Installation Guide
HP BladeSystem PC Blade Switch

Fourth Edition (February 2009)

Third Edition (September 2007)

Second Edition (May 2007)

First Edition (May 2007)

Document part number: 413355-004

About This Book

This guide provides instructions for the installation of the HP BladeSystem PC Blade Switch.

⚠ **WARNING!** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

△ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

Table of contents

1 Introduction

The Consolidated Client Infrastructure (CCI) solution uses a 3U (5.25-inch) HP BladeSystem PC Blade Enclosure supporting 20 HP Blade PCs and redundant, hot-plug power and cooling. The HP BladeSystem PC Blade enclosure with 20 HP blade PCs contains 40 10/100 Mbps network adapters (NIC). Since the CCI solution packages many HP Blade PCs in a small space, the number of network cables within this space can quickly become overwhelming.

The HP PC Blade enclosure includes a slot for an interconnect switch used to provide external Ethernet connectivity. The HP PC Blade Switch can provide up to a 41-to-1 reduction in network cables. This cable reduction significantly reduces the time required to deploy, manage, and service the CCI solution. This Installation Guide describes the HP PC Blade Switch configuration and is intended for applications that require 100 megabit per second (Mbps) Fast Ethernet NIC aggregation to 10/100/1000 megabits per second (Mbps) copper or 1000 Mbps Fiber Ethernet uplinks.

Switch Management

The HP BladeSystem PC Blade Switch is an industry-standard managed layer 2+ Ethernet switch that can be configured and manage the switch like any other industry-standard Ethernet switch.

A browser-based interface and a command line interface (CLI) are embedded in the switch firmware to configure, manage, and monitor the switch. The switch also supports Telnet access, Secure Shell (SSH) support, Simple Network Management Protocol (SNMP) v1-v3, and Remote Monitoring (RMON). Any internal or external ports can be disabled, enabled, configured, or monitored on a per port basis. Dedicated access to the switch management interface is supported locally using the Integrated Administrator or remotely through any configured virtual LAN (VLAN) management interface.

Switch Configuration

You can independently disable or enable the switch ports. Auto-MDI/MDIX with auto negotiation of speed and duplex is supported. The PC Blade Switch includes the following Ethernet ports:

- 41 dedicated internal 10/100 Mb/s Fast Ethernet ports
- Five external Ethernet ports for data
  - Four 10/100/1000 Mbps dual personality Copper/Fiber Ethernet uplinks
  - One 10/100T Fast Ethernet port ideal for optional out-of-band system management, but can be used as an additional data uplink

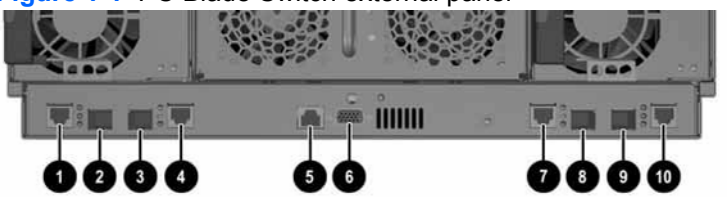
HP PC Blade Enclosure

The HP PC Blade Enclosure supports 20 HP Blade PCs, each with two embedded 10/100Mbps Fast Ethernet network interface controllers. The primary or first NIC of each Blade PC supports Pre-boot eXecution Environment (PXE) and Wake-on-LAN (WoL). Each enclosure can have up to 40 active network adapters at one time.

HP PC Blade Switch Interconnect Tray

The PC Blade Switch has the following port configuration.

Figure 1-1 PC Blade Switch external panel



Item	Description
1	10/100/1000T RJ-45 Connector Gigabit Ethernet Uplink designated as port 43 Combo port with GBIC port next to it on the right side
2	Small Form-factor Pluggable (SFP) GBIC port designated as port 43 Combo port with RJ-45 port next to it on the left side
3	Small Form-factor Pluggable (SFP) GBIC port designated as port 44 Combo port with RJ-45 port next to it on the right side
4	10/100/1000T RJ-45 Connector Gigabit Ethernet Uplink designated as port 44 Combo port with GBIC port next to it on the left side
5	10/100T Fast Ethernet port suited for isolated in-band or out-of-band Integrated Administrator management designated as port 42
6	Integrated Administrator console connector, DB-9 Serial (uses an RS-232 Null modem cable)
7	10/100/1000T RJ-45 Connector Gigabit Ethernet Uplink designated as port 45 Combo port with GBIC port next to it on the right side
8	Small Form-factor Pluggable (SFP) GBIC port designated as port 45 Combo port with RJ-45 port next to it on the left side
9	Small Form-factor Pluggable (SFP) GBIC port designated as port 46 Combo port with RJ-45 port next to it on the right side
10	10/100/1000T RJ-45 Connector Gigabit Ethernet Uplink designated as port 46 Combo port with GBIC port next to it on the left side

Internal Ports

The HP PC Blade Switch includes 40 pre-assigned, embedded 10/100 Mbps Fast Ethernet “downlink” ports connecting the blade PC network adapter signals to the switch. The signals are routed as Ethernet from the blade PCs, across individual category 5e (CAT5e) specified signal traces on the passive center wall assembly of the HP PC Blade enclosure.

One additional 10/100 Mbps Fast Ethernet internal port connects the Integrated Administrator (IA) to the HP PC Blade Switch for IA to switch Ethernet communication.

External Ports

The HP PC Blade Switch includes eight external ports, four 10/100/1000T Mbps Ethernet "uplink" ports with RJ-45 connectors, typically used to connect the switch to the network infrastructure, and four Small Form-factor Pluggable (SFP) GBIC ports which can be used for Gigabit Fiber connectivity. These ports are shared "combo" ports, whereas only one media type can be used at a time. Combo ports are single ports with two physical connections, RJ-45 copper or SFP. If both devices are plugged in, the port that takes priority can be defined through the switch CLI.

In addition, one external 10/100T Fast Ethernet port with an RJ-45 connector is provided for an optional dedicated out-of-band management network or for local administration and diagnostic tasks without unplugging one of the other dedicated uplinks. Although ideally suited for management, this port can be used as an additional data uplink to the network.

System Management

Back-up and Restore

The PC Blade Switch supports trivial file transfer protocol (TFTP) allowing a copy of each switch configuration file to be uploaded or downloaded. This provides a method to rapidly deploy multiple switches with similar configurations and to provide backup and restore capabilities. Configuration settings can be modified through the user interfaces or directly within the configuration file itself. The configuration file may even be reset to the factory default settings at any time by first erasing the existing startup-config, then rebooting the switch.

Users can perform firmware upgrades by using TFTP through any external Ethernet port after boot-up. The switch simplifies firmware upgrades by retaining its configuration after an upgrade and by supporting the HP Support Paq automated firmware process for Windows deployment stations.

IP Addressing

By default, the PC Blade Switch will automatically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) server. Optionally, an administrator can manually assign an IP address through the CLI or from the browser-based interface; however, they would have to reconnect with the newly assigned IP address. For increased security, an administrator can specify the IP-based management stations that are allowed to access the switch.

Web Browser-based Interface

Users can access the browser-based interface by using Internet Explorer or Netscape Navigator over a TCP/IP network. The browser-based interface consists of three main sections:

- The Active Virtual Graphic provides real time status of the switch panel and a means to quickly view statistics of individual ports.
- The Navigation Window contains particular items or features to select and configure.

Command Line Interface (CLI)

The CLI provides many more configuration options than the browser-based interface. There are three methods of accessing these interfaces:

- Locally with the RS-232 console port on the switch tray by way of logging into the Integrated Administrator and connecting to the PC Blade Switch through the internal serial link.
- Remote virtual serial access to the switch through the Integrated Administrator by way of a built-in account. Connect remotely to the IA using either SSH or Telnet. At the login prompt, enter username `switch` and the password `switcha`.
- Remotely using a console Telnet or SSH session (if configured).

SNMP and Remote Monitoring

The switch supports industry-standard SNMP management information bases (MIBs), HP enterprise MIB, SNMP v1 traps, and RMON1 group 1 (Ethernet statistics), 2 (History), 3 (Alarms), and 9 (Events). Four community strings and SNMP trap manager hosts can be configured. This capability allows the switch to be monitored remotely from a Network Management Station.

Switch Security

The switch uses a layer 2 access control list or filtering database to segment the network, control communications between segments, and provide intrusion control. The switch allows manual entry of specific media access control (MAC) addresses to be filtered from the network. Filtering of both Unicast and Multicast traffic is possible. The maximum number of MAC addresses learned on a per port basis may be restricted further.

Several additional features are provided on the switch to allow the network administrator to secure the management interfaces. These features include the ability to:

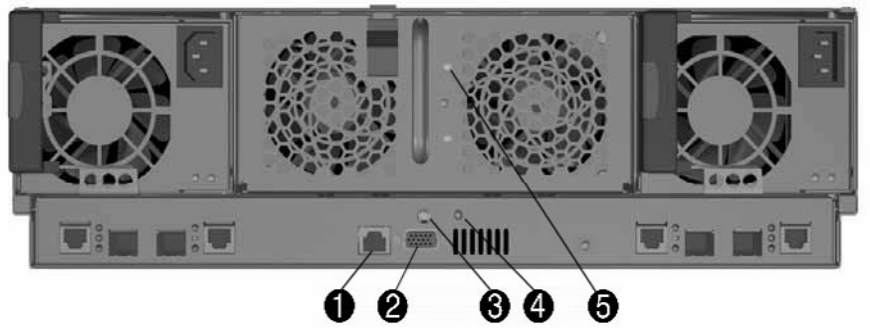
- Configure multiple password protected accounts with two levels of access.
- Specify the IP-based management stations that are allowed to access the switch.
- Specify remote access method and set user interface idle time-out period.
- Configure port-based IEEE 802.1Q tagged VLANs for server grouping and data isolation.

Identifying Integrated Administrator Components

Each HP PC Blade Enclosure interconnect tray ships with the Integrated Administrator module already installed and provides external connectivity using the RJ-45 and RS-232 ports on the rear panel.

External LEDs are provided for enclosure and switch status and for link and speed on each Ethernet uplink (see HP PC Blade Switch tray external panel LEDs). An emergency enclosure shut-down feature is included in case of critical system temperature caused by the switch or other enclosure component.

Figure 1-2 PC Blade Integrated Administrator external panel LED's and ports



Item	Description
1	Management (10/100 Fast Ethernet) connector for remote access through a browser-based user interface, Telnet, or SSH.
2	Console (DB-9 RS-232) connector for local access to the command line interface. (Requires an appropriate null modem cable.)
3	Integrated Administrator reset button.
4	Integrated Administrator health LED.
5	Enclosure Unit Identification button/LED.

Switch Serviceability

The switch provides many additional serviceability and diagnostic features including:

- Port mirroring with the ability to mirror desired type of frames (egress, ingress, or both).
- Power-on self test (POST) at boot for hardware verification.
- Monitoring screens using the user interfaces for port utilization, data packets received/transmitted, error packets, packet size, trunk utilization, SNMP data, etc.
- Details of system information using the user interfaces such as port parameters and link status, switch asset information, configuration values, log entries, etc.
- The ability to “ping” or "traceroute" to test the connectivity on the Ethernet network.
- Local system log (syslog) with ability to view and clear messages that may be saved (uploaded) as text file using TFTP.
- MAC addresses view, clear, and delete from the forwarding database for identifying problems with MAC address learning and packet forwarding.
- The ability to switch to a backup firmware image in case of firmware corruption.

For more detailed information on the administration capabilities of the switch, see the PC Blade Switch user guides.

Virtual LAN

Each switch supports up to 256 port-based IEEE 802.1Q VLANs with GVRP dynamic VLAN registration. Members of a VLAN may be untagged or tagged ports according to IEEE 802.3ac VLAN Ethernet frame extensions for 802.1Q tagging. Therefore, PC Blade Switch VLANs may span other switches that support 802.1Q tagging located within the network infrastructure.

Spanning Tree

The switch meets the IEEE 802.1D spanning tree protocol (STP) to eliminate potential problems caused by redundant networking paths. Users can configure STP switch parameters, including priority and cost, on a per port basis. Each switch can automatically find the STP root bridge on the network. Otherwise, the switch will act as the root bridge for the STP domain.

Spanning tree is a standard requirement for L2 switches (performing transparent bridging) and allows bridges to automatically prevent and resolve L2 forwarding loops. The switches exchange configuration messages using specially formatted frames called Bridge Protocol Data Units (BPDUs), and selectively enable and disable forwarding on ports. The result is that a tree of active forwarding links is created, ensuring there is an active path (series of L2 forwarding links) between any two devices in the network, with no loops.

On a LAN interconnected by multiple bridges, Spanning Tree selects a controlling Root Bridge and Port for the entire bridged LAN, and a Designated Bridge and Port for each individual LAN segment. When traffic passes from one end station to another across the LAN, it is forwarded through the designated Bridge/Port for the LAN segment, to the Root Bridge, which in turn forwards the traffic to the designated Bridges/Ports on the opposite side. Bridges use BPDUs to communicate Spanning Tree information.

While “classic” spanning tree, as defined in IEEE 802.1D, is guaranteed to prevent L2 forwarding loops in a general network topology, it can take up to 50 seconds for it to “converge” (that is, for each bridge/switch in the network to separately decide for each of its ports if it should actively forward traffic or not).

This period is considered too long for many applications. The delay is needed to allow enough time to detect possible loops, allowing time for status changes to propagate and be acted upon by all relevant devices.

In this switch, when network topology allows, faster convergence may be possible. The Rapid Spanning Tree Protocol (RSTP) is designed to detect and make use of network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops. In a well designed network, reconvergence time may take less than one second.

Multiple Spanning Tree (MST) enables grouping and associating VLANs to spanning tree instances. Each Spanning Tree Instance has an independent topology of other Spanning Tree Instances. The architecture provides multiple forwarding paths for data traffic, enabling load balancing in the network and fault tolerance provision.

MSTP-to-RSTP Conversion (PVST Interoperability)

MSTP-to-RSTP Conversion extends the Multiple Spanning Tree Protocol (MSTP) standard to provide limited interoperability with other proprietary Per-VLAN Spanning Tree Protocols such as Cisco's PVST/ PVST+. When enabled on the HP PC Blade Switch, MSTP-to-RSTP conversion is a global parameter which applies to all ports that have Spanning Tree enabled. When this feature is enabled, switchport mode trunk or general are not supported. An error message will be displayed if you attempt to change an interface switchport mode to either trunk or general. If more than two VLANs are required, the four primary uplinks can be used individually as access ports, but at the expense of loosing layer 2 redundancy. If more than two VLANs and redundancy are required, this feature must be disabled. HP recommends using IEEE 802.1s Multiple Spanning Trees for situations where high speed L2 redundancy and support for more than two VLANs is needed.

Upon receiving a spanning tree BPDU, the switch translates it to an MSTP BPDU and assigns it to the appropriate MST instance. Before transmitting an MSTP BPDU, the switch translates the BPDU to an RSTP BPDU. If the switch is connected to another switch running 802.1D, the RSTP BPDU will be sent as an STP BPDU as called for in the IEEE specification.

The default configuration for this feature is as follows:

- MSTP enabled by default
- VLAN 1 mapped to MST instance 1
- MSTP-to-RSTP conversion enabled
- VLAN 2 mapped to MST instance 2
- VLAN 3-4093 mapped to MST instance 15

Instance 0 is reserved for VLAN 4094 (default VLAN to drop all frames)

NOTE: When MSTP-to-RSTP is enabled (enabled by default) if you attempt to put any switchport into trunk or general mode, you will receive the following error message: **Port <Number>, extension separated-bridge exist**. Refer to paragraph one in this section for more detail.

Link Aggregation

The switch complies with IEEE 802.3ad static link aggregation (excluding LACP8) where several links can be bundled into a single logical link of aggregate capacity.

Ports may be aggregated into link-aggregation port-groups. Each group must be composed of ports set to the same speed and set to full-duplex operation. Ports in a link-aggregation group (LAG), also called

an “Aggregated Link” may be of different media types (UTP/Fiber, or different fiber types), provided they are of the same speed and duplex.

Aggregated Links may be set up manually, or automatically by enabling LACP (Link Aggregation Control Protocol) on the relevant links. An Aggregated Link is treated by the system as a single logical port, in the same manner as any other port in the system. In particular, the Aggregated link has port attributes similar to a “regular” port – Auto negotiation state, speed, etc.

Each switch supports up to eight multi-port trunks with up to eight ports per trunk.

Internet Group Management Protocol

By default, a Layer 2 switch forwards multicast frames to all ports of the relevant VLAN, treating the frame as if it were a broadcast. The result is that some ports may receive irrelevant frames only needed by a subset of the ports of that VLAN.

This may be alleviated by explicit system configuration, or by “snooping” (examining the contents of) IGMP frames as they are forwarded by the switch from stations to an upstream multicast router. This allows a switch to conclude the following:

- Where (on which ports) stations interested in joining a specific multicast group are located
- Where (on which ports) multicast routers sending multicast frames are located

This knowledge may be used to exclude irrelevant ports (ports on which no stations have registered to receive a specific multicast group) from the forwarding set of an incoming multicast frame.

The switch provides Internet Group Management Protocol (IGMP) snooping v1 and v2, configurable to a non-querier mode. The IGMP state may be enabled and disabled on a per VLAN basis as well as a configurable response report delay and query interval. Each switch allows a maximum of 191 concurrent multicast groups (127 dynamically learned by IGMP, 64 static Multicast).

Data Storm Prevention

When L2 frames are forwarded, broadcast and multicast frames are flooded to all ports on the relevant VLAN. Moreover, all nodes connected to these ports will accept and try to process these frames, placing load on both the network links and the host operating systems (as each of these frames creates at least an I/O interrupt, if only to decide that it is to be discarded).

The switch permits configurable thresholds (in packets per second) to prevent three types of packet storms: broadcast, Multicast, and destination address unknown. If the threshold is exceeded, any additional packets received would be dropped.

Quality of Service

The system enables various services for specific traffic flows to be defined. This is achieved by two mechanisms:

- Classification — Certain fields are specified within the packet, which are matched to some values. All packets matching those fields are related to the same flow/class.
- Actions — Various actions can be set, such as manipulating fields within the packet (for example, VPT, DSCP), policing at the ingress, scheduling at the egress, and shaping at the egress. Same actions are applied to all packets within a specific flow.

The mechanism for supporting these actions related to bandwidth management and control is the concept of queues. After a packet has been classified it is assigned to one of the output queues. The

system supports eight queues per port. The system services the queues (takes frames out of a queue for transmission) according to the current queue scheduling settings, as defined by the user. These settings determine which queue is handled and how many frames from that queue will be handled before any other queue is managed.

While the system facilities providing Access Control and CoS/QoS are given, there are several ways to configure the system to provide the desired effect. These modes present different levels of functionality and complexity to the user.

NOTE: These Modes are different ways to control and configure the system CoS/QoS facilities, and not different operational modes of the actual system CoS/QoS facilities.

The following list provides CoS/QoS control modes

- Basic Mode — In Basic CoS mode the frames can be classified into broad classes, by the ingress interface or by the value of a single frame header field. Each class can be directed to a desired egress queue, and the queue servicing parameters can also be configured. This is enough to provide relative class-by-class differential services. This mode does NOT include the facility to classify traffic into fine-grained flows (for example, define a flow as a specific value in a frame-header fields, or a combination of values in several header fields) and does not include traffic measurement facilities.
- Advanced Mode — In Advanced mode CoS/QoS the user has access, and must explicitly configure all aspects of all CoS/QoS facilities in use. Traffic may be classified into broad classes or fine-grained flows.

Support for quality of service (QoS) IEEE 802.1p on the switch allows switch administrators to set priority levels on each switch for forwarding packets. Each switch supports four classes of traffic (buffers or queues) for implementing priority based on the priority tag of the packet.

Administrators can map up to eight priority levels to four classes. Traffic from a specific Blade PC port can be given priority over packets from other devices according to this range of priority levels. For example, with multiple packets in a buffer, the packet with the highest priority would be forwarded first, regardless of when it was received.

Enterprise-class Performance

The PC Blade Switch includes the following performance features:

- Non-blocking, full wire speed on all ports.
- 16K MAC addresses per switch with automatic MAC address learning.
- 128-MB SDRAM, 16-MB flash, and 6-MB packet buffer memory per switch (packet buffer memory shared between ports).

Conclusion

The HP BladeSystem PC Blade Enclosure is a 3U rack mountable device capable of supporting 20 HP PC Blades with redundant, hotplug power and cooling. The HP PC Blade Enclosure includes the HP PC Blade Switch interconnect tray that provides Ethernet connectivity for the HP Blade PCs. The HP PC Blade Switch provides up to a 41-to-1 reduction in network cables at the back of the interconnect switch.

The system has an Integrated Administrator daughter card connected to the Interconnect switch that monitors the health of the enclosure (temperature, fans, etc.) Blade PCs and switch. The Integrated Administrator also provides serial access to the interconnect switch.

The switch and the IA have separate and independent IP addresses. The 20 PC blades, switch, and the IA altogether comprise a single chassis. A 42U rack may contain up to 14 chassis.

2 First Time Installation

After completing all external connections, connect a terminal (with terminal emulation software) to the Integrated Administrator 's external DB-9 RS232 serial port. To configure the Integrated Administrator, please refer to the Integrated Administrator documentation. Ensure that the terminal emulation software is configured as follows:

1. Integrated Administrator external serial port: 9600 baud.
2. Set the data format to 8 data bits, 1 stop bit, and no parity.
3. Set **Flow Control** to none.
4. Under **Properties**, select VT100 for Emulation mode.
5. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that the setting is for Terminal keys (not Windows keys).

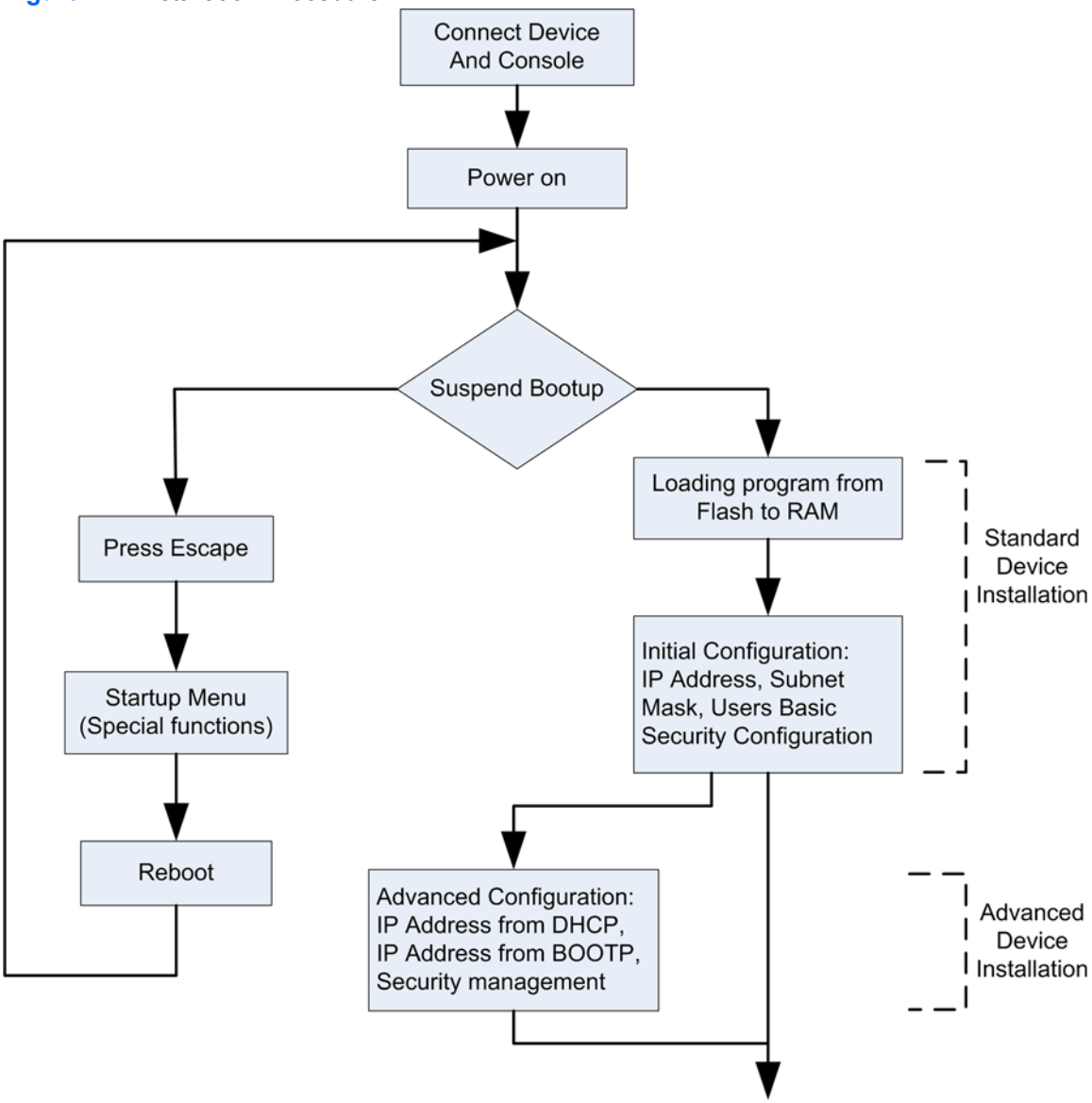
NOTE: When using HyperTerminal with Microsoft Windows 2000, make sure that Windows 2000 Service Pack 2 or later is installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal VT100 emulation. For more information about Windows 2000 service packs, go to http://www.microsoft.com.

Installation Procedure

The order of installation and configuration procedures is illustrated in the following figure. For the initial configuration, the standard device configuration is performed.

Performing other functions is described later in this section.

Figure 2-1 Installation Procedure



Booting the PC Blade Switch

The PC Blade Switch will power on automatically when one or more of the enclosure power supplies are plugged in. The assumed bootup information is as follows:

- The PC Blade Switch is delivered with a default configuration that differs from a typical distribution or edge switch.
- The default user name for the PC Blade Switch Web Management Interface is admin. Note: if connecting to the switch via the Integrated Administrator, no user name is required.
- There is no default password set.

Because the PC Blade Switch boots automatically, to view the POST boot process, the switch needs to be rebooted from its command line interface. To do this, you must be connected to the IA over a local serial port. To connect to the switch CLI and reboot the switch perform the following commands from the IA command prompt.

To reboot the switch from the CLI:

1. Type `connect switch a` at the prompt.

   The following is displayed:

   ```
   The displaying of events will be suspended during your remote console
   session.

   Connecting to integrated switch A at 115200,N81...

   Escape character is '<Ctrl>_'
   ```

2. Press Enter twice to display the switch console.
3. Type `enable` at the **console>** prompt.
4. Type `reload` at the **console#** prompt.
5. Type `Y` when asked if you want to continue without saving your changes.

The PC Blade Switch goes through Power On Self Test (POST). POST runs every time the PC Blade Switch is initialized and checks hardware components to determine if they are fully operational before completely booting. If a critical problem is detected, the program flow stops and the switch LED glows red. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

As the PC Blade Switch boots, the bootup test first counts memory availability and then continues to boot. The following screen is an example of the displayed POST:

```
------ Performing the Power-On Self Test (POST)

-----UART Channel Loopback Test.....................PASS

Testing the System SDRAM.....................PASS

Boot1 Checksum Test.....................PASS

Boot2 Checksum Test.....................PASS

Flash Image Validation Test.....................PASS
```

```
FRU Validation Test.............................PASS

BOOT Software Version x.x.x.xx Built 22-Jan-xxxx 15:09:28

I-Cache x KB. D-Cache x KB. Cache Enabled.

Autoboot in 2 seconds -press RETURN or Esc. to abort and enter prom.

Preparing to decompress...
```

The boot process runs for approximately 60 seconds. The auto-boot message displayed at the end of POST (see the last lines) indicates that no problems were encountered during boot. During boot, the Startup menu can be used to run special procedures. To enter the Startup menu, press Esc or Enter within two seconds after the auto-boot message is displayed.

If the system boot process is not interrupted by pressing Esc or Enter, the process continues decompressing and loading the firmware into RAM.

After the PC Blade Switch boots successfully, a system prompt will be displayed. Before configuring, ensure that the latest firmware version has been installed. If it is not the latest version, please download and install it. For more information about downloading the latest version, see Software Download [option 1].

Configuration Overview

In most cases, the PC Blade Switch can be used without making any changes to the default configuration. If the default configuration needs to be modified, please consider the following information.

NOTE: After making any configuration changes, you must save the new configuration before rebooting. To save the configuration, at the (**console#**) prompt, type: `copy running-config startup-config` and confirm.

Initial Configuration

NOTE: Before proceeding, read the release notes for this product.

Initial configuration, which starts after the PC Blade Switch has booted successfully, includes static IP address and subnet mask configuration and setting user name and privilege level to allow remote management. If you will manage the device from an SNMP-based management station, you must also configure SNMP community strings.

The initial simple configuration uses the following assumptions:

- The PC Blade Switch was never configured before and is in the same state as when it was received.
- The PC Blade Switch booted successfully.
- The Serial connection is established and the console prompt is displayed on the screen of a VT100 terminal console applicaiton. (Press Enter several times to verify that the prompt is displayed correctly.)
- The PC Blade Switch is not configured with a user name and password.

The initial PC Blade Switch configuration is through the serial port. After the initial configuration, you can then manage the PC Blade Switch either from the already connected serial port or remotely through an interface defined during the initial configuration.

The initial configuration consists of the following:

- Setting the user name `TBD`, password as `TBD` with the highest privilege level of 15
- Configuring the static IP address and the default gateway
- Configuring the SNMP read/write community strings

Before applying the initial configuration procedure, please obtain the following information from the network administrator:

- The IP address to be assigned to a VLAN through which the device is managed.
- The IP subnet mask for the network
- The default gateway
- The read and write SNMP community strings

Static IP Address and Subnet Mask

Before assigning a static IP address to the PC Blade Switch, obtain the following information:

- A specific IP address that has been allocated to the PC Blade Switch for it to be configured
- Network mask for the network
- Default gateway

You can configure IP interfaces on each VLAN of the switch. After entering the configuration commands, HP recommends checking that a VLAN was configured with the IP address by typing the `enable show ip interface` command. The commands to configure the PC Blade Switch are VLAN-specific.

To manage the PC Blade Switch from a remote network, you must configure an interface with a valid address and mask, which is an IP address to where packets are sent when no entries are found in the switch tables.

To configure a static address, type the command at the system prompt as shown in the following configuration example, where:

- 192.168.1.123/24 is the specific management station
- The IP address is defined on the appropriate VLAN
- The default gateway is defined as 192.168.1.1

Odd ports 1-41, 42, 45, and 46 are in VLAN 1. Even ports 2-40, 43, and 44 are in VLAN 2.

console# > `enable`

console# `configure`

console(config)# `interface vlan 1`

console(config-if)# `ip address` 192.168.1.123 255.255.255.0

console(config-if)# `exit`

console(config)# `ip default-gateway` 192.168.1.1

console(config)# `exit`

Verifying the IP and Default Gateway Addresses

Ensure that the IP address and the default gateway were properly assigned by executing the command show ip interface and examining its output:

```
Console# show ip interface

Gateway IP Address                Activity status

--------------------              ---------------

192.168.1.1                       active

IP address                        Interface                Type

------------                      ----------               ------

192.168.1.123/24                  VLAN 1                   Static
```

User Name

Use a user name to manage the device remotely, for example through SSH, Telnet, or the browser-based interface. To gain complete administrative (super-user) control over the PC Blade Switch, specify the highest privilege (15).

NOTE: Only the administrator (super-user) with the highest privilege level (15) is allowed to manage the PC Blade Switch through the browser-based interface.

For more information about the privilege level, see the CLI Reference Guide.

The configured user name is entered as a login name for remote management sessions. To configure user name and privilege level, type the command at the system prompt as shown in the configuration example:

console> `enable`

console# `configure`

console(config)# `username admin password lee level` 15

SNMP Community Strings

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run local software (agent). The SNMP agents maintain a list of variables used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings and SNMP community strings.

The PC Blade Switch is SNMP-compliant and contains an SNMP agent that supports a set of standard and private MIB variables. Developers of management stations require the exact structure of the MIB tree and need to receive the complete private MIBs before being able to manage the MIBs. All parameters are manageable from any SNMP management platform, except the SNMP management

station IP address and community (community name and access rights). The SNMP management access to the switch is disabled if no community strings exist.

NOTE: The switch is delivered with the PUBLIC, read-only, community string configured with no password. No write community strings are configured by default.

You can configure the community-string, community-access, and IP address through the switch CLI during the initial configuration procedure.

The SNMP configuration options are:

Community string

- Access rights options:
  - ro (read-only)
  - rw (read-and-write)
  - su (super)
- An option to configure IP address or not: If an IP address is not configured, all community members with the same community name are granted the same access rights.

Common practice is to use two community strings, one (public community) with read-only access and the other (private community) with read-write access. The public string allows authorized management stations to retrieve MIB objects, while the private string allows authorized management stations to retrieve and modify MIB objects.

During initial configuration, HP recommends that you configure the device according to network administrator requirements in accordance with using an SNMP-based management station. During the initial configuration procedure the community-string, community-access, and IP address can be set through the switch CLI.

The SNMP configuration options are:

Community string

- Read Only — Indicates that the community members can view configuration information but cannot change any information.
- Read/Write — Indicates that the community members can view and modify configuration information.
- Super — Indicates that the community members have administration access.

Configurable IP address

If IP address is not configured, all community members with the same community name are granted the same access rights.

To configure SNMP station IP address and community string(s), perform the following:

1. At the console prompt, type `Enable`.

   The prompt is displayed as #.

2. Type `configure` and press Enter.

3. In configuration mode, type the SNMP configuration command with the parameters including community name (private), community access right (read and write) and IP address, as shown in the following example:

   console> `enable`

   console# `configure`

   config(config)# `snmp-server community private rw 192.168.1.2`

   config(config)# `exit`

   console(config)# `show snmp`

```
Community-String                Community-Access                View Name                       IP address

------------------              ------------------                                              ------------------

private                         readWrite                       default                         192.168.1.2


Community-String                Group name                      IP address                      Type


Traps are enabled.

Authentication-failure trap is
enabled.


Version 1,2 notifications

Target address____ Type         Community___ ____Version        Udp_____Filter                  To_____Retries

                                ___port_____name                sec

----------------_____-----      ------------_____------         ----_______-----               --_______--------


Version 3 notifications

Target address___Type           Username_______Security         Udp_____Filter                  To_____Retries

Level                           ____port_______name             sec

----------------____---------   ------------_______------       ----_______-----               --_______--------


SystemContact:

System Location:
```

This completes the initial configuration of the PC Blade Switch from the CLI. The configured parameters enable further configuration from any remote location.

Advanced Configuration

This section provides information about security management based on the Authentication, Authorization, and Accounting (AAA) mechanism, and includes the following topics:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

Security Management and Password Configuration

System security is handled through the AAA (Authentication, Authorization, and Accounting) mechanism that manages user access rights, privileges, and management methods. AAA uses both local and remote user databases. Data encryption is handled through the SSH mechanism.

The system is delivered with no default password configured; all passwords are user-defined. If a user-defined password is lost, you can invoke a password recovery procedure from the Startup menu. The procedure is applicable for the local terminal only and allows a one-time access to the device from the local terminal with no password entered.

Configuring Security Passwords Introduction

You can configure the security passwords can be configured for the following services:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

NOTE: Passwords are user-defined.

When creating a user name, privilege levels are “1” and “15” with the default priority being “1”, which allows access but not configuration rights. A priority of “15” must be set to enable access and configuration rights. Although user names can be assigned a privilege level of “15” without a password, this is not recommended. If there is no specified password, privileged users can access the Web interface with any password.

Configuring an Initial Console Password

To configure an initial console password, type the following commands:

console> `enable`

console# `configure`

console(config)# `aaa authentication login default line`

console(config)# `aaa authentication enable default line`

console(config)# `line console`

console(config-line)# `login authentication default`

console(config-line)# `enable authentication default`

console(config-line)# `password george`

When initially logging onto the PC Blade Switch through a console session, type `george` at the password prompt. When switching to Exec mode, type `george` at the password prompt.

Configuring an Initial Telnet Password

To configure an initial Telnet password, type the following commands:

console> `enable`

console# `configure`

console(config)# `aaa authentication login default line`

console(config)# `aaa authentication enable default line`

console(config)# `line telnet`

console(config-line)# `login authentication default`

console(config-line)# `enable authentication default`

console(config-line)# `password bob`

When initially logging onto the PC Blade Switch through a Telnet session, type `bob` at the password prompt. When switching to Exec mode, type `bob` at the password prompt.

Configuring an Initial SSH Password

To configure an initial SSH password, type the following commands:

console> `enable`

console# `configure`

console(config)# `ip ssh server`

console(config)# `line ssh`

console(config-line)# `login authentication default`

```
console(config-line)# enable authentication default

console(config-line)# password jones

console(config-line)# exit

console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line
```

NOTE: Use one of the following commands to generate either a DSA or RSA key pair. For more information on key generation, please see the CLI guide.

```
console(config)# crypto key generate dsa

console(config)# exit
```

Since this method uses the Default logon, a user name is not required. When initially logging onto the PC Blade Switch through an SSH session, type `jones` at the password prompt. When switching to Exec mode to enable, type `jones` at the password prompt.

NOTE: Configuring only the initial SSH password overrides the console. This means that the PC Blade Switch becomes unaccessible through the local serial console connection.

Configuring an Initial HTTP Password

To configure an initial HTTP password, type the following commands:

```
console# configure

console(config)# ip http authentication local

console(config)# username admin password user1 level 15
```

Configuring an Initial HTTPS Password

To configure an initial HTTPS password, type the following commands:

```
console# configure

console(config)# ip https authentication local

console(config)# username admin password user1 level 15
```

Type the following commands once to configure a console, a Telnet, or SSH to use with an HTTPS session.

```
console# configure

console(config)# crypto certificate generate key_generate

console(config)# ip https server
```

When initially enabling an http or https session, type `admin` for user name and `user1` for password.

NOTE: SSL 2.0 or higher must be enabled in the client browser for the HTTPS session to work properly.

HTTP and HTTPS services require level 15 access and connect directly to the configuration level access.

Software Download from a TFTP Server

This section contains instructions for downloading switch software (system and boot images) from a TFTP server. You must configure the TFTP server before beginning to download the software. This section contains the following topics:

- System Image Download
- Boot Image Download

System Image Download

The switch boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored. When a new image is downloaded, it is saved in the area allocated for the other system image copy. On the next boot, the switch decompresses and runs the currently active system image unless otherwise directed.

To download a system image from the TFTP server:

1. Ensure that an IP address is configured on one of the PC Blade Switch VLANs and the TFTP server can be pinged.
2. Make sure that the System Image file (.ros file) to download is saved on the TFTP server.
3. Type `show version` to verify which software version is currently running on the PC Blade Switch.

   The following is an example of the information that is displayed:

   console# `show version`

   SW version 1.0.1.9 (date 23-Apr-2006 time 11:27:53)

   Boot version 1.0.0.04 (date 06-Apr-2006 time 11:21:43)

   HW version 00.00.01
4. Type `show bootvar` to verify which system image is currently active.

   The following is an example of the information that is displayed:

   console# `show bootvar`

   Images currently available on the FLASH

   Image-1 active (selected for next boot)

   Image-2 not active

   console#
5. Type `copy tftp://{tftp address}/{file name} image` to copy the new system image to the PC Blade Switch.

When the new image is downloaded, it is saved in the area allocated for the "not active" system image (image-2, as given in the example). The following is an example of the information that is displayed:

console# `copy tftp://176.215.31.3/file1.ros image`

!!
!!!!!!!!!!!

Copy took 00:01:11 [hh:mm:ss]

NOTE: Exclamation points indicate that a copying process is in progress. Each symbol (!) corresponds to 512 bytes transferred successfully. A period indicates that the copying process timed out. Many periods in a row indicate that the copying process failed.

6. Type `boot system image-2` to select the image to use during next boot. (image-2, as given in the example).

   The following is an example of the information that is displayed:

   console# `boot system image-2`

   console#

7. Type `reload`.

   The following message is displayed:

   console# `reload`

   This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?

8. Type y to reboot the PC Blade Switch.

   The device reboots.

Boot Image Download

Loading a new boot image from the TFTP server and programming it into the flash updates the boot image. The boot image is loaded when the device is powered on.

To download a boot image to a TFTP server:

1. Ensure that an IP address is configured on one of the PC Blade Switch VLANs and the TFTP server can be pinged.

2. Ensure that the Boot Image file (rfb file) to download is saved on the TFTP server.

3. Type `show version` to verify which software version is currently running on the device.

   The following is an example of the information that is displayed:

   console# `show version`

   SW version 1.0.0.42 (date 22-Jul-2005 time 13:42:41)

   Boot version 1.0.0.18 (date 01-Jun-2005 time 15:12:20)

   HW version 00.00.01 (date 01-May-2005 time 12:12:20)

4. Type `copy tftp://{tftp address}/{file name} boot` to copy the boot image to the device.

   The following is an example of the information that is displayed:

   console# `boot copy tftp://176.215.31.3/332448-10018.rfb boot`

   !!

   Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]

5. Type `reload`.

   The following message is displayed:

   console# `reload`

   This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?

6. Type `y`.

   The device reboots.

Startup Menu Procedures

The procedures called from the Startup menu cover software flash handling and password recovery. The diagnostics procedures are for use by technical support personnel only and are not disclosed in this document. You can also enter the Startup menu when booting the PC Blade Switch.

To enter the Startup menu:

1. Turn the power on and watch for the auto-boot message.

   This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) n?

   y

   ****

   ************************************* SYSTEM RESET ***********************

   ****

   ----- Performing the Power-On Self Test (POST) -----

   ------ Performing the Power-On Self Test (POST) -----

   UART Channel Loopback Test........................PASS

   Testing the System SDRAM..........................PASS

   Boot1 Checksum Test...............................PASS

   Boot2 Checksum Test...............................PASS

   Flash Image Validation Test.......................PASS

FRU Validation Test.....PASS

BOOT Software Version x.x.x.xx Built 22-Jan-xxxx 15:09:28

I-Cache x KB. D-Cache x KB.

Cache Enabled.Autoboot in 2 seconds -press RETURN or Esc. to abort and enter prom.Preparing to decompress...

2. When the auto-boot message appears, press Enter to display the Startup menu.

   [1] Download Software

   [2] Erase Flash File

   [3] Password Recovery Procedure

   [4] Enter Diagnostic Mode

   [5] Set Terminal Baud-Rate

   Enter your choice or press 'ESC' to exit:

You can perform the Startup menu procedures using an ASCII terminal or Windows HyperTerminal. The following sections describe the available Startup menu options.

NOTE: When selecting an option from the Startup menu, you must take time must into account. If no selection is made within 10 seconds (default), the device times out. You can change this default value through the CLI.

Only technical support personnel can use Diagnostics Mode. For this reason, Diagnostics Mode is not described in this guide.

Downloading Software [Option 1]

This feature is not supported at this time.

Erasing the Flash File [Option 2]

In some cases, you must erase the PC Blade Switch configuration. If you erase the configuration, you must reconfigure all parameters configured using CLI, EWS, or SNMP.

To erase the device configuration:

1. Interrupt the boot sequence.
2. From the Startup menu, press 2 within two seconds to erase the flash file.

   The following message is displayed:

   Warning! About to erase a Flash file.

   Are you sure (Y/N)? y

3. Press y.

The following message is displayed.

Write Flash file name (Up to 8 characters, Enter for none.): `config`

File config (if present) will be erased after system initialization

======== Press Enter To Continue ========

4. Enter `config` as the name of the flash file.

   The configuration is erased and the PC Blade Switch reboots.

5. Repeat the initial PC Blade Switch configuration.

Password Recovery [Option 3]

If a password is lost, you can perform the password recovery procedure from the Startup menu. The password recovery procedure enables entry to the PC Blade Switch one time without a password.

To recover a lost password for the local terminal only:

▲ From the Startup menu, type `3` and press Enter.

The password is deleted.

NOTE: To ensure security, reconfigure passwords for all applicable management methods.

Enter Diagnostic Mode [Option 4]

For Technical Support only.

Set Terminal Baud-Rate [Option 5]

To set the terminal baud-rate:

1. From the Startup menu, type `5` and press Enter.
2. Enter your choice or press Esc to exit.
3. Press Enter.

   The baud-rate is set.

⚠ **WARNING!** If you change the terminal baud-rate, you must match these settings for the Integrated Administrator's internal serial link to the PC Blade Switch. To do so, while logged into the PC Blade Switch via the IA console, press Ctrl + Shift + _ then press C to Change Settings, then press R for Remote Port [Switch A]. From there you can adjust the Baud Rate and Flow Control. Note: As the default baud rate is set to 115200, there should be no reason to ever have to change these settings.

A Feature Summary

Switch Performance

- Non-blocking full wire speed architecture
- Store and forward mode layer 2 switching standard
- Auto-negotiation and auto-sensing with full-duplex support and ability to manually force port speed and duplex mode
- Auto-MDI/MDIX on all ports enabled with auto-negotiation
- 16K MAC addresses per switch with automatic MAC address learning
- ARP for IP to MAC address resolution

Switch Network Features

- IEEE 802.3 10Base-T Ethernet, IEEE 802.3u 100Base-TX Ethernet, and IEEE 802.3ab 1000Base-T Ethernet
- IEEE 802.1D, IEEE 802.s, and IEEE 802.w spanning tree protocol (mono-spanning tree)
- Spanning tree bypass fast forwarding mode on a per port basis (recommend disabling for CCI solutions)
- Spanning Tree RSTP-to-MSTP Compatibility feature (allows interoperability with PVST/PVST+) is enabled by default
- IEEE 802.3ad link aggregation (excluding LACP) supporting up to 8 multilink trunk groups with 8 ports per group; compatible with Cisco EtherChannel trunking (Fast EtherChannel, Gigabit EtherChannel)
- IEEE 802.1Q addressable VLAN ID range 1–4094
- IEEE 802.3ac VLAN Ethernet frame extensions for 802.1Q tagging on a per port basis
- Ports may be tagged or untagged members of a VLAN
- GARP VLAN registration protocol (GVRP) providing 802.1Q compliant VLAN pruning and dynamic VLAN creation
- IEEE 802.1p QoS with 8 classes of service mapped to 8 priority levels
- IGMP snooping v1 and v2
- IGMP state enabling and disabling on a per VLAN basis

- IGMP response report delay and query interval configuring
- Broadcast, multicast, and unknown packet storm control with a configurable threshold value
- IEEE 802.3x flow control with manual configuration capability

Switch Deployment and Configuration

- Supports any combination of HP bc1000, bc1500, bc2000, and bc2500 Blade PCs and future compatible blade PCs
- Default pre-configuration for immediate plug-in operation in the HP BladeSystem PC Blade Enclosure
- Communicate to any and all blade network adapters from any Ethernet external port
- Manage the switch from IA enclosure firmware
- Browser-based interface accessible from any switch Ethernet port
- Menu driven console interface accessible from any switch port
- Command line interface (CLI) with scripting capability accessible from any switch port
- Telnet access to the CLI and menu-driven console interfaces accessible from any switch Ethernet port
- SNMP-based scripting with best-case HP recommended example scripts
- Configurable forwarding MAC address aging (default is 300 seconds)
- MAC address user management sorting on a per port and per VLAN basis
- Manual (static) entries in MAC address table
- Manual, or automatic IP settings using a DHCP or BOOTP server
- Ability to restore switch to factory default settings
- TFTP to upload and download (save, restore, and update) the switch configuration
- Switch configuration retention after firmware upgrade
- Human read/write configuration file for viewing, printing, and editing
- Pre-configured customized port naming with respect to blade PC NIC connectivity
- Per port bandwidth control of ingress and egress traffic
- Ability to name ports on a per port basis
- Full ability to enable and disable any port (both internal and external ports)

Switch Diagnostics and Monitoring

- System and management status LEDs
- Per port speed and link activity LEDs adjacent to all external Ethernet ports
- Active virtual graphic in the browser-based switch interface
- Port mirroring with ability to mirror desired type of frames (egress, ingress, or both)
- Switch statistic monitoring, data packets received/transmitted, port error packets, packet size, trunk utilization, SNMP data, etc.
- System reporting such as port parameters and link status, switch asset information, configuration values, log entries, etc.
- Ping capability to test the connectivity on the Ethernet network
- SNMP v1, v2, v3 with four configurable community strings and SNMP trap manager hosts
- MIB-II, Bridge MIB, Interface MIB, Extended Bridge MIB, Ethernet-like MIB, Entity MIB
- Bridge, remote monitoring, and switch environmental traps
- Power on self test (POST) at boot for hardware verification
- Ability to return switch to a valid firmware image in case of firmware corruption
- Local system log (syslog) with ability to view and clear messages, and save (upload) as text file using TFTP

Switch Security

- Password protected multi-level user accounts supported on all management interfaces
- Configurable user interface idle time-out period
- Ability to disable browser-based access to the switch user interfaces
- 256 Port-based IEEE 802.1Q tagged VLANs per switch
- Ability to specify the IP-based management stations that are allowed to access the switch

Switch Ports Per PC Blade Enclosure

- Four external 10/100/1000T Gigabit Ethernet ports
- One external 10/100T Fast Ethernet port
- One external DB-9 serial port providing access to the Integrated Administrator
- 40 internal 10/100 Fast Ethernet ports to blade PC network adapters
- I2C Switch to management module communications
- All external Ethernet ports may be used for data, switch and Integrated Administrator management, and/or PXE remote configuration

- All internal Ethernet signals routed as Ethernet across individual CAT5e signal traces
- Five RJ-45 external Ethernet port connectors

Device Hardware Interfaces

RJ-45 Ports

RJ-45 ports are auto-sensing ports. When inserting a cable into an RJ-45 port, the switch automatically ascertains the maximum speed (10 or 100 or 1000 Mbps) and duplex mode (half- or full-duplex) of the attached device. All ports support only unshielded twisted-pair (UTP) cable terminated with an 8-pin RJ-45 plug.

To simplify the procedure for attaching devices, all RJ-45 ports support Auto MDIX. This technology allows attaching devices to the RJ-45 ports with either straight-through or crossover cables. When inserting a cable into the switch's RJ-45 port, the switch automatically:

- Senses whether the cable is a straight-through or crossover cable.
- Determines whether the link to the attached device requires a "normal" connection (such as when connecting the port to a PC) or an "uplink" connection (such as when connecting the port to a router, switch, or hub).
- Configures the RJ-45 port to enable communications with the attached device, without requiring user intervention. In this way, the Auto MDIX technology compensates for setting uplink connections, while eliminating concern about whether to use crossover or straight-through cables when attaching devices.

SFP GBIC Module

The GBIC module bays accommodate standard SFP GBIC modules, allowing fiber connections on the network. The GBIC port provides a link to a high-speed network or individual workstation at speeds of up to 1000Mbps.

The module bay is a combo port, sharing a connection with an RJ-45 port.

Combo Port

Each Fast Ethernet external port on the back panel is connected to a SFP GBIC port as combo ports which function as combo ports. Combo ports are single ports with two physical connections, SFP fiber and RJ-45 copper with only one type of connection that can be active at any given time. If both devices are plugged in, the two port that takes priority is defined through the CLI commands.

Index