. It can be started with the Start TCP/IP (STRTCP) command.
- The user configuring the wizard requires *ALLOBJ and *IOSYSCFG authority as part of their iSeries user profile.

4.2 Frame relay configuration

Frame relay is a communications networking protocol that defines how frames are routed through a fast-packet network based on the address field in the frame. Frame relay takes advantage of the reliability of data communications networks to minimize the error checking done by the network nodes. This provides a packet-switching protocol similar to, but much faster than, X.25.

Figure 94 shows the network configuration of frame relay. If you have a frame relay line that has a fixed IP address and you want to have a service connection with IBM, follow the procedure to create the frame relay configuration.

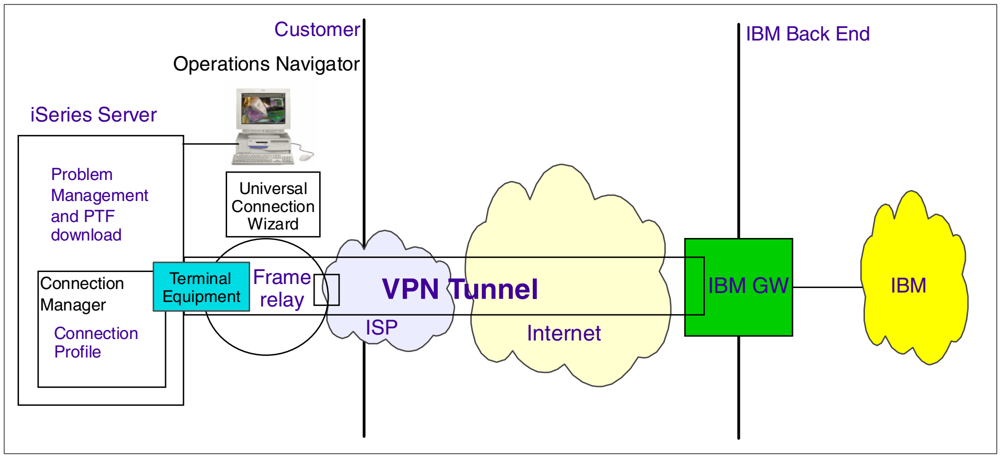


Figure 94. Network configuration using frame relay

4.2.1 Planning worksheet for a direct frame relay configuration

Figure 118 shows the sample network configuration in this section.

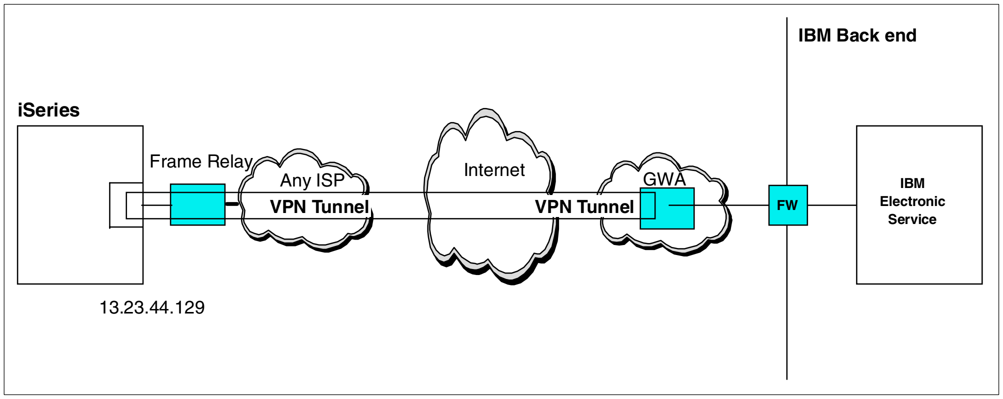


Figure 95. Frame relay network configuration

Complete the iSeries server planning worksheets as shown in Table 24. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 24. AS026 Frame relay configuration: Customer information (Part 1 of 2)

Customer information to create a frame relay connection	Scenario answers
What is the service contact information? - Company - Contact name - Phone - Alternate phone number - Fax number	 IBM ITSO 111-111-1111 222-222-2222 333-333-3333

Customer information to create a frame relay connection	Scenario answers
What is the service contact mailing address? - Street address - City/state - Country - ZIP code - National language version - Media for PTFs	 3605 Hwy 52 North Rochester/Minnesota United States 55901 English (2924) Automatic selection
Where is your server located? - Country - State or province	 United States Minnesota
What application are you using over this connection? - Electronic Customer Support (ECS) or - IBM Electronic Service Agent for AS/400	 Electronic Customer Support
What type of connection are you using for your Universal Connection?	A direct connection to the Internet
What is the IP address and interface type for the frame relay? - IP address - Interface type	 13.23.44.129 Frame relay

4.2.2 Configuring a direct frame relay connection on AS026

In this procedure, you perform the following tasks:

1. Create the frame relay interface and line configuration.
2. Create a frame relay configuration using UVC.
3. Test the connection.

4.2.2.1 Creating a frame relay interface and line configuration

If you have no configuration for the frame relay interface, follow these steps to configure one:

1. Complete the iSeries server planning worksheets as shown in Table 25. The planning worksheets allow you to gather all the configuration data before the actual implementation.

Table 25. AS026 Direct frame relay configuration: Customer information (Part 2 of 2)

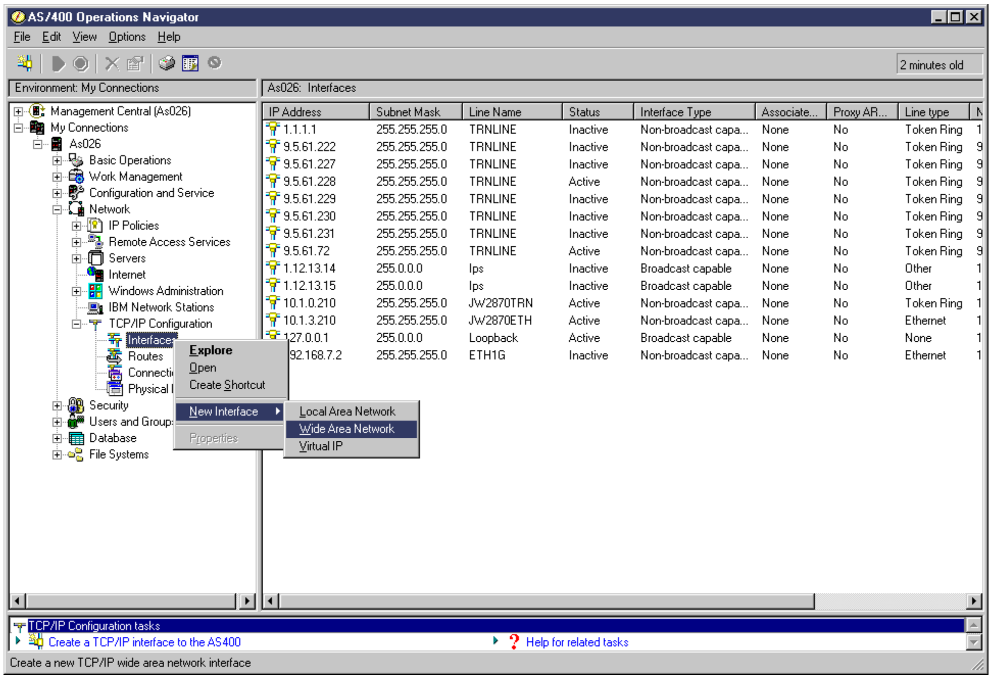
Customer information to create a frame relay configuration	Scenario answers
What is the new frame relay network interface name?	IBMESP
What hardware resource are you going to use for the frame relay network interface? - Hardware resource name - Physical interface - Line speed	 CMN06 *V35 1544000
What is the new line definition name? - Line definition name	 IBMESPLIN

Customer information to create a frame relay configuration	**Scenario answers**
What is the data link connection identifier (DLCI) for the network interface?	10
What is the IP address for the frame relay interface? (**Note**: Must be a globally routable address) - IP address - Subnet mask	13.23.44.129 255.255.255.252

2. On the Operations Navigator display, expand **Network**.

3. Expand **TCP/IP Configuration**.

4. Right-click **Interfaces**. On the pull-down menu, choose **New Interface**. On the next pull-down menu, select **Wide Area Network** as shown in Figure 96.

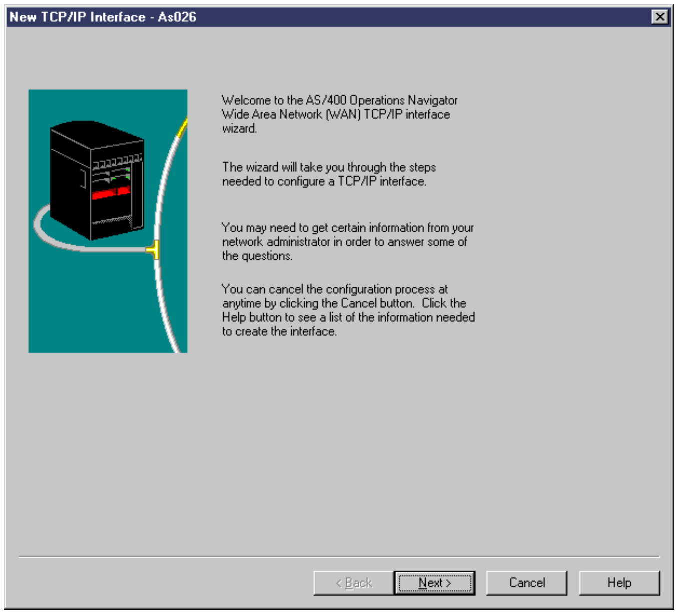


IP Address	Subnet Mask	Line Name	Status	Interface Type	Associate...	Proxy AR...	Line type	N
1.1.1.1	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring	1
9.5.61.222	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring	9
9.5.61.227	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring	9
9.5.61.228	255.255.255.0	TRNLINE	Active	Non-broadcast capa...	None	No	Token Ring	9
9.5.61.229	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring	9
9.5.61.230	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring	9
9.5.61.231	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring	9
9.5.61.72	255.255.255.0	TRNLINE	Active	Non-broadcast capa...	None	No	Token Ring	9
1.12.13.14	255.0.0.0	Ips	Inactive	Broadcast capable	None	No	Other	1
1.12.13.15	255.0.0.0	Ips	Inactive	Broadcast capable	None	No	Other	1
10.1.0.210	255.255.255.0	JW2870TRN	Active	Non-broadcast capa...	None	No	Token Ring	1
10.1.3.210	255.255.255.0	JW2870ETH	Active	Non-broadcast capa...	None	No	Ethernet	1
127.0.0.1	255.0.0.0	Loopback	Active	Broadcast capable	None	No	None	1
92.168.7.2	255.255.255.0	ETH1G	Inactive	Non-broadcast capa...	None	No	Ethernet	1

Create a new TCP/IP wide area network interface

Figure 96. New Interface display

5. The New TCP/IP Interface display (Figure 97) appears. Click **Next** on this panel to continue.


New TCP/IP Interface - As026

Welcome to the AS/400 Operations Navigator Wide Area Network (WAN) TCP/IP interface wizard.

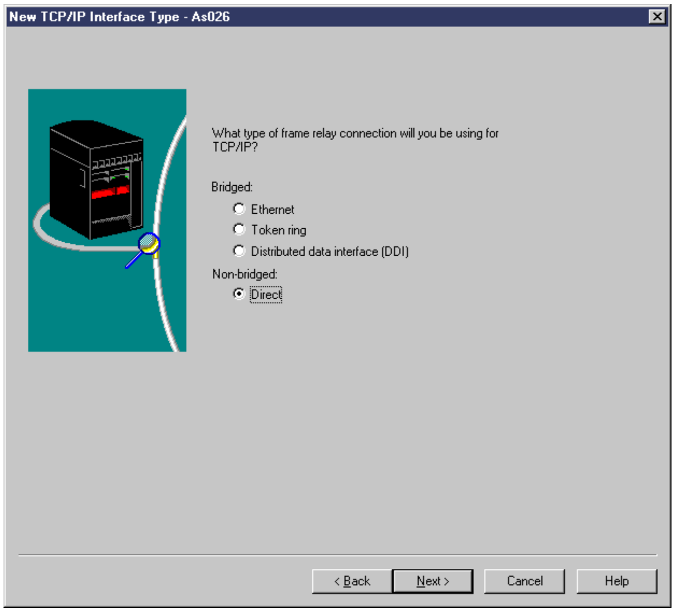
The wizard will take you through the steps needed to configure a TCP/IP interface.

You may need to get certain information from your network administrator in order to answer some of the questions.

You can cancel the configuration process at anytime by clicking the Cancel button. Click the Help button to see a list of the information needed to create the interface.

Figure 97. New TCP/IP Interface display

6. On the New TCP/IP Interface Type (Figure 98) display, choose **Non-bridged Direct**. Click **Next** to continue.


New TCP/IP Interface Type - As026

What type of frame relay connection will you be using for TCP/IP?

Bridged:

○ Ethernet

○ Token ring

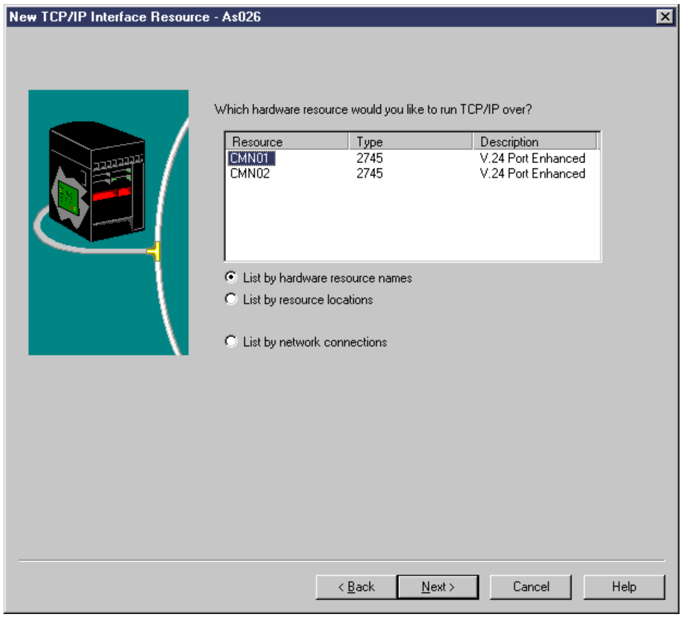
○ Distributed data interface (DDI)

Non-bridged:

● Direct

Figure 98. New TCP/IP Interface Type display

7. On the TCP/IP Interface Resource display (Figure 99), choose a resource name (in this example, choose **CMN01**). Click **Next** to continue.



New TCP/IP Interface Resource - As026

Which hardware resource would you like to run TCP/IP over?

Resource	Type	Description
CMN01	2745	V.24 Port Enhanced
CMN02	2745	V.24 Port Enhanced

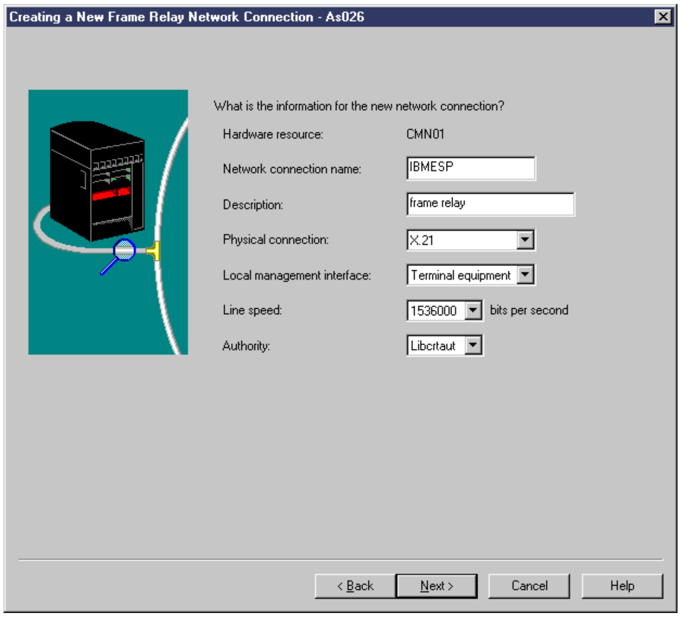
● List by hardware resource names

○ List by resource locations

○ List by network connections

Figure 99. New TCP/IP Interface Resource display

8. On the Creating a New Frame Relay Network Connection display (Figure 100), enter a network connection name (in this example, enter `IBMESP`). Enter a description (in this example, enter `frame relay`). Choose the physical connection (in this example, choose **X.21**). Click **Next** to continue.



Creating a New Frame Relay Network Connection - As026

What is the information for the new network connection?

Hardware resource: CMN01

Network connection name: IBMESP

Description: frame relay

Physical connection: X.21

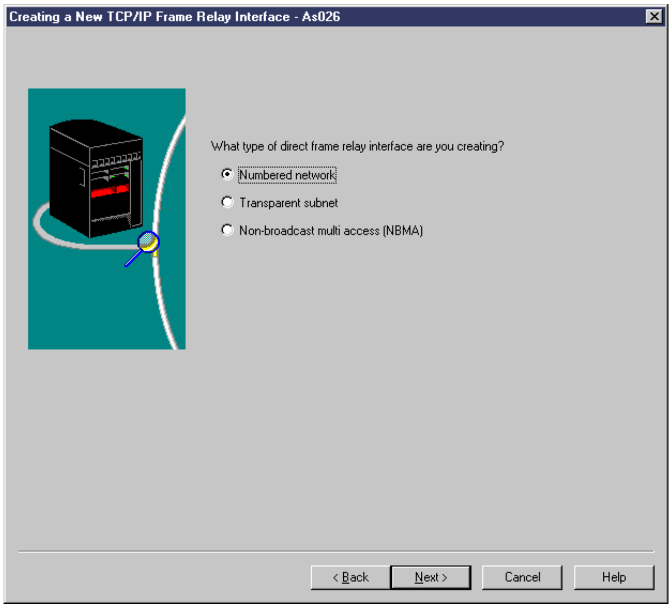
Local management interface: Terminal equipment

Line speed: 1536000 bits per second

Authority: Libcrtaut

Figure 100. Creating a New Frame Relay Network Connection display

9. On the New TCP/IP Frame Relay Interface display (Figure 101), choose **Numbered Network**. Click **Next**.



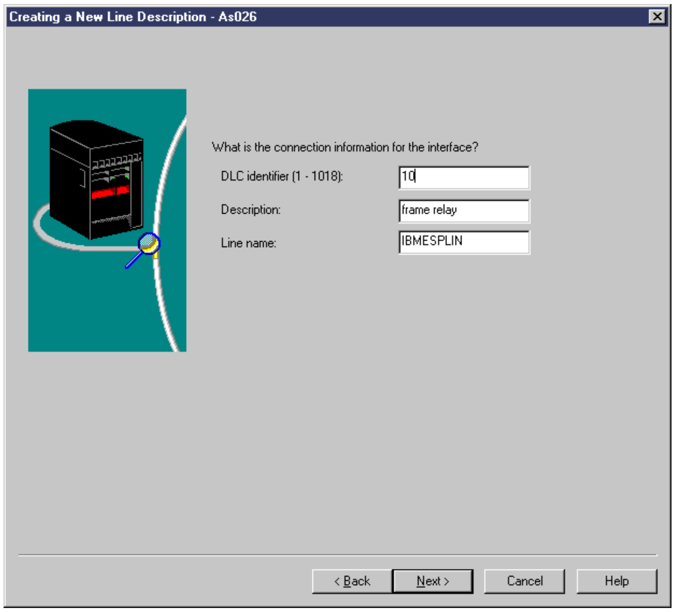
Creating a New TCP/IP Frame Relay Interface - As026

What type of direct frame relay interface are you creating?

- ● Numbered network
- ○ Transparent subnet
- ○ Non-broadcast multi access (NBMA)

Figure 101. Creating a New TCP/IP Frame Relay Interface display

10.On the Creating a New Line Description display (Figure 102), enter the DLC identifier (in this example, enter `10`). Enter the description (in this example, enter `frame relay`). Enter the line name (in this example, enter `IBMESPLIN`). Click **Next** to continue.



Creating a New Line Description - As026

What is the connection information for the interface?

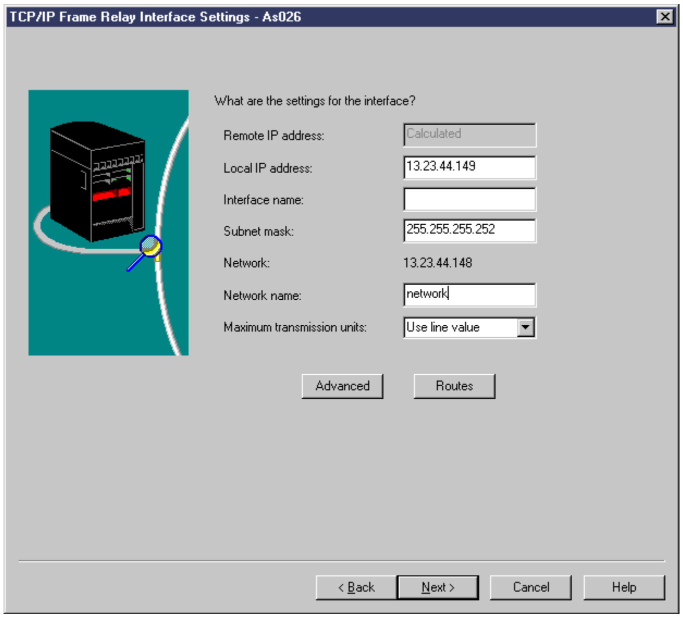
DLC identifier (1 - 1018): 10

Description: frame relay

Line name: IBMESPLIN

Figure 102. Creating a New Line Description display

11.On the Frame Relay Interface Settings display (Figure 103), enter a local IP address (in this example, enter `13.23.44.149`). Enter a subnet mask (in this example, enter `255.255.255.252`). Enter a network name (in this example, enter `network`). Click **Next** to continue.


TCP/IP Frame Relay Interface Settings - As026

What are the settings for the interface?

Remote IP address: Calculated

Local IP address: 13.23.44.149

Interface name:

Subnet mask: 255.255.255.252

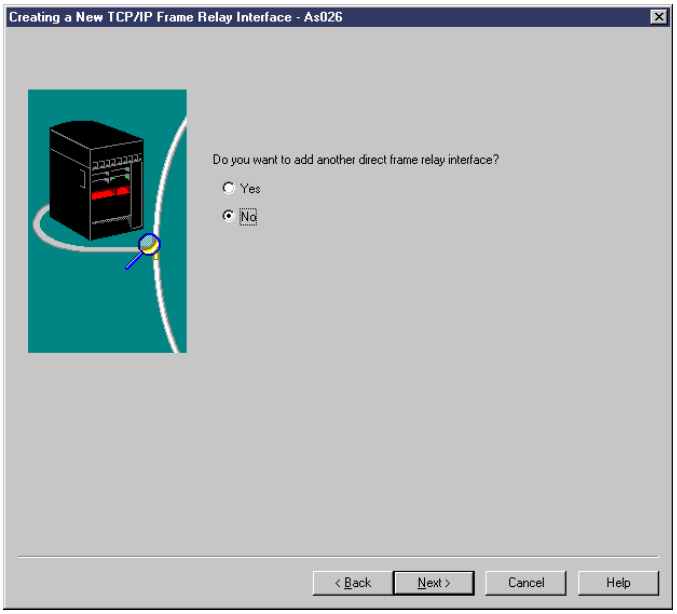
Network: 13.23.44.148

Network name: network

Maximum transmission units: Use line value

Figure 103. TCP/IP Frame Relay Interface Settings display

12.On the Creating a New TCP/IP Frame Relay Interface display (Figure 104), click **No**. Click **Next** to continue.


Creating a New TCP/IP Frame Relay Interface - As026

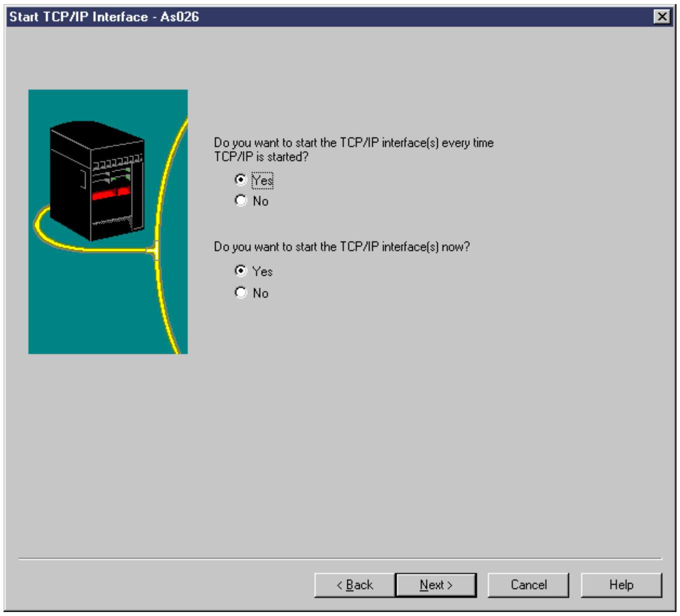
Do you want to add another direct frame relay interface?

○ Yes

● No

Figure 104. Creating a New TCP/IP Frame Relay Interface display

13.On the Start TCP/IP Interface display (Figure 105), change the default value as required. Click **Next** to continue.



Do you want to start the TCP/IP interface(s) every time TCP/IP is started?

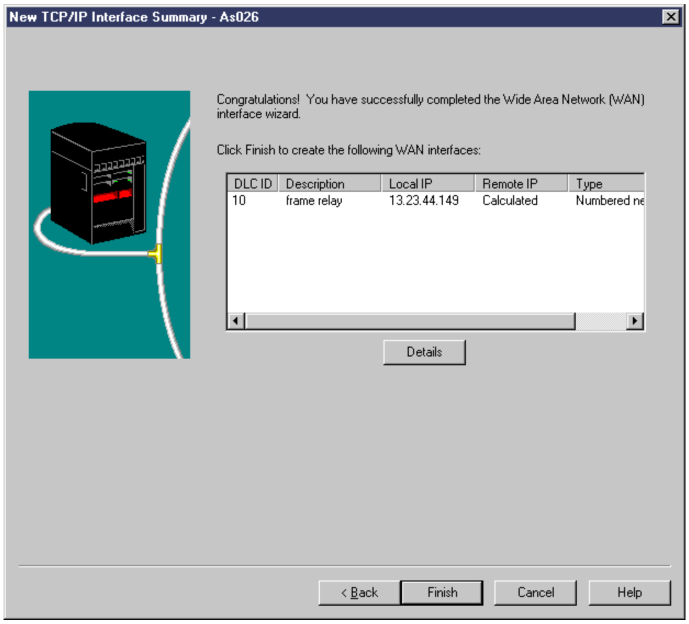
● Yes
○ No

Do you want to start the TCP/IP interface(s) now?

● Yes
○ No

Figure 105. Start TCP/IP Interface display

14.On the TCP/IP Interfaces Summary display (Figure 106), click **Finish** to create the frame relay interface and line configuration.



Congratulations! You have successfully completed the Wide Area Network (WAN) interface wizard.

Click Finish to create the following WAN interfaces:

DLC ID	Description	Local IP	Remote IP	Type
10	frame relay	13.23.44.149	Calculated	Numbered ne

Figure 106. TCP/IP Interfaces Summary display

Note

If you use 5250 emulation to create the frame relay interface for the Universal Connection, perform the following steps:

1. Start 5250 emulation, and sign on to the system with a user profile that has `*IOSYSCFG` and `*ALLOBJ` authorities.
2. Run the `CRTFRNWI` command for the frame relay network interface. In this case, enter the following command:

   ```
   CRTNWIFR NWID(IBMESP) RSRCNAME(CMN06) INTERFACE(*V35) LINESPD(1544000)
   TEXT('TEST for UVC by ITSO')
   ```

3. Create a frame relay line description. Run the `CRTLINFR` command to create the frame relay line description. In this case, enter the following command:

   ```
   CRTLINFR LIND(IBMESPLIN) NWI(IBMESP) NWIDLCI(10) TEXT('TEST for UVC by
   ITSO')
   ```

4. Add a TCP/IP interface for the frame relay line using the `ADDTCPIFC` command:

   ```
   ADDTCPIFC INTNETADR(13.23.44.149) LIND(IBMESPLIN)
   SUBNETMASK(255.255.255.252)
   ```

4.2.2.2 Creating a frame relay connection using UVC

Complete the following steps to configure a frame relay connection on AS026:

1. Start Operations Navigator from the desktop.
2. Expand the iSeries server (in this case, **AS026**). Sign on when prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose the **Universal Connection Wizard** as shown in Figure 119.

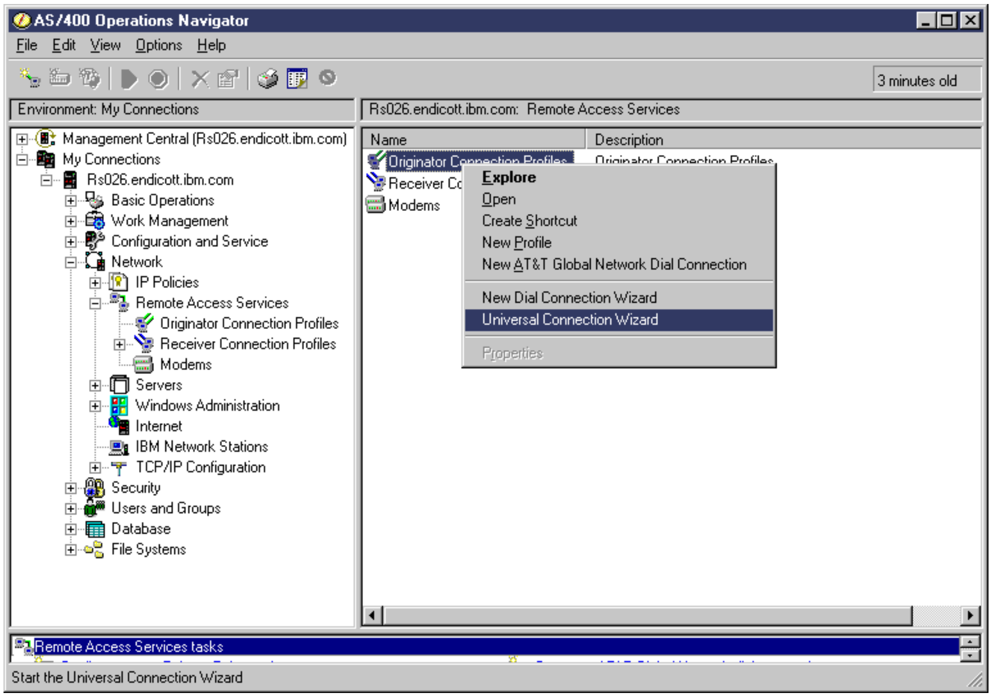
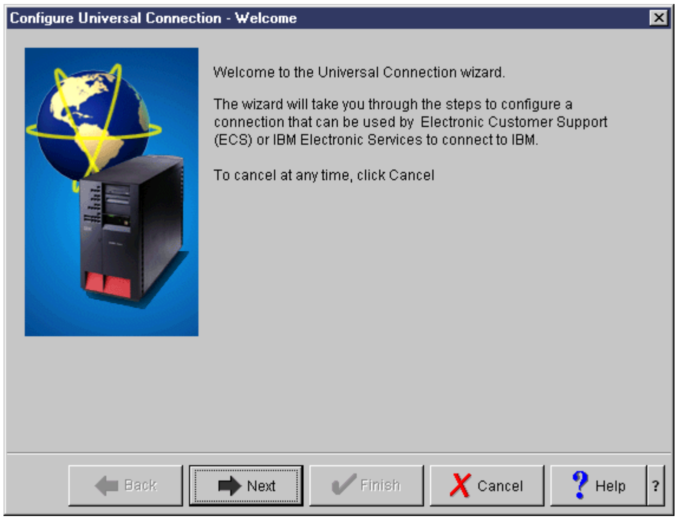

AS/400 Operations Navigator
File Edit View Options Help
3 minutes old
Environment: My Connections
Rs026.endicott.ibm.com: Remote Access Services
Management Central (Rs026.endicott.ibm.com)
My Connections
Rs026.endicott.ibm.com
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profiles
Receiver Connection Profiles
Modems
Servers
Windows Administration
Internet
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
Name
Description
Originator Connection Profiles
Receiver Co
Modems
Originator Connection Profiles
Explore
Open
Create Shortcut
New Profile
New AT&T Global Network Dial Connection
New Dial Connection Wizard
Universal Connection Wizard
Properties
Remote Access Services tasks
Start the Universal Connection Wizard

Figure 107. Universal Connection Wizard

6. Click **Next** on the Welcome dialog as shown in Figure 120.



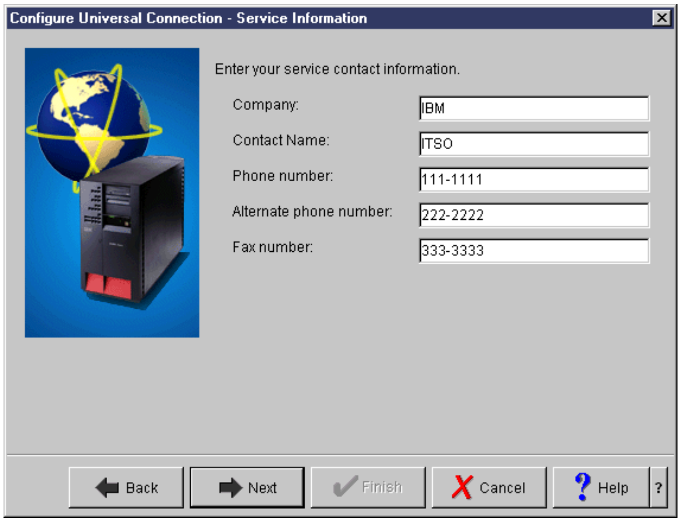
Welcome to the Universal Connection wizard.

The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 108. Configure Universal Connection - Welcome display

7. Enter the service contact information as shown in Figure 121.



Enter your service contact information.

Company: IBM

Contact Name: ITSO

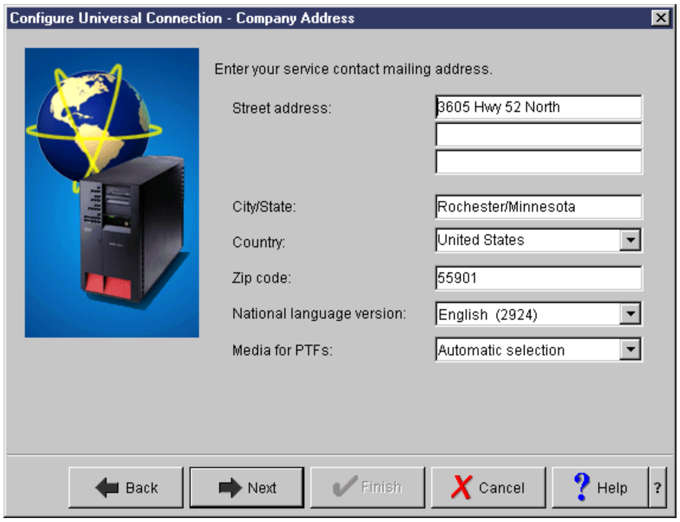
Phone number: 111-1111

Alternate phone number: 222-2222

Fax number: 333-3333

Figure 109. Service contact information

8. Enter the service contact mailing address, national language version, and media for PTFs as shown in Figure 122.



Enter your service contact mailing address.

Street address: 3605 Hwy 52 North

City/State: Rochester/Minnesota

Country: United States

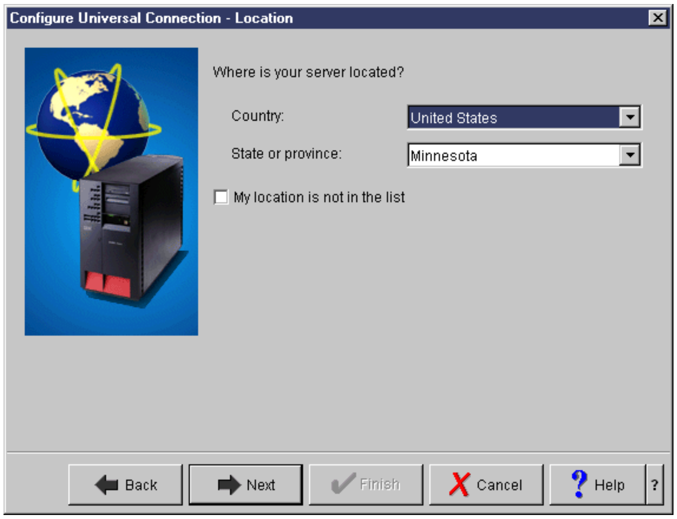
Zip code: 55901

National language version: English (2924)

Media for PTFs: Automatic selection

Figure 110. Service contact mailing address

9. Choose the country, state, or province as shown in Figure 123.


Configure Universal Connection - Location

Where is your server located?

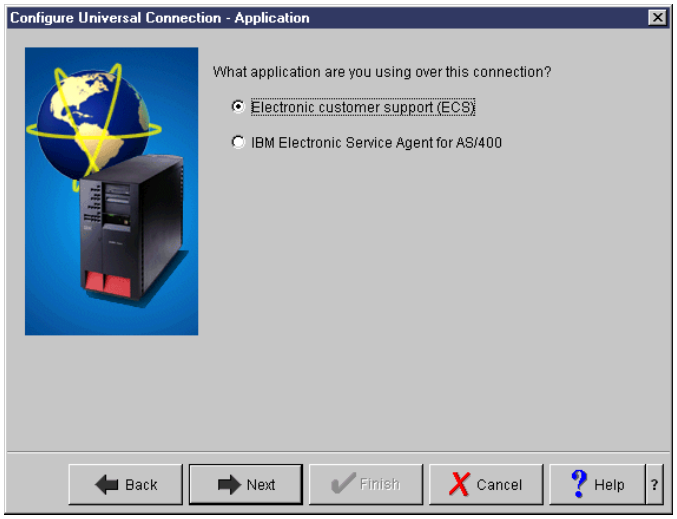
Country: United States

State or province: Minnesota

☐ My location is not in the list

Figure 111. Country, state, or province selection window

10.Select **Electronic Customer Support (ECS)** as shown in Figure 124.


Configure Universal Connection - Application

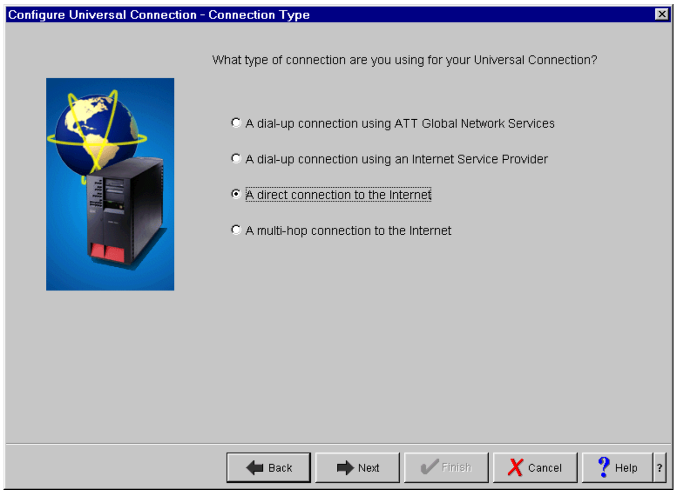
What application are you using over this connection?

● Electronic customer support (ECS)

○ IBM Electronic Service Agent for AS/400

Figure 112. Selecting an application

11.Select **A direct connection to the Internet** as shown in Figure 125.



What type of connection are you using for your Universal Connection?

○ A dial-up connection using ATT Global Network Services

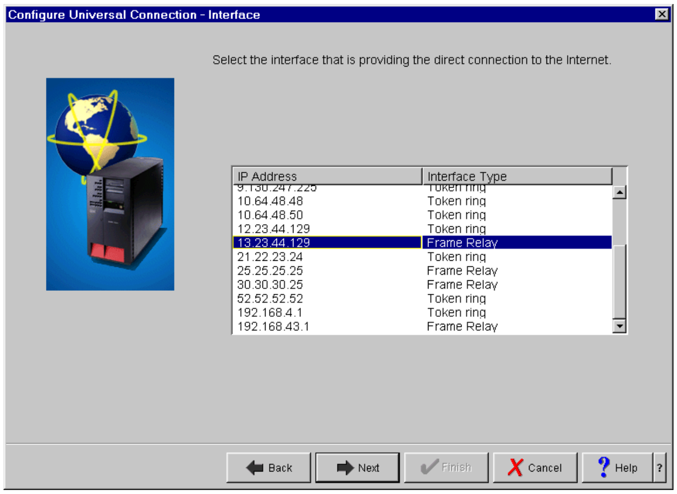
○ A dial-up connection using an Internet Service Provider

● A direct connection to the Internet

○ A multi-hop connection to the Internet

Figure 113. Selecting a connection

12.Select the LAN interface for the frame relay shown in Figure 126.

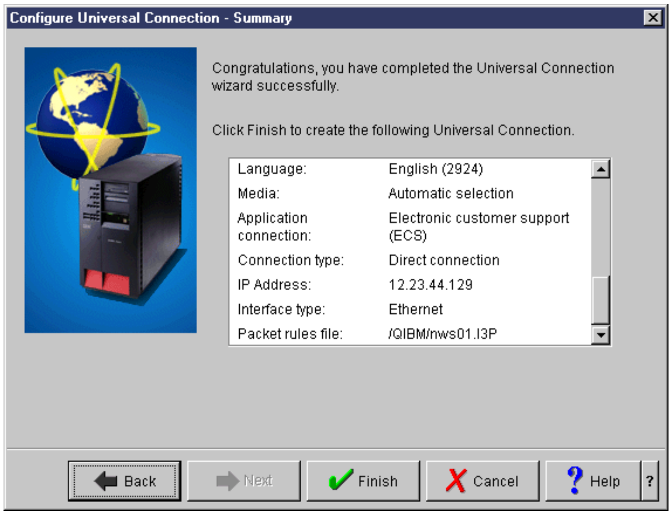


Select the interface that is providing the direct connection to the Internet.

IP Address	Interface Type
9.130.247.225	Token ring
10.64.48.48	Token ring
10.64.48.50	Token ring
12.23.44.129	Token ring
13.23.44.129	Frame Relay
21.22.23.24	Token ring
25.25.25.25	Frame Relay
30.30.30.25	Frame Relay
52.52.52.52	Token ring
192.168.4.1	Token ring
192.168.43.1	Frame Relay

Figure 114. Selecting a LAN interface

13.On the final display (Figure 127), click **Finish**.



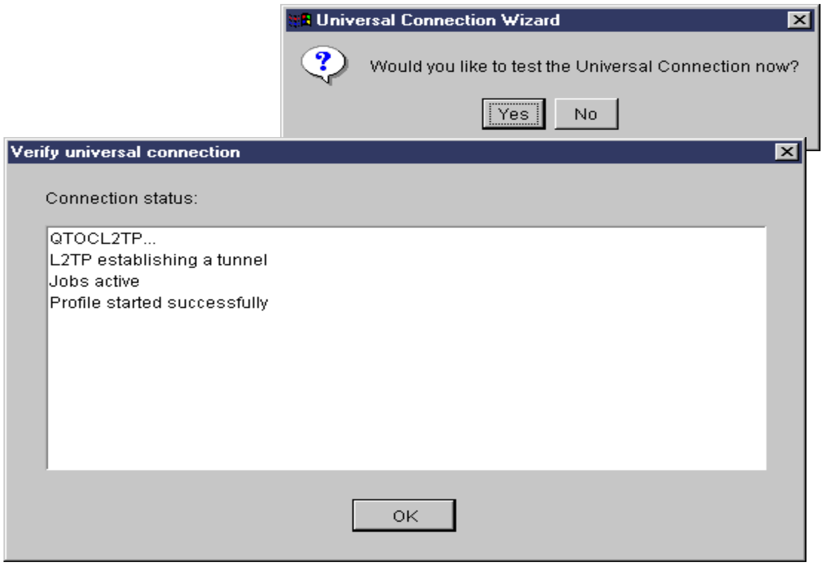
Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

Language:	English (2924)
Media:	Automatic selection
Application connection:	Electronic customer support (ECS)
Connection type:	Direct connection
IP Address:	12.23.44.129
Interface type:	Ethernet
Packet rules file:	/QIBM/nws01.I3P

Figure 115. Final display

14.After you click Finish, the pop-up window in Figure 116 appears. It asks if you want to test the Universal Connection now. Selecting Yes prompts the Universal Connection to initiate a connection for testing purposes. No information is exchanged. A connection status window appears showing whether it was successful. Notice that the frame relay LAN interface must be active prior to the connection test. The Universal Connection Wizard won't activate it.



Would you like to test the Universal Connection now?

Connection status:

```
QTOCL2TP...
L2TP establishing a tunnel
Jobs active
Profile started successfully
```

Figure 116. Testing the connection

4.2.3 The definitions created in the Universal Connection Wizard

Table 31 shows the summary of definitions created in the Universal Connection Wizard.

Table 26. Summary of definitions created in the wizard

Definition name	Definition details
IKE key policies (Wizard named it with the IP address of the VPN endpoint)	It specifies the Internet Key Exchange Policies (IKE) key details: - Preshared key name - Key encryption algorithm
QIBMSERVICE51 - Data policies	It specifies the Encapsulating Security Payload (ESP) encryption details: - ESP mode (Tunnel or Transfer) - Encryption algorithm
QIBMSERVICE51 - Connection definition	It specifies the virtual private network (VPN) connection details: - Remote key server IP address - Local IP address - Remote IP address - Services ports and protocol
QTOCL2TP - L2TP (virtual line) initiator	It specifies the Layer-2 Tunneling Protocol (L2TP) initiator details: - VPN endpoint IP address - IPSec protection connection group name - Link definitions - Authentication PAP/CHAP-MD5, user ID and password - DNS

The details of each definition described in Table 31 are explained in the following list:

- **IKE key policies**

  You can reach the IKE key policies definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Internet Key Exchange Policies**.

- **QIBMSERVICE51 - Security Data policies and Secure connection definition**

  There are two QIBMSERVICE51 definitions created by the wizard. One is an IP Security Data Policies definition, and the other is a Secure connection definition. You can reach the IP Security definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

e. Click **Data Policies**.

The values of the QIBMSERVICE51 IP Security Data Policies definition created in the wizard are shown in Table 27.

Table 27. Values of the IBMSERVICE51 Data Policies definition created in the wizard

Parameters	Values
General - Name - Description - Use Diffie-Hellman perfect forward secrecy - Diffie-Hellman group	 QIBMSERVICE51 IBM Universal Connection Check the Use Diffie-Hellman perfect forward secrecy Group 1 (768-bit MODP)
Proposals - Protocol - Encapsulation - Key expiration expire after - Key expiration expire at size limit - Algorithms authentication - Encryption algorithm	 ESP Transfer mode 15 minutes No size limit MD5 DES-CBC

You can reach the Secure connection definition by performing the following steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **IP Policies**.

c. Expand **Virtual Private Networking**.

d. Expand **Secure Connections**.

e. Click **All Connections**.

The values of the QIBMSERVICE51 Secure connection definition created in the wizard are shown in Table 28.

Table 28. Values of the IBMSERVICE51 Secure Connections definition created by the wizard

Parameters	Values
General - Remote key server identifier type - IP address - Start when the VPN server starts - Start on-demand	 IP version 4 address Assigned by wizard Not selected Not selected
Local addresses - Identifier type - Identifier	 IP version 4 address 13.23.44.129 (depends on your environment)
Remote addresses - Identifier type - Identifier	 IP version 4 address Assigned by wizard
Services - Local port - Remote port - Protocol	 1701 1701 UDP

- **QTOCL2TP - L2TP (virtual line) initiator**

  QTOCL2TP is the L2TP (virtual line) initiator. You can reach the QTOCL2TP definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **Remote Access Services**.

  c. Click **Originator Connection Profiles**.

  The values of the QTOCL2TP definition created in the wizard are shown in Table 29.

Table 29. Values of the QTOCL2TP definition created by the wizard

Parameters	**Values**
General - Name - Description - Protocol type - Mode type	 QTOCL2TP Created by Universal Connection Wizard PPP L2TP (virtual line) - initiator
Connection - Link configuration type of line service - Virtual line name - Remote tunnel endpoint IP address - Requires IPSec protection connection group name - Line inactivity time-out	 Virtual Line (L2TP) QTOCL2TP Assigned by wizard QIBMSERVICE51 600
QTOCL2TP Link definition General - Name - Description - Mode type Link - Bandwidth reservation - Maximum frame size - Enable packet sequence numbering - Activate tunnel keep alive Limits - LCP authentication Authenticate remote peer periodically Maximum authentication attempts - LCP configuration Configuration retry timer Maximum configuration failures Maximum configuration requests Maximum termination requests - Recovery limits Count limit Maximum time-out Authentication - Local host name Remote system L2TP tunnel authentication - Require this iSeries server to verify the identity of the remote L2TP terminator system	 QTOCL2TP Created by Universal Connection Wizard L2TP (virtual line) - initiator 115200 1500 Not selected Not selected Not selected 8 5 5 10 10 2 10 as026 Not selected

Parameters	Values
Authentication Local system identification - allow the remote system to verify the identity of this iSeries server - Authentication protocol to use - Remote system identification requires this iSeries server to verify the identity of the remote system	Selected Require encrypted password (CHAP-MD5) Not selected
TCP/IP settings - Local IP address - Remote IP address - Routing - Hide addresses (full masquerading)	Assigned by remote system Assigned by remote system Define additional static routes Not selected
QTOCL2TP routing	These IP address will vary based on the iSeries server location.
DNS - Domain name server	Do not use
Other Subsystem - Enter the name of the subsystem in which to run name Connection - Use connection script - Script ASCII coded character set identifier	QSYSWRK Not selected 819

4.3 Using a cable modem or DSL modem

Figure 117 shows the network configuration of a Universal Connection with a cable or DSL modem. If you have an iSeries server that has a fixed global routable IP address connected cable or DSL modem, and you want to have a service connection with IBM, follow the procedure to create the cable or DSL modem configuration.

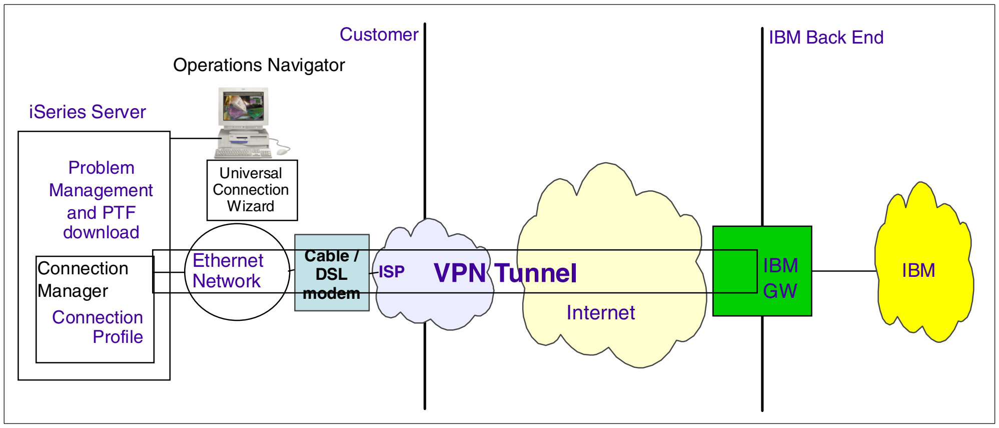


Figure 117. Direct cable modem/DSL modem network configuration

4.3.1 Planning worksheet for a cable modem configuration

Figure 118 shows a sample network configuration using a cable modem.

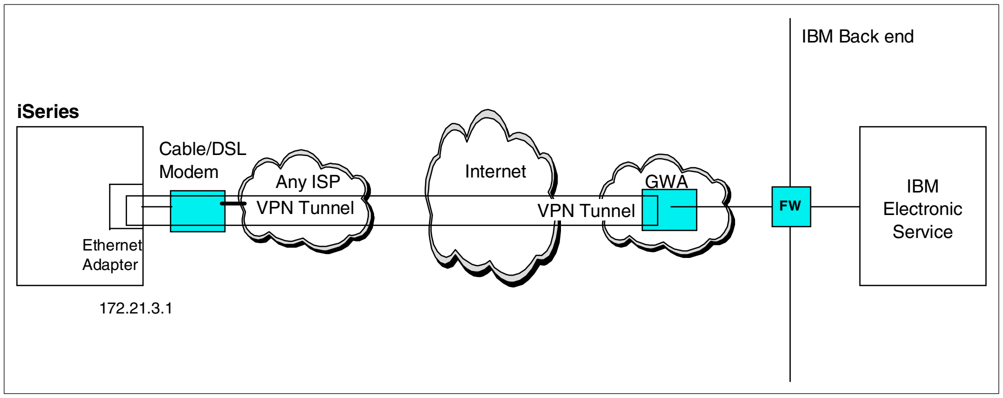


Figure 118. Direct cable modem network configuration

Complete the iSeries server planning worksheets as shown in Table 30. The planning worksheets allow you to gather all the configuration data before the actual implementation occurs.

Table 30. AS026 Direct cable modem configuration: Customer information

This is the customer information to create a direct cable modem configuration	Scenario answers
What is the service contact information? - Company - Contact name - Phone - Alternate phone number - Fax number	 IBM ITSO 111-111-1111 222-222-2222 333-333-3333
What is the service contactmailing address? - Street address - City/state - Country - ZIP code - National language version - Media for PTFs	 3605 Hwy 52 North Rochester/Minnesota United States 55901 English (2924) Automatic selection
Where is your server located? - Country - State or province	 United States Minnesota
What application are you using over this connection? - Electronic Customer Support (ECS) or - IBM Electronic Service Agent for AS/400	Electronic Customer Support
What type of connection are you using for your Universal Connection?	A direct connection to the Internet
What is the IP address and interface type for the cable modem or DSL modem? (**Note**: Must be a globally routable address) - IP address - Interface type	 172.21.3.1 Ethernet

4.3.2 Configuring a direct cable modem on AS026

In this procedure, you:

1. Create a cable modem configuration using the Universal Connection Wizard.
2. Test the connection.

Perform the following steps to configure Universal Connection with a cable modem on AS026:

1. Start Operations Navigator from the desktop.
2. Expand the iSeries server (in this case, **AS026**). Sign on when prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **Universal Connection Wizard** as shown in Figure 119.

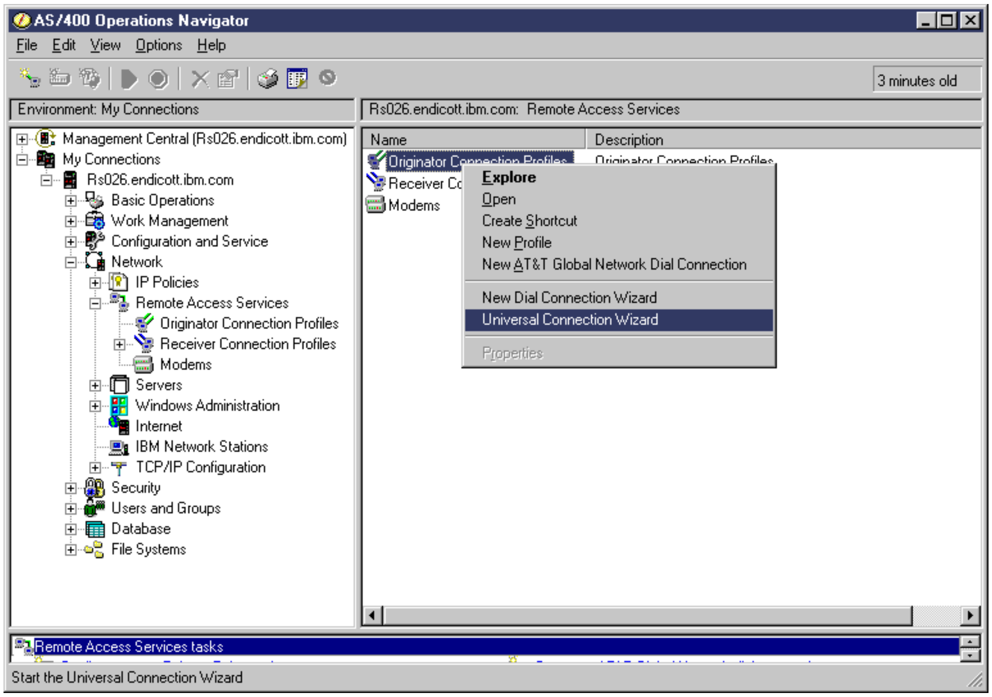
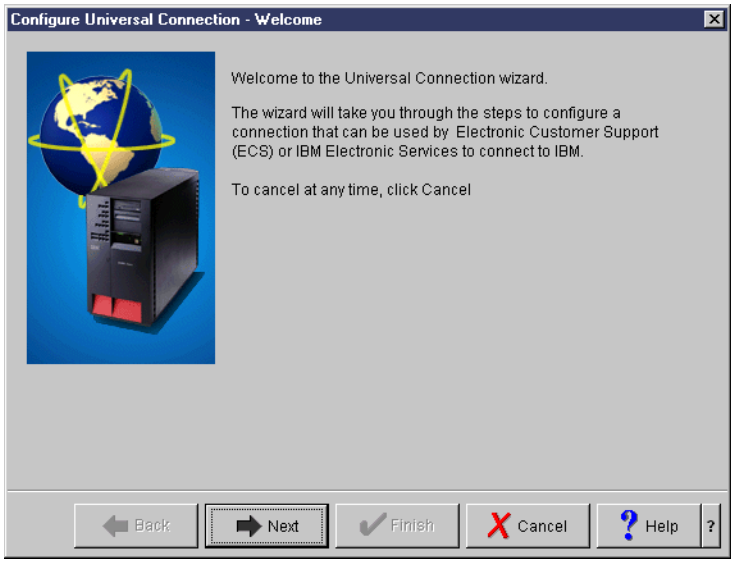

AS/400 Operations Navigator
File Edit View Options Help
3 minutes old
Environment: My Connections
Rs026.endicott.ibm.com: Remote Access Services
Management Central (Rs026.endicott.ibm.com)
My Connections
Rs026.endicott.ibm.com
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profiles
Receiver Connection Profiles
Modems
Servers
Windows Administration
Internet
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
Name
Description
Originator Connection Profiles
Receiver Co
Modems
Originator Connection Profiles
Explore
Open
Create Shortcut
New Profile
New AT&T Global Network Dial Connection
New Dial Connection Wizard
Universal Connection Wizard
Properties
Remote Access Services tasks
Start the Universal Connection Wizard

Figure 119. Universal Connection Wizard

6. Click **Next** in the Welcome dialog (Figure 120).


Configure Universal Connection - Welcome

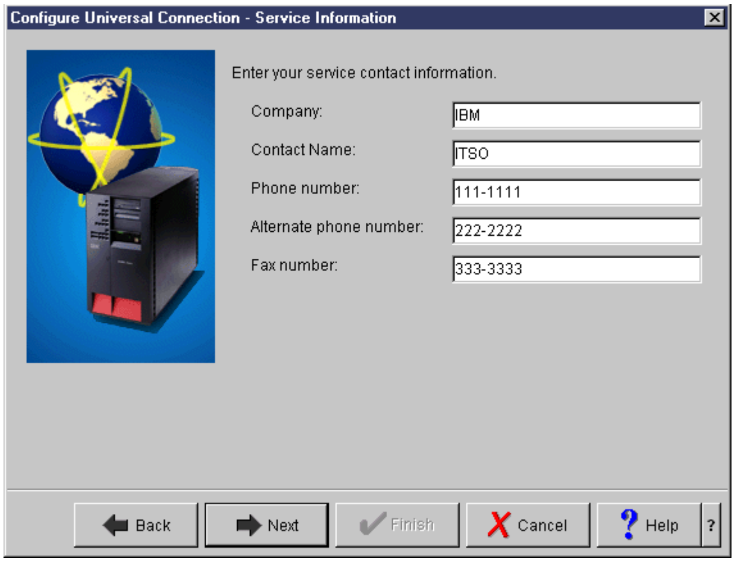
Welcome to the Universal Connection wizard.

The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 120. Configure Universal Connection - Welcome

7. Enter the service contact information as shown in Figure 121.

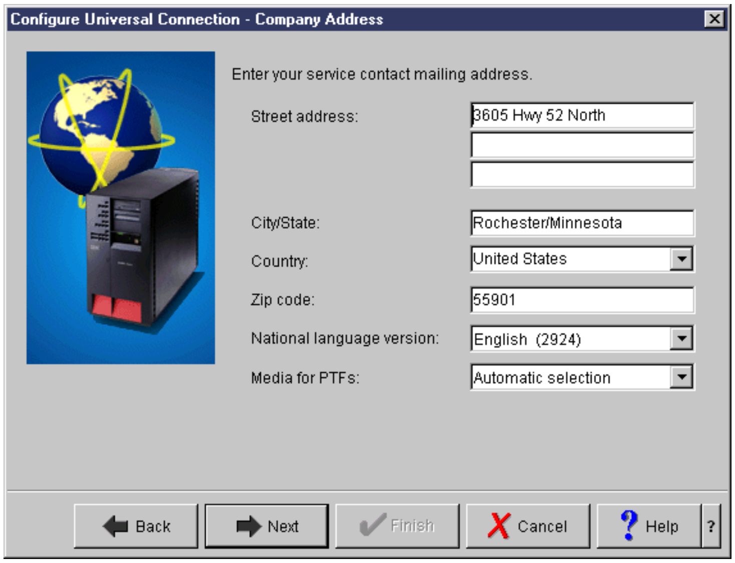

Configure Universal Connection - Service Information

Enter your service contact information.

Company:	IBM
Contact Name:	ITSO
Phone number:	111-1111
Alternate phone number:	222-2222
Fax number:	333-3333

Figure 121. Service contact information

8. Enter the service contact mailing address, national language version, and media for PTFs as shown in Figure 122.



Configure Universal Connection - Company Address

Enter your service contact mailing address.

Street address: 3605 Hwy 52 North

City/State: Rochester/Minnesota

Country: United States

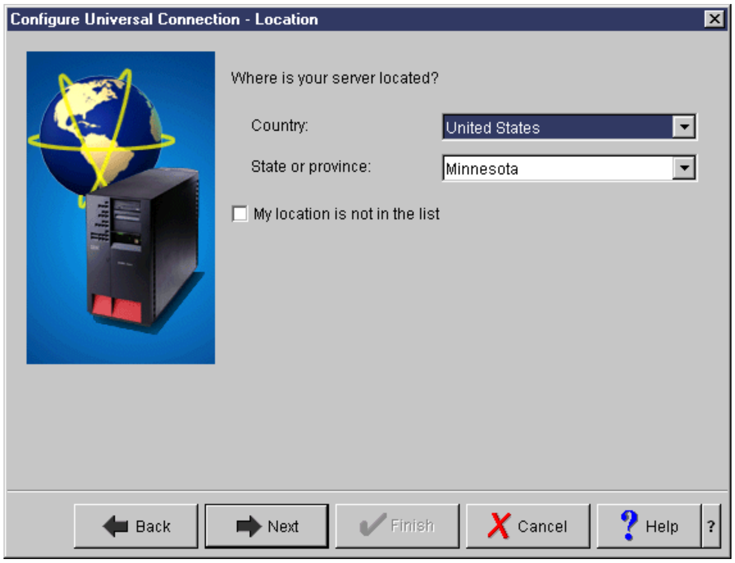
Zip code: 55901

National language version: English (2924)

Media for PTFs: Automatic selection

Figure 122. Service contact mailing address

9. Choose the country, state, or province as shown in Figure 123.



Configure Universal Connection - Location

Where is your server located?

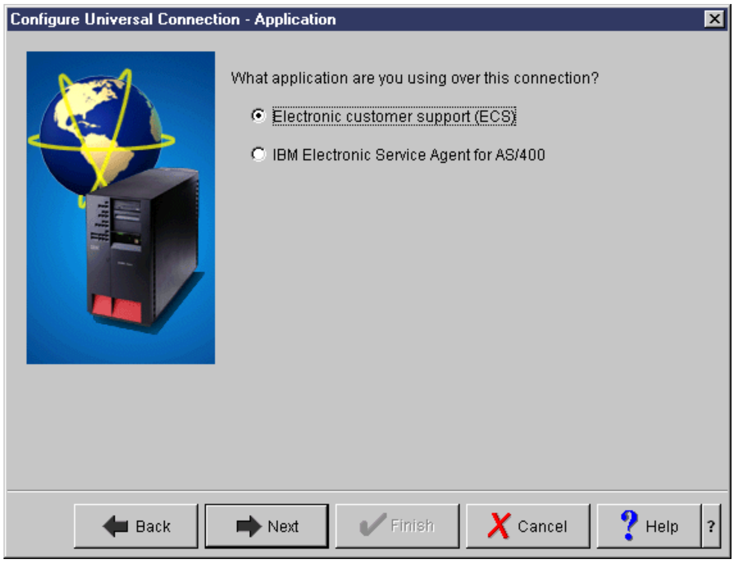
Country: United States

State or province: Minnesota

☐ My location is not in the list

Figure 123. Selecting the country, state, or province

10.Select **Electronic Customer Support (ECS)** as shown in Figure 124.



Configure Universal Connection - Application

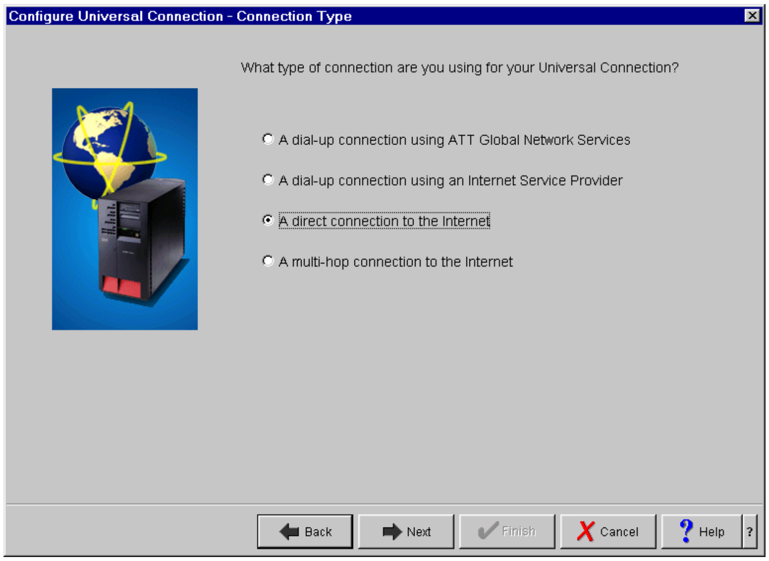
What application are you using over this connection?

● Electronic customer support (ECS)

○ IBM Electronic Service Agent for AS/400

Figure 124. Selecting an application

11.Select **A direct connection to the Internet** as shown in Figure 125.



Configure Universal Connection - Connection Type

What type of connection are you using for your Universal Connection?

○ A dial-up connection using ATT Global Network Services

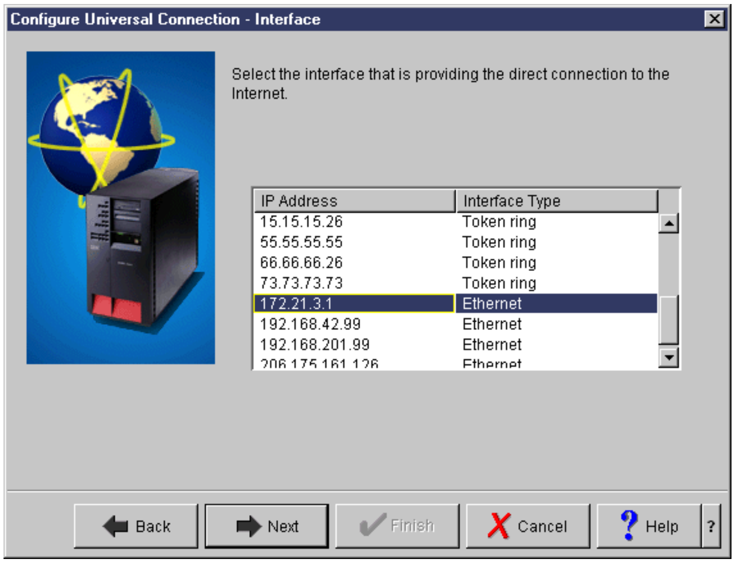
○ A dial-up connection using an Internet Service Provider

● A direct connection to the Internet

○ A multi-hop connection to the Internet

Figure 125. Selecting a connection

12.Select the LAN interface for the direct cable modem as shown in Figure 126.

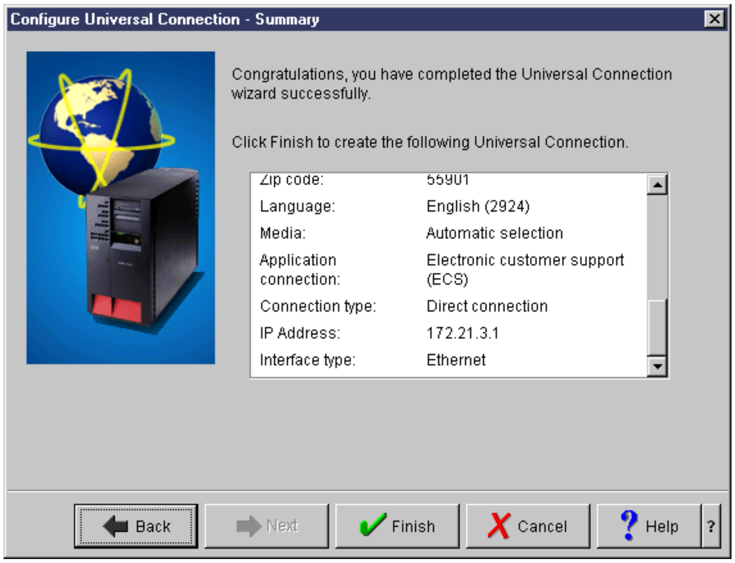


Select the interface that is providing the direct connection to the Internet.

IP Address	Interface Type
15.15.15.26	Token ring
55.55.55.55	Token ring
66.66.66.26	Token ring
73.73.73.73	Token ring
172.21.3.1	Ethernet
192.168.42.99	Ethernet
192.168.201.99	Ethernet
206.175.161.126	Ethernet

Figure 126. Selecting a LAN interface

13.On the Summary display (Figure 127), click **Finish**.



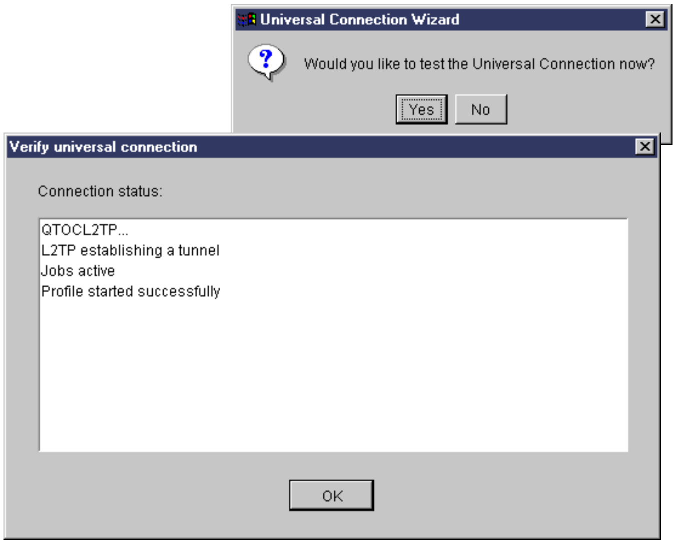
Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

Zip code:	55901
Language:	English (2924)
Media:	Automatic selection
Application connection:	Electronic customer support (ECS)
Connection type:	Direct connection
IP Address:	172.21.3.1
Interface type:	Ethernet

Figure 127. Summary display

14.After you click Finish, the pop-up window shown in Figure 128 appears. It asks if you want to test the Universal Connection now. Selecting Yes causes the Universal Connection to initiate a connection for testing purposes. No information is exchanged. A connection status window appears that shows whether it was successful. Notice that the LAN interface must be active prior to the connection test. The Universal Connection Wizard won't activate it.


Universal Connection Wizard
Would you like to test the Universal Connection now?
Yes
No
Verify universal connection
Connection status:
OK

QTOCL2TP...
L2TP establishing a tunnel
Jobs active
Profile started successfully

Figure 128. Testing the connection

4.3.3 Definitions created in the Universal Connection Wizard

Table 31 shows a summary of the definitions created in the Universal Connection Wizard.

Table 31. Summary of definitions created in the wizard

Definition name	Definition details
IKE key policies (wizard named it with IP address of VPN endpoint)	It specifies the Internet Key Exchange Policies (IKE) key details: - Preshared key name - Key encryption algorithm
QIBMSERVICE51 - Data policies	It specifies the Encapsulating Security Payload (ESP) encryption details: - ESP mode (tunnel or transfer) - Encryption algorithm
QIBMSERVICE51 - Connection definition	It specifies the virtual private network (VPN) connection details: - Remote key server IP address - Local IP address - Remote IP address - Services ports and protocol
QTOCL2TP - L2TP (virtual line) initiator	It specifies the Layer-2 Tunneling Protocol (L2TP) initiator details: - VPN endpoint IP address - IPSec protection connection group name - Link definitions - Authentication PAP/CHAP-MD5, user ID and password - DNS

The details of each definition described in Table 31 are presented in the following list:

- **IKE key policies**

  You can reach the IKE key policies definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Internet Key Exchange Policies**.

- **QIBMSERVICE51 - Security Data policies and Secure connection definition**

  There are two QIBMSERVICE51 definitions created by the wizard. One is the IP Security Data Policies definition, and the other is the Secure connection definition. You can reach the IP Security definition by performing these steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Data Policies**.

  The values of the QIBMSERVICE51 IP Security Data Policies definition created in the wizard are shown in Table 32.

Table 32. Values of the IBMSERVICE51 Data Policies definition created in the wizard

Parameters	Values
General - Name - Description - Use Diffie-Hellman perfect forward secrecy - Diffie-Hellman group	 QIBMSERVICE51 IBM UNIVERSAL CONNECTION Check the Use Diffie-Hellman perfect forward secrecy Group 1 (768-bit MODP)
Proposals - Protocol - Encapsulation - Key Expiration expire after - Key Expiration expire at size limit - Algorithms authentication - Encryption algorithm	 ESP transfer mode 15 minutes No size limit MD5 DES-CBC

  You can reach the Secure connection definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **Secure Connections**.

  e. Click **All Connections**.

The values of the QIBMSERVICE51 Secure connection definition created in the wizard are shown in Table 33.

Table 33. Values of the IBMSERVICE51 Secure Connections definition created by wizard

Parameters	**Values**
General - Remote key server Identifier type - IP address - Start when the VPN server starts - Start on-demand	 IP version 4 address Assigned by wizard Not selected Not selected
Local addresses - Identifier type - Identifier	 IP version 4 address 172.21.3.1 (depends on your ISP)
Remote addresses - Identifier type - Identifier	 IP version 4 address Assigned by wizard
Services - Local port - Remote port - Protocol	 1701 1701 UDP

- **QTOCL2TP - L2TP (virtual line) initiator**

  QTOCL2TP is the L2TP (virtual line) initiator. You can reach the QTOCL2TP definition by following these steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **Remote Access Services**.

  c. Click **Originator Connection Profiles**.

  The values of the QTOCL2TP definition created in the wizard are shown in Table 34.

Table 34. Values of the QTOCL2TP definition created by the wizard

Parameters	**Values**
General - Name - Description - Protocol type - Mode type	 QTOCL2TP Created by Universal Connection Wizard PPP L2TP (virtual line) - initiator
Connection - Link configuration type of line service - Virtual line name - Remote tunnel endpoint IP address - Requires IPSec protection connection group name - Line inactivity time-out	 Virtual Line (L2TP) QTOCL2TP Assigned by wizard QIBMSERVICE51 600

Parameters	Values
QTOCL2TP Link definition	
General	
- Name	QTOCL2TP
- Description	Created by Universal Connection Wizard
- Mode type	L2TP (virtual line) - initiator
Link	
- Bandwidth reservation	115200
- Maximum frame size	1500
- Enable packet sequence numbering	Not selected
- Activate tunnel keep alive	Not selected
Limits	
- LCP authentication	
Authenticate remote peer periodically	Not selected
Maximum authentication attempts	8
- LCP configuration	
Configuration retry timer	5
Maximum configuration failures	5
Maximum configuration requests	10
Maximum termination requests	10
- Recovery limits	
Count limit	2
Maximum time-out	10
Authentication	
- Local host name	as026
Remote system L2TP tunnel authentication	
- Require this iSeries server to verify the identity of the remote L2TP terminator system	Not selected
Authentication	
Local system identification	
- allow the remote system to verify the identity of this iSeries server	Selected
- Authentication protocol to use	Require encrypted password (CHAP-MD5)
- Remote system identification Require this iSeries server to verify the identity of the remote system	Not selected
TCP/IP settings	
- Local IP address	Assigned by remote system
- Remote IP address	Assigned by remote system
- Routing	Define additional static routes
- Hide addresses (full masquerading)	Not selected
QTOCL2TP routing	IP address will vary based on the iSeries server location.
DNS	
- Domain name server	Do not use
Other	
Subsystem	
- Enter the name of the subsystem in which to run name	QSYSWRK
Connection	
- Use connection script	Not selected
- Script ASCII-coded character set identifier	819

4.4 Router isolated access configuration

Figure 129 shows the network configuration of router isolated access. If you have a router that has IP filter rules for inbound and outbound traffic, follow the procedure to create the router isolated access configuration.

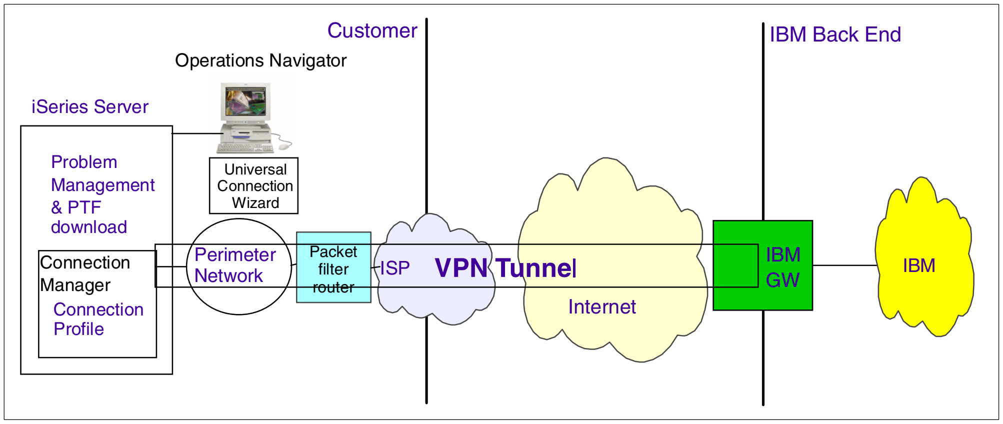


Figure 129. Router isolated access network configuration

4.4.1 Planning worksheet for a router isolated access configuration

Figure 130 shows the sample network configuration with router isolated access.

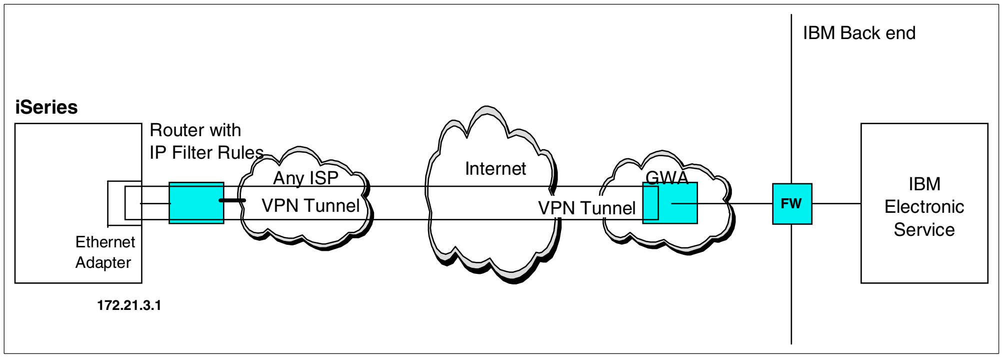


Figure 130. Router isolated access network configuration

Complete the iSeries server planning worksheets as shown in Table 35. The planning worksheets allow you to gather all the configuration data before the actual implementation occurs.

Table 35. AS026 Direct cable modem configuration: Customer information

Customer information to create a router isolated access configuration	Scenario answers
What is the service contact information? - Company - Contact name - Phone - Alternate phone number - Fax number	 IBM ITSO 111-111-1111 222-222-2222 333-333-3333

Customer information to create a router isolated access configuration	**Scenario answers**
What is the service contact mailing address? - Street address - City/state - Country - ZIP code - National language version - Media for PTFs	 3605 Hwy 52 North Rochester/Minnesota United States 55901 English (2924) Automatic selection
Where is your server located? - Country - State or province	 United States Minnesota
What application are you using over this connection? - Electronic Customer Support (ECS) or - IBM Electronic Service Agent for AS/400	Electronic Customer Support
What type of connection are you using for your Universal Connection?	A direct connection to the Internet
What is the IP address and interface type for the LAN access to the packet filter router? (**Note**: Must be a globally routable address) - IP address - Interface type	 172.21.3.1 Ethernet

Table 36 shows the IP filter rules that must be configured on your router so that your server can access the IBM Electronic Service. IP address A varies based on the iSeries server location. After you run the Universal Connection Wizard, you can see IP address A by following these steps:

1. On the Operations Navigator display, expand **Network**.
2. Expand **IP Policies**.
3. Expand **Virtual Private Networking**.
4. Expand **IP Security Policies**.
5. Click **Internet Key Exchange Policies**.
6. Look for the IKE definition name that consists of four dot-separated decimal numbers. The numbers are IP address A.

Note

You can find IP address A on the Web by going to:
`http://www.as400service.ibm.com`

Click the **Technical Databases** hyperlink. On the page that appears, click the **Registered Software Knowledge Base** hyperlink. A password is required to access this page. You must have a valid support line contract to access these articles. Once you enter your password, you can perform a search on **VPN Cisco Multi-Hop Connection Configuration** or **23300444**. This page provides IP address A as the IBM gateway address.

Table 36. IP filter rules for your router

The IP filter rule that must be created on your router	Filter values
UDP Inbound traffic filter rule	Allow port 500 for source IP address A.
UDP Outbound traffic filter rule	Allow port 500 for destination IP address A.
ESP Inbound traffic filter rule	Allow ESP protocol (X’32’) for source IP address A.
ESP Outbound traffic filter rule	Allow ESP protocol (X’32’) for destination IP address A.

4.4.2 Configuring router isolated access on AS026

In this procedure, you perform the following tasks:

1. Create a router isolated access configuration using the Universal Connection Wizard.
2. Configure your router to include IP filter rules to allow the connection with the IBM Electronic Support.
3. Test the connection.

Perform the following steps to configure router isolated access on AS026:

1. Start Operations Navigator from the desktop.
2. Expand the iSeries server (in this case, **AS026**). Sign on when prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **Universal Connection Wizard** as shown in Figure 131.

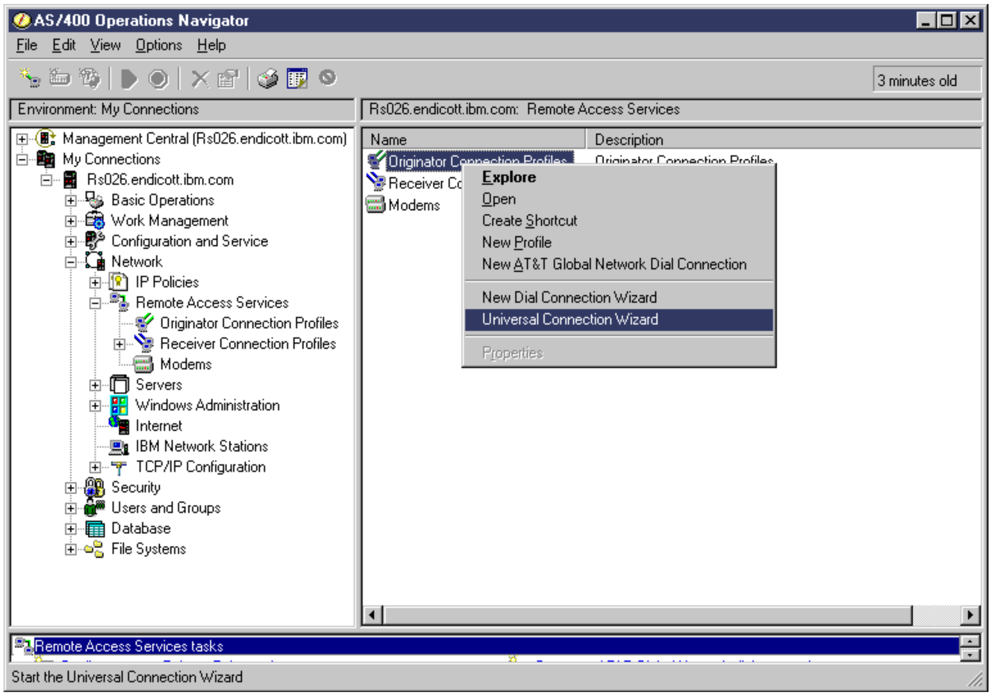
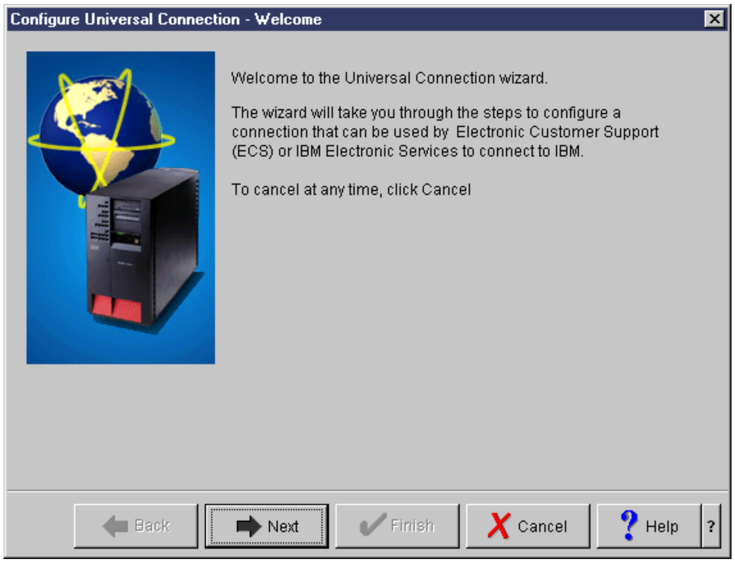

AS/400 Operations Navigator
File Edit View Options Help
3 minutes old
Environment: My Connections
Rs026.endicott.ibm.com: Remote Access Services
Management Central (Rs026.endicott.ibm.com)
My Connections
Rs026.endicott.ibm.com
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profiles
Receiver Connection Profiles
Modems
Servers
Windows Administration
Internet
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
Name
Description
Originator Connection Profiles
Receiver Co
Modems
Originator Connection Profiles
Explore
Open
Create Shortcut
New Profile
New AT&T Global Network Dial Connection
New Dial Connection Wizard
Universal Connection Wizard
Properties
Remote Access Services tasks
Start the Universal Connection Wizard

Figure 131. Universal Connection Wizard

6. Click **Next** in the Welcome dialog (Figure 132).



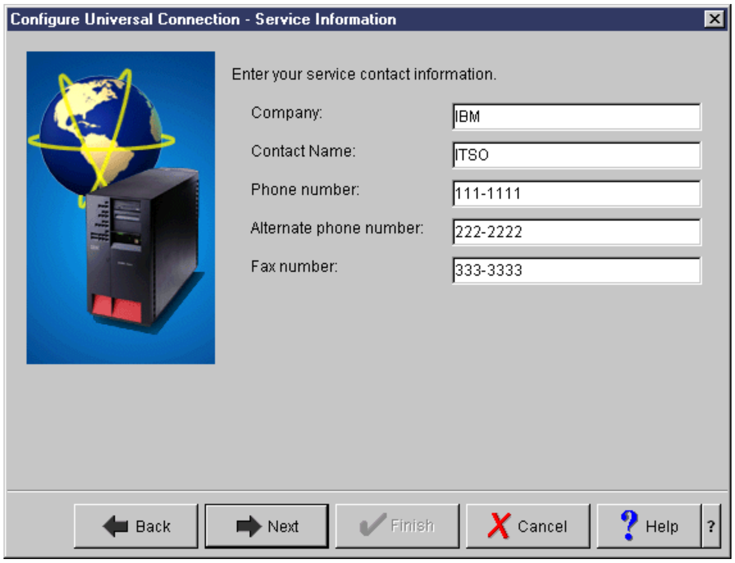
Welcome to the Universal Connection wizard.

The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 132. Configure Universal Connection - Welcome

7. Enter the service contact information as shown in Figure 133.

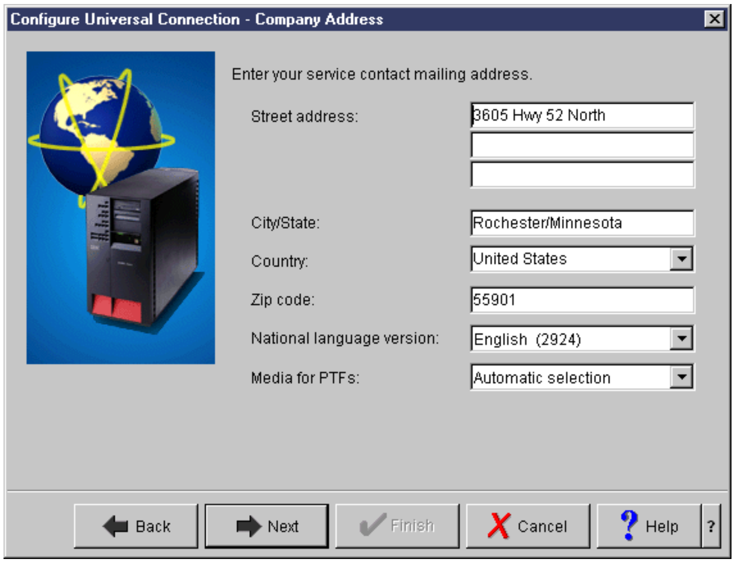

Configure Universal Connection - Service Information

Enter your service contact information.

Company:	IBM
Contact Name:	ITSO
Phone number:	111-1111
Alternate phone number:	222-2222
Fax number:	333-3333

Figure 133. Service contact information

8. Enter the service contact mailing address, national language version, and media for PTFs as shown in Figure 134.

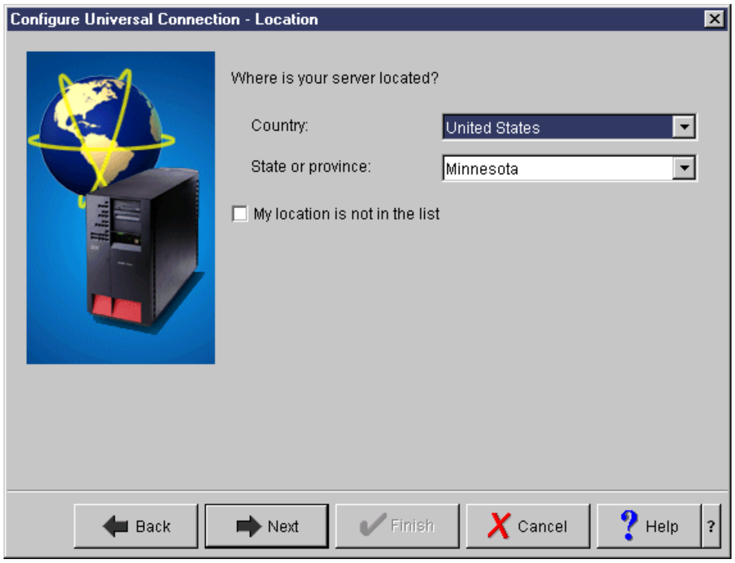

Configure Universal Connection - Company Address

Enter your service contact mailing address.

Street address:	3605 Hwy 52 North
City/State:	Rochester/Minnesota
Country:	United States
Zip code:	55901
National language version:	English (2924)
Media for PTFs:	Automatic selection

Figure 134. Service contact mailing address

9. Choose the country, state, or province as shown in Figure 135.



Configure Universal Connection - Location

Where is your server located?

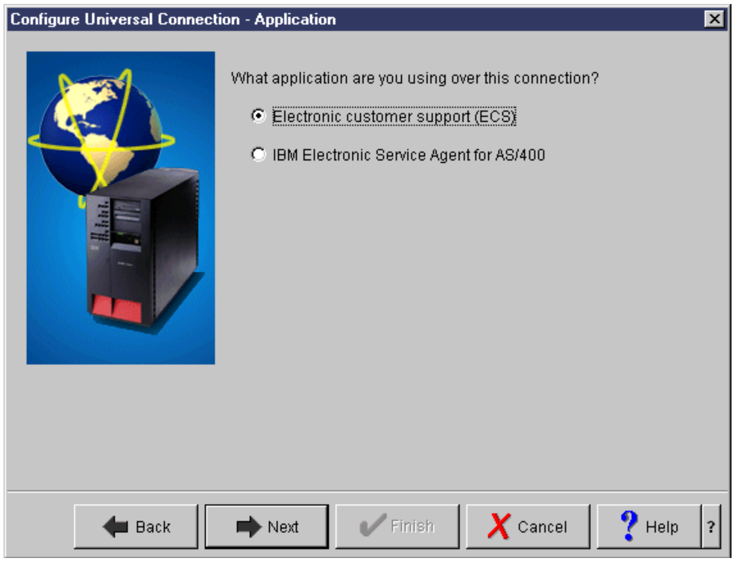
Country: United States

State or province: Minnesota

□ My location is not in the list

Figure 135. Selecting the country, state, or province

10.Select **Electronic Customer Support (ECS)** as shown in Figure 136.



Configure Universal Connection - Application

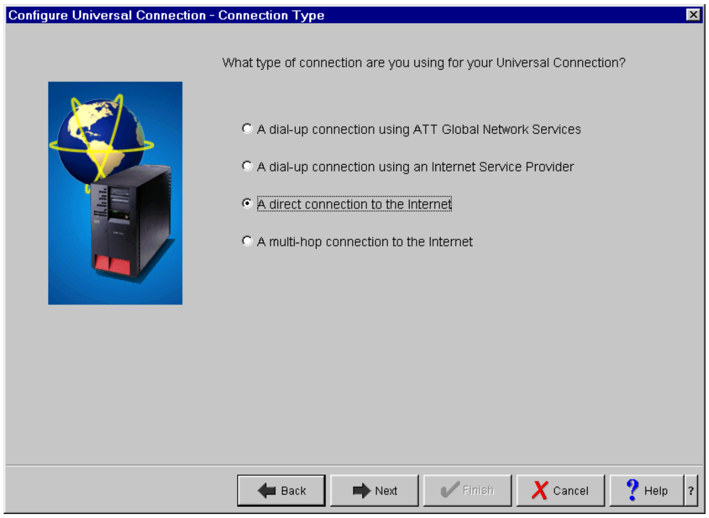
What application are you using over this connection?

● Electronic customer support (ECS)

○ IBM Electronic Service Agent for AS/400

Figure 136. Selecting an application

11.Select **A direct connection to the Internet** as shown in Figure 137.



Configure Universal Connection - Connection Type

What type of connection are you using for your Universal Connection?

○ A dial-up connection using ATT Global Network Services

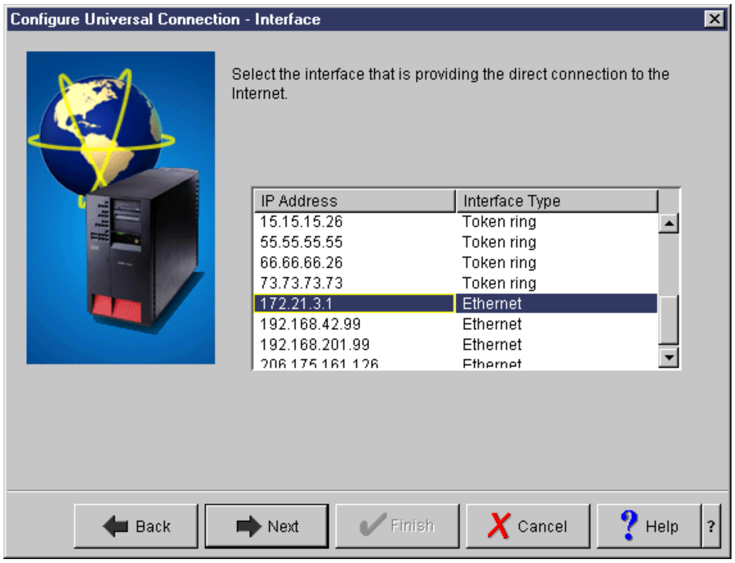
○ A dial-up connection using an Internet Service Provider

● A direct connection to the Internet

○ A multi-hop connection to the Internet

Figure 137. Connection selection

12.Select the LAN interface for the router isolated access as shown in Figure 138.



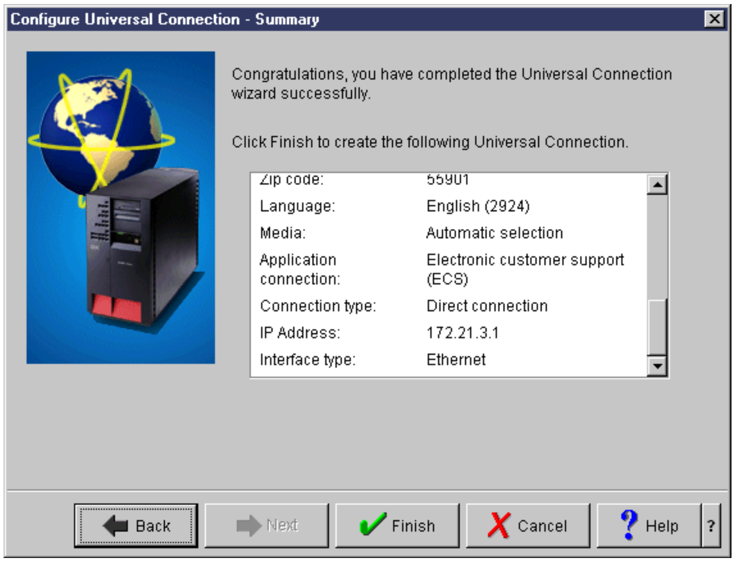
Configure Universal Connection - Interface

Select the interface that is providing the direct connection to the Internet.

IP Address	Interface Type
15.15.15.26	Token ring
55.55.55.55	Token ring
66.66.66.26	Token ring
73.73.73.73	Token ring
172.21.3.1	Ethernet
192.168.42.99	Ethernet
192.168.201.99	Ethernet
206.175.161.126	Ethernet

Figure 138. Selecting a LAN interface

13.On the Summary display (Figure 139), click **Finish**.



Configure Universal Connection - Summary

Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

Zip code:	55901
Language:	English (2924)
Media:	Automatic selection
Application connection:	Electronic customer support (ECS)
Connection type:	Direct connection
IP Address:	172.21.3.1
Interface type:	Ethernet

Figure 139. Summary display

14.After you click Finish, the pop-up display shown in Figure 140 appears. It asks if you want to test the Universal Connection now. To find the IP address that is used to create the IP packet filter on your router, click **No** to end the wizard.

Follow these steps to see IP address A, which is used to create the IP packet filter on your router and configure the IP filter on your router:

1. On the Operations Navigator display, expand **Network**.
2. Expand **IP Policies**.
3. Expand **Virtual Private Networking**.
4. Expand **IP Security Policies**.
5. Click **Internet Key Exchange Policies**.
6. Look for the IKE definition name that consists of four dot-separated decimal numbers. The numbers indicate IP address A.

Note

You can find IP address A on the Web by going to:

`http://www.as400service.ibm.com`

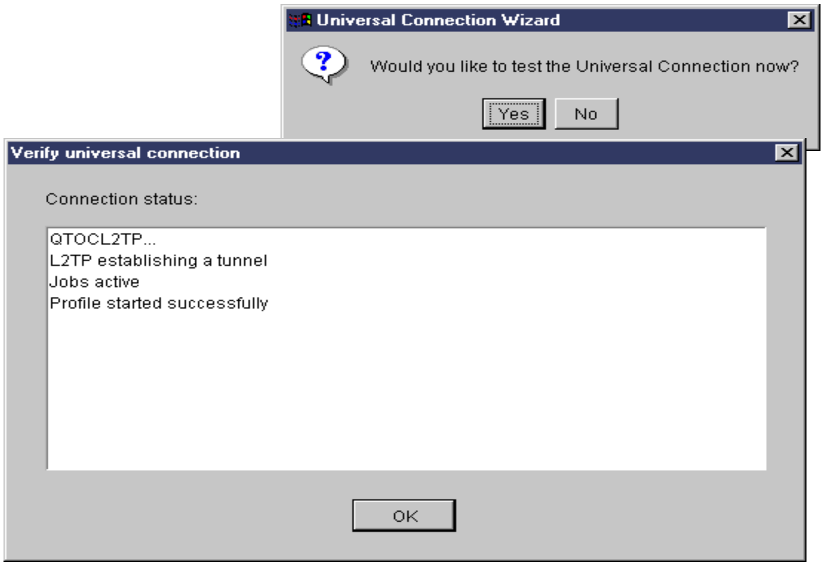
Click the **Technical Databases** hyperlink. On the page that appears, click the **Registered Software Knowledge Base** hyperlink. A password is required to access this page. You must have a valid support line contract to access these articles. Once you enter your password, you can perform a search on **VPN Cisco Multi-Hop Connection Configuration** or **23300444**. This page provides IP address A as the IBM gateway address.

7. Configure the IP filter rule on your router using the information provided in Table 37.

Table 37. IP filter rules for your router

IP filter rules that must be created on your router	Filter values
UDP Inbound traffic filter rule	Allow port 500 for source IP address A.
UDP Outbound traffic filter rule	Allow port 500 for destination IP address A.
ESP Inbound traffic filter rule	Allow ESP protocol (X’32’) for source IP address A.
ESP Outbound traffic filter rule	Allow ESP protocol (X’32’) for destination IP address A.

8. After configuring the IP filter on your router, go back to step 6 on page 140 and run the Universal Connection Wizard again. After you click Finish, the pop-up window shown in Figure 140 appears. Selecting Yes causes the Universal Connection to initiate a connection for testing purposes. No information is exchanged. A connection status window appears showing whether it was successful. Notice that the LAN interface must be activated prior to testing the connection. The Universal Connection Wizard won’t activate it.


Universal Connection Wizard
Would you like to test the Universal Connection now?
Yes
No
Verify universal connection
Connection status:
OK

```
QTOCL2TP...
L2TP establishing a tunnel
Jobs active
Profile started successfully
```

Figure 140. Testing the connection

4.4.3 The definitions created in the wizard

Table 38 shows a summary of the definitions created in the wizard.

Table 38. Summary of the definitions created in the wizard

Definition name	Definition details
IKE key policies	It specifies the Internet Key Exchange Policies (IKE) key details: - Preshared key name - Key encryption algorithm

Definition name	Definition details
QIBMSERVICE51 - Data policies	It specifies the Encapsulating Security Payload (ESP) encryption details: - ESP mode (Tunnel or Transfer) - Encryption algorithm
QIBMSERVICE51 - Connection definition	It specifies the virtual private network (VPN) connection details: - Remote key server IP address - Local IP address - Remote IP address - Services ports and protocol
QTOCL2TP - L2TP (virtual line) initiator	It specifies the Layer-2 Tunneling Protocol (L2TP) initiator details: - VPN endpoint IP address - IPSec protection connection group name - Link definitions - Authentication PAP/CHAP-MD5, user ID and password - DNS

The details of each definition described in Table 38 are as follows:

- **IKE key policies**

  You can reach the IKE key policies definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Internet Key Exchange Policies**.

- **QIBMSERVICE51 - Security Data policies and Secure connection definition**

  There are two QIBMSERVICE51 definitions created by the wizard. One is an IP Security Data Policies definition, and the other is a Secure connection definition. You can reach the IP Security definition by performing the following steps:

  a. On the Operations Navigator display, expand **Network**.

  b. Expand **IP Policies**.

  c. Expand **Virtual Private Networking**.

  d. Expand **IP Security Policies**.

  e. Click **Data Policies**.

The values of the QIBMSERVICE51 IP Security Data Policies definition created in the wizard are shown in Table 39.

Table 39. Values of the IBMSERVICE51 Data Policies definition created in the wizard

Parameters	Values
General - Name - Description - Use Diffie-Hellman perfect forward secrecy - Diffie-Hellman group	 QIBMSERVICE51 IBM UNiversal Connection Check the Use Diffie-Hellman perfect forward secrecy Group 1 (768-bit MODP)
Proposals - Protocol - Encapsulation - Key expiration expire after - Key expiration expire at size limit - Algorithms authentication - Encryption algorithm	 ESP transfer mode 15 minutes No size limit MD5 DES-CBC

You can reach the Secure connection definition by performing these steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **IP Policies**.

c. Expand **Virtual Private Networking**.

d. Expand **Secure Connections**.

e. Click **All Connections**.

The values of the QIBMSERVICE51 Secure connection definition created in the wizard are shown in Table 40.

Table 40. Values of the IBMSERVICE51 Secure Connections definition created by the wizard

Parameters	Values
General - Remote key server Identifier type - IP address - Start when the VPN server starts - Start on-demand	 IP version 4 address Assigned by wizard Not selected Not selected
Local addresses - Identifier type - Identifier	 IP version 4 address 172.21.3.1 (depends on your ISP)
Remote addresses - Identifier type - Identifier	 IP version 4 address Assigned by wizard
Services - Local port - Remote port - Protocol	 1701 1701 UDP

- **QTOCL2TP - L2TP (virtual line) initiator**

  QTOCL2TP is the L2TP (virtual line) initiator. You can reach the QTOCL2TP definition by performing the following steps:

a. On the Operations Navigator display, expand **Network**.

b. Expand **Remote Access Services**.

c. Click **Originator Connection Profiles**.

The values of the QTOCL2TP definition created in the wizard are shown in Table 41.

Table 41. Values of the QTOCL2TP definition created by wizard

Parameters	**Values**
General	
- Name	QTOCL2TP
- Description	Created by Universal Connection Wizard
- Protocol type	PPP
- Mode type	L2TP (virtual line) - initiator
Connection	
- Link configuration type of line service	Virtual Line (L2TP)
- Virtual line name	QTOCL2TP
- Remote tunnel endpoint IP address	Assigned by wizard
- Requires IPSec protection connection group name	QIBMSERVICE51
- Line inactivity time-out	600
QTOCL2TP Link definition	
General	
- Name	QTOCL2TP
- Description	Created by Universal Connection Wizard
- Mode type	L2TP (virtual line) - initiator
Link	
- Bandwidth reservation	115200
- Maximum frame size	1500
- Enable packet sequence numbering	Not selected
- Activate tunnel keep alive	Not selected
Limits	
- LCP authentication	
Authenticate remote peer periodically	Not selected
Maximum authentication attempts	8
- LCP configuration	
Configuration retry timer	5
Maximum configuration failures	5
Maximum configuration requests	10
Maximum termination requests	10
- Recovery limits	
Count limit	2
Maximum time-out	10
Authentication	
- Local host name	as026
Remote system L2TP tunnel authentication	
- Require this iSeries server to verify the identity of the remote L2TP terminator system	Not selected

Parameters	Values
Authentication Local system identification - allow the remote system to verify the identity of this iSeries server - Authentication protocol to use - Remote system identification require this iSeries server to verify the identity of the remote system	Selected Require encrypted password (CHAP-MD5) Not selected
TCP/IP settings - Local IP address - Remote IP address - Routing - Hide addresses (full masquerading)	Assigned by remote system Assigned by remote system Define additional static routes Not selected
QTOCL2TP routing	The IP address will vary based on the iSeries server location.
DNS - Domain name server	Do not use
Other Subsystem - Enter the name of the subsystem in which to run Name Connection - Use connection script - Script ASCII-coded character set identifier	QSYSWRK Not selected 819

4.5 Security over a direct connection

The wizard creates the security-related definitions to establish encrypted, safe, and reliable connections between your iSeries server and IBM Electronic Support. This works the same as security over a PPP dial-up to any ISP connection. This section explains:

- How the VPN connection works
- How safe VPN connections can be established between your iSeries server and IBM Electronic Support
- How IP packet filters work to protect your iSeries server from intrusion
- The differences for a direct connect customer

4.5.1 IBM Electronic Support connection using VPN

This connection occurs in exactly the same manner as when establishing security over a PPP dial-up to any ISP connection. For more information, see 3.5.1, “IBM Electronic Support connection using VPN” on page 102.

4.5.2 IP packet filtering

The wizard also creates the IP packet filter rules for the TCP interface that is used for the direct connection profile. The IP packet filters watch each IP packet to see if the packet meets the condition described in the filter rules. The IP filter prevents the threat of intrusions in Active Attack cases and Denial of Service Attack cases.

You may notice that IP packet filtering in this case is very similar to IP packet filtering when using security over a PPP dial-up to any ISP connection. For more information, see 3.5.2, “IP packet filtering” on page 103. Figure 93 on page 104 shows the IP packet filter rules.

The difference for direct connection customers is explained here. If you’ve already defined the IP filter rules on the TCP interface used for the direct connection profile, the wizard adds the required IP filter rules on the TCP interface to allow the VPN connection for the IBM Electronic Support to be established. You must also modify your firewall filter set to enable VPN traffic.

Chapter 5. Multi-hop scenario

This chapter covers the special configuration referred to as multi-hop in relation to the Universal Connection. It presents various network configurations that can be used with multi-hop. It also shows how the ECS and Electronic Service Agent functions can be used over these configurations.

5.1 What is multi-hop?

A multi-hop scenario enables the iSeries server to redirect L2TP traffic on behalf of L2TP Access Concentrators (LACs) and L2TP Network Servers (LNSs) client. To establish an L2TP multi-hop connection, the iSeries server acts as both an LNS to one or more LACs and as an LAC to a given LNS. A tunnel is established from a client LAC to this iSeries server (L2TP Terminator profile). Another tunnel is established between this iSeries server (L2TP multi-hop initiator profile) and a target LNS. Then, L2TP traffic from the client LAC is redirected by the iSeries server to the target LNS. L2TP traffic from the target LNS is redirected by the iSeries server to the client LAC.

“Hopping” over two different VPN tunnels was not allowed until the emergence of multi-hop. A “hop” refers to the passage of an IP packet between two network nodes, such as two routers. L2TP can be used over a multi-hop connection, as long as the network nodes (in most cases, routers) can support L2TP.

The Universal Connection can be configured using a multi-hop connection. This type of connection is useful if the iSeries server is located on a private network, does not have a global IP address, and there is access to a packet filter router that allows the iSeries server to establish a connection to the Internet via an ISP. This network configuration is shown in Figure 141.

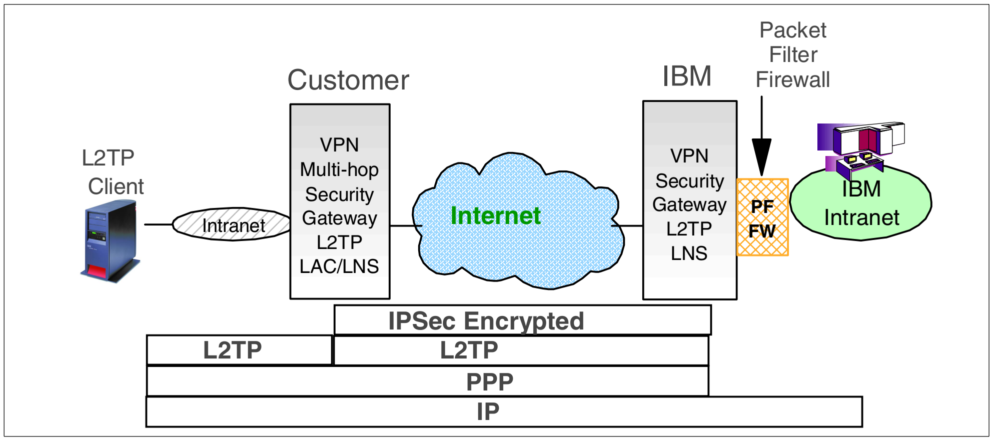


Figure 141. Multi-hop L2TP VPN secure gateway configuration

The multi-hop connection basically allows a connection to the IBM Service system by establishing multiple L2TP tunnel connections from the iSeries server to the IBM Service system. The L2TP client (in this case, the iSeries server) initiates an L2TP tunnel directly to the local packet filter (PF) router with the VPN secure gateway. The gateway then initiates an IPSec/L2TP tunnel to the IBM gateway via the Internet. The IBM gateway then assigns an IP address to the L2TP client from the available pool of IP addresses that it has. The L2TP client establishes end-to-end IP connectivity over these tunnels to the IBM Service system on the IBM intranet. The IBM packet filter firewall restricts access to the IBM intranet by only allowing a limited set of services.

To establish a route, a VPN connection from an intranet that is not globally routable (a VPN secure gateway) is necessary. This gateway can be incorporated with the packet filter router as a service, or it can exist as a stand-alone hardware device. Certain packet filter rules are necessary to allow the local packet filter router to be used in the multi-hop connection. These are discussed in more detail in the following section.

5.2 Multi-hop network configurations

There are six network configurations that can use the multi-hop connection:

- Exterior router merged with VPN secure gateway
- Interior router merged with VPN secure gateway
- Interior/exterior router merged with VPN secure gateway

  The VPN secure gateway can also be added as a new hardware device instead of as part of the packet filter router. This does not change the functionality of the connection. However, it does introduce additional IP packet filter rules, depending on the network configuration being used. This section briefly discusses how the VPN secure gateway can be implemented as a new hardware device for each scenario mentioned earlier, and what new packet filter rules would need to be configured.

- Standalone VPN secure gateway behind a firewall
- Standalone VPN secure gateway as bastion host on a DMZ
  - Separate interior/exterior routers
  - Combined interior/exterior routers

5.2.1 Extreme router merged with a VPN secure gateway connection

Figure 142 shows the extreme router merged with VPN secure gateway configuration.

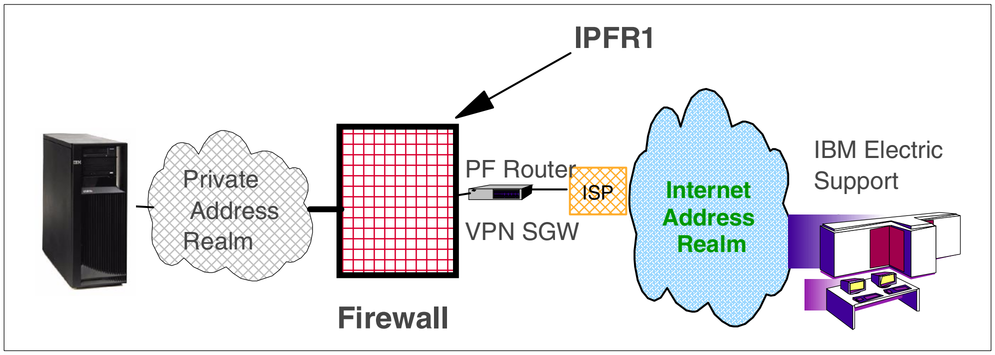


Figure 142. Standalone VPN secure gateway

In this configuration, the packet filter router acts as the VPN secure gateway and is located in front of the firewall. The iSeries server is located on the intranet and has a private IP address (that is, it is not a globally routable IP address). The IP filter rules shown in Table 42 must be configured on the firewall for this configuration. This is indicated by IPFR1 in Figure 142.

Table 42. IP filter rules for a stand-alone VPN configuration

IP filter rule	IP filter value
UDP Outbound traffic filter rule	Allow port 1701 for source IP address of VPN secure gateway (for example, 10.10.10.1)
UDP Inbound traffic filter rule	Allow port 1701 for destination IP address of VPN secure gateway (for example, 10.10.10.1)

5.2.2 Interior router merged with VPN secure gateway connection

Figure 143 show an illustration of the configuration of an interior router merged with VPN secure gateway.

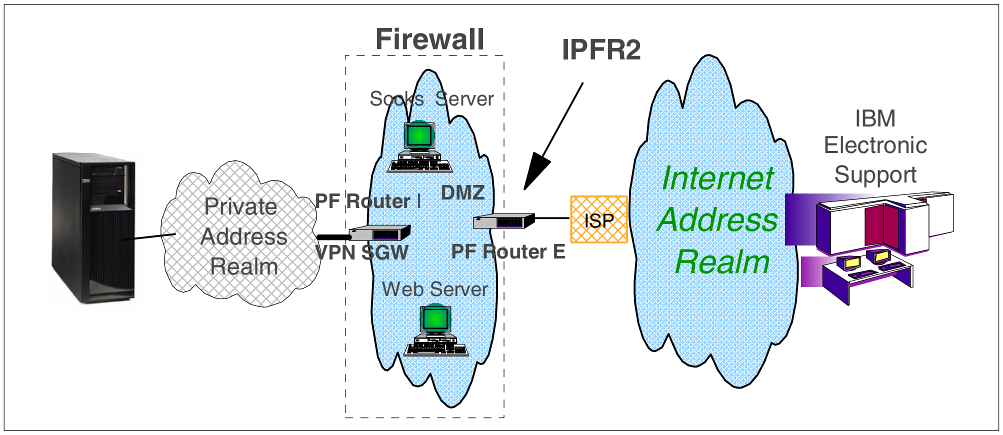


Figure 143. Merged interior router with VPN secure gateway configuration

In this configuration, PF router I acts as the VPN secure gateway and coexists with the firewall router. Other servers, such as the socks server, Web servers, and mail servers, can also be located within the firewall. The IP filter rules, indicated by IPFR2, must be applied to the PF router E. These rules are outlined in Table 43.

Table 43. Packet filter rules for the merged interior configuration

IP filter rules	IP filter values
UDP Inbound traffic filter rule	Allow port 500 for GWA IP address
UDP Outbound traffic filter rule	Allow port 500 for GWA IP address
ESP Inbound traffic filter rule	Allow ESP protocol (X’32’) for GWA IP address
ESP Outbound traffic filter rule	Allow ESP protocol (X’32’) for GWA IP address

Note

You can find the GWA IP address on the Web by going to:

`http://www.as400service.ibm.com`

Click the **Technical Databases** hyperlink. On the page that appears, click the **Registered Software Knowledge Base** hyperlink. A password is required to access this page. You must have a valid support line contract to access these articles. Once you enter your password, you can perform a search on **VPN Cisco Multi-Hop Connection Configuration** or **23300444**. This page provides the GWA IP address as an IBM gateway address.

5.2.3 Interior/exterior router with a VPN secure gateway connection

Figure 144 shows an illustration of a configuration of an interior/exterior router merged with a VPN secure gateway.

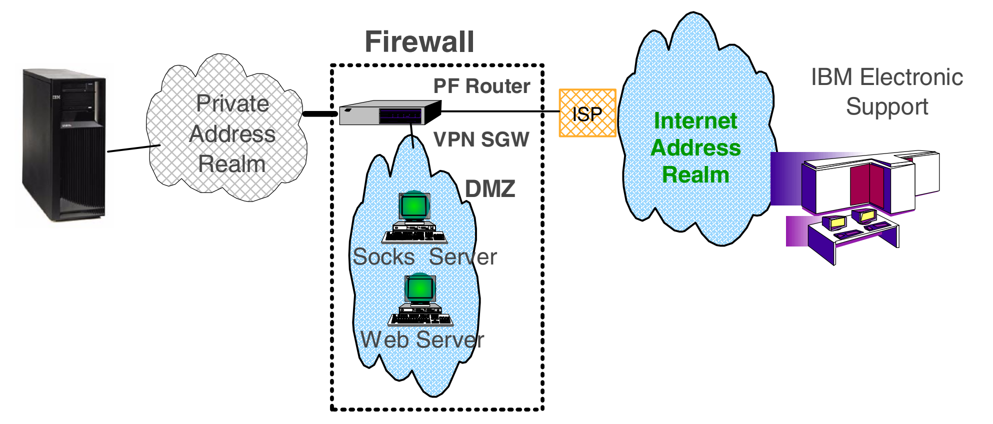


Figure 144. Merged exterior router with VPN secure gateway configuration

In this implementation, the packet filter router coexists as part of the firewall but is external to the DMZ. This means that IP traffic does *not* need to be routed through the DMZ to reach the Internet.

5.2.4 Standalone VPN secure gateway behind a firewall

Figure 145 shows a configuration of a stand-alone VPN secure gateway behind a firewall.

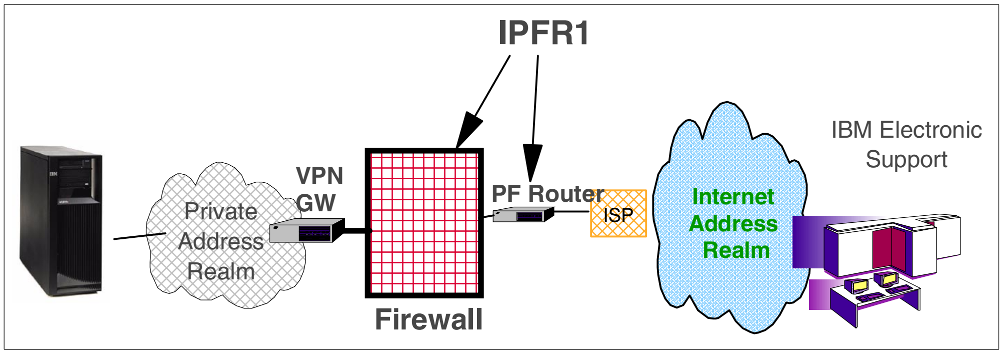


Figure 145. Standalone VPN gateway with Packet Filter router

In this implementation, the IP packet filter rules must be configured on both the packet filter router and the firewall because the VPN gateway is now behind the firewall. The IP packet filter rules are indicated by the IPFR1 tag, in Figure 145, and are outlined in Table 44.

Table 44. IP packet filter rules for stand-alone VPN secure gateway and packet filter router

IP filter rules	IP filter values
UDP Inbound traffic filter rule	Allow port 500 for GWA IP address
UDP Outbound traffic filter rule	Allow port 500 for GWA IP address
ESP Inbound traffic filter rule	Allow ESP protocol (X’32’) for GWA IP address
ESP Outbound traffic filter rule	Allow ESP protocol (X’32’) for GWA IP address

You can find the GWA IP address by going to: `http://www.as400service.ibm.com`

See “Note” on page 154 for details.

5.2.5 Standalone VPN secure gateway as a bastion host on DMZ

This scenario has the following two types of connections:

- Separate interior/exterior routers
- Combined interior/exterior routers

5.2.5.1 Separate interior/exterior routers

Figure 146 shows the separate interior/exterior routers configuration.

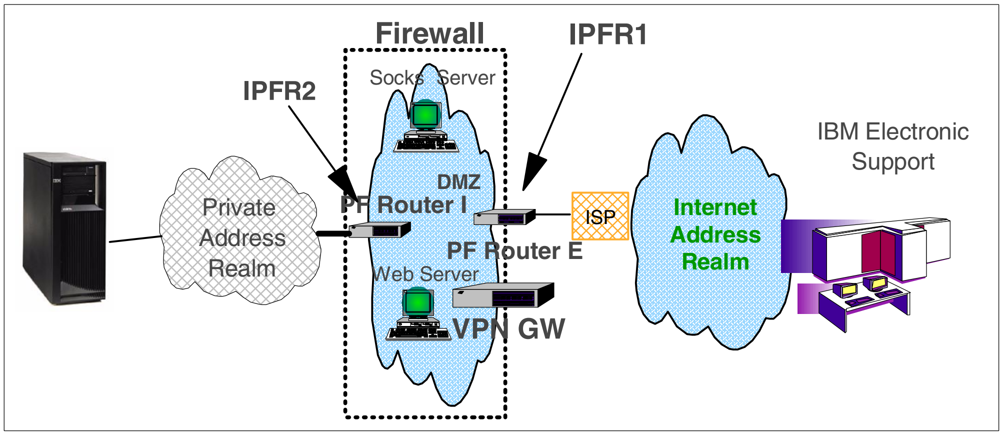


Figure 146. Merged interior router and stand-alone VPN secure gateway configuration

In this implementation, an additional packet filter router is necessary to route traffic through the VPN secure gateway to PF router E, which is connected to the ISP. Therefore, the additional packet filter router must be configured with IP packet filter rules, as indicated by IPFR1 and IPFR2 in Figure 146. Those rules are outlined in Table 45 and Table 46. The IP packet filter rules on the packet filter router that is connected to the ISP are the same as those in Table 45.

Table 45. IP packet filter rules for IPFR1

IP filter rules	IP filter values
UDP Inbound traffic filter rule	Allow port 500 for GWA IP address
UDP Outbound traffic filter rule	Allow port 500 for GWA IP address
ESP Inbound traffic filter rule	Allow ESP protocol (X'32') for GWA IP address
ESP Outbound traffic filter rule	Allow ESP protocol (X'32') for GWA IP address

You can find the GWA IP address by going to: `http://www.as400service.ibm.com`

See “Note” on page 154 for details.

Table 46. IP packet filter rules for IPFR2

IP filter rule	IP filter value
UDP Outbound traffic filter rule	Allow port 1701 for source IP address of VPN secure gateway (for example, 10.10.10.1)
UDP Inbound traffic filter rule	Allow port 1701 for destination IP address of VPN secure gateway (for example, 10.10.10.1)

5.2.5.2 Combined interior/exterior routers

Figure 147 shows the combined interior/exterior routers configuration.

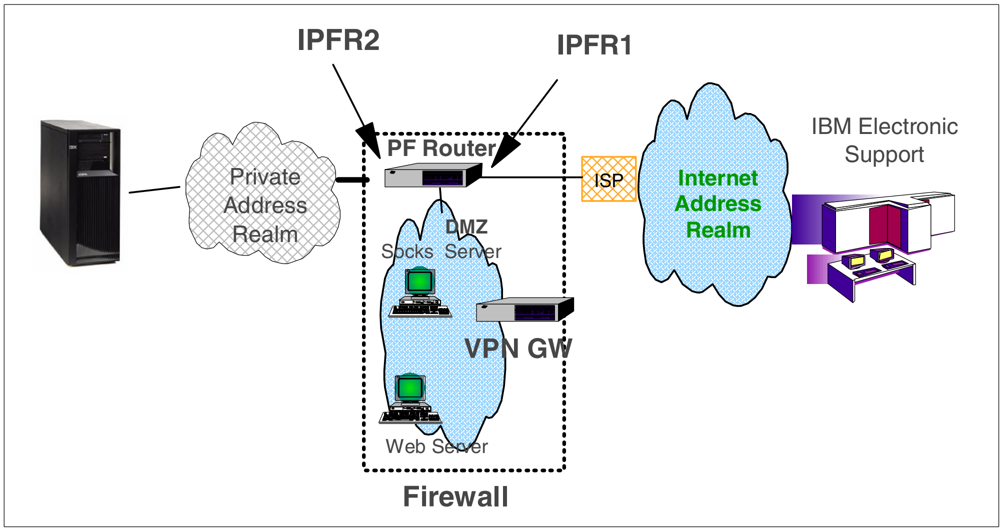


Figure 147. Merged exterior router and stand-alone VPN secure gateway configuration

In this implementation, additional filter rules are necessary on the packet filter router since the VPN secure gateway is now included as part of the DMZ. These filter rules are indicated by IPFR1 and IPFR2 in Figure 147. Rules for IPFR1 are outlined in Table 47 and those for IPFR2 are outlined in Table 48.

Table 47. IP packet filter rules for IPFR1

IP filter rules	IP filter values
UDP Inbound traffic filter rule	Allow port 500 for GWA IP address
UDP Outbound traffic filter rule	Allow port 500 for GWA IP address
ESP Inbound traffic filter rule	Allow ESP protocol (X'32') for GWA IP address
ESP Outbound traffic filter rule	Allow ESP protocol (X'32') for GWA IP address

You can find the GWA IP address by going to `http://www.as400service.ibm.com`

For details, see “Note” on page 154.

Table 48. IP packet filter rules for IPFR2

IP filter rule	IP filter value
UDP Outbound traffic filter rule	Allow port 1701 for source IP address of VPN secure gateway (for example, 10.10.10.1)
UDP Inbound traffic filter rule	Allow port 1701 for destination IP address of VPN secure gateway (for example, 10.10.10.1)

5.3 Prerequisites

The prerequisites for creating a multi-hop connection using the Universal Connection Wizard include:

- Client Access Express V5R1M0 with the latest Service Pack is required to obtain the wizard.

- TCP/IP Connectivity Utilities (5722-TC1) is required.
- Crypto Access Provider 128-bit/56-bit for AS/400 (5722-AC3) or Crypto Access Provider 56-bit for AS/400 (5722-AC2) is required.
- Ensure that the iSeries server is at OS/400 V5R1M0 with the latest cumulative applied.
- Ensure the QRETSVRSEC system value is set to `1`, which can be done by using the Display System Value (DSPSYSVAL) command. If it is not set to “1”, run the Change System Value (CHGSYSVAL) command to change it.
- TCP/IP must be active on the iSeries server (it can be started using the Start TCP/IP (STRTCP) command).
- The user that is configuring the wizard requires *ALLOBJ and *IOSYSCFG authority as part of their iSeries user profile.
- The router to be used must support L2TP with IP/FW plus IPSEC56. The following Cisco platforms meet these standards:
  - Cisco 1600 series
  - Cisco 1700 series
  - Cisco 2500 series
  - Cisco 2600 series
  - Cisco 3600 series
  - Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
  - Cisco AS5200
  - Cisco AS5300
  - Cisco 6400 series
  - Cisco 7200 series
  - Cisco 7500 series

  You can find more information on configuring the packet filter router for multi-hop at: `http://www.cisco.com/warp/public/471/l2tp_multihop1.html`

  Or contact your packet filter router vendor.
- Configure IP packet filter rules on the VPN secure gateway router according to the network configuration that is used.

5.4 Completing the planning worksheet for multi-hop

Figure 148 shows a sample diagram of the multi-hop network configuration.

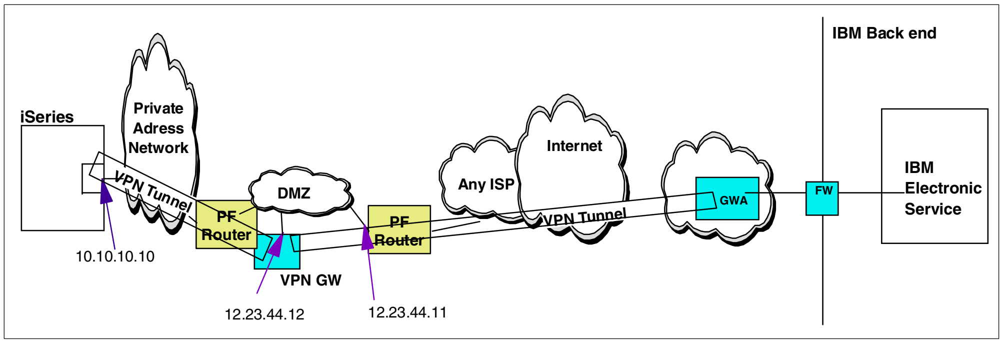


Figure 148. Multi-hop network configuration example

Complete the iSeries server planning worksheet as shown in Table 49. The planning worksheet allows you to gather all the configuration data before the actual implementation occurs.

Table 49. Multi-hop configuration information

Wizard questions	Possible answers
What is the service contact information? - Company - Contact name - Phone - Alternate phone number - Fax number	 IBM Mike Alexander 111-111-1111 222-222-2222 333-333-3333
What is the service contact mailing address? - Street address - City/state - Country - ZIP code - National language version - Media for PTFs	 Hwy 52 North Rochester/Minnesota United States 55901 English (2924) Automatic selection
Where is your server located? - Country - State or Province	 United States Minnesota
What country is your server located in? (if My location is not in list was selected) - Country code - Country name - State or province code - State or province name - Hemisphere	Only if needed
What application are you using over this connection? - Electronic Customer Support (ECS) or - IBM Electronic Service Agent	Electronic Customer Support
What type of connection are you using for your Universal Connection?	A multi-hop connection to the Internet
What is the packet filter router with VPN secure gateway IP address?	12.23.44.12

5.5 Requirements for the packet filter router configuration

This section briefly discusses the key configuration parameters that must be configured in the packet filter router with VPN secure gateway for the multi-hop connection. Some examples are also given using the Cisco Model 2600 router configuration file. This is not intended to be an exhaustive list of steps to follow in configuring the packet filter router but only as a guide to the requirements that are necessary for the multi-hop connection to work. Any detailed information on how to configure a specific router to meet these requirements should be addressed to the router vendor.

As mentioned in 5.3, “Prerequisites” on page 157, the router used in the multi-hop scenarios must support L2TP with IP firewall and IPSec56. The following lines take you through an example of how this is done on the Cisco 2600 router when used as a Standalone Packet Filter router with VPN secure gateway. To familiarize yourself with this configuration, refer to 5.2.1, “Extreme router merged with a VPN secure gateway connection” on page 152. The comments in parentheses that follow each line explain its function. These comments should not be included in your configuration file.

The first step in configuring the packet filter router is to enable VPN and multi-hop:

- `vpdn enable`: This is the master switch for the VPN function.
- `vpdn multihop`: This is the master switch for muti-hop.

As mentioned earlier, these parameters vary from router to router. Contact your router vendor for more specific information on its configuration.

The next step is to create two groups: one to accept client connections (in this case, a connection from the iSeries server) and another to initiate a server connection (in this case, a connection to the IBM gateway). In this example, you create these groups with the names *Clients* and *Servers*. The configuration on the Cisco 2600 looks something like this:

```
vpdn-group Clients (group name)
accept-dialin (accept an incoming connection)
protocol l2tp (select L2TP protocol)
virtual-template 1 (PPP portion of virtual interface; described on page 161)
no l2tp tunnel authentication

vpdn-group Servers (group name)
request-dialin (initiate an outgoing connection)
protocol l2tp (select L2TP protocol)
domain iecare1.ibm.com (domain to contact)
initiate-to xxx.xxx.xxx.xxx (GWA IP address to contact)
no l2tp tunnel authentication
```

Clients is a simple L2TP Network Server (LNS). An LNS is defined as a device operating on any platform capable of PPP termination that handles the server side of the L2TP protocol. Since L2TP relies on the single media over which L2TP tunnels arrive, an LNS may have only a single LAN or WAN interface, yet still terminate calls arriving, if configured, from the whole range of individual LACs. In general, an LNS is the initiator of outgoing calls and the receiver of incoming calls. However, if multi-hop is enabled, the LNS is restricted to only being the receiver and not the initiator. In our example, the Clients group simply accepts an incoming L2TP connection from the iSeries server.

Servers is a simple L2TP Access Concentrator (LAC). A LAC is defined as a device co-located with a PPP end system capable of handling the L2TP protocol. A LAC device implements the media, over which L2TP passes traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. In general, LAC is the initiator of incoming calls and the receiver of outgoing calls. However, if multi-hop is enabled, the LAC is restricted to only being the initiator and not the receiver. In addition, the LAC only initiates if the mapping process succeeded and a match is found. In this example, the Servers group is responsible for initiating the connection to the IBM gateway. That’s because the dial-in user identifies itself with the string userID@iecare1.ibm.com, and the LAC group Servers is recognized as the one configured with domain iecare1.ibm.com (the domain to contact). Therefore, a match is found.

The next step is to set the authentication policies to be used in the connection from the packet filter router to the IBM gateway. First, the policies for the pre-share IKE key exchange are defined. An example on the Cisco 2600 is shown here:

```
crypto isakmp policy 1
encr des
hash md5
authentication pre-share
DF group 1
lifetime 1 day
crypto isakmp key IBMGW address xxx.xxx.xxx.xxx (*)
crypto ipsec transform-set IBMGW esp-des esp-md5-hmac
mode transport
crypto map IBMGW 1 ipsec-iaskmp
set peer 207.25.252.196
set transform-set IBMGW
set pfs group1
match address 101 (use access-list 101; discussed on page 162)
```

Note (*)

You can find the GWA IP address by going to: `http://www.as400service.ibm.com`
For details, see “Note” on page 154.

Refer to your router vendor for more information on setting these parameters on your specific router.

The interface on the router that handles both incoming and outgoing traffic must also be configured. It is assumed that this would have already been done when initially configuring the router. The IPSecCD is applied on this interface. Access lists can also be referenced here that funnel traffic only through the tunnel that is going to be created from the multi-hop connection. The Cisco 2600 example shows this:

```
interface FastEthernet0/1
ip address 12.34.44.12 255.255.255.0 (IP address of router)
duplex auto
speed auto
random-detect
crytpo map IBMGW (IPSec CD)
ip rsvp bandwidth 7500 7500
```

Earlier in your Clients group definition, you specified a virtual template that is the PPP portion of the routers virtual interface. This virtual interface must also be configured on the router since it acts as the mutli-hop incoming interface. This interface plays the role of the LNS as described previously. Its main function is to redirect the PPP connection to the multi-hop destination. This, in turn, accepts the delivered user ID name from the iSeries server L2TP connection. This user ID is then attached to the domain specified in the Servers group. An example on the Cisco 2600 is shown here:

```
interface Virtual-Template1
```

```
ip unnumbered FastEthernet0/1 (references the physical interface name)
ip mroute-cache
no peer default ip address
ppp authentication chap (chap is used for PPP authentication)
```

One of the most important configuration steps that must be taken is to add a route to the IBM gateway. This route should specify the address of the gateway as well as the next hop. A static route is suggested. An example of this is shown on the following line, where *xxx.xxx.xxx.xxx* is the GWA IP address:

```
ip route xxx.xxx.xxx.xxx 255.255.255.255 12.34.44.11 (12.34.44.11 is next hop)
```

Note

You can find the GWA IP address on the Web at: `http://www.as400service.ibm.com` For details, see “Note” on page 154.

The access list is also an important part of the packet filter router configuration. You have already seen an instance where an access list is referenced. For this example, with the 2600 Cisco router, this is the access-list entry that is needed:

```
access-list 101 permit udp host 12.34.44.12 host xxx.xxx.xxx.xxx log
```

udp must be specified. *xxx.xxx.xxx.xxx* is the GWA IP address.

Once these packet filter parameters are configured, the Universal Connection multi-hop connection should function properly. If it does not, you must address any troubleshooting or problem determination from the packet filter router with the router vendor. Keep in mind what is required for the multi-hop scenarios. Problem determination on the connection between the iSeries server and the packet filter router are discussed further in Chapter 6, “Troubleshooting tips” on page 173.

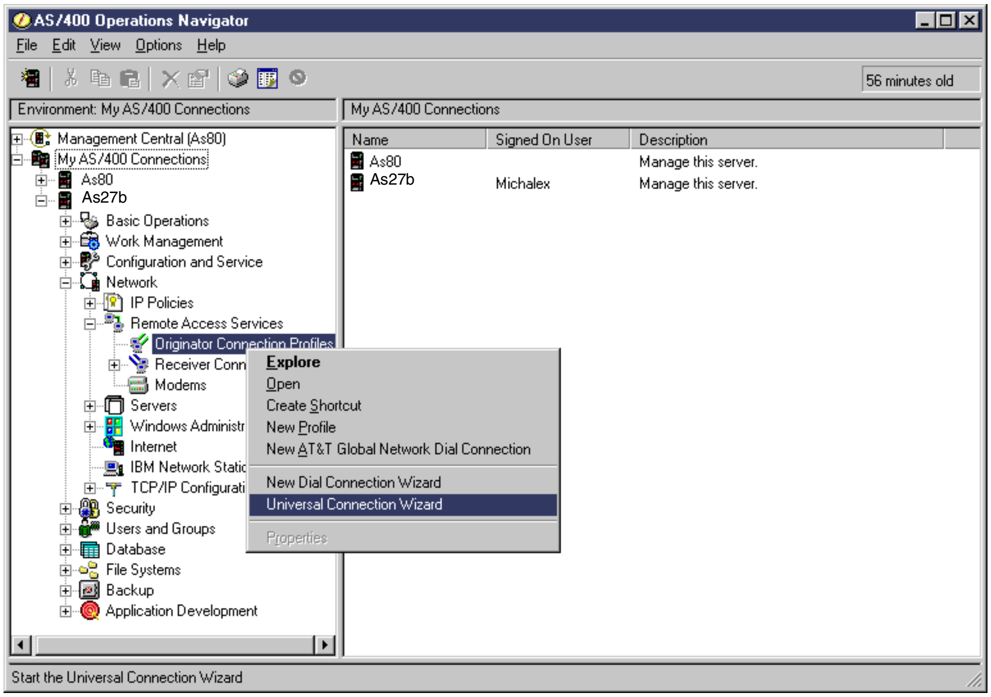
5.6 Configuring a multi-hop connection

This section outlines how the Universal Connection is configured using the multi-hop configurations that we’ve discussed in this chapter. The packet filter router and all IP packet filter rules must be configured prior to running the Universal Connection Wizard. Refer to 5.2, “Multi-hop network configurations” on page 152, for more information on network configurations and IP packet filter rules.

For this example, you use the stand-alone router with VPN secure gateway configuration. The IP address provided in the wizard is the IP address of the packet filter router that is located in front of the firewall as shown in Figure 142 on page 152. Perform the following steps to configure the multi-hop connection using the Universal Connection Wizard:

1. Start Operations Navigator.
2. Expand the iSeries server and sign on with a valid iSeries user ID and password if prompted.
3. Expand **Network**.
4. Click **Remote Access Services**.

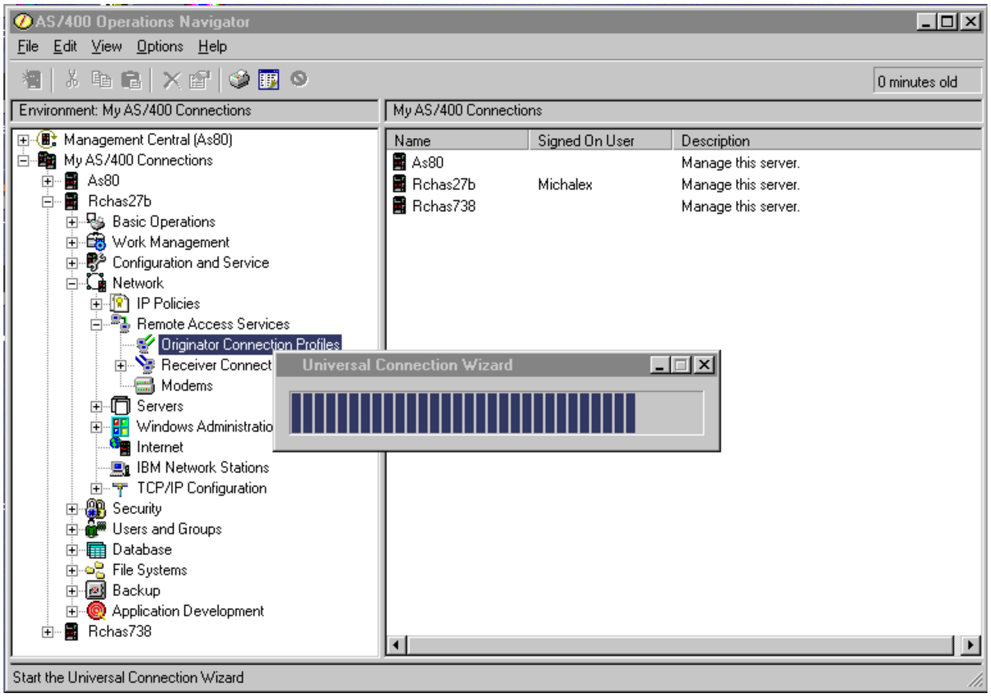
5. Right-click **Originator Connection Profiles**. On the pull-down menu, choose **Universal Connection Wizard** as shown in Figure 149.



Name	Signed On User	Description
As80		Manage this server.
As27b	Michalex	Manage this server.

Figure 149. Selecting Universal Connection Wizard

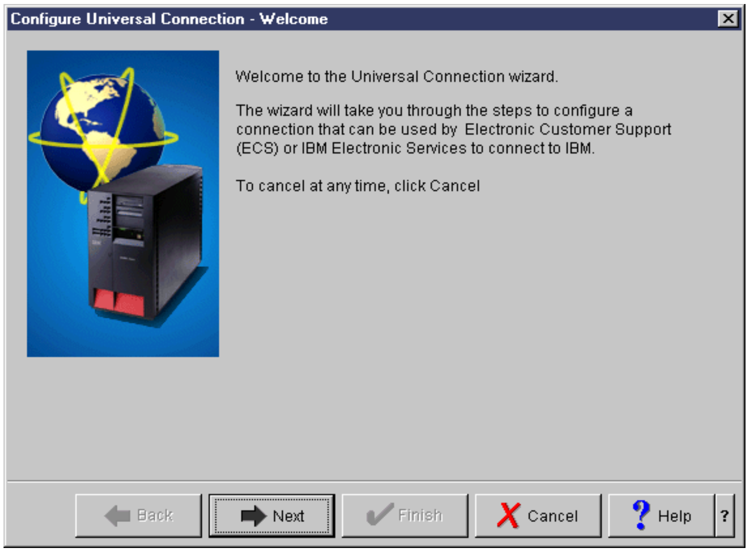
6. A progress bar, like the example shown in Figure 150, appears indicating that the application is in processing mode.



Name	Signed On User	Description
As80		Manage this server.
Rchas27b	Michalex	Manage this server.
Rchas738		Manage this server.

Figure 150. Progress bar for the Universal Connection Wizard

7. The Welcome display (Figure 151) appears first for the wizard. Click **Next** to continue to the next display.



Configure Universal Connection - Welcome

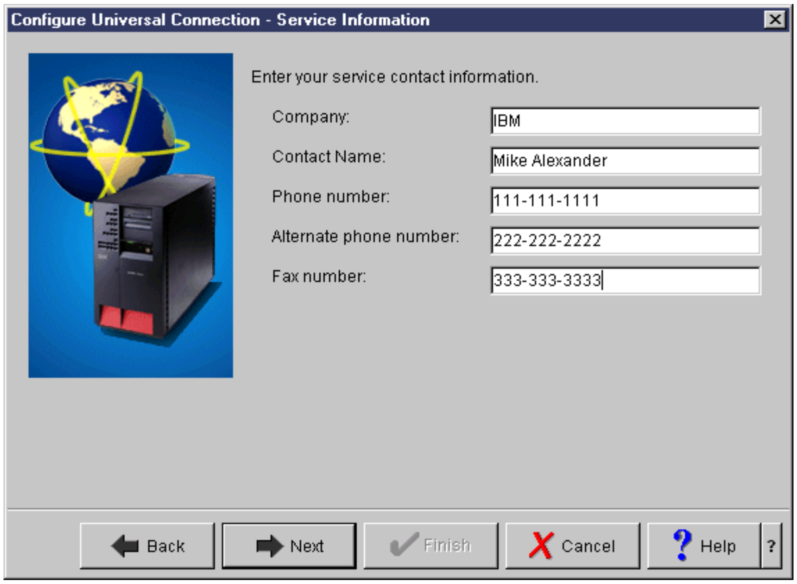
Welcome to the Universal Connection wizard.

The wizard will take you through the steps to configure a connection that can be used by Electronic Customer Support (ECS) or IBM Electronic Services to connect to IBM.

To cancel at any time, click Cancel

Figure 151. Universal Connection Wizard - Welcome display

8. The Service Information display shown in Figure 152 allows you to enter service contact information. You must complete the first three fields. This display updates the same information as the Work with Contact Information (WRKCNTINF) option 2 on a 5250 emulation screen. If that information has already been entered on the iSeries server, these parameters are pre-filled. Click **Next** to continue.



Configure Universal Connection - Service Information

Enter your service contact information.

Company: IBM

Contact Name: Mike Alexander

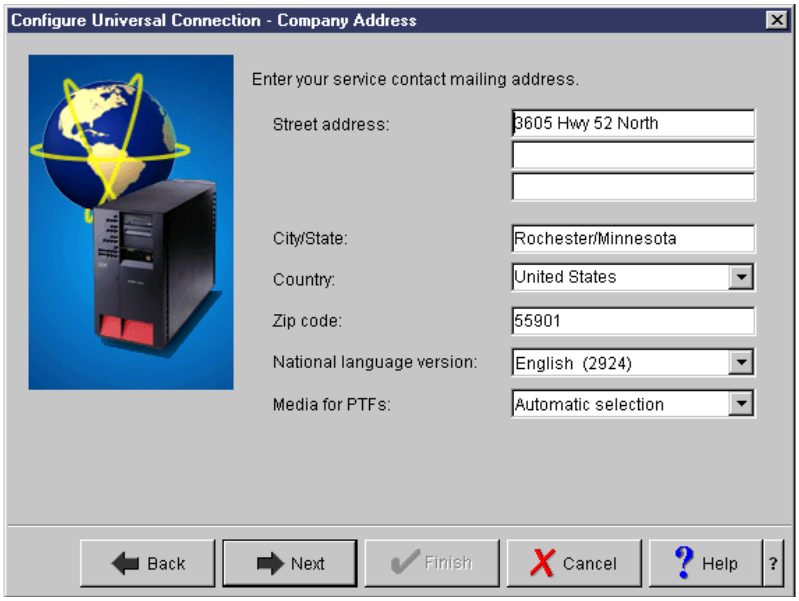
Phone number: 111-111-1111

Alternate phone number: 222-222-2222

Fax number: 333-333-3333

Figure 152. Service contact information

9. On the display shown in Figure 153, enter the address where the iSeries server service contact is located. For Country, National language version, and Media for PTFs, select from the pull-down lists. Click **Next** to continue.


Configure Universal Connection - Company Address

Enter your service contact mailing address.

Street address: 3605 Hwy 52 North

City/State: Rochester/Minnesota

Country: United States

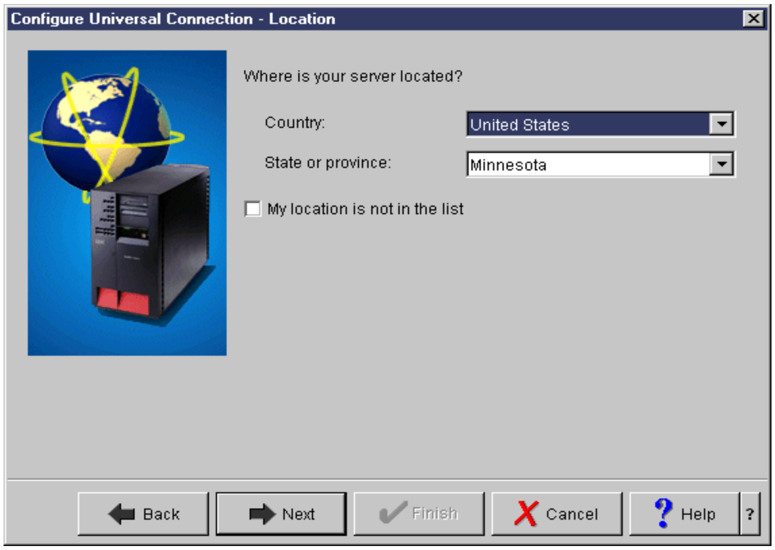
Zip code: 55901

National language version: English (2924)

Media for PTFs: Automatic selection

Figure 153. Company Address display

10.At the Location display shown in Figure 154, select the country, state, or province. The My location is not in the list check box is only selected if a country is not listed. Click **Next** to continue.


Configure Universal Connection - Location

Where is your server located?

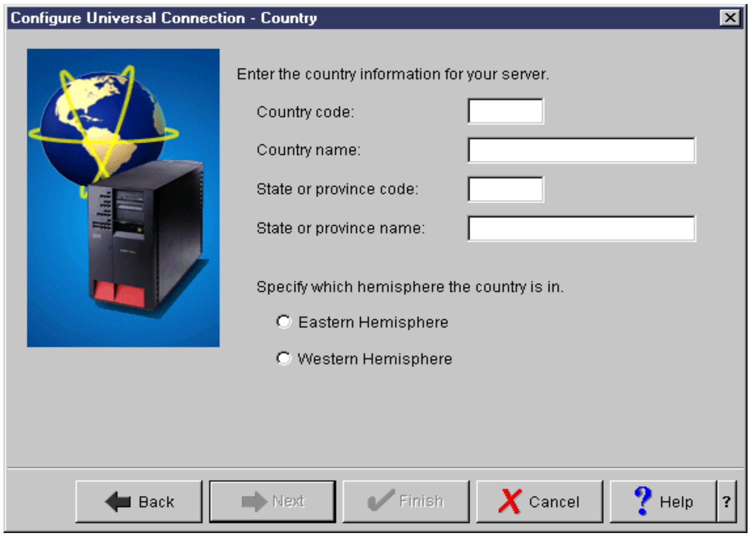
Country: United States

State or province: Minnesota

□ My location is not in the list

Figure 154. Location information

Figure 155 shows the display that appears if the My location is not in the list box is selected. Hemisphere specification is used to look up default nodes for the application.



Configure Universal Connection - Country

Enter the country information for your server.

Country code:

Country name:

State or province code:

State or province name:

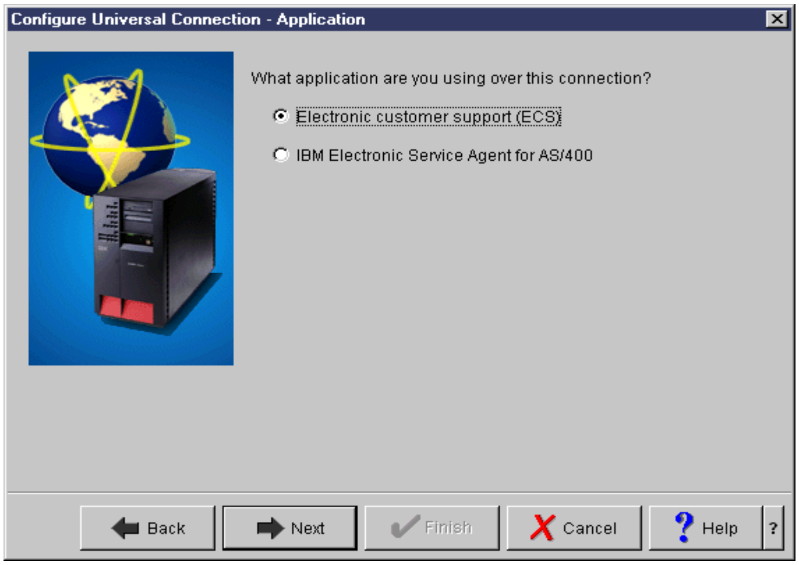
Specify which hemisphere the country is in.

○ Eastern Hemisphere

○ Western Hemisphere

Figure 155. Country information if not in list

11. The Application selection display appears next as shown in Figure 156. There are two applications listed: ECS and Electronic Service Agent. ECS is part of OS/400, while Electronic Service Agent requires product 5798RZG. If that product is installed, you can select the Electronic Service Agent radio button. Selecting Electronic Service Agent has no effect on how ECS works. Select the application to be used, and click **Next** to continue.



Configure Universal Connection - Application

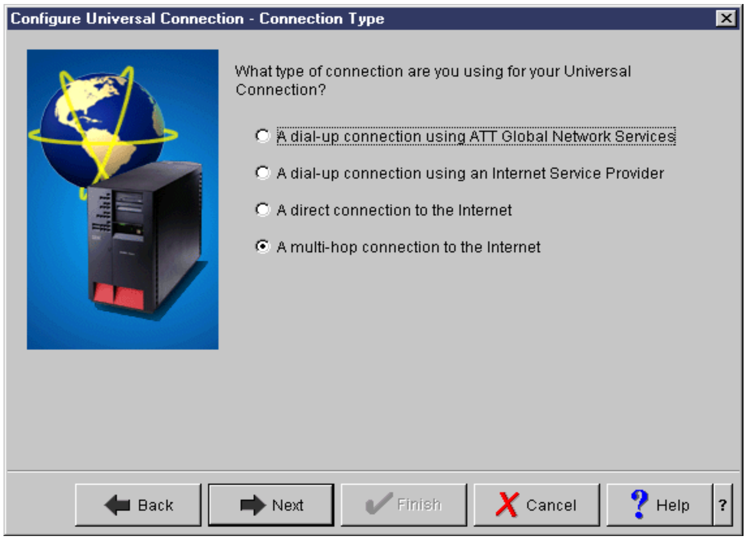
What application are you using over this connection?

● Electronic customer support (ECS)

○ IBM Electronic Service Agent for AS/400

Figure 156. Application selection

12. The next display prompts for the Connection Type as shown in Figure 157. There are four options. Select **A multi-hop connection to the Internet**, and click **Next** to continue.



Configure Universal Connection - Connection Type

What type of connection are you using for your Universal Connection?

○ A dial-up connection using ATT Global Network Services

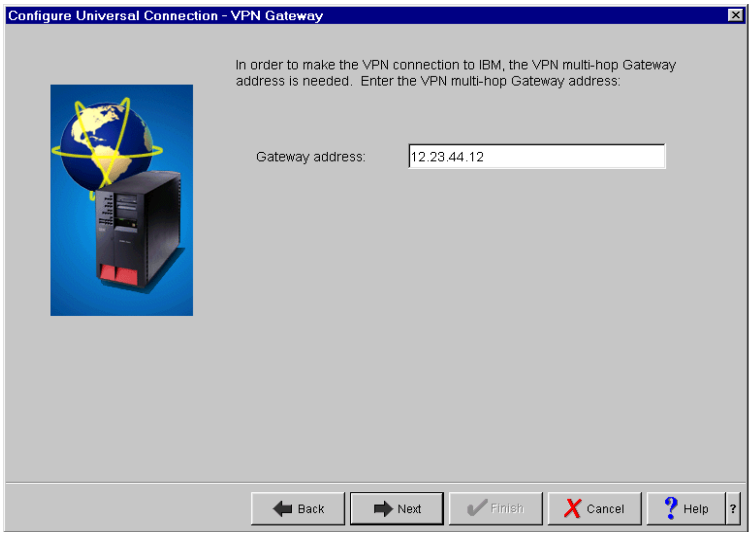
○ A dial-up connection using an Internet Service Provider

○ A direct connection to the Internet

● A multi-hop connection to the Internet

Figure 157. Connection Type

13.The next display, shown in Figure 158, prompts for the VPN multi-hop gateway address. This is the IP address of the packet filter router that connects to the ISP. Type this IP address, and click **Next** to continue.



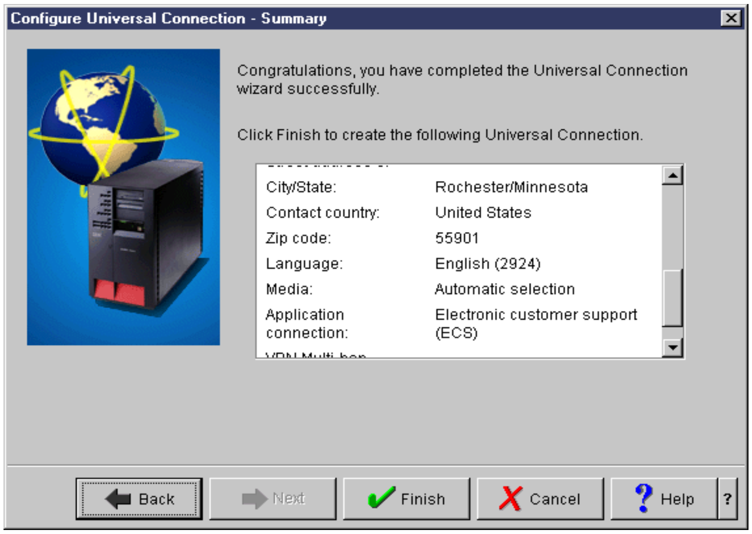
Configure Universal Connection - VPN Gateway

In order to make the VPN connection to IBM, the VPN multi-hop Gateway address is needed. Enter the VPN multi-hop Gateway address:

Gateway address: 12.23.44.12

Figure 158. Entering the packet filter router IP address

14.This concludes the Universal Connection configuration for the multi-hop connection. On the display shown in Figure 159, click **Finish** to accept the parameters provided.



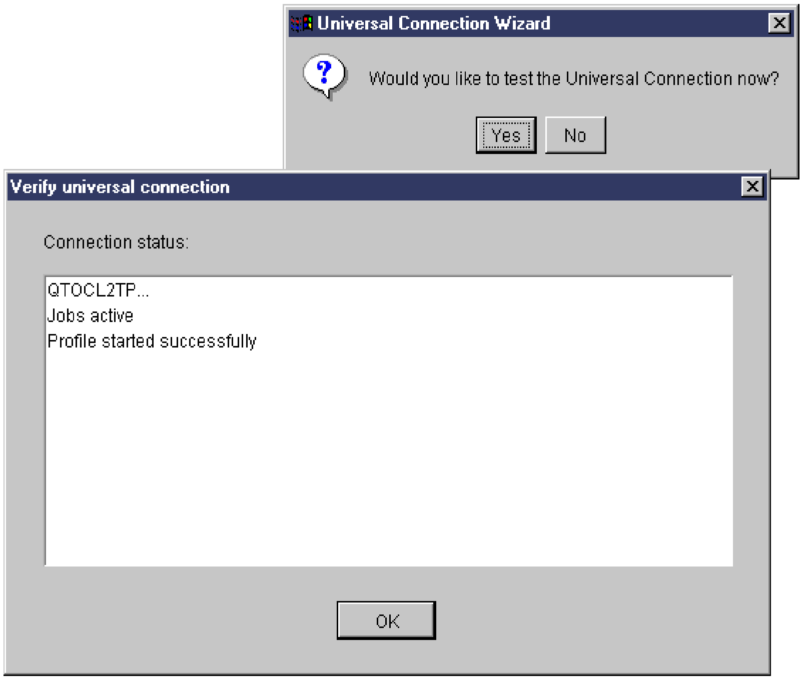
Congratulations, you have completed the Universal Connection wizard successfully.

Click Finish to create the following Universal Connection.

City/State:	Rochester/Minnesota
Contact country:	United States
Zip code:	55901
Language:	English (2924)
Media:	Automatic selection
Application connection:	Electronic customer support (ECS)

Figure 159. Summary display

15.After you click Finish, the pop-up window shown in Figure 160 appears. It asks if you want to test the Universal Connection. Selecting Yes causes Universal Connection to start the VPN profile for testing purposes. No information is exchanged. A connection status window appears showing whether the test was successful.



Would you like to test the Universal Connection now?

Connection status:

```
QTOCL2TP...
Jobs active
Profile started successfully
```

Figure 160. Verifying the Universal Connection

5.7 Definitions created by the wizard for a multi-hop connection

For the multi-hop connection, there is only one definition that is created by the Universal Connection Wizard. Unlike Direct Connection cases mentioned earlier, the Universal Connection Wizard is only responsible for creating the L2TP connection from the private intranet to the packet filter router. This L2TP connection is not secured by IPSec, so no IPsec definitions are created.

5.7.1 QTOCL2TP profile

The QTOCL2TP L2TP initiator profile is the only definition created by the Universal Connection Wizard. To access the QTOCL2TP definition, follow these steps:

1. Start Operations Navigator.
2. Expand the iSeries server. Sign on with a valid iSeries user ID and password if prompted.
3. Expand **Network**.
4. Expand **Remote Access Services**.
5. Click **Originator Connection Profiles**.
6. Locate and right-click **QTOCL2TP** in the right pane of Operations Navigator. Select **Properties**.

The values of the QTOCL2TP definition created by the Universal Connection wizard are shown in Table 50.

Table 50. Values of the QTOCL2TP definition created by the wizard

Parameters	Values
General - Name - Description - Protocol type - Mode type	 QTOCL2TP Created by Universal Connection Wizard PPP L2TP (virtual line) - initiator
Connection - Link configuration type of line service - Virtual line name - Remote tunnel endpoint IP address - Requires IPSec protection connection group name - Line inactivity time-out	 Virtual Line (L2TP) QTOCL2TP 10.10.10.1 Not checked None 600

Parameters	Values
QTOCL2TP Line definition	
General	
- Name	QTOCL2TP
- Description	Created by Universal Connection Wizard
- Mode type	L2TP (virtual line) - initiator
Link	
- Bandwidth reservation	115200
- Maximum frame size	1500
- Enable packet sequence numbering	Not checked
- Activate tunnel keep alive	Checked
Limits	
- LCP authentication	
Authenticate remote peer periodically	Not checked
Maximum authentication attempts	8
- LCP configuration	
Configuration retry timer	5
Maximum configuration failures	5
Maximum configuration requests	10
Maximum termination requests	10
- Recovery limits	
Count limit	2
Maximum time-out	10
Authentication	
- Local host name	as026
Remote system L2TP tunnel authentication	
- Require this iSeries server to verify the identity of the remote L2TP terminator system	Not checked
Authentication	
Local system identification	
- allow the remote system to verify the identity of this iSeries server	Checked
- Authentication protocol to use	Require encrypted password (CHAP-MD5)
User name	`i400@iecare1.ibm.com`
Password	*****************
- Remote system identification requires this iSeries server to verify the identity of the remote system	Not checked
TCP/IP settings	
- Local IP address	Assigned by remote system
- Remote IP address	Assigned by remote system
- Routing	Define additional static routes
- Hide addresses (full masquerading)	Not selected
QTOCL2TP routing	IP address will vary based on the iSeries system location.
DNS	
- Domain name server	Do not use
Other	
Subsystem	
- Enter the name of the subsystem in which to run L2TP connection jobs	QSYSWRK
Connection Scripts	
- Use connection script	Not selected
- Script ASCII coded character set identifier	819

5.8 Security over a multi-hop connection

Security over a multi-hop connection is contingent on the VPN secure gateway function of the packet filter router that makes the initial connection to the Internet. As mentioned before, no IPSec definitions are created by the Universal Connection since the first L2TP tunnel connects the iSeries server on a private intranet to the packet filter router with the VPN secure gateway.

The L2TP specification proposes the use of the IPSec protocol suite to protect L2TP traffic over IP when security is required (for example, over the Internet). Therefore, the L2TP connection from this VPN secure gateway to the IBM gateway is secured by IPSec based on how the packet filter router with VPN secure gateway is configured.

In summary, L2TP is an excellent way to provide cost-effective remote access. When used in conjunction with IPSec, it is the technique for providing secure remote access. However, without the complementary use of IPSec, an L2TP tunnel alone does not furnish adequate security for business communications over the Internet.

For more information on L2TP, multi-hop, and Cisco security measures and considerations, refer to the following Web sites:

- L2TP Tunnel Switching:
  `http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121dc/121dc1/l2switch.htm`
- Multi-hop: `http://www.cisco.com/warp/public/471/l2tp_multihop2.html`
- L2TP protocol:
  `http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm`
- Security:
  `http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scoverv.htm#27433`
- L2TP protocol extensions:
  `http://www.ietf.org/html.charters/l2tpext-charter.html`
- VPN and L2TP:
  `http://www.as400.ibm.com/tcpip/common/remoteacc/html/remoteaccc.htm`

Chapter 6. Troubleshooting tips

This chapter provides information on how to isolate connection problems. It includes useful commands and screen examples from good connection scenarios to better assist you in problem determination.

6.1 Considerations for using the Universal Connection Wizard

The following list presents some considerations and suggestions that you need to keep in mind when configuring a new Universal Connection:

- Hardware requirements for using Operations Navigator: Follow these requirements as listed here:

  To install and use AS/400 Operations Navigator, your PC must be running one of the following Windows operating systems. The processor and memory requirements for each operating system are provided in the list:

  – *Microsoft Windows NT 4.0*: Pentium processor (100 MHz or faster) and at least 64 MB of memory

  – *Microsoft Windows 95*: Pentium processor (100 MHz or faster) and at least 64 MB of memory

  – *Microsoft Windows 98*: Pentium processor (100 MHz or faster) and at least 64 MB of memory

  – *Microsoft Windows 2000*: No requirements beyond the Microsoft recommendations for installing Windows 2000

  – *Microsoft Windows ME (Millenium Edition)*: No requirements beyond the Microsoft recommendations for installing Windows Millenium Edition

  We strongly recommended that each of these operating systems have 128 MB of memory for V5R1 of Client Access Express.

- The Universal Connection Wizard is a Java-based application, which means that problems may be encountered if using Windows 95 machines that do not have the latest Winsock client. The latest Winsock client is recommended for use with Operations Navigator in general. Windows 95 with Service Pack 2 or 2.1 contains the latest Winsock updates. Therefore, PCs at this code level do not need to be updated. Only if Windows 95 Service Pack release 1 or earlier is installed, updates are needed. The update can be found at

  `http://www.microsoft.com`

  The Windows 98, ME, and 2000 clients come equipped with the latest clients in its base code. A Windows NT client should also have the latest Service Packs installed to be at the correct Winsock level.

- The progress bar shown in Figure 161 may not always look the same. This is simply an adaptation of the Java code in certain environments. It does not indicate a failure or that the application is not behaving as it should.

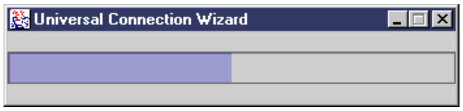
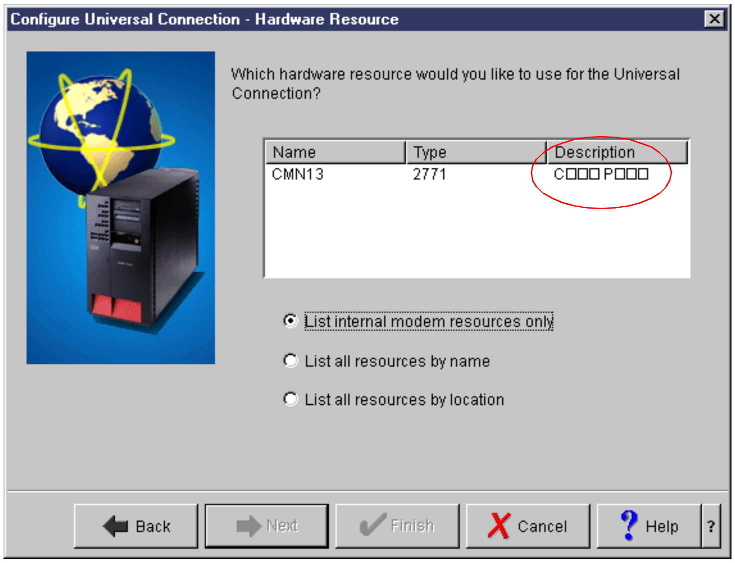


Figure 161. Progress bar may not always look the same

- If you are using a double byte character set (DBCS) iSeries server, some of the options in the wizard may contain extra characters as shown in Figure 162. Ignore these since they have no effect on the configuration of the PPP profile.



Which hardware resource would you like to use for the Universal Connection?

Name	Type	Description
CMN13	2771	C□□□ P□□□

● List internal modem resources only
○ List all resources by name
○ List all resources by location

Figure 162. Description field contains invalid characters

- Hardware considerations for the iSeries server, such as usage and support for the new 9771 adapter card, can be reviewed at the following Web site:

  `http://www.as400.ibm.com/tstudio/planning/esa/esa.htm`

  This site also outlines using the 7852-400 with the new 9771 adapter and what functions can be used.

6.2 PC troubleshooting

Problems that exist on the PC are usually either caused by the operating system on the PC or the application being used. Operating system issues are outside the scope of this section, but mention is made of some of the symptoms to look for.

The following sections cover some basic and common areas where problems can occur. Possible causes for each are addressed as well as solutions or workarounds.

No network component is listed

If the network component is not listed under your iSeries server in Operations Navigator, chances are it was not installed or it was removed at some time. A typical installation of Client Access Express only gives the Basic Operations component of Operations Navigator. To obtain the network component, either install Client Access Express using the Full option, or select Custom Install and choose Network as an option to install. Otherwise, if Client Access Express has already been installed, run the Selective Setup function and add the network component to Operations Navigator.

No Remote Access Service function is listed under Network

If Client Access Express V4R5M0 with SF64217 or later was installed on the PC, then there is no Remote Access Service function under Network. This was introduced in V5R1M0 of the client. Instead, go to **Point-to-Point** and right-click

Connection Profiles. This is the equivalent of selecting Remote Access Service and then Originator Connection Profiles in V5R1M0 of Client Access Express.

No Universal Connection Wizard option is listed

If, after right-clicking Originator Connection Profiles (Connection Profiles for V4R5M0), there is no Universal Connection Wizard option, check for the following possibilities:

- Is Client Access Express V4R5M0 with SF64217 or later installed on the PC?
- Is the iSeries server being accessed at V4R5M0 of OS/400 or above?
- Are PTFs SF64122, SF64123, and SF64124 applied on the iSeries server if the system is at V4R5M0 of OS/400?

Nothing appears on the screen after selecting Universal Connection Wizard

After you click the Universal Connection Wizard option, a progress bar should appear on the screen. This indicates that the wizard is currently being loaded. If that does not appear, or an error box pops up, this may indicate that the PC operating system does not have the latest Windows Service packs and Winsock clients installed. Obtain these, install them, and retry the wizard.

After choosing the ECS application, there is no selection for Connection Type

If, after choosing the ECS application, you are taken to the screen to select Resource Name for the connection, the iSeries server you are using may not have VPN connectivity support. Currently, only systems running at V5R1M0 have this capability. Therefore, if the iSeries server is at a lower release of OS/400, this screen does not appear.

There is no prompt to enter a line description for your connection

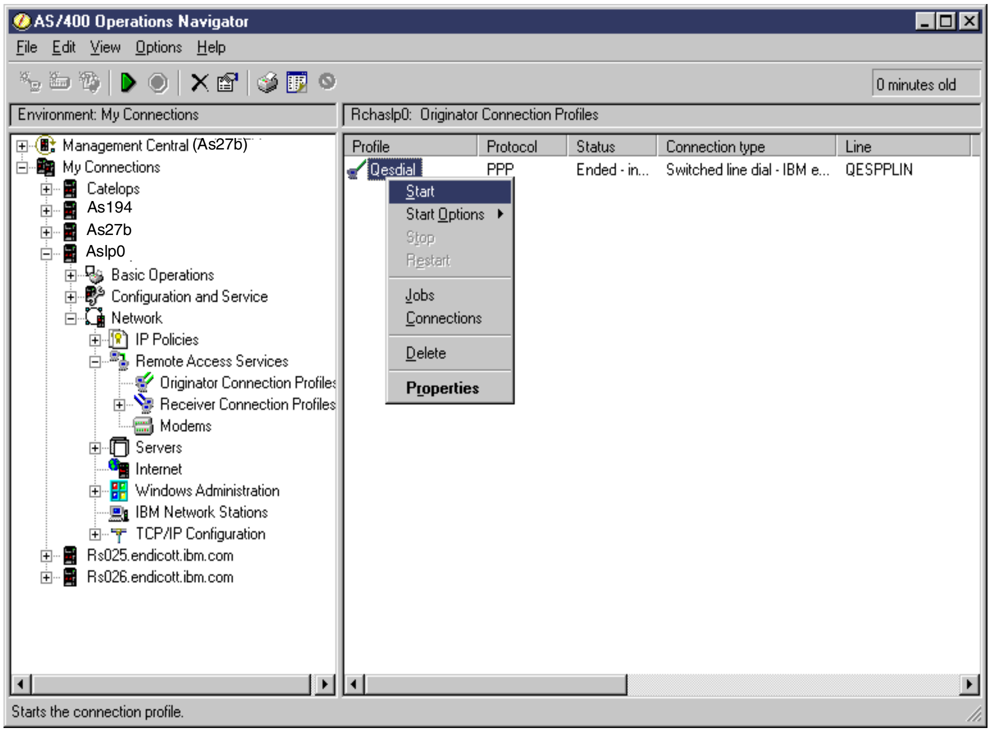
If only one line description already exists for the resource that was selected earlier, that line is automatically selected for use with the AGNS connection. If you want to specify a different line name, either delete the existing line or create a dummy line for that resource. You are then prompted to create a new line for this connection.

You ran the wizard but your contact information did not automatically update on your iSeries server

If the wizard is being run using Client Access Express V4R5M0, the contact information is not automatically updated if it did not previously exist. Contact information is, however, updated if data was already there. This feature is changed in the V5R1M0 version of Client Access Express so that contact information is updated regardless of whether it existed. To manually update the Contact Information, use the `WRKCNTINF` command. Then, select option `2` (Work with local service information) and select option `2` (Change service contact information) on the next screen.

You did not test the connection after the wizard was finished (manually testing it afterwards)

The Test option that is presented at the end of the configuration only attempts to start the new PPP profile. This can be manually done either through Operations Navigator or a 5250 emulation. From Operations Navigator, expand the iSeries server, then select **Network->Remote Access Services->Originator Connection Profiles**. Right-click **QESDIAL** and select the **Start** option as shown in Figure 163. If the PPP profile is functional, it becomes Active.



Profile	Protocol	Status	Connection type	Line
Qesdial	PPP	Ended - in...	Switched line dial - IBM e...	QESPPLIN

Starts the connection profile.

Figure 163. Using the Start option to test the AGNS PPP profile

From a 5250 emulation screen, issue the `WRKTCPPTP` command and type option `9` next to the QESDIAL profile to start it. If the profile becomes active, the connection is successful.

6.3 iSeries server troubleshooting

This section describes in detail how to troubleshoot the iSeries server under each specific connection type. The connection types are:

- Dial-up AGNS
- Dial-up any ISP
- Direct connection
- Multi-hop connection

6.3.1 Dial-up AT&T Global Network Service

The Dial-up AT&T Global Network Service (AGNS) connection is the simplest of all the Universal Connections. It involves establishing a simple PPP connection from the iSeries server machine to AGNS. The wizard is responsible for creating the correct user ID and password that are used for authentication with AGNS, as well as all iSeries IFS objects.

Most problems relating to an AGNS connection can be resolved by rerunning the Universal Connection Wizard. This allows the existing QESDIAL profile to be recreated, including any damaged or corrupt IFS objects. If the problem exists on the iSeries server, a message is usually posted to indicate the failure.

To facilitate problem determination for the PPP AGNS connection, a number of new messages were introduced to the iSeries server from the Universal Connection PTFs. These message are listed and explained here:

- `TCP9302 PHONE NUMBER PROVIDED WAS NOT FOUND`

  The phone number being used to connect to AT&T Global Network Services is no longer valid. Update the current phone list by running the wizard before the next connection attempt.

- `TCP9303 CONFIGURATION INFORMATION NOT FOUND`

  There is no PPP profile and no IFS objects have been created. Run the wizard to create both the profile and the necessary objects. Otherwise, the SNA path for ECS use is used if available.

- `TCP9305 A SERVICE INFORMATION UPDATE WAS NOT PERFORMED FOR &1`

  The service application requested an update to the Connection Information table and the corresponding record was not found. The Operations Navigator Universal Connection Wizard should be run to set up the proper connection record in the table.

- `TCP930B Connection profile has failed to achieve an acceptable status.`

  The Universal Connection Manager has attempted to detect a stable status from the connection profile but failed to do so. Check the connection PPP profile for any errors and correct them using the Universal Connection Wizard.

Some other messages that you can use to troubleshoot the connection include:

- `TCP8211 Point-to-Point profile not found.`

  The PPP profile in the mapping table has been deleted or does not exist. The Universal Connection Wizard must be rerun.

- `CPF8C2E IBM ECS ERROR OCCURRED ON &1`

  See the previously listed errors in the job log for more information.

- `CPEnnnn` (where *nnnn* is the error number received by ECS)

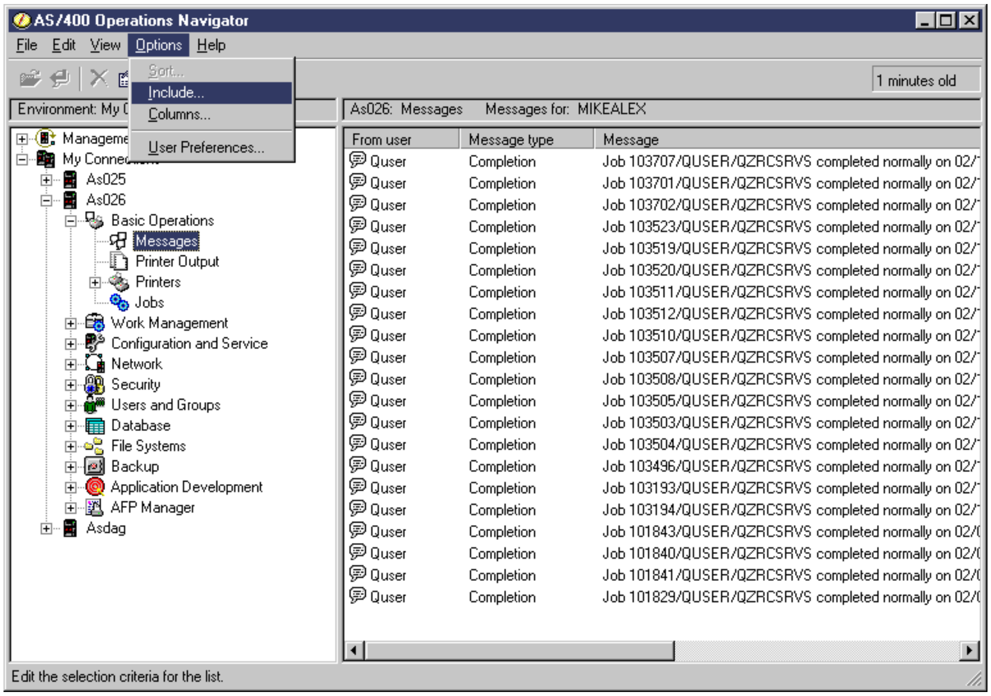
  Check the TCP/IP interface that is being used on the iSeries server for the Universal Connection and make sure it has been started.

These messages are all posted to the QSYSOPR message queue. They can be viewed either through Operations Navigator or a 5250 emulation screen. The following sections describe how to view and work with these messages in both environments.

6.3.1.1 Operations Navigator access

You can view all messages posted to the QSYSOPR system message queue through Operations Navigator. Follow these steps to look at the QSYSOPR messages:

1. Start Operations Navigator.
2. Expand the iSeries server with the QSYSOPR message queue to be viewed. Sign on with a valid iSeries user ID and password if prompted.
3. Expand **Basic Operations**.
4. Click **Messages**. Choose the **Options** menu, and click **Include** as shown in Figure 164.

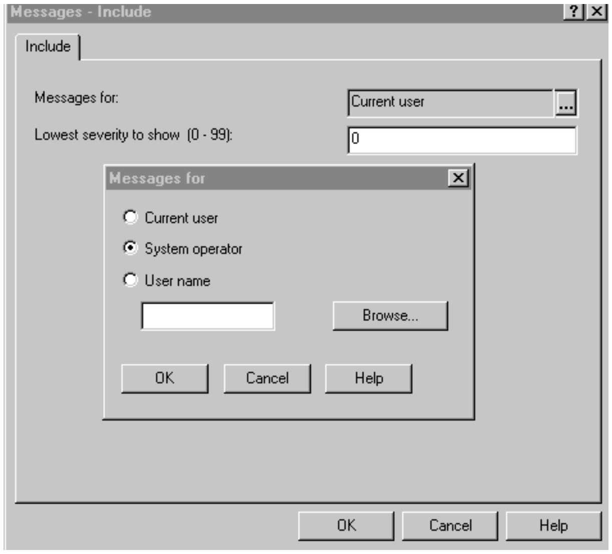


As026: Messages Messages for: MIKEALEX

From user	Message type	Message
Quser	Completion	Job 103707/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103701/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103702/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103523/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103519/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103520/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103511/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103512/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103510/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103507/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103508/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103505/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103503/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103504/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103496/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103193/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 103194/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 101843/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 101840/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 101841/QUSER/QZRCSRVS completed normally on 02/
Quser	Completion	Job 101829/QUSER/QZRCSRVS completed normally on 02/

Figure 164. Working with the Message option in Basic Operations

5. The Messages for parameter shows Current user. Click the drop-down menu and select **System operator** as shown in Figure 165.



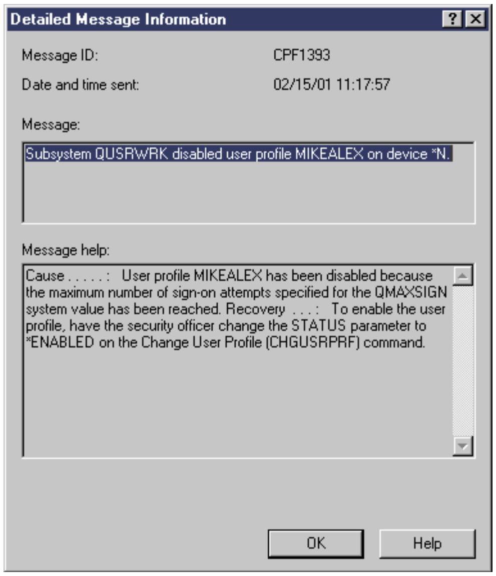
Messages for: Current user

Lowest severity to show (0 - 99): 0

○ Current user
● System operator
○ User name

Figure 165. Selecting the System Operator (QSYSOPR) message queue

6. The messages from QSYSOPR appear on the right pane of the Operations Navigator. To view details on any message, such as message ID, cause, and recovery, simply right-click the user who generated the message and choose **Details**. A display like the example shown in Figure 166 shows all the details of the message.



Message ID: CPF1393

Date and time sent: 02/15/01 11:17:57

Message:

Subsystem QUSRWRK disabled user profile MIKEALEX on device *N.

Message help:

Cause . . . . . : User profile MIKEALEX has been disabled because the maximum number of sign-on attempts specified for the QMAXSIGN system value has been reached. Recovery . . . : To enable the user profile, have the security officer change the STATUS parameter to *ENABLED on the Change User Profile (CHGUSRPRF) command.

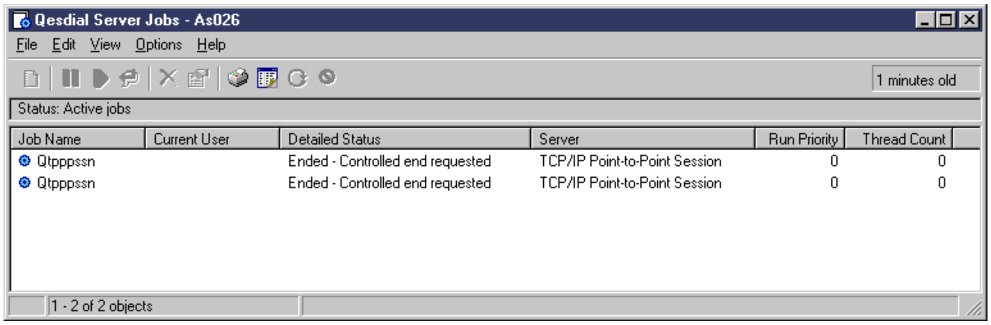
Figure 166. Details for a message posted in the QSYSOPR message queue

The job log of the QESDIAL profile can also be viewed using Operations Navigator. The following steps outline how this is done:

1. Start Operations Navigator.
2. Expand the iSeries server and sign on with a valid user ID and password if prompted.
3. Expand the **Network** component.
4. Expand **Remote Access Services** and then click **Originator Connection Profiles**.
5. A list of PPP profiles appears on the right pane of the Operations Navigator window. Locate and right-click **QESDIAL**.
6. Select the **Jobs** option. A display appears like the example shown in Figure 167.

Note

The Jobs option is not listed if the status of the PPP profile is *Inactive*. The job log of the profile can only be viewed if it has another status other than Inactive.



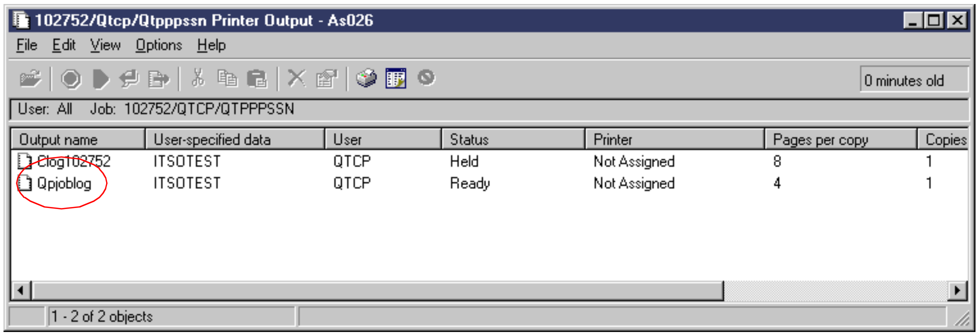
Status: Active jobs

Job Name	Current User	Detailed Status	Server	Run Priority	Thread Count
Qtpppssn		Ended - Controlled end requested	TCP/IP Point-to-Point Session	0	0
Qtpppssn		Ended - Controlled end requested	TCP/IP Point-to-Point Session	0	0

1 - 2 of 2 objects

Figure 167. Working with the QESDIAL PPP session jobs

7. Right-click the session job you want to view and select **Printer Output**. The most recent session job is usually located at the bottom of the list if there are multiple entries listed. This results in the display are shown in Figure 168.



102752/Qtcp/Qtpppssn Printer Output - As026

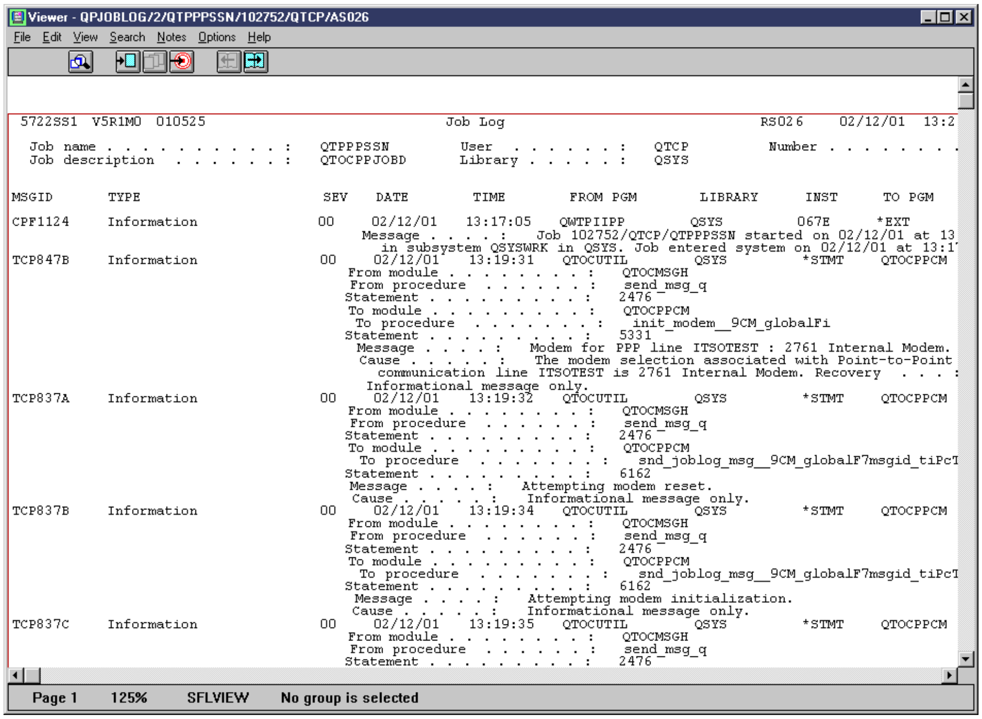
User: All   Job: 102752/QTCP/QTPPPSSN

Output name	User-specified data	User	Status	Printer	Pages per copy	Copies
Clog102752	ITSOTEST	QTCP	Held	Not Assigned	8	1
Qpjoblog	ITSOTEST	QTCP	Ready	Not Assigned	4	1

1 - 2 of 2 objects

Figure 168. Printer Output for PPP session job

8. Locate the **Qpjoblog** file, right-click, and select **Open**. This opens the job log in the viewer provided with Operations Navigator. An example of the job log is shown in Figure 169.



Viewer - QPJOBLOG/2/QTPPPSSN/102752/QTCP/AS026

```
 5722SS1  V5R1M0  010525                              Job Log                           RS02 6    02/12/01   13:2

  Job name . . . . . . . . . . :   QTPPPSSN       User  . . . . . . :   QTCP         Number . . . . . . . .
  Job description  . . . . . . :   QTOCPPJOBD     Library . . . . . :   QSYS

MSGID       TYPE                        SEV   DATE        TIME        FROM PGM       LIBRARY     INST      TO PGM

CPF1124     Information                 00    02/12/01    13:17:05   QWTPIIPP       QSYS        067E      *EXT
                                            Message . . . . :   Job 102752/QTCP/QTPPPSSN started on 02/12/01 at 13
                                              in subsystem QSYSWRK in QSYS. Job entered system on 02/12/01 at 13:1
TCP847B     Information                 00     02/12/01    13:19:31   QTOCUTIL       QSYS        *STMT     QTOCPPCM
                                           From module . . . . . . . . :   QTOCMSGH
                                           From procedure  . . . . . . :   send_msg_q
                                          Statement . . . . . . . . . :   2476
                                           To module . . . . . . . . . :   QTOCPPCM
                                            To procedure  . . . . . . . :   init_modem__9CM_globalFi
                                          Statement . . . . . . . . . :   5331
                                             Message . . . . :   Modem for PPP line ITSOTEST : 2761 Internal Modem.
                                              Cause . . . . . :   The modem selection associated with Point-to-Point
                                                communication line ITSOTEST is 2761 Internal Modem. Recovery  . . . :
                                              Informational message only.
TCP837A     Information                 00     02/12/01    13:19:32   QTOCUTIL       QSYS        *STMT     QTOCPPCM
                                           From module . . . . . . . . :   QTOCMSGH
                                           From procedure  . . . . . . :   send_msg_q
                                          Statement . . . . . . . . . :   2476
                                           To module . . . . . . . . . :   QTOCPPCM
                                             To procedure  . . . . . . . :   snd_joblog_msg__9CM_globalF7msgid_tiPcT
                                          Statement . . . . . . . . . :   6162
                                           Message . . . . :   Attempting modem reset.
                                            Cause . . . . . :   Informational message only.
TCP837B     Information                 00     02/12/01    13:19:34   QTOCUTIL       QSYS        *STMT     QTOCPPCM
                                           From module . . . . . . . . :   QTOCMSGH
                                           From procedure  . . . . . . :   send_msg_q
                                          Statement . . . . . . . . . :   2476
                                           To module . . . . . . . . . :   QTOCPPCM
                                             To procedure  . . . . . . . :   snd_joblog_msg__9CM_globalF7msgid_tiPcT
                                          Statement . . . . . . . . . :   6162
                                            Message . . . . :   Attempting modem initialization.
                                            Cause . . . . . :   Informational message only.
TCP837C     Information                 00     02/12/01    13:19:35   QTOCUTIL       QSYS        *STMT     QTOCPPCM
                                           From module . . . . . . . . :   QTOCMSGH
                                           From procedure  . . . . . . :   send_msg_q
                                          Statement . . . . . . . . . :   2476
```

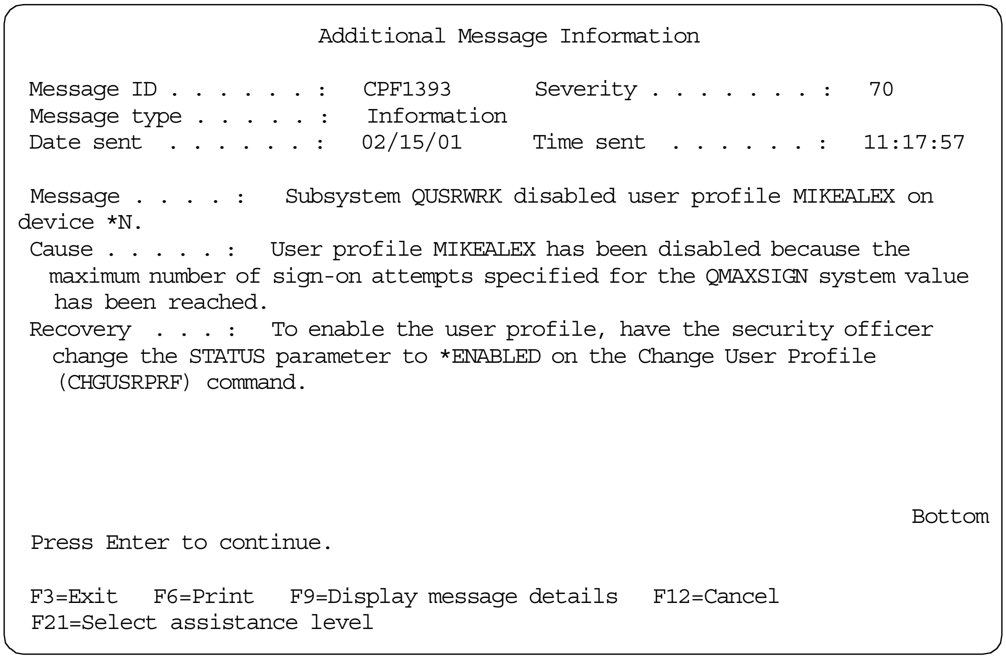
Page 1   125%   SFLVIEW   No group is selected

Figure 169. An example of a PPP session job log

It is also possible to view the PPP component log in the same manner. If the Clogxxxxxx file (here, *xxxxxx* can be any 6-digit number) is opened, you can view the component information. This log provides information on the modem being used and communications problems. It is discussed further in the next section.

6.3.1.2 5250 emulation access

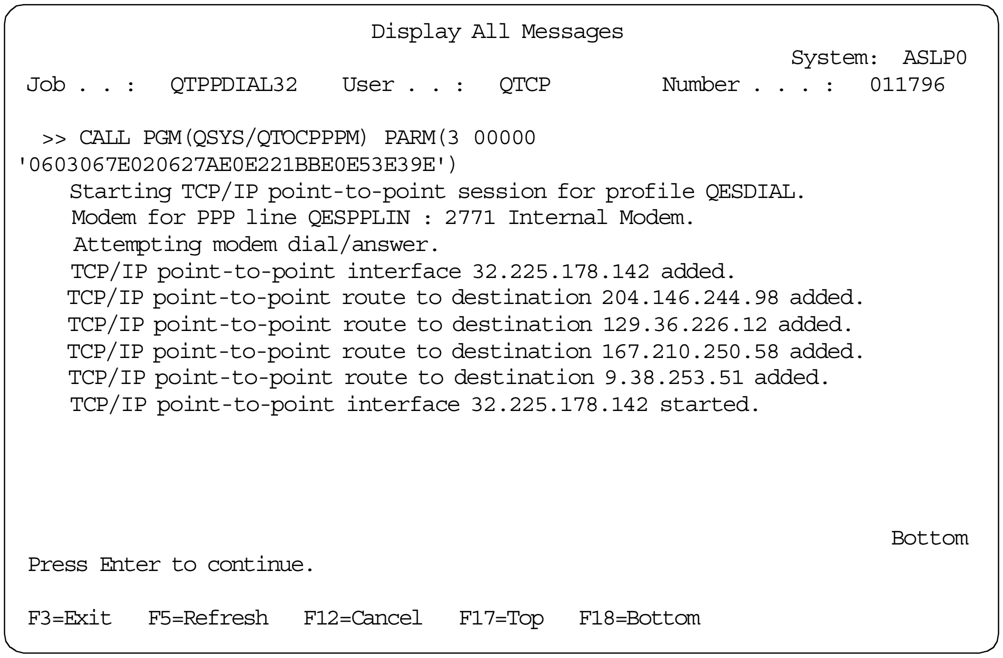
The QSYSOPR message queue can be viewed from a 5250 emulation screen by using the `DSPMSG QSYSOPR` command on an OS/400 command line. To view the details of any message in QSYSOPR, place the cursor below the message and press F1. This results in a screen similar to the one shown in Figure 170.



```
                          Additional Message Information

 Message ID . . . . . . :   CPF1393       Severity . . . . . . . :   70
 Message type . . . . . :   Information
 Date sent  . . . . . . :   02/15/01      Time sent  . . . . . . :   11:17:57

 Message . . . . :   Subsystem QUSRWRK disabled user profile MIKEALEX on
device *N.
 Cause . . . . . :   User profile MIKEALEX has been disabled because the
   maximum number of sign-on attempts specified for the QMAXSIGN system value
   has been reached.
 Recovery  . . . :   To enable the user profile, have the security officer
   change the STATUS parameter to *ENABLED on the Change User Profile
   (CHGUSRPRF) command.




                                                                       Bottom
 Press Enter to continue.

 F3=Exit   F6=Print   F9=Display message details   F12=Cancel
 F21=Select assistance level
```

Figure 170. 5250 emulation view of details of the QSYSOPR message

You can determine the status of the PPP profile from a 5250 emulation screen by using the `WRKTCPPTP` command. Here, you can see the status of the connection and look at the job log of the PPP session job using option 14. From the Work with Job screen, select option `10` to display the job log. A normal job log for the PPP session job is shown in Figure 171.

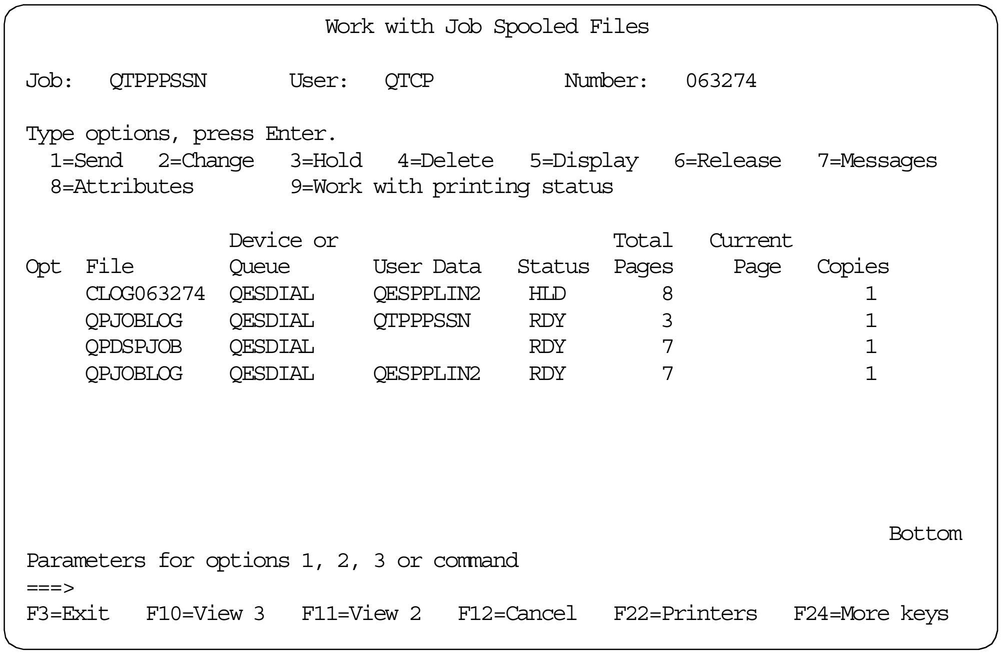


```
                              Display All Messages
                                                             System:  ASLP0
 Job . . :   QTPPDIAL32    User . . :   QTCP         Number . . . :   011796

  >> CALL PGM(QSYS/QTOCPPPM) PARM(3 00000
'0603067E020627AE0E221BBE0E53E39E')
    Starting TCP/IP point-to-point session for profile QESDIAL.
    Modem for PPP line QESPPLIN : 2771 Internal Modem.
    Attempting modem dial/answer.
    TCP/IP point-to-point interface 32.225.178.142 added.
    TCP/IP point-to-point route to destination 204.146.244.98 added.
    TCP/IP point-to-point route to destination 129.36.226.12 added.
    TCP/IP point-to-point route to destination 167.210.250.58 added.
    TCP/IP point-to-point route to destination 9.38.253.51 added.
    TCP/IP point-to-point interface 32.225.178.142 started.




                                                                      Bottom
 Press Enter to continue.

 F3=Exit   F5=Refresh   F12=Cancel   F17=Top   F18=Bottom
```

Figure 171. Example of a functional PPP dial job

Notice that the session for QESDIAL is started first and then the line appears with the modem type being used. Always ensure that the modem type listed is correct. All of the TCP/IP routes are then added as the interface for the PPP connection is started. Also, notice that this job log is different than the one shown in Figure 169. This is because the PPP session job has not ended. Once it is ended, select option `4` from the Work with Job screen and then option `5`, which allows the user to display the Qpjoblog. This is similar to the one shown in Figure 169.

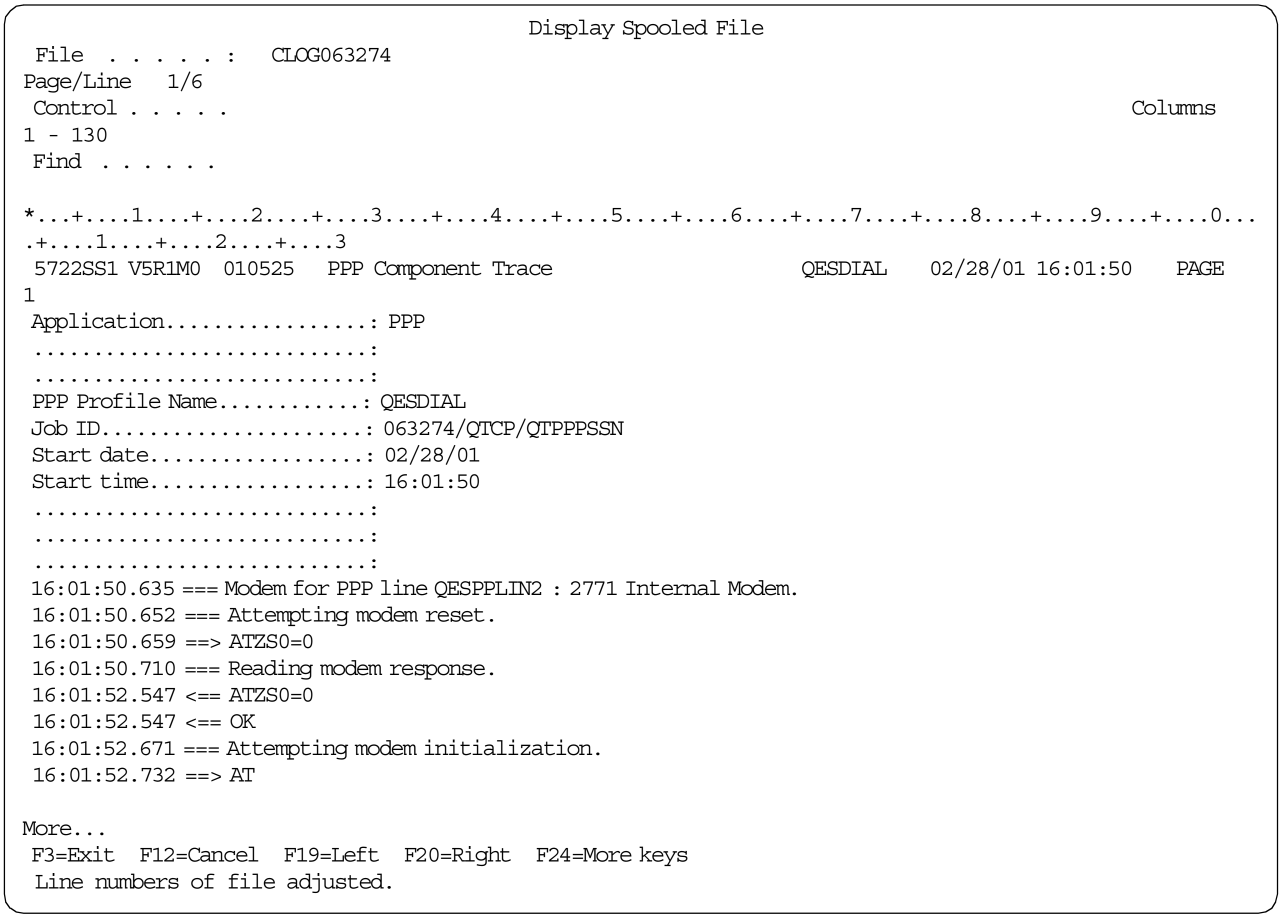
It is also possible to look at the PPP component log after a connection has been attempted. This log is useful when debugging errors with modem communications, such as no dial tone or a busy line. To view this log, run the `WRKTCPPTP` command, type option `14` next to QESDIAL, and then select option `4` to Work with spooled files. An example of the screen that appears is shown in Figure 172.



```
                           Work with Job Spooled Files

Job:   QTPPPSSN       User:   QTCP          Number:   063274

Type options, press Enter.
  1=Send   2=Change   3=Hold   4=Delete   5=Display   6=Release   7=Messages
  8=Attributes        9=Work with printing status

                Device or                          Total   Current
Opt  File         Queue         User Data   Status  Pages     Page    Copies
     CLOG063274   QESDIAL      QESPPLIN2    HLD         8                 1
     QPJOBLOG     QESDIAL      QTPPPSSN     RDY         3                 1
     QPDSPJOB     QESDIAL                   RDY         7                 1
     QPJOBLOG     QESDIAL      QESPPLIN2    RDY         7                 1




                                                                       Bottom
Parameters for options 1, 2, 3 or command
===>
F3=Exit   F10=View 3   F11=View 2   F12=Cancel   F22=Printers   F24=More keys
```

Figure 172. Spooled files associated with the QESDIAL PPP profile

Type option `5` next to the CLOGxxxxxx. Here, *xxxxxx* can be any 6-digit number to view the PPP component log. This log looks very similar to the example in Figure 173.

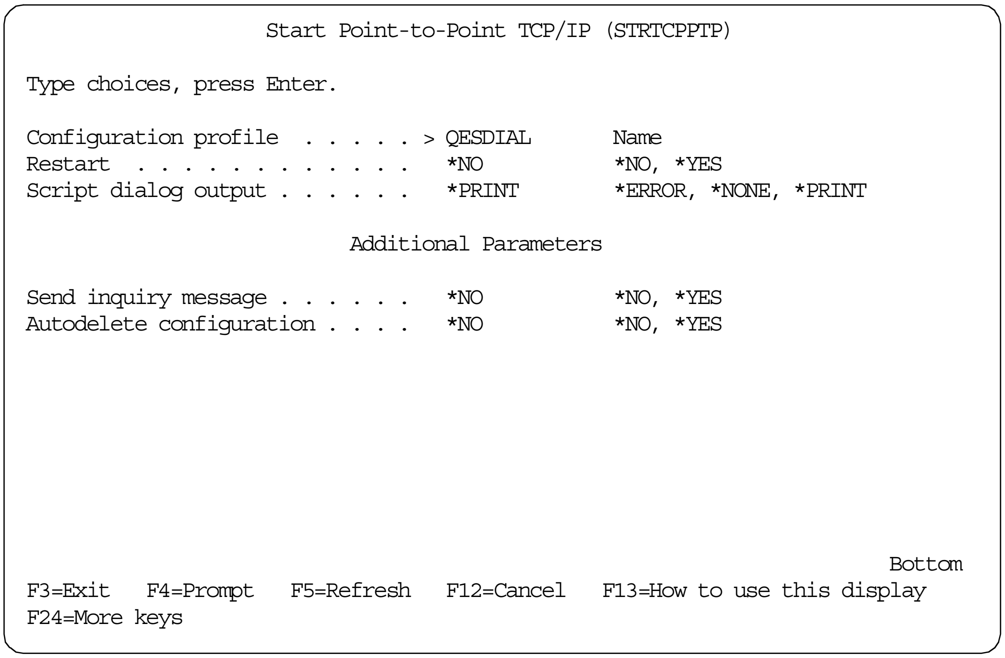


```
                                        Display Spooled File
 File  . . . . . :   CLOG063274
Page/Line   1/6
 Control . . . . .                                                                                Columns
1 - 130
 Find  . . . . . .

*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0...
.+....1....+....2....+....3
 5722SS1 V5R1M0  010525   PPP Component Trace                     QESDIAL    02/28/01 16:01:50    PAGE
1
 Application.................: PPP
 ............................:
 ............................:
 PPP Profile Name............: QESDIAL
 Job ID......................: 063274/QTCP/QTPPPSSN
 Start date..................: 02/28/01
 Start time..................: 16:01:50
 ............................:
 ............................:
 ............................:
 16:01:50.635 === Modem for PPP line QESPPLIN2 : 2771 Internal Modem.
 16:01:50.652 === Attempting modem reset.
 16:01:50.659 ==> ATZS0=0
 16:01:50.710 === Reading modem response.
 16:01:52.547 <== ATZS0=0
 16:01:52.547 <== OK
 16:01:52.671 === Attempting modem initialization.
 16:01:52.732 ==> AT

More...
 F3=Exit   F12=Cancel   F19=Left   F20=Right   F24=More keys
 Line numbers of file adjusted.
```

Figure 173. PPP component log for the QESDIAL profile

Note: At OS/400 V4R5M0, it is not possible to view this PPP component log file if the profile has already ended. The component file is deleted after the profile has ended or is inactivated. To capture the log file, complete the following steps:

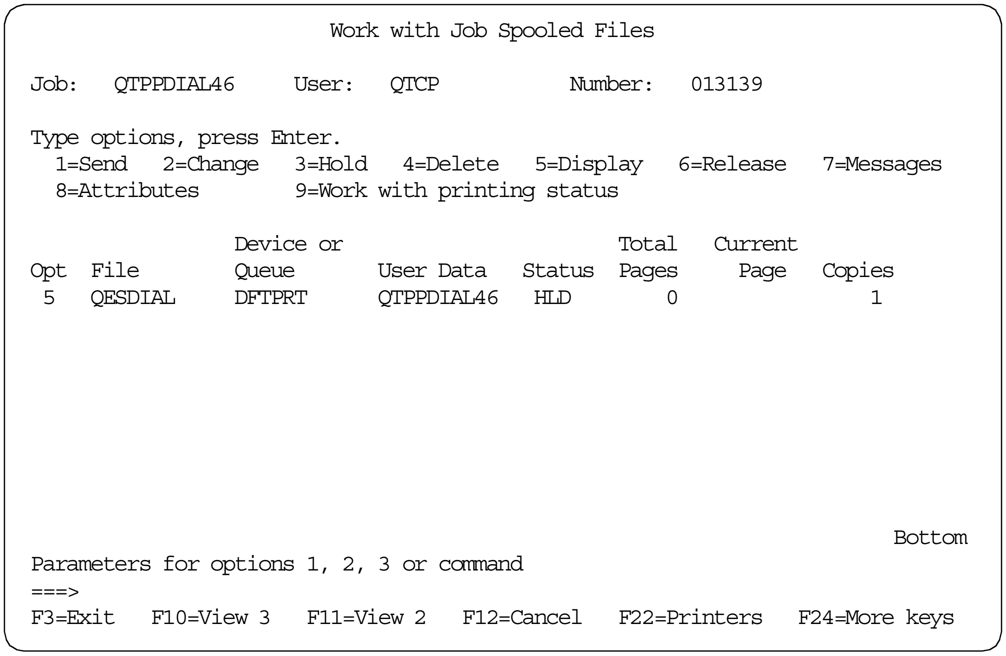
1. From an OS/400 command line, issue the `WRKTCPPTP` command.
2. Type option `9` next to QESDIAL and prompt using an F4 keystroke.
3. Press the F10 key for additional parameters.
4. Change the Script dialog output parameter from *ERROR to `*PRINT`. Then press Enter. This is shown in Figure 174.



```
                    Start Point-to-Point TCP/IP (STRTCPPTP)

Type choices, press Enter.

Configuration profile  . . . . . > QESDIAL       Name
Restart  . . . . . . . . . . . .   *NO           *NO, *YES
Script dialog output . . . . . .   *PRINT        *ERROR, *NONE, *PRINT

                           Additional Parameters

Send inquiry message . . . . . .   *NO           *NO, *YES
Autodelete configuration . . . .   *NO           *NO, *YES











                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 174. Changing Script dialog output to *PRINT

5. The iSeries server attempts to activate the QESDIAL profile.
6. From the Work with Point-to-Point TCP/IP screen, type option 14 next to QESDIAL, and select option 4 to work with spooled files.
7. Enter option 5 next to the file that has the same name as the PPP profile. In this case, it is QESDIAL as shown in Figure 175.



```
                         Work with Job Spooled Files

Job:   QTPPDIAL46     User:   QTCP          Number:   013139

Type options, press Enter.
  1=Send   2=Change   3=Hold   4=Delete   5=Display   6=Release   7=Messages
  8=Attributes        9=Work with printing status

                 Device or                        Total   Current
Opt  File        Queue       User Data   Status  Pages      Page   Copies
 5   QESDIAL     DFTPRT      QTPPDIAL46   HLD        0                 1










                                                                      Bottom
Parameters for options 1, 2, 3 or command
===>
F3=Exit   F10=View 3   F11=View 2   F12=Cancel   F22=Printers   F24=More keys
```

Figure 175. Displaying the spool file that has the same name as the PPP profile

The log file shows the PPP profile name, the PPP dial job name, number and user, and when it was started. The first line of the log shows the line description name being used and also the name of the modem being used. A list of modem commands are then listed, which are followed by authentication and IP address allocation processes. This log file is very useful in determining whether there is a modem problem or possibly a communications problem in dialing out. Further problem determination regarding the authentication and IP allocation processes is outside the scope of this chapter and should be pursued with an IBM Support Representative.

For other PPP problems, refer to *TCP/IP Configuration and Reference*, SC41-5420, or contact IBM Support. Information is also available online at the iSeries Information Center at:

```
http://publib.boulder.ibm.com/pubs/html/as400/infocenter.html
```

6.3.1.3 Remote support on non-English systems

As mentioned in Chapter 3, “Point-to-Point Protocol (PPP) connection examples” on page 37, the STRRMTSPT function was changed after applying SF64123 to allow for Remote Support over the 56 Kbps internal modem. If the STRRMTSPT command is prompted on a non-English system, and no *PPP option is listed, try the following command:

```
QSYS/STRRMTSPT
```

Then, press F4.

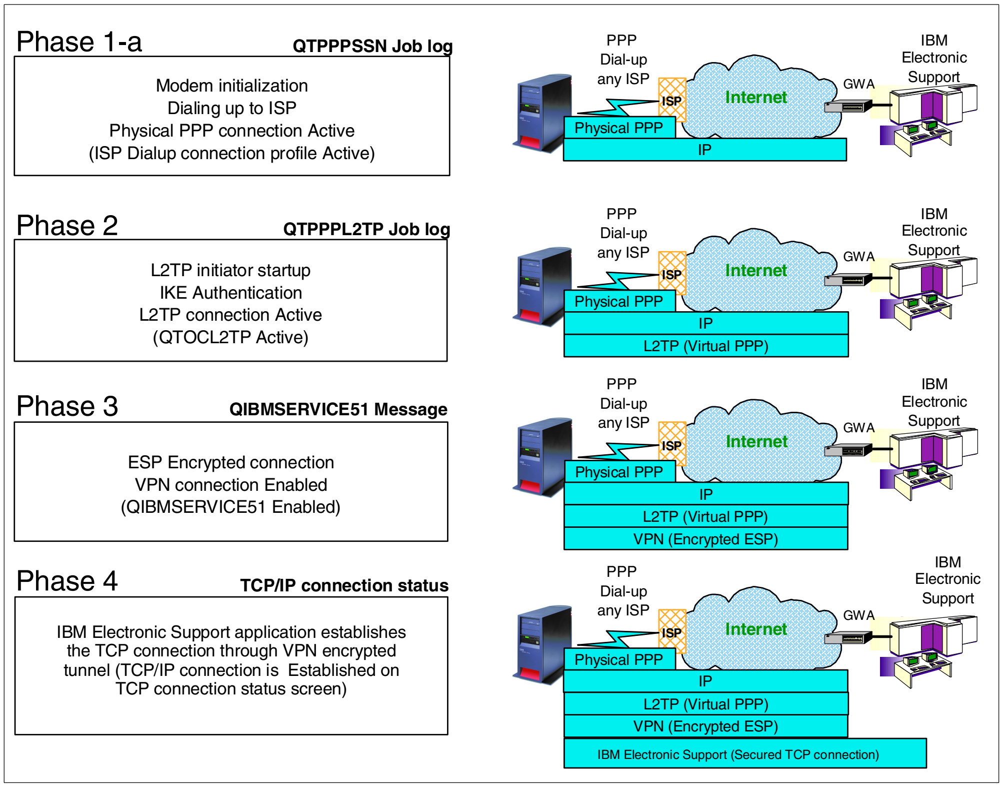
This ensures that the correct STRRMTSPT command is being called. Only the STRRMTSPT command in QSYS is updated by PTF SF64123 in V4R5M0 of OS/400.

6.3.2 ISP connection case troubleshooting

This section provides troubleshooting information for any ISP dial-up and direct connection cases. Before performing problem determination, you must understand how the IBM Electronic Support connection is established. If you only need to isolate the connection problem quickly, go to 6.3.2.3, “Problem determination procedure” on page 189.

6.3.2.1 Dial-up any ISP case connection phases overview

Figure 176 shows the connection phases of a dial-up any ISP case. After you invoke the SNDPTFORD command, your iSeries server automatically processes each phase one after another to establish the IBM Electronic Support connection between your iSeries server and IBM Electronic Support.



Phase 1-a QTPPPSSN Job log

Modem initialization
Dialing up to ISP
Physical PPP connection Active
(ISP Dialup connection profile Active)

Phase 2 QTPPPL2TP Job log

L2TP initiator startup
IKE Authentication
L2TP connection Active
(QTOCL2TP Active)

Phase 3 QIBMSERVICE51 Message

ESP Encrypted connection
VPN connection Enabled
(QIBMSERVICE51 Enabled)

Phase 4 TCP/IP connection status

IBM Electronic Support application establishes the TCP connection through VPN encrypted tunnel (TCP/IP connection is Established on TCP connection status screen)

Figure 176. IBM Electronic Support VPN connection overview: Dial-up any ISP case

Each phase in Figure 176 is explained here:

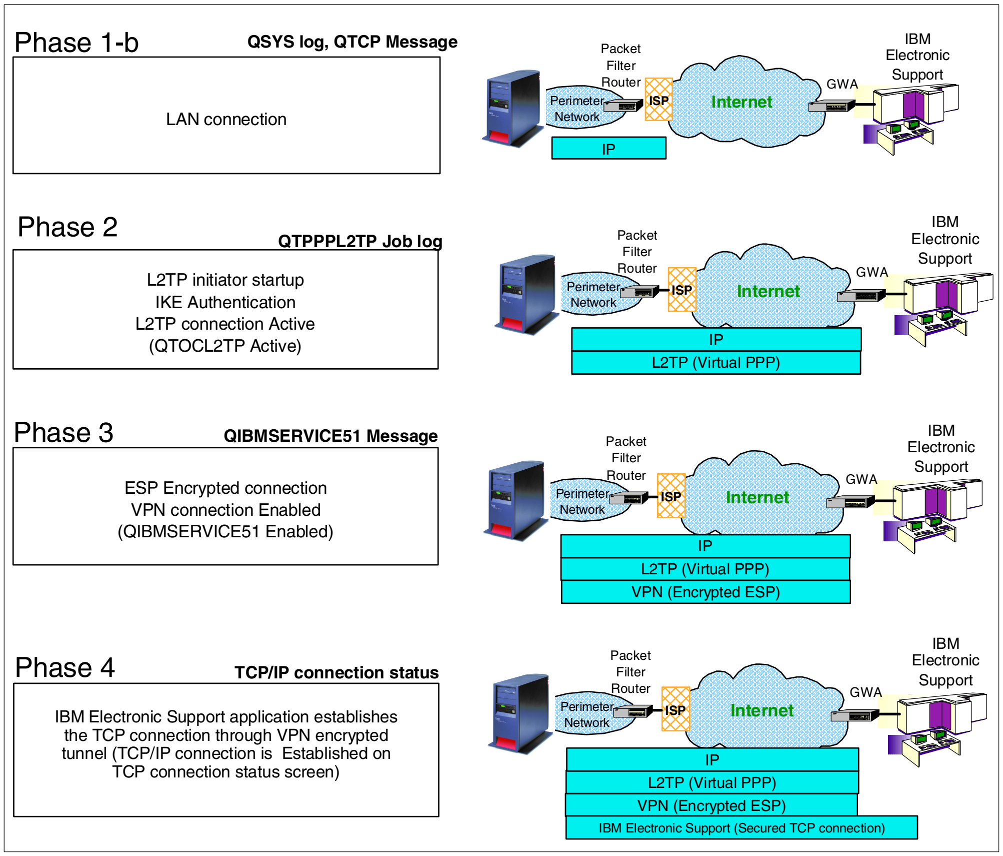
- **Phase 1-a**
  - Your iSeries server initializes the modem with an AT command.
  - If the modem is initialized successfully, the iSeries server sends the AT command strings with the ISP dial-up number included. The modem initiates the dial-up connection with your ISP.
  - If the phone connection is established successfully, each modem begins the negotiation steps. Each modem negotiates the line speed and the protocol to make a connection.
  - If the modem negotiation is completed, the PPP protocol on the iSeries server sends the user ID and password to the ISP to get the authentication.
  - After the authentication is done, IP addresses are assigned at the ISP side and the iSeries server side. The status of the ISP connection profile becomes *Active*.
  - Internet Key Exchange (IKE) protocol exchanges the secured data stream that is encrypted with the pre-shared key. Both the iSeries server and GWA router calculate the secured data stream and determine if the stream data matches their pre-shared key. If the stream data matches the pre-shared key at each peer, the authentication is completed.
  - IP datagrams can now be routed from the iSeries server to the GWA router through the Internet.

- **Phase 2**
  - The L2TP initiator QTOCL2TP starts the Layer 2 Tunneling Protocol connection initialization. L2TP is also called a Virtual PPP connection. An L2TP connection can be established between an L2TP-enabled client and an L2TP Network Server (LNS) unit. The iSeries server plays the role of the L2TP enabled client while the GWA router's role is as the LNS, so they can establish the L2TP connection. Each L2TP frame is divided into IP datagrams, and these IP datagrams go through the Internet.
  - If the L2TP connection is established successfully, the status of QTOCL2TP becomes *JobsActive*.
- **Phase 3**
  - Encapsulating Security Payload establishes the encrypted VPN connection between the iSeries server and GWA router. ESP uses the secret number that is generated from the pre-shared key to encrypt the data.
  - The VPN secured connection is established between your iSeries server and GWA. Notice that the GWA is the router that belongs to IBM, and the GWA is located in the same site as IBM Electronic Service. The status of QIBMSERVICE51 is now *Enabled*.
- **Phase 4**

  IBM Electronic Support connection is now established between your iSeries server and IBM Electronic Support. ECS establishes the TCP connection between the iSeries server and IBM Electronic Support through the ESP encrypted tunnel. All IP datagrams of the TCP connection are invisible because these datagrams are encapsulated and encrypted by the ESP protocol. The TCP connection for the IBM Electronic Support application is now *established*.

6.3.2.2 Direct connection case connection phases overview

Figure 177 shows the connection phases of the direct connection case. After you run the SNDPTFORD command, your iSeries server automatically processes each phase one after another to establish the IBM Electronic Support connection between your iSeries server and IBM Electronic Support.



Phase 1-b — QSYS log, QTCP Message

LAN connection

Phase 2 — QTPPPL2TP Job log

L2TP initiator startup
IKE Authentication
L2TP connection Active
(QTOCL2TP Active)

Phase 3 — QIBMSERVICE51 Message

ESP Encrypted connection
VPN connection Enabled
(QIBMSERVICE51 Enabled)

Phase 4 — TCP/IP connection status

IBM Electronic Support application establishes the TCP connection through VPN encrypted tunnel (TCP/IP connection is Established on TCP connection status screen)

Figure 177. IBM Electronic Support VPN connection overview: Direct connection case

The phases in Figure 177 are explained here:

- **Phase 1**

  Before you start the IBM Electronic Support connection with direct connection, you must have these prerequisites:

  – The TCP interface that is used for the IBM Electronic Support connection must be active.

  – IP datagrams must be ratable for both outbound and inbound directions. If you applied the IP filter rules on the packet filter router, review Chapter 4, “Direct connection examples” on page 107, and determine what IP filter rules must be applied on the packet filter router.

  The difference between the dial-up any ISP case and direct connection case is that the dial-up case needs a physical PPP connection to start the IBM Electronic Support connection. The direct connection doesn’t require a PPP dial-up connection. Direct connection starts the connection with L2TP startup.

- **Phase 2**

  – The L2TP initiator QTOCL2TP starts the Layer 2 Tunneling Protocol (L2TP) connection initialization. L2TP is also called a virtual PPP connection. An L2TP connection can be established between an L2TP enabled client and an L2TP Network Server (LNS) unit. The iSeries server plays the role of the L2TP enabled client, while the GWA router’s role is as the LNS, so they can establish the L2TP connection. Each L2TP frame is divided into IP datagrams, and these IP datagrams go through the Internet.

- Internet Key Exchange protocol exchanges the secured data stream that is encrypted with the pre-shared key. Both the iSeries server and the GWA router calculate the secured data stream and determine if the stream data matches their pre-shared key. If the stream data matches the pre-shared key at each peer, the authentication is completed.
- If the L2TP connection is established successfully, the status of QTOCL2TP becomes *JobsActive*.

- **Phase 3**
  - Encapsulating Security Payload establishes the encrypted VPN connection between the iSeries server and the GWA router. ESP uses the secret number that is generated from the pre-shared key to encrypt the data.
  - The VPN secured connection is established between your iSeries server and GWA. Notice that the GWA is the router that belongs to IBM and the GWA is located in the same site as IBM Electronic Service. The status of QIBMSERVICE51 is now *enabled*.
- **Phase 4**

  The IBM Electronic Support connection is now established between the iSeries server and IBM Electronic Support. ECS establishes the TCP connection between the iSeries server and IBM Electronic Support through the ESP encrypted tunnel. All IP datagrams of the TCP connection are invisible because these datagrams are encapsulated and encrypted by ESP protocol. The TCP connection for the IBM Electronic Support application is now *established*.

6.3.2.3 Problem determination procedure

This section provides problem determination procedures if you cannot make an IBM Electronic Support connection. If you are working with the dial-up any ISP case problem determination, start the procedure in “Phase 1-a: Checking the status of the ISP connection profile” on page 189. If you are working with the direct connection case problem determination, start the procedure at step 6. on page 193.

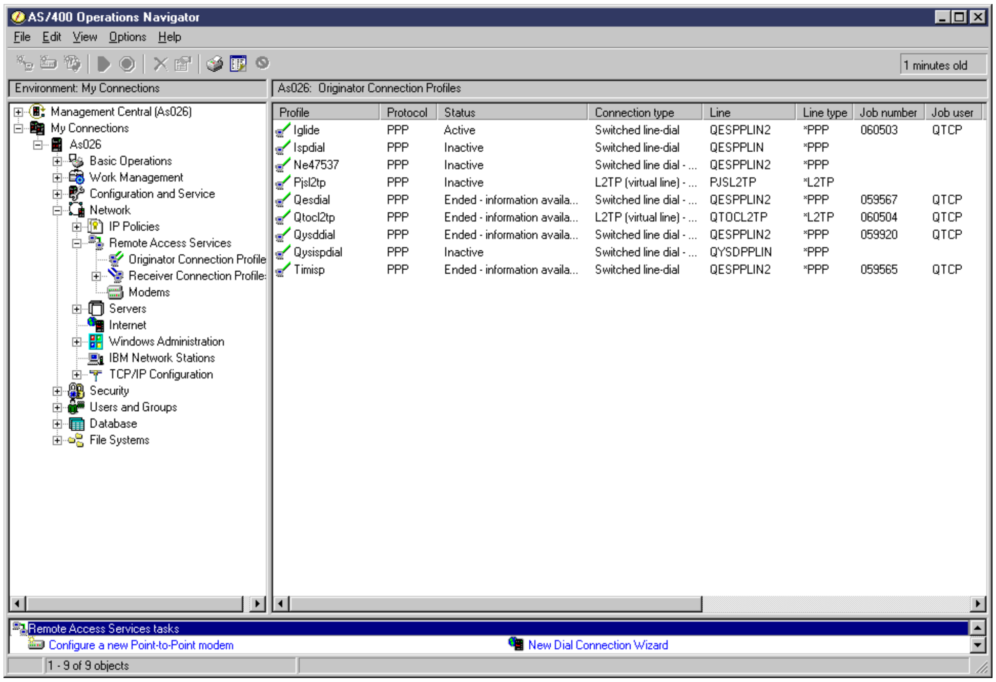
For more detailed VPN problem determination, refer to the iSeries Information Center at: `http://publib.boulder.ibm.com/pubs/html/as400/infocenter.html`

Phase 1-a: Checking the status of the ISP connection profile

Check the ISP connection status by performing the following steps:

1. Start the Operations Navigator from the desktop.
2. Expand the iSeries server (in this case, **AS026**). Sign on when prompted.
3. Expand **Network**.
4. Expand **Remote Access Services**.
5. Click **Originator Connection Profiles**.

   Look for the connection profile that you are currently using for the IBM Electronic Support connection as shown in Figure 178. In this example, the ISP connection profile *Iglide* is Active. The status is idle at the beginning, but then changes to *Active*. You can see this status when you start the PPP profile.


AS/400 Operations Navigator
File Edit View Options Help
1 minutes old
Environment: My Connections
Management Central (As026)
My Connections
As026
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profile
Receiver Connection Profile:
Modems
Servers
Internet
Windows Administration
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
Remote Access Services tasks
Configure a new Point-to-Point modem
New Dial Connection Wizard
1 - 9 of 9 objects

As026: Originator Connection Profiles

Profile	Protocol	Status	Connection type	Line	Line type	Job number	Job user
Iglide	PPP	Active	Switched line-dial	QESPPLIN2	*PPP	060503	QTCP
Ispdial	PPP	Inactive	Switched line-dial	QESPPLIN	*PPP		
Ne47537	PPP	Inactive	Switched line dial - ...	QESPPLIN2	*PPP		
Pjsl2tp	PPP	Inactive	L2TP (virtual line) - ...	PJSL2TP	*L2TP		
Qesdial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059567	QTCP
Qtocl2tp	PPP	Ended - information availa...	L2TP (virtual line) - ...	QTOCL2TP	*L2TP	060504	QTCP
Qysddial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059920	QTCP
Qysispdial	PPP	Inactive	Switched line dial - ...	QYSDPPLIN	*PPP		
Timisp	PPP	Ended - information availa...	Switched line-dial	QESPPLIN2	*PPP	059565	QTCP

Figure 178. ISP connection profile status

If the status of the ISP connection profile is Active, but you cannot make the IBM Electronic Support connection, go to step 6. on page 193 to check the IP datagram connectivity.

If the status of the ISP connection profile is not Active, perform the following steps to check the QTPPPSSN job log contents:

1. Check the QTPPPSSN job log.

   The QTPPPSSN job log contains many useful messages to isolate the problem. To look at the QTPPPSSN job log on the Operations Navigator display, perform the following steps:

   a. Start the Operations Navigator from the desktop.

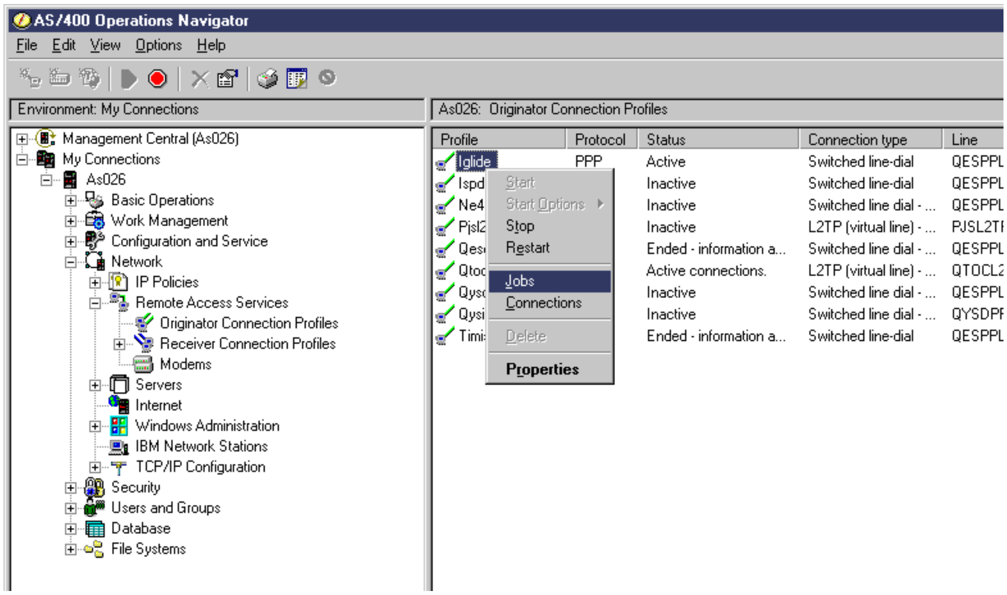
   b. Expand the iSeries server (in this case, **AS026**). Sign on when prompted.

   c. Expand **Network**.

   d. Expand **Remote Access Services**.

   e. Click **Originator Connection Profiles**.

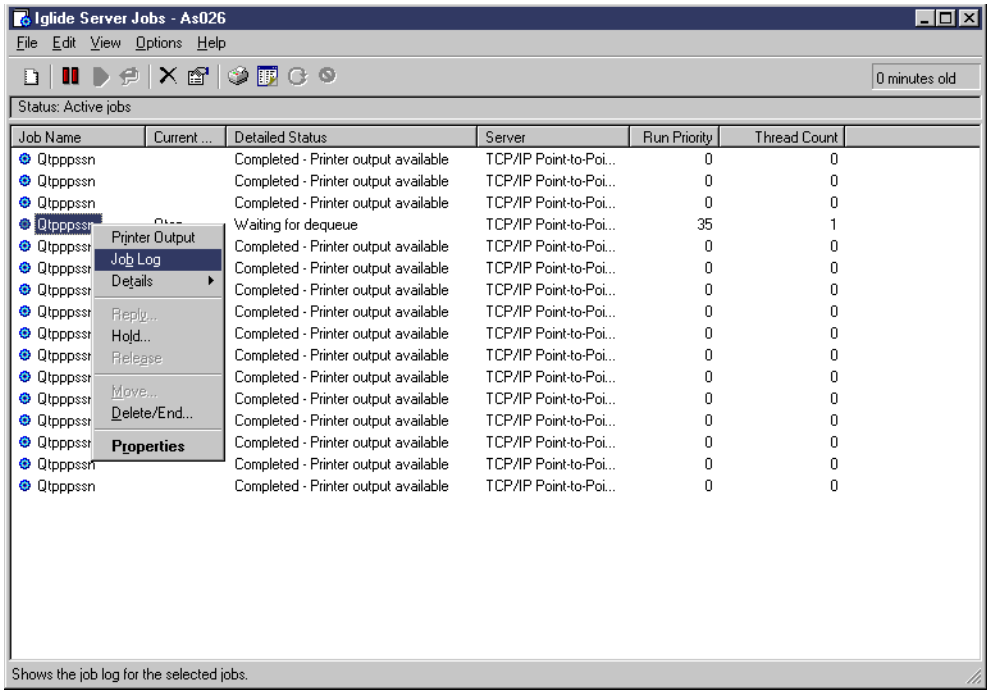
   f. Look for the connection profile that you are currently using for the IBM Electronic Support connection. Right-click the connection profile name (in this case, **Iglide**). On the pull-down menu, choose **Jobs** as shown in Figure 179.



Profile	Protocol	Status	Connection type	Line
Iglide	PPP	Active	Switched line-dial	QESPPL
Ispd		Inactive	Switched line-dial	QESPPL
Ne4		Inactive	Switched line dial - ...	QESPPL
Pjsl2		Inactive	L2TP (virtual line) - ...	PJSL2TI
Qes		Ended - information a...	Switched line dial - ...	QESPPL
Qtoc		Active connections.	L2TP (virtual line) - ...	QTOCL2
Qysc		Inactive	Switched line dial - ...	QESPPL
Qysi		Inactive	Switched line dial - ...	QYSDPF
Timi		Ended - information a...	Switched line-dial	QESPPL

Figure 179. Selecting the Jobs connection profile

2. Find and right-click the **QTPPPSSN** job log where Detailed Status is *Waiting for dequeue*. From the pull-down menu, choose **Job Log** as shown in Figure 180.



Job Name	Current ...	Detailed Status	Server	Run Priority	Thread Count
Qtpppssn		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssn		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssn		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssn		Waiting for dequeue	TCP/IP Point-to-Poi...	35	1
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssr		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssn		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0
Qtpppssn		Completed - Printer output available	TCP/IP Point-to-Poi...	0	0

Figure 180. QTPPPSSN job list

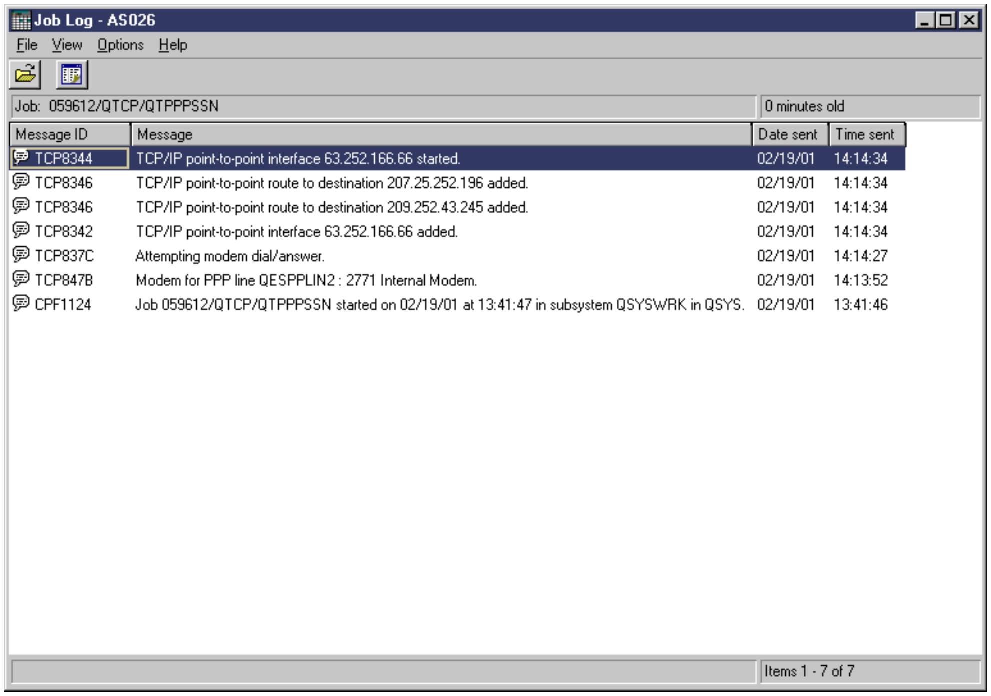
If there is no QTPPPSSN job log that specifies Detailed Status is *Waiting for dequeue*, perform the following steps to find the most recent completed or ended job:

a. Click the Number tag to sort jobs with the job number. Number tag is found at the rightmost of the job tags to the right of Thread Count.

b. Scroll down the jobs list. The job that has the biggest number is the job that has completed or ended recently.

c. Right-click the job name. On the pull-down menu, choose **Job Log**.

3. You can now look at the QTPPPSSN job log contents as shown in Figure 181. If you cannot see the job log contents because the job has already completed, initiate the IBM Electronic Support connection again and try to find the current job.



Job Log - AS026

Job: 059612/QTCP/QTPPPSSN

0 minutes old

Message ID	Message	Date sent	Time sent
TCP8344	TCP/IP point-to-point interface 63.252.166.66 started.	02/19/01	14:14:34
TCP8346	TCP/IP point-to-point route to destination 207.25.252.196 added.	02/19/01	14:14:34
TCP8346	TCP/IP point-to-point route to destination 209.252.43.245 added.	02/19/01	14:14:34
TCP8342	TCP/IP point-to-point interface 63.252.166.66 added.	02/19/01	14:14:34
TCP837C	Attempting modem dial/answer.	02/19/01	14:14:27
TCP847B	Modem for PPP line QESPPLIN2 : 2771 Internal Modem.	02/19/01	14:13:52
CPF1124	Job 059612/QTCP/QTPPPSSN started on 02/19/01 at 13:41:47 in subsystem QSYSWRK in QSYS.	02/19/01	13:41:46

Items 1 - 7 of 7

Figure 181. QTPPPSSN job log contents

This procedure allows you to determine what is the required action to fix the connection problem:

`TCP847B Modem for PPP line QESPPLIN2(line definition name): 2771modem(modem type can be different) is logged?`

- **Yes**: The modem initialization is completed and the modem is ready for use. Continue to step 4.
- **No**: The modem may have a problem. Call the hardware representative to ask for service.

4. Is there any error message logged after the TCP837C Attempting modem dial/answer? Error messages would include `No dial tone detected` and `The line is busy`.

   - **Yes**: If the message is "No Carrier", ensure that the phone line is seated securely into the RJ11 phone plug jack on your modem. If you think the phone line is not working properly, call your local phone service provider to ask for the repair. If the message is "The line is busy", try to dial the ISP dial-up number with your desk phone to make sure that the line is really busy. Also, verify that any dial prefixes that must be used from your location have been included in the profile. Retrying the connection operation may fix the problem.

- **No**: It suspects the dial-up is completed and the phone connection is already established between your modem and your ISP. Continue with step 5.

5. Verify whether the following messages are logged:

   - **TCP8342** TCP/IP point-to-point interface 63.252.166.66 added
   - **TCP8346** TCP/IP point-to-point route to destination 209.252.43.245 added
   - **TCP8346** TCP/IP point-to-point route to destination xxx.xxx.xxx.xxx added

     Here, *xxx.xxx.xxx.xxx* is the GWA IP address.
   - **TCP8344** TCP/IP point-to-point interface 63.252.166.66 started

   Note: IP addresses vary depending on your ISP.

   The local IP address on your iSeries server side is shown in TCP8344 message. In this example, Local IP address is 63.252.166.66. Record the Local IP address for later use.

   Are all these message logged?

   - **Yes**: PPP authentication has completed successfully. An IP address is assigned on the iSeries server side and ISP side, and the IP routes to the GWA router (GWA IP address) are added. You still need to check the IP datagram connectivity with the TRACEROUTE command. Continue with step 6.
   - **No**: PPP authentication may have failed. Most likely the problem exists in the PAP or CHAP authentication setting in the ISP connection profile definition, or the user ID and the password may be wrong. Ask your ISP if your PAP or CHAP setting is correct.

6. Check IP datagram connectivity with the PING command.

   If the PPP authentication is completed, all required IP routes to the GWA router are added. However, there is a possibility that the IP datagram doesn’t go through the Internet if there is a malfunction on the Internet. The PING command uses the ICMP protocol to verify the connectivity of the IP datagram.

   Perform the following steps to check the IP datagram connectivity with the PING command:

   a. Open the 5250 Emulator screen. Sign on the with user ID and password.

   b. Type `CALL QCMD` and press Enter to access the command entry screen.

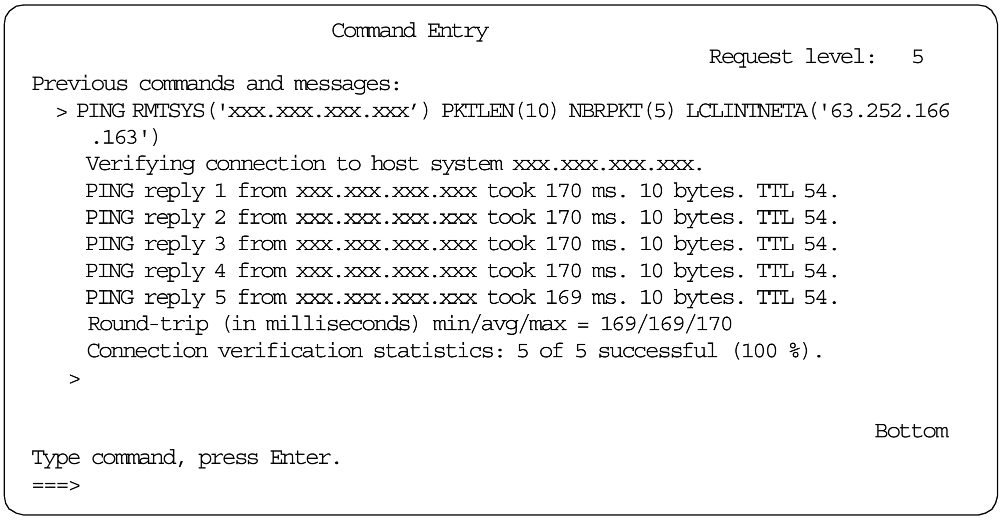
   c. Make sure the ISP connection profile status is still Active. Go back to step 1. on page 190 to check the status if required.

   d. Type the following command:

   ```
   PING RMTSYS('xxx.xxx.xxx.xxx') PKTLEN(10) NBRPKT(5)
   LCLINTNETA('63.252.166.163')
   ```

   Press Enter as shown in Figure 182 (here, *xxx.xxx.xxx.xxx* is the GWA IP address).

   Note: LCLINETNETA means the local IP address that you recorded in step 5. This local IP address varies depending on your ISP. If you are working with the direct connection, use the IP address of the TCP interface being used for the IBM Electronic Support connection. This address can be obtained from the L2TP initiator profile.



```
                         Command Entry
                                                       Request level:   5
Previous commands and messages:
  > PING RMTSYS('xxx.xxx.xxx.xxx’) PKTLEN(10) NBRPKT(5) LCLINTNETA('63.252.166
     .163')
    Verifying connection to host system xxx.xxx.xxx.xxx.
    PING reply 1 from xxx.xxx.xxx.xxx took 170 ms. 10 bytes. TTL 54.
    PING reply 2 from xxx.xxx.xxx.xxx took 170 ms. 10 bytes. TTL 54.
    PING reply 3 from xxx.xxx.xxx.xxx took 170 ms. 10 bytes. TTL 54.
    PING reply 4 from xxx.xxx.xxx.xxx took 170 ms. 10 bytes. TTL 54.
    PING reply 5 from xxx.xxx.xxx.xxx took 169 ms. 10 bytes. TTL 54.
    Round-trip (in milliseconds) min/avg/max = 169/169/170
    Connection verification statistics: 5 of 5 successful (100 %).
   >

                                                                    Bottom
Type command, press Enter.
===>
```

Figure 182. PING command execution screen

Did you get the PING reply from GWA?

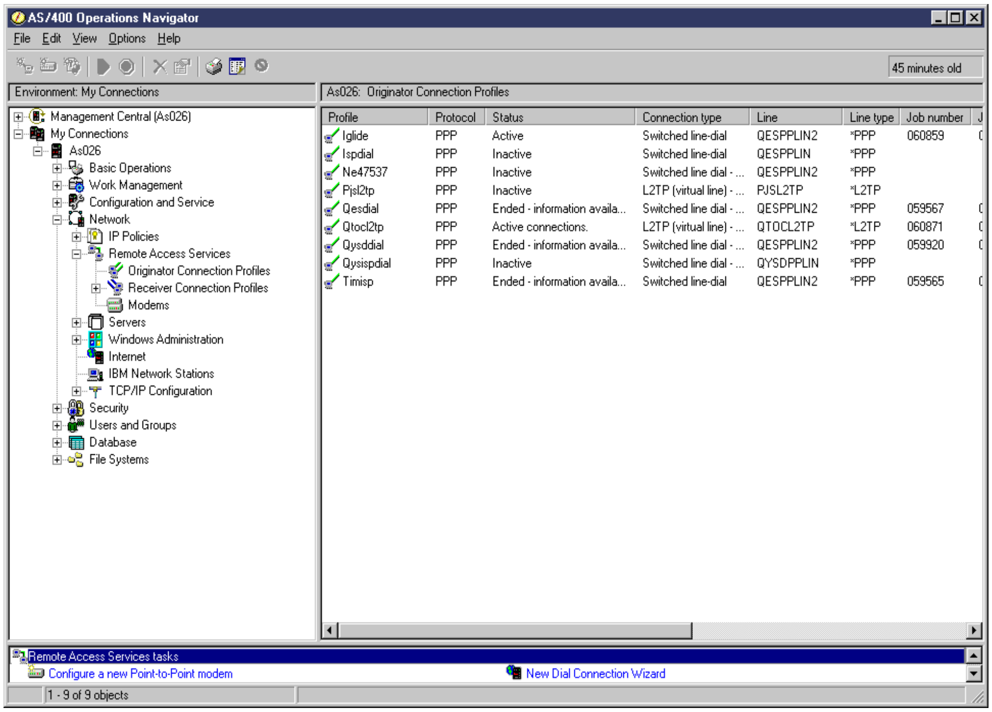
- **Yes**: IP datagram connectivity is OK. Proceed to Phase 2 to check the L2TP initiator status.
- **No**: There may be a network problem between your iSeries server and the GWA router. Call your ISP to report the connectivity problem.

Phase 2: Checking the status of the L2TP initiator QTOCL2TP

Check the L2TP initiator QTOCL2TP status by performing the following steps:

1. Click **Originator Connection Profiles**.

   Look for QTOCL2TP as shown in Figure 183. The status is idle at the beginning. The status then changes to *Active connections*.


AS/400 Operations Navigator
File Edit View Options Help
45 minutes old
Environment: My Connections
Management Central (As026)
My Connections
As026
Basic Operations
Work Management
Configuration and Service
Network
IP Policies
Remote Access Services
Originator Connection Profiles
Receiver Connection Profiles
Modems
Servers
Windows Administration
Internet
IBM Network Stations
TCP/IP Configuration
Security
Users and Groups
Database
File Systems
Remote Access Services tasks
Configure a new Point-to-Point modem
New Dial Connection Wizard
1 - 9 of 9 objects

As026: Originator Connection Profiles

Profile	Protocol	Status	Connection type	Line	Line type	Job number
Iglide	PPP	Active	Switched line-dial	QESPPLIN2	*PPP	060859
Ispdial	PPP	Inactive	Switched line-dial	QESPPLIN	*PPP	
Ne47537	PPP	Inactive	Switched line dial - ...	QESPPLIN2	*PPP	
Pjsl2tp	PPP	Inactive	L2TP (virtual line) - ...	PJSL2TP	*L2TP	
Qesdial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059567
Qtocl2tp	PPP	Active connections.	L2TP (virtual line) - ...	QTOCL2TP	*L2TP	060871
Qysddial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059920
Qysispdial	PPP	Inactive	Switched line dial - ...	QYSDPPLIN	*PPP	
Timisp	PPP	Ended - information availa...	Switched line-dial	QESPPLIN2	*PPP	059565

Figure 183. QTOCL2TP status display

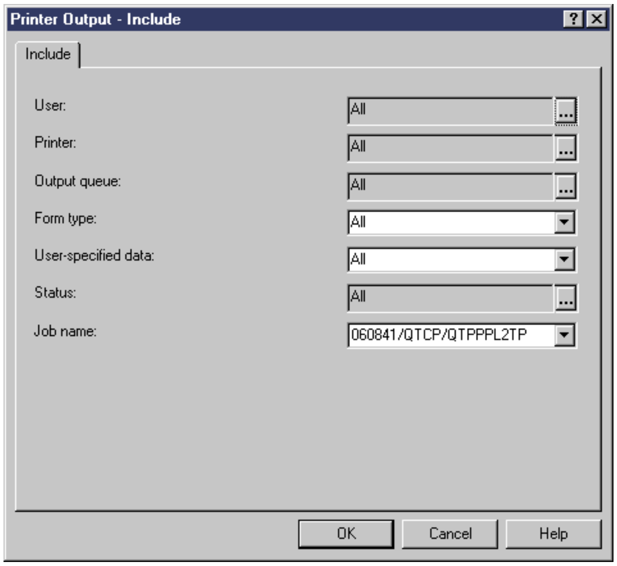
If the status of the QTCOL2TP is Active connections, but you cannot make the IBM Electronic Support connection, proceed to Phase 3 to check the VPN connection status.

If the status of the QTOCL2TP is not Active connections, check the QTPPPL2TP job log contents.

The QTPPPL2TP job log contains useful messages to isolate the problem. To view the QTPPPL2TP job log on the Operations Navigator display, perform the following steps:

1. Click **Originator Connection Profiles**. Look for the QTOCL2TP profile. Write down the Job number, Job User, and Job of the QTOCL2TP. This information appears on the right side of the QTOCL2TP. Scroll the screen to the right to see the information if required.
2. Click **Basic Operations**.
3. Click **Printer output**.
4. Click **Options** on the task bar. On the pull-down menu, choose **Include.** On the next screen, click the small box to the right of the **User** column. Click **ALL** and click **OK**.

   Click the small box to the right of the Job name column, and type in the job number, job user, and job that you wrote down in step 1. Click **OK** as shown in Figure 184.



User: All

Printer: All

Output queue: All

Form type: All

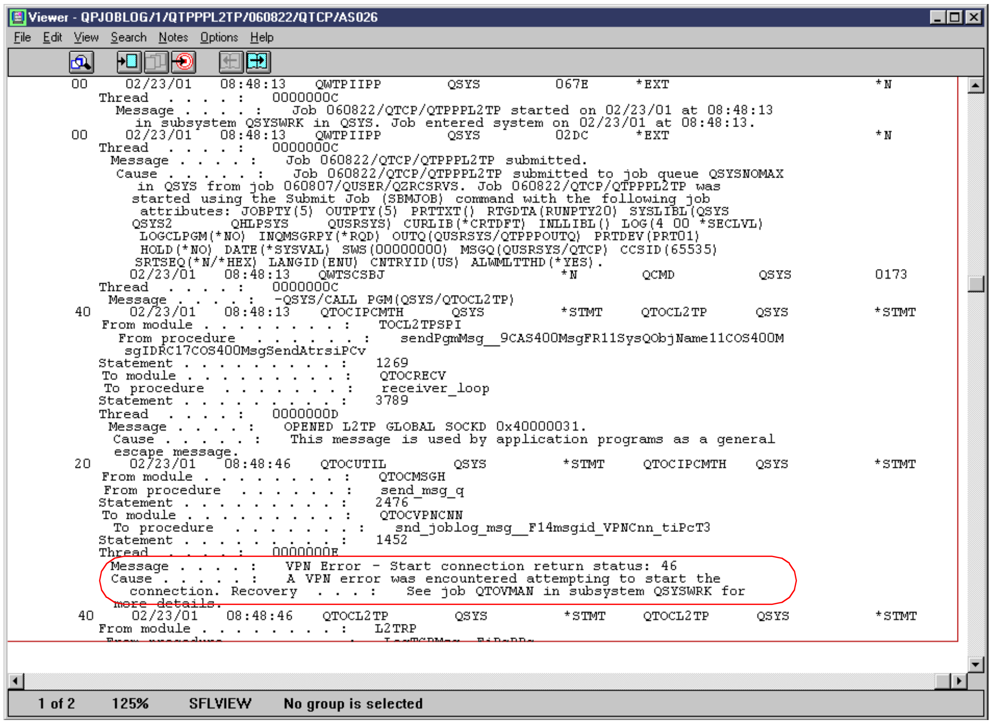
User-specified data: All

Status: All

Job name: 060841/QTCP/QTPPPL2TP

Figure 184. QTOCL2TP Job name selection

5. Double-click the job name **QTOCL2TP** to look at the QTOCL2TP job log. Check if any error is logged on the job log. In this case, a VPN error is logged. Write down the error code and description and contact IBM Support.



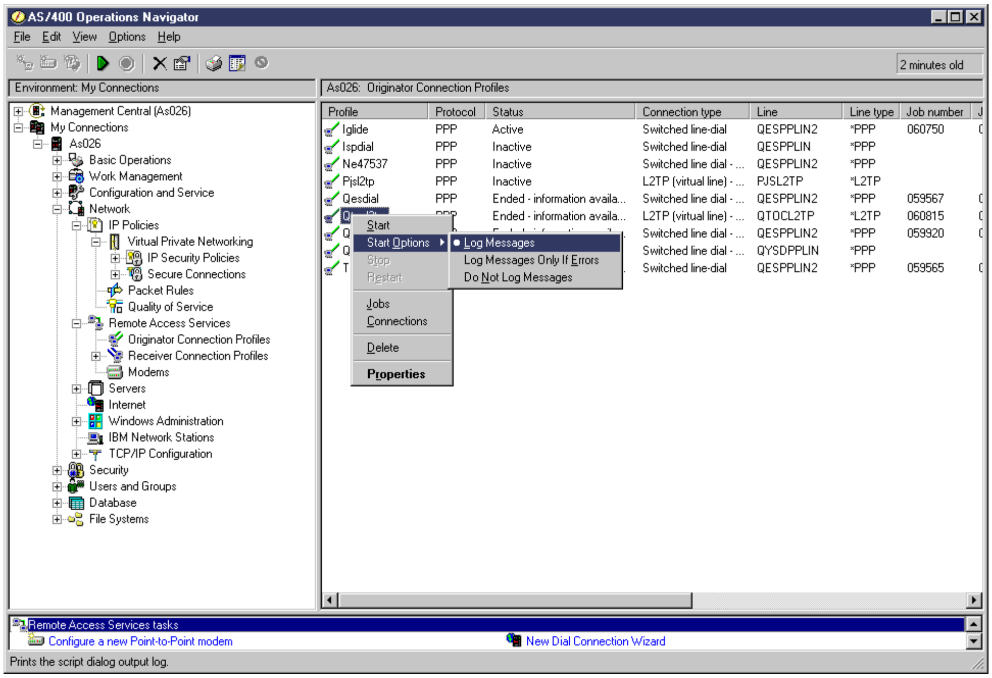
Viewer - QPJOBLOG/1/QTPPPL2TP/060822/QTCP/AS026
File Edit View Search Notes Options Help

```
 00    02/23/01    08:48:13    QWTPIIPP         QSYS          067E      *EXT                         *N
     Thread  . . . . :   0000000C
      Message . . . . :    Job 060822/QTCP/QTPPPL2TP started on 02/23/01 at 08:48:13
        in subsystem QSYSWRK in QSYS. Job entered system on 02/23/01 at 08:48:13.
 00    02/23/01    08:48:13    QWTPIIPP         QSYS          02DC      *EXT                         *N
     Thread  . . . . :   0000000C
      Message . . . . :   Job 060822/QTCP/QTPPPL2TP submitted.
       Cause . . . . . :    Job 060822/QTCP/QTPPPL2TP submitted to job queue QSYSNOMAX
         in QSYS from job 060807/QUSER/QZRCSRVS. Job 060822/QTCP/QTPPPL2TP was
        started using the Submit Job (SBMJOB) command with the following job
         attributes: JOBPTY(5) OUTPTY(5) PRTTXT() RTGDTA(RUNPTY20) SYSLIBL(QSYS
        QSYS2       QHLPSYS      QUSRSYS) CURLIB(*CRTDFT) INLLIBL() LOG(4 00 *SECLVL)
         LOGCLPGM(*NO) INQMSGRPY(*RQD) OUTQ(QUSRSYS/QTPPPOUTQ) PRTDEV(PRT01)
         HOLD(*NO) DATE(*SYSVAL) SWS(00000000) MSGQ(QUSRSYS/QTCP) CCSID(65535)
        SRTSEQ(*N/*HEX) LANGID(ENU) CNTRYID(US) ALWMLTTHD(*YES).
        02/23/01    08:48:13    QWTSCSBJ                        *N         QCMD          QSYS          0173
     Thread  . . . . :   0000000C
      Message . . . . :  -QSYS/CALL PGM(QSYS/QTOCL2TP)
 40     02/23/01    08:48:13    QTOCIPCMTH     QSYS          *STMT     QTOCL2TP      QSYS          *STMT
     From module . . . . . . . . :   TOCL2TPSPI
       From procedure . . . . . . :    sendPgmMsg__9CAS400MsgFR11SysQObjName11COS400M
        sgIDRC17COS400MsgSendAtrsiPCv
     Statement . . . . . . . . . :   1269
      To module . . . . . . . . . :   QTOCRECV
      To procedure  . . . . . . . :   receiver_loop
     Statement . . . . . . . . . :   3789
     Thread  . . . . :   0000000D
      Message . . . . :    OPENED L2TP GLOBAL SOCKD 0x40000031.
       Cause . . . . . :    This message is used by application programs as a general
       escape message.
 20     02/23/01    08:48:46    QTOCUTIL        QSYS          *STMT     QTOCIPCMTH    QSYS          *STMT
     From module . . . . . . . . :   QTOCMSGH
      From procedure  . . . . . . :   send_msg_q
     Statement . . . . . . . . . :   2476
      To module . . . . . . . . . :   QTOCVPNCNN
       To procedure  . . . . . . . :    snd_joblog_msg__F14msgid_VPNCnn_tiPcT3
     Statement . . . . . . . . . :   1452
     Thread  . . . . :   0000000E
      Message . . . . :    VPN Error - Start connection return status: 46
      Cause . . . . . :    A VPN error was encountered attempting to start the
        connection. Recovery  . . . :    See job QTOVMAN in subsystem QSYSWRK for
       more details.
 40     02/23/01    08:48:46    QTOCL2TP        QSYS          *STMT     QTOCL2TP      QSYS          *STMT
     From module . . . . . . . . :   L2TRP
```

Figure 185. QTOCL2TP job log contents

If you see the message that the job has ended already and there is no QTOCL2TP job log left, perform the following steps to change the setting to keep the QTOCL2TP job log. Then, try to make the IBM Electronic Support connection again to access the error message on the QTOCL2TP job log. Perform the following steps:

1. Click **Originator Connection Profiles**.
2. Right-click **QTOCL2TP**. On the pull-down menu, choose **Start Options**, and then choose **Log Messages** as shown in Figure 186.



As026: Originator Connection Profiles

Profile	Protocol	Status	Connection type	Line	Line type	Job number
Iglide	PPP	Active	Switched line-dial	QESPPLIN2	*PPP	060750
Ispdial	PPP	Inactive	Switched line-dial	QESPPLIN	*PPP	
Ne47537	PPP	Inactive	Switched line dial - ...	QESPPLIN2	*PPP	
Pjsl2tp	PPP	Inactive	L2TP (virtual line) - ...	PJSL2TP	*L2TP	
Qesdial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059567
Q		Ended - information availa...	L2TP (virtual line) - ...	QTOCL2TP	*L2TP	060815
Q			Switched line dial - ...	QESPPLIN2	*PPP	059920
Q			Switched line dial - ...	QYSDPPLIN	*PPP	
T			Switched line-dial	QESPPLIN2	*PPP	059565

Figure 186. QTOCL2TP job Start Options change

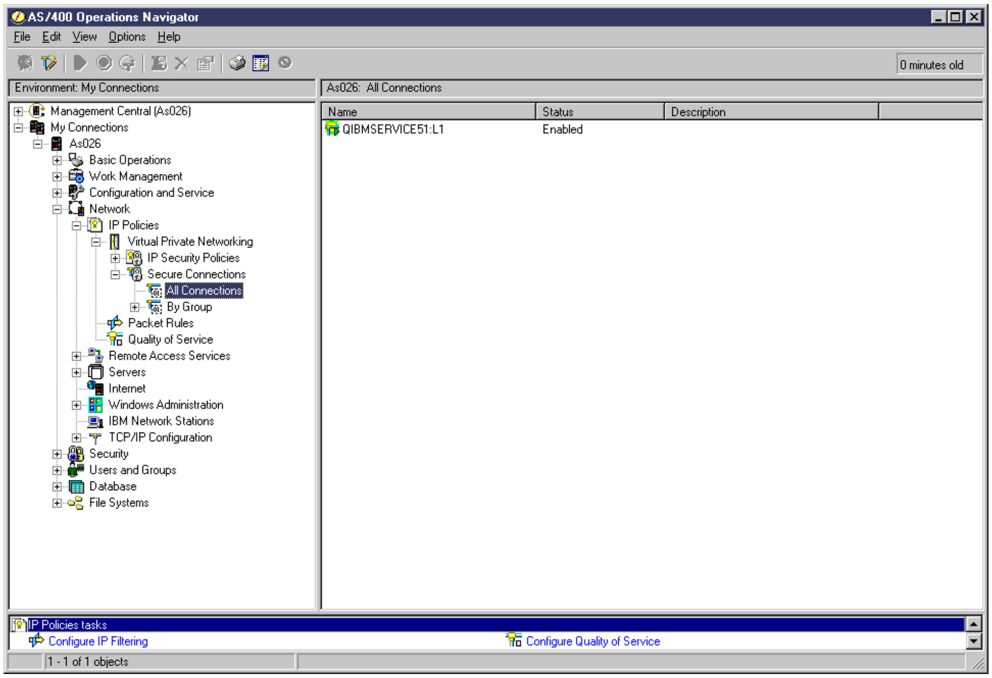
3. Try to make an IBM Electronic Support connection again. Now, the QTOCL2TP job log should remain in the system. Return to step 5. on page 196 to examine the error message.

Phase 3: Checking the status of QIBMSERVICE51

Check the Secure connection profile for the IBM Electronic Support QIBMSERVICE51 status by performing the following steps:

1. Expand **Network**.
2. Expand **IP Policies**.
3. Expand **Virtual Private Networking**.
4. Expand **Secure Connections**.
5. Click **All Connections**.

   Look at the status of QIBMSERVICE51 as shown in Figure 187. The status is idle at the beginning, but then changes to *Enabled*.



Name	Status	Description
QIBMSERVICE51:L1	Enabled	

Figure 187. QIBMSERVICE51 status

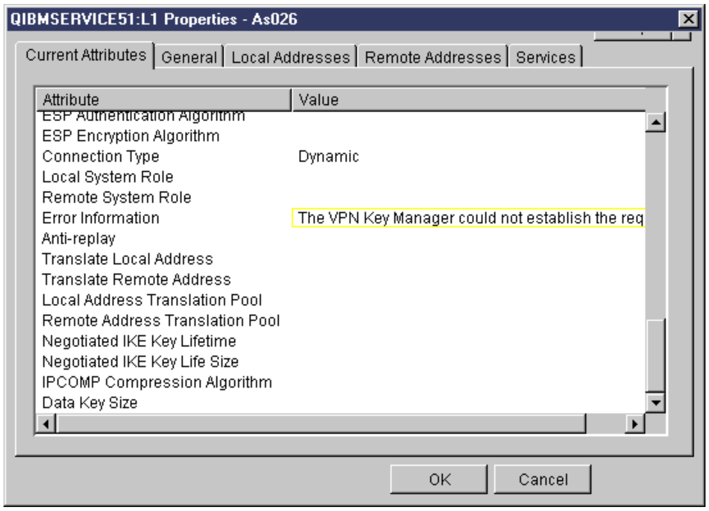
If the status of the QIBMSERVICE51 is Enabled, but you cannot make the IBM Electronic Support connection, proceed to Phase 4 to check the IBM Electronic Support application connection status.

If the status of the QIBMSERVICE51 is not Enabled, check the error information on QIBMSERVICE51.

QIBMSERVICE51 error information contains useful messages to isolate the problem. To look at the QIBMSERVICE51 error information on the Operations Navigator display, perform the following steps:

1. Right-click **QIBMSERVICE51**. On the pull-down menu, choose **Error Information**.

   Figure 188 shows the error information example. In this example, the VPN key manager could not establish the request. Contact IBM Support with this error information.



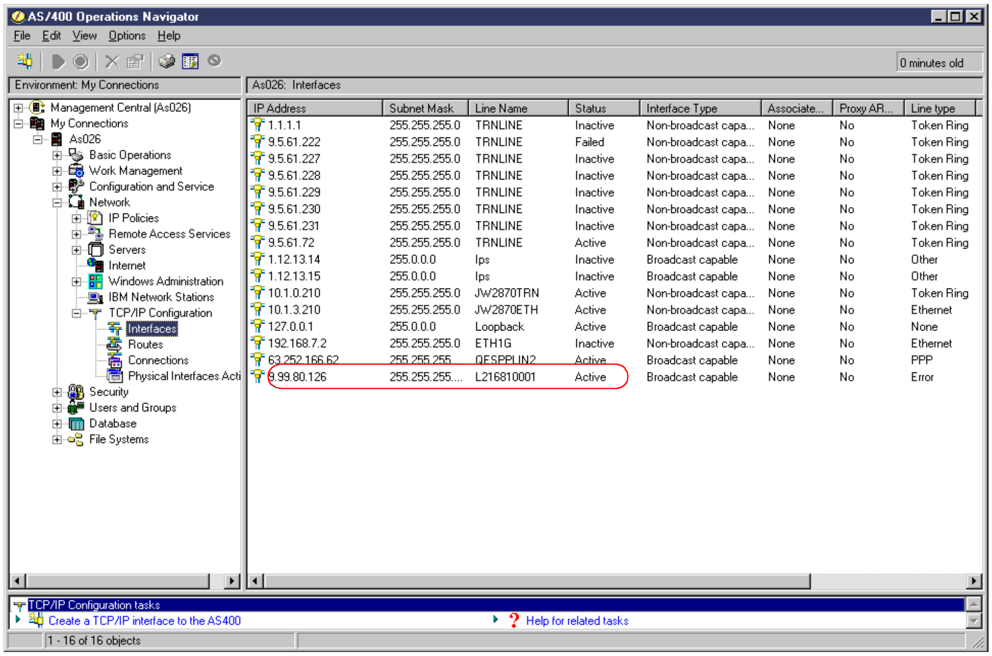
Attribute	Value
ESP Authentication Algorithm	
ESP Encryption Algorithm	
Connection Type	Dynamic
Local System Role	
Remote System Role	
Error Information	The VPN Key Manager could not establish the req
Anti-replay	
Translate Local Address	
Translate Remote Address	
Local Address Translation Pool	
Remote Address Translation Pool	
Negotiated IKE Key Lifetime	
Negotiated IKE Key Life Size	
IPCOMP Compression Algorithm	
Data Key Size	

Figure 188. QIBMSERVICE51 Error Information

Phase 4: Check the IBM Electronic Support application connection status

Check the IBM Electronic Support application connection status on the Operations Navigator display by performing the following steps:

1. Expand **Network**.
2. Expand **TCP/IP configuration**.
3. Click **Interfaces**.
4. On the 5250 emulation screen, type `SNDPTFORD` and order a PTF or, preferably, a PTF cover letter, to invoke a connection test to IBM Electronic Support.
5. Carefully watch the Interfaces screen. A new interface is generated on the Interface screen as shown in Figure 189. In this example, the IP address is 9.99.80.126 and the Line Name is L216810001. Write down the IP address.

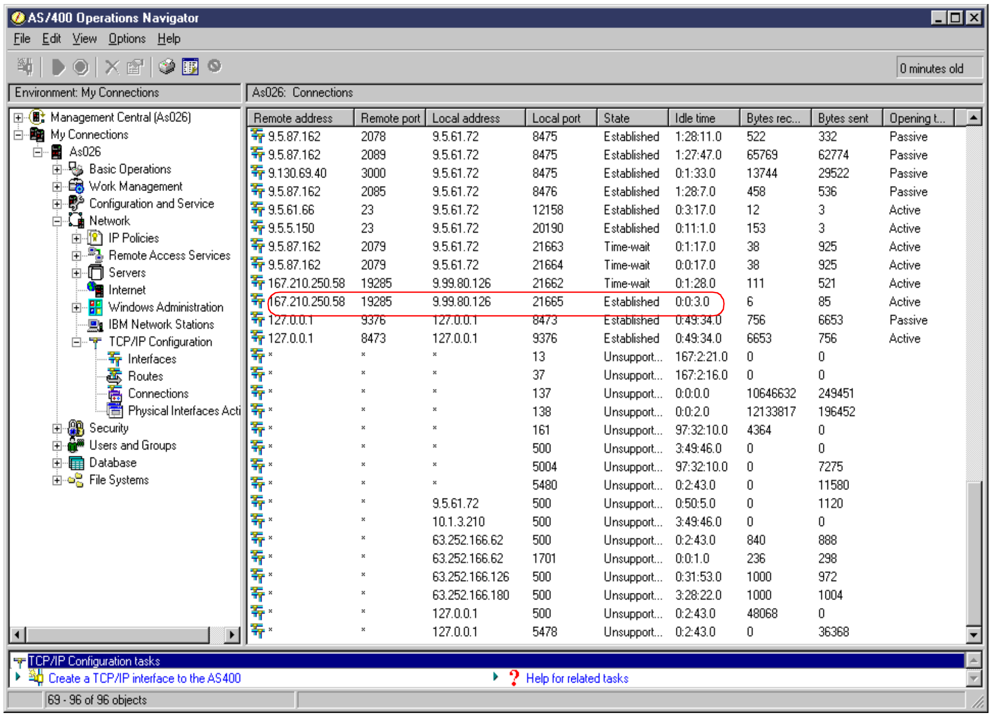


As026: Interfaces

IP Address	Subnet Mask	Line Name	Status	Interface Type	Associate...	Proxy AR...	Line type
1.1.1.1	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring
9.5.61.222	255.255.255.0	TRNLINE	Failed	Non-broadcast capa...	None	No	Token Ring
9.5.61.227	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring
9.5.61.228	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring
9.5.61.229	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring
9.5.61.230	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring
9.5.61.231	255.255.255.0	TRNLINE	Inactive	Non-broadcast capa...	None	No	Token Ring
9.5.61.72	255.255.255.0	TRNLINE	Active	Non-broadcast capa...	None	No	Token Ring
1.12.13.14	255.0.0.0	Ips	Inactive	Broadcast capable	None	No	Other
1.12.13.15	255.0.0.0	Ips	Inactive	Broadcast capable	None	No	Other
10.1.0.210	255.255.255.0	JW2870TRN	Active	Non-broadcast capa...	None	No	Token Ring
10.1.3.210	255.255.255.0	JW2870ETH	Active	Non-broadcast capa...	None	No	Ethernet
127.0.0.1	255.0.0.0	Loopback	Active	Broadcast capable	None	No	None
192.168.7.2	255.255.255.0	ETH1G	Inactive	Non-broadcast capa...	None	No	Ethernet
63.252.166.62	255.255.255....	QESPPLIN2	Active	Broadcast capable	None	No	PPP
9.99.80.126	255.255.255....	L216810001	Active	Broadcast capable	None	No	Error

Figure 189. TCP/IP interfaces display

6. Click **Connections**. Look for the connection in which the local IP address is the one you wrote down in Step 5. In this example, a connection is found on the screen (remote IP address is 167.210.250.58). The remote address varies based on your locations.



As026: Connections

Remote address	Remote port	Local address	Local port	State	Idle time	Bytes rec...	Bytes sent	Opening t...
9.5.87.162	2078	9.5.61.72	8475	Established	1:28:11.0	522	332	Passive
9.5.87.162	2089	9.5.61.72	8475	Established	1:27:47.0	65769	62774	Passive
9.130.69.40	3000	9.5.61.72	8475	Established	0:1:33.0	13744	29522	Passive
9.5.87.162	2085	9.5.61.72	8476	Established	1:28:7.0	458	536	Passive
9.5.61.66	23	9.5.61.72	12158	Established	0:3:17.0	12	3	Active
9.5.5.150	23	9.5.61.72	20190	Established	0:11:1.0	153	3	Active
9.5.87.162	2079	9.5.61.72	21663	Time-wait	0:1:17.0	38	925	Active
9.5.87.162	2079	9.5.61.72	21664	Time-wait	0:0:17.0	38	925	Active
167.210.250.58	19285	9.99.80.126	21662	Time-wait	0:1:28.0	111	521	Active
167.210.250.58	19285	9.99.80.126	21665	Established	0:0:3.0	6	85	Active
127.0.0.1	9376	127.0.0.1	8473	Established	0:49:34.0	756	6653	Passive
127.0.0.1	8473	127.0.0.1	9376	Established	0:49:34.0	6653	756	Active
*	*	*	13	Unsupport...	167:2:21.0	0	0	
*	*	*	37	Unsupport...	167:2:16.0	0	0	
*	*	*	137	Unsupport...	0:0:0.0	10646632	249451	
*	*	*	138	Unsupport...	0:0:2.0	12133817	196452	
*	*	*	161	Unsupport...	97:32:10.0	4364	0	
*	*	*	500	Unsupport...	3:49:46.0	0	0	
*	*	*	5004	Unsupport...	97:32:10.0	0	7275	
*	*	*	5480	Unsupport...	0:2:43.0	0	11580	
*	*	9.5.61.72	500	Unsupport...	0:50:5.0	0	1120	
*	*	10.1.3.210	500	Unsupport...	3:49:46.0	0	0	
*	*	63.252.166.62	500	Unsupport...	0:2:43.0	840	888	
*	*	63.252.166.62	1701	Unsupport...	0:0:1.0	236	298	
*	*	63.252.166.126	500	Unsupport...	0:31:53.0	1000	972	
*	*	63.252.166.180	500	Unsupport...	3:28:22.0	1000	1004	
*	*	127.0.0.1	500	Unsupport...	0:2:43.0	48068	0	
*	*	127.0.0.1	5478	Unsupport...	0:2:43.0	0	36368	

Figure 190. TCP/IP connections display

Is there an established connection in which the local IP address is the one you wrote down in step 5? If you couldn't find any newly generated interface in step 5, proceed to No for this question.

- **Yes**: A part of IBM Electronic Support application may be out of service. Contact IBM Support with this information.
- **No**: The IBM Electronic Support connection cannot be established for some reason. Contact IBM Support.

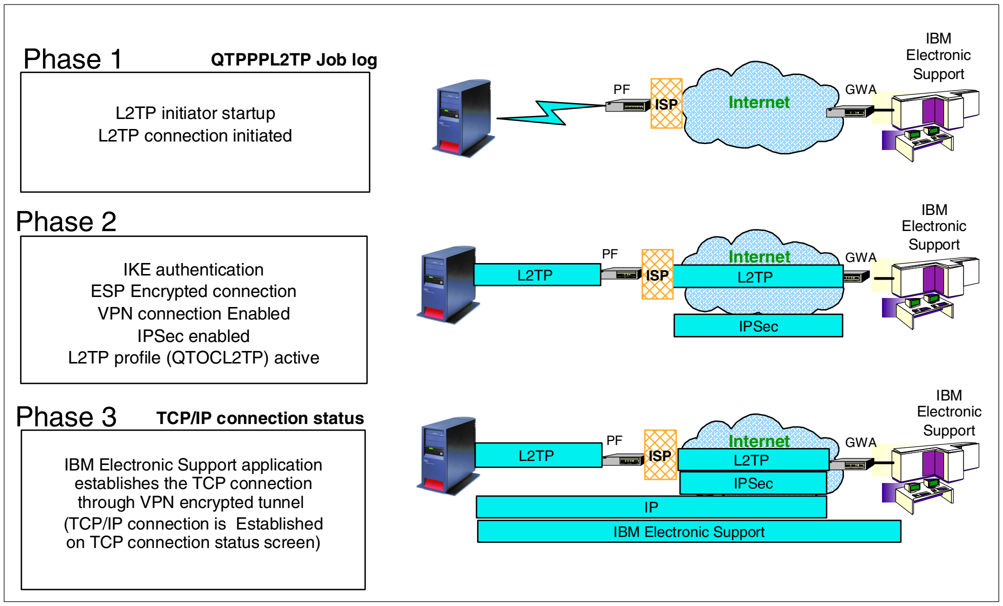
This ends the problem determination procedure.

6.3.3 Multi-hop troubleshooting

In a multi-hop connection, there are two L2TP tunnels involved: one from the iSeries server to the packet filter router and another from the router to the IBM gateway. The L2TP connection from the iSeries server to the packet filter router is covered in this section since it is created by the Universal Connection Wizard. The second L2TP connection is created by the packet filter router, which means that any problem determination for it must be done at the router level. In this case, it is best to contact the router vendor for further information and debugging procedures.

As mentioned in Chapter 5, “Multi-hop scenario” on page 151, the L2TP connection from the iSeries server to the packet filter router is not secured using IPSec since it does not involve routing IP data over the Internet. This creates a simpler connection than the other L2TP cases, such as dial-up any ISP and direct, since all these involved routing data over the Internet. However, the troubleshooting concepts are still the same since it involves the QTOCL2TP definition.

There are three phases in the multi-hop connection, which are outlined in Figure 191.


Phase 1 QTPPPL2TP Job log

L2TP initiator startup
L2TP connection initiated

Phase 2

IKE authentication
ESP Encrypted connection
VPN connection Enabled
IPSec enabled
L2TP profile (QTOCL2TP) active

Phase 3 TCP/IP connection status

IBM Electronic Support application establishes the TCP connection through VPN encrypted tunnel (TCP/IP connection is Established on TCP connection status screen)

Figure 191. Phases of a multi-hop connection

The phases in Figure 191 are explained in the following list:

- **Phase 1**
  - The L2TP initiator QTOCL2TP starts Layer 2 Tunneling Protocol (L2TP) connection initialization. L2TP is also called a virtual PPP connection. An L2TP connection can be established between an L2TP enabled client and an L2TP Network Server (LNS) unit. The iSeries server plays the role of the L2TP enabled client while the packet filter router's role is as the LNS, so they can establish the L2TP connection. Each L2TP frame is divided into IP datagrams, and these IP datagrams go through the Internet.
  - The L2TP connection is not established at this point. A request comes into the packet filter router to establish a connection to the IBM gateway. The router is then responsible for establishing the second connection to that IBM gateway.
- **Phase 2**
  - Internet Key Exchange protocol exchanges the secured data stream that is encrypted with the pre-shared key. Both the packet filter router and the GWA router calculate the secured data stream and determine if the stream data matches their pre-shared key. If the stream data matches the pre-shared key at each peer, the authentication is completed.
  - Encapsulating Security Payload (ESP) establishes the encrypted VPN connection between the Packet Filter router and GWA router. ESP uses the secret number that is generated from the pre-shared key to encrypt the data.
  - The VPN secured connection is established between your Packet Filter router and GWA. Notice that the GWA is the router that belongs to IBM, and the GWA is located in the same site as IBM Electronic Service.
  - A VPN connection is also established between the packet filter router and the iSeries server. The QTOCL2TP profile becomes active.
- **Phase 3**

  IBM Electronic Support connection is now established between the iSeries server and IBM Electronic Support. ECS establishes the TCP connection between the iSeries server and IBM Electronic Support through the ESP encrypted tunnel. All IP datagrams of the TCP connection are invisible because these datagrams are encapsulated and encrypted by ESP protocol. The TCP connection for the IBM Electronic Support application is now established.

Before you start the IBM Electronic Support connection with multi-hop, check that these prerequisites are in place:

- The TCP interface that will be used for the packet filter router and the IBM Electronic Service connection must be Active.
- IP datagrams must be routable for both Outbound and Inbound directions. If you applied the IP filter rules on the Packet Filter Router, review Chapter 5, "Multi-hop scenario" on page 151, and determine what IP filter rules must be applied on the packet filter router.

The following steps provide a troubleshooting guide for the multi-hop scenario. They cover the connection between the iSeries server and the packet filter router.

Keep in mind that a successful connection is only attained once complete connectivity is available from the iSeries server to IBM Electronic Support.

1. Check IP datagram connectivity with the PING command.

   If both tunnels are created, all required IP routes to the IBM Electronic Server are added. However, there is a possibility that the IP datagram doesn't go through the Internet if there is a malfunction on the Internet. The PING command uses the ICMP protocol to verify the connectivity of the IP datagram.

   Perform the following steps to check the IP datagram connectivity with the PING command:

   a. Open the 5250 Emulator screen. Sign on the with the user ID and password.

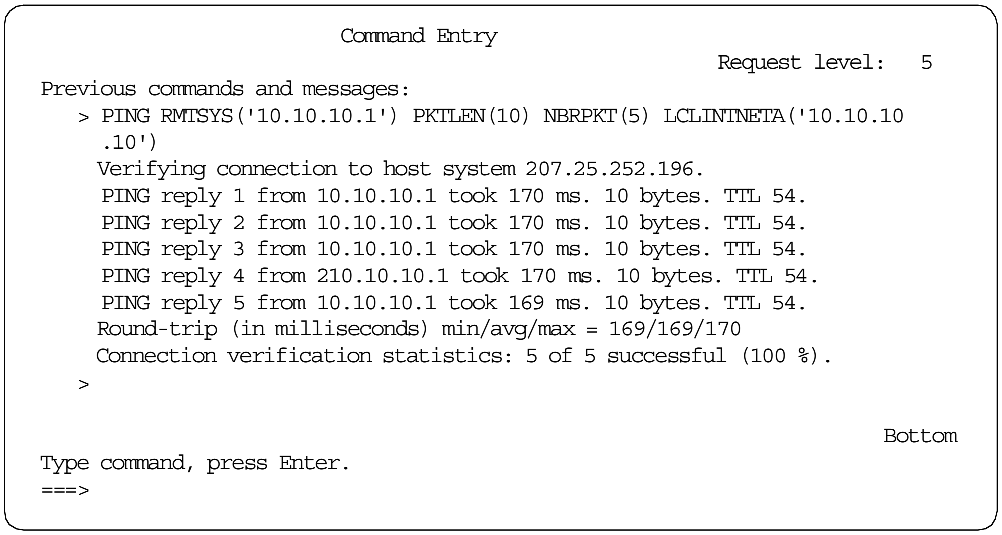
   b. Type `CALL QCMD` and press Enter to go to the command entry screen.

   c. Type the following command:

   ```
   PING RMTSYS('10.10.10.1') PKTLEN(10) NBRPKT(5) LCLINTNETA('10.10.10.10')
   ```

   Press Enter as shown in Figure 192.

   Note: LCLINETNETA means the local IP address of the TCP interface being used for the IBM Electronic Support connection. This address can be obtained from the L2TP initiator profile.



```
                              Command Entry
                                                     Request level:   5
Previous commands and messages:
   > PING RMTSYS('10.10.10.1') PKTLEN(10) NBRPKT(5) LCLINTNETA('10.10.10
     .10')
     Verifying connection to host system 207.25.252.196.
      PING reply 1 from 10.10.10.1 took 170 ms. 10 bytes. TTL 54.
      PING reply 2 from 10.10.10.1 took 170 ms. 10 bytes. TTL 54.
      PING reply 3 from 10.10.10.1 took 170 ms. 10 bytes. TTL 54.
      PING reply 4 from 210.10.10.1 took 170 ms. 10 bytes. TTL 54.
      PING reply 5 from 10.10.10.1 took 169 ms. 10 bytes. TTL 54.
     Round-trip (in milliseconds) min/avg/max = 169/169/170
     Connection verification statistics: 5 of 5 successful (100 %).
   >

                                                                    Bottom
Type command, press Enter.
===>
```

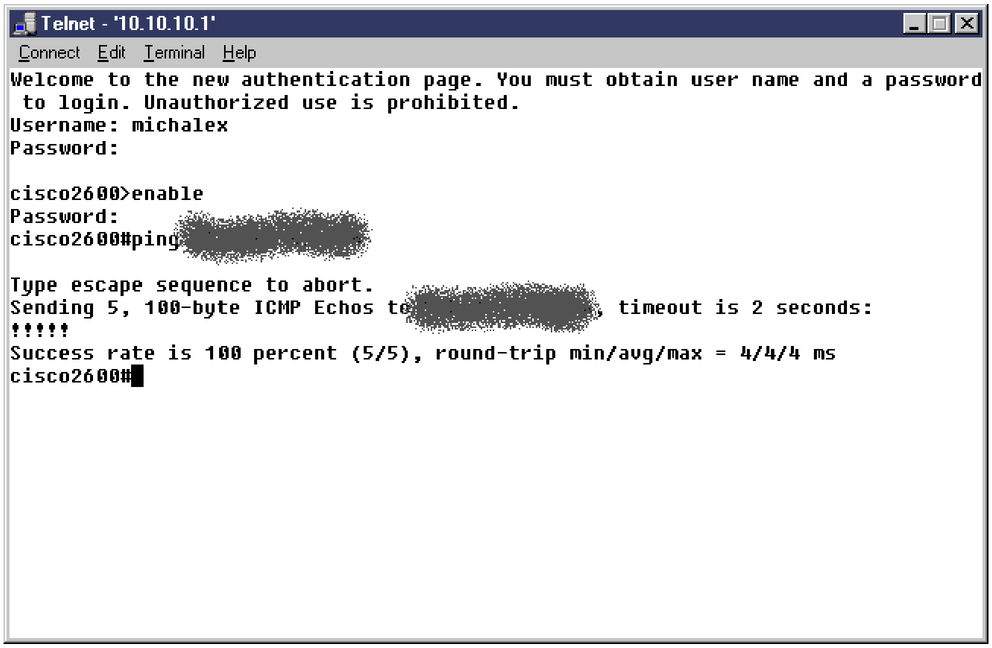
Figure 192. PING command execution screen

   Did you received the PING reply from the packet filter router (10.10.10.1)?

   - **Yes**: IP datagram connectivity is OK. Proceed to step 2.
   - **No**: There may be a network problem between your iSeries server and the packet filter router. Call your router vendor to report the connectivity problem.

2. Check the connectivity between the packet filter router and IBM gateway.

   Log on to the packet filter router using the Telnet application. We recommend that you do this from an MS-DOS prompt on a PC that is directly connected to the router. If you do not have access to the router, or you need further assistance in following this step, contact your router vendor. Once logged into the router, try to Ping the IP address of the IBM gateway. An example is shown in Figure 193.



```
Welcome to the new authentication page. You must obtain user name and a password
 to login. Unauthorized use is prohibited.
Username: michalex
Password:

cisco2600>enable
Password:
cisco2600#ping [redacted]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to [redacted], timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
cisco2600#
```

Figure 193. PING request to IBM gateway from a Cisco router

Did you receive a PING reply from the IBM gateway (GWA IP address)?

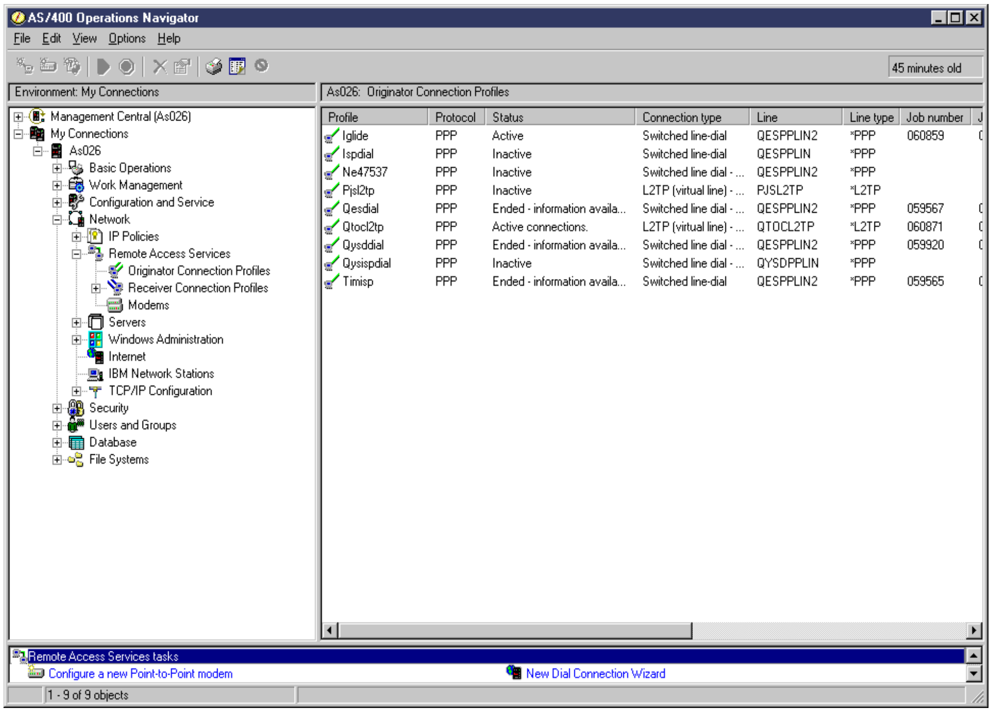
- **Yes**: IP datagram connectivity is OK. Proceed to Step 3.
- **No**: There may be a network problem between your packet filter router and the IBM gateway. Contact your ISP vendor to report this problem.

3. Check the L2TP initiator QTOCL2TP status.

   Check the L2TP initiator profile by following these steps:

   a. Click **Originator Connection Profiles**.

      Look for QTOCL2TP as shown in Figure 194. The status is idle at the beginning, but then changes to *Active*.



As026: Originator Connection Profiles

Profile	Protocol	Status	Connection type	Line	Line type	Job number	J
Iglide	PPP	Active	Switched line-dial	QESPPLIN2	*PPP	060859	(
Ispdial	PPP	Inactive	Switched line-dial	QESPPLIN	*PPP		
Ne47537	PPP	Inactive	Switched line dial - ...	QESPPLIN2	*PPP		
Pjsl2tp	PPP	Inactive	L2TP (virtual line) - ...	PJSL2TP	*L2TP		
Qesdial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059567	(
Qtocl2tp	PPP	Active connections.	L2TP (virtual line) - ...	QTOCL2TP	*L2TP	060871	(
Qysddial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059920	(
Qysispdial	PPP	Inactive	Switched line dial - ...	QYSDPPLIN	*PPP		
Timisp	PPP	Ended - information availa...	Switched line-dial	QESPPLIN2	*PPP	059565	(

Figure 194. QTOCL2TP status display

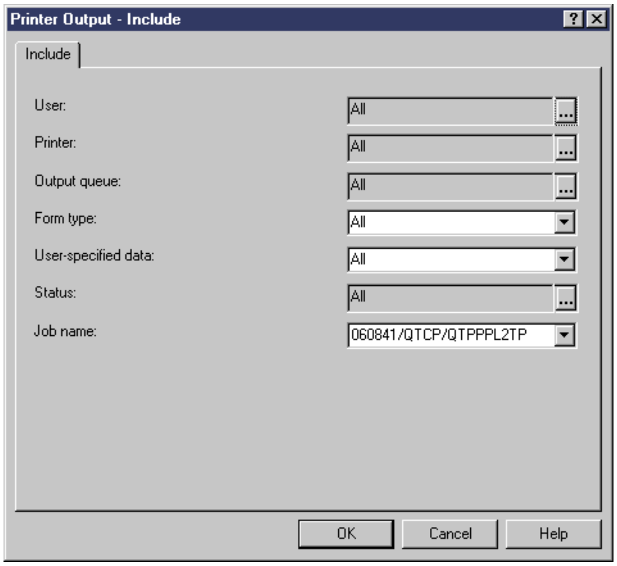
Is the QTOCL2TP profile in an Active connections state?

- **Yes**: Contact IBM Support.
- **No**: If the status of the QTOCL2TP profile is not Active connections, check the QTPPPL2TP job log contents.

  The QTPPPL2TP job log contains useful messages to isolate the problem. To look at the QTPPPL2TP job log on the Operations Navigator display, complete these steps:

  1. Click **Originator Connection Profiles**. Look for the QTOCL2TP profile. Write down the job number, job user, and job of the QTOCL2TP. This information is shown on the right side of the QTOCL2TP. Scroll the screen to the right to see the information if required.
  2. Click **Basic Operations**.
  3. Click **Printer output**.
  4. Click **Options** on the task bar. On the pull-down menu, choose **Include**. On the next screen, click the small box that is the rightmost of the User column. Click **ALL** and click **OK**.

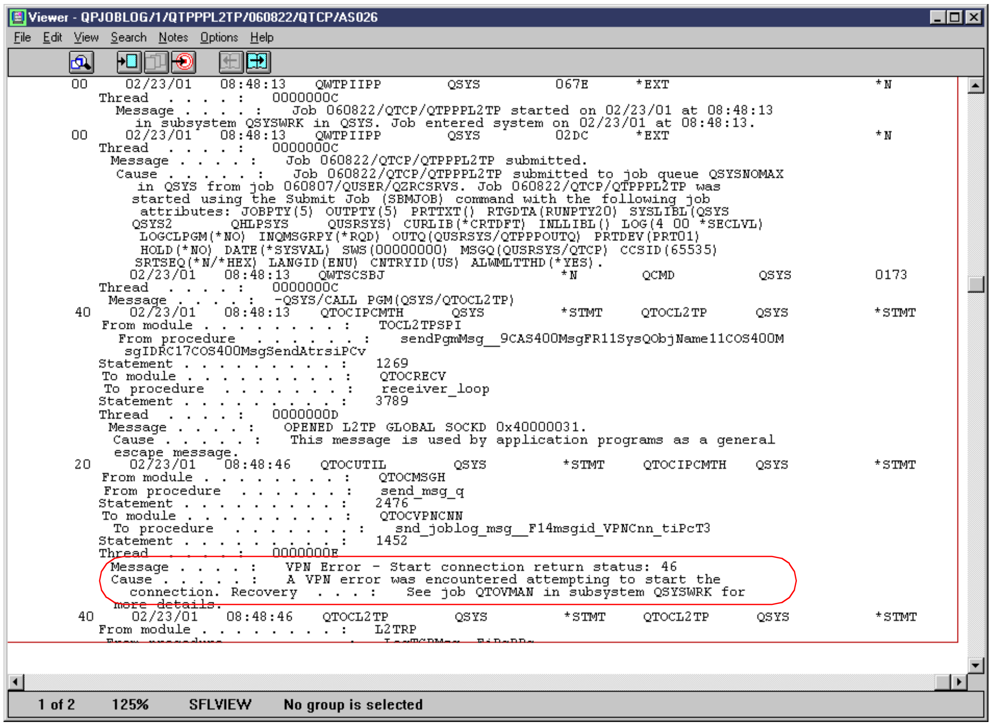
     Click the small box that is to the right of the Job name column and type in the job number, job user, and job that you wrote down in step 1. Click **OK** as shown in Figure 195.



User: All
Printer: All
Output queue: All
Form type: All
User-specified data: All
Status: All
Job name: 060841/QTCP/QTPPPL2TP

Figure 195. QTOCL2TP Job name selection

4. Double-click the Job name **QTOCL2TP** to see the QTOCL2TP job log (Figure 196). Check if any error is logged on the job log. In this case, a VPN error is logged. Write down the error code and description and contact IBM Support.

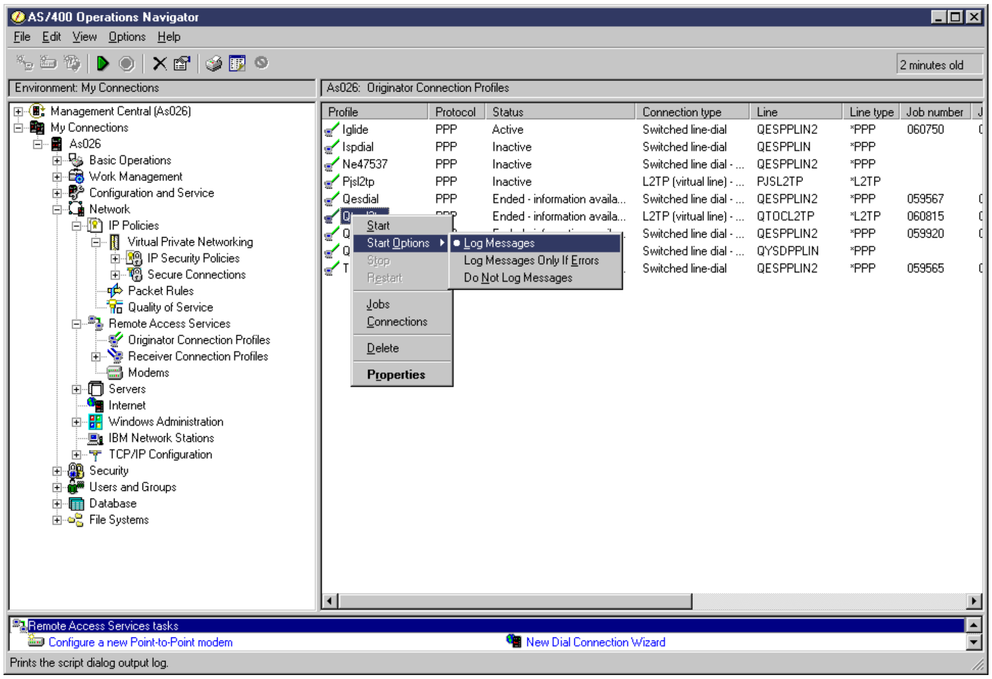


```
  00    02/23/01   08:48:13   QWTPIIPP       QSYS        067E     *EXT                       *N
      Thread  . . . . :   0000000C
        Message . . . . :   Job 060822/QTCP/QTPPPL2TP started on 02/23/01 at 08:48:13
          in subsystem QSYSWRK in QSYS. Job entered system on 02/23/01 at 08:48:13.
  00    02/23/01   08:48:13   QWTPIIPP       QSYS        02DC     *EXT                       *N
      Thread  . . . . :   0000000C
       Message . . . . :   Job 060822/QTCP/QTPPPL2TP submitted.
        Cause . . . . . :   Job 060822/QTCP/QTPPPL2TP submitted to job queue QSYSNOMAX
          in QSYS from job 060807/QUSER/QZRCSRVS. Job 060822/QTCP/QTPPPL2TP was
         started using the Submit Job (SBMJOB) command with the following job
          attributes: JOBPTY(5) OUTPTY(5) PRTTXT() RTGDTA(RUNPTY20) SYSLIBL(QSYS
         QSYS2      QHLPSYS     QUSRSYS) CURLIB(*CRTDFT) INLLIBL() LOG(4 00 *SECLVL)
          LOGCLPGM(*NO) INQMSGRPY(*RQD) OUTQ(QUSRSYS/QTPPPOUTQ) PRTDEV(PRT01)
          HOLD(*NO) DATE(*SYSVAL) SWS(00000000) MSGQ(QUSRSYS/QTCP) CCSID(65535)
         SRTSEQ(*N/*HEX) LANGID(ENU) CNTRYID(US) ALWMLTTHD(*YES).
        02/23/01   08:48:13   QWTSCSBJ                      *N       QCMD        QSYS        0173
      Thread  . . . . :   0000000C
       Message . . . . :  -QSYS/CALL PGM(QSYS/QTOCL2TP)
  40    02/23/01   08:48:13   QTOCIPCMTH     QSYS        *STMT    QTOCL2TP    QSYS        *STMT
      From module . . . . . . . . :   TOCL2TPSPI
        From procedure  . . . . . . :   sendPgmMsg__9CAS400MsgFR11SysQObjName11COS400M
         sgIDRC17COS400MsgSendAtrsiPCv
      Statement . . . . . . . . . :   1269
      To module . . . . . . . . . :   QTOCRECV
       To procedure  . . . . . . . :   receiver_loop
      Statement . . . . . . . . . :   3789
      Thread  . . . . :   0000000D
       Message . . . . :   OPENED L2TP GLOBAL SOCKD 0x40000031.
        Cause . . . . . :   This message is used by application programs as a general
        escape message.
  20    02/23/01   08:48:46   QTOCUTIL       QSYS        *STMT    QTOCIPCMTH  QSYS        *STMT
      From module . . . . . . . . :   QTOCMSGH
       From procedure  . . . . . . :   send_msg_q
      Statement . . . . . . . . . :   2476
      To module . . . . . . . . . :   QTOCVPNCNN
        To procedure  . . . . . . . :   snd_joblog_msg__F14msgid_VPNCnn_tiPcT3
      Statement . . . . . . . . . :   1452
      Thread  . . . . :   0000000E
       Message . . . . :   VPN Error - Start connection return status: 46
       Cause . . . . . :   A VPN error was encountered attempting to start the
         connection. Recovery  . . . :   See job QTOVMAN in subsystem QSYSWRK for
        more details.
  40    02/23/01   08:48:46   QTOCL2TP       QSYS        *STMT    QTOCL2TP    QSYS        *STMT
      From module . . . . . . . . :   L2TRP
```

Figure 196. QTOCL2TP job log contents

If you see the message that the job has ended already and there is no QTOCL2TP job log left, perform the following steps to change the setting to keep the QTOCL2TP job log. Then, try to make the IBM Electronic Support connection again to get the error message on the QTOCL2TP job log.

1. Click **Originator Connection Profiles**.
2. Right-click **QTOCL2TP**. On the pull-down menu, choose **Start Options**, and then choose **Log Messages** as shown in Figure 197.



As026: Originator Connection Profiles

Profile	Protocol	Status	Connection type	Line	Line type	Job number
Iglide	PPP	Active	Switched line-dial	QESPPLIN2	*PPP	060750
Ispdial	PPP	Inactive	Switched line-dial	QESPPLIN	*PPP	
Ne47537	PPP	Inactive	Switched line dial - ...	QESPPLIN2	*PPP	
Pjsl2tp	PPP	Inactive	L2TP (virtual line) - ...	PJSL2TP	*L2TP	
Qesdial	PPP	Ended - information availa...	Switched line dial - ...	QESPPLIN2	*PPP	059567
Q		Ended - information availa...	L2TP (virtual line) - ...	QTOCL2TP	*L2TP	060815
Q			Switched line dial - ...	QESPPLIN2	*PPP	059920
Q			Switched line dial - ...	QYSDPPLIN	*PPP	
T			Switched line-dial	QESPPLIN2	*PPP	059565

Prints the script dialog output log.

Figure 197. QTOCL2TP job Start Options change

3. Try to make an IBM Electronic Support connection again. The QTOCL2TP job log should now remain in the system. Examine the job log and report any VPN errors to IBM Support.

This ends the problem determination procedure for the multi-hop connection.

Appendix A. Special notices

The information in this publication is not intended as the specification of any programming interfaces that are provided IBM @server iSeries Universal Connection. See the PUBLICATIONS section of the IBM Programming Announcement 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 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.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

e (logo)®
IBM ®
AS/400
AS/400e
AT
CT
Current
Hummingbird
IBM
Netfinity
Network Station
OS/2
OS/400
RS/6000
Redbooks
Redbooks Logo
Service Director
SP
System/390
Wizard
XT
400
Lotus
Lotus Notes
Domino
Notes
Tivoli

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

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 other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

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 IBM Redbooks

For information on ordering these publications see “How to get IBM Redbooks” on page 215.

- *TCP/IP Tutorial Technical Overview*, GG24-3376
- *Remote Access to AS/400 with Windows 2000 VPN Clients*, REDP0036
- *IBM Firewall for AS/400 V4R3: VPN and NAT Support*, SG24-5376
- *AS/400 Internet Security: Implementing AS/400 Virtual Private Networks,* SG24-5404
- *AS/400 Internet Security Scenarios: A Practical Approach*, SG24-5954

B.2 Other resources

These publications are also relevant as further information sources:

- *TCP/IP Configuration and Reference*, SC41-5420
- Chapman, D. Brent; Zwicky, Elizabeth D., *Building Internet Firewalls.* O’Reilly & Associates, 1995 (ISBN 1-56592-124-0).
- Liu, Cricket; Albitz, Paul; Loukides, Mike. *DNS and BIND.* O’Reilly & Associates, 1998 (ISBN 1-56-592512-2).
- The following RFCs are available on the Web at: `http://www.rfc-editor.org/rfc`
  – *Domain Names - Concepts and Facilities*, RFC 1034
  – *Domain Names - Implementation and Specification*, RFC 1035
  – *Requirements for Internet hosts: Communication Layers*, RFC1122
  – *Requirements for IP Version 4 Routers*, RFC 1812
  – *Domain Name System Security Extensions*, RFC 2065
  – *Site Security Handbook*, RFC 2196
  – *The TLS Protocol Version 1.0*, RFC 2246

B.3 Referenced Web sites

These Web sites are also relevant as further information sources:

- iSeries home page: `http://www.ibm.com/eserver/iseries`
- IBM @server Technical Support: `http://www.ibm.com/servers/support`
- iSeries and AS/400 Technical Support: `http://www.ibm.com/as400/support`
- Electronic Services for AS/400 and iSeries sign in page: `https://www.ibm.com/services/electronic/`
- IBM Electronic Services: `http://www.ibm.com/support/electronic/navpage`

- Managing Performance, PM/400e home page: `http://www.ibm.com/eserver/iseries/pm400`
- IBM Workload Estimator for iSeries: `http://www.as400service.ibm.com/estimator`
- Physical Device Placement Assistant: `http://www.ibm.com/eserver/iseries/cif`
- IBM white paper *AS/400 and Network Security Directions* at: `http://www-1.ibm.com/servers/eserver/iseries/software/firewall/pdf/fw_whitepaper.pdf`
- Tivoli Risk Manager: `http://www.tivoli.com/products/index/secureway_risk_mgr/`
- *Security Problems in the TCP/IP Protocol Suite* `http://www.insecure.org/stf/tcpip_smb.txt`
- CERT Coordination Center: `http://www.cert.org`
- National Institute of Standards and Technology: `http://www.nist.gov`
- National Security Institute/Computer Security: `http://www.nsi.org/compsec.html`
- NSI's Extensive List of Links: `http://www.nsi.org/Computer/links.html`
- ICSA.net: `http://www.icsa.net`
- CERT Coordination Center: `http://www.cert.org/index.html`
- CERT Denial of Service: `http://www.cert.org/tech_tips/denial_of_service.html#3`
- National Institute of Standards and Technology: `http://cs-www.ncsl.nist.gov/`
- Center for Information Technology / Security: `http://www.cit.nih.gov/security.html`
- SANS Institute: `http://www.sans.org/newlook/home.htm`
- Global Incident Analysis Center: `http://www.sans.org/giac.htm`
- IBM Emergency Response Service (ERS): `http://www.ers.ibm.com/`
- SecurityFocus.com: `http://Securityfocus.com/`
- SecurityPortal.com: `http://www.securityportal.com`
- SecurityWatch.com: `http://www.securitywatch.com`
- Info Security Magazine: `http://www.infosecuritymag.com`
- SC Magazine: `http://www.infosecnews.com`
- Network Computing: Security Technology Guide: `http://www.networkcomputing.com/core/core8.html`
- Tech Web: Security Tech Center: `http://www.planetit.com/techcenters/security`
- ZDNET / Security: `http://www.zdnet.com/enterprise/security`/
- IBM Security Services:
  `http://www.ibm.com/security/services`
  `http://www.ibm.com/services/e-business/security`
- Mail Abuse Prevention System (MAPS): `http://www.mail-abuse.org/`

- Purdue University Intrusion detection projects: `http://www.cerias.purdue.edu/coast/ids/`
- Modes of Attack: `http://www.cert.org/tech_tips/denial_of_service.html#3`
- Exchange, SMTP, and DNS issues: `http://www.swinc.com/resource/exch_smtp_dnsissues.htm`
- Cisco Systems New Feature Documentation site for information on L2TP Tunnel Switching: `http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121dc/121dc1/l2switch.htm`
- *Configuring L2TP Multihop to Perform Several Hops from the NAS to the LNS*: `http://www.cisco.com/warp/public/471/l2tp_multihop2.html`
- Cisco IOS 11.3 Configuration Guides, Command References: `http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scoverv.htm#27433`
- L2TP protocol extensions: `http://www.ietf.org/html.charters/l2tpext-charter.html`
- VPN and L2TP: `http://www.as400.ibm.com/tcpip/common/remoteacc/html/remoteaccc.htm`

B.4 How to get IBM Redbooks

Search for additional Redbooks or redpieces, view, download, or order hardcopy from the Redbooks Web Site

ibm.com/redbooks

Also 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.

B.5 IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the CD-ROMs button on the Redbooks Web Site for information about all the CD-ROMs offered, updates and formats.

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** **ibm.com**/redbooks

  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 IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.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.

Index

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 845 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6224-00 iSeries Universal Connection for Electronic Support and Services Electronic Services
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	 O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

IBM Redbooks

IBM @server iSeries Universal Connection for Electronic Support and Services

(0.2”spine)
0.17”<->0.473”
90<->249 pages

IBM

IBM @server iSeries Universal Connection

for Electronic Support and Services

Redbooks

Explains the supported functions with Universal Connection

Shows how to install, tailor, and configure Universal Connection

Helps you determine communications problems

Introducing IBM @server iSeries Universal Connection! Now you have more options in OS/400 V5R1 and V4R5 for Electronic Customer Support (ECS) and Electronic Service Agent connectivity. Universal Connection offers dial-up support over TCP/IP via AT&T Global Network Services. It supports an Internet connection using a virtual private network (VPN) for more secure connections over the Internet. For example, you can have a direct Internet connection through an integrated modem (9771) with an Internet Service Provider (ISP) of your choice. Or you can have higher speed direct Internet connections (T1, T2, Ethernet-attached cable, or DSL modems).

This IBM Redbook explains how to use the variety of ESP support tools that report inventories of software and hardware on your machine to IBM so you can get personalized electronic support, based on your system data. This helps streamline your support process so that you can spend more time running your business rather than maintaining your systems. You control the transmission of data to IBM (what is sent and when it is sent). Then IBM helps secure your customer data and use that data to appropriately provide you our world-class, personalized support. This book also shows you how to install, tailor, and configure the new Universal Connection Wizard for your environment.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6224-00 ISBN 0738422282