Installationshandbuch
HP BladeSystem PC Blade Switch

Vierte Ausgabe (Februar 2009)

Dritte Ausgabe (September 2007)

Zweite Ausgabe (Mai 2007)

Erste Ausgabe (Mai 2007)

Dokumenten-Teilenummer: 413355-044

Allgemeines

Dieses Handbuch enthält Anleitungen für die Installation des HP BladeSystem PC Blade Switch.

⚠ **VORSICHT!** In dieser Form gekennzeichneter Text weist auf Verletzungs- oder Lebensgefahr bei Nichtbefolgen der Anleitungen hin.

△ **ACHTUNG:** In dieser Form gekennzeichneter Text weist auf die Gefahr von Hardwareschäden oder Datenverlust bei Nichtbefolgen der Anleitungen hin.

Inhaltsverzeichnis

1 Einführung

Die CCI (Consolidated Client Infrastructure)-Lösung verwendet einen 3U (5,25 Zoll) HP BladeSystem PC Blade-Baugruppenträger, der 20 HP Blade PCs und redundante Hot-Plug-Netzteile sowie Kühlung unterstützt. Der HP BladeSystem PC Blade-Baugruppenträger mit 20 HP Blade PCs enthält 40 10/100-MBit/s-Netzwerkadapter (NIC). Da die CCI-Lösungspakete viele HP Blade PCs auf kleinem Raum enthalten, wird die Anzahl der Netzwerkkabel schnell unübersichtlich.

Der PC Blade-Baugruppenträger umfasst einen Steckplatz für einen Verbindungsswitch, über den eine externe Ethernet-Verbindung hergestellt werden kann. Mit dem HP PC Blade Switch kann die Anzahl der Netzwerkkabel von 41 auf 1 reduziert werden. Dank weniger Kabel kann die CCI-Lösung auch schneller implementiert, verwaltet und instand gehalten werden. In diesem Installationshandbuch wird die Konfiguration des HP PC Blade Switch für Anwendungen beschrieben, die eine 100-MBit/s-Fast-Ethernet-Netzwerkadapter-Aggregation auf 10/100/1.000-MBit/s-Kupfer- oder 1.000-MBit/s-Glasfaser-Ethernet-Uplinks erfordern.

Switch-Verwaltung

Der HP BladeSystem PC Blade Switch ist ein Standard-Layer-2+-Ethernet-Switch, der wie jeder andere Standard-Ethernet-Switch konfiguriert und verwaltet werden kann.

In die Switch-Firmware sind eine browserbasierte Schnittstelle und eine Befehlszeilenschnittstelle (CLI) integriert, um den Switch verwalten und überwachen zu können. Darüber hinaus unterstützt der Switch den Telnet-Zugriff, das SSH (Secure Shell)-Protokoll, das SNMP (Simple Network Management)-Protokoll v1-v3 und RMNO (Remote Monitoring). Alle internen und externen Ports können einzeln deaktiviert, aktiviert, konfiguriert oder überwacht werden. Zugriff auf die Switch-Verwaltungsschnittstelle wird lokal über Integrated Administrator oder remote über jede beliebige konfigurierte, virtuelle LAN (VLAN)-Verwaltungsschnittstelle unterstützt.

Switch-Konfiguration

Sie können die Switch-Ports einzelnen deaktivieren oder aktivieren. Auto-MDI/MDIX mit automatischer Erkennung (Auto Negotiation) der Geschwindigkeit und des Duplexmodus wird unterstützt. Der PC Blade Switch umfasst folgende Ethernet-Ports:

- 41 dedizierte interne 10/100-MBit/s-Fast-Ethernet-Ports
- Fünf externe Ethernet-Ports für Daten
  - Vier Dual-Personality-Ethernet-Uplinks (Kupfer/Glasfaser) mit 10/100/1.000 MBit/s
  - Ein 10/100T-Fast-Ethernet-Port, der sich für die optionale Out-of-Band-Systemverwaltung eignet, aber auch als zusätzlicher Daten-Uplink verwendet werden kann

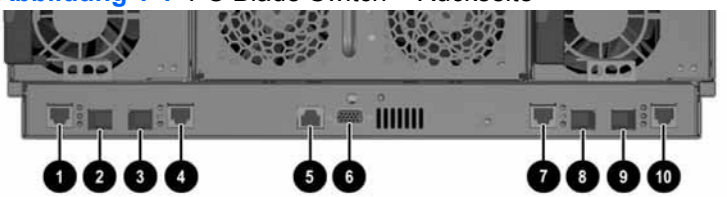
HP PC Blade-Baugruppenträger

Der HP PC Blade-Baugruppenträger unterstützt 20 HP Blade PCs, von denen jeder zwei eingebettete 10/100-MBit/s-Fast-Ethernet-Netzwerk-Controller enthält. Der primäre Netzwerk-Controller eines jeden Blade PCs unterstützt Pre-boot Execution Environment (PXE) und Wake-on-LAN (WoL). Jeder Baugruppenträger kann bis zu 40 aktive Netzwerkadapter gleichzeitig umfassen.

HP PC Blade Switch-Verbindungstray

Der PC Blade Switch hat die folgende Portkonfiguration:

Abbildung 1-1 PC Blade Switch – Rückseite



Nummer	Beschreibung
1	10/100/1.000T-RJ-45-Anschluss-Gigabit-Ethernet-Uplink, als Port 43 gekennzeichnet Combo-Port mit GBIC-Port rechts daneben
2	SFP (Small Form-Factor Pluggable)-GBIC-Port, als Port 43 gekennzeichnet Combo-Port mit RJ-45-Port links daneben
3	SFP (Small Form-Factor Pluggable)-GBIC-Port, als Port 44 gekennzeichnet Combo-Port mit RJ-45-Anschluss rechts daneben
4	10/100/1.000T-RJ-45-Anschluss-Gigabit-Ethernet-Uplink, als Port 44 gekennzeichnet Combo-Port mit GBIC-Port links daneben
5	10/100T-Fast-Ethernet-Port, der sich für die isolierte In-Band oder Out-of-Band-Integrated-Administrator-Verwaltung eignet, als Port 42 gekennzeichnet
6	Integrated Administrator-Konsolenanschluss, serieller DB-9-Anschluss (verwendet ein RS-232-Nullmodem-Kabel)
7	10/100/1.000T-RJ-45-Anschluss-Gigabit-Ethernet-Uplink, als Port 45 gekennzeichnet Combo-Port mit GBIC-Port rechts daneben
8	SFP (Small Form-Factor Pluggable)-GBIC-Port, als Port 45 gekennzeichnet Combo-Port mit RJ-45-Port links daneben
9	SFP (Small Form-Factor Pluggable)-GBIC-Port, als Port 46 gekennzeichnet Combo-Port mit RJ-45-Port rechts daneben
10	10/100/1.000T-RJ-45-Anschluss-Gigabit-Ethernet-Uplink, als Port 46 gekennzeichnet Combo-Port mit GBIC-Port links daneben

Interne Ports

Der HP PC Blade Switch verfügt über 40 zugewiesene, integrierte 10/100-MBit/s-Fast-Ethernet-„Downlink“-Ports, über die Signale des Blade PC-Netzwerkadapters an den Switch gesendet werden. Die Signale werden von den Blade PCs mit Ethernet über einzelne Signalwege der Kategorie 5e (CAT5e) zum passiven mittleren Bauträger des HP PC Blade-Baugruppenträgers weitergeleitet.

Für die Ethernet-Kommunikation wird Integrated Administrator (IA) über einen zusätzlichen internen 10/100-MBit/s-Fast-Ethernet-Port mit dem HP PC Blade Switch verbunden.

Externe Ports

Der HP PC Blade Switch verfügt über acht externe Ports, vier 10/100/1.000T-MBit/s-Ethernet-Uplink-Ports mit RJ-45-Ports, die dazu verwendet werden, den Switch mit der Netzwerkinfrastruktur zu verbinden, und vier SFP (Small Form-Factor Pluggable)-GBIC-Ports, die für Gigabit-Glasfaserverbindungen verwendet werden können. Diese Ports sind freigegebene „Combo“-Ports, wobei jeweils nur ein Medientyp verwendet werden kann. Combo-Ports sind einzelne Ports mit zwei physischen Verbindungen, RJ-45-Kupfer oder SFP. Falls beide Geräte angeschlossen sind, kann der prioritäre Port über die Switch-CLI definiert werden.

Darüber hinaus steht ein 10/100T-Fast-Ethernet-Port mit einem RJ-45-Anschluss für ein optionales, dediziertes Out-of-Band-Verwaltungsnetzwerk oder für lokale Administrations- und Diagnoseaufgaben zur Verfügung. Die dedizierten Uplinks können angeschlossen bleiben. Dieser Port eignet sich für die Netzwerkverwaltung, kann aber auch als zusätzlicher Daten-Uplink zum Netzwerk verwendet werden.

Systemverwaltung

Sicherung und Wiederherstellung

Der PC Blade Switch unterstützt das TFTP (Trivial File Transfer)-Protokoll, mit dem eine Kopie jeder Switch-Konfigurationsdatei hoch- bzw. heruntergeladen werden kann. Auf diese Weise können mehrere Switches mit ähnlichen Konfigurationen schnell implementiert sowie Funktionen zur Sicherung und Wiederherstellung von Daten bereitgestellt werden. Die Konfigurationseinstellungen können über die Benutzeroberflächen oder direkt in der Konfigurationsdatei geändert werden. Die Konfigurationsdatei kann jederzeit auf die werkseitigen Standardeinstellungen zurückgesetzt werden, indem die vorhandene Startkonfiguration gelöscht und der Switch anschließend neu gestartet wird.

Benutzer können Firmware-Aktualisierungen durchführen, indem sie das TFTP-Protokoll nach dem Start über einen externen Port verwenden. Die Durchführung von Firmware-Upgrades ist unkompliziert, da die Konfiguration des Switch nach einem Upgrade beibehalten und der von HP Support Paq automatisierte Firmware-Prozess für Windows-Einsatzstationen unterstützt wird.

IP-Adressen

Der PC Blade Switch erhält standardmäßig eine IP-Adresse von einem DHCP (Dynamic Host Configuration Protocol)- oder einem BOOTP (Bootstrap Protocol)-Server. Der Administrator kann manuell eine IP-Adresse über die CLI oder eine browserbasierte Schnittstelle zuweisen. In diesem Fall muss die neu zugewiesene IP-Adresse jedoch erneut verbunden werden. Zur Erhöhung der Sicherheit kann der Administrator die IP-basierten Verwaltungsstationen festlegen, die für den Zugriff auf den Switch zulässig sind.

Web-Browser-Schnittstelle

Benutzer können auf die browserbasierte Schnittstelle mit Internet Explorer oder Netscape Navigator über ein TCP/IP-Netzwerk zugreifen. Die browserbasierte Schnittstelle besteht aus zwei Fensterbereichen:

- Der linke Fensterbereich bzw. die Baumstruktur bieten einfache Navigation durch die Switch-Funktionen. Die Hauptzweige können erweitert werden und ermöglichen dadurch den Zugriff auf die Unterfunktionen.
- Im rechten Fensterbereich bzw. der Geräteansicht finden Sie Informationen über Ports, die aktuelle Konfiguration und den Status, Tabelleninformationen, Funktionsmerkmale und konfigurierbare Parameter.

Befehlszeile (CLI, Command Line Interface)

Über die CLI können wesentlich mehr Konfigurationsoptionen eingestellt werden als über die browserbasierte Schnittstelle. Sie haben drei Möglichkeiten, um auf diese Schnittstellen zuzugreifen:

- Lokal, über den RS-232-Konsolenanschluss am Switch-Tray, indem Sie sich bei Integrated Administrator anmelden und über den internen, seriellen Anschluss eine Verbindung zum PC Blade Switch herstellen.
- Virtueller serieller Remote-Zugriff auf den Switch über den Integrated Administrator und ein integriertes Konto. Stellen Sie remote über SSH oder Telnet eine Verbindung zum IA her. Geben Sie bei der entsprechenden Anmeldeaufforderung den Benutzernamen `switch` und das Kennwort `switcha` ein.
- Remote, indem Sie eine Telnet- oder SSH-Konsolensitzung (falls konfiguriert) verwenden.

SNMP und Remote Monitoring

Der Switch unterstützt Standard-SNMP-MIBs (Management Information Bases), HP Enterprise-MIB, SNMP v1 Traps und RMON1-Gruppen 1 (Ethernet-Statistiken), 2 (Verlauf), 3 (Alarme) und 9 (Ereignisse). Es können vier Community-Strings und SNMP-Trap-Manager-Hosts konfiguriert werden. Mit dieser Funktion kann der Switch remote über eine Netzwerkverwaltungsstation überwacht werden.

Switch-Sicherheit

Der Switch verwendet eine Layer-2-Zugriffssteuerungsliste oder Filterdatenbank, um das Netzwerk zu segmentieren, die Kommunikation zwischen den Segmenten zu steuern und eine Störungskontrolle zu ermöglichen. Der Switch ermöglicht die manuelle Eingabe von bestimmten MAC (Media Access Control)-Adressen, die aus dem Netzwerk gefiltert werden. Sowohl Unicast- als auch Multicast-Verkehr kann gefiltert werden. Die maximale Anzahl der erfassten MAC-Adressen pro Port kann zusätzlich eingeschränkt werden.

Der Switch umfasst mehrere zusätzliche Funktionen, die es dem Netzwerkadministrator ermöglichen, die Verwaltungsschnittstellen zu sichern. Diese Funktionen bieten die Möglichkeit, folgende Aufgaben durchzuführen:

- Konfigurieren mehrerer kennwortgeschützter Konten mit zwei Zugriffsebenen
- Festlegen der IP-basierten Verwaltungsstationen, die auf den Switch zugreifen können
- Auswählen der Remote-Zugriffsmethode und Festlegen des Leerlauftimeouts für die Benutzeroberfläche
- Konfigurieren der portbasierten IEEE 802.1Q-getaggten VLANs für die Servergruppierung und Datenisolation

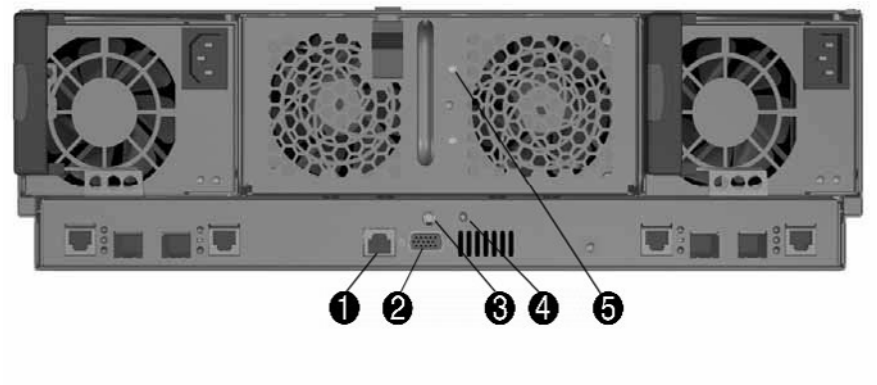
Bestimmen der Position der Integrated Administrator-Komponenten

Das HP PC Blade-Baugruppenträger-Verbindungstray wird mit dem vorinstallierten Integrated Administrator-Modul geliefert. Externe Verbindungen sind über die RJ-45- und RS-232-Anschlüsse an der Rückseite des Geräts möglich.

Anhand von externen LEDs können der Baugruppenträger- und Switch-Status sowie der Geschwindigkeits- und Verbindungsstatus der einzelnen Ethernet-Uplinks überprüft werden (siehe LEDs an der Rückseite des HP PC Blade Switch-Trays). Eine Funktion zur Notabschaltung des

Baugruppenträgers ist für den Fall vorhanden, dass durch den Switch oder eine andere Bauträgergruppenkomponente eine Überhitzung verursacht wird.

Abbildung 1-2 Externe LEDs und Anschlüsse am HP PC Blade-Integrated Administrator



Nummer	Beschreibung
1	Verwaltungsanschluss (10/100-Fast Ethernet) für den Remotezugriff über eine browserbasierte Benutzeroberfläche, Telnet oder SSH
2	Konsolenanschluss (DB-9 RS-232) für den lokalen Zugriff auf die Befehlszeile. (Erfordert ein entsprechendes Nullmodemkabel)
3	Reset-Taste für Integrated Administrator
4	LED für den Integrated Administrator-Zustand
5	UID (Enclosure Unit Identification)-LED

Switch-Wartung

Der Switch bietet viele zusätzliche Wartungs- und Diagnosefunktionen:

- Port-Spiegelung mit der Möglichkeit, die gewünschten Frametypen (Egress, Ingress oder beide) zu spiegeln
- Selbsttest beim Systemstart (POST) zur Hardware-Überprüfung
- Überwachen von Bildschirmen über die Benutzeroberflächen für die Portverwendung, empfangene/übertragene Datenpakete, Fehlerpakete, Paketgröße, Trunk-Verwendung, SNMP-Daten usw.
- Anzeigen von Systeminformationen, wie z. B. Portparameter und Verbindungsstatus, Switch-Bestandsinformationen, Konfigurationswerte, Protokolleinträge usw., über die Benutzeroberflächen
- „Ping“ und „Traceroute“-Funktionen zum Testen der Konnektivität im Ethernet-Netzwerk
- Lokales Systemprotokoll (syslog) mit der Möglichkeit, Mitteilungen anzuzeigen und zu löschen, die über TFTP als Textdatei gespeichert (hochgeladen) wurden.
- Anzeigen und Löschen von MAC-Adressen aus der weiterleitenden Datenbank, um Probleme mit dem Erfassen von MAC-Adressen und der Paketweiterleitung zu identifizieren
- Die Möglichkeit, ein Backup-Firmware-Image zu verwenden, falls die Firmware beschädigt ist

Detaillierte Informationen zu den Administrationsfunktionen des Switch finden Sie in den Benutzerhandbüchern zu PC Blade Switch.

Virtuelles LAN

Jeder Switch unterstützt bis zu 256 portbasierte IEEE 802.1Q-VLANs mit GVRP-dynamischer VLAN-Registrierung. Mitglieder eines VLANs können gemäß den IEEE 802.3ac-VLAN-Ethernet-Frameerweiterungen für 802.1Q-Tagging ungetaggte oder getaggte Ports sein. Daher können PC Blade Switch-VLANs weitere Switches anbinden, die 802.1Q-Tagging innerhalb der Netzwerkinfrastruktur unterstützen.

Spanning-Tree

Der Switch erfüllt das IEEE 802.1D-STP (Spanning Tree)-Protokoll zum Beheben möglicher Probleme, die durch redundante Netzwerkpfade verursacht wurden. Benutzer können für jeden Port STP-Switch-Parameter (z. B. Priorität und Kosten) konfigurieren. Jeder Switch kann die STP-Root-Bridge automatisch im Netzwerk ermitteln. Falls nicht, fungiert der Switch selbst als Root-Bridge für die STP-Domäne.

Der Spanning-Tree ist eine Standardanforderung für L2-Switches, die transparentes Bridging durchführen, um L2-Weiterleitungsschleifen automatisch verhindern bzw. aufheben zu können. Die Switches tauschen Konfigurationsmitteilungen unter Verwendung speziell formatierter Frames wie BPDUs (Bridge Protocol Data Units) aus, wodurch sich die Weiterleitung an Ports selektiv aktivieren bzw. deaktivieren lässt. Es wird ein Baum mit aktiven Leitwegen erstellt und sichergestellt, dass ein aktiver Pfad (eine Reihe von L2-Leitwegen) zwischen zwei beliebigen Geräten im Netzwerk ohne Schleifen vorhanden ist.

In einem LAN, das durch mehrere Bridges zusammengeschaltet ist, wählt der Spanning-Tree eine steuernde Root-Bridge und einen Port für das gesamte mit Bridges ausgelegte LAN sowie eine designierte Bridge und einen designierten Port für jedes einzelne LAN-Segment aus. Datenverkehr, der

von einer Endstation zu einer anderen Endstation im LAN fließt, wird über die designierte Bridge bzw. den designierten Port für das LAN-Segment bis zur Root-Bridge weitergeleitet, welche den Datenverkehr wiederum an die designierten Bridges/Ports der entgegengesetzten Seite weiterleitet. Bridges verwenden zur Weiterleitung der Spanning-Tree-Informationen BPDUs.

Während der „Classic“-Spanning-Tree, wie unter IEEE 802.1D definiert, L2-Weiterleitungsschleifen in einer allgemeinen Netzwerktopologie verhindert, kann es bis zu 50 Sekunden dauern, bis er „konvergiert“, d. h. bis jede Bridge bzw. jeder Switch im Netzwerk für jeden einzelnen Port entschieden hat, ob Datenverkehr weitergeleitet wird oder nicht. Die Reaktionszeit von 50 Sekunden ist für viele Anwendungen zu lang. Während dieser Zeit werden mögliche Schleifen erkannt, wobei der Zeitaufwand für die Verbreitung von Statusänderungen sowie für die Reaktion aller relevanten Geräte eingeplant wird.

In diesem Switch ist eine schnellere Konvergenz möglich, sofern es die Netzwerktopologie zulässt. RSTP (Rapid Spanning Tree) erkennt, wie Netzwerktopologien genutzt werden, und ermöglicht daher eine schnellere Konvergenz des Spanning-Tree – ohne Generierung von Weiterleitungsschleifen. In einem gut strukturierten Netzwerk beträgt die Rekonvergenzzeit weniger als eine Sekunde.

MSTP (Multiple Spanning Tree) ermöglicht die Gruppierung und Zuordnung von VLANs zu Spanning-Tree-Instanzen. Jede Spanning-Tree-Instanz hat eine unabhängige Topologie anderer Spanning-Tree-Instanzen. MSTP unterstützt mehrere Leitpfade für den Datenverkehr und ermöglicht somit einen Lastausgleich im Netzwerk sowie eine Fehlertoleranz.

Konvertierung von MSTP zu RSTP (PVST-Interoperatibilität)

Die Konvertierung von MSTP zu RSTP erweitert den MSTP-Standard (Multiple Spanning Tree Protocol), um eine begrenzte Interoperabilität mit anderen proprietären Per-VLAN-Spanning-Tree-Protokollen wie PVST/PVST+ von Cisco bereitzustellen. Wenn die MSTP-zu-RSTP-Konvertierung im HP PC Blade Switch aktiviert ist, ist die Konvertierung ein globaler Parameter, der auf alle Ports angewendet wird, bei denen die Spanning-Tree-Funktion aktiviert ist. Wenn diese Funktion aktiviert ist, werden die Switchport-Modi „Trunk“ und „General“ nicht unterstützt. Es wird eine Fehlermeldung angezeigt, wenn Sie versuchen, den Switchport-Modus für eine Schnittstelle in „Trunk“ oder „General“ zu ändern. Sind mehr als zwei VLANs erforderlich, können die vier primären Uplinks als individuelle Zugriffsports verwendet werden, wobei jedoch die Layer-2-Redundanz verloren geht. Falls mehr als zwei VLANs und Redundanz erforderlich sind, muss diese Funktion deaktiviert werden. HP empfiehlt die Verwendung von IEEE 802.1s-MSTPs (Multiple Spanning Trees) für Fälle, in denen Hochgeschwindigkeits-L2-Redundanz und Unterstützung für mehr als zwei VLANs erforderlich sind.

Wenn eine Spanning-Tree-BPDU empfangen wird, konvertiert der Switch diese BPDU in eine MSTP-BPDU und weist sie der entsprechenden MST-Instanz zu. Vor der Übermittlung einer MSTP-BPDU wird die BDU in eine RSTP-BPDU konvertiert. Falls der Switch mit einem anderen Switch verbunden ist, auf dem 802.1D ausgeführt wird, wird der RSTP-BPDU als STP-BPDU gesendet, wie in der IEEE-Spezifikation festgelegt.

Diese Funktion ist standardmäßig folgendermaßen konfiguriert:

- MSTP ist standardmäßig aktiviert
- VLAN 1 ist MST-Instanz 1 zugeordnet
- MSTP-zu-RSTP-Konvertierung ist aktiviert
- VLAN 2 ist MST-Instanz 2 zugeordnet
- VLAN 3-4093 ist MST-Instanz 15 zugeordnet

Instanz 0 ist für VLAN 4094 (Standard-VLAN zum Verwerfen aller Frames) reserviert

HINWEIS: Wenn MSTP-zu-RSTP aktiviert ist (wird standardmäßig aktiviert) und Sie versuchen, einen Switchport in den Modus „Trunk“ oder „General“ zu versetzen, wird folgende Fehlermeldung angezeigt: **Port <Number>, extension separated-bridge exist**. Weitere Informationen hierzu finden Sie in Paragraph 1 dieses Abschnitts.

Link-Aggregation

Der Switch erfüllt den IEEE-Standard 802.3ad zur statischen Zusammenfassung von Leitungen (außer LACP8). Gemäß diesem Standard können mehrere Leitungen zu einer einzigen logischen Leitung gebündelter Kapazität zusammengefasst werden.

Ports können in LAGs (Link Aggregated Groups) zusammengefasst werden. Innerhalb einer Gruppe müssen alle Ports auf dieselbe Geschwindigkeit und auf den Vollduplexmodus eingestellt sein. Ports in einer LAG (auch „aggregierter Link“ genannt) können unterschiedliche Medientypen (UTP/Glasfaser oder andere Fasertypen) aufweisen, vorausgesetzt, sie arbeiten mit der gleichen Geschwindigkeit und im Vollduplexmodus.

Aggregierte Links können manuell oder automatisch festgelegt werden, indem das LACP (Link Aggregation Control Protocol) für die relevanten Links aktiviert wird. Ein aggregierter Link wird vom System als einzelner logischer Port betrachtet und entsprechend den anderen Ports im System behandelt. Der aggregierte Link besitzt ähnliche Portattribute wie ein „normaler“ Port (Auto-Negotiation-Status, Geschwindigkeit usw.).

Jeder Switch unterstützt bis zu acht Multiport-Trunks mit bis zu acht Ports pro Trunk.

Internet Group Management Protocol

Ein Layer-2-Switch leitet standardmäßig Multicast-Frames an alle Ports des relevanten VLANs weiter, wobei das Frame wie ein Broadcast behandelt wird. Aus diesem Grund erhalten einige Ports möglicherweise irrelevante Frames, die nur von bestimmten Ports dieses VLAN benötigt werden.

Dies kann verhindert werden, indem eine explizite Systemkonfiguration durchgeführt oder der Inhalt von IGMP-Frames abgehört wird („Snooping“), wenn die IGMP-Frames über den Switch von Stationen an einen Upstream-Multicast-Router weitergeleitet werden. In diesem Fall kann der Switch Folgendes erkennen:

- Wo (an welchen Ports) sich Stationen befinden, die einer bestimmten Multicast-Gruppe angehören möchten
- Wo (an welchen Ports) sich Multicast-Router befinden, die Multicast-Frames senden

Auf Grundlage dieser Informationen können irrelevante Ports (Ports, bei denen sich keine Stationen für den Empfang einer bestimmten Multicast-Gruppe registriert haben) von der Weiterleitung eines eingehenden Multicast-Frames ausgeschlossen werden.

Der Switch bietet IGMP (Internet Group Management)-Protokoll-Snooping v1 und v2. Für diese Funktion kann ein Non-Querier-Modus (keine Versendung von Abfragen) konfiguriert werden. Der IGMP-Status kann für jedes einzelne VLAN aktiviert bzw. deaktiviert werden. Darüber hinaus kann eine Verzögerung der Antwortberichte und ein Abfrageintervall konfiguriert werden. Jeder Switch unterstützt maximal 191 Multicast-Gruppen (127 über IGMP dynamisch erfasste Gruppen und 64 statische Multicast-Gruppen).

Datensturmunterbindung

Bei der Übermittlung von L2-Frames werden alle Ports des jeweiligen VLAN mit Broadcast- und Multicast-Frames überflutet. Alle mit diesen Ports verbundenen Knoten akzeptieren diese Frames und versuchen, sie zu verarbeiten, wodurch in beiden Netzwerkleitungen und den Host-Betriebssystemen

eine Überlastung entsteht (da jeder einzelne Frame mindestens eine E/A-Unterbrechung verursacht, um zu entscheiden, ob dieser Frame auszuschließen ist).

Der Switch erlaubt konfigurierbare Schwellenwerte (in Paketen pro Sekunde), um drei Typen von Paketstürmen zu verhindern: Broadcast, Multicast und unbekannte Zieladresse. Bei Überschreitung des Schwellenwerts werden alle weiteren empfangenen Pakete verworfen.

Quality of Service

Das System aktiviert verschiedene Dienste zum Definieren bestimmter Verkehrsflüsse. Hierbei werden folgende Mechanismen verwendet:

- Klassifizierung — Bestimmte Felder im Paket werden spezifischen Werten zugewiesen. Alle mit den benutzerdefinierten Spezifikationen übereinstimmenden Pakete werden unter einer Kategorie (Fluss/Klasse) zusammengefasst.
- Aktionen — Verschiedene Aktionen, wie z. B. die Bearbeitung von Feldern im Paket (VPT, DSCP), Ingress Policing, Egress Scheduling und Egress Shaping können definiert werden. Die Aktionen werden auf alle Pakete in einem bestimmten Verkehrsfluss angewandt.

Warteschlangen unterstützen diese Aktionen, die sich auf die Bandbreitenverwaltung und -steuerung beziehen. Nachdem ein Paket klassifiziert wurde, wird es einer der Ausgabewarteschlangen zugewiesen. Das System unterstützt acht Warteschlangen pro Port. Das System verwaltet die Warteschlangen (entnimmt der Warteschlange Frames zur Übertragung) entsprechend den aktuellen vom Benutzer definierten Scheduling-Einstellungen. Diese Einstellungen bestimmen, aus welcher Warteschlange wie viele Frames verarbeitet werden, bevor eine andere Warteschlange verwaltet wird.

Es sind Systemeinrichtungen für die Zugriffssteuerung und CoS/QoS vorhanden, die vom Benutzer den Anforderungen entsprechend konfiguriert werden können. Die verfügbaren Konfigurationsmodi bieten dem Benutzer unterschiedliche Funktions- und Komplexitätsstufen.

HINWEIS: Es handelt sich hierbei um unterschiedliche Methoden zum Steuern und Konfigurieren der CoS/QoS-Einrichtungen des Systems, jedoch nicht um unterschiedliche Betriebsmodi der CoS/QoS-Einrichtungen.

Nachfolgend werden die verschiedenen CoS/QoS-Zugriffsmodi aufgeführt:

- Basismodus — Im CoS-Basismodus können die Frames nach Ingress-Schnittstelle oder dem Wert eines einzelnen Frame-Header-Feldes in weitgefasste Klassen unterteilt werden. Jede Klasse kann an eine bestimmte Egress-Warteschlange umgeleitet werden und die Parameter der Warteschlangenverwaltung können konfiguriert werden. Dies ist ausreichend, um relative Dienste nach Klasse bereitzustellen. Dieser Modus umfasst NICHT die Funktion zum Klassifizieren von Datenverkehr in feinkörnige Flüsse (z. B. Definieren eines Flusses als bestimmten Wert in Frame-Header-Feldern oder mehrerer Werte in verschiedenen Header-Feldern) und bietet keine Funktionen zum Messen von Datenverkehr.
- Erweiterter Modus — Im erweiterten CoS/QoS-Modus hat der Benutzer Zugriff auf alle verfügbaren CoS/QoS-Funktionen und muss diese ausdrücklich konfigurieren. Der Datenverkehr kann in weitgefasste Klassen oder in feinkörnige Flüsse unterteilt werden.

Mittels Quality of Service (QoS) IEEE 802.1p können Switch-Administratoren Prioritätsstufen zum Weiterleiten von Paketen für jeden Switch festlegen. Jeder Switch unterstützt vier Datenverkehrsklassen (Puffer oder Warteschlangen) zum Implementieren von Prioritäten basierend auf dem Prioritätstag des Pakets.

Administratoren können bis zu acht Prioritätsstufen zu vier Klassen zuordnen. Datenverkehr, der von einem bestimmten Blade PC-Port ausgeht, kann Priorität gegenüber Paketen anderer Geräte haben.

Beispiel: Wenn sich mehrere Pakete in einem Puffer befinden, wird das Paket mit der höchsten Priorität zuerst weitergeleitet, unabhängig davon, wann es empfangen wurde.

Leistungsmerkmale der Enterprise-Klasse

Der PC Blade Switch besitzt folgende Leistungsmerkmale:

- Ungeblocktes Full-Wire-Speed an allen Ports
- 16.000 MAC-Adressen pro Switch, mit automatischer Erfassung von MAC-Adressen
- 128 MB SDRAM, 16 MB Flash und 6 MB Paketpufferspeicher pro Switch (Paketpufferspeicher wird von allen Ports gemeinsam genutzt)

Fazit

Der HP BladeSystem PC Blade-Baugruppenträger ist ein 3U-Rack-montierbares Gerät, das 20 HP PC Blades mit redundantem Hot-Plug-Netzteil und Kühlung unterstützt. Der HP PC Blade-Baugruppenträger ist mit dem HP PC Blade Switch-Verbindungstray ausgestattet, das Ethernet-Konnektivität für HP Blade PCs ermöglicht. Mit dem HP PC Blade Switch kann die Anzahl der Netzwerkkabel an der Rückseite des Verbindungsswitch von 41 auf 1 reduziert werden.

Am Verbindungsswitch ist eine Integrated Administrator-Tochterkarte angeschlossen, über die der Zustand des Baugruppenträgers (Temperatur, Lüfter usw.), der Blade PCs und des Switch überwacht werden kann. Der Integrated Administrator bietet auch seriellen Zugriff auf den Verbindungsswitch.

Der Switch und der Integrated Administrator haben separate und unabhängige IP-Adressen. Die 20 PC-Blades, der Switch und der Integrated Administrator sind in einem einzigen Gehäuse untergebracht. Ein 42U-Rack kann bis zu 14 Gehäuse enthalten.

2 Erstmalige Installation

Wenn alle externen Verbindungen hergestellt sind, schließen Sie ein Terminal (mit Emulationssoftware) am externen seriellen DB-9 RS323-Port des Integrated Administrator an. Informationen zum Konfigurieren von Integrated Administrator finden Sie in der Dokumentation für den Integrated Administrator. Vergewissern Sie sich, dass die Terminal-Emulationssoftware folgendermaßen konfiguriert ist:

1. Externer serieller Port des Integrated Administrator: 9600 Baud.
2. Stellen Sie das Datenformat auf 8 Datenbits, 1 Stopp-Bit und keine Parität ein.
3. Wählen Sie unter **Flow Control** (Flusskontrolle) die Option „Keine“.
4. Wählen Sie unter **Properties** (Eigenschaften) den Emulationsmodus „VT100“.
5. Wählen Sie Terminal-Tasten für Funktionstasten, Pfeiltasten und die Strg-Taste aus. Vergewissern Sie sich, dass Sie die Einstellung für Terminal-Tasten (nicht für Windows-Tasten) vornehmen.

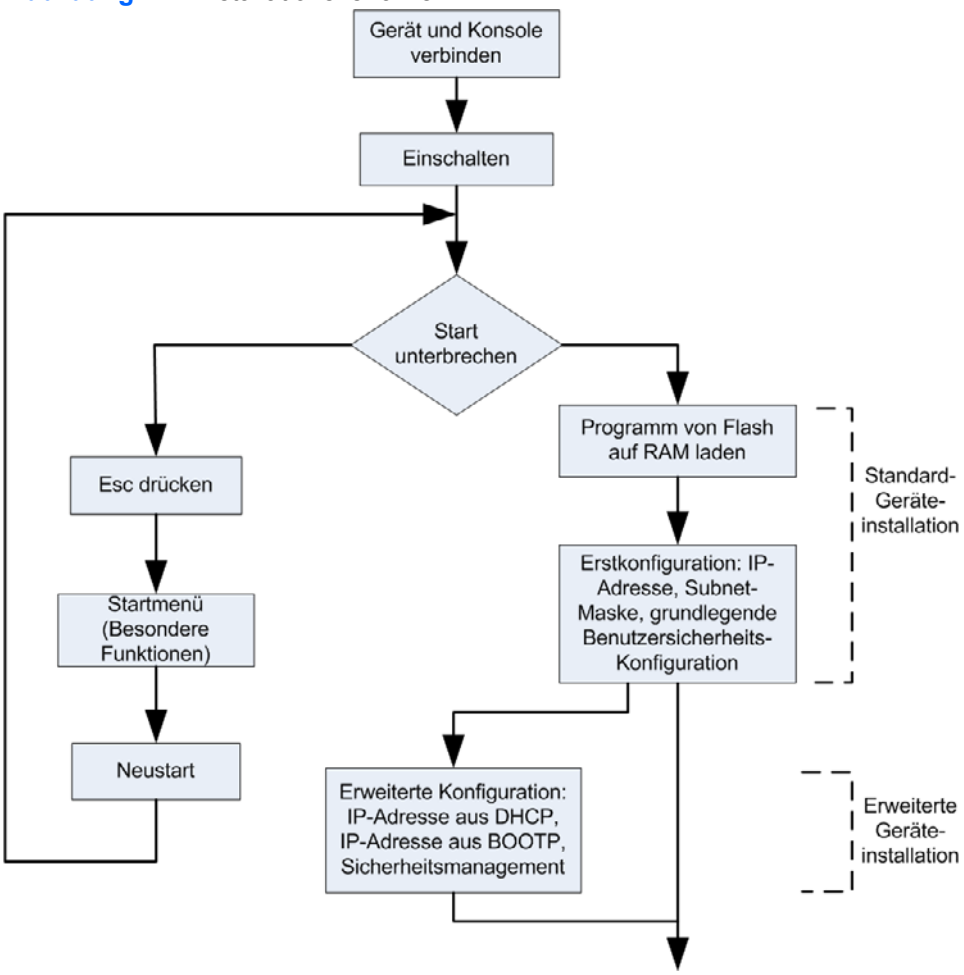
HINWEIS: Wenn Sie HyperTerminal in Verbindung mit Microsoft Windows 2000 verwenden, muss Windows 2000 Service Pack 2 oder höher installiert sein. Unter Windows 2000 Service Pack 2 funktionieren die Pfeiltasten in der HyperTerminal-VT100-Emulation einwandfrei. Weitere Informationen zu Service Packs für Windows 2000 finden Sie unter http://www.microsoft.com.

Installationsverfahren

Die Reihenfolge der Installations- und Konfigurationsmaßnahmen ist in der folgenden Abbildung dargestellt. Für die Erstkonfiguration wird die Standard-Gerätekonfiguration ausgeführt.

Die Ausführung anderer Funktionen wird weiter unten in diesem Abschnitt beschrieben.

Abbildung 2-1 Installationsverfahren



Starten des PC Blade Switch

Der PC Blade Switch wird automatisch gestartet, sobald eines oder mehrere der Baugruppenträger-Netzteile angeschlossen sind. Die voraussichtlichen Startinformationen lauten folgendermaßen:

- Der PC Blade Switch wird mit einer Standardkonfiguration geliefert, die sich von einem typischen Distributions- oder Edge-Switch unterscheidet.
- Der Standard-Benutzername für die Web-Management-Schnittstelle des Blade Switch ist „admin“. Hinweis: Wenn Sie die Verbindung zum Switch über Integrated Administrator herstellen, ist kein Benutzername erforderlich.
- Es ist kein Standardkennwort festgelegt.

Da der PC Blade Switch automatisch gestartet wird, müssen Sie zum Anzeigen des POST-Startprozesses den Switch über seine Befehlszeilenschnittstelle neu starten. Dazu muss eine Verbindung mit dem IA über den lokalen seriellen Port bestehen. Führen Sie die folgenden Befehle über die IA Eingabeaufforderung aus, um eine Verbindung zur Befehlszeilenschnittstelle für den Switch herzustellen und den Switch neu zu starten.

So starten Sie den Switch über die Befehlszeilenschnittstelle neu:

1. Geben Sie hinter der Eingabeaufforderung `connect switch a` ein.

   Daraufhin wird Folgendes angezeigt:

   ```
   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. Drücken Sie zweimal die Eingabetaste, um die Switch-Konsole anzuzeigen.
3. Geben Sie `enable` hinter der Eingabeaufforderung **console>** ein.
4. Geben Sie `reload` hinter der Eingabeaufforderung **console#** ein.
5. Geben Sie `Y` ein, wenn Sie gefragt werden, ob Sie ohne Speichern der Änderungen fortfahren möchten.

Der PC Blade Switch durchläuft den Selbsttest beim Systemstart (POST). Der Selbsttest beim Systemstart wird bei jedem Neustart des PC Blade Switch ausgeführt. Bei diesem Test werden Hardware-Komponenten überprüft, um zu ermitteln, ob das Gerät vor dem Start vollständig betriebsbereit ist. Falls ein kritisches Problem erkannt wird, wird der Programmablauf unterbrochen und die Switch-LED leuchtet rot. Bei erfolgreicher Ausführung des Selbsttests wird ein Image in den RAM geladen. Fehler- bzw. Erfolgsmeldungen des Selbsttests beim Systemstart werden auf dem Terminal angezeigt.

Beim Starten des PC Blade Switch berechnet der Starttest zunächst die Speicherverfügbarkeit und fährt dann mit dem Startvorgang fort. Folgendes wird auf dem POST-Bildschirm angezeigt (Beispiel):

```
------ 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...
```

Der Startvorgang dauert ungefähr 60 Sekunden. Wenn am Ende des POST die Meldung „Auto-Boot“ (Automatischer Start) angezeigt wird (siehe letzte Zeilen), war der Startvorgang fehlerfrei. Während des Startvorgangs können über das Startmenü bestimmte Vorgänge ausgeführt werden. Um das Startmenü aufzurufen, drücken Sie innerhalb von zwei Sekunden, nachdem die Meldung „Auto-Boot“ (Automatischer Start) angezeigt wurde, die Esc-Taste oder die Eingabetaste.

Sofern der Systemstart nicht durch Drücken der Esc-Taste oder der Eingabetaste unterbrochen wird, wird die Firmware dekomprimiert und in den RAM geladen.

Nach erfolgreichem Laden des PC Blade Switch wird eine Eingabeaufforderung angezeigt. Bevor Sie fortfahren, vergewissern Sie sich, dass die neueste Firmware-Version installiert ist. Ist dies nicht der Fall, laden Sie sie herunter, und installieren Sie sie. Weitere Informationen zum Herunterladen der neuesten Version finden Sie unter „Software Download“ [Option 1].

Konfigurationsübersicht

In der Regel müssen für die Verwendung des PC Blade Switch keine Änderungen an der Standardkonfiguration vorgenommen werden. Falls sie doch geändert werden muss, lesen Sie folgende Informationen.

HINWEIS: Wenn Sie Konfigurationsänderungen vorgenommen haben, müssen Sie die neue Konfiguration speichern, bevor Sie einen Neustart ausführen. Um die Konfiguration zu speichern, geben Sie in der Eingabeaufforderung (**console#**) den Befehl `Copy Running-config Startup-config` ein, und bestätigen die Eingabe.

Erstkonfiguration

HINWEIS: Bevor Sie fortfahren, lesen Sie die Versionshinweise für dieses Produkt.

Die Erstkonfiguration, die nach dem erfolgreichen Start des PC Blade Switch initialisiert wird, umfasst die Konfiguration einer statischen IP-Adresse und einer Subnetz-Maske. Darüber hinaus wird der Benutzername und die Berechtigungsstufe für die Remote-Verwaltung festgelegt. Wenn Sie das Gerät über eine SNMP-basierte Verwaltungsstation verwalten, müssen Sie auch SNMP-Community-Strings konfigurieren.

Für die Erstkonfiguration wird Folgendes vorausgesetzt:

- Der PC Blade Switch wird zum ersten Mal konfiguriert und befindet sich in dem gleichen Zustand, in dem Sie ihn erhalten haben.
- Der PC Blade Switch wurde erfolgreich gestartet.

- Es besteht eine serielle Verbindung und die Konsoleneingabeaufforderung wird auf dem Bildschirm eines VT100-Terminals angezeigt. (Drücken Sie mehrmals die Eingabetaste, um zu überprüfen, ob die Eingabeaufforderung richtig angezeigt wird.)
- Der PC Blade Switch ist nicht mit einem Benutzernamen und Kennwort konfiguriert.

Die Erstkonfiguration des PC Blade Switch erfolgt über den seriellen Port. Nach der Erstkonfiguration können Sie den PC Blade Switch entweder über den bereits verbundenen seriellen Port oder remote über eine Schnittstelle verwalten, die während der Erstkonfiguration definiert wurde.

Die Erstkonfiguration umfasst folgende Aufgaben:

- Festlegen des Benutzernamens als `TBD` und des Kennworts als `TBD` mit der höchsten Prioritätsstufe (15)
- Konfigurieren der statischen IP-Adresse und des Standard-Gateways
- Konfigurieren der SNMP-Lese/Schreib-Community-Strings

Erfragen Sie vor dem Konfigurieren des Gerätes die folgenden Informationen vom Netzwerkadministrator:

- Die IP-Adresse für die VLAN-1-Schnittstelle, über die das Gerät verwaltet werden soll
- Die IP-Subnetz-Maske für das Netzwerk
- Das Standard-Gateway
- Die Lese/Schreib-SNPM-Community-Strings

Statische IP-Adresse und Subnetz-Maske

Bevor Sie dem PC Blade Switch eine statische IP-Adresse zuweisen, rufen Sie folgende Informationen ab:

- IP-Adresse, die dem PC Blade Switch zur Konfiguration zugeordnet wurde
- Netzwerkmaske für das Netzwerk
- Standard-Gateway

Sie können die IP-Schnittstellen in jedem VLAN des Switch konfigurieren. Nachdem Sie die Konfigurationsbefehle eingegeben haben, stellen Sie sicher, dass das VLAN mit der IP-Adresse konfiguriert wurde, indem Sie den Befehl `enable show ip interface` eingeben. Die Befehle zum Konfigurieren des PC Blade Switch sind VLAN-spezifisch.

Um den PC Blade Switch über ein Remote-Netzwerk zu verwalten, müssen Sie eine Schnittstelle mit einer gültigen Adresse und Maske konfigurieren, also eine IP-Adresse, an die Pakete gesendet werden, wenn in den Switch-Tabellen keine Einträge gefunden werden.

Um eine statische Adresse zu konfigurieren, geben Sie den Befehl in die Eingabeaufforderung des Systems ein, wie im nachfolgenden Konfigurationsbeispiel gezeigt. Für dieses Beispiel gilt:

- 192.168.1.123/24 ist die jeweilige Verwaltungsstation.
- Die IP-Adresse ist im entsprechenden VLAN definiert.
- Das Standard-Gateway ist als 192.168.1.1 definiert.

VLAN 1 enthält die ungeraden Portnummern 1-41, 42, 45 und 46. VLAN 2 enthält die geraden Portnummern 2-40, 43 und 44.

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`

Überprüfen der IP-Adressen und der Standard-Gateway-Adressen

Vergewissern Sie sich, dass die IP-Adresse und das Standard-Gateway ordnungsgemäß zugewiesen wurden, indem Sie den Befehl „show ip interface“ (IP-Schnittstelle anzeigen) ausführen und die Befehlsausgabe überprüfen:

```
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
```

Benutzername

Verwenden Sie einen Benutzernamen, um das Gerät remote zu verwalten, z. B. über SSH, Telnet oder die browserbasierte Schnittstelle. Wenn Sie den PC Blade Switch mit Administratorrechten ausführen möchten, legen Sie die höchste Berechtigungsstufe fest.

HINWEIS: Nur der Administrator mit der höchsten Berechtigungsstufe (15) ist dazu berechtigt, den PC Blade Switch über die browserbasierte Schnittstelle zu verwalten.

Weitere Informationen zu Berechtigungsstufen finden Sie im CLI-Benutzerhandbuch.

Der konfigurierte Benutzername wird als Anmeldename für Remote-Verwaltungssitzungen eingegeben. Um den Benutzernamen und die Berechtigungsstufe zu konfigurieren, geben Sie den Befehl in die Systemeingabeaufforderung ein, wie im folgenden Konfigurationsbeispiel gezeigt.

console> `enable`

console# `configure`

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

SNMP-Community-String

SNMP (Simple Network Management Protocol) stellt eine Methode zum Verwalten von Netzwerkgeräten bereit. Das SNMP-Protokoll unterstützende Geräte führen lokale Software (Agenten) aus. Die SNMP-Agenten verwalten eine Liste der Variablen, die zur Verwaltung des Geräts verwendet werden. Die Variablen werden in der MIB (Management Information Base) definiert. Die MIB enthält die vom Agenten gesteuerten Variablen. Der SNMP-Agent definiert das Format für die MIB-Spezifikation sowie das Format, das für den Zugriff auf Informationen über das Netzwerk verwendet wird. Die Zugriffsrechte für die SNMP-Agenten werden über Zugriffsstrings und SNMP-Community-Strings gesteuert.

Der PC Blade Switch ist SNMP-konform und enthält einen SNMP-Agenten, der eine Reihe von Standard-MIB-Variablen und privaten MIB-Variablen unterstützt. Entwickler von Verwaltungsstationen müssen die genaue Struktur des MIB-Baums kennen und alle privaten MIBs empfangen, um sie verwalten zu können. Alle Parameter können über jede beliebige SNMP-Verwaltungsplattform verwaltet werden, mit Ausnahme der IP-Adresse und der Community (Community-Name und Zugriffsrechte) der SNMP-Verwaltungsstation. Der SNMP-Verwaltungszugriff auf den Switch wird deaktiviert, wenn keine Community-Strings vorhanden sind.

HINWEIS: Der Switch wird mit dem schreibgeschützten Community-String PUBLIC geliefert, für den kein Kennwort konfiguriert ist. Standardmäßig sind keine Community-Strings mit Schreibzugriff konfiguriert.

Sie können den Community-String, den Community-Zugriff und die IP-Adresse während der Erstkonfiguration über die Switch-CLI konfigurieren.

Folgende SNPM-Konfigurationsoptionen stehen zur Verfügung:

Community-String

- Optionen für Zugriffsrechte:
  - ro (read-only, schreibgeschützt)
  - rw (read-and-write, Lese-/Schreibzugriff)
  - su (super, Administratorzugriff)
- Eine Option zum Konfigurieren der IP-Adresse: Falls keine IP-Adresse konfiguriert ist, erhalten alle Community-Mitglieder mit dem gleichen Community-Namen die gleichen Zugriffsrechte.

In der Regel werden zwei Community-Strings verwendet: eine (öffentliche Community) mit schreibgeschütztem Zugriff und eine (private Community) mit Lese-/Schreibzugriff. Der öffentliche String ermöglicht autorisierten Verwaltungsstationen, MIB-Objekte abzurufen. Der private String ermöglicht autorisierten Verwaltungsstationen, MIB-Objekte abzurufen und zu bearbeiten.

Wenn Sie das Gerät zum ersten Mal konfigurieren, empfiehlt HP, die Konfiguration gemäß den Anforderungen des Netzwerkadministrators in Übereinstimmung mit der Verwendung einer SNMP-basierten Verwaltungsstation durchzuführen. Im Verlauf der Erstkonfiguration können Sie den Community-String, den Community-Zugriff und die IP-Adresse über die Switch-CLI festlegen.

Folgende SNPM-Konfigurationsoptionen stehen zur Verfügung:

Community-String

- Read Only (Schreibgeschützt) — Gibt an, dass die Community-Mitglieder Konfigurationsinformationen anzeigen, aber nicht ändern können
- Read/Write (Lese-/Schreibzugriff) — Gibt an, dass die Community-Mitglieder Konfigurationsinformationen anzeigen und ändern können
- Super (Administratorzugriff) — Gibt an, dass die Community-Mitglieder Administratorzugriff haben

Konfigurierbare IP-Adresse

Falls keine IP-Adresse konfiguriert ist, erhalten alle Community-Mitglieder mit dem gleichen Community-Namen die gleichen Zugriffsrechte.

Um die IP-Adresse und Community-Strings der SNMP-Station zu konfigurieren, führen Sie folgende Schritte aus:

1. Geben Sie in der Eingabeaufforderung der Konsole den Wert `Enable` (Aktivieren) ein.

   Die Eingabeaufforderung wird als # angezeigt.

2. Geben Sie `configure` (Konfigurieren) ein, und drücken Sie die Eingabetaste.

3. Geben Sie im Konfigurationsmodus den SNMP-Konfigurationsbefehl mit den Parametern Community-Name (privat), Community-Zugriffsrechte (Lese-/Schreibzugriff) und die IP-Adresse ein, wie im folgenden Beispiel gezeigt:

   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              Standard           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
Stufe                        ____port_______name        sec
----------------____---------  -----------_______------  ----_______-----       --_______--------

SystemContact:
System Location:
```

Hiermit ist die Erstkonfiguration des PC Blade Switch über die CLI abgeschlossen. Die konfigurierten Parameter ermöglichen die erweiterte Konfiguration über einen beliebigen Remote-Standort.

Erweiterte Konfiguration

Dieser Abschnitt enthält Informationen zum AAA (Authentifizierung, Autorisierung und Accounting)-Mechanismus im Rahmen der Sicherheitsverwaltung. Außerdem werden hier folgende Themen behandelt:

- Konsole
- Telnet
- SSH
- HTTP
- HTTPS

Sicherheitsverwaltung und Kennwortkonfiguration

Die Systemsicherheit wird über den AAA (Authentifizierung, Autorisierung und Accounting)-Mechanismus realisiert, der eine Verwaltung der benutzerspezifischen Zugriffsrechte, Berechtigungen und Verwaltungsmethoden ermöglicht. AAA greift hierbei auf lokale und remote installierte Benutzerdatenbanken zurück. Die Datenverschlüsselung erfolgt über den SSH-Mechanismus.

Das System wird ohne vorkonfiguriertes Standard-Kennwort geliefert. Sämtliche Kennwörter sind benutzerseitig definiert. Falls ein benutzerdefiniertes Kennwort verloren geht, kann über das Startmenü eine Prozedur zur Kennwortwiederherstellung aufgerufen werden. Diese Prozedur, die am lokalen Terminal verfügbar ist, bietet die Möglichkeit, von diesem Terminal aus einmalig ohne Kennworteingabe auf das Gerät zuzugreifen.

Konfigurieren von Sicherheitskennwörtern – Einführung

Für folgende Dienste können Sicherheitskennwörter konfiguriert werden:

- Konsole
- Telnet
- SSH

- HTTP
- HTTPS

HINWEIS: Kennwörter sind benutzerdefiniert.

Bei der Einrichtung eines Benutzernamens wird standardmäßig die Priorität 1 vereinbart (d. h. einfacher Zugang ohne Konfigurationsrechte). Um Gerätzugriffe mit Konfigurationsrechten zu ermöglichen, muss die Priorität 15 festgelegt werden. Es ist zwar grundsätzlich möglich, einem Benutzer die Berechtigungsstufe 15 zuzuweisen, ohne ein Kennwort festzulegen, die Kennwortvergabe wird aber empfohlen. Wenn kein Kennwort vorhanden ist, können Benutzer mit entsprechenden Berechtigungen die Web-Schnittstelle ohne Kennworteingabe aufrufen.

Konfigurieren eines ersten Terminal-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes Terminal-Kennwort zu konfigurieren:

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`

Wenn Sie sich erstmalig über eine Konsolensitzung beim PC Blade Switch anmelden, geben Sie bei der Kennwort-Eingabeaufforderung `george` ein. Wenn Sie in den Ausführungsmodus wechseln, geben Sie bei der Kennwort-Eingabeaufforderung `george` ein.

Konfigurieren eines ersten Telnet-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes Telnet-Kennwort zu konfigurieren:

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`

Wenn Sie sich erstmalig über eine Telnetsitzung beim PC Blade Switch anmelden, geben Sie bei der Kennwort-Eingabeaufforderung `bob` ein. Wenn Sie in den Ausführungsmodus wechseln, geben Sie bei der Kennwort-Eingabeaufforderung `bob` ein.

Konfigurieren eines ersten SSH-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes SSH-Kennwort zu konfigurieren:

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`

HINWEIS: Verwenden Sie einen der folgenden Befehle, um entweder ein DSA- oder ein RSA-Schlüsselpaar zu generieren. Weitere Informationen zur Schlüsselgenerierung finden Sie im CLI-Benutzerhandbuch.

console(config)# `crypto key generate dsa`

console(config)# `exit`

Da bei dieser Methode die Standardanmeldung verwendet wird, ist kein Benutzername erforderlich. Wenn Sie sich erstmalig über eine SSH-Sitzung beim PC Blade Switch anmelden, geben Sie bei der Kennwort-Eingabeaufforderung `jones` ein. Wenn Sie in den Ausführungsmodus wechseln, geben Sie bei der Kennwort-Eingabeaufforderung `jones` ein.

HINWEIS: Beim Konfigurieren des ersten SSH-Kennworts wird die Konsole überschrieben. Dies bedeutet, dass der PC Blade Switch nicht mehr über die lokale, serielle Konsolenverbindung zugänglich ist.

Konfigurieren eines ersten HTTP-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes HTTP-Kennwort zu konfigurieren:

console# `configure`

console(config)# `ip http authentication local`

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

Konfigurieren eines ersten HTTPS-Kennworts

Geben Sie die folgenden Befehle ein, um ein erstes HTTPS-Kennwort zu konfigurieren:

console# `configure`

console(config)# `ip https authentication local`

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

Geben Sie die nachfolgenden Befehle einmalig ein, wenn Sie eine Konsole, Telnet oder SSH zur Verwendung mit einer HTTPS-Sitzung konfigurieren möchten.

console# `configure`

console(config)# `crypto certificate generate key_generate`

console(config)# `ip https server`

Wenn Sie eine HTTP- oder HTTPS-Sitzung erstmalig aktivieren, geben Sie `admin` als Benutzername und `user1` als Kennwort ein.

HINWEIS: SSL 2.0 oder höher muss im Client-Browser aktiviert sein, damit die HTTPS-Sitzung ordnungsgemäß ausgeführt wird.

Eine Nutzung der Dienste HTTP und HTTPS ist nur auf Zugriffsebene 15 sowie bei direkter Anbindung an den Konfigurationszugang möglich.

Software-Download von einem TFTP-Server

Dieser Abschnitt enthält Anleitungen zum Herunterladen der Switch-Software (System- und Boot-Images) über einen TFTP-Server. Vor dem Herunterladen der Software muss der TFTP-Server konfiguriert werden. Dieser Abschnitt behandelt die folgenden Themen:

- Herunterladen des System-Image
- Herunterladen des Boot-Image

Herunterladen des System-Image

Der Switch wird gestartet und ausgeführt, wenn das System-Image aus dem Flash-Speicherbereich, wo eine Kopie des System-Image gespeichert ist, dekomprimiert wird. Beim Herunterladen eines neuen Image wird dieses in einem Bereich gespeichert, der für eine weitere Kopie des System-Image vorgesehen ist. Beim nächsten Startvorgang dekomprimiert und startet der Switch vom derzeit aktiven System-Image, falls nicht anders festgelegt.

So laden Sie ein System-Image vom TFTP-Server herunter:

1. Stellen Sie sicher, dass an einem der VLANs des PC Blade Switch eine IP-Adresse konfiguriert ist und Ping-Befehle an einen TFTP-Server gesendet werden können.
2. Die herunterzuladende System-Image-Datei (.ros-Datei) muss auf dem TFTP-Server gespeichert sein.
3. Geben Sie den Befehl `show version` ein, um die derzeitige Versionsnummer der Gerätesoftware zu überprüfen.

Es werden beispielsweise folgende Informationen angezeigt:

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. Geben Sie den Befehl `show bootvar` ein, um festzustellen, welches System-Image derzeit aktiv ist.

   Es werden beispielsweise folgende Informationen angezeigt:

   console# `show bootvar`

   Images currently available on the FLASH

   Image-1 active (selected for next boot)

   Image-2 not active

   console#

5. Geben Sie den Befehl `copy tftp://{TFTP-Adresse}/{Dateiname} image` ein, um ein neues System-Image auf den PC Blade Switch zu kopieren.

   Nach dem Herunterladen des neuen Image wird es in dem Bereich gespeichert, der für das „nicht aktive" System-Image vorgesehen ist (im Beispiel image-2). Es werden beispielsweise folgende Informationen angezeigt:

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

   !!

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

HINWEIS: Ausrufezeichen zeigen den Fortschritt des Kopiervorgangs an. Jedes Ausrufezeichen (!) entspricht 512 Byte übertragener Daten. Ein Punkt zeigt an, dass das Zeitlimit für den Kopiervorgang überschritten wurde. Viele Punkte in einer Reihe zeigen an, dass der Kopiervorgang fehlgeschlagen ist.

6. Wählen Sie das Image für den nächsten Start aus, indem Sie den Befehl `boot system image-2` eingeben (im Beispiel image-2).

   Es werden beispielsweise folgende Informationen angezeigt:

   console# `boot system image-2`

   console#

7. Geben Sie den Befehl `reload` ein.

Die folgende Meldung wird angezeigt:

console# `reload`

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

8. Geben Sie y ein, um den PC Blade Switch neu zu starten.

   Das Gerät wird neu gestartet.

Herunterladen des Boot-Image

Zum Aktualisieren des Boot-Image wird ein neues Boot-Image vom TFTP-Server geladen und in den Flash-Speicher programmiert. Das Boot-Image wird bei eingeschaltetem Gerät geladen.

So laden Sie ein Boot-Image vom TFTP-Server herunter:

1. Stellen Sie sicher, dass an einem der VLANs des PC Blade Switch eine IP-Adresse konfiguriert ist und Ping-Befehle an einen TFTP-Server gesendet werden können.

2. Die herunterzuladende Boot-Image-Datei (.rfb-Datei) muss auf dem TFTP-Server gespeichert sein.

3. Geben Sie den Befehl `show version` ein, um die derzeitige Versionsnummer der Gerätesoftware zu überprüfen.

   Es werden beispielsweise folgende Informationen angezeigt:

   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. Geben Sie den Befehl `copy tftp://{TFTP-Adresse}/{Dateiname} boot` ein, um ein neues Boot-Image auf das Gerät zu kopieren.

   Es werden beispielsweise folgende Informationen angezeigt:

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

   !!!

   Copy: 2.739.187 bytes copied in 00:01:13 [hh:mm:ss]

5. Geben Sie den Befehl `reload` ein.

   Die folgende Meldung wird angezeigt:

   console# `reload`

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

6. Geben Sie y ein.

Das Gerät wird neu gestartet.

Startmenü-Prozeduren

Über das Startmenü lassen sich verschiedene Prozeduren für Software-Downloads, die Flash-Handhabung und die Wiederherstellung von Kennwörtern aufrufen. Die Diagnoseprozeduren sind nur für die Mitarbeiter des technischen Supports vorgesehen und werden im vorliegenden Dokument daher nicht näher beschrieben. Sie können das Startmenü während des Starts von PC Blade Switch aufrufen.

So rufen Sie das Startmenü auf:

1. Schalten Sie das Gerät ein, und achten Sie auf die Selbststartmeldung.

```
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. Wenn die Selbststartmeldung angezeigt wird, drücken Sie die Eingabetaste, um das Startmenü anzuzeigen.

```
[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:

Sie können die Startmenü-Prozeduren über einen ASCII-Terminal oder einen Windows-HyperTerminal ausführen. In den folgenden Abschnitten werden die verfügbaren Startmenüoptionen beschrieben.

HINWEIS: Beachten Sie bei der Auswahl einer Option im Startmenü folgende Zeitbeschränkung: Erfolgt die Optionsauswahl nicht innerhalb von 10 Sekunden (Standard), läuft das Gerätezeitlimit ab. Dieser Standardwert kann über die CLI geändert werden.

Der Diagnosemodus kann nur von Mitarbeitern des technischen Supports aktiviert werden. Der Diagnosemodus wird daher in diesem Handbuch nicht näher beschrieben.

Downloading Software [Option 1] (Software herunterladen [Option 1])

Diese Funktion wird derzeit nicht unterstützt.

Erasing the Flash File [Option 2] (Flash-Datei löschen [Option 2])

In einigen Fällen muss die Konfiguration des PC Blade Switch gelöscht werden. Nach dem Löschen der Konfiguration müssen alle über CLI, EWS oder SNMP konfigurierten Parameter neu konfiguriert werden.

So löschen Sie die Gerätekonfiguration:

1. Unterbrechen Sie die Boot-Sequenz.
2. Drücken Sie im Startmenü innerhalb von zwei Sekunden auf [2], um die Flash-Datei zu löschen.

   Die folgende Meldung wird angezeigt:

   Warning! About to erase a Flash file.

   Are you sure (Y/N)? `y`
3. Drücken Sie die Taste y.

   Die folgende Meldung wird angezeigt:

   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. Geben Sie `config` als Namen für die Flash-Datei ein.

   Die Konfiguration wird gelöscht, und der PC Blade Switch wird neu gestartet.
5. Wiederholen Sie die Erstkonfiguration des PC Blade Switch.

Password Recovery [Option 3] (Kennwort wiederherstellen [Option 3])

Falls ein Kennwort verloren geht, können Sie die Prozedur zur Kennwortwiederherstellung über das Startmenü aufrufen. Die Prozedur zur Kennwortwiederherstellung ermöglicht einen einmaligen Zugriff auf den PC Blade Switch ohne vorherige Kennworteingabe.

So stellen Sie ein verloren gegangenes Kennwort wieder her (nur für das lokale Terminal):

▲ Geben Sie im Startmenü `3` ein, und drücken Sie die Eingabetaste.

Das Kennwort wird gelöscht.

HINWEIS: Um die Gerätesicherheit sicherzustellen, müssen die Kennwörter für alle relevanten Verwaltungsmethoden neu konfiguriert werden.

Enter Diagnostic Mode [Option 4] (Diagnosemodus aufrufen [Option 4])

Nur für den technischen Support.

Set Terminal Baud-Rate [Option 5] (Terminal-Baudrate festlegen [Option 5])

So legen Sie die Baudrate des Terminals fest:

1. Geben Sie im Startmenü `5` ein, und drücken Sie die Eingabetaste.
2. Wählen Sie eine Menüoption, oder drücken Sie die Esc-Taste, um das Menü zu verlassen.
3. Drücken Sie die Eingabetaste.

   Die Baudrate wurde festgelegt.

VORSICHT! Wenn Sie die Baudrate des Terminals ändern, müssen Sie dieselben Einstellungen auch für die interne serielle Verbindung von Integrated Administrator zu PC Blade Switch vornehmen. Führen Sie zu diesem Zweck folgende Schritte aus: Melden Sie sich bei PC Blade Switch über die IA-Konsole an, drücken Sie die Tasten Strg + Umschalt + _, und drücken Sie anschließend C für „Change Settings“ (Einstellungen ändern) und R für „Remote Port“ [Switch A]. Daraufhin können Sie die Baudrate und die Flusskontrolle anpassen. Hinweis: Da die Baudrate standardmäßig auf 115.200 eingestellt ist, müssen diese Einstellungen normalerweise nicht geändert werden.

A Funktionsübersicht

Switch-Leistung

- Ungeblockte Full-Wire-Speed-Architektur
- Speicher- und Weiterleitungsmodus Layer-2-Switching-Standard
- Auto-Negotiation und Auto-Sensing mit Vollduplexbetrieb und der Möglichkeit, die Port-Geschwindigkeit und den Duplexmodus manuell zu ändern
- Auto-MDI/MDIX mit aktivierter Auto-Negotiation an allen Ports
- 16.000 MAC-Adressen pro Switch, mit automatischer Erfassung von MAC-Adressen
- ARP für die Auflösung von IP- zu MAC-Adresse

Switch-Netzwerkfunktionen

- IEEE 802.3 10Base-T Ethernet, IEEE 802.3u 100Base-TX Ethernet und IEEE 802.3ab 1.000Base-T Ethernet
- IEEE 802.1D, IEEE 802.s und IEEE 802.w Spanning-Tree-Protokoll (Mono-Spanning-Tree)
- Spanning Tree Bypass Fast Forwarding-Modus auf Portbasis (Deaktivierung für CCI-Lösungen wird empfohlen)
- Spanning-Tree-Funktion RSTP-zu-MSTP-Kompatibilität (ermöglicht Interoperabilität mit PVST/PVST+) ist standardmäßig installiert
- IEEE 802.3ad Link-Aggregation (außer LACP); unterstützt bis zu 8 Multilink-Trunk-Gruppen mit 8 Ports pro Gruppe; kompatibel mit Cisco EtherChannel-Trunking (Fast EtherChannel, Gigabit EtherChannel)
- IEEE 802.1Q adressierbarer VLAN ID-Bereich 1 – 4094
- IEEE 802.3ac-VLAN Ethernet-Frame-Erweiterungen für 802.1Q-Tagging auf Portbasis
- Ports können getaggte oder ungetaggte Mitglieder eines VLANs sein
- GARP-VLAN-Registrierungsprotokoll (GVRP); unterstützt ein 802.1Q-konformes VLAN Pruning und eine dynamische VLAN-Generierung
- IEEE 802.1p-QoS mit 8 Dienstklassen, die 8 Prioritätsstufen zugeordnet sind
- IGMP-Snooping v1 und v2
- IGMP-Status – Aktiviert oder deaktiviert IGM-Snooping für einzelne VLANs

- Konfigurieren der IGMP-Antwortberichtsverzögerung und des IGMP-Abfrageintervalls
- Kontrolle über Broadcast- und Multicaststürme und unbekannte Pakete mit einem konfigurierbaren Schwellenwert
- IEEE 802.3x-Flusskontrolle, die manuell konfiguriert werden kann

Switch-Installation und -Konfiguration

- Unterstützt jede beliebige Kombination aus HP bc1000-, bc1500-, bc2000- und bc2500-Blade PCs und zukünftigen, kompatiblen Blade PCs
- Standardkonfiguration für den sofortigen Einsatz im HP BladeSystem PC Blade-Baugruppenträger
- Verbindung zu allen Blade-Netzwerkadaptern über einen beliebigen, externen Port
- Verwalten des Switch mit IA-Baugruppenträger-Firmware
- Browserbasierte Schnittstelle, die über jeden Switch-Ethernet-Port zugänglich ist
- Menübasierte Konsolenschnittstelle, die über jeden Switch-Port zugänglich ist
- Befehlszeile (CLI) mit Skriptfunktionen, die über jeden Switch-Port zugänglich ist
- Telnet-Zugriff auf die CLI und menübasierte Konsolenschnittstellen, die über jeden Ethernet-Port zugänglich sind
- SNMP-basierte Skriptfunktionen mit von HP empfohlenen Beispielskripts
- Konfigurierbares Altern von weiterleitenden MAC-Adressen (Standard ist 300 Sekunden)
- MAC-Adressen-Benutzerverwaltung auf Port- und VLAN-Basis
- Manuelle (statische) Einträge in der MAC-Adressen-Tabelle
- Manuelle oder automatische IP-Einstellungen über einen DHCP- oder BOOTP-Server
- Wiederherstellen der Switch-Standardeinstellungen
- TFTP zum Hoch- und Herunterladen (Speichern, Wiederherstellen und Aktualisieren) der Switch-Konfiguration
- Beibehaltung der Switch-Konfiguration nach dem Firmware-Upgrade
- Konfigurationsdatei mit Lese-/Schreibzugriff zum Anzeigen, Drucken und Bearbeiten
- Vorkonfigurierte, benutzerdefinierte Portbenennung mit Bezug auf Blade PC-NIC-Verbindungen
- Portbasierte Bandbreitenkontrolle des Ingress- und Egress-Verkehrs
- Möglichkeit, Ports individuell zu benennen
- Möglichkeit, jeden beliebigen Port zu aktivieren (sowohl interne als auch externe Ports)

Switch-Diagnose und -Monitoring

- LEDs für System- und Verwaltungsstatus
- Portbasierte LEDs für die Portgeschwindigkeit und Verbindungsaktivität aller externen Ethernet-Ports
- Aktive virtuelle Grafik in der browserbasierten Schnittstelle
- Port-Spiegelung mit der Möglichkeit, die gewünschten Frametypen (Egress, Ingress oder beide) zu spiegeln
- Monitoring von Switch-Statistiken, empfangene/übertragene Datenpakete, Port-Fehlerpakete, Paketgröße, Trunk-Verwendung, SNMP-Daten usw.
- Systeminformationen zu Portparametern und Verbindungsstatus, Switch-Bestandsinformationen, Konfigurationswerte, Protokolleinträge usw.
- Ping-Befehle zum Testen der Konnektivität im Ethernet-Netzwerk
- SNMP v1, v2, v3 mit vier konfigurierbaren Community-Strings und SNMP-Trap-Manager-Hosts
- MIB-II, Bridge MIB, Interface MIB, Extended Bridge MIB, Ethernet-like MIB, Entity MIB
- Bridge, Remote Monitoring und Switch-Umgebungs-Traps
- Selbsttest beim Systemstart (POST) zur Hardware-Überprüfung
- Möglichkeit, zu einem gültigen Firmware-Image zu wechseln, falls die Firmware beschädigt ist
- Lokales Systemprotokoll (syslog) mit der Möglichkeit, Mitteilungen anzuzeigen, zu löschen und über TFTP als Textdatei zu speichern (hochzuladen)

Switch-Sicherheit

- Kennwortgeschützte Multi-Level-Benutzerkonten, die in allen Verwaltungsschnittstellen unterstützt werden
- Konfigurierbares Leerlauftimeout der Benutzeroberfläche
- Möglichkeit, den browserbasierten Zugriff auf Switch-Benutzeroberflächen zu deaktivieren
- 256 portbasierte IEEE 802.1Q-getaggte VLANs pro Switch
- Möglichkeit, die IP-basierten Verwaltungsstationen festzulegen, die zum Zugreifen auf den Switch berechtigt sind

Switch-Ports pro PC Blade-Baugruppenträger

- Vier externe 10/100/1.000T-Gigabit-Ethernet-Ports
- Ein externer 10/100T-Fast-Ethernet-Port
- Ein externer serieller DB-Port für den Zugriff auf Integrated Administrator
- 40 interne 10/100-Fast-Ethernet-Ports für Blade PC-Netzwerkadapter
- I2C-Switch für Management-Modulverbindungen

- Alle externen Ethernet-Ports können für die Datenverwaltung, Switch-Verwaltung und Integrated Administrator-Verwaltung und/oder für die PXE-Remote-Konfiguration verwendet werden
- Alle internen Ethernet-Signale werden als Ethernet über individuelle CAT5e-Signalwege weitergeleitet
- Fünf externe RJ-45-Port-Anschlüsse

Gerätehardware-Schnittstellen

RJ-45-Ports

RJ-45-Ports sind Autosensing-Ports. Wenn Sie ein Kabel an den RJ-45-Port anschließen, erkennt der Switch automatisch die maximale Portgeschwindigkeit (10, 100 oder 1.000 MBit/s) und den Duplexmodus (Halb- oder Vollduplex) des angeschlossenen Geräts. Alle Ports unterstützen ausschließlich UTP (Unshielded Twisted-Pair)-Kabel mit einem 8-Pin-RJ-45-Stecker.

Um die Prozedur zum Anschließen von Geräten zu vereinfachen, unterstützen alle RJ-45-Ports Auto-MDIX. Mit dieser Technologie können Geräte an RJ-45-Ports mit durchgehenden oder gekreuzten Kabeln angeschlossen werden. Wenn Sie ein Kabel an den RJ-45-Port anschließen, führt der Switch automatisch folgende Aufgaben aus:

- Erkennt, ob das angeschlossene Kabel durchgehend oder gekreuzt ist
- Bestimmt, ob die Verbindung mit dem angeschlossen Gerät eine „normale“ Verbindung (z. B. beim Verbinden des Ports mit einem PC) oder eine „Uplink“-Verbindung (z. B. beim Verbinden des Ports mit einem Router, einem Switch oder einem Hub) erfordert.
- Konfiguriert den RJ-45-Port, um die Verbindungen mit dem angeschlossenen Gerät ohne Benutzereingriff zu aktivieren. Auf diese Weise kompensiert die Auto-MDIX-Technologie das Einrichten von Uplink-Verbindungen und nimmt dem Benutzer die Entscheidung ab, durchgehende oder gekreuzte Kabel zu verwenden.

SFP-GBIC-Modul

Die GBIC-Modulschächte sind mit SFP-GBIC-Modulen ausgestattet, die Glasfaserverbindungen im Netzwerk ermöglichen. Der GBIC-Port stellt eine Verbindung zu einem Hochgeschwindigkeitsnetzwerk oder einer individuellen Workstation bei einer Geschwindigkeit von 1.000 MBit/s bereit.

Der Modulschacht ist ein Combo-Port, der sich eine Verbindung mit einem RJ-45-Port teilt.

Combo-Port

Jeder externe Fast-Ethernet-Port an der Rückseite ist mit einem SFP-GBIC-Port verbunden, der wie ein Combo-Port funktioniert. Combo-Ports sind einzelne Ports mit zwei physischen Verbindungen, SFP-Glasfaser und RJ-45-Kupfer, mit nur einem Verbindungstyp, der zu jeder bestimmten Zeit aktiv sein kann. Falls beide Geräte angeschlossen sind, wird der prioritäre Port über die CLI-Befehle definiert.

Index