IBM System p5™
Firmware and Microcode
Service Strategies and Best Practices

IBM CORPORATION®

INTRODUCTION

In May 2002, firmware and microcode update control was returned to customers to eliminate the requirement to schedule an IBM® engineer for any and all updates. Although IBM services may still be requested to plan and implement microcode updates, each individual customer is now provided the choice of maintenance strategies. Firmware currency remains a vital foundation to availability in any environment. Although some IBM System p™ customers may choose a conservative approach to firmware and software updates, choosing to remain at levels that differ from the most recent release or service pack, falling too far behind in currency creates a substantial hazard. It is important to stay on supported levels of firmware and to maintain good microcode hygiene. Furthermore, establishing maintenance windows, and architecture and change methodologies suitable to a chosen availability level are an essential component of system planning and administration.

In response to client's increasing dependencies on their IT structure, 24/7 business continuity and critical yet disparate workloads that share machines and regions, IBM has introduced the concept of concurrent firmware (CFM) updates for IBM System p5 client environments managed by Hardware Management Consoles (HMC). CFM allows a substantial number of firmware and microcode updates that do not require an Initial Program Load (IPL). This allows the IBM System p5™ environment to significantly reduce planned downtime and simplifies much of the maintenance burden. In conjunction with changes in AIX 5L™ service strategies, CFM was introduced as a means of reducing the number of required outages that a server must sustain in order to maintain currency. Both AIX 5L technology levels (TL) and CFM strive for twice-yearly coordinated release dates supported by subsequent service packs. This enables IBM System p clients to plan for a twice per year cadence for releases supplemented by subsequent service pack implementations as required by the environment. This document is intended to provide an overview of firmware strategies and to suggest best practices in updating IBM POWER5™ environments. It is limited to addressing strategies for IBM POWER5 System Firmware and Bulk Power code.

Purpose

This document is intended to provide a simply stated explanation of firmware maintenance options and recommended strategies. The focus is on new concepts and functions that have been designed to simplify installation processes and help customers maintain the firmware on their System p5 systems with minimal impact. This document is not intended to provide an in-depth technical explanation of the internal processes by which firmware is applied and activated. Furthermore, there are tools that add to the stability and availability of an environment such as properly installed and configured Service Agent that are addressed in other documents and are only mentioned here for completeness.

Terms and Concepts

Concurrent Firmware (CFM) is the IBM term used to describe the IBM POWER 5 firmware updates that *can* be partially or wholly 'concurrent' or nondisruptive. Nondisruptive is the term we will use to describe a microcode fix or collection of fixes that can be deployed on a running system without rebooting partitions or performing an Initial Program Load (IPL). Although CFM is often collectively used as a general term to describe the System p5 firmware process, System p5 firmware releases and often service packs may contain both fixes which are concurrent and some which require a platform reboot to implement. We will discuss two concepts; release levels and service packs. We must also understand three key terms: concurrent, deferred and disruptive fixes. For the purposes of this discussion we will use the definitions described below.

- ✓ **Concurrent: A fix or set of fixes which can be applied and activated concurrently (i.e., no system IPL is required). In other words this can be applied and activated on a running system.**
    - **Deferred: A fix or set of fixes which can be applied concurrently but which contains some which affect the IPL path and therefore are not activated until the next IPL. In most cases most of the fixes can be activated concurrently and only a subset of the fixes require an IPL to activate.**
        - Only specific fixes that are designated as 'deferred' within a service pack require an IPL for activation. These fixes will be activated at the next IPL. Fixes contained within the same service pack that are designated as 'concurrent' will be installed and activated concurrently without an IPL. In very early releases of CFM at SF230 all deferred fixes had to be cleared with an IPL prior to subsequent downloads. This is no longer the case.
- ✓ **Disruptive: When a *release or a disruptive fixpack* is installed, a system IPL will be required. (note: all RELEASEs are disruptive).**

With the introduction of CFM in Release 230, IBM also introduced N and N-1 Support. Simply stated, this means that when IBM makes a new release available ("N" level), the previous level ("N-1" level) will continue to be supported with fixes for a period of time (More information on this is provided later in this document). In support of this, there are 2 different types of firmware packages.

Firmware *Releases* enable new function and may also contain fixes or enhancements.

Firmware *Service Packs* provide fixes and enhancements within a specific release.

Release Level: A Release Level is the term for firmware that is released to support major new function (introduction of new hardware models and significant new function/features enabled via firmware. IBM intends to limit the introduction of Release Levels to no more than twice per year. In addition to the new function/hardware support, Release Levels will also contain fixes. In the past, we have used the term Firmware GA to describe these Release Levels internally within IBM.

Releases are targeted to be released twice yearly generally coinciding with IBM's hardware announcements. AIX clients embracing the new AIX 5L service strategy will notice that AIX releases are also on this 2-per-year cadence and for those clients with limited maintenance windows who are comfortable with simultaneously implementing O/S and firmware updates can reduce their total planned outage time by synchronizing the two update activities.

Upgrading from one release level to another will always be disruptive to customer operations, but release levels are not always required. For clients wishing to limit total planned maintenance time and not needing extensive new hardware function, it may be valid to skip release levels. It may be appropriate to upgrade from one release level to another release level while bypassing an interim level in order to reduce the downtime required to support an environment but it remains important to formulate a release strategy and methodology that allows the environment to maintain good firmware currency. Environments that cannot afford regular maintenance windows should embrace a *rolling* upgrade supported by failover software such as High Availability Cluster Management Protocol (HACMP) and the appropriate failover methodologies.

Service Pack: A Service Pack, also referred to as a fixpack, contains a group of fixes within a specific release level. Service packs primarily contain only fixes rather than new functionality; however, minor function changes may be released within a service pack. Fixes are deployed for highly pervasive, critical, or security related issues. Service packs are released following a release level and apply to a specific release level. The first service pack will generally be released approximately six to eight weeks following a release level and at subsequent 3 to 4 month intervals. To reduce the maintenance burden for System p5 clients, IBM has extended the length of time that an environment may remain on a release level. Release levels will be supported by service packs for a period of one year following the initial availability of the release. This sustains a particular release level supported by fixpacks without having to upgrade to a later release level.

CFM was introduced in system firmware release level SF230 (released June, 2005). Updating with concurrent service pack levels (within the same release level) can be performed concurrently for systems managed by an HMC. This allows you to make firmware updates without requiring an IPL thus, reducing downtime to install firmware maintenance. As with Release levels, a service pack can be skipped. Service Packs are cumulative, so if Service Pack 3 is applied, all of the previous fixes contained within Service Packs 1 and 2 will also be applied. It is important to note however that if a service pack level is skipped that is marked as disruptive, the cumulative level updated will force an IPL. This concept will be further explored under the section Concurrent Firmware Maintenance Overview.

Throughout the rest of this document, we will explore best practices and maintenance strategies predicated on an understanding of the terms defined on the following page.

Firmware Terminology

Accepted level: The lowest level of code on the system; resides on the p-side flash.

Activated level: The code level that the system is currently running; resides on the t-side flash.

Adapter microcode is the operating code of the adapter; it initializes the adapter when power is applied and controls many of the ongoing operations executed by the adapter. Device microcode provides these same functions for devices such as tape drives.

Bulk Power Subsystem Firmware: BPC Firmware interfaces with bulk power for power monitoring and control.

Concurrent Firmware Maintenance - the ability to deploy firmware updates on a running system without rebooting partitions or perturbing applications

Concurrent Update - – Firmware that can be applied and activated on running systems.

Deferred Update - Firmware that can be concurrently applied, but contains some fixes which can not be activated until the next IPL because the fixes affect the IPL path.

Disruptive Upgrade/Update – A Platform IPL is required to activate. None of the content contained in the Release/Service Pack will be activated until the next IPL.

Inband update: Firmware fix updates are initiated by the OS. This is used on non-HMC controlled systems.

Installed level: The highest level of code on the system. This code may or may not have been activated (i.e., loaded into memory).

Out of band update: Firmware fix updates are initiated by the HMC.

p-side : is the permanent side of the flash; it usually contains the older level of firmware code. **t-side**: is the temporary side of the flash and usually contains the newer level of firmware code.

System microcode, also called system firmware, initializes the hardware configuration enabling the system to boot up and operate correctly; it also provides the interface between the operating system software and the hardware. The terms microcode and firmware are used fairly interchangeably throughout this and other IBM documents.

FIRMWARE MAINTENANCE STRATEGIES

It is essential to periodically update the firmware on your System p5 servers. Keeping firmware current will help in attaining the maximum reliability and functionality from your systems. It is imperative that each environment have maintenance strategies that support the ability to maintain firmware currency. This may involve advertised maintenance windows that are negotiated with the application owners for applications which share partitions or machines or may necessitate architecting machine failovers for rolling firmware upgrades using cluster failover software. It is recommended that you develop a change control methodology, including a timetable, for keeping your system's firmware current while still meeting your business needs. It is further recommended that hardware monitoring with a product such as IBM's Service Agent be configured and installed.

IBM provides firmware subscription notifications to alert clients of firmware release or fixpack actions. Each environment should have a verified e-mail or notification for at least one administrator. Reviewing the firmware subscription notifications and the associated firmware README documents will help you make informed decisions regarding the updating of firmware as it applies to your environment. This will provide you with information regarding the content of firmware changes and severities so that you can determine whether the update affects your model and configuration. Assessing and understanding the content, along with understanding the severity of the problems addressed, can help you determine if and when to apply the firmware.

Your own firmware maintenance strategy will be largely determined by the priorities of your business. Since priorities often shift, it may be desirable to periodically review the methodology and the criteria being used to define the firmware strategy, and modify as necessary. Server consolidation scenarios warrant additional planning so that firmware hygiene and currency can be maintained. CFM makes practicing periodic firmware maintenance easier to implement by eliminating the need to IPL in most cases when updating firmware within a major release.

If adding new function to existing servers is a priority, customers may chose to monitor the Firmware README(s) (XML files) and announcement information to review functionality. This may best be viewed by following the DESC link on the firmware download webpage. This information may be utilized to help determine if and when upgrading to a new release is right for the business. Occasionally, situations will arise where a critical problem (i.e. security, etc) is discovered by IBM and a new level of firmware is released to correct it. In the event that this occurs, IBM will notify you via subscription service and provide you with the information needed to allow you to evaluate the situation as it relates to your operating environment. If a given problem affects your systems, the appropriate firmware update should be applied. as soon as possible to avoid potential problems.

GENERAL FIRMWARE STRATEGIES

IBM releases new firmware for the following reasons:

1. The addition of new system function.
2. To correct or avoid a problem.

There are some natural points at which firmware should be evaluated for potential updates:

- ✓ When a subscription notice advises of a critical or HIPER (highly pervasive) fix, the environment should be reviewed to determine if the fix should be applied.
- ✓ When one of the twice-yearly updates is released.
- ✓ Whenever new hardware is introduced into the environment the firmware pre-reqs and co-reqs should be evaluated.
- ✓ Anytime HMC firmware levels are adjusted.
- ✓ Whenever an outage is scheduled for a system which otherwise has limited opportunity to update or upgrade.
- ✓ When the firmware level your system is on is approaching end-of-service.
- ✓ If other similar hardware systems are being upgraded and firmware consistency can be maximized by a more homogenous firmware level.
- ✓ On a yearly cycle if firmware has not been updated or upgraded within the last year.

Both *releases* and *service packs* are cumulative in nature. This means that each new Release or Service Pack is a “superset” of the previous level. Simply put, each new release/service pack is comprised of its previous level plus new fixes.

Both are full replacements of the previous image and usually contain multiple fixes. They are packaged in this way to provide the firmware as an "installable entity." The installation of a firmware ***release*** is called an "upgrade," while the installation of a ***service pack*** within a release is called an "update." While Service Packs labeled concurrent can be backed out, it is necessary to note that back-leveling Firmware Release levels is not generally recommended.

Since System p5 as a whole may be comprised of an HMC and a Power Frame (575, 590 and 595 models only) as well the server, the Bulk Power and HMC code may also be considered to be a part of a Release and/or Service Pack, but are packaged separately.

System Firmware function often have interdependencies with HMC and/or Bulk Power code. To better understand the associated levels of each, refer to the System p5 code matrix. The matrix can be found at:

http://www14.software.ibm.com/webapp/set2/sas/f/hmc

There are some general guidelines that should be considered as a starting point in pre-planning for a firmware event:

1. First and foremost, review the environment for any existing issues or problems. Check hardware and software logs and resolve as many outstanding issues as possible before undertaking the maintenance event. (For Release level SF235 and beyond, there is a firmware tool available to assist with this).
2. Existing HMC, Bulk Power and System firmware levels should be determined and documented.
3. Determine the correct level of code for HMC, Bulk Power and System Firmware. Locate this and review all README(s) and current documentation.
4. Review the system's hardware inventory and validate that against firmware levels. If a piece of hardware is introduced that requires higher level of firmware, this may necessitate upgrading other components.
5. Determine whether the proposed fixes are concurrent / deferred / disruptive.
6. Put together a plan for ALL related firmware events (example – HMC should be upgraded and at highest level in the complex).
7. Some of the suggested physical checks would include reviewing the current Installed Level of code for FSP and BPC through the Licensed Internal Code Maintenance folder on the HMC.
   - The Installed Level indicates the level of firmware that has been installed and will be loaded into memory after the managed system is powered off and powered on.
   - The Activated Level indicates the level of firmware that is active and running in memory.
   - The Accepted Level indicates the backup level of firmware.
   - The HMC code level can be ascertained by right clicking on the HMC GUI desktop, selecting 'rshterm' and entering *lshmc –V*.
8. Schedule and announce a maintenance event even when firmware is concurrent. There will be no planned reboot but there should be advance notice to users of the timeframe.

POWER5™ Firmware Concepts

POWER5 system firmware is comprised of various system components and may be broken down into the following subsystems (collectively referred to as system *firmware* or *microcode* within this document). (see Figure 1).

- The Flexible Service Processor (FSP) firmware provides diagnostics, initialization, configuration, run-time error detection, and correction.
- The Power Hypervisor (PHYP) firmware, which is based on the IBM System i™ hypervisor, provides VLAN, virtual I/O, and partitioning support.

- The Platform Firmware (PFW) supports the System p Power Architecture Platform Requirements+ (PAPR+) interface.
- The System Power Control Network (SPCN) firmware interfaces with bulk power for power monitoring and control.

The above firmware components are packaged and installed together as a single entity.

The installation process of a System Firmware Release or Service Pack has five steps:

1. You must "retrieve" the fixes by obtaining them from a repository location. The repository may be the Microcode Website, an FTP site or physical media.
2. You must install the firmware on the system. Installing is the process that writes on flash the code that is to be loaded into memory at the next system Initial Program Load (IPL). Flash is a nonvolatile storage location in FSP where firmware is contained for the next activation.
3. For a Release, you must perform a platform IPL.
4. For Firmware installed concurrently via the HMC, you must "activate" the firmware by loading the firmware code level to be run into system memory. When people talk about an "activated level," they are referring to the level of firmware code running in system memory.
5. When you are satisfied with firmware upgrade, you may request that the system "accept" the firmware by copying the installed level of firmware code to the p-side flash. When people talk about an "accepted level," they are referring to the lowest firmware code level on the two flash sides; usually, this is on the p-side code level.
6. Although Service Packs may be backed out, a new release is applied to both t and p sides. 'Backleveling a release' involves installing an older release to BOTH t and p sides. IBM does not generally recommend backleveling Firmware Releases.

Additionally, some System p5 systems also require additional firmware as described below:

- The Bulk Power Control (BPC) firmware controls each bulk power unit in the CEC as well as within power expansion frames for the 575, 590 and 595 models

- The Hardware Management Console (HMC) firmware provides configuration, management, and service functions on HMC controlled System p5 systems.

The Bulk Power and HMC firmware are each individually packaged and installed.

The HMC firmware will properly update BPC and Server firmware in the correct sequence if both images are obtained from the designated repository. This applies only to models 575, 590 and 595. The Server firmware and BPC firmware must be at the same release level, so it is very important to install a new release from a designated repository that has both Server firmware and BPC firmware images.

Figure 1 below provides a visual description of the System p5 firmware components:

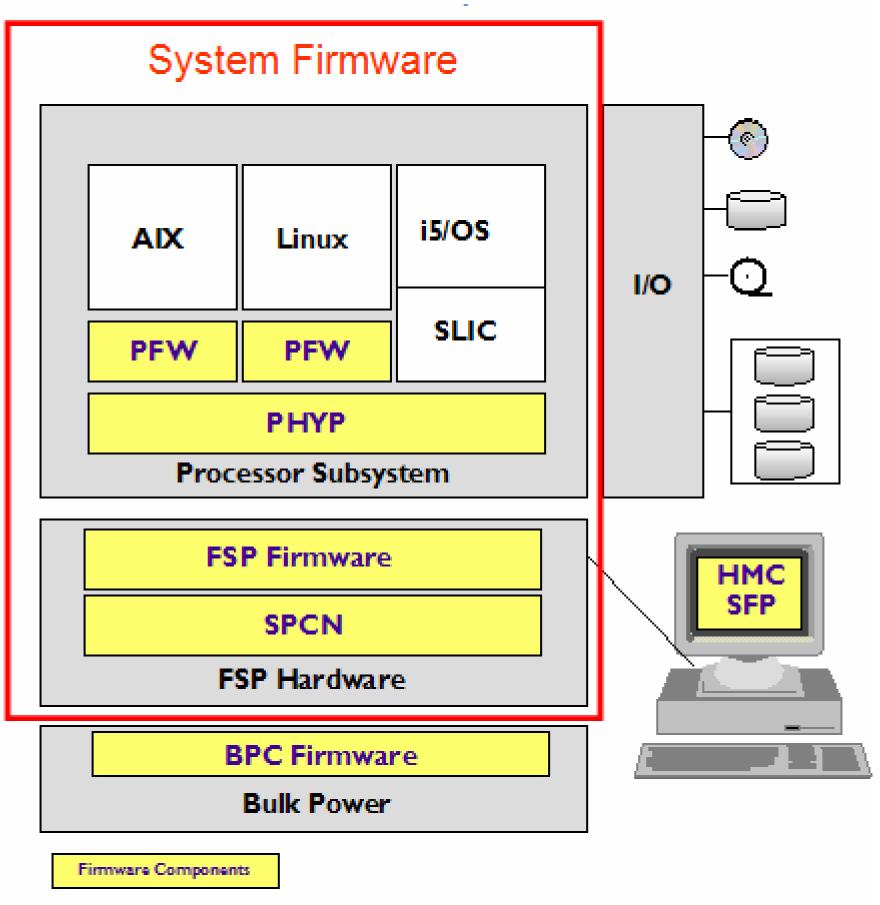


Figure 1: These are the system firmware components.

Throughout this document the terms microcode and firmware should be considered synonymous. Firmware Readme's will also use these term interchangeably.

Concurrent Firmware Maintenance (CFM) Overview

Concurrent Firmware Maintenance (CFM) is the ability to deploy firmware updates on a running system without rebooting partitions or perturbing applications. This function is only available on HMC controlled System p5 servers.

- When using the HMC Code Update function, the concurrent update process is seen by the user as one process, but actually involves two steps:

- Apply the firmware (update what is in flash)
- Activate the firmware (cause the new firmware to be running on the system)

Again, the CFM implementation involves the introduction of N and N-1 Support. This simply means that while IBM will continue to introduce new system function and provide fixes via new 'releases' (referred to here as 'N'), there will also be continued fix support, via 'Service Packs' for the previous release for a period of 1 year from the original release date.

For example, "Release A" becomes generally available on 2/15/2005. It enables newly announced function. It also provides fixes to the previous release. Upgrading a system to "Release A" from an earlier release requires a reboot. New releases are always disruptive to server operations, meaning that an IPL is required to activate the new firmware.

"Release B" then becomes available on 8/15/2005. It again provides new system function as well as fixes to the previous release (in this case, "Release A").

If the customer chooses to utilize any of the new functions introduced in "Release B", an *upgrade* from "Release A" to "Release B" is required. This is a disruptive action and requires that the system be rebooted to activate the new release level for firmware.

However, if the customer does not need to enable new function, CFM provides the option of allowing the system to remain at "Release A" while still obtaining fixes that are relevant to that system. Since the customer has chosen not to cross the release boundary, these fixes can, in most cases, be applied and activated on the system concurrently, or without the need to reboot. The fixes are packaged, tested and released in *'Service Packs'*. These Service packs are cumulative and contain multiple fixes.

It is important to note that not all service packs within a release can be installed and activated concurrently. Although IBM will make every attempt to allow as many fixes to be concurrent as possible, most concurrent fixpacks will contain at least some deferred content.

- To review, there are three types of service packs:
    - **Concurrent** – Apply and activate on running system
    - **Deferred** – Concurrent apply but contains fixes which affect IPL path – which are not activated until next IPL
        - Only specific fixes that are designated as 'deferred' within a service pack require an IPL for activation. These fixes will be activated at the next IPL. Fixes contained within the same service pack that are

designated as 'concurrent' will be installed and activated concurrently without an IPL. In very early releases of CFM at SF230 all deferred fixes had to be cleared with an IPL prior to subsequent downloads. This is no longer the case.

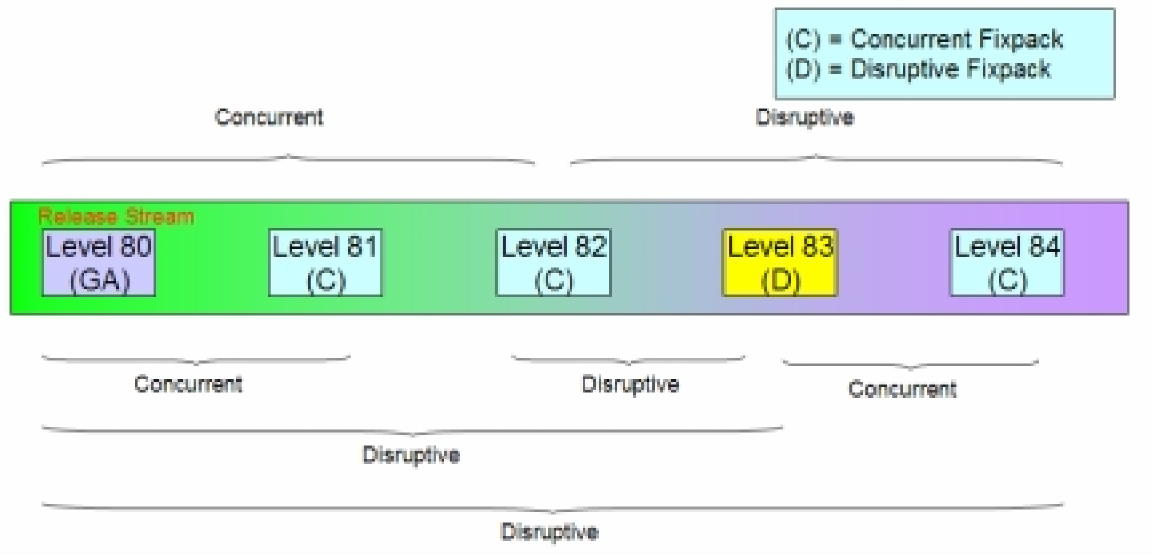
- **Disruptive –** Platform IPL required to activate
  - None of the service pack contents are activated until next IPL

Although most service packs within a release can be applied and activated concurrently (without reboot), there may be specific instances where a disruptive fix is required. As illustrated in Figure 2, service pack levels 81, 82, and 84 are concurrent. However, service pack level 83 is a disruptive service pack, although it is within the same release level.

If the system currently has Level 81 installed, Level 82 may be installed using the concurrent firmware method without an IPL. However, when moving from Level 81 to Level 83, the system must be IPL'd, because Level 83 is a disruptive service pack.

Following Service pack 83, the move to the service pack 84 would again be concurrent.

If the chosen installation path was an update from service pack level 81 to service pack level 84 (marked concurrent), Service pack levels 83's fixes which would be installed within the cumulative Level 84 update, would still necessitate an IPL.



–

- CFM capability exists only for System p5 systems that are HMC Controlled. Firmware maintenance on systems that are not HMC controlled continues to be a disruptive action

- The Concurrent Firmware maintenance scope is limited to server (system) firmware

    - Power subsystem (BPC) is a separate process and to date all BPC service packs have been concurrent with respect to server operations.

    - HMC itself is a separate process and concurrent with respect to servers managed. Refer to the HMC Best practices document for more detailed information on this.

Identifying firmware levels and Impacts

System p5 System Firmware File Naming Convention

All system and bulk power firmware releases and service packs are labeled as follows:

PPNNSSS_FFF_DDD

- PP = package identifier;

    a) If this value is **01**, it is identifying server (system) firmware
    b) If this value is **02**, it identifies power subsystem firmware (Bulk Power Code).

- NN = machine type/model group

    a) If this value is **SF**, it is identifying server (system) firmware
    b) If this value is **BP**, it is identifying power subsystem firmware (Bulk Power Code).

- SSS = Release Level Indicator (e.g., 230)
- FFF = Service pack level within that release (this number is incremental and increases with each service pack)
- DDD = Release or Service Pack level of the last disruptive level

Releases and service packs consist of a cover letter, an XML file and the firmware RPM file (for example, 01SF230_001_001.xml and 01SF230_001_001.rpm

Impact Statements

Classification Flag	**Description**
Availability	Fixes that improve the availability of resources.
Data	Fixes that resolve Customer data error
Function	Fixes that add(introduce) or affect system/machine operation with regards to Features, Connectivity, Resource
Security	Fixes that improve or resolve security issues.
Serviceability	Fixes that influence problem determination/fault isolation and maintenance with regards to Diagnostic errors, Incorrect FRU calls, False Error (No operational impact)
Performance	Fixes that improve or resolve throughput or response times
Usability	Fixes that improve user interfaces/messages

Severity Definitions

Classification Flag	Symbol Meaning	Description
HIPER	**H**igh **I**mpact/**PER**vasive	Should be installed as soon as possible.
SPE	**SPE**cial Attention	Should be installed at earliest convenience. Fixes for low potential high impact problems
ATT	**ATT**ention	Should be installed at earliest convenience. Fixes for low potential low to medium impact problems.
PE	**P**rogramming **E**rror	Can install when convenient. Fixes minor problems.

FIRMWARE MAINTENANCE CONSIDERATIONS

Firmware Release Schedules

IBM plans to make new functions available via Firmware Releases no more than twice yearly. These releases will be scheduled approximately six months apart. Each new release will be supported with service packs for a period of one year after its initial availability date. Service Packs will be released quarterly, or as required. Early versions of CFM required that all deferred fixes be cleared with an IPL prior to downloading an additional release which suggested four outages per year. Subsequent releases allow a System p environment to plan for fewer IPL's but most customers will still advertise a 'maintenance event' that is negotiated with their business units that share a machine image. Again, cluster technology permits rolling upgrades that limit downtime to the failover window.

It is highly recommended that all customers sign up for the firmware subscription service. This service will provide notification whenever new Firmware Releases and Service Packs become available. Subscriptions can be customized to provide only the information that is relevant to your business environment. This is the IBM recommended method for an administrator to be automatically notified of critical fixes in a timely fashion.

Go to https://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd to sign up for this service.

Another general rule for upgrading firmware is to avoid other maintenance activities during a CFM update. Complete the CFM update successfully prior to starting subsequent maintenance. The CFM design supports updating firmware without stopping partitions, it does not support updating firmware and performing other platform maintenance operations at the same -- it should be the only maintenance activity on the system while it is running. This includes any hardware maintenance operations from the HMC as well as any Capacity Upgrade on Demand (CoD) actions or dynamic reconfiguration (DLPAR) actions. It is recommended that no partitions be activated or ended during the CFM operation. The code update readiness checker can and *should* be run prior to starting an update if you are on V5R1 or newer HMC. This will be discussed further under managing firmware with an HMC.

Firmware *Releases* add new function that may not be initially required, as well as fixes to problems that may not be applicable to your environment. While there is no immediate need to upgrade to these new releases, it is a good practice to plan a disruptive upgrade to a new release at least once per year, with concurrent updates to service packs within your current release recommended quarterly.

Managing Firmware with an HMC

If a system is HMC-managed, you will use the HMC for firmware updates. Using the HMC allows you to take advantage of the concurrent firmware maintenance option when concurrent service packs are available.

With the introduction of CFM, IBM is significantly increasing a client's opportunity to stay on a given release level for longer periods of time. This allows clients that want maximum stability to stay on the same release level (e.g., 2.3.0) until there is a compelling reason to upgrade such as:

- A release level is approaching its end-of-service date (i.e., has been available for about a year and hence will go out of service support soon).
- Moving a system to a more standardized release level when there are multiple systems in an environment with similar hardware.
- A new release has new function that is needed in the environment.
- A scheduled maintenance action will cause a platform reboot. This provides an opportunity to also upgrade to a new firmware release.

The general rule is that the HMC code level must be equal to or greater than the firmware release level installed on the server. When upgrading the HMC firmware, it is important to note that all systems attached to and served by an HMC should be evaluated for firmware co-requisites and pre-requisites. Before upgrading firmware on an HMC controlled server to a new release, check the POWER5™ code matrix at:

http://www14.software.ibm.com/webapp/set2/sas/f/power5cm/home.html

The matrix will identify the appropriate HMC level required to support the server firmware being installed. When planning to upgrade the system firmware to a new release, ensure that the HMC code is upgraded prior to doing the system firmware upgrade.

By scheduling regular maintenance intervals, the number of fixes that must be installed at any one time is minimized and therefore risk is also minimized. It is good practice to install concurrent service packs regularly. IBM suggests quarterly updates at a minimum.

The content of any service pack, especially those that would result in a disruptive install (non-concurrent) should be examined to determine applicability to a given environment. The README(s) or XML file(s) can be examined to determine whether or not the problems addressed would impact your system. IBM releases disruptive service packs only when it is absolutely necessary to fix specific problems; therefore, if one of these fixes in the service pack affects your system, it is strongly advised to schedule a maintenance window at the earliest opportunity install the fixes. Every service pack has a corresponding

README file (also known as the "XML" file) that describes the service pack contents. Disruptive fixes are listed first, and these disruptive changes should be examined closely to see whether your system requires any of them.

If it is necessary to install a disruptive service pack consider whether a new release is available that also contains the fix. If the service pack is disruptive and a new release is available that contains the fix, upgrading to the most recent and most comprehensive level may be advisable to minimize downtime. IBM will release a Fix Level Recommendation Tool (FLRT) late in 2006 that will provide more comprehensive information about available fixes, number of downloads, and availability dates.

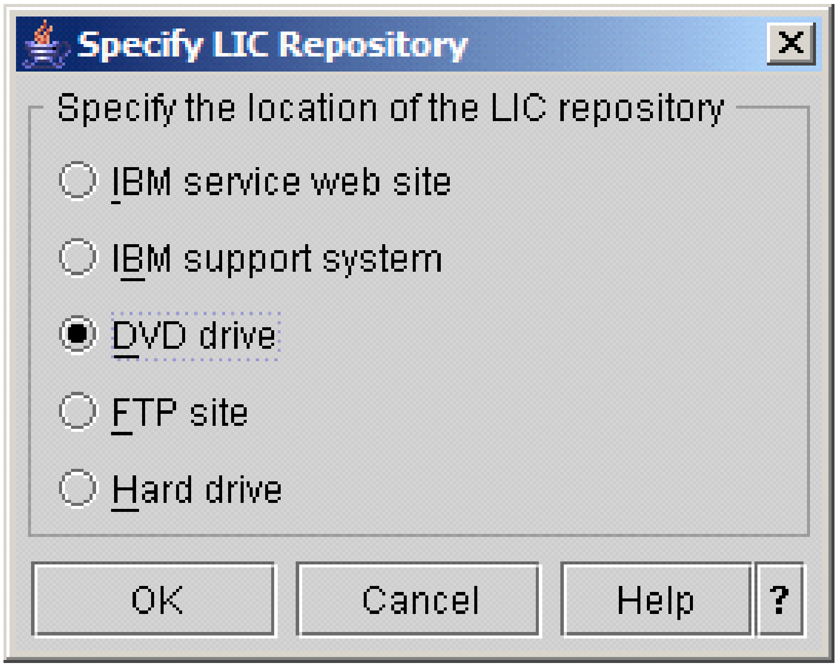
If the firmware is being downloaded from a remote repository, for best performance during the firmware installation, you should first download the latest firmware levels to the Service Repository located on your HMC. Then, the firmware may be installed from the HMC hard drive. Note: All outstanding deferred fixes had to be cleared prior to additional downloads on early SF230 (GA5) release which is no longer a requirement.

Running Code Update Readiness Checker in advance

The Code Update Readiness Checker is a feature in the V5R1 or newer HMC that can uncover errors which do not affect normal system operation but which will prevent a code update from being successful. Any such error must be resolved prior to performing the code update. This is especially important for models with have redundant FSP or have a BPC power controller (models 575, 590 and 595). This pertains both to installing service packs within a release or upgrading to a new release. We recommend that you run readiness checker one week in advance of the code update to allow time to resolve errors if they are found.

The Code Update Readiness Checker runs as part of the code update process and at this time there is no option to run a stand-alone mode. It can be run without performing a code update by going to the Licensed Internal Code Updates menu and then taking the following options.

- Change Licensed Internal Code for Current Release
- Select target
- Start Change Licensed Internal Code Wizard
- If you reach “Specify LIC Repository” panel, the readiness checker has passed – select Cancel to abort



Specify LIC Repository

Specify the location of the LIC repository

○ IBM service web site

○ IBM support system

● DVD drive

○ FTP site

○ Hard drive

FIRMWARE MAINTENANCE: USER SCENARIOS

IBM has developed a variety of tools and procedures to help you in understanding the state of your system's firmware. If your system is internet connected, we offer a firmware management utility that will survey your system, check for available updates and offer the option to have the utility download new firmware from the web and update your systems. This is all done without sending any of your systems data to IBM. Using the HMC to update your system firmware provides you with the best evaluation tools to aid in maintenance decisions.

IBM also offers tools and techniques for customers who choose to isolate their systems from the internet due to security concerns and for systems that are not HMC controlled.

The tools provided by IBM are detailed in the following section. Each one fits a different environment. Carefully evaluate the offerings outlined below, and select the set of tools and techniques that best fits your operating environment.

The following sections will detail firmware maintenance scenarios for several options:

- Maintaining Firmware on HMC controlled System p5
- Non-HMC controlled AIX Systems
- Considerations for Internet connected systems
- Considerations for systems which are not connected to the Internet

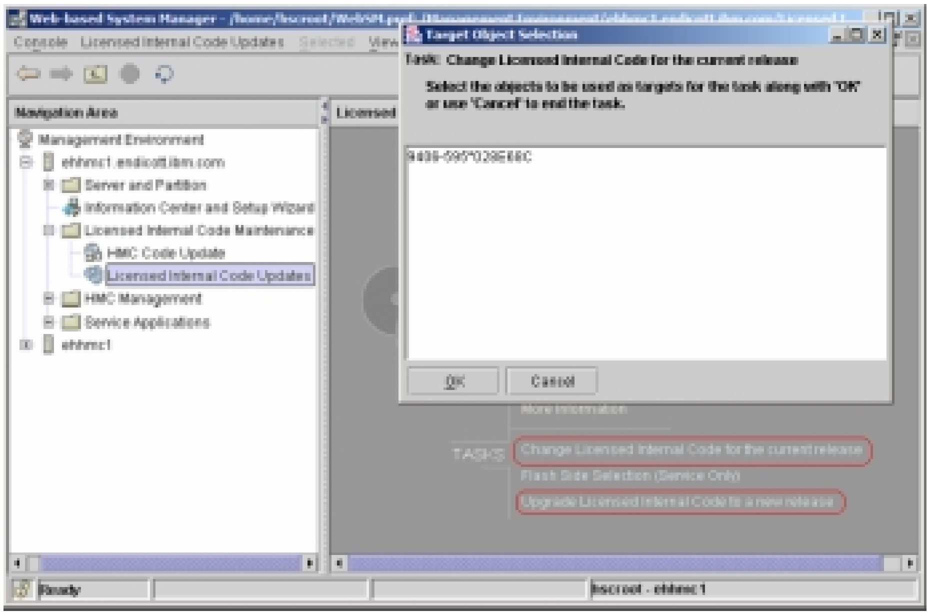
Maintaining Firmware on HMC Controlled System P5

The HMC may be utilized to determine the level of system firmware currently installed on a system. On the left side of the HMC main menu (Figure 1), systems managed by the HMC will be shown.

Expand the Licensed Internal Code Maintenance option and click on Licensed Internal Code Updates.

The *Licensed Internal Code Updates* menu supports Service Pack updates via the *Licensed Internal Code for the current release* option.

The *Licensed Internal Code Updates* menu supports the installation of release upgrades via *Upgrade Licensed Internal Code to a new release* option.



Task: Change Licensed Internal Code for the current release

Select the objects to be used as targets for the task along with 'OK' or use 'Cancel' to end the task.

9406-595*0286E6C

Web-based System Manager - /home/hscroot/WebSM.pref: /Management Environment/ehhmc1.endicott.ibm.com/Licensed I
Console
Licensed Internal Code Updates
Selected
View
Navigation Area
Management Environment
ehhmc1.endicott.ibm.com
Server and Partition
Information Center and Setup Wizard
Licensed Internal Code Maintenance
HMC Code Update
Licensed Internal Code Updates
HMC Management
Service Applications
ehhmc1
Licensed
Target Object Selection
OK
Cancel
More Information
TASKS
Change Licensed Internal Code for the current release
Flash Side Selection (Service Only)
Upgrade Licensed Internal Code to a new release
Ready
hscroot - ehhmc1

Figure 1: Perform Licensed Internal Code installation via the HMC.

The Microcode downloads Web page is an excellent resource for information about firmware fixes (such as current firmware levels, service pack cover letters, etc). Additionally, it is useful to review the Hardware Management Console Support page at http://www14.software.ibm.com/webapp/set2/firmware/gjsn for the latest information on HMC fixes and releases.

Again, it is advisable to run the Code Update Readiness Checker in advance as documented above under Managing Firmware with and HMC. This is available after V5R1 and can uncover errors which do not affect normal system operation but which will prevent a code update from being successful. Any such error must be resolved prior to performing the code update.

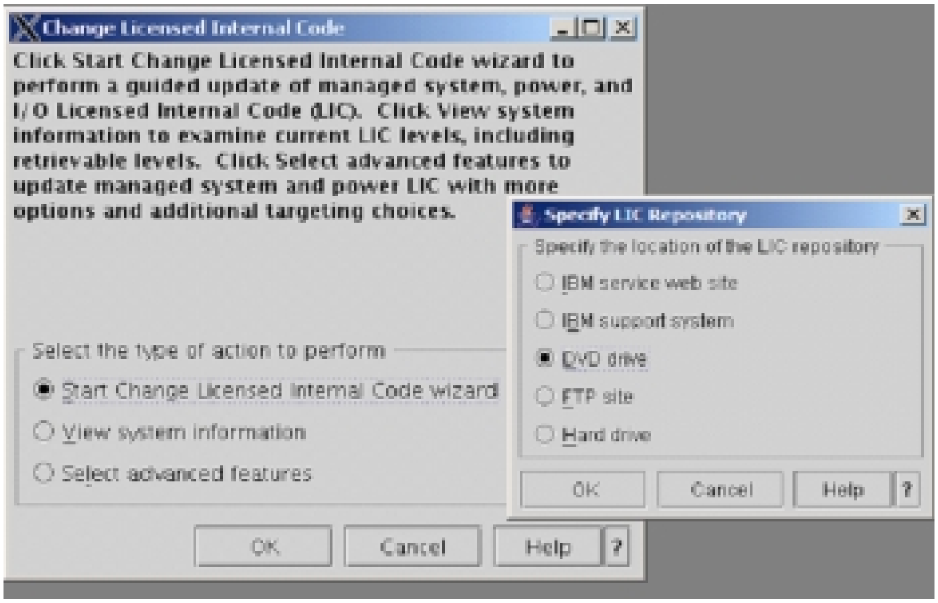
Installing a Service Pack via the HMC

When you choose to install a service pack, a "target object" must be selected. Typically, this target object is the system that will be the object of the firmware installation.

Select the system or systems that the firmware is to be installed on and click on OK. (A message may be displayed directing you to wait while system information is being retrieved.)

Three options are then given (Figure 2):

- To install the firmware update via the wizard
- To view system information
- To use advanced firmware installation features



Click Start Change Licensed Internal Code wizard to perform a guided update of managed system, power, and I/O Licensed Internal Code (LIC). Click View system information to examine current LIC levels, including retrievable levels. Click Select advanced features to update managed system and power LIC with more options and additional targeting choices.

Select the type of action to perform

● Start Change Licensed Internal Code wizard
○ View system information
○ Select advanced features

Specify the location of the LIC repository

○ IBM service web site
○ IBM support system
● DVD drive
○ FTP site
○ Hard drive

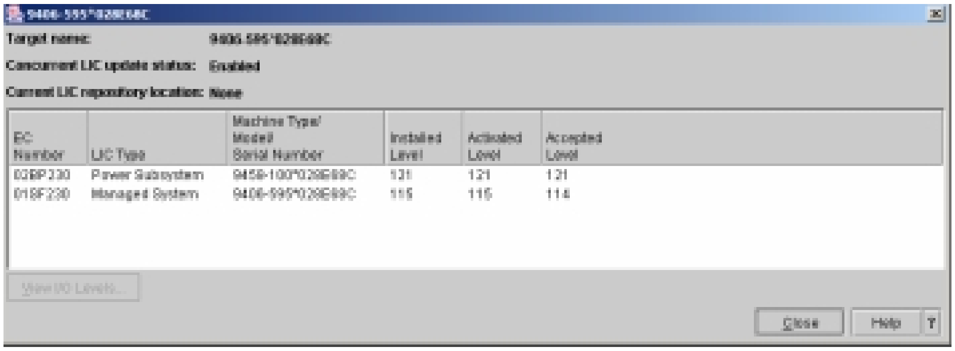
Figure 2: Change Licensed Internal Code for the current Release

The option to view system information allows you to see what has been installed and activated on the managed system. It also allows you to view what is available in the LIC (Service) repository (location of the firmware to be installed) and to determine what can be activated concurrently based on the existing activated level.

In reviewing the system firmware information (Figures 3a and 3b), the following information should be understood.

- ✓ The *installed level* is the highest level of code on the system. This code may or may not have been activated (i.e., loaded into memory).
- ✓ The *activated level* is the code level that the system is currently running; it's usually on the t-side flash.
- ✓ The *accepted level* is the lowest level of code on the system; it's usually on the p-side flash.

If you specified a repository for firmware fixes, you'll also see information regarding concurrent and disruptive service packs. The Retrievable Disruptive Activate Level designates the highest code level in the service repository. This code, if installed would result in a disruptive firmware update (i.e., you'll need to shut down all partitions and either turn the system off or put it in standby mode). Likewise, the Retrievable Concurrent Activate Level is the highest code level available in the repository location that can be retrieved, installed, and activated without a disruption.



9406-595*028E69C

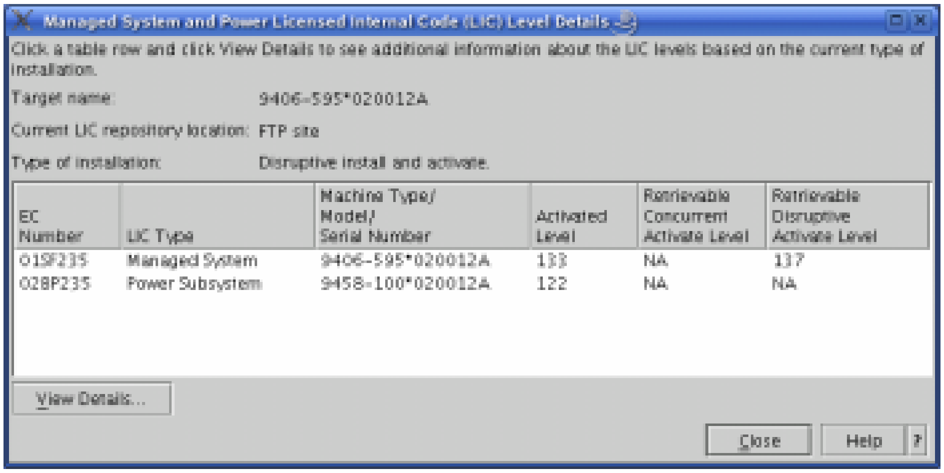
Target name: 9406-595*028E69C

Concurrent LIC update status: Enabled

Current LIC repository location: None

EC Number	LIC Type	Machine Type/ Model/ Serial Number	Installed Level	Activated Level	Accepted Level
028P230	Power Subsystem	9458-100*028E69C	121	121	121
01SF230	Managed System	9406-595*028E69C	115	115	114

Figure 3a: Check your installed, activated, and accepted code levels. (Note any deferred fixes as they may prevent downloads until an IPL is performed).



Managed System and Power Licensed Internal Code (LIC) Level Details

Click a table row and click View Details to see additional information about the LIC levels based on the current type of installation.

Target name: 9406-595*020012A

Current LIC repository location: FTP site

Type of installation: Disruptive install and activate.

EC Number	LIC Type	Machine Type/ Model/ Serial Number	Activated Level	Retrievable Concurrent Activate Level	Retrievable Disruptive Activate Level
01SF235	Managed System	9406-595*020012A	133	NA	137
028P235	Power Subsystem	9458-100*020012A	122	NA	NA

Figure 3b: Check the status of your Licensed Internal Code.

Installing Firmware Service Packs via the HMC Wizard

The *Start Change Licensed Internal Code Wizard* option is the simplest way to install firmware service packs. It installs the latest level and automatically accepts the previously activated level or moves the previous level of fixes from the t-side to the p-side flash.

The wizard prompts for the location of the Service Pack (Figure 3).

This is followed by 2 additional prompts, click *Next* at both of these prompts.

The first prompt is a notification that a firmware update is being attempted, and that if no Service Packs are in the firmware repository, nothing will happen and no further prompts will be shown. Click *next* at this prompt.

The second prompt identifies whether the firmware update will be concurrent, disruptive, or deferred. It also gives provides the option of changing the installation method to the advanced procedure. Click *next* at this prompt

The wizard will also tell you whether you are already at the latest Service Pack level (i.e., no firmware update required) and whether a new release level of firmware is available (in case you would prefer to cancel the Service Pack update and instead perform a disruptive release upgrade).

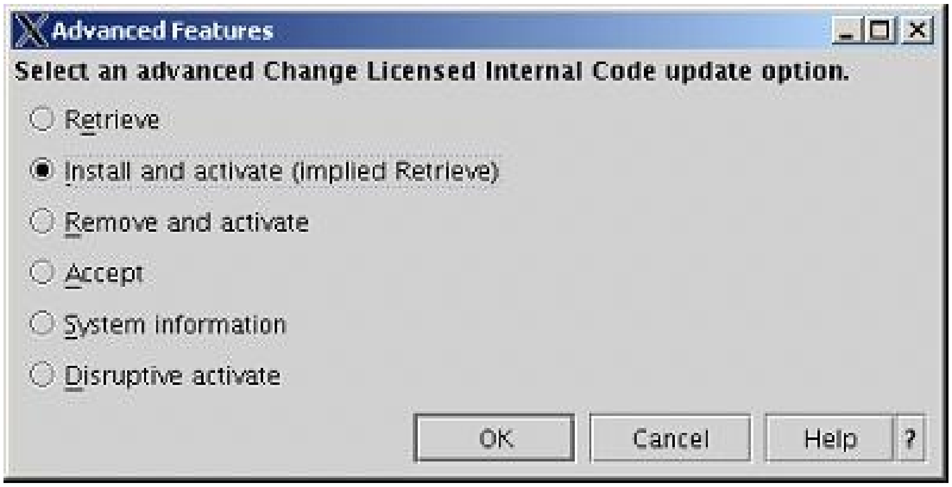
Lastly, you'll be shown a confirmation menu (Figure 6). Note that on the confirmation screen, both managed system and power subsystem updates are available. The power subsystem updates (if required for your system) will be installed first. Then system firmware updates will be installed. A failure in the power subsystem update will stop the update process, and the managed system firmware update will not occur.

Installing Service Packs via the HMC Advanced Option

To start the system firmware installation, Select the Licensed Internal Code Updates option under the Licensed Internal Code Maintenance tree (Figure 1).

Select the target of the firmware update (i.e., your system) and click on OK.

At the *Change Licensed Internal Code* menu, choose the *Select Advanced Features* option. This option allows you to perform the individual parts of the installation processes (such as install and activate a service pack and accept a service pack). It also allows you to remove a service pack and activate the previous level (this means copy the p-side flash over to the t-side flash and reload memory with this level) and to download service packs from the IBM repository onto a DVD or the hard drive of the HMC (Figure 4). The option for system information is identical to that of the View System Information option previously discussed.



Select an advanced Change Licensed Internal Code update option.

○ Retrieve
● Install and activate (implied Retrieve)
○ Remove and activate
○ Accept
○ System information
○ Disruptive activate

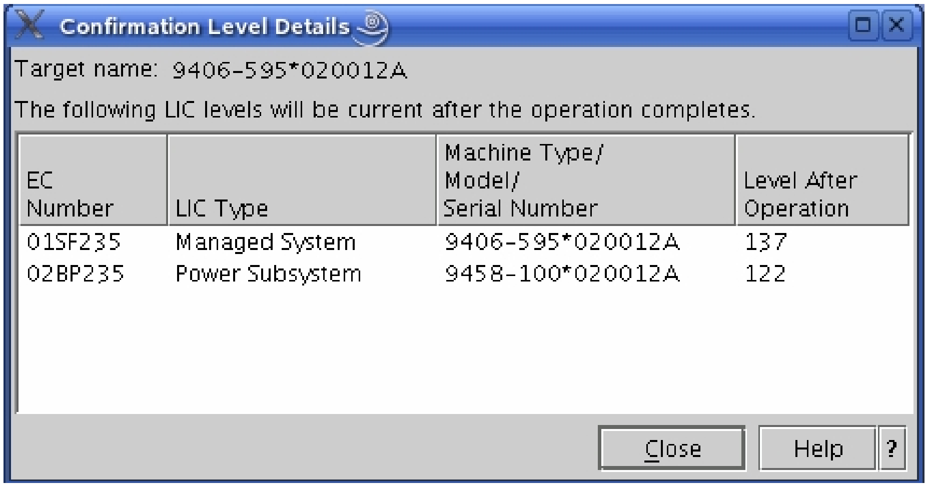
Figure 4: Take advantage of the HMC's advanced features.

If you want to install fixes, select *Install and Activate* (implied Retrieve). In addition to being asked where your service pack is located, 3 options are given:

- install the latest concurrent service pack,
- install the latest service pack (even if disruptive),
- install a specific level of service pack.

The option to move the t-side code over to the p-side, prior to the installation is also offered.

If you select to specify LIC levels, you'll be shown the Specify LIC Levels screen (Figure 5). From this screen, you can choose whether to view the available levels or to specify the level that you want to install.



Target name: 9406-595*020012A

The following LIC levels will be current after the operation completes.

EC Number	LIC Type	Machine Type/ Model/ Serial Number	Level After Operation
01SF235	Managed System	9406-595*020012A	137
02BP235	Power Subsystem	9458-100*020012A	122

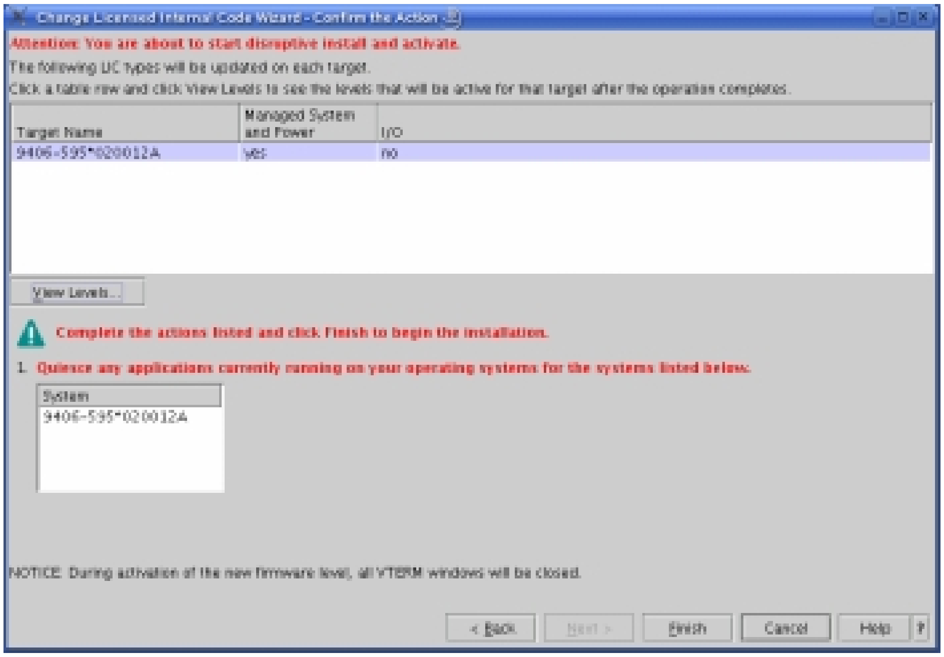
Figure 5: Specify LIC levels.

When you click OK from the Specify LIC Levels screen, you'll be told what type of install (concurrent or disruptive) this update will be.

In addition, you'll be given the option to perform a concurrent install (with deferred disruptive activate) or a disruptive install and activate.

If the type of update is disruptive, then the install selection should be disruptive "install and activate."

You'll be given a confirmation menu (Figure 6) that provides information about the type of install (disruptive or concurrent) and information about the systems to be updated and the firmware levels to be installed.



Change Licensed Internal Code Wizard - Confirm the Action

Attention: You are about to start disruptive install and activate.

The following LIC types will be updated on each target.

Click a table row and click View Levels to see the levels that will be active for that target after the operation completes.

Target Name	Managed System and Power	I/O
9406-595*020012A	yes	no

Complete the actions listed and click Finish to begin the installation.

1. Quiesce any applications currently running on your operating systems for the systems listed below.

System
9406-595*020012A

NOTICE: During activation of the new firmware level, all VTERM windows will be closed.

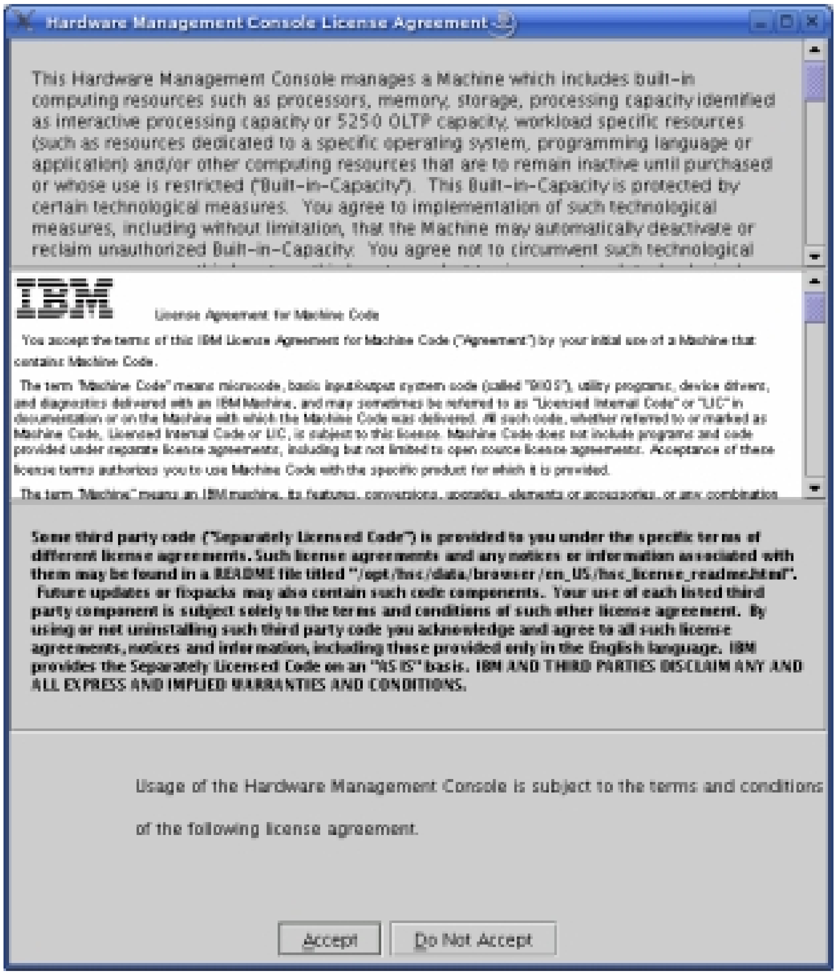
Figure 6: Confirm the action.

Upgrading to a New Release Level

Starting from the panel called Licensed Internal Code Installation via the HMC, select Update Licensed Internal Code to a New Release.

The next steps will be nearly the same as the Change Licensed Internal Code path. Target selection and repository selection are just as described above in the section titled ***Installing a Service Pack via the HMC***

The first difference when upgrading to a new release level (as opposed to updating within a release) is that you must accept the license for the new firmware (Figure 7).



This Hardware Management Console manages a Machine which includes built-in computing resources such as processors, memory, storage, processing capacity identified as interactive processing capacity or 5250 OLTP capacity, workload specific resources (such as resources dedicated to a specific operating system, programming language or application) and/or other computing resources that are to remain inactive until purchased or whose use is restricted ("Built-in-Capacity"). This Built-in-Capacity is protected by certain technological measures. You agree to implementation of such technological measures, including without limitation, that the Machine may automatically deactivate or reclaim unauthorized Built-in-Capacity. You agree not to circumvent such technological

IBM License Agreement for Machine Code

You accept the terms of this IBM License Agreement for Machine Code ("Agreement") by your initial use of a Machine that contains Machine Code.

The term "Machine Code" means microcode, basic input/output system code (called "BIOS"), utility programs, device drivers, and diagnostics delivered with an IBM Machine, and may sometimes be referred to as "Licensed Internal Code" or "LIC" in documentation or on the Machine with which the Machine Code was delivered. All such code, whether referred to or marked as Machine Code, Licensed Internal Code or LIC, is subject to this license. Machine Code does not include programs and code provided under separate license agreements, including but not limited to open source license agreements. Acceptance of these license terms authorizes you to use Machine Code with the specific product for which it is provided.

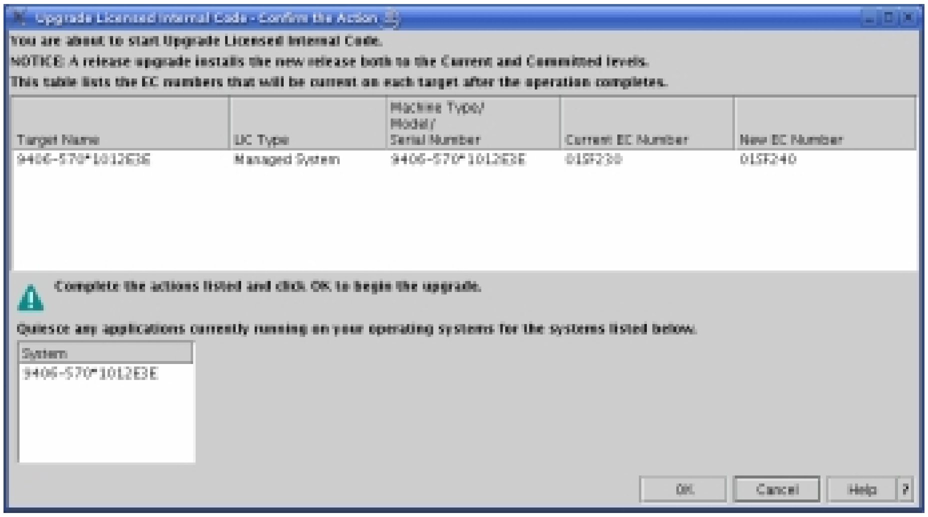
The term "Machine" means an IBM machine, its features, conversions, upgrades, elements or accessories, or any combination

Some third party code ("Separately Licensed Code") is provided to you under the specific terms of different license agreements. Such license agreements and any notices or information associated with them may be found in a README file titled "/opt/hsc/data/browser/en_US/hsc_license_readme.html". Future updates or fixpacks may also contain such code components. Your use of each listed third party component is subject solely to the terms and conditions of such other license agreement. By using or not uninstalling such third party code you acknowledge and agree to all such license agreements, notices and information, including those provided only in the English language. IBM provides the Separately Licensed Code on an "AS IS" basis. IBM AND THIRD PARTIES DISCLAIM ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS.

Usage of the Hardware Management Console is subject to the terms and conditions of the following license agreement.

Figure 7: Accept the license for the new firmware.

After accepting the license, a panel will show which firmware components will be updated and which firmware levels will be installed (Figure 8). When you press OK on this panel, the installation will begin, and a progress panel will be shown.



You are about to start Upgrade Licensed Internal Code.
NOTICE: A release upgrade installs the new release both to the Current and Committed levels.
This table lists the EC numbers that will be current on each target after the operation completes.

Target Name	LIC Type	Machine Type/ Model/ Serial Number	Current EC Number	New EC Number
9406-570*1012E3E	Managed System	9406-570*1012E3E	01SF230	01SF240

Complete the actions listed and click OK to begin the upgrade.

Quiesce any applications currently running on your operating systems for the systems listed below.

System
9406-570*1012E3E

Figure 8: Confirm the action.

Key information relevant to Upgrading Firmware to a new release in an HMC controlled system.

- The HMC must be upgraded to the new release level before updating any system firmware components to the new release.
- As described above, an upgrade to a new release is always disruptive, so there will be no option to do this concurrently; therefore, it's important to plan for a maintenance window when you can perform a deep IPL.
- A release upgrade automatically performs the "accept" step as well, so at the end of the upgrade, both the temporary and permanent flash sides will be at the new release.
- If your system has Bulk Power Control (BPC) firmware (models 575, 590 and 595 only) both the BPC and the system firmware will be updated to the new release; it is not an option to have the components at different release levels.

Additional Options
The following sections will attempt to clarify the additional options available for firmware maintenance. These sections will cover accessing the firmware and firmware management tools

Tools for Managing Firmware if Internet Connected

The internet offers easy access to newly available firmware releases and service packs in real time. The firmware management tools can locate, download, and install the latest firmware from the internet with minimal user interaction. This can be done remotely from the system.

Note: Currently, this option can only be used for upgrading firmware on the following:

- Non-HMC controlled machines
- HMC Controlled machines where the system is to be upgraded to the latest Release level
- It can not be used to upgrade an HMC controlled system to an interim release level or to update an HMC controlled system to a new service pack within the installed release. Enhancements are being developed to allow this to be done in a future release.
- To upgrade an HMC Controlled machine to an interim release level or to update to a new service pack within the current release level, obtain the .iso image for the desired level from the Firmware Website and create a CD containing only that image. Upgrade or update using that CD.
- The .iso image can be obtained from http://www14.software.ibm.com/webapp/set2/firmware/gjsn?mode=10&page=cdrom.html

Internet Firmware Evaluation

Firmware management utility, available as an optional installable Web-based System Manager feature on AIX, and a standard feature on HMC's.

Note: Currently, this option can only be used for upgrading firmware on the following:

- Non-HMC controlled machines, where all firmware actions are disruptive
- HMC Controlled machines where the system is to be upgraded to the latest Release level

It can not be used to upgrade an HMC controlled system to an interim release level or to update an HMC controlled system to a new service pack within the installed release. Enhancements are being developed to allow this to be done in a future release.

- To upgrade an HMC Controlled machine to an interim release level or to update to a new service pack within the current release level, obtain the .iso image for the desired level from the Firmware Website and create a CD containing only that image. Upgrade or update using that CD.
- The .iso image can be obtained from http://www14.software.ibm.com/webapp/set2/firmware/gjsn?mode=10&page=cdrom.html

MDSapplet can quickly survey your system and give you the current state of the firmware installed, with links to documentation and firmware when applicable.

Tools for Maintaining if Not Connected to Internet

IBM has provided a set of tools and techniques to help manage your system in this environment.

The available options without a direct internet connection are:

- **System p Firmware CD.** This CD effectively replaces the need for an internet connection. It can be used by the firmware management utilities, allowing all survey/ update/ apply operations to be done on the local machine.

Note: Currently, this option can only be used for upgrading firmware on the following:

- Non-HMC controlled machines
- HMC Controlled machines where the system is to be upgraded to the latest Release level

It can not be used to upgrade an HMC controlled system to an interim release level or to update an HMC controlled system to a new service pack within the installed release. Enhancements are being developed to allow this to be done in a future release.

- To upgrade an HMC Controlled machine to an interim release level or to update to a new service pack within the current release level, obtain the .iso image for the desired level from the Firmware Website and create a CD containing only that image. Upgrade or update using that CD.
- The .iso image can be obtained from http://www14.software.ibm.com/webapp/set2/firmware/gjsn?mode=10&page=cdrom.html

<u>MDSApplet</u>

- Using a single machine connected to the internet, the **MDSapplet** can be run against systems to provide a survey of current machine state. This requires that your systems are running the invscoutd daemon and have a password set for the invscout userid.
- In cases where running the invscoutd daemon is not desirable, the latest catalog of available firmware can be downloaded, copied to the managed systems, and

executed via the command line invocation of invscout. The /var/adm/invscout/<hostname>.mup file is then retrieved and uploaded where the results are displayed

- Users can also go to the microcode internet site, find update for their machines download and apply the firmware.

Another option is to go to the microcode internet site, locate the .iso image for the System p5 system firmware needed and create a CD that can be used to install and apply the firmware to the target system.

Non-HMC controlled AIX Systems

Multiple options exist for users to manage a System p system that is not HMC controlled.

1. The **Microcode management web-based system manager application** can be installed from the AIX installations CDs. With this application installed, the user can start web-based system manager and select the microcode update Icon. The system will be surveyed using data from www.ibm.com® if internet connected or from the firmware CD if no direct internet connection is feasible.

2. The **MDSapplet** can be used to survey the system if internet connected. This will allow you to check the state of your system's firmware components. The user will be presented with pointers to documentation regarding available updates, and will be given the option to download updates to the system.

   The MDSapplet requires the invscoutd daemon be started and a password created for the user invscout on the target system(s).

3. The firmware CD is the simplest method for upgrading systems that can not access the internet. Once the firmware CD has been obtained or the image has been downloaded and the CD burned, the user has two options:

   o- If running AIX 5.2-ML3 or AIX 5.3 and the user can identify the devices that are down level, AIX diag microcode download service aids can be used to update these devices, specifying the firmware CD as the location of the updates.

   o- The firmware CD also contains a wizard like application that will analyze and guide you through the tools available to assist you, based on the environment it detects on your system.

Obtaining Firmware Updates: Resources

Current firmware for System p systems may be viewed online on the System p microcode website: http://www14.software.ibm.com/webapp/set2/firmware/gjsn. This website contains the system firmware and bulk power code for all System p products.

Navigating the IBM System p Microcode website

Finding the latest levels of firmware available for your systems requires that you understand your system configuration. This section provides instruction on manually determining this information. The sections that follow explain the use of tools that can automate this process for you, thereby simplifying the task of manually identifying the firmware packages applicable to your system(s).

If you do not know the Machine Type and Model of the target system, you can get this information from the system by typing **uname –M** on the command line. Make a note of the value that is returned from this command, and use that value as a reference when reviewing the information on the website.

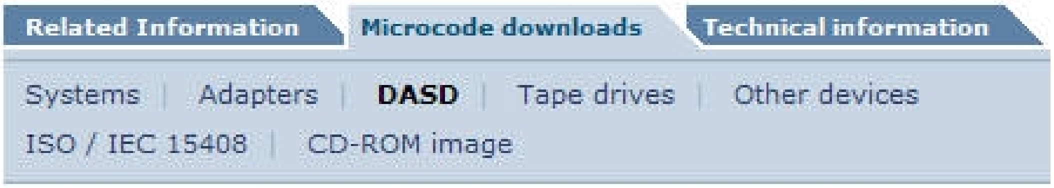
To find out what level of system firmware is currently installed on your system, type **lsmcode –d sys0** on the command line.

Adapters and Device microcode

While this document focuses primarily on the server firmware, the microcode for devices and adapters can also be found at this site. If you determine that an update is available, you can download the newest adapter microcode images, and install them on your system.

Identifying new firmware for adapters and devices requires a bit more system knowledge. There are adapters, DASD, Tape Drives, and other devices (i.e. CD or DVD drives).

Adapters and Devices are organized using separate tabs on within the website



You can determine the devices on your system which utilize firmware by issuing the command lsmcode –A.

This command lists all devices that have diagnostic services to manage microcode.

Example:

```
lsmcode –A
sys0!system:SF230_126 (t) SF230_126 (p) SF230_126 (t)
ent0!14108902.DV0210
ent1!14108902.DV0210
sisscsia0!44415254.05080064
sisscsia1!44415254.05080064
ent2!14106902.GOL021
sisioa0!5052414E.030D0056
cd0!IBM-RMBO002050.H106
hdisk0!ST33675.53583133.433531
```

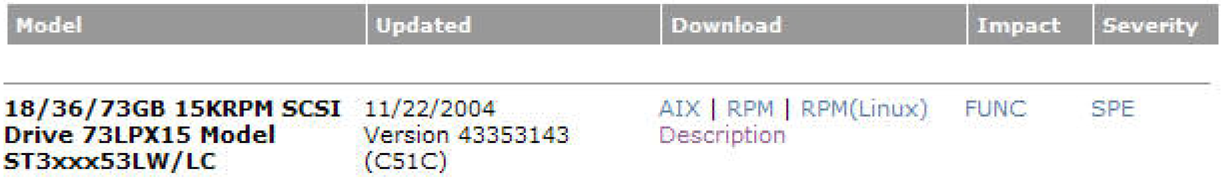
Detailed information about a specific device can be surfaced by using the lscfg command.

Ex:

```
lscfg -vl hdisk0
  hdisk0          U0.1-P1/Z1-A4  16 Bit LVD SCSI Disk Drive (4500 MB)

        Manufacturer................IBM
        Machine Type and Model......DDRS-34560D
        FRU Number..................83H7105
        ROS Level and ID............44433247
        Serial Number...............RDHG2745
        EC Level....................F21977
        Part Number.................22L0352
        Device Specific.(Z0)........000002029F00003A
        Device Specific.(Z1)........21L9832DC2G
        Device Specific.(Z2)........0933
        Device Specific.(Z3)........0199
        Device Specific.(Z4)........0001
        Device Specific.(Z5)........22
        Device Specific.(Z6)........F21420
```

Once you have identified the levels of microcode on your system, Locate the corresponding firmware package on the website



Model	Updated	Download	Impact	Severity
18/36/73GB 15KRPM SCSI Drive 73LPX15 Model ST3xxx53LW/LC	11/22/2004 Version 43353143 (C51C)	AIX | RPM | RPM(Linux) Description	FUNC	SPE

For each firmware entry on the website, there is a description field that links to the readme documentation, and one or more links to the firmware updates for downloading the code. This is provided in a variety of packaging formats.

The readme contains information about how to identify your device, the reasons for the new release of firmware, and instructions on how to update your system. Prior to updating any device, it is a good idea to print off a recent copy of these instructions.

The firmware is obtained by clicking on one of the download choices. The package you need depends on your preference and the environment you are operating in.

RPM The firmware is packaged in a format that will install on your AIX system and place the firmware files in the correct location for diag service aids to update the system component.   This should be your preferred method of getting individual firmware updates. It eliminates the multiple steps of making directories, unpacking files, moving files, etc. Using RPM's the typical sequence to update a device is:

```
rpm  -ihv – ingnoreos <rpm filename>
diag  -c –d <logical dev>  -T  “download –f –l latest”
```

RPM(Linux) This is similar to the AIX rpm file, but for systems/partitions running LINUX on the System p systems.

AIX This is a legacy format. It consists of a compressed self extracting executable. This format will typically require you to create directories and copy/move files to required destinations.

System p Firmware CD

The latest microcode updates for adapters and devices is contained on the System p firmware CD.

The firmware CD can be used by a multiple of applications

Note: Beginning with release 5200-03, AIX Diagnostics has the ability to read firmware directly from optical media devices. If you know the devices that are downlevel, you will:

- run the diag command,
- select task selection menu,
- select Microcode Task,
- select Download microcode
- select the devices to be updated and commit

The CD image also includes a Discovery Tool that compares microcode levels on your system to current levels and allows you to select and update to latest levels of microcode.

You can download this CD-ROM image from the microcode website and burn your own "Microcode Update Files & Discovery Tool CD-ROM". The image is in ISO 9660 format.

You may order the CD-ROM through the Delivery Service Center. This CD-ROM will also contain the "Microcode Update Files & Discovery Tool".

Note: CD-ROM updates are available as a downloadable image several days before they are available to be shipped on physical media. If you order CD-ROMs during this period, you will receive the older level of the CD-ROM microcode. When placing the order, you will be notified of the PTF level that will be shipped.

Managing Firmware : Tools

AIX Diagnostics: AIX Update System Flash Service aid

AIX provides a service aid to update system firmware for many systems. The update_flash service aid is available on most System p systems without HMC’s.

Warning: Updating the flash using this technique, will cause your system to reboot.

This utility can be accessed via the diagnostic menu’s:

Diag -> task selection -> Microcode Tasks -> Update System or Service Processor Flash

Select where you have the new flash image located, i.e Filesystem or device (CD or diskette)

i.e filesystem : /tmp/fwupdate/Newimage or you can select to have the file found on either the CD or diskette.

This command can also be performed from the command line for users who may want to develop remote procedures to copy out firmware files and execute commands to update the system.

```
/usr/lpp/diagnostics/bin/update_flash
Usage: update_flash [-q] -f file-name
       update_flash [-q] -D device-name -f file-name
       update_flash [-q] -D device-name –l
```

The command used to update your system is typically:
/usr/lpp/diagnostics/bin/./update_flash -f <path_to_fw>/firmware_filename>

AIX Download microcode Service Aids

AIX diagnostics also provides service aids to update adapters and devices. An option is available to selectively download a particular update for your system, and update the device using these diagnostics service aids.

The microcode files can be installed from the /etc/microcode directory, diskette in bff format, or CD. These service aids also have the ability to find and update the files using the System p Firmware~~,~~ available on the internet.

The diagnostic menu service aids can be found by entering

diag -> Task Selection -> Microcode Tasks -> Download Microcode

From here, select the devices to be updated based on the available updates. These updates can exist in /etc/microcode, CD or diskette

These tasks can be execute via the command line to allow the ability for remote operation, etc..

Diag –d <logical device to be updated> –T “download -l latest”

You can optionally use the –c option, no console mode, to automate your operation.

Inventory Scout

Inventory Scout provides a method to survey the microcode status of your system. The proper execution of a microcode survey requires that a current copy of the latest firmware levels available from IBM be copied to your system. The copying of this file to your system is automatically handled when using the newer of firmware management tools such as: web-based system manager microcode management, MDSapplet, and the Firmware CD discovery tool.

See command line usage below to understand how to do this without using IBM supplied utilities.

Command Line usage

First, a current catalog of available firmware needs to be obtained from IBM. This can be found by going to:

https://techsupport.services.ibm.com/server/mdownload//catalog.mic

and downloading the catalog.mic file. This file needs to be copied to /var/adm/invscout/microcode directory of the machine to be surveyed.

Invoke a survey with /usr/sbin/invscout

The results of the survey are put into a file /var/adm/invscout/<hostname>.mup

Currently this file can only be externally read by uploading the file to the MDSapplet. The applet is available at:
http://www14.software.ibm.com/webapp/set2/mds/fetch?page=mds.html

Invscoutd daemon

The invscoutd daemon is a much misunderstood feature. The daemon has two requirements on the systems that are to be managed by it.

1. It requires that the invscout userid have a password established for it.

2. The daemon needs to be started on the systems.

The invscout daemon opens a listening port (default: 808) waiting for an applet connection to request a survey. The applet will request a survey by first downloading the latest catalog.mic file, executing the survey, and sending the results of the survey back to the applet.

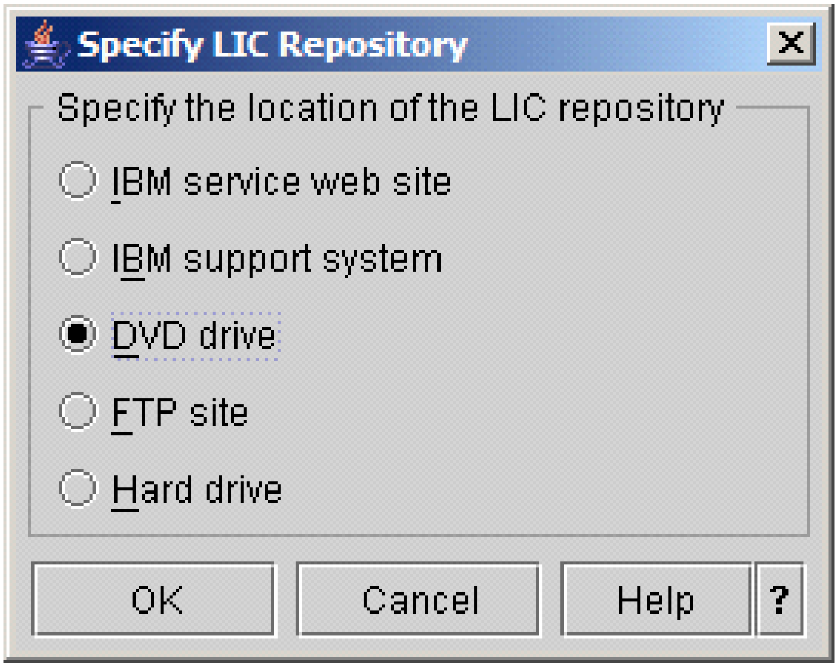
The security level of the userid and password is similar to telnet or ftp. Users requiring greater security are encouraged to copy the catalog.mic file out to system using local security procedure (scp, etc), and executing the command line invocation described in previous section.

Running Code Update Readiness Checker in advance

The Code Update Readiness Checker is a feature in the V5R1 or newer HMC that can uncover errors which do not affect normal system operation but which will prevent a code update from being successful. Any such error must be resolved prior to performing the code update. This is especially important for models with have redundant FSP or have a BPC power controller (models 575, 590 and 595). This pertains both to installing service packs within a release or upgrading to a new release. We recommend that you run readiness checker one week in advance of the code update to allow time to resolve errors if they are found.

The Code Update Readiness Checker runs as part of the code update process and at this time there is no option to run a stand-alone mode. It can be run without performing a code update by going to the Licensed Internal Code Updates menu and then taking the following options.

- Change Licensed Internal Code for Current Release
- Select target
- Start Change Licensed Internal Code Wizard
- If you reach "Specify LIC Repository" panel, the readiness checker has passed – select Cancel to abort



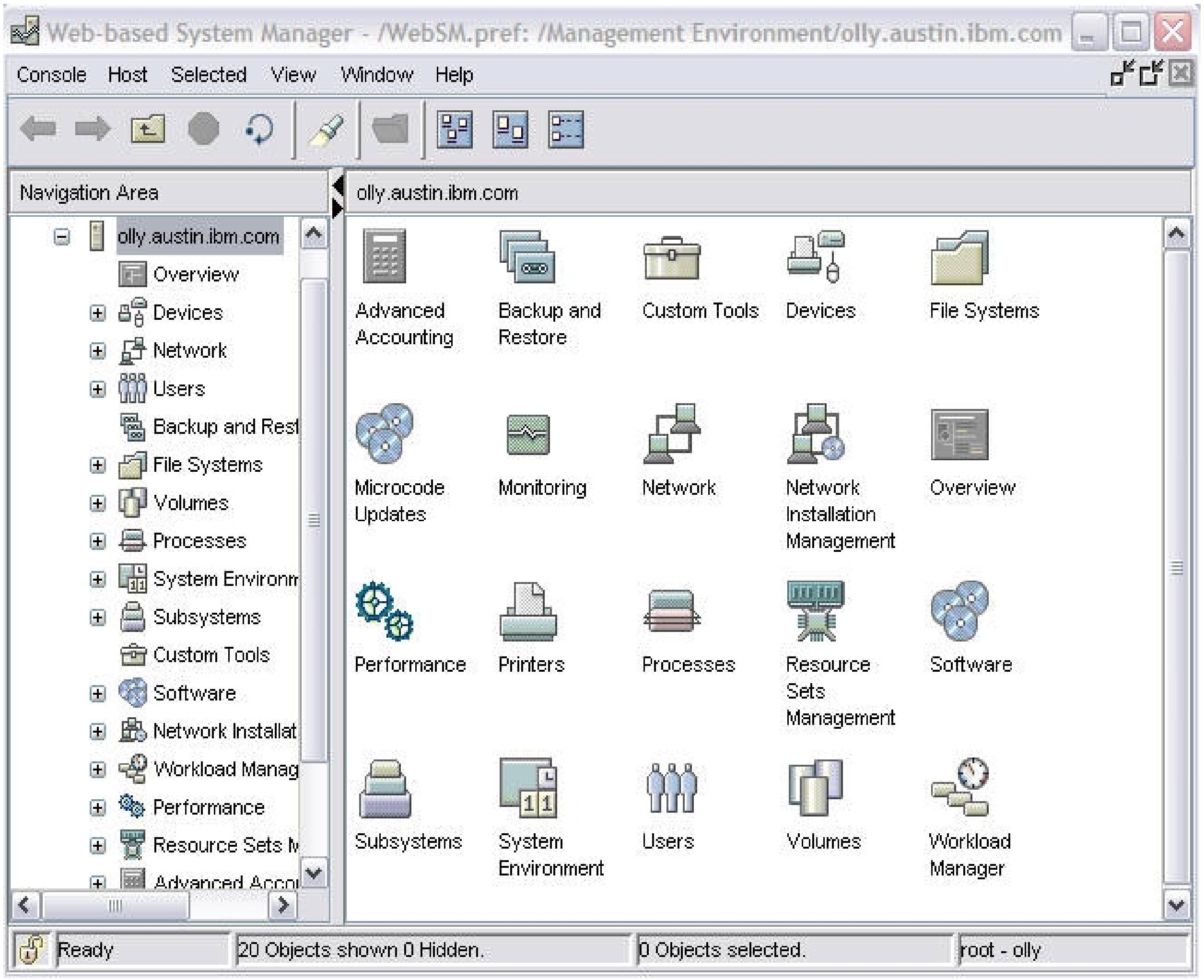
Specify LIC Repository

Specify the location of the LIC repository

○ IBM service web site
○ IBM support system
● DVD drive
○ FTP site
○ Hard drive

AIX Web-based system manager Microcode management

A web-based system manager GUI is provided to assist with maintaining your system's firmware. Installing the optional invscout.web-based system manager fileset onto your system, and then starting WebSM presents the user with a new icon "**Microcode Updates**".



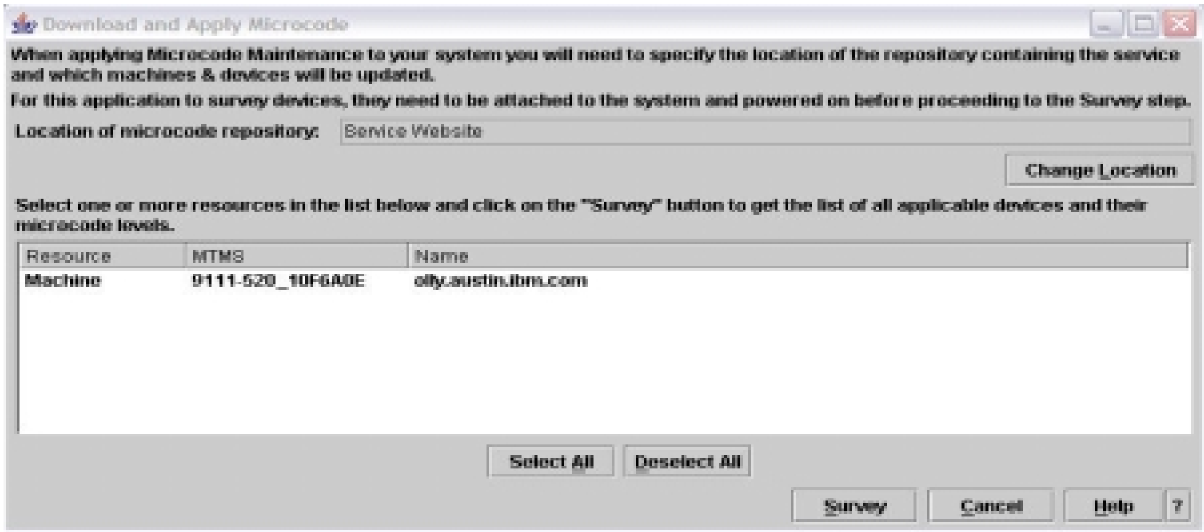
Ready

20 Objects shown 0 Hidden.

0 Objects selected.

root - olly

Clicking on the icon will bring up a selection panel.



When applying Microcode Maintenance to your system you will need to specify the location of the repository containing the service and which machines & devices will be updated.

For this application to survey devices, they need to be attached to the system and powered on before proceeding to the Survey step.

Location of microcode repository: Service Website

Select one or more resources in the list below and click on the "Survey" button to get the list of all applicable devices and their microcode levels.

Resource	MTMS	Name
Machine	9111-520_10F6A0E	olly.austin.ibm.com

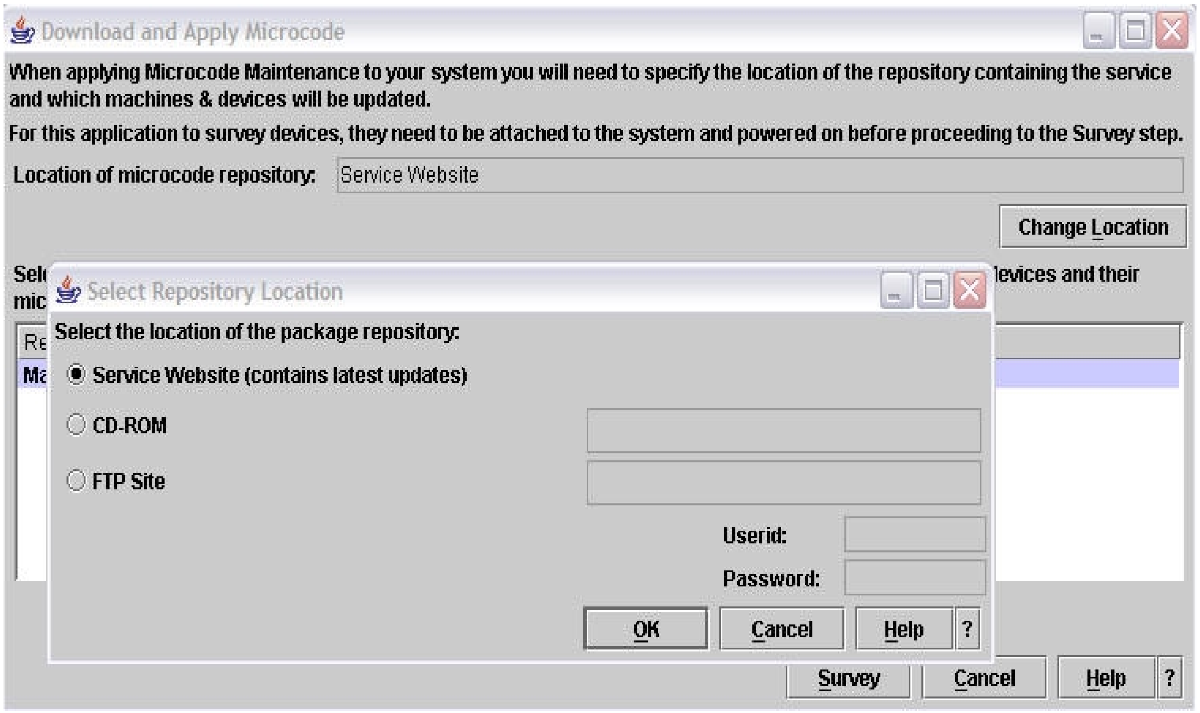
On a standalone server only a single system will be displayed. The user can select from the following survey sources, with internet being the default.

A) Internet

B) Firmware CD

To change from the internet default to ‘firmware CD’, Click on the “Change Location” button, then click OK.

Select machine, or ‘select all’ and click on the survey button.



When applying Microcode Maintenance to your system you will need to specify the location of the repository containing the service and which machines & devices will be updated.

For this application to survey devices, they need to be attached to the system and powered on before proceeding to the Survey step.

Location of microcode repository: Service Website

Select the location of the package repository:

● Service Website (contains latest updates)

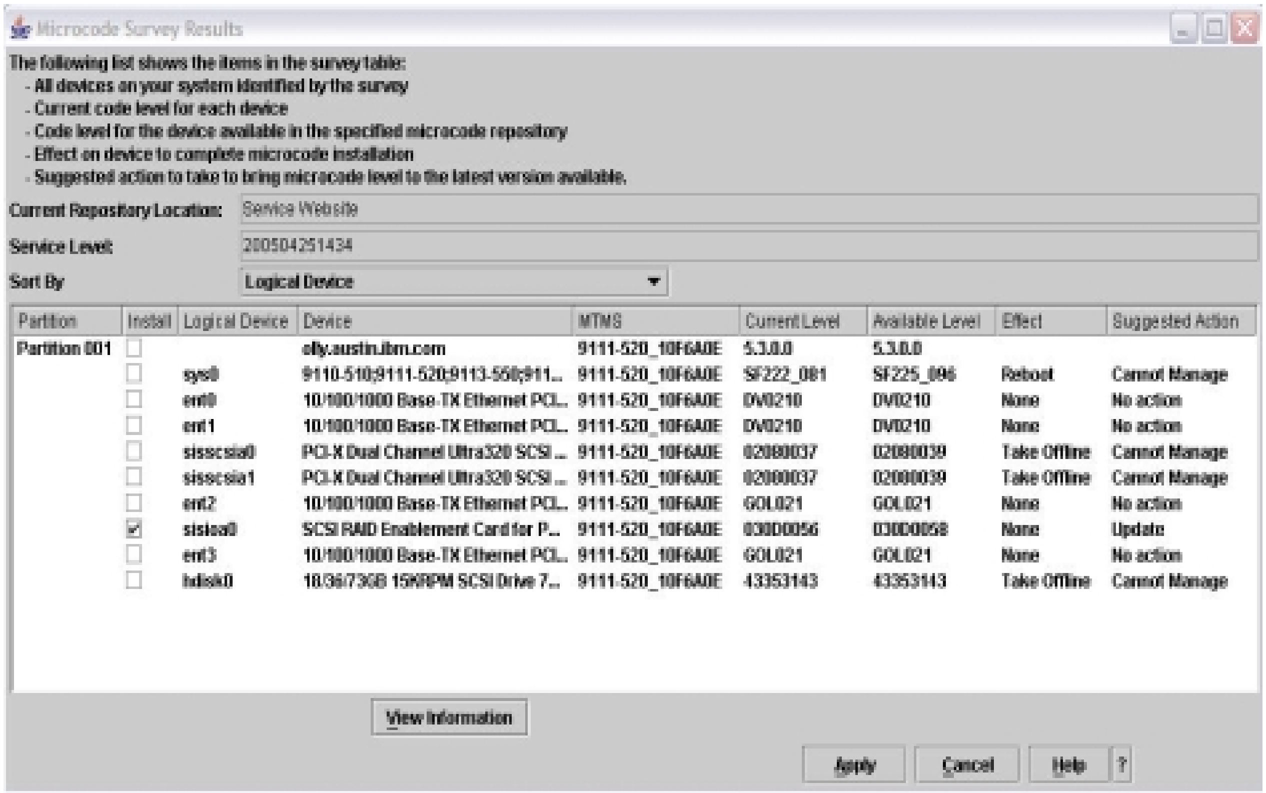
○ CD-ROM

○ FTP Site

Userid:

Password:

The system will survey the firmware installed on your system against the available catalog of current firmware. Upon completion of the survey, a report will be generated on the system.



The following list shows the items in the survey table:
- All devices on your system identified by the survey
- Current code level for each device
- Code level for the device available in the specified microcode repository
- Effect on device to complete microcode installation
- Suggested action to take to bring microcode level to the latest version available.

Current Repository Location: Service Website

Service Level: 200504251434

Sort By: Logical Device

Partition	Install	Logical Device	Device	MTMS	Current Level	Available Level	Effect	Suggested Action
Partition 001	☐		olly.austin.ibm.com	9111-520_10F6A0E	5.3.0.0	5.3.0.0		
	☐	sys0	9110-510;9111-520;9113-550;911...	9111-520_10F6A0E	SF222_081	SF225_096	Reboot	Cannot Manage
	☐	ent0	10/100/1000 Base-TX Ethernet PCI...	9111-520_10F6A0E	DV0210	DV0210	None	No action
	☐	ent1	10/100/1000 Base-TX Ethernet PCI...	9111-520_10F6A0E	DV0210	DV0210	None	No action
	☐	sisscsia0	PCI-X Dual Channel Ultra320 SCSI ...	9111-520_10F6A0E	02080037	02080039	Take Offline	Cannot Manage
	☐	sisscsia1	PCI-X Dual Channel Ultra320 SCSI ...	9111-520_10F6A0E	02000037	02000039	Take Offline	Cannot Manage
	☐	ent2	10/100/1000 Base-TX Ethernet PCI...	9111-520_10F6A0E	GOL021	GOL021	None	No action
	☑	sisioa0	SCSI RAID Enablement Card for P...	9111-520_10F6A0E	030D0056	030D0058	None	Update
	☐	ent3	10/100/1000 Base-TX Ethernet PCI...	9111-520_10F6A0E	GOL021	GOL021	None	No action
	☐	hdisk0	18/36/73GB 15KRPM SCSI Drive 7...	9111-520_10F6A0E	43353143	43353143	Take Offline	Cannot Manage

If the device can be managed by this utility, and it is down level, the install box will be checked by default. To skip a firmware update on a checked device or system, uncheck the corresponding box.

Clicking the apply button will download the update files to the system, and update the firmware system or devices.

Items that are listed as ***can not manage*** should be researched on the firmware website to understand the impact to your system and how to get the update if required.

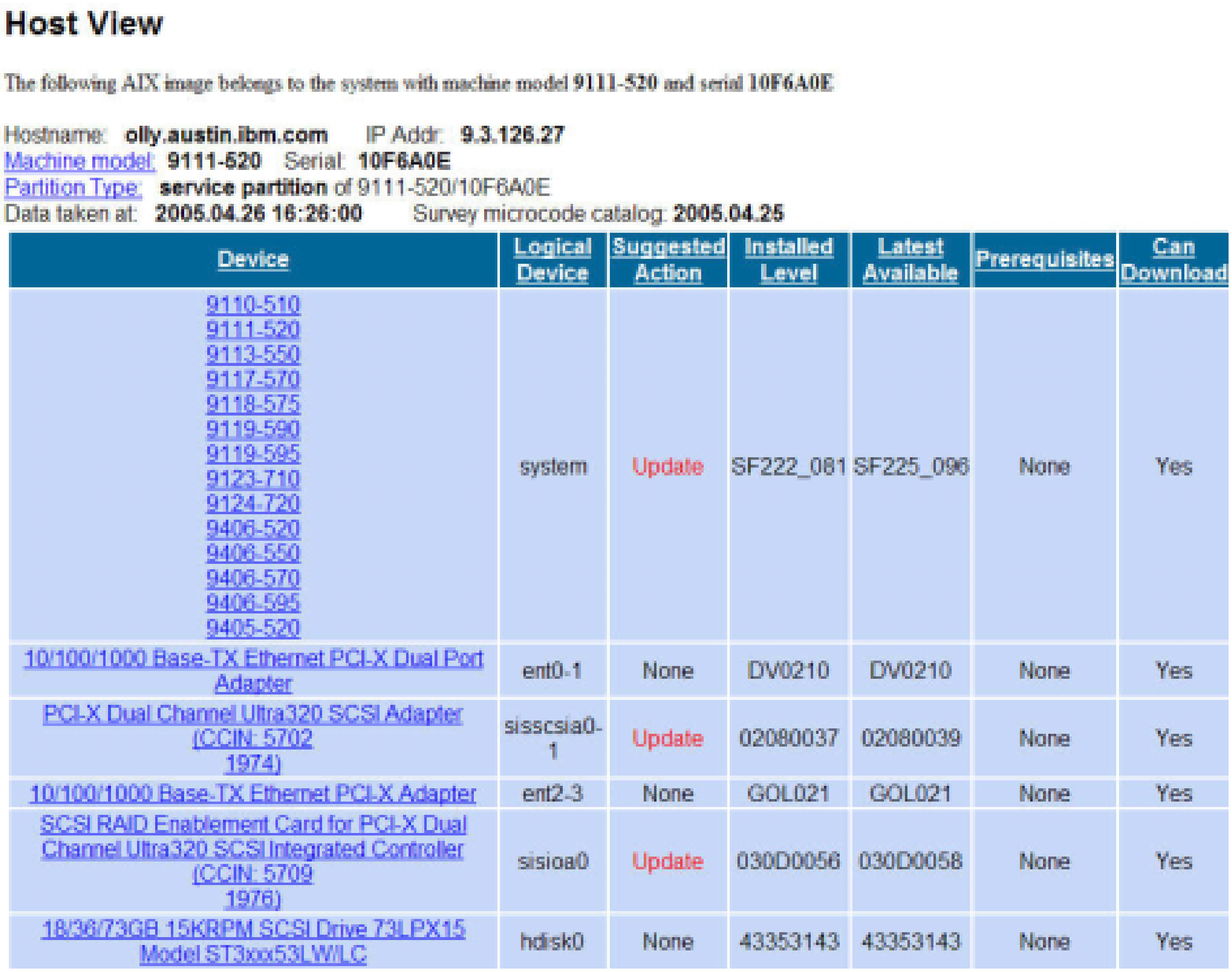
MDS Applet

The MDSapplet provides a convenient method of surveying systems and displaying results if the system is internet connected and the invscoutd daemon has been started.

The MDSapplet provides the same level of display capability, should you opt to run invscout via the command line method, transfer *.mup files to a system with internet access and upload file to MDSapplet for display.

The MDSapplet can be found here:
http://www14.software.ibm.com/webapp/set2/mds/fetch?page=mds.html

After selecting the method to use and executing the applet, the user will be presented with a graphical view of your systems firmware.



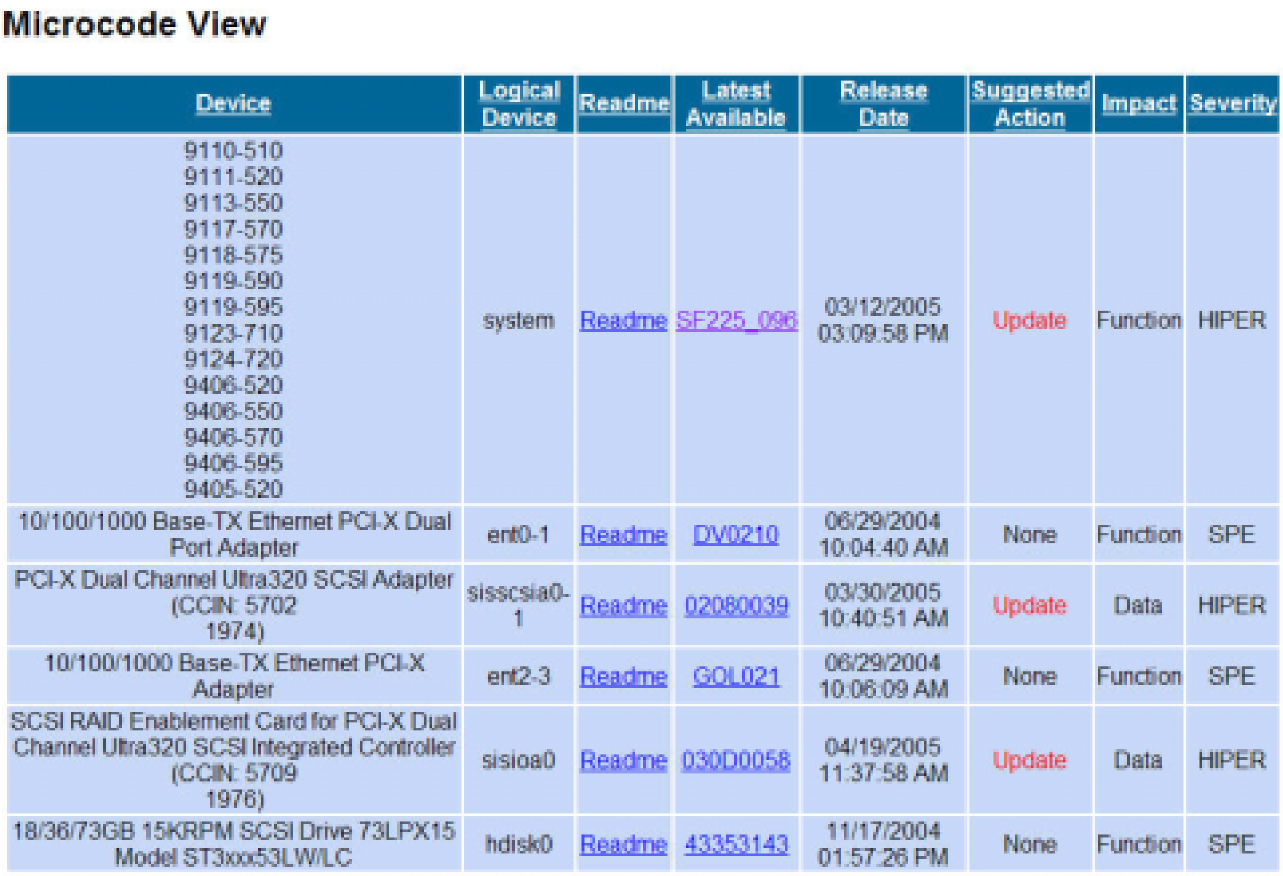
Host View

The following AIX image belongs to the system with machine model **9111-520** and serial **10F6A0E**

Hostname: **olly.austin.ibm.com** IP Addr: **9.3.126.27**
Machine model: **9111-520** Serial: **10F6A0E**
Partition Type: **service partition** of 9111-520/10F6A0E
Data taken at: **2005.04.26 16:26:00** Survey microcode catalog: **2005.04.25**

Device	Logical Device	Suggested Action	Installed Level	Latest Available	Prerequisites	Can Download
9110-510 9111-520 9113-550 9117-570 9118-575 9119-590 9119-595 9123-710 9124-720 9406-520 9406-550 9406-570 9406-595 9405-520	system	Update	SF222_081	SF225_096	None	Yes
10/100/1000 Base-TX Ethernet PCI-X Dual Port Adapter	ent0-1	None	DV0210	DV0210	None	Yes
PCI-X Dual Channel Ultra320 SCSI Adapter (CCIN: 5702 1974)	sisscsia0-1	Update	02080037	02080039	None	Yes
10/100/1000 Base-TX Ethernet PCI-X Adapter	ent2-3	None	GOL021	GOL021	None	Yes
SCSI RAID Enablement Card for PCI-X Dual Channel Ultra320 SCSI Integrated Controller (CCIN: 5709 1976)	sisioa0	Update	030D0056	030D0058	None	Yes
18/36/73GB 15KRPM SCSI Drive 73LPX15 Model ST3xxx53LW/LC	hdisk0	None	43353143	43353143	None	Yes

Followed by a listing of resources to update your system:



Microcode View

Device	Logical Device	Readme	Latest Available	Release Date	Suggested Action	Impact	Severity
9110-510 9111-520 9113-550 9117-570 9118-575 9119-590 9119-595 9123-710 9124-720 9406-520 9406-550 9406-570 9406-595 9405-520	system	Readme	SF225_096	03/12/2005 03:09:58 PM	Update	Function	HIPER
10/100/1000 Base-TX Ethernet PCI-X Dual Port Adapter	ent0-1	Readme	DV0210	06/29/2004 10:04:40 AM	None	Function	SPE
PCI-X Dual Channel Ultra320 SCSI Adapter (CCIN: 5702 1974)	sisscsia0-1	Readme	02080039	03/30/2005 10:40:51 AM	Update	Data	HIPER
10/100/1000 Base-TX Ethernet PCI-X Adapter	ent2-3	Readme	GOL021	06/29/2004 10:06:09 AM	None	Function	SPE
SCSI RAID Enablement Card for PCI-X Dual Channel Ultra320 SCSI Integrated Controller (CCIN: 5709 1976)	sisioa0	Readme	030D0058	04/19/2005 11:37:58 AM	Update	Data	HIPER
18/36/73GB 15KRPM SCSI Drive 73LPX15 Model ST3xxx53LW/LC	hdisk0	Readme	43353143	11/17/2004 01:57:26 PM	None	Function	SPE

Firmware CD Discovery Tool

This service provides a CD image in ISO 9660 format which contains microcode updates as well as a Microcode Discovery Tool for use in certain system environments. A README accompanies the CD and provides recommended methods for surveying and installing microcode.

This CD provides a convenient way to update microcode on systems that are not accessible to the Internet. You can perform updates at a time most convenient for you.
Use this CD and tools to keep your microcode current with the latest available updates. These tools assist you in managing your own system and I/O adapter microcode by surveying, retrieving, and in some cases installing the latest updates.

More information on this can be found at:

http://www14.software.ibm.com/webapp/set2/firmware/gjsn?mode=10&page=compare.html

Additional Information

You can install microcode remotely by copying the microcode to the correct directory on the remote system or systems, and then remotely executing the same commands that you would run to update microcode locally. You can manually copy and install microcode files from the CD-ROM or Internet download site to other systems anywhere in your network. You need root authority on the remote system to install microcode. You also need to make sure you have enough directory space to install the microcode. Before proceeding, read the installation instructions for the microcode you want to install, and then follow these steps:

1. Use your preferred file transfer protocol, and binary format, to copy the microcode file into the correct directory on the remote system to be updated.
2. Run a checksum on the files to be sure they were transferred correctly.
3. Log in to the remote system and execute the installation command(s) listed in the individual microcode installation instructions.

Note: If you update the system microcode, the system will reboot after the microcode is installed.

Query the VPD on the remote system or systems to ensure that the new microcode is installed.

SUMMARY

With the advent of concurrent firmware and the AIX 5L Service Strategy, IBM System p clients are even better equipped to create firmware maintenance strategies more closely tailored to their availability needs. Firmware planning remains a customer responsibility and IBM is committed to reviewing the fix acquisition and dissemination process adding strategic tools and maintenance planning enhancements designed to improve the client experience.

A well designed architecture is at the heart of any well-maintained system and good firmware hygiene and currency is necessary to increase availability and stability. Client methodologies and techniques must compliment IBM's maintenance strategies, RAS and hardware design. Rolling firmware upgrades are necessary if the business availability needs stipulate restricted maintenance windows. It is possible through these techniques along with Concurrent Firmware Maintenance strategies to provide optimal availability on a well-run and managed hardware platform.