Total Systems Integration, Inc.
"Tying it all Together"

PO Box 0687, 1263 State Route 598
Gallon, Ohio 44833-0687
(419) 468-1855
(419) 462-1606 FAX

May 9, 2012

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street
Charleston, WV 25305-0130
Attention: Krista Ferrell
(305) 558-2596

George Dallas
President

(419) 544-1331
georgedallas@total-systems.net

Dear Ms. Ferrell

Total Systems Integration (TSI), Inc. and Hewlett Packard (HP) are pleased to have the opportunity to respond to ISCM0112 RFP. The proposed HP networking products are high quality and high performance, and can help The State of West Virginia Office of Technology achieve enhanced productivity, increased business agility and greater competitive advantage. Key differentiators of the proposed HP networking solution include:

- Lower cost of ownership: The proposed HP networking products, featuring industry-leading warranties with technical support and software upgrades, are engineered for high reliability to industry-standard specifications. No need for expensive Cisco *SmartNet* contracts.
- Product lifecycle management: Our team will work with you to ensure that you are informed of product roadmaps and are able to address end-of-life product issues in a proactive fashion. This will enable the West Virginia Broadband Technology Opportunities Program to maintain a consistent and predictable network infrastructure.
- End-to-end solution: HP can deliver world-class, standards based, networking products, plus deployment and maintenance services
- High Performance, non-blocking Networking equipment, with up to 66% lower TCO with unmatched price/performance, lower power and cooling costs, and reduced complexity and no license costs.

TSI and HP are committed to your project's success and we are confident that our solution addresses your critical business requirements. We look forward to meeting with you to review our capabilities, to discuss the benefits of our proposed solution and to explore the next steps in creating a strong and mutually beneficial business relationship.

You can reach me at (419) 544-1331 or georgedallas@total-systems.net.

Sincerely,

George Dallas

George Dallas

President

Executive Summary

Introduction

Total Systems Integration and Hewlett-Packard Company (HP) appreciate the opportunity to present WVOT with an HP networking solution in response to the Green Bank Observatory Network Upgrade RFP ISCM0112. We understand the technical and business requirements of WVOT and this proposal response will demonstrate the depth of HP's expertise as a world-class network solution provider. The proposal will highlight a comprehensive HP networking product portfolio that includes competitively priced, fully featured, Ethernet Enterprise Switch, that will meet your business needs. In addition, HP offers WVOT the flexibility to choose just the right level of maintenance. Our proposal includes a Five (5) Year, 24 x 7 x 4 ON-SITE warranty with software upgrades, and technical support. In addition we have included a block of hours that can be used to train existing maintenance staff and to assist in the installation and configuration of the system.

Meeting Business Requirements

HP has created a global networking powerhouse and is changing the rules of networking. It is raising the bar through innovation to deliver a differentiated portfolio of edge to core and data center networking solutions, complemented by global service and support capabilities. This expanded portfolio delivers best-in-class solutions that enable clients to harness the power of convergence and accelerate business growth at a lower total cost of ownership. In the updated version of research and advisory firm Gartner Inc.'s 2011 Magic Quadrant for Enterprise LAN (Global)[1], HP is positioned in the Leaders quadrant.

HP is in a unique position to deliver on the promise of the Broadband Initiative Infrastructure, with advanced technology, broad innovation, unparalleled expertise in technology services and enterprise services, and our broad partner ecosystem. Here are some of the benefits that WVOT can realize with an HP networking solution.

- **Open standards-based networking** facilitates incremental migration and leverages the existing expertise of trained network engineers and partners. Allows customer-focused innovation and interoperability instead of vendor lock-in, allowing a choice of best-in-class products and solutions with each purchase.
- **Comprehensive interoperability with tools, best practices and expertise** ensures that you can take advantage of HP networking solutions incrementally with no disruption in existing operations and no rip and replace. This allows customers to evolve networks in a deliberate and safe fashion.
- **Better energy efficiency is achieved** with technologies like variable-speed fans and front-to-back cooling. Our solutions complement HP data center smart grid technologies by driving higher utilization and reducing hardware needs as well as power and cooling requirements.
- **Best- in-class solutions working with industry-leading partners** ("HP AllianceONE") has been pretested and configured to run either within the network fabric infrastructure or by way of dedicated platforms. These include Unified Communications and Collaboration (UC&C) partners like Microsoft, Avaya, and Aastra, application delivery partners, like Riverbed and F5, and a variety of security partners for fast time-to-value.
- **Leading warranties** across our entire Enterprise Networking portfolio contribute to significantly lower Total Cost of Ownership (TCO) and reduce reliance on expensive support contracts.
- **HP FlexNetwork architecture,** the only converged networking architecture that spans from the virtualized data center to the virtual workplace for cloud, multimedia, and mobile services with integrated security solutions. It is the only end-to-end networking architecture that solves legacy network challenges by delivering the scale, security, and manageability needed for cloud-based, video-centric, mobile applications.
- **A fully converged and secure network fabric across voice, video, and data.** Optimized for application delivery and integrated with leaders in application networking, unified communications and other areas, customers can quickly and cost-effectively deploy application services across the extended enterprise.

- **Single-pane-of-glass management deeply integrated with industry-leading IT orchestration software** offers seamless heterogeneous network management and provisioning linked directly to end-user and business demands. HP networking solutions are also integrated with solutions from HP Software to facilitate top-to-bottom management and orchestration across the infrastructure.
- **Secure unified wired and wireless solutions** deliver a seamless experience managed from a single pane of glass across the entire secure campus LAN and branch network.
- **"Intelligent edge capability"** offers centralized command and control at the network edge delivering central policy control to reduce management and security overhead, fewer layers of network hierarchy, and higher throughput and a more efficient network.

HP is transforming networking by delivering a complete portfolio of innovative products, solutions, and services designed to meet the complexities faced by enterprise customers.

The portfolio, with superior technology, delivers a dramatically simpler network infrastructure, flexible application-centric environment, open standards, and proven interoperability to dramatically lower total cost of ownership.

HP customers will better align their application and service delivery needs with user demands across their entire extended enterprise.

By changing the rules of networking and driving toward a converged infrastructure, HP will help free up scarce resources to allow customers to invest in innovation that will drive their IT and business forward.

Customers tell us that the single-vendor paradigm has left their current network infrastructures too complex, too rigid, and too expensive. In addition, emerging compute and delivery models like virtualization and cloud computing are driving even stronger needs for heightened security and IT flexibility.

But because the current status quo left IT with a legacy and proprietary networking environment, many IT organizations lack the ability or resources to address rapid business change.

Moreover, Cisco proposals force organizations to contemplate a complete network and infrastructure refresh—with further **proprietary lock-in** and costly investments and without a coherent vision across network infrastructure, security, and management.

The opportunity has never been better for HP to change the rules of networking by bringing superior technologies and proven deployment experience to a $40B (USD) market.

HP is the only company to offer a full portfolio of standards-based, integrated solutions and services developed specifically to solve the complexities of the extended enterprise. As part of a converged infrastructure solution, HP will help customers dramatically simplify their networks, deliver business services more flexibly, and aggressively contain costs to open up new opportunities for business growth and fulfill the promise of a unified, converged IT infrastructure.

HP's family of data center networking solutions is a dramatically more flexible and scalable alternative to Cisco's Nexus portfolio for a virtualization-enabled, converged infrastructure.

HP's portfolio provides unique features for simpler network designs and reduces the cost of ownership with better energy efficiency and stronger management.

Customers can now build a complete standards-based core-to-edge, non-blocking network with a dramatically streamlined architecture requiring fewer systems and staff and delivering a much lower TCO across both CapEx and OpEx.

Meeting RFQ Requirements

Our fully compliant proposal addresses your technology upgrade needs with HP's best of breed Networking Products.

We provided our 10500 series Layer-3 Core switch with Full Advanced IP Premium Routing software and non-blocking switching fabric. The 10500 series is equipped with four switch fabrics, six 2000 watt power supplies and can be equipped with a variety of networking interfaces from 10 Gbps Copper and Fiber to 1000 Mbps Copper and Fiber.

The 10500 greatly exceed the capabilities of the RFP's Cisco switch in terms of Capacity, Performance, Power Consumption, Price and Total Cost of Ownership.

The HP 10500 Switch Series is one of the central building blocks of the HP FlexFabric Solution. As part of the HP Converged Infrastructure strategy, the HP 10500 series delivers high performance, core switching to the HP FlexNetwork architecture.

The HP 10500 series provides low-latency, high-density 1G/10G ports.

The HP 10500 Switch Series provides an unmatched list of features from L2, L3 IPv4 Unicast/Multicast, L3 IPv6 Unicast/Multicast, MPLS, MPLS VPNs, and VPLS, all features included, **without the cost of a complex software licensing model**. Coupled to the HP Intelligent Resilient Framework (IRF), which allows four chassis to be aggregated into a virtual switching fabric (up to 128 10GE line rate from L2 up to VPLS), the HP 10500 Switch Series combines simpler data center designs with the highest level of resiliency in the industry.

The HP 10500 Switch Series is ideal for data center core and broadband network backbones. With its extremely low latency, deep buffering, and 10GbE port density, the HP 10500 Switch Series is capable of handling even the most demanding network traffic loads.

The HP 10500 is 40GbE and 100GbE ready.

HP's IRF is a superior technology versus the Cisco vPC. IRF provides true virtualization of physical devices by unifying the control plane and simplifying management. Cisco's vPC on the other hand maintains two separate control planes and two separate complex configurations. IRF also scales to four devices whereas vPC is limited to two.

HP IRF can be used across up to four 10500 chassis, providing massive scalability with up to 512 10GbE ports in a single logical device.

We provided our 6600 Series 10 Gbe Router with Full Advanced IP Premium Routing software.

HP routers are built with an advanced architecture, modular platform, flexible applications, embedded security, and high performance capabilities that make them some of the best alternative routers in the market.

HP routers run on the same operating system as HP switches, WLAN, and security products, and are managed by HP Intelligent Management Center (IMC), a key differentiator compared to Cisco. HP routers provide additional services through open architecture that allows integrated applications such as WAN optimization and voice application.

HP is the #2 router vendor globally and, with its broad product offering, is the only company that can directly compete with Cisco. Routers are sold to the enterprise or as managed services offered by service providers (SPs) or system integrators (SIs).

Some key points:

- **Competitive MSR/CPE portfolio**: HP MSR routers can integrate multiple services and provide additional features such as IPv6 and multiprotocol label switching (MPLS) at no extra charge. The routers are managed by HP IMC, making their price/performance very competitive vs. Cisco.
- **Breadth of offerings:** HP's breadth of networking products, which have the same OS across all products, is a key differentiator compared to Cisco, which has multiple operating systems that add to the complexity of the network.
- **Architectural advantage:** Many Cisco customers need to use both a pair of Cisco Nexus switches and a pair of ASR routers because the switches and routers don't have the same functionality (like MPLS) and run two different operating systems. HP customers need only one pair of routers or switches.
- **Flexibility:** HP routers are based on open standards and have all the feature and performance capabilities that Cisco routers have. However, HP routers leverage our overall portfolio when it comes to OS integration, management, and operations.
- **Low complexity in configuring the bill of materials**: While a customer must use many stock-keeping units (SKUs) to configure a Cisco router, HP routers need fewer SKUs during configuration, lowering the complexity.

- **Capability:** HP is one of two vendors that can provide end-to-end routers: HP is the only vendor besides Cisco that has a broad WAN router portfolio and a full network infrastructure solution.
- **Unified Comware platform:** All HP routers share a single core software platform, which reduces management complexity for network administrators.
- **Open platform for more applications:** HP routers use a service-blade architecture that is based on an open application platform, which allows the extension of core switching and routing capabilities through a 100 percent compatible slide approach. This allows customers to add third-party applications and services, such as WAN optimization and VoIP solutions, as modules in the router.
- **Lower total cost of ownership:** HP routers are competitively priced, and we do not charge extra fees for licenses—all the features supported are in the software. **Cisco charges for customer licenses or service activation on their routers for some features.**
- **HP routers reduce operating expenses by offering:**
    - Multicore CPUs that realize high-performance, Value adding, native software
    - Adaptable optical Ethernet interface
    - Router-speed-adaptable point-of-sale interface
    - Comprehensive IPv6 and MPLS
- **PCI Express and multiple-bus architecture:** These features help HP routers deliver faster performance and greater value to customers than the competition by allowing concurrent service processing.
- **"Green" advantage:** HP is socially responsible, and our products are compliant with Restriction of Hazardous Substances and Waste Electrical and Electronic Equipment directives.

HP has been innovative in its router line since inception. HP is one of the first vendors to apply multicore CPUs on enterprise routers, in the HP A6600 Router Series. HP routers have had comprehensive IPv6 and MPLS features for over five years, an indication of leadership. In 2006, the HP MSR series was among the first routers with an open architecture that integrated third party applications.

HP enterprise routers have been deployed globally in many large banks and enterprises. Examples of customers that have thousands of HP A-Series routers are: the Industrial and Commercial Bank of China, Savings Bank of the Russian Federation, La Poste (the French postal service), Taser International (in North America), Telefonica, and BT Brasil.

Closing

Our fully compliant RFP response takes into consideration all the core values and general goals of our customer base, and solidifies a partnership that:

a. is second to none in the industry, offering lower TCO, better performance and less complexity,

b. that provides advanced functionality at affordable prices, and anticipates WVOT's future needs, and

c. is built upon commitment to providing flexible easy-to-use products, which interoperate easily with other manufacturers' products in the industry.

HP simply provides a partnership unlike any other in the network community with better support and lower Total Cost of Ownership.

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
ISCM0112	1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
KRISTA FERRELL
304-558-2596

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Total Systems Integration (TSI), Inc.
1263 SR 598
PO 687
Galion, Ohio 44833-0687
(419) 544-1331
georgedallas@total-systems.net

SHIP TO
DEPARTMENT OF ADMINISTRATION
WVOT NETWORKING SUPERVISOR
1900 KANAWHA BLVD. E.
BUILDING 5, 10TH FLOOR
CHARLESTON, WV
25305 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/12/2012				

BID OPENING DATE: 05/03/2012 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	1	EA		205-43		

PERIPHERAL DEVICES AND ACCESSORIES, COMPUTER SYSTEM

REQUEST FOR QUOTATION
(RFQ)

THE WEST VIRGINIA STATE PURCHASING DIVISION FOR THE AGENCY, THE WEST VIRGINIA OFFICE OF TECHNOLOGY, IS SOLICITING BIDS TO PROVIDE THE AGENCY WITH NETWORK INFRASTRUCTURE EQUIPMENT FOR THE GREENBANK OBSERVATORY LOCATED IN GREENBANK, WEST VIRGINIA PER THE ATTACHED SPECIFICATIONS.

THIS SOLICITION IS FOR MATERIALS ONLY. NO INSTALLATION IS REQUIRED.

TECHNICAL QUESTIONS CONCERNING THIS SOLICITATION MUST BE SUBMITTED IN WRITING TO KRISTA FERRELL IN THE WEST VIRGINIA STATE PURCHASING DIVISION VIA FAX AT 304-558-4115 OR VIA EMAIL AT KRISTA.S.FERRELL@WV.GOV.

DEADLINE FOR ALL TECHNICAL QUESTIONS IS 04/24/2012 AT THE CLOSE OF BUSINESS.

ANY TECHNICAL QUESTIONS RECEIVED WILL BE ANSWERED BY FORMAL WRITTEN ADDENDUM TO BE ISSUED BY THE PURCHASING DIVISION AFTER THE DEADLINE HAS LAPSED.

VERBAL COMMUNICATION: ANY VERBAL COMMUNICATION BETWEEN THE VENDOR AND ANY STATE PERSONNEL IS NOT BINDING, INCLUDING THAT MADE AT THE MANDATORY PRE-BID MEETING.

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
George Dallas	(419) 544-1331	May 9, 2010
TITLE: President	FEIN: 34-1757782	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

GENERAL TERMS & CONDITIONS
REQUEST FOR QUOTATION (RFQ) AND REQUEST FOR PROPOSAL (RFP)

1. Awards will be made in the best interest of the State of West Virginia.

2. The State may accept or reject in part, or in whole, any bid.

3. Prior to any award, the apparent successful vendor must be properly registered with the Purchasing Division and have paid the required $125 fee.

4. All services performed or goods delivered under State Purchase Order/Contracts are to be continued for the term of the Purchase Order/Contracts, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise available for these services or goods this Purchase Order/Contract becomes void and of no effect after June 30.

5. Payment may only be made after the delivery and acceptance of goods or services.

6. Interest may be paid for late payment in accordance with the ***West Virginia Code***.

7. Vendor preference will be granted upon written request in accordance with the ***West Virginia Code***.

8. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

9. The Director of Purchasing may cancel any Purchase Order/Contract upon 30 days written notice to the seller.

10. The laws of the State of West Virginia and the ***Legislative Rules*** of the Purchasing Division shall govern the purchasing process.

11. Any reference to automatic renewal is hereby deleted. The Contract may be renewed only upon mutual written agreement of the parties.

12. **BANKRUPTCY:** In the event the vendor/contractor files for bankruptcy protection, the State may deem this contract null and void, and terminate such contract without further order.

13. **HIPAA BUSINESS ASSOCIATE ADDENDUM:** The West Virginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, is available online at **www.state.wv.us/admin/purchase/vrc/hipaa.html** and is hereby made part of the agreement provided that the Agency meets the definition of a Cover Entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the vendor.

14. **CONFIDENTIALITY:** The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/noticeConfidentiality.pdf.

15. **LICENSING:** Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, and the West Virginia Insurance Commission. The vendor must provide all necessary releases to obtain information to enable the director or spending unit to verify that the vendor is licensed and in good standing with the above entities.

16. **ANTITRUST:** In submitting a bid to any agency for the State of West Virginia, the bidder offers and agrees that if the bid is accepted the bidder will convey, sell, assign or transfer to the State of West Virginia all rights, title and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to the bidder.

I certify that this bid is made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, or person or entity submitting a bid for the same material, supplies, equipment or services and is in all respects fair and without collusion or Fraud. I further certify that I am authorized to sign the certification on behalf of the bidder or this bid.

INSTRUCTIONS TO BIDDERS

1. Use the quotation forms provided by the Purchasing Division. Complete all sections of the quotation form.

2. Items offered must be in compliance with the specifications. Any deviation from the specifications must be clearly indicated by the bidder. Alternates offered by the bidder as **EQUAL** to the specifications must be clearly defined. A bidder offering an alternate should attach complete specifications and literature to the bid. The Purchasing Division may waive minor deviations to specifications.

3. Unit prices shall prevail in case of discrepancy. All quotations are considered F.O.B. destination unless alternate shipping terms are clearly identified in the quotation.

4. All quotations must be delivered by the bidder to the office listed below prior to the date and time of the bid opening. Failure of the bidder to deliver the quotations on time will result in bid disqualifications: Department of Administration, Purchasing Division, 2019 Washington Street East, P.O. Box 50130, Charleston, WV 25305-0130

5. Communication during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited (W.Va. C.S.R. §148-1-6.6).

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
ISCM0112	2

ADDRESS CORRESPONDENCE TO ATTENTION OF:
KRISTA FERRELL
304-558-2596

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Total Systems Integration (TSI), Inc.
1263 SR 598
PO 687
Galion, Ohio 44833-0687
(419) 544-1331
georgedallas@total-systems.net

SHIP TO
DEPARTMENT OF ADMINISTRATION
WVOT NETWORKING SUPERVISOR
1900 KANAWHA BLVD. E.
BUILDING 5, 10TH FLOOR
CHARLESTON, WV
25305 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/12/2012				

BID OPENING DATE: 05/03/2012 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

ONLY INFORMATION ISSUED IN WRITING AND ADDED TO THE RFQ SPECIFICATIONS BY AN OFFICIAL WRITTEN ADDENDUM BY PURCHASING IS BINDING.

NO CONTACT BETWEEN THE VENDOR AND THE AGENCY IS PERMITTED WITHOUT THE EXPRESS WRITTEN CONSENT OF THE STATE BUYER. VIOLATION MAY RESULT IN REJECTION OF THE BID. THE STATE BUYER LISTED ABOVE IS THE SOLE CONTACT FOR ANY AND ALL INQUIRIES AFTER THIS RFQ HAS BEEN RELEASED.

EXHIBIT 10

REQUISITION NO.: .....

ADDENDUM ACKNOWLEDGEMENT

I HEREBY ACKNOWLEDGE RECEIPT OF THE FOLLOWING CHECKED ADDENDUM(S) AND HAVE MADE THE NECESSARY REVISIONS TO MY PROPOSAL, PLANS AND/OR SPECIFICATION, ETC.

ADDENDUM NO.'S:

NO. 1 x

NO. 2 .....

NO. 3 .....

NO. 4 .....

NO. 5 .....

I UNDERSTAND THAT FAILURE TO CONFIRM THE RECEIPT OF THE ADDENDUM(S) MAY BE CAUSE FOR REJECTION OF BIDS.

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
George Dallas	(419) 544-1331	May 09, 2012

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE
President	34-1757782	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
ISCM0112	3

ADDRESS CORRESPONDENCE TO ATTENTION OF:
KRISTA FERRELL
304-558-2596

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Total Systems Integration (TSI), Inc.
1263 SR 598
PO 687
Galion, Ohio 44833-0687
(419) 544-1331
georgedallas@total-systems.net

SHIP TO
DEPARTMENT OF ADMINISTRATION
WVOT NETWORKING SUPERVISOR
1900 KANAWHA BLVD. E.
BUILDING 5, 10TH FLOOR
CHARLESTON, WV
25305 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/12/2012				

BID OPENING DATE: 05/03/2012 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

VENDOR MUST CLEARLY UNDERSTAND THAT ANY VERBAL REPRESENTATION MADE OR ASSUMED TO BE MADE DURING ANY ORAL DISCUSSION HELD BETWEEN VENDOR'S REPRESENTATIVES AND ANY STATE PERSONNEL IS NOT BINDING. ONLY THE INFORMATION ISSUED IN WRITING AND ADDED TO THE SPECIFICATIONS BY AN OFFICIAL ADDENDUM IS BINDING.

George Dallas

.....
SIGNATURE

Total Systems Integration (TSI), Inc.
.....
COMPANY

02 May 2012
.....
DATE

NOTE: THIS ADDENDUM ACKNOWLEDGEMENT SHOULD BE SUBMITTED WITH THE BID.

REV. 09/21/2009
BANKRUPTCY: IN THE EVENT THE VENDOR/CONTRACTOR FILES FOR BANKRUPTCY PROTECTION, THE STATE MAY DEEM THE CONTRACT NULL AND VOID, AND TERMINATE SUCH CONTRACT WITHOUT FURTHER ORDER.

ANY INDIVIDUAL SIGNING THIS BID IS CERTIFYING THAT: (1) HE OR SHE IS AUTHORIZED BY THE BIDDER TO EXECUTE THE BID OR ANY DOCUMENTS RELATED THERETO ON BEHALF OF THE BIDDER, (2) THAT HE OR SHE IS AUTHORIZED TO BIND THE BIDDER IN A CONTRACTUAL RELATIONSHIP, AND (3) THAT THE BIDDER HAS PROPERLY REGISTERED WITH ANY STATE AGENCIES THAT MAY REQUIRE REGISTRATION.

NOTICE

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE George Dallas	TELEPHONE (419) 544-1331	DATE May 09, 2012
TITLE President	FEIN 34-1757782	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER	PAGE
ISCM0112	4

ADDRESS CORRESPONDENCE TO ATTENTION OF:
KRISTA FERRELL
304-558-2596

VENDOR
RFQ COPY
TYPE NAME/ADDRESS HERE
Total Systems Integration (TSI), Inc.
1263 SR 598
PO 687
Galion, Ohio 44833-0687
(419) 544-1331
georgedallas@total-systems.net

SHIP TO
DEPARTMENT OF ADMINISTRATION
WVOT NETWORKING SUPERVISOR
1900 KANAWHA BLVD. E.
BUILDING 5, 10TH FLOOR
CHARLESTON, WV
25305 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/12/2012				

BID OPENING DATE: 05/03/2012 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT

A SIGNED BID MUST BE SUBMITTED TO:

DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
BUILDING 15
2019 WASHINGTON STREET, EAST
CHARLESTON, WV 25305-0130

THE BID SHOULD CONTAIN THIS INFORMATION ON THE FACE OF THE ENVELOPE OR THE BID MAY NOT BE CONSIDERED:

SEALED BID

BUYER: KRISTA FERRELL-FILE 21

RFQ. NO.: ISCM0112

BID OPENING DATE: 05/03/2012

BID OPENING TIME: 1:30 PM

PLEASE PROVIDE A FAX NUMBER IN CASE IT IS NECESSARY TO CONTACT YOU REGARDING YOUR BID:
GEORGEDALLAS@TOTAL-SYSTEMS.NET

CONTACT PERSON (PLEASE PRINT CLEARLY):
GEORGE DALLAS (419) 544-1331

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
George Dallas	(419) 544-1331	May 09, 2012

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE
President	34-1757782	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

REQUEST FOR QUOTATION
ISCM0112

The Acquisition and Contract Administration Section of the Purchasing Division, hereinafter referred to as "State", is soliciting bids for the Office of Technology, hereinafter referred to as "WVOT", on behalf of the Green Bank Observation located at 1 Observatory Road, Green Bank, WV 24944, to acquire network infrastructure equipment.

I. PURPOSE

The WVOT is requesting quotations to provide network infrastructure equipment based on the attached equipment list for an upgrade to the Green Bank Observatory facility. Green Bank Observatory will manage, in collaboration with the Office of Technology, all wide area communications in the State, including data, voice and video. Green Bank Observatory serves the network needs of public libraries, K-12 and technical schools, and state government, both for intrastate applications and Internet access.

II. DEFINITIONS

A. "Vendor": The successful bidder
B. "BTOP": The Broadband Technology Opportunities Program (BTOP) is a grant program associated with the American Recovery and Reinvestment Act (ARRA). The grant program was created to promote the development and adoption of broadband throughout the United States, particularly in unserved and underserved areas.

III. BACKGROUND

The West Virginia Broadband Technology Opportunities Program (BTOP) is deploying broadband services throughout the state of West Virginia. This will allow high quality, affordable, broadband services to schools, libraries, hospitals, public safety agencies, jails and residence of West Virginia.

In order to meet the demands of the robust broadband infrastructure deployment, Green Bank Observatory needs to upgrade their network infrastructure to be reliable for the higher volume of internet access.

IV. GENERAL REQUIREMENTS

1. Warranty - Materials and workmanship hereinafter specified and furnished shall be fully guaranteed by the vendor for five (5) years.

The Vendor's obligation under its manufacturer warranty is limited to the cost of repair of the warranted item or replacement thereof, at the vendor's option. Insurance covering said equipment from damage or loss is to be borne by the Vendor until full acceptance of equipment and services.

2. Equipment Requirements - This RFQ specifies Cisco name brand products, "or equal" and must be able to expand and upgrade with the existing Green Bank Observatory hardware and system architecture. Any alternative products must seamlessly fit into, integrate with and interchange with the existing Cisco infrastructure investment with zero loss of feature, functionality and no infrastructure configuration changes. Vendors who are

bidding alternates should so state and include pertinent literature and specifications. Failure to provide information for any alternates may be grounds for rejection of bid.

V. INVOICING AND DELIVERY

1. Invoicing: Invoicing shall be made to the Office of Technology, P.O. Box 50110 Charleston, WV 25305.

2. Delivery Location: Equipment shall be shipped to Green Bank Observatory located at 1 Observatory Road, Green Bank, WV 24944.

3. Delivery Requirements: Delivery requirements are 30 Days or less ARO (Standard delivery time). Standard order delivery shall be F.O.B. destination to the above delivery location. Vendor shall include the cost of standard order delivery charges in its bid pricing/discount and is not permitted to charge the Agency separately for such delivery.

VI. AWARD

The Contract shall be awarded to the Vendor that provides the lowest overall total cost for the items listed on the Equipment Bids Price Sheet.

ISCM0112 Bid Price Sheet

Quantity	Product Number	Description	Unit Price	Extended Price
1	ASR1006	Cisco ASR1006 Chassis, Dual P/S		
2	ASR1000-ESP40	Cisco ASR1000 Embedded Services Processor, 40G		
1	ASR1000-RP2	Cisco ASR1000 Route Processor 2, 8GB DRAM		
1	M-ASR1K-RP2-8GB	Cisco ASR1000 RP2 8GB DRAM		
1	M-ASR1K-HDD-80GB	Cisco ASR1000 RP2 80GB HDD		
1	ASR1000-RP2	Cisco ASR1000 Route Processor 2, 8GB DRAM		
1	M-ASR1K-RP2-8GB	Cisco ASR1000 RP2 8GB DRAM		
1	M-ASR1K-HDD-80GB	Cisco ASR1000 RP2 80GB HDD		
1	ASR1000-SIP40	Cisco ASR1000 SPA Interface Processor 40		
1	SPA-1X10GE-L-V2	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter		
1	SPA-2XT3/E3	2-port Clear Channel T3/E3 Shared Port Adapter		
1	SPA-5X1GE-V2	Cisco 5-Port Gigabit Ethernet Shared Port Adapter		
1	SPA-8XCHT1/E1	8-port Channelized T1/E1 to DS0 Shared Port Adapter		
1	XFP-10G-MM-SR=	10GBASE-SR XFP Module		
1	SFP-GE-L	1000BASE-LX/LH SFP (DOM)		
1	SFP-GE-S	1000BASE-SX SFP (DOM)		
2	SFP-GE-T	1000BASE-T SFP (NEBS 3 ESD)		
1	ASR1000-SIP40	Cisco ASR1000 SPA Interface Processor 40		
1	SPA-1X10GE-L-V2	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter		
1	XFP-10GLR-OC192SR	Multirate XFP module for 10GBASE-LR and OC192 SR-1		
1	SASR1R2-AESK9-34S	Cisco ASR 1000 Series RP2 ADVANCED ENTERPRISE SERVICES		
1	FLASR1-FPI-RTU	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series		
1	FLASR1-FW-RTU	Firewall Right-To-Use Feature Lic for ASR1000 Series		
1	FLASR1-IPSEC-RTU	Encryption Right-To-Use Feature Lic for ASR1000 Series		
2	ASR1013/06-PWR-AC	Cisco ASR1000 1600w AC Power Supply		
2	CAB-9K20A-NA	Power Cord, 125VAC 20A NEMA 5-20 Plug, North America/Japan		
1	MEMUSB-1024FT	1GB USB Flash Token		
1	Included: ASR1000-SPA	SPA for ASR1000; No Physical Part; For Tracking Only		
1	Included: ASR1000-SPA	SPA for ASR1000; No Physical Part; For Tracking Only		
1	Included: ASR1000-SPA	SPA for ASR1000; No Physical Part; For Tracking Only		
1	Included: ASR1000-SPA	SPA for ASR1000; No Physical Part; For Tracking Only		
1	Included: ASR1000-SPA	SPA for ASR1000; No Physical Part; For Tracking Only		
6	CON-SNTE-ASR1000E	SMARTNET 8X5X4 Cisco ASR1000 Embedded Services Processo		
3	CON-SNTE-ASRRP2	SMARTNET 8X5X4 ASR1000 RP2		
3	CON-SNTE-ASRRP2	SMARTNET 8X5X4 ASR1000 RP2		
3	CON-SNTE-1000SP40	SMARTNET 8X5X4 Cisco ASR1000 SPA Interface Processor 40		
3	CON-SNTE-1000SP40	SMARTNET 8X5X4 Cisco ASR1000 SPA Interface Processor 40		
3	CON-SNTE-ASR1K6	SMARTNET 8X5X4 Cisco ASR1006 Chassis, Dual P/S		
3	CON-SNTE-ASR1FPI	SMARTNET 8X5X4 Flex. Pack Insp. Right-To-Use Feat Lic		
3	CON-SNTE-ASR1FWRT	SMARTNET 8X5X4 Firewall Right-To-Use Feature Lic		

ISCM0112 Bid Price Sheet

3	CON-SNTE-ASRIPSEC	SMARTNET 8X5X4 Encryption Right-To-Use Feature Lic		
3	CON-SNTE-R2AES34	SMARTNET 8X5X4 Cisco ASR 1000 Series RP2 ADVANCED ENTER		
3	CON-SNTE-1X10GEV2	SMARTNET 8X5X4 1-Pt 10GE LAN-PHY Shared PT Adptr		
3	CON-SNTE-1X10GEV2	SMARTNET 8X5X4 1-Pt 10GE LAN-PHY Shared PT Adptr		
3	CON-SNTE-2XT3E3	SMARTNET 8X5X4 2-port T3/E3 Serial		
3	CON-SNTE-5X1GEV2	SMARTNET 8X5X4 5-Pt Gigabit Enet Shared Pt Adptr		
3	CON-SNTE-8XCHT1E1	SMARTNET 8X5X4 8Prt Channel T1/E1		
1	N7K-C7010-BUN2-R	Nexus 7010 Bundle (Chassis,(2)SUP1,(5)FAB2,(3)AC-6KW PSU)		
1	N7KS1K9-60	Cisco NX-OS Release 6.0		
1	N7K-C7010-SBUN-P1	Inc LAN,ADV,TRS,EL2,DCNM,DCNMSAN,MPLS,SAN,XL gd thru 1HFY12		
1	N7K-M148GT-11L	Nexus 7000 - 48 Port 10/100/1000 Module with XL option		
1	N7K-M148GT-11L	Nexus 7000 - 48 Port 10/100/1000 Module with XL option		
1	N7K-M148GT-11L	Nexus 7000 - 48 Port 10/100/1000 Module with XL option		
1	N7K-M148GT-11L	Nexus 7000 - 48 Port 10/100/1000 Module with XL option		
1	N7K-CPF-2GB	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)		
1	N7K-CPF-2GB	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)		
1	N7K-F248XP-25	Nexus 7000 F2-Series 48 Port 10GbE (req. SFP+)		
2	SFP-10G-LR	10GBASE-LR SFP Module		
12	SFP-10G-LRM	10GBASE-LRM SFP Module		
14	SFP-10G-SR	10GBASE-SR SFP Module		
1	N7K-M148GS-11L	Nexus 7000 - 48 Port GE Module with XL Option (req. SFP)		
8	GLC-LH-SM	GE SFP, LC connector LX/LH transceiver		
8	GLC-SX-MM	GE SFP, LC connector SX transceiver		
4	GLC-T	1000BASE-T SFP		
6	CAB-AC-C6K-TWLK	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US		
1	N7K-C7010-AFLT	Nexus 7010 Air Filter		
1	N7K-C7010-FD-MB	Nexus 7010 Front Door Kit		
1	Included: DCNM-N7K-K9-SBUN	DCNM for LAN Enterprise License for one Nexus 7000 Chassis		
1	Included: DCNM-SANN7KK9-SBUN	DCNM for SAN Advanced Edition for Nexus 7000		
1	Included: N7K-ADV1K9-SBUN	Nexus 7000 Advanced LAN Enterprise License (VDC, CTS ONLY)		
1	Included: N7K-C7010-XL-SBUN	Nexus 7010 Scalable Feature License		
1	Included: N7K-EL21K9-SBUN	Nexus 7000 Enhanced Layer 2 License (FabricPath)		
1	Included: N7K-LAN1K9-SBUN	Nexus 7000 LAN Enterprise License (L3 protocols)		
1	Included: N7K-MPLS1K9-SBUN	Nexus 7000 MPLS License		
1	Included: N7K-SAN1K9-SBUN	Nexus 7000 SAN Enterprise License		
1	Included: N7K-TRS1K9-SBUN	Nexus 7000 Transport Services License (OTV)		
1	Included: N7K-SUP1-BUN	Nexus 7000 - Supervisor 1, Includes External 8GB Flash		
1	Included: N7K-SUP1-8GBUPG	Nexus 7000 Supervisor 1 8GB Memory Upgrade Kit		
1	Included: N7K-SUP1-BUN	Nexus 7000 - Supervisor 1, Includes External 8GB Flash		
1	Included: N7K-SUP1-8GBUPG	Nexus 7000 Supervisor 1 8GB Memory Upgrade Kit		
5	Included: N7K-C7010-FAB-2	Nexus 7000 - 10 Slot Chassis - 110Gbps/Slot Fabric Module		

ISCM0112 Bid Price Sheet

3	Included: N7K-AC-6.0KW	Nexus 7000 - 6.0KW AC Power Supply Module		
3	CON-SNTE-7010B2R	SMARTNET 8X5X4 Nexus 7010 Bundle (Chassis,(2)SUP1		
		Subtotal		
		Shipping charges		
		TOTAL		

An electronic version of this price sheet is available online to registered vendors at http://www.state.wv.us/admin/purchase/newbul.htm. Non-registered vendors may request an electronic copy by emailing krista.s.ferrell@wv.gov.

SEE ATTACHED PRICING SCHEDULE WE ARE PROPOSING HEWLETT PACKARD EQUIPMENT THAT MEETS OR EXCEEDS SPECIFICATIONS

Rev. 09/08

ISCM0112

State of West Virginia

VENDOR PREFERENCE CERTIFICATE

Certification and application* is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Resident Vendor Preference, if applicable.

1. **Application is made for 2.5% resident vendor preference for the reason checked:**

____ Bidder is an individual resident vendor and has resided continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**

____ Bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; or 80% of the ownership interest of Bidder is held by another individual, partnership, association or corporation resident vendor who has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**

____ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. **Application is made for 2.5% resident vendor preference for the reason checked:**

____ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. **Application is made for 2.5% resident vendor preference for the reason checked:**

____ Bidder is a nonresident vendor employing a minimum of one hundred state residents or is a nonresident vendor with an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia employing a minimum of one hundred state residents who certifies that, during the life of the contract, on average at least 75% of the employees or Bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

4. **Application is made for 5% resident vendor preference for the reason checked:**

____ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. **Application is made for 3.5% resident vendor preference who is a veteran for the reason checked:**

____ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. **Application is made for 3.5% resident vendor preference who is a veteran for the reason checked:**

____ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) reject the bid; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Under penalty of law for false swearing (West Virginia Code, §61-5-3), Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: _____ Signed: _____

Date: _____ Title: _____

**Check any combination of preference consideration(s) indicated above, which you are entitled to receive.*

RFQ No. ISCM0112

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

West Virginia Code §5A-3-10a states: No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owed is an amount greater than one thousand dollars in the aggregate.

DEFINITIONS:
"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Debtor" means any individual, corporation, partnership, association, limited liability company or any other form or business association owing a debt to the state or any of its political subdivisions. "Political subdivision" means any county commission; municipality; county board of education; any instrumentality established by a county or municipality; any separate corporation or instrumentality established by one or more counties or municipalities, as permitted by law; or any public body charged by law with the performance of a government function or whose jurisdiction is coextensive with one or more counties or municipalities. "Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

EXCEPTION: The prohibition of this section does not apply where a vendor has contested any tax administered pursuant to chapter eleven of this code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

Under penalty of law for false swearing (***West Virginia Code*** §61-5-3), it is hereby certified that the vendor affirms and acknowledges the information in this affidavit and is in compliance with the requirements as stated.

WITNESS THE FOLLOWING SIGNATURE

Vendor's Name: Total Systems Integration (TSI), Inc.

Authorized Signature: Marie C. Dallas Date: 05/02/2012

Secretary Treasurer

State of Ohio

County of Crawford, to-wit:

Taken, subscribed, and sworn to before me this 2nd day of May, 20 12.

My Commission expires _____, 20___.

AFFIX SEAL HERE NOTARY PUBLIC _____

Original Notarized Form was sent under separate cover

Part Number	Description	QTY	Cost	Extend
	ISCM0112 Network Equipment			
JC612A	HP 10508 Switch Chassis	1	$ 3,570.00	$ 3,570.00
JC665A	HP X421 Chassis Universal Rck Mntg Kit	1	$ 105.00	$ 105.00
JC616A	HP 10508 640Gbps Type A Fabric Module	4	$ 2,730.00	$ 10,920.00
JC614A	HP 10500 Main Processing Unit	2	$ 3,780.00	$ 7,560.00
JC610A	HP 10500 2500W AC Power Supply	6	$ 840.00	$ 5,040.00
JC623A	HP 10500 48-port Gig-T EA Module	4	$ 8,820.00	$ 35,280.00
JC628A	HP 10500 16-port 10GbE SFP+ SC Module	3	$ 13,020.00	$ 39,060.00
JC625A	HP 10500 48-port GbE SFP EB Module	1	$ 12,600.00	$ 12,600.00
JD094B	HP X130 10G SFP+ LC LR Transceiver	2	$ 1,553.58	$ 3,107.16
JD093B	HP X130 10G SFP+ LC LRM Transceiver	12	$ 671.58	$ 8,058.96
JD092B	HP X130 10G SFP+ LC SR Transceiver	14	$ 637.98	$ 8,931.72
JD119B	HP X120 1G SFP LC LX Transceiver	8	$ 377.58	$ 3,020.64
JD118B	HP X120 1G SFP LC SX Transceiver	8	$ 175.98	$ 1,407.84
JD089B	HP X120 1G SFP RJ45 T Transceiver	4	$ 150.78	$ 603.12
			Hardware	**$ 139,264.44**
	5 Year Maintenance			
HT116E	HP 5y SupportPlus24 10508 Switch Svc *7 x 24 x 4 On-Site, Software Upgrades, Tech Support*	1	$ 44,836.35	$ 44,836.35
			Services	**$ 44,836.35**
			SubTotal:	**$ 184,100.79** <<<<
	ISCM0112 Router Equipment			
JC496A	HP 6616 Router Chassis	1	$ 5,068.98	$ 5,068.98
JC665A	HP X421 Chassis Universal Rck Mntg Kit	1	$ 105.00	$ 105.00
JC180A	HP 6600 Router Software License	1	$ 1,343.58	$ 1,343.58
JC492A	HP 6616 650W AC Router Power Supply	2	$ 381.78	$ 763.56
JC566A	HP A6600 RSE-X1 Main Processing Unit	2	$ 6,414.66	$ 12,829.32
JD118B	HP X120 1G SFP LC SX Transceiver	1	$ 175.98	$ 175.98
JD119B	HP X120 1G SFP LC LX Transceiver	1	$ 377.58	$ 377.58
JD548A	HP MSR 2-port Gig-T MIM Module	1	$ 1,440.18	$ 1,440.18
JC160A	HP 6600 8-port T1 MIM Router Module	1	$ 2,225.58	$ 2,225.58
JD628A	HP MSR 1-port FT3/CT3 MIM Module	2	$ 2,448.18	$ 4,896.36
JC166B	HP A6600 FIP-110 Flex Int Platform Mod	1	$ 1,918.98	$ 1,918.98
JD089B	HP X120 1G SFP RJ45 T Transceiver	1	$ 150.78	$ 150.78
JD117B	HP X130 10G XFP LC SR Transceiver	1	$ 763.98	$ 763.98
JC168A	HP 6600 1p 10GbE XFP HIM Rtr Module	1	$ 3,073.98	$ 3,073.98
JC167B	HP A6600 FIP-210 Flex Int Platform Mod	2	$ 5,375.58	$ 10,751.16
JC164A	HP 6600 8GbE WAN HIM Router Module	1	$ 3,073.98	$ 3,073.98
JC161A	HP 6600 1p OC-3 (E1/T1) CPOS HIM Rtr Mod	1	$ 6,144.18	$ 6,144.18
JD250A	HP 6600 Firewall Processing Router Module	1	$ 12,250.98	$ 12,250.98
JD639A	HP X260 8T1 RJ45 3m Router Cable	2	$ 268.38	$ 536.76
			Hardware	**$ 67,890.90**
	5 Year Maintenance			
UV945E	HP 5y SupportPlus24 Networks 66xx Svc *7 x 24 x 4 On-Site, Software Upgrades, Tech Support*	1	$ 14,945.45	$ 14,945.45
			Services	**$ 14,945.45**
			SubTotal:	**$ 82,836.35** <<<<
			Grand:Total:	**$ 266,937.14** <<<<
	Optional - Pro Services			
HPOSENG	HP On-Site Engineer, training, configure, support, etc.	1	$ 9,000.00	$ 9,000.00

TSI, Inc.
George Dallas
(419) 544-1331

HP NETWORKING VS. CISCO

6 Compelling Total Cost of Ownership (TCO) Comparisons

Voice

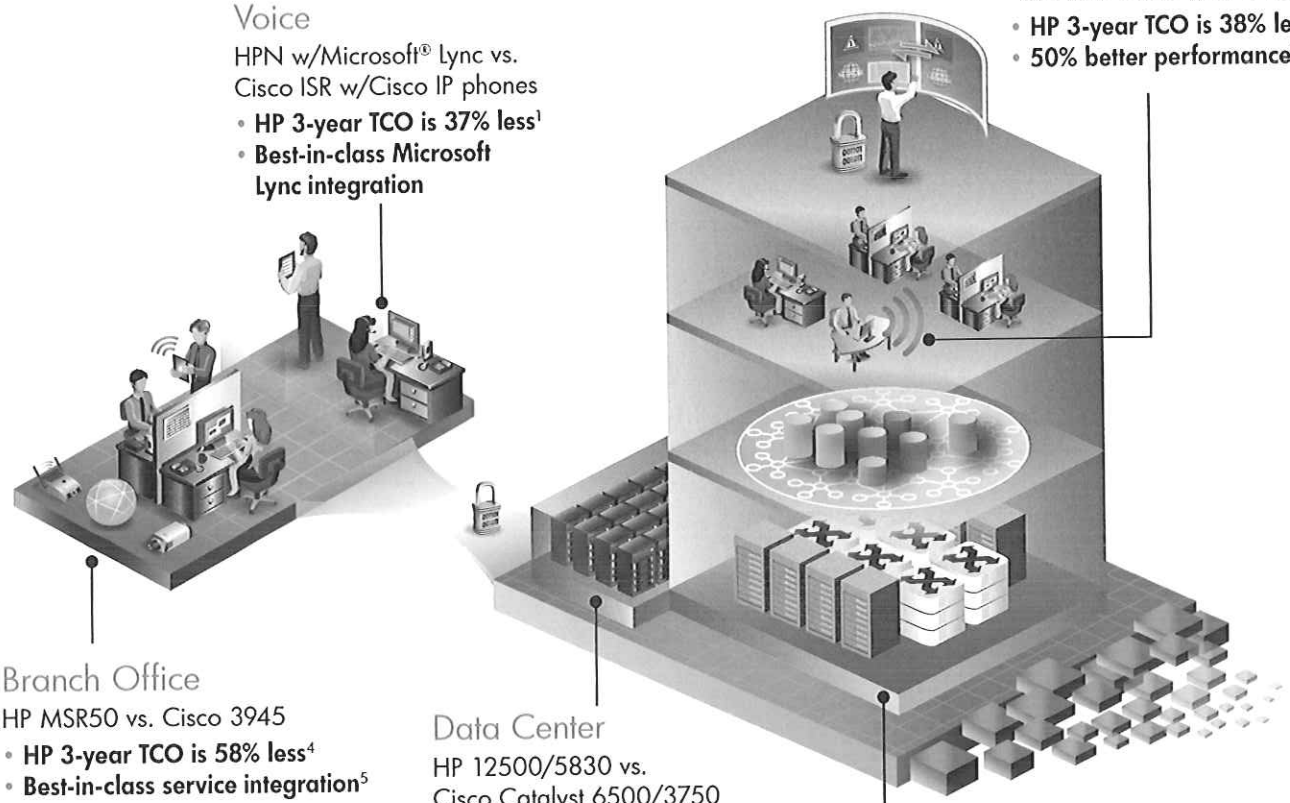
HPN w/Microsoft® Lync vs.
Cisco ISR w/Cisco IP phones

- **HP 3-year TCO is 37% less**[1]
- **Best-in-class Microsoft Lync integration**

Wireless

HP MSM760 with MSM466
vs. Cisco 5508 with 1142

- **HP 3-year TCO is 38% less**[2]
- **50% better performance**[3]



Branch Office

HP MSR50 vs. Cisco 3945

- **HP 3-year TCO is 58% less**[4]
- **Best-in-class service integration**[5]

Data Center

HP 12500/5830 vs.
Cisco Catalyst 6500/3750

- **HP 3-year TCO is 50% less**[6]
- **233% better performance**[7]
- **7000% more buffering**[8]

HP 12500/5830 vs.
Cisco Nexus 7000/5000/2000

- **HP 3-year TCO is 25% less**[9]
- **100% better routing performance**[10]
- **3900% more buffering**[11]

Campus

HP 10500/3800 vs.
Cisco Catalyst 6500/3750

- **HP 3-year TCO is 53% less**[12]
- **376% better performance**[13]

1 Based on 24-user Enterprise Branch solution with HP and Microsoft Lync hardware and software with 3-year maintenance vs. Cisco ISR G2 hardware and software with 3-year maintenance.

2 Based on list price for HP MSM760 controller and MSM466 access point hardware and software with 3-year maintenance vs. Cisco 5508 and 802.11a/g/n Fixed Unified Access point hardware and software with 3-year maintenance.

3 Based on MSM466 450 Mbps per radio vs. Cisco 1142 300 Mbps.

4 Based on list price for HP MSR50-40 hardware and software with 3-year maintenance vs. Cisco 3945 hardware and software with 3-year maintenance.

5 Service integration provided by AllainceONE partners: Avaya, F5, Microsoft, and Riverbed.

6 Based on list price for HP 12508 core and HP 5830 TOR hardware and software with 3-year maintenance vs. Cisco Catalyst 6509 core, 6509 distribution, and 4948 TOR hardware and software with 3-year maintenance.

7 Based on HP 12518 6.66 Tbps throughput capacity vs. Cisco Catalyst 6500 2.0 Tbps throughput capacity.

8 Based on HP 5830 1.25 Gigabytes buffering vs. Cisco 4948 17.5 Megabytes buffering.

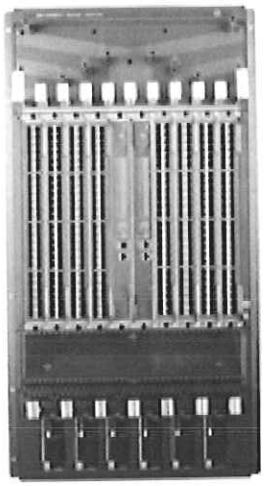
9 Based on list price for HP 12508 core with HP 5830 TOR hardware and software with 3-year maintenance vs. Cisco Nexus 7010 core, 5548 distribution, and 2248 TOR hardware and software with 3-year maintenance.

10 Based on HP 12508 960 million pps vs. Cisco Nexus 7010 480 million pps.

11 Based on HP 5830 1.25 Gigabytes buffering vs. Cisco 2248 32 Megabytes buffering.

12 Based on list price for HP 10500 core and HP 3800 edge hardware and software with 3-year maintenance vs. Cisco Catalyst 6509 core, 6509 distribution, and 3560 access hardware and software with 3-year maintenance.

13 Based on HP 10500 1905 million pps and 2.6 Tbps throughput capacity vs. Cisco Catalyst 6509 400 million pps and 2.0 Tbps throughput capacity.



HP 10500 Switch Series

Data sheet

Product overview

The HP 10500 series of switches for the HP FlexCampus solution is ideally positioned for the next-generation enterprise network core. The 10500 series is designed to set a new benchmark for performance, low latency, reliability, and future-proof scalability, as well as green technology to enable a video-ready network and provide an unmatched user experience with an advanced, simplified network architecture.

Key features

- Leading CLOS architecture
- Greater than 11 terabit-per-second capacity
- Full Layer 3 features and IPv6/MPLS functionality
- HP IRF for simpler, flatter, more agile networks
- Ultra-high 10GbE/Gigabit density; 40/100GbE ready

Features and benefits

Quality of Service (QoS)

- **IEEE 802.1p prioritization:** delivers data to devices based on the priority and type of traffic
- **Class of Service (CoS):** sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- **Bandwidth shaping:**
  - **Port-based rate limiting:** provides per-port ingress-/egress-enforced maximum bandwidth
  - **Classifier-based rate limiting:** uses an access control list (ACL) to enforce maximum bandwidth for ingress traffic on each port
  - **Guaranteed minimum:** provides per-port, per-queue egress-based guaranteed minimum bandwidth
- **Traffic policing:** supports Committed Access Rate (CAR) and line rate
- **Congestion avoidance:** Weighted Random Early Detection (WRED)/Random Early Detection (RED)
- **Powerful QoS feature:** supports the following congestion actions: strict priority (SP) queuing, weighted round robin (WRR), weighted fair queuing (WFQ), and WRED

Virtual private network (VPN)

- **IPsec:** provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two endpoints of the network
- **Generic Routing Encapsulation (GRE):** can be used to transport Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site
- **Manual or automatic Internet Key Exchange (IKE):** provides both manual or automatic key exchange required for the algorithms used in encryption or authentication; auto-IKE allows automated management of the public key exchange, providing the highest levels of encryption

Management

- **Management interface control:** each of the following interfaces can be enabled or disabled depending on security preferences: console port, telnet port, or reset button
- **Industry-standard CLI with a hierarchical structure:** reduces training time and expenses, and increases productivity in multivendor installations
- **Management security:** multiple privilege levels with password protection restrict access to critical configuration commands; ACLs provide telnet and SNMP access; local and remote syslog capabilities allow logging of all access
- **SNMPv1, v2, and v3:** provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption
- **sFlow (RFC 3176):** provides scalable ASIC-based wire-speed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes
- **Remote monitoring (RMON):** uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- **FTP, TFTP, and SFTP support:** FTP allows bidirectional transfers over a TCP/IP network and is used for configuration updates; Trivial FTP is a simpler method using User Datagram Protocol (UDP)
- **Debug and sampler utility:** supports ping and traceroute for both IPv4 and IPv6
- **Network Time Protocol (NTP):** synchronizes timekeeping among distributed time servers and clients; keeps consistent timekeeping among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time
- **Network Quality Analyzer (NQA):** analyzes network performance and service quality by sending test packets, and provides network performance and service quality parameters such as jitter, TCP, or FTP connection delays and file transfer rates; allows network manager to determine overall network performance and to diagnose and locate network congestion points or failures

- **Info center:** provides a central information center for system and network information; aggregates all logs, traps, and debugging information generated by the system and maintains them in order of severity; outputs the network information to multiple channels based on user-defined rules
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP):** automated device discovery protocol provides easy mapping by network management applications
- **Dual flash images:** provide independent primary and secondary operating system files for backup while upgrading
- **Multiple configuration files:** can be stored to the flash image

Connectivity

- **High-density port connectivity:** up to 8 interface module slots; up to 128 10-GbE ports, 384 gigabit fiber ports per system
- **Jumbo frames:** up to 9216 bytes allow high-performance backups and disaster-recovery systems
- **Loopback:** supports internal loopback testing for maintenance purposes and an increase in availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
- **Ethernet OAM:** provides a Layer 2 link performance and fault detection monitoring tool, which reduces failover and network convergence times
- **Flexible port selection:** provides a combination of fiber and copper interface modules, 100/1000BASE-X auto-speed selection, and 10/100/1000BASE-T auto-speed detection plus auto duplex and MDI/MDI-X
- **Monitor link:** collects statistics on performance and errors on physical links, increasing system availability
- **Dual-personality functionality:** includes four 10/100/1000 ports or SFP slots for optional fiber connectivity such as Gigabit-SX, -LX, and -LH, or 100-FX
- **Packet storm protection:** protects against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
- **Flow control:** using standard IEEE 802.3x, it provides back pressure to reduce congestion in heavy traffic situations

Performance

- **High-speed fully distributed architecture:** 7.68 Tbps backplane supports current 2.56 Tbps switching capacity maximum, providing enhanced performance and future 3x expansion capability; with 4 fabrics, the switch delivers up to 1905 Mpps throughput; all switching and routing is performed in the I/O modules; meets today's and future demand of 10 GbE-intensive applications
- **Scalable system design:** backplane is designed for bandwidth increases; provides investment protection to support future technologies and higher speed connectivity
- **Flexible chassis selection:** enables customers to tailor product selections to their budgets with a choice of three chassis; 10504 (4 open module slots), 10508 (8 open module slots), and 10508-V (8 vertical open module slots)

Resiliency and high availability

- **Redundant/Load-sharing fabrics, management, fan assemblies, and power supplies:** increase total performance and power available while providing hitless, stateful failover
- **Hot-swappable modules:** allow replacement of modules without any impact on other modules
- **Separate data and control paths:** keeps control separated from services and keeps service processing isolated; increases security and performance
- **Passive design system:** backplane has no active components for increased system reliability
- **Intelligent Resilient Framework (IRF):** creates virtual resilient switching fabrics, where two or more switches perform as a single Layer 2 switch and Layer 3 router; switches do not have to be co-located and can be part of a disaster-recovery system; servers or switches can be attached using standard LACP for automatic load balancing and high availability; simplifies network operation by eliminating the complexity of Spanning Tree Protocol, Equal-Cost Multipath (ECMP), or VRRP
- **Rapid Ring Protection Protocol (RRPP):** provides standard sub 200 ms recovery for ring Ethernet-based topology
- **Virtual Router Redundancy Protocol (VRRP):** allows groups of two routers to dynamically back each other up to create highly available routed environments

- **Device Link Detection Protocol (DLDP):** monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks
- **Hitless patch upgrades:** allow patches and new service features to be installed without restarting the equipment, increasing network uptime and facilitating maintenance
- **IEEE 802.3ad Link Aggregation Control Protocol (LACP):** supports up to 128 trunks, each with 8 links per trunk; supports static or dynamic groups and user-selectable hashing algorithm
- **Graceful restart:** features are fully supported, including graceful restart for OSPF, IS-IS, BGP, LDP, and RSVP; network remains stable during the active-standby switchover; after the switchover, the device quickly learns the network routes by communicating with adjacent routers; forwarding remains uninterrupted during the switchover to realize nonstop forwarding (NSF)
- **Ultrafast protocol convergence (sub second) with standard-based failure detection—Bidirectional Forwarding Detection (BFD):** enables link connectivity monitoring and reduces network convergence time for RIP, OSPF, BGP, IS-IS, VRRP, MPLS, and IRF
- **Smart link:** allows 100ms failover between links
- **Multiple internal power supply:** provides high reliability; 10504 provide 3+1 redundancy; 10508/10508-V provide 5+1 redundancy

Layer 2 switching

- **VLAN:** supports up to 4,094 port-based or IEEE 802.1Q-based VLANs; also supports MAC-based VLANs, protocol-based VLANs, and IP-subnet-based VLANs for added flexibility
- **Port isolation:** increases security by isolating ports within a VLAN while still allowing them to communicate with other VLANs
- **Bridge Protocol Data Unit (BPDU) tunneling:** transmits Spanning Tree Protocol BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs
- **GARP VLAN Registration Protocol:** allows automatic learning and dynamic assignment of VLANs
- **Port mirroring:** duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports four mirroring groups, with an unlimited number of ports per group
- **Spanning Tree:** fully supports standard IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol
- **Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping:** effectively control and manage the flooding of multicast packets in a Layer 2 network
- **IEEE 802.1ad QinQ and Selective QinQ:** increase the scalability of an Ethernet network by providing a hierarchical structure; connect multiple LANs on a high-speed campus or metro network
- **Per-VLAN Spanning Tree Plus (PVST+):** allows each virtual LAN (VLAN) to build a separate spanning tree to improve link bandwidth usage in network environments where multiple VLANs exist

Layer 3 services

- **Address Resolution Protocol (ARP):** determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
- **User Datagram Protocol (UDP) helper:** redirects UDP broadcasts to specific IP subnets to prevent server spoofing
- **Dynamic Host Configuration Protocol (DHCP):** simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
- **Domain Name System (DNS):** is a distributed database that provides translation between a domain name and an IP address, which simplifies network design; supports client and server

Layer 3 routing

- **Static IPv4 routing:** provides simple, manually configured IPv4 routing
- **Routing Information Protocol:** uses a distance vector algorithm with UDP packets for route determination; supports RIPv1 and RIPv2 routing; includes loop protection
- **OSPF:** Interior Gateway Protocol (IGP) using link-state protocol for faster convergence; supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

- **Intermediate system to intermediate system (IS-IS):** Interior Gateway Protocol (IGP) using path vector protocol, which is defined by the ISO organization for IS-IS routing and extended by IETF RFC 1195 to operate in both TCP/IP and the OSI reference model (Integrated IS-IS)
- **Border Gateway Protocol 4 (BGP-4):** Exterior Gateway Protocol (EGP) with path vector protocol uses TCP for enhanced reliability for the route discovery process, reduces bandwidth consumption by advertising only incremental updates, and supports extensive policies for increased flexibility, as well as scales to very large networks
- **Policy-based routing:** makes routing decisions based on policies set by the network administrator
- **IP performance optimization:** is a set of tools to improve performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICNP error packets, and extensive display capabilities
- **Unicast Reverse Path Forwarding (uRPF):** is defined by RFC 3704 and limits erroneous or malicious traffic
- **Static IPv6 routing:** provides simple, manually configured IPv6 routing
- **Dual IP stack:** maintains separate stacks for IPv4 and IPv6 to ease transition from an IPv4-only network to an IPv6-only network design
- **Routing Information Protocol next generation (RIPng):** extends RIPv2 to support IPv6 addressing
- **OSPFv3:** provides OSPF support for IPv6
- **IS-IS for IPv6:** extends IS-IS to support IPv6 addressing
- **BGP+:** extends BGP-4 to support Multiprotocol BGP (MBGP), including support for IPv6 addressing
- **Multiprotocol Label Switching (MPLS):** uses BGP to advertise routes across Label Switched Paths (LSPs), but uses simple labels to forward packets from any Layer 2 or Layer 3 protocol, thus reducing complexity and increasing performance; supports graceful restart for reduced failure impact; supports LSP tunneling and multilevel stacks
- **Multiprotocol Label Switching (MPLS) Layer 3 VPN:** allows Layer 3 VPNs across a provider network; uses MP-BGP to establish private routes for increased security; supports RFC 2547bis multiple autonomous system VPNs for added flexibility
- **Multiprotocol Label Switching (MPLS) Layer 2 VPN:** establishes simple Layer 2 point-to-point VPNs across a provider network using only MPLS Label Distribution Protocol (LDP); requires no routing and therefore decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; supports Circuit Cross Connect (CCC), Static Virtual Circuits (SVCs), Martini draft, and Kompella-draft technologies
- **Virtual Private LAN Service (VPLS):** establishes point-to-multipoint Layer 2 VPNs across a provider network
- **Super VLAN:** RFC 3069 standard, also called VLAN aggregation, is used to save IP address space
- **Equal-Cost Multipath (ECMP):** enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth
- **IPv6 tunneling:** is an important element for the transition from IPv4 to IPv6; allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6to4, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels and 6VPE(IPv6 on VPN to Provider Edge Router) tunnel

Security

- **Access control list (ACL):** supports powerful ACLs for both IPv4 and IPv6; ACLs are used for filtering traffic to prevent illegal users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header; rules can be set to operate on specific dates or times
- **RADIUS:** eases switch security access administration by using a password authentication server
- **TACACS+:** is an authentication tool using TCP with encryption of the full authentication request that provides additional security
- **Switch management logon security:** can require either RADIUS or TACACS+ authentication for secure switch CLI logon
- **Secure Shell (SSHv2):** uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers

- **DHCP snooping:** helps ensure that DHCP clients receive IP addresses from authorized DHCP servers and maintain a list of DHCP entries for trusted ports; prevents reception of fake IP addresses and reduces ARP attacks, improving security
- **IP Source Guard:** filters packets on a per-port basis, which prevents illegal packets from being forwarded
- **ARP attack protection:** protects from attacks using a large number of ARP requests by using a host-specific, user-selectable threshold
- **Port security:** allows access only to specified MAC addresses, which can be learned or specified by the administrator
- **IEEE 802.1X:** provides port-based user authentication with support for Extensible Authentication Protocol (EAP) MD5, TLS, TTLS, and PEAP with choice of AES, TKIP, and static or dynamic WEP encryption for protecting wireless traffic between authenticated clients and the access point
- **Media access control (MAC) authentication:** provides simple authentication based on a user's MAC address; supports local or RADIUS-based authentication
- **Multiple user authentication methods:**
  - **IEEE 802.1X:** is an industry-standard method of user authentication using an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server
  - **Web-based authentication:** similar to IEEE 802.1X, it provides a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant
  - **MAC-based authentication:** client is authenticated with the RADIUS server based on the client's MAC address
- **DHCP protection:** blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks
- **Endpoint Admission Defense (EAD):** provides security policies to users accessing a network
- **Port isolation:** secures and adds privacy, and prevents malicious attackers from obtaining user information

Convergence

- **LLDP-MED (Media Endpoint Discovery):** is a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- **Multicast Source Discovery Protocol (MSDP):** is used for inter-domain multicast applications, allowing multiple PIM-SM domains to interoperate
- **Internet Group Management Protocol (IGMP):** is used by IP hosts to establish and maintain multicast groups; supports v1, v2, and v3; utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks
- **Protocol Independent Multicast (PIM):** is used for IPv4 and IPv6 multicast applications; supports PIM Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Source-Specific Mode (PIM-SSM)
- **Multicast Border Gateway Protocol (MBGP):** allows multicast traffic to be forwarded across BGP networks and kept separate from unicast traffic
- **Multicast Listener Discovery (MLD) protocol:** is used by IP hosts to establish and maintain multicast groups; supports v1 and v2 and utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv6 multicast networks
- **Multicast VLAN:** allows multiple VLANs to receive the same IPv4 or IPv6 multicast traffic, reducing network bandwidth demand by eliminating multiple streams to each VLAN
- **Voice VLAN:** automatically assigns VLAN and priority for IP phones, simplifying network configuration and maintenance

Additional information

- **Green initiative support:** provides support for RoHS and WEEE regulations
- **Low power consumption:** is rated to have one of the lowest power usages in the industry by Miercom independent tests
- **OPEX savings:** a common operating system simplifies and streamlines deployment, management, and training, thereby cutting costs as well as reducing the chance for human errors associated with having to manage multiple operating systems across different platforms and network layers

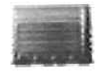
- **Unified, modular Comware operating system with modular architecture:** all switching, routing, and security platforms leverage Comware, a common unified modular operating system; provides an easy-to-enhance-and-extend feature set without wholesale changes

Warranty and support

- **1-year warranty:** with advance replacement and 10-calendar-day delivery (available in most countries)
- **Electronic and telephone support:** limited electronic and telephone support is available from HP; refer to www.hp.com/networking/warranty for details on the support provided and the period during which support is available
- **Software releases:** refer to www.hp.com/networking/warranty for details on the software releases provided and the period during which software releases are available for your product(s)

HP 10500 Switch Series

Specifications



	HP 10508-V Switch Chassis (JC611A)	HP 10508 Switch Chassis (JC612A)	HP 10504 Switch Chassis (JC613A)
Ports	2 MPU (for management modules) slots 4 switch fabric slots 8 I/O module slots Supports a maximum of 128 10-GbE ports or 384 Gigabit ports or 384 SFP ports, or a combination	2 MPU (for management modules) slots 4 switch fabric slots 8 I/O module slots Supports a maximum of 128 10-GbE ports or 384 Gigabit ports or 384 SFP ports, or a combination	2 MPU (for management modules) slots 4 switch fabric slots 4 I/O module slots Supports a maximum of 64 10-GbE ports or 192 Gigabit ports or 192 SFP ports, or a combination
Power supplies	6 power supply slots 1 minimum power supply required (ordered separately)	6 power supply slots 1 minimum power supply required (ordered separately)	4 power supply slots 1 minimum power supply required (ordered separately)
Fan tray	includes: 1 x JC634A 1 fan tray slot	includes: 1 x JC633A 1 fan tray slot	includes: 1 x JC632A 1 fan tray slot
Physical characteristics			
Dimensions	25.98(d) x 17.32(w) x 34.88(h) in. (66.0 x 44.0 x 88.6 cm) (20U height)	25.98(d) x 17.32(w) x 24.41(h) in. (66.0 x 44.0 x 62.0 cm) (14U height)	25.98(d) x 17.32(w) x 13.9(h) in. (66.0 x 44.0 x 35.3 cm) (8U height)
Weight	169.53 lb. (76.9 kg) chassis	125 lb. (56.7 kg) chassis	85.32 lb. (38.7 kg) chassis
Full configuration weight	317.02 lb. (143.8 kg)	271.06 lb. (122.95 kg)	184.28 lb. (83.59 kg)
Memory and processor			
Management module	MIPS64 @ 1G MHz, 128 MB flash, 1024 MB DDR2 SDRAM	MIPS64 @ 1G MHz, 128 MB flash, 1024 MB DDR2 SDRAM	MIPS64 @ 1G MHz, 128 MB flash, 1024 MB DDR2 SDRAM
Mounting	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); horizontal surface mounting only	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); horizontal surface mounting only	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); horizontal surface mounting only
Performance			
Throughput	1905 million pps (64-byte packets)	1905 million pps (64-byte packets)	952 million pps (64-byte packets)
Switching capacity	2.6 Tbps	2.6 Tbps	1.3 Tbps
Routing table size	512000 entries	512000 entries	512000 entries
MAC address table size	256000 entries	256000 entries	256000 entries
Reliability			
MTBF (years)	89.57	97.36	95.62
Availability	99.999%	99.999%	99.999%
Environment			
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing	10% to 95%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing	5% to 95%, noncondensing
Altitude	up to 13,123 ft. (4 km)	up to 13,123 ft. (4 km)	up to 13,123 ft. (4 km)
Acoustic	Low-speed fan: 61.6 dB, High-speed fan: 72.6 dB	Low-speed fan: 63 dB, High-speed fan: 75.8 dB	Low-speed fan: 62.3 dB, High-speed fan: 75.5 dB
Electrical characteristics			
Voltage	100-120/200-240 VAC	100-120/200-240 VAC	100-120/200-240 VAC
Current	16 A	16 A	16 A
Power output	2500 W	2500 W	2500 W
Frequency	50/60 Hz	50/60 Hz	50/60 Hz
Notes	Based on common power supply 2,500 W (AC)	Based on common power supply 2,500 W (AC)	Based on common power supply 2,500 W (AC)
Safety	CAN/CSA 22.2 No. 60950-1; FCC Part 15, Subpart B; FDA 21 CFR Subchapter J; ROHS Compliance; IEC 60950-1 :Second Edition ; EN 60950-1:2006 + A11:2009; AS/NZS 60950-1; IEC 60825-1; UL 60950-1, 2nd Edition; EN60825-2:2004+A1:2007	CAN/CSA 22.2 No. 60950-1; FCC Part 15, Subpart B; FDA 21 CFR Subchapter J; ROHS Compliance; IEC 60950-1 :Second Edition ; EN 60950-1:2006 + A11:2009; AS/NZS 60950-1; IEC 60825-1; UL 60950-1, 2nd Edition; EN60825-2:2004+A1:2007	CAN/CSA 22.2 No. 60950-1; FCC Part 15, Subpart B; FDA 21 CFR Subchapter J; ROHS Compliance; IEC 60950-1 :Second Edition ; EN 60950-1:2006 + A11:2009; AS/NZS 60950-1; IEC 60825-1, 2nd Edition; UL 60950-1, 2nd Edition; EN60825-2:2004+A1:2007
Emissions	VCCI Class A; EN 55022 Class A; CISPR 22 Class A; IEC/EN 61000-3-2; IEC/EN 61000-3-3; ICES-003 Class A; AS/NZS CISPR22 Class A; FCC (CFR 47, Part 15) Class A; GB9254	VCCI Class A; EN 55022 Class A; CISPR 22 Class A; IEC/EN 61000-3-2; IEC/EN 61000-3-3; ICES-003 Class A; AS/NZS CISPR22 Class A; FCC (CFR 47, Part 15) Class A; GB9254	VCCI Class A; EN 55022 Class A; CISPR 22 Class A; IEC/EN 61000-3-2; IEC/EN 61000-3-3; ICES-003 Class A; AS/NZS CISPR22 Class A; FCC (CFR 47, Part 15) Class A; GB9254
Immunity			
Generic	Directive 2004/108/EC	Directive 2004/108/EC	Directive 2004/108/EC
EN	EN 55024:1998+ A1:2001 + A2:2003; ETSI EN 300 386 V1.3.3	EN 55024:1998+ A1:2001 + A2:2003; ETSI EN 300 386 V1.3.3	EN 55024:1998+ A1:2001 + A2:2003; ETSI EN 300 386 V1.3.3
ESD	EN 61000-4-2	EN 61000-4-2	EN 61000-4-2
Radiated	EN 61000-4-3	EN 61000-4-3	EN 61000-4-3
EFT/Burst	EN 61000-4-4	EN 61000-4-4	EN 61000-4-4

Specifications (continued)

	HP 10508-V Switch Chassis (JC611A)	HP 10508 Switch Chassis (JC612A)	HP 10504 Switch Chassis (JC613A)
Surge	EN 61000-4-5	EN 61000-4-5	EN 61000-4-5
Conducted	EN 61000-4-6	EN 61000-4-6	EN 61000-4-6
Power frequency magnetic field	IEC 61000-4-8	IEC 61000-4-8	IEC 61000-4-8
Voltage dips and interruptions	EN 61000-4-11	EN 61000-4-11	EN 61000-4-11
Harmonics	EN 61000-3-2, IEC 61000-3-2	EN 61000-3-2, IEC 61000-3-2	EN 61000-3-2, IEC 61000-3-2
Flicker	EN 61000-3-3, IEC 61000-3-3	EN 61000-3-3, IEC 61000-3-3	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; command-line interface; out-of-band management (serial RS-232C); SNMP Manager; Telnet; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB	IMC - Intelligent Management Center; command-line interface; out-of-band management (serial RS-232C); SNMP Manager; Telnet; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB	IMC - Intelligent Management Center; command-line interface; out-of-band management (serial RS-232C); SNMP Manager; Telnet; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB
Services	3-year, parts only, global next-day advance exchange (HT092E)	3-year, parts only, global next-day advance exchange (HT092E)	3-year, parts only, global next-day advance exchange (HT059E)
	3-year, 4-hour onsite, 13x5 coverage for hardware (HT093E)	3-year, 4-hour onsite, 13x5 coverage for hardware (HT093E)	3-year, 4-hour onsite, 13x5 coverage for hardware (HT060E)
	3-year, 4-hour onsite, 24x7 coverage for hardware (HT095E)	3-year, 4-hour onsite, 24x7 coverage for hardware (HT095E)	3-year, 4-hour onsite, 24x7 coverage for hardware (HT062E)
	3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (HT100E)	3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (HT100E)	3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (HT067E)
	3-year, 24x7 SW phone support, software updates (HT099E)	3-year, 24x7 SW phone support, software updates (HT099E)	3-year, 24x7 SW phone support, software updates (HT066E)
	Installation with minimum configuration, system-based pricing (UX033E)	Installation with minimum configuration, system-based pricing (UX033E)	Installation with minimum configuration, system-based pricing (UX033E)
	4-year, 4-hour onsite, 13x5 coverage for hardware (HT101E)	4-year, 4-hour onsite, 13x5 coverage for hardware (HT101E)	4-year, 4-hour onsite, 13x5 coverage for hardware (HT068E)
	4-year, 4-hour onsite, 24x7 coverage for hardware (HT103E)	4-year, 4-hour onsite, 24x7 coverage for hardware (HT103E)	4-year, 4-hour onsite, 24x7 coverage for hardware (HT070E)
	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HT108E)	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HT108E)	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HT075E)
	4-year, 24x7 SW phone support, software updates (HT107E)	4-year, 24x7 SW phone support, software updates (HT107E)	4-year, 24x7 SW phone support, software updates (HT074E)
	5-year, 4-hour onsite, 13x5 coverage for hardware (HT109E)	5-year, 4-hour onsite, 13x5 coverage for hardware (HT109E)	5-year, 4-hour onsite, 13x5 coverage for hardware (HT076E)
	5-year, 4-hour onsite, 24x7 coverage for hardware (HT111E)	5-year, 4-hour onsite, 24x7 coverage for hardware (HT111E)	5-year, 4-hour onsite, 24x7 coverage for hardware (HT078E)
	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HT116E)	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HT116E)	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HT083E)
	5-year, 24x7 SW phone support, software updates (HT115E)	5-year, 24x7 SW phone support, software updates (HT115E)	5-year, 24x7 SW phone support, software updates (HT082E)
	3 Yr 6 hr Call-to-Repair Onsite (HT097E)	3 Yr 6 hr Call-to-Repair Onsite (HT097E)	3 Yr 6 hr Call-to-Repair Onsite (HT064E)
	4 Yr 6 hr Call-to-Repair Onsite (HT105E)	4 Yr 6 hr Call-to-Repair Onsite (HT105E)	4 Yr 6 hr Call-to-Repair Onsite (HT072E)
	5 Yr 6 hr Call-to-Repair Onsite (HT113E)	5 Yr 6 hr Call-to-Repair Onsite (HT113E)	5 Yr 6 hr Call-to-Repair Onsite (HT080E)
	1-year, 4-hour onsite, 13x5 coverage for hardware (HT084E)	1-year, 4-hour onsite, 13x5 coverage for hardware (HT084E)	1-year, 4-hour onsite, 13x5 coverage for hardware (HT051E)
	1-year, 4-hour onsite, 24x7 coverage for hardware (HT086E)	1-year, 4-hour onsite, 24x7 coverage for hardware (HT086E)	1-year, 4-hour onsite, 24x7 coverage for hardware (HT053E)
	1-year, 6 hour Call-To-Repair Onsite for hardware (HT088E)	1-year, 6 hour Call-To-Repair Onsite for hardware (HT088E)	1-year, 6 hour Call-To-Repair Onsite for hardware (HT055E)
	1-year, 24x7 software phone support, software updates (HT090E)	1-year, 24x7 software phone support, software updates (HT090E)	1-year, 24x7 software phone support, software updates (HT057E)
	1-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support and software updates (HT091E)	1-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support and software updates (HT091E)	1-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support and software updates (HT058E)
	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Specifications (continued)

	HP 10508-V Switch Chassis (JC611A)	HP 10508 Switch Chassis (JC612A)	HP 10504 Switch Chassis (JC613A)
Standards and protocols (applies to all products in series)	**BGP** RFC 1771 BGPv4 RFC 1772 Application of the BGP RFC 1965 BGP4 confederations RFC 1997 BGP Communities Attribute RFC 1998 PPP Gandalf FZA Compression Protocol RFC 2385 BGP Session Protection via TCP MD5 RFC 2439 BGP Route Flap Damping RFC 2796 BGP Route Reflection RFC 2858 BGP-4 Multi-Protocol Extensions RFC 2918 Route Refresh Capability RFC 3065 Autonomous System Confederations for BGP RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4) RFC 4272 BGP Security Vulnerabilities Analysis RFC 4273 Definitions of Managed Objects for BGP-4 RFC 4274 BGP-4 Protocol Analysis RFC 4275 BGP-4 MIB Implementation Survey RFC 4276 BGP-4 Implementation Report RFC 4277 Experience with the BGP-4 Protocol RFC 4360 BGP Extended Communities Attribute RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) RFC 5291 Outbound Route Filtering Capability for BGP-4 RFC 5292 Address-Prefix-Based Outbound Route Filter for BGP-4 **Denial of service protection** RFC 2267 Network Ingress Filtering Automatic filtering of well-known denial-of-service packets CPU DoS Protection Rate Limiting by ACLs **Device management** RFC 1157 SNMPv1/v2c RFC 1305 NTPv3 RFC 1902 (SNMPv2) RFC 2271 FrameWork RFC 2579 (SMIv2 Text Conventions) RFC 2580 (SMIv2 Conformance) RFC 2819 (RMON groups Alarm, Event, History and Statistics only) HTTP, SSHv1, and Telnet Multiple Configuration Files Multiple Software Images SSHv1/SSHv2 Secure Shell TACACS/TACACS+ Web UI **General protocols** IEEE 802.1ad Q-in-Q IEEE 802.1ag Service Layer OAM IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1X PAE IEEE 802.3ab 1000BASE-T IEEE 802.3ac (VLAN Tagging Extension) IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3af Power over Ethernet IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber - EFMF IEEE 802.3at IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP	RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 894 IP over Ethernet RFC 903 RARP RFC 906 TFTP Bootstrap RFC 925 Multi-LAN Address Resolution RFC 950 Internet Standard Subnetting Procedure RFC 959 File Transfer Protocol (FTP) RFC 1027 Proxy ARP RFC 1035 Domain Implementation and Specification RFC 1042 IP Datagrams RFC 1058 RIPv1 RFC 1142 OSI IS-IS Intra-domain Routing Protocol RFC 1195 OSI ISIS for IP and Dual Environments RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1293 Inverse Address Resolution Protocol RFC 1305 NTPv3 RFC 1350 TFTP Protocol (revision 2) RFC 1393 Traceroute Using an IP Option RFC 1519 CIDR RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1701 Generic Routing Encapsulation RFC 1721 RIP-2 Analysis RFC 1723 RIP v2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2082 RIP-2 MD5 Authentication RFC 2091 Trigger RIP RFC 2131 DHCP RFC 2138 Remote Authentication Dial In User Service (RADIUS) RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2 RFC 2644 Directed Broadcast Control RFC 2763 Dynamic Name-to-System ID mapping support RFC 2784 Generic Routing Encapsulation (GRE) RFC 2865 Remote Authentication Dial In User Service (RADIUS) RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS RFC 2973 IS-IS Mesh Groups RFC 3022 Traditional IP Network Address Translator (Traditional NAT) RFC 3277 IS-IS Transient Blackhole Avoidance RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS) RFC 3784 ISIS TE support RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS) RFC 3847 Restart signaling for IS-IS RFC 4251 The Secure Shell (SSH) Protocol Architecture RFC 4884 Extended ICMP to Support Multi-Part Messages RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6 RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags **IP multicast**	RFC 2236 IGMPv2 RFC 2283 Multiprotocol Extensions for BGP-4 RFC 2362 PIM Sparse Mode RFC 3376 IGMPv3 RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) RFC 3618 Multicast Source Discovery Protocol (MSDP) RFC 3973 PIM Dense Mode RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches RFC 4601 Draft 10 PIM Sparse Mode RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast RFC 4605 IGMP/MLD Proxying RFC 4607 Source-Specific Multicast for IP RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) **IPv6** RFC 1886 DNS Extension for IPv6 RFC 1887 IPv6 Unicast Address Allocation Architecture RFC 1981 IPv6 Path MTU Discovery RFC 2080 RIPng for IPv6 RFC 2081 RIPng Protocol Applicability Statement RFC 2292 Advanced Sockets API for IPv6 RFC 2373 IPv6 Addressing Architecture RFC 2375 IPv6 Multicast Address Assignments RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2462 IPv6 Stateless Address Auto-configuration RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2473 Generic Packet Tunneling in IPv6 RFC 2526 Reserved IPv6 Subnet Anycast Addresses RFC 2529 Transmission of IPv6 Packets over IPv4 RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2710 Multicast Listener Discovery (MLD) for IPv6 RFC 2740 OSPFv3 for IPv6 RFC 2767 Dual stacks IPv46 & IPv6 RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers RFC 3056 Connection of IPv6 Domains via IPv4 Clouds RFC 3307 IPv6 Multicast Address Allocation RFC 3315 DHCPv6 (client and relay) RFC 3484 Default Address Selection for IPv6 RFC 3513 IPv6 Addressing Architecture RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 RFC 3810 MLDv2 for IPv6 RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration **MIBs** RFC 1156 (TCP/IP MIB) RFC 1157 A Simple Network Management Protocol (SNMP) RFC 1215 A Convention for Defining Traps for use with the SNMP RFC 1229 Interface MIB Extensions RFC 1493 Bridge MIB RFC 1573 SNMP MIB II RFC 1643 Ethernet MIB RFC 1657 BGP-4 MIB

Specifications (continued)

	HP 10508-V Switch Chassis (JC611A)	HP 10508 Switch Chassis (JC612A)	HP 10504 Switch Chassis (JC613A)
Standards and protocols (applies to all products in series)	RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP RFC 2013 SNMPv2 MIB for UDP RFC 2096 IP Forwarding Table MIB RFC 2233 Interface MIB RFC 2452 IPV6-TCP-MIB RFC 2454 IPV6-UDP-MIB RFC 2465 IPv6 MIB RFC 2466 ICMPv6 MIB RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB RFC 2573 SNMP-Notification MIB RFC 2573 SNMP-Target MIB RFC 2578 Structure of Management Information Version 2 (SMIv2) RFC 2580 Conformance Statements for SMIv2 RFC 2618 RADIUS Client MIB RFC 2620 RADIUS Accounting MIB RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2787 VRRP MIB RFC 2819 RMON MIB RFC 2925 Ping MIB RFC 2932IP (Multicast Routing MIB) RFC 2933 IGMP MIB RFC 2934 Protocol Independent Multicast MIB for IPv4 RFC 3414 SNMP-User based-SM MIB RFC 3415 SNMP-View based-ACM MIB RFC 3417 Simple Network Management Protocol (SNMP) over IEEE 802 Networks RFC 3418 MIB for SNMPv3 RFC 3595 Textual Conventions for IPv6 Flow Label RFC 3621 Power Ethernet MIB RFC 3813 MPLS LSR MIB RFC 3814 MPLS FTN MIB RFC 3815 MPLS LDP MIB RFC 3826 AES for SNMP's USM MIB RFC 4133 Entity MIB (Version 3) RFC 4444 Management Information Base for Intermediate System to Intermediate System (IS-IS) **MPLS** RFC 2205 Resource ReSerVation Protocol RFC 2209 Resource ReSerVation Protocol (RSVP) RFC 2702 Requirements for Traffic Engineering Over MPLS RFC 2858 Multiprotocol Extensions for BGP-4 RFC 2961 RSVP Refresh Overhead Reduction Extensions RFC 3031 Multiprotocol Label Switching Architecture RFC 3032 MPLS Label Stack Encoding RFC 3107 Carrying Label Information in BGP-4 RFC 3212 Constraint-Based LSP Setup using LDP RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP) RFC 3487 Graceful Restart Mechanism for LDP RFC 3564 Requirements for Support of Differentiated Service-aware MPLS Traffic Engineering RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4379 Detecting Multi-Protocol Label Switched	(MPLS) Data Plane Failures RFC 4447 Pseudowire Setup and Maintenance Using LDP RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks RFC 4664 Framework for Layer 2 Virtual Private Networks RFC 4665 Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling RFC 5036 LDP Specification **Network management** IEEE 802.1AB Link Layer Discovery Protocol (LLDP) RFC 1155 Structure of Management Information RFC 1157 SNMPv1 RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 2211 Controlled-Load Network RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) RFC 3176 sFlow RFC 3411 SNMP Management Frameworks RFC 3412 SNMPv3 Message Processing RFC 3414 SNMPv3 User-based Security Model (USM) RFC 3415 SNMPv3 View-based Access Control Model VACM) ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) **OSPF** RFC 1245 OSPF protocol analysis RFC 1246 Experience with OSPF RFC 1765 OSPF Database Overflow RFC 1850 OSPFv2 Management Information Base (MIB), traps RFC 2154 OSPF w/ Digital Signatures (Password, MD-5) RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option RFC 3101 OSPF NSSA RFC 3137 OSPF Stub Router Advertisement RFC 3623 Graceful OSPF Restart RFC 3630 Traffic Engineering Extensions to OSPFv2 RFC 4061 Benchmarking Basic OSPF Single Router Control Plane Convergence RFC 4062 OSPF Benchmarking Terminology and Concepts RFC 4063 Considerations When Using Basic OSPF Convergence Benchmarks RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4811 OSPF Out-of-Band LSDB Resynchronization RFC 4812 OSPF Restart Signaling	RFC 4813 OSPF Link-Local Signaling RFC 4940 IANA Considerations for OSPF **QoS/CoS** IEEE 802.1P (CoS) RFC 1349 Type of Service in the Internet Protocol Suite RFC 2211 Specification of the Controlled-Load Network Element Service RFC 2212 Guaranteed Quality of Service RFC 2474 DSCP DiffServ RFC 2475 DiffServ Architecture RFC 2597 DiffServ Assured Forwarding (AF) RFC 2598 DiffServ Expedited Forwarding (EF) **Security** IEEE 802.1X Port Based Network Access Control RFC 1321 The MD5 Message-Digest Algorithm RFC 1334 PPP Authentication Protocols (PAP) RFC 1492 TACACS+ RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 The Internet Key Exchange (IKE) RFC 2716 PPP EAP TLS Authentication Protocol RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2869 RADIUS Extensions Access Control Lists (ACLs) Guest VLAN for 802.1x MAC Authentication Port Security SSHv1/SSHv2 Secure Shell **VPN** RFC 2403 - HMAC-MD5-96 RFC 2404 - HMAC-SHA1-96 RFC 2405 - DES-CBC Cipher algorithm RFC 2407 - Domain of interpretation RFC 2547 BGP/MPLS VPNs RFC 2917 A Core MPLS IP VPN Architecture RFC 3947 - Negotiation of NAT-Traversal in the IKE RFC 4302 - IP Authentication Header (AH) RFC 4303 - IP Encapsulating Security Payload (ESP) **IPsec** RFC 1828 IP Authentication using Keyed MD5 RFC 1829 The ESP DES-CBC Transform RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention RFC 2401 IP Security Architecture RFC 2402 IP Authentication Header RFC 2406 IP Encapsulating Security Payload RFC 2410 - The NULL Encryption Algorithm and its use with IPsec RFC 2411 IP Security Document Roadmap

HP 10500 Switch Series accessories

Modules

HP 10500 Main Processing Unit (JC614A)
HP 10500 16-port GbE SFP/8-port GbE Combo/2-port 10GbE XFP SE Module (JC617A)
HP 10500 48-port Gig-T SE Module (JC618A)
HP 10500 48-port GbE SFP SE Module (JC619A)
HP 10500 4-port 10GbE XFP SE Module (JC620A)
HP 10500 16-port GbE SFP/8-port GbE Combo/2-port 10GbE XFP EA Module (JC621A)
HP 10500 48-port GbE SFP EA Module (JC622A)
HP 10500 48-port Gig-T EA Module (JC623A)
HP 10500 4-port 10GbE XFP EA Module (JC624A)
HP 10500 48-port GbE SFP EB Module (JC625A)
HP 10500 16-port GbE SFP/8-port GbE Combo/2-port 10GbE XFP EB Module (JC626A)
HP 10500 4-port 10GbE XFP EB Module (JC627A)
HP 10500 16-port 10GbE SFP+ SC Module (JC628A)
HP 10500 8-port 10GbE SFP+ EB Module (JC629A)
HP 10500 8-port 10GbE SFP+ EA Module (JC630A)
HP 10500 8-port 10GbE SFP+ SE Module (JC631A)

Transceivers

HP X180 10G XFP LC LH 80km 1560.61nm DWDM Transceiver (JG233A)
HP X180 10G XFP LC LH 80km 1559.79nm DWDM Transceiver (JG232A)
HP X180 10G XFP LC LH 80km 1558.98nm DWDM Transceiver (JG231A)
HP X180 10G XFP LC LH 80km 1542.94nm DWDM Transceiver (JG230A)
HP X180 10G XFP LC LH 80km 1542.14nm DWDM Transceiver (JG229A)
HP X180 10G XFP LC LH 80km 1540.56nm DWDM Transceiver (JG228A)
HP X180 10G XFP LC LH 80km 1539.77nm DWDM Transceiver (JG227A)
HP X180 10G XFP LC LH 80km 1538.98nm DWDM Transceiver (JG226A)
HP X130 10G SFP+ LC ER 40km Transceiver (JG234A)
HP X125 1G SFP LC LH40 1310nm Transceiver (JD061A)
HP X120 1G SFP LC LH40 1550nm Transceiver (JD062A)
HP X125 1G SFP LC LH70 Transceiver (JD063B)
HP X120 1G SFP RJ45 T Transceiver (JD089B)
HP X110 100M SFP LC LH40 Transceiver (JD090A)
HP X110 100M SFP LC LH80 Transceiver (JD091A)
HP X130 10G SFP+ LC SR Transceiver (JD092B)
HP X130 10G SFP+ LC LRM Transceiver (JD093B)
HP X130 10G SFP+ LC LR Transceiver (JD094B)
HP X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable (JD095B)
HP X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable (JD096B)
HP X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable (JD097B)
HP X120 1G SFP LC BX 10-U Transceiver (JD098B)
HP X120 1G SFP LC BX 10-D Transceiver (JD099B)
HP X115 100M SFP LC BX 10-U Transceiver (JD100A)
HP X115 100M SFP LC BX 10-D Transceiver (JD101A)
HP X110 100M SFP LC FX Transceiver (JD102B)
HP X120 1G SFP LC LH100 Transceiver (JD103A)
HP X130 10G XFP LC ZR Transceiver (JD107A)
HP X130 10G XFP LC LR Transceiver (JD108B)
HP X170 1G SFP LC LH70 1550 Transceiver (JD109A)
HP X170 1G SFP LC LH70 1570 Transceiver (JD110A)
HP X170 1G SFP LC LH70 1590 Transceiver (JD111A)
HP X170 1G SFP LC LH70 1610 Transceiver (JD112A)
HP X170 1G SFP LC LH70 1470 Transceiver (JD113A)
HP X170 1G SFP LC LH70 1490 Transceiver (JD114A)
HP X170 1G SFP LC LH70 1510 Transceiver (JD115A)
HP X170 1G SFP LC LH70 1530 Transceiver (JD116A)
HP X130 10G XFP LC SR Transceiver (JD117B)
HP X120 1G SFP LC SX Transceiver (JD118B)
HP X120 1G SFP LC LX Transceiver (JD119B)
HP X110 100M SFP LC LX Transceiver (JD120B)
HP X135 10G XFP LC ER Transceiver (JD121A)
HP X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable (JG081B)

Power Supply

HP 10500 2500W AC Power Supply (JC610A)

Mounting Kit

HP X421 A-Series Chassis Universal 4-post Rack Mounting Kit (JC665A)

HP 10508-V Switch Chassis (JC611A)

HP 10508/10508-V 640Gbps Type A Fabric Module (JC616A)
HP 10508-V Spare Fan Assembly (JC634A)

HP 10508 Switch Chassis (JC612A)

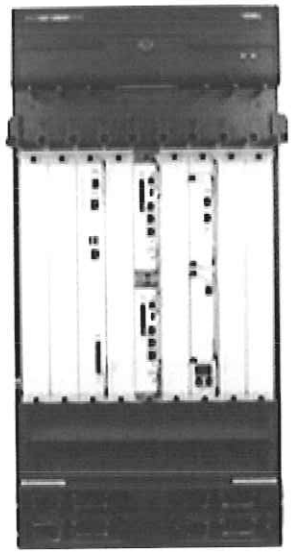
HP 10508/10508-V 640Gbps Type A Fabric Module (JC616A)
HP 10508 Spare Fan Assembly (JC633A)

HP 10504 Switch Chassis (JC613A)

HP 10504 320Gbps Type A Fabric Module (JC615A)
HP 10504 Spare Fan Assembly (JC632A)

To learn more, visit www.hp.com/networking

4AA3-6264ENW, Created August 2011; Updated October 2011, Rev. 2



HP 6600 Router Series

Data sheet

Product overview

As the first service convergence routers based on a multi-core processor, the HP 6600 series routers dramatically enhance service processing capacity with HP FlexNetwork architecture. Distributed processing architecture, isolated routing, and service engines, as well as isolated control and service panels, provide higher reliability and continual services. Different software service engines can handle different services such as network address translation (NAT), Quality of Service (QoS), IPsec, and NetStream with no services modules needed. 6600 routers feature a modular design, embedded hardware encryption, and flexible deployment configurations, including High-speed Interface Modules (HIMs), Multi-function Interface Modules (MIMs), and Open Application Architecture (OAA)-enabled modules that provide network customization and investment protection. These routers provide carrier-class reliability at network, device, link, and service layers.

Key features

- Multi-core CPU and distributed processing
- Carrier-class reliability and aggregation
- Open Application Architecture platform
- Embedded hardware encryption
- Fully redundant and hot-swappable hardware

Features and benefits

Quality of Service (QoS)

- **Traffic policing:** supports Committed Access Rate (CAR) and line rate
- **Congestion management:** supports FIFO, PQ, CQ, WFQ, CBQ, and RTPQ
- **Other QoS technologies:** supports traffic shaping, FR QoS, MPLS QoS, and MP QoS/LFI
- **Congestion avoidance:** weighted Random Early Detection (WRED)/RED

Management

- **Management interface control:** provides management access through modem port and terminal interface, as well as in-band and out-of-band Ethernet ports
- **Management security:** includes multiple administration levels, with password protection and restricted access to critical configuration commands; access control lists (ACLs) provide telnet and SNMP access; local and remote syslog capability allows logging of all access
- **SNMP v1, v2, and v3:** provides complete support of SNMP as well as full support of industry-standard MIBs and private MIB extensions
- **Industry-standard CLI with a hierarchical structure:** reduces training needs and increases productivity in multivendor installations
- **Remote monitoring (RMON):** uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- **Debug and sampler utility:** supports ping and traceroute for both IPv4 and IPv6
- **Network Quality Analyzer (NQA):** analyzes network performance and service quality by sending test packets, and provides network performance and service quality parameters such as jitter, TCP, or FTP connection delays and file transfer rates; allows network manager to determine overall network performance and to diagnose and locate network congestion points or failures
- **Network Time Protocol (NTP):** synchronizes timekeeping among distributed time servers and clients; keeps consistent timekeeping among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time
- **Info center:** provides a central information center for system and network information; aggregates all logs, traps, and debugging information generated by the system and maintains them in order of severity; outputs the network information to multiple channels based on user-defined rules
- **FTP and TFTP support:** File Transfer Protocol allows bidirectional transfers over a TCP/IP network and is used for configuration updates; Trivial FTP is a simpler method using User Datagram Protocol (UDP)
- **Loopback:** supports internal loopback testing for maintenance purposes and high availability; loopback detection protects the system from incorrect cabling or network configurations and can be enabled on a port or VLAN
- **Internet Group Management Protocol (IGMP):** is used by IP hosts to establish and maintain multicast groups; supports v1, v2, and v3; utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks

Connectivity

- **NEW High port density:** provides up to 16 interface module slots, and high-density Ethernet interface cards; a single card can provide up to 48 GbE interfaces; therefore, the routers can fully satisfy the demands of high-density Ethernet (MSTP) link distribution
- **Multiple WAN interfaces:** support Fast Ethernet/Gigabit Ethernet/10 GbE ports, OC3~OC48 POS/CPOS, and ATM ports
- **Flexible port selection:** provides a combination of fiber and copper interface modules, 100/1000BASE-X auto speed selection, and 10/100/1000BASE-T auto speed detection plus auto duplex and MDI/MDI-X; speed is adaptable between 155 M POS and 622 M POS

Performance

- **NEW Industry-leading performance:** provides up to 252 Mpps forwarding performance
- **Flexible chassis selection:** consists of 4 models: 16 HIM-slot chassis, 8 HIM-slot chassis, 4 HIM-slot chassis, and 2 HIM-slot chassis
- **Scalable system design:** backplane is designed for smooth bandwidth upgrade

Resiliency and high availability

- **Separate data and control planes:** provide greater flexibility and enable continual services
- **Hitless software upgrades:** allow patches to be installed without restarting the device, increasing network uptime and simplifying maintenance
- **Redundant design of main processing unit and power supply:** increases the overall system availability
- **Virtual Router Redundancy Protocol (VRRP):** enables fast convergence of routes and packet forwarding when links fail, ensuring high network availability
- **IP Fast Reroute Framework (FRR):** nodes are configured with backup ports and routes; local implementation requires no cooperation of adjacent devices, simplifying the deployment; solves the traditional convergence faults in IP forwarding; realizes restoration within 50 ms, with the restoration time independent of the number of routes and fast link switchovers without route convergence
- **Graceful restart:** features are fully supported, including graceful restart for OSPF, IS-IS, Border Gateway Protocol (BGP), LDP, and RSVP; network remains stable during the active-standby switchover; after the switchover, the device quickly learns the network routes by communicating with adjacent routers; forwarding remains uninterrupted during the switchover to realize nonstop forwarding (NSF)
- **Hot-swappable modules:** help ensure the replacement of hardware interface modules without impacting the traffic flow through the system

Layer 3 services

- **Address Resolution Protocol (ARP):** determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
- **User Datagram Protocol (UDP) helper:** redirects UDP broadcasts to specific IP subnets to prevent server spoofing
- **Dynamic Host Configuration Protocol (DHCP):** simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
- **Domain Name System (DNS):** is a distributed database that provides translation between a domain name and an IP address, which simplifies network design; supports client and server

Layer 3 routing

- **Static IPv4 routing:** provides simple, manually configured IPv4 routing
- **Routing Information Protocol:** uses a distance vector algorithm with UDP packets for route determination; supports RIPv1 and RIPv2 routing; includes loop protection
- **OSPF:** Interior Gateway Protocol (IGP) using link-state protocol for faster convergence; supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery
- **Intermediate system to intermediate system (IS-IS):** Interior Gateway Protocol (IGP) using path vector protocol, which is defined by the ISO organization for IS-IS routing and extended by IETF RFC 1195 to operate in both TCP/IP and the OSI reference model (Integrated IS-IS)
- **Static IPv6 routing:** provides simple, manually configured IPv6 routing
- **Dual IP stack:** maintains separate stacks for IPv4 and IPv6 to ease transition from an IPv4-only network to an IPv6-only network design
- **Routing Information Protocol next generation (RIPng):** extends RIPv2 to support IPv6 addressing
- **OSPFv3:** provides OSPF support for IPv6
- **BGP+:** extends BGP-4 to support Multiprotocol BGP (MBGP), including support for IPv6 addressing
- **IS-IS for IPv6:** extends IS-IS to support IPv6 addressing
- **IPv6 tunneling:** is an important element for the transition from IPv4 to IPv6; allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6to4, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels
- **Multiprotocol Label Switching (MPLS):** uses BGP to advertise routes across Label Switched Paths (LSPs), but uses simple labels to forward packets from any Layer 2 or Layer 3 protocol, thus reducing complexity and increasing performance; supports graceful restart for reduced failure impact; supports LSP tunneling and multilevel stacks
- **Multiprotocol Label Switching (MPLS) Layer 3 VPN:** allows Layer 3 VPNs across a provider network; uses MP-BGP to establish private routes for increased security; supports RFC 2547bis multiple autonomous system VPNs for added flexibility

- **Multiprotocol Label Switching (MPLS) Layer 2 VPN:** establishes simple Layer 2 point-to-point VPNs across a provider network using only MPLS Label Distribution Protocol (LDP); requires no routing and therefore decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; supports Circuit Cross Connect (CCC), Static Virtual Circuits (SVCs), Martini draft, and Kompella-draft technologies
- **Policy routing:** allows custom filters for increased performance and security; supports ACLs, IP prefix, AS paths, community lists, and aggregate policies
- **Multicast VPN:** supports Multicast Domain (MD) multicast VPN, which can be distributed on separate service cards, providing high performance and flexible configuration
- **Border Gateway Protocol 4:** Exterior Gateway Protocol (EGP) with path vector protocol uses TCP for enhanced reliability for the route discovery process, reduces bandwidth consumption by advertising only incremental updates, and supports extensive policies to increase flexibility and scale to large networks
- **OSPFv3 MCE:** Multi-VPN-Instance CE (MCE) binds different VPNs to different interfaces on one single CE; the OSPFv3 MCE feature creates and maintains separate OSPFv3 routing tables for each IPv6 VPN to isolate VPN services in the device

Security

- **Access control list:** supports powerful ACLs for both IPv4 and IPv6; ACLs are used for filtering traffic to prevent illegal users from accessing the network or for controlling network traffic flow; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header; rules can also be set to operate on specific dates or times
- **RADIUS:** eases switch security access administration by using a password authentication server
- **TACACS+:** is an authentication tool using TCP with encryption of the full authentication request that provides additional security
- **Network address translation (NAT):** supports repeated multiplexing of a port and automatic 5-tuple collision detection, enabling NAPT to support unlimited connections; supports blacklist in NAT/NAPT/internal server, a limit on the number of connections, session log, and multi-instance
- **Secure Shell (SSHv2):** uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers
- **Unicast Reverse Path Forwarding (URPF):** allows normal packets to be forwarded correctly, but discards the attaching packet due to lack of reverse path route or incorrect inbound interface; prevents source spoofing and distributed attacks; supports distributed URPF
- **DVPN (Dynamic Virtual Private Network):** collects, maintains, and distributes dynamic public addresses through the VPN Address Management (VAM) protocol, making VPN establishment available between enterprise branches that use dynamic addresses to access the public network; compared to traditional VPN technologies, DVPN technology is more flexible and has richer features, such as NAT traversal of DVPN packets, AAA identity authentication, IPsec protection of data packets, and multiple VPN domains

Multicast support

- **Internet Group Management Protocol (IGMP):** is used by IP hosts to establish and maintain multicast groups; supports v1, v2, and v3; utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks
- **Protocol Independent Multicast (PIM):** is used for IPv4 and IPv6 multicast applications; supports PIM Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Source-Specific Mode (PIM-SSM)
- **Multicast Source Discovery Protocol (MSDP):** is used for interdomain multicast applications, allowing multiple PIM-SM domains to interoperate
- **Multicast Border Gateway Protocol (MBGP):** allows multicast traffic to be forwarded across BGP networks, separate from unicast traffic

Integration

- **Embedded VPN firewall:** provides enhanced stateful packet inspection and filtering; provides advanced VPN services with 3DES and AES encryption at high performance and low latency
- **Open Application Architecture (OOA):** provides both software and hardware platform based on open standards so that third-party applications can be integrated seamlessly into routers

Additional information

- **Green initiative support:** provides support for RoHS and WEEE regulations

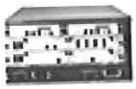
Product architecture

- **Multi-core CPU:** the first service convergence router based on multi-core, multi-thread processing, with eight cores and 32 hardware threads
- **Distributed processing:** the main processing engine and service engine have separate hardware for high performance and parallel processing; the main processing engine is used for route calculation and system management, while the service engine is used for service processing
- **Separate FIP card and interface card:** interface cards are separated from the FIP card to support flexible service configurations

Warranty and support

- **1-year warranty:** with advance replacement and 30-calendar-day delivery (available in most countries)
- **Electronic and telephone support:** limited electronic and telephone support is available from HP; refer to www.hp.com/networking/warranty for details on the support provided and the period during which support is available
- **Software releases:** refer to www.hp.com/networking/warranty for details on the software releases provided and the period during which software releases are available for your product(s)

Specifications

	 HP 6602 Router Chassis (JC176A)	 HP 6604 Router Chassis (JC178B)
Ports	2 HIM slots	4 HIM slots 2 MPU (for management modules) slots
Physical characteristics		
Dimensions	18.11(d) x 17.40(w) x 1.73(h) in. (46 x 44.2 x 4.4 cm) (1U height)	18.9(d) x 17.17(w) x 8.66(h) in. (48.01 x 43.61 x 22 cm) (5U height)
Full configuration weight	16.53 lb. (7.5 kg)	83.77 lb. (38 kg)
Memory and processor	Multi-core MIPS @ 1000 MHz, 2 GB DDR2 SDRAM, 4 GB DDR2 SDRAM, 256 MB flash, 1 GB flash; packet buffer size: 128 MB DDR2 SDRAM	
Mounting	EIA standard 19 in. rack	EIA standard 19 in. rack
Performance		
Throughput	4.5 million pps	up to 36 million pps
Routing table size	1000000 entries	2000000 entries
Environment		
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing
Electrical characteristics		
Maximum heat dissipation	512 BTU/hr (540.16 kJ/hr)	2217 BTU/hr (2338.94 kJ/hr)
Voltage	100-120/200-240 VAC	100-120/200-240 VAC
Maximum power rating	150 W	650 W
Frequency	50/60 Hz	50/60 Hz
Notes	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.
Safety	CSA 22.2 No. 60950; cUL (CSA 22.2 No. 60950); CSA 22.2 No. 60950 3rd edition; CSA 22.2 No. 950; CSA 950; cUL (CSA 950); EN 60950/IEC 60950; UL 1950 3rd edition; UL 1950; UL 60950; UL 60950-1; CAN/CSA 22.2 No. 60950; CAN/CSA 22.2 No. 60950-1; EN 60825; AS/NZS 60950; KN 60950; GOST R MEK60950; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; EN 609500 Safety Information Technology Equipment; UL 60950; CSA 22.2 No. 60950/cUL; IEC 60950; IEC 60950-1; EN 60950; EN 60950-1; IEC 60825; CSA 22.2 No. 950-95; IEC 60950-1:2001 (with CB Report); CAN/CSA-C22.2 No. 60950-1-03; CAN/CSA-C22.2 No. 60950-1; CSA 60950-1; CSA C22.2 60950-1; EU RoHS Compliant; EN 60950-1/A11; CSA 22.2 60950-1; EN 60950: 2000, ZB and ZC Deviations; IEC 60950: 1999, Corr Feb 2000, all national deviations; As/NZS 60950:2000, Australia; UL 60950-1:2003; UL 60950-1:2001; CSA 22.2 60950-1:2003; IEC 60950-1:2001; EN 60950-1:2001; CSA 22.2-60950; AS/NZS 60950: 2000 Australia, Russian GOST Safety Approval; CSA 22.2 No. 950 3rd Edition 1995; UL 60950 3rd Edition; CAN/CSA 22.2 No. 60950-00/UL 60950 3rd Edition, Safety Information for Technology Equipment; EN 60950/IEC 60950 3rd Edition; UL 60950 Standard for the Safety of Information Technology Equipment; EN 60825: Safety of Laser Products	CSA 22.2 No. 60950; cUL (CSA 22.2 No. 60950); CSA 22.2 No. 60950 3rd edition; CSA 22.2 No. 950; CSA 950; cUL (CSA 950); EN 60950/IEC 60950; UL 1950 3rd edition; UL 1950; UL 60950; UL 60950-1; CAN/CSA 22.2 No. 60950; CAN/CSA 22.2 No. 60950-1; EN 60825; AS/NZS 60950; KN 60950; GOST R MEK60950; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; EN 609500 Safety Information Technology Equipment; UL 60950; CSA 22.2 No. 60950/cUL; IEC 60950; IEC 60950-1; EN 60950; EN 60950-1; IEC 60825; CSA 22.2 No. 950-95; IEC 60950-1:2001 (with CB Report); CAN/CSA-C22.2 No. 60950-1-03; CAN/CSA-C22.2 No. 60950-1; CSA 60950-1; CSA C22.2 60950-1; EU RoHS Compliant; EN 60950-1/A11; CSA 22.2 60950-1; EN 60950: 2000, ZB and ZC Deviations; IEC 60950: 1999, Corr Feb 2000, all national deviations; As/NZS 60950:2000, Australia; UL 60950-1:2003; UL 60950-1:2001; CSA 22.2 60950-1:2003; IEC 60950-1:2001; EN 60950-1:2001; CSA 22.2-60950; AS/NZS 60950: 2000 Australia, Russian GOST Safety Approval; CSA 22.2 No. 950 3rd Edition 1995; UL 60950 3rd Edition; CAN/CSA 22.2 No. 60950-00/UL 60950 3rd Edition, Safety Information for Technology Equipment; EN 60950/IEC 60950 3rd Edition; UL 60950 Standard for the Safety of Information Technology Equipment; EN 60825: Safety of Laser Products
Emissions	FCC part 15 Class A; FCC Rules Part 15, Subpart B Class A; EN 55022/CISPR-22 Class A; VCCI Class A; EN 55022/CISPR 22 Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; CISPR 22/A2; IEC/EN 61000-3-2; IEC/EN 61000-3-3; EN 55024/A1; IEC 61000:4-2, 4-3, 4-4, 4-5, 4-6, 4-8, 4-11; BSMI CNS 13438; EMC Directive 89/336/EEC; ICES-003 Class A; ANSI C63.4 2003; CISPR 24; ETSI EN 300 386 V1.3.3; AS/NZS CISPR22 Class A; EN 61000-3-2; EN 61000-3-3; Korean EMI Class A; CNS 13438 Class A; EN 55024:1998; EN 61000-4-2; EN 61000-4-3; EN 61000-4-4; EN 61000-4-5; EN 61000-4-6; EN 61000-4-11	FCC part 15 Class A; FCC Rules Part 15, Subpart B Class A; EN 55022/CISPR-22 Class A; VCCI Class A; EN 55022/CISPR 22 Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; CISPR 22/A2; IEC/EN 61000-3-2; IEC/EN 61000-3-3; EN 55024/A1; IEC 61000:4-2, 4-3, 4-4, 4-5, 4-6, 4-8, 4-11; BSMI CNS 13438; EMC Directive 89/336/EEC; ICES-003 Class A; ANSI C63.4 2003; CISPR 24; ETSI EN 300 386 V1.3.3; AS/NZS CISPR22 Class A; EN 61000-3-2; EN 61000-3-3; Korean EMI Class A; CNS 13438 Class A; EN 55024:1998; EN 61000-4-2; EN 61000-4-3; EN 61000-4-4; EN 61000-4-5; EN 61000-4-6; EN 61000-4-11
Management	IMC - Intelligent Management Center; command-line interface; limited command-line interface; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); out-of-band management; SNMP Manager; Telnet; RMON1; FTP; in-line and out-of-band; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB	IMC - Intelligent Management Center; command-line interface; limited command-line interface; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); out-of-band management; SNMP Manager; Telnet; RMON1; FTP; in-line and out-of-band; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB
Services	3-year, parts only, global next-day advance exchange (HP826E) 3-year, 4-hour onsite, 13x5 coverage for hardware (HP830E) 3-year, 4-hour onsite, 24x7 coverage for hardware (HP817E) 3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (HP820E) 3-year, 24x7 SW phone support, software updates (HP823E)	3-year, parts only, global next-day advance exchange (UW054E) 3-year, 4-hour onsite, 13x5 coverage for hardware (UW062E) 3-year, 4-hour onsite, 24x7 coverage for hardware (UV930E) 3-year, 4-hour onsite, 24x7 coverage for hardware (HR530E) 3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (UV943E)

Specifications (continued)

	HP 6602 Router Chassis (JC176A)	HP 6604 Router Chassis (JC178B)
	1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (HR524E)	3-year, 24x7 SW phone support, software updates (UV955E)
	1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware (HR525E)	1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (HR529E)
	1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (HR526E)	1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (HR531E)
	4-year, 4-hour onsite, 13x5 coverage for hardware (HP831E)	4-year, 4-hour onsite, 13x5 coverage for hardware (UW063E)
	4-year, 4-hour onsite, 24x7 coverage for hardware (HP818E)	4-year, 4-hour onsite, 24x7 coverage for hardware (UV931E)
	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HP821E)	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UV944E)
	4-year, 24x7 SW phone support, software updates (HP824E)	4-year, 24x7 SW phone support, software updates (UV956E)
	5-year, 4-hour onsite, 13x5 coverage for hardware (HP832E)	5-year, 4-hour onsite, 13x5 coverage for hardware (UW064E)
	5-year, 4-hour onsite, 24x7 coverage for hardware (HP819E)	5-year, 4-hour onsite, 24x7 coverage for hardware (UV932E)
	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (HP822E)	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UV945E)
	5-year, 24x7 SW phone support, software updates (HP825E)	5-year, 24x7 SW phone support, software updates (UV957E)
	3 Yr 6 hr Call-to-Repair Onsite (HP827E)	3 Yr 6 hr Call-to-Repair Onsite (UW055E)
	4 Yr 6 hr Call-to-Repair Onsite (HP828E)	4 Yr 6 hr Call-to-Repair Onsite (UW056E)
	5 Yr 6 hr Call-to-Repair Onsite (HP829E)	5 Yr 6 hr Call-to-Repair Onsite (UW057E)
	1-year, 6 hour Call-To-Repair Onsite for hardware (HR528E)	1-year, 6 hour Call-To-Repair Onsite for hardware (HR533E)
	1-year, 24x7 software phone support, software updates (HR527E)	1-year, 24x7 software phone support, software updates (HR532E)
	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Specifications (continued)

	HP 6602 Router Chassis (JC176A)	HP 6604 Router Chassis (JC178B)

Standards and protocols
(applies to all products in series)

BGP
RFC 1267 Border Gateway Protocol 3 (BGP-3)
RFC 1657 Definitions of Managed Objects for BGPv4
RFC 1771 BGPv4
RFC 1772 Application of the BGP
RFC 1773 Experience with the BGP-4 Protocol
RFC 1774 BGP-4 Protocol Analysis
RFC 1965 BGP4 confederations
RFC 1997 BGP Communities Attribute
RFC 1998 PPP Gandalf FZA Compression Protocol
RFC 2385 BGP Session Protection via TCP MD5
RFC 2439 BGP Route Flap Damping
RFC 2796 BGP Route Reflection
RFC 2842 Capability Advertisement with BGP-4
RFC 2858 BGP-4 Multi-Protocol Extensions
RFC 2918 Route Refresh Capability

Denial of service protection
CPU DoS Protection
Rate Limiting by ACLs

Device management
RFC 1155 Structure and Mgmt Information (SMIv1)
RFC 1157 SNMPv1/v2c
RFC 1305 NTPv3
RFC 1901 (Community based SNMPv2)
RFC 1901-1907 SNMPv2c, SMIv2 and Revised MIB-II
RFC 1902 (SNMPv2)
RFC 1908 (SNMP v1/2 Coexistence)
RFC 1945 Hypertext Transfer Protocol - HTTP/1.0
RFC 2068 Hypertext Transfer Protocol - HTTP/1.1
RFC 2271 FrameWork
RFC 2452 MIB for TCP6
RFC 2454 MIB for UDP6
RFC 2573 (SNMPv3 Applications)
RFC 2576 (Coexistence between SNMP V1, V2, V3)
RFC 2578-2580 SMIv2
RFC 2579 (SMIv2 Text Conventions)
RFC 2580 (SMIv2 Conformance)
RFC 2819 (RMON groups Alarm, Event, History and Statistics only)
RFC 2819 RMON
RFC 3410 (Management Framework)
RFC 3416 (SNMP Protocol Operations v2)
RFC 3417 (SNMP Transport Mappings)
Multiple Configuration Files
Multiple Software Images
SNMP v3 and RMON RFC support
SSHv1/SSHv2 Secure Shell
TACACS/TACACS+

General protocols
IEEE 802.1ad Q-in-Q
IEEE 802.1ad Q-in-Q
IEEE 802.1ag Service Layer OAM
IEEE 802.1ah Provider Backbone Bridges
IEEE 802.1AX-2008 Link Aggregation
IEEE 802.1D MAC Bridges
IEEE 802.1p Priority
IEEE 802.1Q (GVRP)
IEEE 802.1Q VLANs
IEEE 802.1s (MSTP)
IEEE 802.1s Multiple Spanning Trees
IEEE 802.1v VLAN classification by Protocol and Port
IEEE 802.1w Rapid Reconfiguration of Spanning Tree
IEEE 802.1X PAE
IEEE 802.3 Type 10BASE-T
IEEE 802.3ab 1000BASE-T
IEEE 802.3ac (VLAN Tagging Extension)
IEEE 802.3ad Link Aggregation (LAG)
IEEE 802.3ad Link Aggregation Control Protocol (LACP)
IEEE 802.3ae 10-Gigabit Ethernet
IEEE 802.3ag Ethernet OAM
IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber - EFMF
IEEE 802.3i 10BASE-T
IEEE 802.3u 100BASE-X
IEEE 802.3x Flow Control
IEEE 802.3z 1000BASE-X
RFC 768 UDP
RFC 783 TFTP Protocol (revision 2)
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 TELNET
RFC 855 Telnet Option Specification
RFC 856 TELNET
RFC 857 Telnet Echo Option
RFC 858 Telnet Suppress Go Ahead Option
RFC 894 IP over Ethernet
RFC 896 Congestion Control in IP/TCP Internetworks
RFC 906 TFTP Bootstrap
RFC 925 Multi-LAN Address Resolution
RFC 950 Internet Standard Subnetting Procedure
RFC 951 BOOTP
RFC 959 File Transfer Protocol (FTP)
RFC 1006 ISO transport services on top of the TCP: Version 3
RFC 1027 Proxy ARP
RFC 1034 Domain Concepts and Facilities
RFC 1035 Domain Implementation and Specification
RFC 1042 IP Datagrams
RFC 1058 RIPv1
RFC 1071 Computing the Internet Checksum
RFC 1091 Telnet Terminal-Type Option
RFC 1093 NSFNET routing architecture
RFC 1122 Host Requirements
RFC 1141 Incremental updating of the Internet checksum
RFC 1142 OSI IS-IS Intra-domain Routing Protocol
RFC 1144 Compressing TCP/IP headers for low-speed serial links
RFC 1171 Point-to-Point Protocol for the transmission of multi-protocol datagrams over Point-to-Point links
RFC 1195 OSI ISIS for IP and Dual Environments
RFC 1213 Management Information Base for Network Management of TCP/IP-based internets
RFC 1253 (OSPF v2)
RFC 1256 ICMP Router Discovery Protocol (IRDP)
RFC 1293 Inverse Address Resolution Protocol
RFC 1305 NTPv3
RFC 1315 Management Information Base for Frame Relay DTEs
RFC 1321 The MD5 Message-Digest Algorithm
RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
RFC 1333 PPP Link Quality Monitoring
RFC 1334 PPP Authentication Protocols (PAP)
RFC 1334 PPP Authentication Protocols (PAP)
RFC 1349 Type of Service
RFC 1350 TFTP Protocol (revision 2)
RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)
RFC 1381 SNMP MIB Extension for X.25 LAPB
RFC 1389 RIPv2 MIB Extension
RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC 1472 The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol
RFC 1490 Multiprotocol Interconnect over Frame Relay
RFC 1519 CIDR
RFC 1531 Dynamic Host Configuration Protocol
RFC 1533 DHCP Options and BOOTP Vendor Extensions
RFC 1534 DHCP/BOOTP Interoperation
RFC 1541 DHCP
RFC 1542 BOOTP Extensions
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1552 The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
RFC 1577 Classical IP and ARP over ATM
RFC 1631 NAT
RFC 1638 PPP Bridging Control Protocol (BCP)
RFC 1661 The Point-to-Point Protocol (PPP)
RFC 1662 PPP in HDLC-like Framing
RFC 1695 Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2
RFC 1700 Assigned Numbers
RFC 1701 Generic Routing Encapsulation
RFC 1702 Generic Routing Encapsulation over IPv4 networks
RFC 1721 RIP-2 Analysis
RFC 1722 RIP-2 Applicability
RFC 1723 RIP v2
RFC 1812 IPv4 Routing
RFC 1829 The ESP DES-CBC Transform
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1944 Benchmarking Methodology for Network Interconnect Devices
RFC 1945 Hypertext Transfer Protocol - HTTP/1.0
RFC 1973 PPP in Frame Relay
RFC 1974 PPP Stac LZS Compression Protocol
RFC 1981 Path MTU Discovery for IP version 6
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2082 RIP-2 MD5 Authentication
RFC 2091 Trigger RIP
RFC 2104 HMAC: Keyed-Hashing for Message Authentication
RFC 2131 DHCP
RFC 2132 DHCP Options and BOOTP Vendor Extensions
RFC 2138 Remote Authentication Dial In User Service (RADIUS)
RFC 2205 Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification
RFC 2209 Resource ReSerVation Protocol (RSVP) - Version 1 Message Processing Rules
RFC 2236 IGMP Snooping
RFC 2246 The TLS Protocol Version 1.0
RFC 2251 Lightweight Directory Access Protocol (v3)
RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2280 Routing Policy Specification Language (RPSL)
RFC 2283 MBGP
RFC 2284 EAP over LAN
RFC 2338 VRRP
RFC 2338 VRRP (Premium Edge License)
RFC 2364 PPP Over AAL5
RFC 2374 An Aggregatable Global Unicast Address Format
RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2453 RIPv2
RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2511 Internet X.509 Certificate Request Message Format
RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2616 HTTP Compatibility v1.1
RFC 2622 Routing Policy Specification Language (RPSL)

Specifications (continued)

Standards and protocols
(applies to all products in series)

HP 6602 Router Chassis (JC176A)

RFC 2663 NAT Terminology and Considerations
RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2694 DNS extensions to Network Address Translators (DNS_ALG)
RFC 2702 Requirements for Traffic Engineering Over MPLS
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2747 RSVP Cryptographic Authentication
RFC 2763 Dynamic Name-to-System ID mapping support
RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT)
RFC 2766 Network Address Translation - Protocol Translation (NAT-PT)
RFC 2767 Dual Stacks IPv4 & IPv6
RFC 2784 Generic Routing Encapsulation (GRE)
RFC 2787 Definitions of Managed Objects for VRRP
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2866 RADIUS Accounting
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 2993 Architectural Implications of NAT
RFC 3022 Traditional IP Network Address Translator (Traditional NAT)
RFC 3027 Protocol Complications with the IP Network Address Translator
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3036 LDP Specification
RFC 3046 DHCP Relay Agent Information Option
RFC 3063 MPLS Loop Prevention Mechanism
RFC 3065 Support AS confederation
RFC 3137 OSPF Stub Router Advertisement
RFC 3209 RSVP-TE Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP-Tunnels
RFC 3212 Constraint-Based LSP setup using LDP (CR-LDP)
RFC 3214 LSP Modification Using CR-LDP
RFC 3215 LDP State Machine
RFC 3246 Expedited Forwarding PHB
RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3277 IS-IS Transient Blackhole Avoidance
RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3392 Support BGP capabilities advertisement
RFC 3410 Applicability Statements for SNMP
RFC 3416 Protocol Operations for SNMP
RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP)
RFC 3487 Graceful Restart Mechanism for LDP
RFC 3509 OSPF ABR Behavior
RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

HP 6604 Router Chassis (JC178B)

RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC 3619 Ethernet Automatic Protection Switching (EAPS)
RFC 3623 Graceful OSPF Restart
RFC 3704 Unicast Reverse Path Forwarding (URPF)
RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3768 VRRP
RFC 3768 VRRP
RFC 3768 VRRP (Premium Edge License)
RFC 3784 ISIS TE support
RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management
RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
RFC 3847 Restart signaling for IS-IS
RFC 4213 Basic IPv6 Transition Mechanisms
IP Ping

IP multicast
RFC 1112 IGMP
RFC 2236 IGMPv2
RFC 2283 Multiprotocol Extensions for BGP-4
RFC 2362 PIM Sparse Mode
RFC 2362 PIM Sparse Mode (Premium Edge License)
RFC 2362 PIM Sparse Mode
RFC 2934 Protocol Independent Multicast MIB for IPv4
RFC 3376 IGMPv3
RFC 3376 IGMPv3 (host joins only)
RFC 3569 An Overview of Source-Specific Multicast (SSM)
RFC 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3973 Draft 2 PIM Dense Mode
RFC 3973 Draft 2 PIM Dense Mode
RFC 3973 PIM Dense Mode
RFC 3973 PIM Dense Mode (Premium Edge License)
RFC 3973 PIM Dense Mode
RFC 4601 Draft 10 PIM Sparse Mode
RFC 4601 Draft 10 PIM Sparse Mode
RFC 4605 IGMP/MLD Proxying

IPv6
RFC 1350 TFTP
RFC 1881 IPv6 Address Allocation Management
RFC 1886 DNS Extension for IPv6
RFC 1887 IPv6 Unicast Address Allocation Architecture
RFC 1981 IPv6 Path MTU Discovery
RFC 2080 RIPng for IPv6
RFC 2292 Advanced Sockets API for IPv6
RFC 2373 IPv6 Addressing Architecture
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 IPv6 Specification
RFC 2461 IPv6 Neighbor Discovery
RFC 2462 IPv6 Stateless Address Auto-configuration
RFC 2463 ICMPv6
RFC 2464 Transmission of IPv6 over Ethernet Networks
RFC 2472 IP Version 6 over PPP
RFC 2473 Generic Packet Tunneling in IPv6
RFC 2475 IPv6 DiffServ Architecture
RFC 2529 Transmission of IPv6 Packets over IPv4
RFC 2545 Use of MP-BGP-4 for IPv6
RFC 2553 Basic Socket Interface Extensions for IPv6
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2711 IPv6 Router Alert Option
RFC 2740 OSPFv3 for IPv6
RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 2925 Remote Operations MIB (Ping only)
RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
RFC 3162 RADIUS and IPv6
RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
RFC 3307 IPv6 Multicast Address Allocation
RFC 3315 DHCPv6 (client and relay)
RFC 3315 DHCPv6 (client only)
RFC 3363 DNS support
RFC 3484 Default Address Selection for IPv6
RFC 3493 Basic Socket Interface Extensions for IPv6
RFC 3513 IPv6 Addressing Architecture
RFC 3542 Advanced Sockets API for IPv6
RFC 3587 IPv6 Global Unicast Address Format
RFC 3596 DNS Extension for IPv6
RFC 3810 MLDv2 (host joins only)
RFC 3810 MLDv2 for IPv6
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4022 MIB for TCP
RFC 4113 MIB for UDP
RFC 4251 SSHv6 Architecture
RFC 4252 SSHv6 Authentication
RFC 4252 SSHv6 Transport Layer
RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4291 IP Version 6 Addressing Architecture
RFC 4293 MIB for IP
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
RFC 5340 OSPF for IPv6
RFC 5340 OSPFv3 for IPv6
RFC 5722 Handling of Overlapping IPv6 Fragments

MIBs
IEEE 8021-PAE-MIB
IEEE 8023-LAG-MIB
RFC 1156 (TCP/IP MIB)
RFC 1212 Concise MIB Definitions
RFC 1213 MIB II
RFC 1229 Interface MIB Extensions
RFC 1286 Bridge MIB
RFC 1493 Bridge MIB
RFC 1573 SNMP MIB II
RFC 1643 Ethernet MIB
RFC 1650 Ethernet-Like MIB
RFC 1657 BGP-4 MIB
RFC 1724 RIPv2 MIB
RFC 1757 Remote Network Monitoring MIB
RFC 1850 OSPFv2 MIB
RFC 1907 SNMPv2 MIB
RFC 2011 SNMPv2 MIB for IP
RFC 2012 SNMPv2 MIB for TCP
RFC 2013 SNMPv2 MIB for UDP
RFC 2021 RMONv2 MIB
RFC 2096 IP Forwarding Table MIB
RFC 2233 Interface MIB
RFC 2233 Interfaces MIB
RFC 2273 SNMP-NOTIFICATION-MIB
RFC 2452 IPV6-TCP-MIB
RFC 2454 IPV6-UDP-MIB
RFC 2465 IPv6 MIB
RFC 2466 ICMPv6 MIB
RFC 2571 SNMP Framework MIB
RFC 2572 SNMP-MPD MIB

Specifications (continued)

	HP 6602 Router Chassis (JC176A)	HP 6604 Router Chassis (JC178B)

Standards and protocols
(applies to all products in series)

RFC 2574 SNMP USM MIB
RFC 2618 RADIUS Client MIB
RFC 2620 RADIUS Accounting MIB
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
RFC 2674 802.1p and IEEE 802.1Q Bridge MIB
RFC 2688 MAU-MIB
RFC 2737 Entity MIB (Version 2)
RFC 2787 VRRP MIB
RFC 2819 RMON MIB
RFC 2863 The Interfaces Group MIB
RFC 2925 Ping MIB
RFC 2932IP (Multicast Routing MIB)
RFC 2933 IGMP MIB
RFC 3273 HC-RMON MIB
RFC 3414 SNMP-User based-SM MIB
RFC 3415 SNMP-View based-ACM MIB
RFC 3418 MIB for SNMPv3
RFC 3621 Power Ethernet MIB
RFC 3813 MPLS LSR MIB
RFC 3814 MPLS FTN MIB
RFC 3815 MPLS LDP MIB
RFC 3826 AES for SNMP's USM MIB
RFC 4113 UDP MIB
RFC 4133 Entity MIB (Version 3)
RFC 4221 MPLS FTN MIB
LLDP-EXT-DOT1-MIB
LLDP-EXT-DOT3-MIB
LLDP-MIB

Network management
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
IEEE 802.1D (STP)
RFC 1098 A Simple Network Management Protocol (SNMP)
RFC 1155 Structure of Management Information
RFC 1157 SNMPv1
RFC 1215 SNMP Generic traps
RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
RFC 1901 SNMPv2 Introduction
RFC 1902 SNMPv2 Structure
RFC 1903 SNMPv2 Textual Conventions
RFC 1904 SNMPv2 Conformance
RFC 1905 SNMPv2 Protocol Operations
RFC 1906 SNMPv2 Transport Mappings
RFC 1918 Private Internet Address Allocation
RFC 2272 SNMPv3 Management Protocol
RFC 2273 SNMPv3 Applications
RFC 2274 USM for SNMPv3
RFC 2275 VACM for SNMPv3
RFC 2570 SNMPv3 Overview
RFC 2571 SNMP Management Frameworks
RFC 2572 SNMPv3 Message Processing
RFC 2573 SNMPv3 Applications
RFC 2574 SNMPv3 User-based Security Model (USM)
RFC 2575 SNMPv3 View-based Access Control Model (VACM)
RFC 2575 VACM for SNMP
RFC 2576 Coexistence between SNMP versions
RFC 2578 SMIv2
RFC 2581 TCP6
RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events)
RFC 3164 BSD syslog Protocol
RFC 3176 sFlow
RFC 3411 SNMP Management Frameworks
RFC 3412 SNMPv3 Message Processing
RFC 3414 SNMPv3 User-based Security Model (USM)
RFC 3415 SNMPv3 View-based Access Control Model VACM)
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2
SNMPv1/v2c
SNMPv1/v2c (read only)
SNMPv1/v2c/v3

OSPF
RFC 1245 OSPF protocol analysis
RFC 1246 Experience with OSPF
RFC 1253 OSPFv2 MIB
RFC 1583 OSPFv2
RFC 1587 OSPF NSSA
RFC 1745 OSPF Interactions
RFC 1765 OSPF Database Overflow
RFC 1850 OSPFv2 Management Information Base (MIB), traps
RFC 2178 OSPFv2
RFC 2328 OSPFv2
RFC 2328 OSPFv2
RFC 2328 OSPFv2 (Premium Edge License)
RFC 2370 OSPF Opaque LSA Option
RFC 3101 OSPF NSSA
RFC 3623 Graceful OSPF Restart
RFC 5340 OSPF for IPv6
RFC 5340 OSPFv3 for IPv6

QoS/CoS
IEEE 802.1P (CoS)
RFC 2474 DiffServ Precedence, including 8 queues/port
RFC 2474 DiffServ precedence, with 4 queues per port
RFC 2474 DS Field in the IPv4 and IPv6 Headers
RFC 2474 DSCP DiffServ
RFC 2474, with 4 queues per port
RFC 2475 DiffServ Architecture
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2597 DiffServ Assured Forwarding (AF)- partial support
RFC 2598 DiffServ Expedited Forwarding (EF)
Ingress Rate Limiting

Security
IEEE 802.1X Port Based Network Access Control
RFC 1321 The MD5 Message-Digest Algorithm
RFC 1492 TACACS+
RFC 2082 RIP-2 MD5 Authentication
RFC 2104 Keyed-Hashing for Message Authentication
RFC 2138 RADIUS Authentication
RFC 2139 RADIUS Accounting
RFC 2209 RSVP-Message Processing
RFC 2246 Transport Layer Security (TLS)
RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2548 Microsoft Vendor-specific RADIUS Attributes
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2818 HTTP Over TLS
RFC 2865 RADIUS (client only)
RFC 2865 RADIUS Authentication
RFC 2866 RADIUS Accounting
RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 3567 Intermediate System (IS) to IS Cryptographic Authentication
RFC 3576 Dynamic Authorization Extensions to RADIUS
RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1X RADIUS
Access Control Lists (ACLs)
Guest VLAN for 802.1x
MAC Authentication
Port Security
Secure Sockets Layer (SSL)
SSHv1 Secure Shell
SSHv1.5 Secure Shell
SSHv1/SSHv2 Secure Shell
SSHv2 Secure Shell

VPN
RFC 2403 - HMAC-MD5-96
RFC 2404 - HMAC-SHA1-96
RFC 2405 - DES-CBC Cipher algorithm
RFC 2407 - Domain of interpretation
RFC 2547 BGP/MPLS VPNs
RFC 2764 A Framework for IP Based Virtual Private Networks
RFC 2796 BGP Route Reflection - An Alternative to Full Mesh IBGP
RFC 2842 Capabilities Advertisement with BGP-4
RFC 2858 Multiprotocol Extensions for BGP-4
RFC 2917 A Core MPLS IP VPN Architecture
RFC 2918 Route Refresh Capability for BGP-4
RFC 3107 Carrying Label Information in BGP-4
RFC 4301 - Security Architecture for the Internet Protocol
RFC 4302 - IP Authentication Header (AH)
RFC 4303 - IP Encapsulating Security Payload (ESP)
RFC 4305 - Cryptographic Algorithm Implementation Requirements for ESP and AH

IPsec
RFC 1828 IP Authentication using Keyed MD5
RFC 2401 IP Security Architecture
RFC 2402 IP Authentication Header
RFC 2406 IP Encapsulating Security Payload
RFC 2407 - Domain of interpretation
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange
RFC 2410 - The NULL Encryption Algorithm and its use with IPsec
RFC 2411 IP Security Document Roadmap
RFC 2412 – OAKLEY
RFC 2865 - Remote Authentication Dial In User Service (RADIUS)

IKEv1
RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
RFC 3748 - Extensible Authentication Protocol (EAP)

Specifications (continued)

	 HP 6616 Router Chassis (JC496A)	 HP 6608 Router Chassis (JC177B)
Ports	16 HIM slots 2 MPU (for management modules) slots	8 HIM slots 2 MPU (for management modules) slots
Physical characteristics		
Dimensions	18.74(d) x 17.17(w) x 34.88(h) in. (47.6 x 43.61 x 88.6 cm) (20U height)	18.74(d) x 17.17(w) x 12.13(h) in. (47.6 x 43.61 x 30.81 cm) (7U height)
Full configuration weight	220.46 lb. (100 kg)	110.23 lb. (50 kg)
Mounting	EIA standard 19 in. rack	EIA standard 19 in. rack
Performance		
Throughput	up to 252 million pps	up to 108 million pps
Routing table size	2000000 entries	2000000 entries
Environment		
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 95%, noncondensing	10% to 95%, noncondensing
Electrical characteristics		
Maximum heat dissipation	6650 BTU/hr (7015.75 kJ/hr)	2217 BTU/hr (2338.94 kJ/hr)
Voltage	100-120/200-240 VAC	100-120/200-240 VAC
Maximum power rating	1950 W	650 W
Frequency	50/60 Hz	50/60 Hz
Notes	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.
Safety	CSA 22.2 No. 60950; cUL (CSA 22.2 No. 60950); CSA 22.2 No. 60950 3rd edition; CSA 22.2 No. 950; CSA 950; cUL (CSA 950); EN 60950/IEC 60950; UL 1950 3rd edition; UL 1950; UL 60950; UL 60950-1; CAN/CSA 22.2 No. 60950; CAN/CSA 22.2 No. 60950-1; EN 60825; AS/NZS 60950; KN 60950; GOST R MEK60950; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; EN 609500 Safety Information Technology Equipment; UL 60950; CSA 22.2 No. 60950/cUL; IEC 60950; IEC 60950-1; EN 60950; EN 60950-1; IEC 60825; CSA 22.2 No. 950-95; IEC 60950-1:2001 (with CB Report); CAN/CSA-C22.2 No. 60950-1-03; CAN/CSA-C22.2 No. 60950-1; CSA 60950-1; CSA C22.2 60950-1; EU RoHS Compliant; EN 60950-1/A11; CSA 22.2 60950-1; EN 60950: 2000, ZB and ZC Deviations; IEC 60950: 1999, Corr Feb 2000, all national deviations; As/NZS 60950:2000, Australia; UL 60950-1:2003; UL 60950-1:2001; CSA 22.2 60950-1:2003; IEC 60950-1:2001; EN 60950-1:2001; CSA 22.2-60950; AS/NZS 60950: 2000 Australia, Russian GOST Safety Approval; CSA 22.2 No. 950 3rd Edition 1995; UL 60950 3rd Edition; CAN/CSA 22.2 No. 60950-00/UL 60950 3rd Edition, Safety Information for Technology Equipment; EN 60950/IEC 60950 3rd Edition; UL 60950 Standard for the Safety of Information Technology Equipment; EN 60825: Safety of Laser Products	CSA 22.2 No. 60950; cUL (CSA 22.2 No. 60950); CSA 22.2 No. 60950 3rd edition; CSA 22.2 No. 950; CSA 950; cUL (CSA 950); EN 60950/IEC 60950; UL 1950 3rd edition; UL 1950; UL 60950; UL 60950-1; CAN/CSA 22.2 No. 60950; CAN/CSA 22.2 No. 60950-1; EN 60825; AS/NZS 60950; KN 60950; GOST R MEK60950; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; EN 609500 Safety Information Technology Equipment; UL 60950; CSA 22.2 No. 60950/cUL; IEC 60950; IEC 60950-1; EN 60950; EN 60950-1; IEC 60825; CSA 22.2 No. 950-95; IEC 60950-1:2001 (with CB Report); CAN/CSA-C22.2 No. 60950-1-03; CAN/CSA-C22.2 No. 60950-1; CSA 60950-1; CSA C22.2 60950-1; EU RoHS Compliant; EN 60950-1/A11; CSA 22.2 60950-1; EN 60950: 2000, ZB and ZC Deviations; IEC 60950: 1999, Corr Feb 2000, all national deviations; As/NZS 60950:2000, Australia; UL 60950-1:2003; UL 60950-1:2001; CSA 22.2 60950-1:2003; IEC 60950-1:2001; EN 60950-1:2001; CSA 22.2-60950; AS/NZS 60950: 2000 Australia, Russian GOST Safety Approval; CSA 22.2 No. 950 3rd Edition 1995; UL 60950 3rd Edition; CAN/CSA 22.2 No. 60950-00/UL 60950 3rd Edition, Safety Information for Technology Equipment; EN 60950/IEC 60950 3rd Edition; UL 60950 Standard for the Safety of Information Technology Equipment; EN 60825: Safety of Laser Products
Emissions	FCC part 15 Class A; FCC Rules Part 15, Subpart B Class A; EN 55022/CISPR-22 Class A; VCCI Class A; EN 55022/CISPR 22 Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; CISPR 22/A2; IEC/EN 61000-3-2; IEC/EN 61000-3-3; EN 55024/A1; IEC 61000:4-2, 4-3, 4-4, 4-5, 4-6, 4-8, 4-11; BSMI CNS 13438; EMC Directive 89/336/EEC; ICES-003 Class A; ANSI C63.4 2003; CISPR 24; ETSI EN 300 386 V1.3.3; AS/NZS CISPR22 Class A; EN 61000-3-2; EN 61000-3-3; Korean EMI Class A; CNS 13438 Class A; EN 55024:1998; EN 61000-4-2; EN 61000-4-3; EN 61000-4-4; EN 61000-4-5; EN 61000-4-6; EN 61000-4-11	FCC part 15 Class A; FCC Rules Part 15, Subpart B Class A; EN 55022/CISPR-22 Class A; VCCI Class A; EN 55022/CISPR 22 Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; CISPR 22/A2; IEC/EN 61000-3-2; IEC/EN 61000-3-3; EN 55024/A1; IEC 61000:4-2, 4-3, 4-4, 4-5, 4-6, 4-8, 4-11; BSMI CNS 13438; EMC Directive 89/336/EEC; ICES-003 Class A; ANSI C63.4 2003; CISPR 24; ETSI EN 300 386 V1.3.3; AS/NZS CISPR22 Class A; EN 61000-3-2; EN 61000-3-3; Korean EMI Class A; CNS 13438 Class A; EN 55024:1998; EN 61000-4-2; EN 61000-4-3; EN 61000-4-4; EN 61000-4-5; EN 61000-4-6; EN 61000-4-11
Management	IMC - Intelligent Management Center; command-line interface; limited command-line interface; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); out-of-band management; SNMP Manager; Telnet; RMON1; FTP; in-line and out-of-band; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB	IMC - Intelligent Management Center; command-line interface; limited command-line interface; out-of-band management (serial RS-232C); out-of-band management (DB-9 serial port console); out-of-band management; SNMP Manager; Telnet; RMON1; FTP; in-line and out-of-band; terminal interface (serial RS-232C); modem interface; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB
Services	3-year, parts only, global next-day advance exchange (UW054E) 3-year, 4-hour onsite, 13x5 coverage for hardware (UW062E) 3-year, 4-hour onsite, 24x7 coverage for hardware (UV930E) 3-year, 4-hour onsite, 24x7 coverage for hardware (HR530E) 3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (UV943E) 3-year, 24x7 SW phone support, software updates (UV955E) 1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (HR529E) 1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (HR531E)	3-year, parts only, global next-day advance exchange (UW054E) 3-year, 4-hour onsite, 13x5 coverage for hardware (UW062E) 3-year, 4-hour onsite, 24x7 coverage for hardware (UV930E) 3-year, 4-hour onsite, 24x7 coverage for hardware (HR530E) 3-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 SW phone support and SW updates (UV943E) 3-year, 24x7 SW phone support, software updates (UV955E) 1-year, post-warranty, 4-hour onsite, 13x5 coverage for hardware (HR529E) 1-year, post-warranty, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone support (HR531E)

Specifications (continued)

	HP 6616 Router Chassis (JC496A)	HP 6608 Router Chassis (JC177B)
	4-year, 4-hour onsite, 13x5 coverage for hardware (UW063E)	4-year, 4-hour onsite, 13x5 coverage for hardware (UW063E)
	4-year, 4-hour onsite, 24x7 coverage for hardware (UV931E)	4-year, 4-hour onsite, 24x7 coverage for hardware (UV931E)
	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UV944E)	4-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UV944E)
	4-year, 24x7 SW phone support, software updates (UV956E)	4-year, 24x7 SW phone support, software updates (UV956E)
	5-year, 4-hour onsite, 13x5 coverage for hardware (UW064E)	5-year, 4-hour onsite, 13x5 coverage for hardware (UW064E)
	5-year, 4-hour onsite, 24x7 coverage for hardware (UV932E)	5-year, 4-hour onsite, 24x7 coverage for hardware (UV932E)
	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UV945E)	5-year, 4-hour onsite, 24x7 coverage for hardware, 24x7 software phone (UV945E)
	5-year, 24x7 SW phone support, software updates (UV957E)	5-year, 24x7 SW phone support, software updates (UV957E)
	3 Yr 6 hr Call-to-Repair Onsite (UW055E)	3 Yr 6 hr Call-to-Repair Onsite (UW055E)
	4 Yr 6 hr Call-to-Repair Onsite (UW056E)	4 Yr 6 hr Call-to-Repair Onsite (UW056E)
	5 Yr 6 hr Call-to-Repair Onsite (UW057E)	5 Yr 6 hr Call-to-Repair Onsite (UW057E)
	1-year, 6 hour Call-To-Repair Onsite for hardware (HR533E)	1-year, 6 hour Call-To-Repair Onsite for hardware (HR533E)
	1-year, 24x7 software phone support, software updates (HR532E)	1-year, 24x7 software phone support, software updates (HR532E)
	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.	Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Specifications (continued)

	HP 6616 Router Chassis (JC496A)	HP 6608 Router Chassis (JC177B)

Standards and protocols
(applies to all products in series)

BGP
RFC 1267 Border Gateway Protocol 3 (BGP-3)
RFC 1657 Definitions of Managed Objects for BGPv4
RFC 1771 BGPv4
RFC 1772 Application of the BGP
RFC 1773 Experience with the BGP-4 Protocol
RFC 1774 BGP-4 Protocol Analysis
RFC 1965 BGP4 confederations
RFC 1997 BGP Communities Attribute
RFC 1998 PPP Gandalf FZA Compression Protocol
RFC 2385 BGP Session Protection via TCP MD5
RFC 2439 BGP Route Flap Damping
RFC 2796 BGP Route Reflection
RFC 2842 Capability Advertisement with BGP-4
RFC 2858 BGP-4 Multi-Protocol Extensions
RFC 2918 Route Refresh Capability

Denial of service protection
CPU DoS Protection
Rate Limiting by ACLs

Device management
RFC 1155 Structure and Mgmt Information (SMIv1)
RFC 1157 SNMPv1/v2c
RFC 1305 NTPv3
RFC 1901 (Community based SNMPv2)
RFC 1901-1907 SNMPv2c, SMIv2 and Revised MIB-II
RFC 1902 (SNMPv2)
RFC 1908 (SNMP v1/2 Coexistence)
RFC 1945 Hypertext Transfer Protocol - HTTP/1.0
RFC 2068 Hypertext Transfer Protocol - HTTP/1.1
RFC 2271 FrameWork
RFC 2452 MIB for TCP6
RFC 2454 MIB for UDP6
RFC 2573 (SNMPv3 Applications)
RFC 2576 (Coexistence between SNMP V1, V2, V3)
RFC 2578-2580 SMIv2
RFC 2579 (SMIv2 Text Conventions)
RFC 2580 (SMIv2 Conformance)
RFC 2819 (RMON groups Alarm, Event, History and Statistics only)
RFC 2819 RMON
RFC 3410 (Management Framework)
RFC 3416 (SNMP Protocol Operations v2)
RFC 3417 (SNMP Transport Mappings)
Multiple Configuration Files
Multiple Software Images
SNMP v3 and RMON RFC support
SSHv1/SSHv2 Secure Shell
TACACS/TACACS+

General protocols
IEEE 802.1ad Q-in-Q
IEEE 802.1ad Q-in-Q
IEEE 802.1ag Service Layer OAM
IEEE 802.1ah Provider Backbone Bridges
IEEE 802.1AX-2008 Link Aggregation
IEEE 802.1D MAC Bridges
IEEE 802.1p Priority
IEEE 802.1Q (GVRP)
IEEE 802.1Q VLANs
IEEE 802.1s (MSTP)
IEEE 802.1s Multiple Spanning Trees
IEEE 802.1v VLAN classification by Protocol and Port
IEEE 802.1w Rapid Reconfiguration of Spanning Tree
IEEE 802.1X PAE
IEEE 802.3 Type 10BASE-T
IEEE 802.3ab 1000BASE-T
IEEE 802.3ac (VLAN Tagging Extension)
IEEE 802.3ad Link Aggregation (LAG)
IEEE 802.3ad Link Aggregation Control Protocol (LACP)
IEEE 802.3ae 10-Gigabit Ethernet
IEEE 802.3ag Ethernet OAM
IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber - EFMF
IEEE 802.3i 10BASE-T
IEEE 802.3u 100BASE-X
IEEE 802.3x Flow Control
IEEE 802.3z 1000BASE-X
RFC 768 UDP
RFC 783 TFTP Protocol (revision 2)
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 TELNET
RFC 855 Telnet Option Specification
RFC 856 TELNET
RFC 857 Telnet Echo Option
RFC 858 Telnet Suppress Go Ahead Option
RFC 894 IP over Ethernet
RFC 896 Congestion Control in IP/TCP Internetworks
RFC 906 TFTP Bootstrap
RFC 925 Multi-LAN Address Resolution
RFC 950 Internet Standard Subnetting Procedure
RFC 951 BOOTP
RFC 959 File Transfer Protocol (FTP)
RFC 1006 ISO transport services on top of the TCP: Version 3
RFC 1027 Proxy ARP
RFC 1034 Domain Concepts and Facilities
RFC 1035 Domain Implementation and Specification
RFC 1042 IP Datagrams
RFC 1058 RIPv1
RFC 1071 Computing the Internet Checksum
RFC 1091 Telnet Terminal-Type Option
RFC 1093 NSFNET routing architecture
RFC 1122 Host Requirements
RFC 1141 Incremental updating of the Internet checksum
RFC 1142 OSI IS-IS Intra-domain Routing Protocol
RFC 1144 Compressing TCP/IP headers for low-speed serial links
RFC 1171 Point-to-Point Protocol for the transmission of multi-protocol datagrams over Point-to-Point links
RFC 1195 OSI ISIS for IP and Dual Environments
RFC 1213 Management Information Base for Network Management of TCP/IP-based internets
RFC 1253 (OSPF v2)
RFC 1256 ICMP Router Discovery Protocol (IRDP)
RFC 1293 Inverse Address Resolution Protocol
RFC 1305 NTPv3
RFC 1315 Management Information Base for Frame Relay DTEs
RFC 1321 The MD5 Message-Digest Algorithm
RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
RFC 1333 PPP Link Quality Monitoring
RFC 1334 PPP Authentication Protocols (PAP)
RFC 1334 PPP Authentication Protocols (PAP)
RFC 1349 Type of Service
RFC 1350 TFTP Protocol (revision 2)
RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)
RFC 1381 SNMP MIB Extension for X.25 LAPB
RFC 1389 RIPv2 MIB Extension
RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC 1472 The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol
RFC 1490 Multiprotocol Interconnect over Frame Relay
RFC 1519 CIDR
RFC 1531 Dynamic Host Configuration Protocol
RFC 1533 DHCP Options and BOOTP Vendor Extensions
RFC 1534 DHCP/BOOTP Interoperation
RFC 1541 DHCP
RFC 1542 BOOTP Extensions
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1552 The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
RFC 1577 Classical IP and ARP over ATM
RFC 1631 NAT
RFC 1638 PPP Bridging Control Protocol (BCP)
RFC 1661 The Point-to-Point Protocol (PPP)
RFC 1662 PPP in HDLC-like Framing
RFC 1695 Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2
RFC 1700 Assigned Numbers
RFC 1701 Generic Routing Encapsulation
RFC 1702 Generic Routing Encapsulation over IPv4 networks
RFC 1721 RIP-2 Analysis
RFC 1722 RIP-2 Applicability
RFC 1723 RIP v2
RFC 1812 IPv4 Routing
RFC 1829 The ESP DES-CBC Transform
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1944 Benchmarking Methodology for Network Interconnect Devices
RFC 1945 Hypertext Transfer Protocol - HTTP/1.0
RFC 1973 PPP in Frame Relay
RFC 1974 PPP Stac LZS Compression Protocol
RFC 1981 Path MTU Discovery for IP version 6
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2082 RIP-2 MD5 Authentication
RFC 2091 Trigger RIP
RFC 2104 HMAC: Keyed-Hashing for Message Authentication
RFC 2131 DHCP
RFC 2132 DHCP Options and BOOTP Vendor Extensions
RFC 2138 Remote Authentication Dial In User Service (RADIUS)
RFC 2205 Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification
RFC 2209 Resource ReSerVation Protocol (RSVP) - Version 1 Message Processing Rules
RFC 2236 IGMP Snooping
RFC 2246 The TLS Protocol Version 1.0
RFC 2251 Lightweight Directory Access Protocol (v3)
RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2280 Routing Policy Specification Language (RPSL)
RFC 2283 MBGP
RFC 2284 EAP over LAN
RFC 2338 VRRP
RFC 2338 VRRP (Premium Edge License)
RFC 2364 PPP Over AAL5
RFC 2374 An Aggregatable Global Unicast Address Format
RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2453 RIPv2
RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2511 Internet X.509 Certificate Request Message Format
RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2616 HTTP Compatibility v1.1
RFC 2622 Routing Policy Specification Language (RPSL)

Specifications (continued)

	HP 6616 Router Chassis (JC496A)	HP 6608 Router Chassis (JC177B)

Standards and protocols
(applies to all products in series)

RFC 2663 NAT Terminology and Considerations
RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2694 DNS extensions to Network Address Translators (DNS_ALG)
RFC 2702 Requirements for Traffic Engineering Over MPLS
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2747 RSVP Cryptographic Authentication
RFC 2763 Dynamic Name-to-System ID mapping support
RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT)
RFC 2766 Network Address Translation - Protocol Translation (NAT-PT)
RFC 2767 Dual Stacks IPv4 & IPv6
RFC 2784 Generic Routing Encapsulation (GRE)
RFC 2787 Definitions of Managed Objects for VRRP
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2866 RADIUS Accounting
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 2993 Architectural Implications of NAT
RFC 3022 Traditional IP Network Address Translator (Traditional NAT)
RFC 3027 Protocol Complications with the IP Network Address Translator
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3036 LDP Specification
RFC 3046 DHCP Relay Agent Information Option
RFC 3063 MPLS Loop Prevention Mechanism
RFC 3065 Support AS confederation
RFC 3137 OSPF Stub Router Advertisement
RFC 3209 RSVP-TE Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP-Tunnels
RFC 3212 Constraint-Based LSP setup using LDP (CR-LDP)
RFC 3214 LSP Modification Using CR-LDP
RFC 3215 LDP State Machine
RFC 3246 Expedited Forwarding PHB
RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3277 IS-IS Transient Blackhole Avoidance
RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3392 Support BGP capabilities advertisement
RFC 3410 Applicability Statements for SNMP
RFC 3416 Protocol Operations for SNMP
RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP)
RFC 3487 Graceful Restart Mechanism for LDP
RFC 3509 OSPF ABR Behavior
RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC 3619 Ethernet Automatic Protection Switching (EAPS)
RFC 3623 Graceful OSPF Restart
RFC 3704 Unicast Reverse Path Forwarding (URPF)
RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3768 VRRP
RFC 3768 VRRP
RFC 3768 VRRP (Premium Edge License)
RFC 3784 ISIS TE support
RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management
RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
RFC 3847 Restart signaling for IS-IS
RFC 4213 Basic IPv6 Transition Mechanisms
IP Ping

IP multicast
RFC 1112 IGMP
RFC 2236 IGMPv2
RFC 2283 Multiprotocol Extensions for BGP-4
RFC 2362 PIM Sparse Mode
RFC 2362 PIM Sparse Mode (Premium Edge License)
RFC 2362 PIM Sparse Mode
RFC 2934 Protocol Independent Multicast MIB for IPv4
RFC 3376 IGMPv3
RFC 3376 IGMPv3 (host joins only)
RFC 3569 An Overview of Source-Specific Multicast (SSM)
RFC 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3973 Draft 2 PIM Dense Mode
RFC 3973 Draft 2 PIM Dense Mode
RFC 3973 PIM Dense Mode
RFC 3973 PIM Dense Mode (Premium Edge License)
RFC 3973 PIM Dense Mode
RFC 4601 Draft 10 PIM Sparse Mode
RFC 4601 Draft 10 PIM Sparse Mode
RFC 4605 IGMP/MLD Proxying

IPv6
RFC 1350 TFTP
RFC 1881 IPv6 Address Allocation Management
RFC 1886 DNS Extension for IPv6
RFC 1887 IPv6 Unicast Address Allocation Architecture
RFC 1981 IPv6 Path MTU Discovery
RFC 2080 RIPng for IPv6
RFC 2292 Advanced Sockets API for IPv6
RFC 2373 IPv6 Addressing Architecture
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 IPv6 Specification
RFC 2461 IPv6 Neighbor Discovery
RFC 2462 IPv6 Stateless Address Auto-configuration
RFC 2463 ICMPv6
RFC 2464 Transmission of IPv6 over Ethernet Networks
RFC 2472 IP Version 6 over PPP
RFC 2473 Generic Packet Tunneling in IPv6
RFC 2475 IPv6 DiffServ Architecture
RFC 2529 Transmission of IPv6 Packets over IPv4
RFC 2545 Use of MP-BGP-4 for IPv6
RFC 2553 Basic Socket Interface Extensions for IPv6
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2711 IPv6 Router Alert Option
RFC 2740 OSPFv3 for IPv6
RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 2925 Remote Operations MIB (Ping only)
RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
RFC 3162 RADIUS and IPv6
RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
RFC 3307 IPv6 Multicast Address Allocation
RFC 3315 DHCPv6 (client and relay)
RFC 3315 DHCPv6 (client only)
RFC 3363 DNS support
RFC 3484 Default Address Selection for IPv6
RFC 3493 Basic Socket Interface Extensions for IPv6
RFC 3513 IPv6 Addressing Architecture
RFC 3542 Advanced Sockets API for IPv6
RFC 3587 IPv6 Global Unicast Address Format
RFC 3596 DNS Extension for IPv6
RFC 3810 MLDv2 (host joins only)
RFC 3810 MLDv2 for IPv6
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4022 MIB for TCP
RFC 4113 MIB for UDP
RFC 4251 SSHv6 Architecture
RFC 4252 SSHv6 Authentication
RFC 4252 SSHv6 Transport Layer
RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4291 IP Version 6 Addressing Architecture
RFC 4293 MIB for IP
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
RFC 5340 OSPF for IPv6
RFC 5340 OSPFv3 for IPv6
RFC 5722 Handling of Overlapping IPv6 Fragments

MIBs
IEEE 8021-PAE-MIB
IEEE 8023-LAG-MIB
RFC 1156 (TCP/IP MIB)
RFC 1212 Concise MIB Definitions
RFC 1213 MIB II
RFC 1229 Interface MIB Extensions
RFC 1286 Bridge MIB
RFC 1493 Bridge MIB
RFC 1573 SNMP MIB II
RFC 1643 Ethernet MIB
RFC 1650 Ethernet-Like MIB
RFC 1657 BGP-4 MIB
RFC 1724 RIPv2 MIB
RFC 1757 Remote Network Monitoring MIB
RFC 1850 OSPFv2 MIB
RFC 1907 SNMPv2 MIB
RFC 2011 SNMPv2 MIB for IP
RFC 2012 SNMPv2 MIB for TCP
RFC 2013 SNMPv2 MIB for UDP
RFC 2021 RMONv2 MIB
RFC 2096 IP Forwarding Table MIB
RFC 2233 Interface MIB
RFC 2233 Interfaces MIB
RFC 2273 SNMP-NOTIFICATION-MIB
RFC 2452 IPV6-TCP-MIB
RFC 2454 IPV6-UDP-MIB
RFC 2465 IPv6 MIB
RFC 2466 ICMPv6 MIB
RFC 2571 SNMP Framework MIB
RFC 2572 SNMP-MPD MIB

Specifications (continued)

Standards and protocols
(applies to all products in series)

HP 6616 Router Chassis (JC496A)

RFC 2574 SNMP USM MIB
RFC 2618 RADIUS Client MIB
RFC 2620 RADIUS Accounting MIB
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
RFC 2674 802.1p and IEEE 802.1Q Bridge MIB
RFC 2688 MAU-MIB
RFC 2737 Entity MIB (Version 2)
RFC 2787 VRRP MIB
RFC 2819 RMON MIB
RFC 2863 The Interfaces Group MIB
RFC 2925 Ping MIB
RFC 2932IP (Multicast Routing MIB)
RFC 2933 IGMP MIB
RFC 3273 HC-RMON MIB
RFC 3414 SNMP-User based-SM MIB
RFC 3415 SNMP-View based-ACM MIB
RFC 3418 MIB for SNMPv3
RFC 3621 Power Ethernet MIB
RFC 3813 MPLS LSR MIB
RFC 3814 MPLS FTN MIB
RFC 3815 MPLS LDP MIB
RFC 3826 AES for SNMP's USM MIB
RFC 4113 UDP MIB
RFC 4133 Entity MIB (Version 3)
RFC 4221 MPLS FTN MIB
LLDP-EXT-DOT1-MIB
LLDP-EXT-DOT3-MIB
LLDP-MIB

Network management
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
IEEE 802.1D (STP)
RFC 1098 A Simple Network Management Protocol (SNMP)
RFC 1155 Structure of Management Information
RFC 1157 SNMPv1
RFC 1215 SNMP Generic traps
RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
RFC 1901 SNMPv2 Introduction
RFC 1902 SNMPv2 Structure
RFC 1903 SNMPv2 Textual Conventions
RFC 1904 SNMPv2 Conformance
RFC 1905 SNMPv2 Protocol Operations
RFC 1906 SNMPv2 Transport Mappings
RFC 1918 Private Internet Address Allocation
RFC 2272 SNMPv3 Management Protocol
RFC 2273 SNMPv3 Applications
RFC 2274 USM for SNMPv3
RFC 2275 VACM for SNMPv3
RFC 2570 SNMPv3 Overview
RFC 2571 SNMP Management Frameworks
RFC 2572 SNMPv3 Message Processing
RFC 2573 SNMPv3 Applications
RFC 2574 SNMPv3 User-based Security Model (USM)
RFC 2575 SNMPv3 View-based Access Control Model (VACM)
RFC 2575 VACM for SNMP
RFC 2576 Coexistence between SNMP versions
RFC 2578 SMIv2
RFC 2581 TCP6
RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events)
RFC 3164 BSD syslog Protocol
RFC 3176 sFlow
RFC 3411 SNMP Management Frameworks
RFC 3412 SNMPv3 Message Processing

HP 6608 Router Chassis (JC177B)

RFC 3414 SNMPv3 User-based Security Model (USM)
RFC 3415 SNMPv3 View-based Access Control Model VACM)
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2
SNMPv1/v2c
SNMPv1/v2c (read only)
SNMPv1/v2c/v3

OSPF
RFC 1245 OSPF protocol analysis
RFC 1246 Experience with OSPF
RFC 1253 OSPFv2 MIB
RFC 1583 OSPFv2
RFC 1587 OSPF NSSA
RFC 1745 OSPF Interactions
RFC 1765 OSPF Database Overflow
RFC 1850 OSPFv2 Management Information Base (MIB), traps
RFC 2178 OSPFv2
RFC 2328 OSPFv2
RFC 2328 OSPFv2
RFC 2328 OSPFv2 (Premium Edge License)
RFC 2370 OSPF Opaque LSA Option
RFC 3101 OSPF NSSA
RFC 3623 Graceful OSPF Restart
RFC 5340 OSPF for IPv6
RFC 5340 OSPFv3 for IPv6

QoS/CoS
IEEE 802.1P (CoS)
RFC 2474 DiffServ Precedence, including 8 queues/port
RFC 2474 DiffServ precedence, with 4 queues per port
RFC 2474 DS Field in the IPv4 and IPv6 Headers
RFC 2474 DSCP DiffServ
RFC 2474, with 4 queues per port
RFC 2475 DiffServ Architecture
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2597 DiffServ Assured Forwarding (AF)- partial support
RFC 2598 DiffServ Expedited Forwarding (EF)
Ingress Rate Limiting

Security
IEEE 802.1X Port Based Network Access Control
RFC 1321 The MD5 Message-Digest Algorithm
RFC 1492 TACACS+
RFC 2082 RIP-2 MD5 Authentication
RFC 2104 Keyed-Hashing for Message Authentication
RFC 2138 RADIUS Authentication
RFC 2139 RADIUS Accounting
RFC 2209 RSVP-Message Processing
RFC 2246 Transport Layer Security (TLS)
RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2548 Microsoft Vendor-specific RADIUS Attributes
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2818 HTTP Over TLS
RFC 2865 RADIUS (client only)
RFC 2865 RADIUS Authentication
RFC 2866 RADIUS Accounting
RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 3567 Intermediate System (IS) to IS Cryptographic Authentication
RFC 3576 Dynamic Authorization Extensions to RADIUS
RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1X RADIUS
Access Control Lists (ACLs)
Guest VLAN for 802.1x
MAC Authentication
Port Security
Secure Sockets Layer (SSL)
SSHv1 Secure Shell
SSHv1.5 Secure Shell
SSHv1/SSHv2 Secure Shell
SSHv2 Secure Shell

VPN
RFC 2403 - HMAC-MD5-96
RFC 2404 - HMAC-SHA1-96
RFC 2405 - DES-CBC Cipher algorithm
RFC 2407 - Domain of interpretation
RFC 2547 BGP/MPLS VPNs
RFC 2764 A Framework for IP Based Virtual Private Networks
RFC 2796 BGP Route Reflection - An Alternative to Full Mesh IBGP
RFC 2842 Capabilities Advertisement with BGP-4
RFC 2858 Multiprotocol Extensions for BGP-4
RFC 2917 A Core MPLS IP VPN Architecture
RFC 2918 Route Refresh Capability for BGP-4
RFC 3107 Carrying Label Information in BGP-4
RFC 4301 - Security Architecture for the Internet Protocol
RFC 4302 - IP Authentication Header (AH)
RFC 4303 - IP Encapsulating Security Payload (ESP)
RFC 4305 - Cryptographic Algorithm Implementation Requirements for ESP and AH

IPsec
RFC 1828 IP Authentication using Keyed MD5
RFC 2401 IP Security Architecture
RFC 2402 IP Authentication Header
RFC 2406 IP Encapsulating Security Payload
RFC 2407 - Domain of interpretation
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange
RFC 2410 - The NULL Encryption Algorithm and its use with IPsec
RFC 2411 IP Security Document Roadmap
RFC 2412 – OAKLEY
RFC 2865 - Remote Authentication Dial In User Service (RADIUS)

IKEv1
RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
RFC 3748 - Extensible Authentication Protocol (EAP)

HP 6600 Router Series accessories

Transceivers

HP X110 100M SFP LC LH40 Transceiver (JD090A)
HP X110 100M SFP LC LH80 Transceiver (JD091A)
HP X110 100M SFP LC FX Transceiver (JD102B)
HP X110 100M SFP LC LX Transceiver (JD120B)
HP X120 622M SFP LC LX 15km Transceiver (JF829A)
HP X120 622M SFP LC LH 40km 1310 Transceiver (JF830A)
HP X120 622M SFP LC LH 80km 1550 Transceiver (JF831A)
HP X125 1G SFP LC LH40 1310nm Transceiver (JD061A)
HP X120 1G SFP LC LH40 1550nm Transceiver (JD062A)
HP X120 1G SFP LC BX 10-U Transceiver (JD098B)
HP X120 1G SFP LC BX 10-D Transceiver (JD099B)
HP X120 1G SFP LC LH100 Transceiver (JD103A)
HP X120 1G SFP LC SX Transceiver (JD118B)
HP X120 1G SFP LC LX Transceiver (JD119B)
HP X125 1G SFP LC LH70 Transceiver (JD063B)
HP X120 1G SFP RJ45 T Transceiver (JD089B)
HP X160 2.5G SFP LC 2km Transceiver (JD084A)
HP X160 2.5G SFP LC 15km Transceiver (JD085A)
HP X160 2.5G SFP LC 40km Transceiver (JD086A)
HP X160 2.5G SFP LC 80km Transceiver (JD087A)
HP X135 10G XFP LC ER Transceiver (JD121A)
HP X130 10G XFP LC LR Transceiver (JD108B)
HP X130 10G XFP LC SR Transceiver (JD117B)

Cables

HP X200 V.24 DTE 3m Serial Port Cable (JD519A)
HP X200 V.24 DCE 3m Serial Port Cable (JD521A)
HP X200 V.35 DTE 3m Serial Port Cable (JD523A)
HP X200 V.35 DCE 3m Serial Port Cable (JD525A)
HP X200 X.21 DTE 3m Serial Port Cable (JD527A)
HP X200 X.21 DCE 3m Serial Port Cable (JD529A)
HP X260 RS449 3m DTE Serial Port Cable (JF825A)
HP X260 RS449 3m DCE Serial Port Cable (JF826A)
HP X260 RS530 3m DTE Serial Port Cable (JF827A)
HP X260 RS530 3m DCE Serial Port Cable (JF828A)
HP X260 8E1 BNC 75 ohm 3m Router Cable (JD512A)
HP X260 E1 RJ45 BNC 75-120 ohm Conversion Router Cable (JD511A)

Security Modules

HP A6600 VPN Firewall Module (JC639A)

Router Modules

HP 6600 1-port OC-3/STM-1 (E1/T1) CPOS SFP HIM Module (JC161A)
HP 6600 2-port OC-3/STM-1 (E1/T1) CPOS SFP HIM Module (JC162A)
HP 6600 2-port OC-3/STM-1 (E3/T3) CPOS SFP HIM Module (JC169A)
HP 6600 1-port OC-3/STM-1 (E3/T3) CPOS SFP HIM Module (JC170A)
HP 6600 4-port OC-3c/STM-1c or 2-port OC-12c/STM-4c POS SFP HIM Module (JC172A)
HP 6600 2-port OC-3c/STM-1c or 1-port OC-12c/STM-4c POS SFP HIM Module (JC173A)
HP 6600 1-port OC-48c/STM-16c POS/CPOS SFP HIM Module (JC494A)
HP 6600 1-port OC-3c/STM-1c ATM SFP HIM Module (JC175A)
HP 6600 2-port OC-3c/STM-1c ATM SFP HIM Module (JC495A)
HP 6600 4-port GbE SFP HIM Module (JC171A)
HP 6600 8-port GbE SFP HIM Module (JC174A)
HP 6600 4-port Gig-T HIM Module (JC163A)
HP 6600 8-port Gig-T HIM Module (JC164A)
HP 6600 1-port 10-GbE XFP HIM Module (JC168A)
HP MSR 2-port Enhanced Sync/Async Serial MIM Module (JD540A)
HP MSR 4-port Enhanced Sync/Async Serial MIM Module (JD541A)
HP MSR 8-port Enhanced Sync/Async Serial MIM Module (JD552A)
HP MSR 2-port Gig-T MIM Module (JD548A)
HP MSR 8-port E1/CE1/PRI (75ohm) MIM Module (JD563A)
HP MSR 8-port E1/Fractional E1 (75ohm) MIM Module (JF255A)
HP MSR 8-port T1/CT1/PRI MIM Module (JC160A)
HP MSR 1-port E3/CE3/FE3 MIM Module (JD630A)
HP MSR 8-port T1/Fractional T1 MIM Module (JC159A)
HP MSR 1-port T3/CT3/FT3 MIM Module (JD628A)
NEW HP 6600 8-port 10/100Base-T HIM Module (JC575A)
NEW HP 6600 2-port OC-48c/STM-16c RPR SFP HIM Module (JC576A)

Memory

HP 6600 1GB SDRAM (JC179A)

HP 6602 Router Chassis (JC176A)

HP RPS 800 Redundant Power Supply (JD183A)
HP X290 MSR30 1m RPS Cable (JD637A)

HP 6604 Router Chassis (JC178B)

HP 7500 650W DC Power Supply (JD209A)
HP 7500 650W AC Power Supply (JD217A)
NEW HP 6604 Dustproof Frame (JC572A)
NEW HP 6604 Spare Fan Assembly (JC569A)
HP 6600 Router Software License (JC180A)
HP 6600 RPE-X1 Main Processing Unit (JC165A)
HP 6600 FIP-110 Flexible Interface Platform Module (JC166A)
HP 6600 FIP-200 Router Module (JC167A)
NEW HP 6600 RSE-X1 Main Processing Unit (JC566A)

HP 6600 Router Series accessories (continued)

NEW HP 6600 24-port GbE SFP Service Aggregation Platform (SAP) Module (JC568A)
NEW HP 6600 48-port Gig-T Service Aggregation Platform (SAP) Module (JC567A)
HP 6600 FIP-110 Flexible Interface Platform Module (JC166B)
HP 6600 FIP-210 Flexible Interface Platform Module (JC167B)
HP 6600 Firewall Processing Router Module (JD250A)

HP 6616 Router Chassis (JC496A)

HP 6600 650W AC Power Supply (JC492A)
HP 6600 650W DC Power Supply (JC493A)
NEW HP 6616 Spare Fan Assembly (JC571A)
NEW HP 6616 Dustproof Frame (JC574A)
HP 6600 RPE-X1 Carrier Card (JC497A)
HP 6600 Router Software License (JC180A)
HP 6600 RPE-X1 Main Processing Unit (JC165A)
HP 6600 FIP-110 Flexible Interface Platform Module (JC166A)
HP 6600 FIP-200 Router Module (JC167A)
NEW HP 6600 RSE-X1 Main Processing Unit (JC566A)
NEW HP 6600 24-port GbE SFP Service Aggregation Platform (SAP) Module (JC568A)
NEW HP 6600 48-port Gig-T Service Aggregation Platform (SAP) Module (JC567A)
HP 6600 FIP-110 Flexible Interface Platform Module (JC166B)
HP 6600 FIP-210 Flexible Interface Platform Module (JC167B)
HP 6600 Firewall Processing Router Module (JD250A)

HP 6608 Router Chassis (JC177B)

HP 7500 650W DC Power Supply (JD209A)
HP 7500 650W AC Power Supply (JD217A)
NEW HP 6608 Spare Fan Assembly (JC570A)
NEW HP 6608 Dustproof Frame (JC573A)
HP 6600 Router Software License (JC180A)
HP 6600 RPE-X1 Main Processing Unit (JC165A)
HP 6600 FIP-110 Flexible Interface Platform Module (JC166A)
HP 6600 FIP-200 Router Module (JC167A)
NEW HP 6600 RSE-X1 Main Processing Unit (JC566A)
NEW HP 6600 24-port GbE SFP Service Aggregation Platform (SAP) Module (JC568A)
NEW HP 6600 48-port Gig-T Service Aggregation Platform (SAP) Module (JC567A)
HP 6600 FIP-110 Flexible Interface Platform Module (JC166B)
HP 6600 FIP-210 Flexible Interface Platform Module (JC167B)
HP 6600 Firewall Processing Router Module (JD250A)

To learn more, visit www.hp.com/networking

4AA3-0765ENW, Created August 2010; Updated September 2011, Rev. 3

networktest

HP/Cisco Switching and Routing Interoperability Test Results

April 2011

Executive Summary

HP commissioned Network Test to assess interoperability between its enterprise switch/routers and those of Cisco Systems. Working with an extensive test bed that included core-, distribution-, and access-layer devices, Network Test successfully validated interoperability of 13 key protocols used in enterprise networks. Tests involved IPv4 and IPv6; switching and routing; and unicast and multicast traffic. **In all cases described here, the HP and Cisco switch/routers correctly forwarded traffic.**

The following table summarizes results of interoperability testing.

HP / Cisco Protocol Interoperability			
	HP A9505	**HP E5406zl**	**HP A5800**
VLAN trunking			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
L2/L3 jumbo frame handling			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
Link aggregation			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
Spanning tree protocol			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
OSPFv2 for IPv4			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
OSPFv3 for IPv6			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
Multicast switching and routing			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓
VRRP			
Cisco Catalyst 3750-E	✓	✓	✓
Cisco Catalyst 4506	✓	✓	✓
Cisco Catalyst 6509	✓	✓	✓

Methodology and Results

Figure 1 below illustrates the test bed used to validate interoperability. The HP and Cisco switch/routers used a three-tier design commonly found in enterprise campus networks, with separate devices at the core, distribution, and access layers. A Spirent TestCenter traffic generator/analyzer emulated clients and servers, and externally verified interoperability of the various protocols.

Except where otherwise noted, tests involved connections between each layer of the network, thus validating interoperability of each protocol using every device on the test bed. Also unless otherwise noted, tests also used multiple redundant connections between switch/routers to exercise link aggregation, spanning tree, and routing protocols.

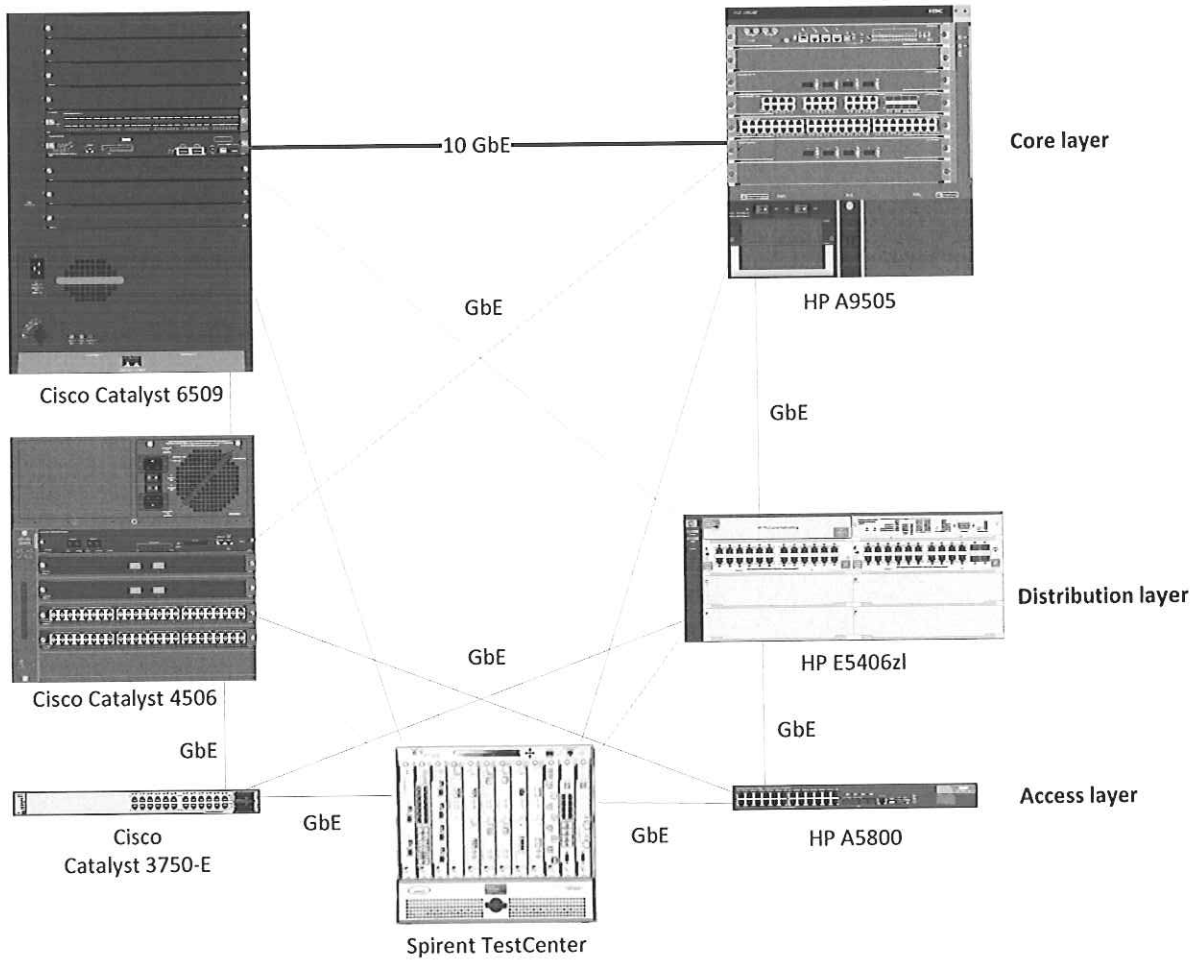


Figure 1: The HP-Cisco Interoperability Test Bed

VLAN Trunking

Network Test evaluated interoperability of IEEE 802.1Q VLAN trunking in three ways: forwarding of allowed tagged traffic; forwarding of allowed untagged (native) traffic; and blocking of disallowed untagged traffic.

Engineers configured five VLANs on each switch, and configured trunk ports between switches to allow traffic from three VLANs as tagged frames and a fourth VLAN as untagged frames. To determine if switches would correctly block disallowed traffic, engineers did not include the fifth VLAN ID in the list of VLANs allowed across trunk ports.

Spirent TestCenter then offered untagged traffic to each HP and Cisco access and distribution switch in a bidirectional pattern. In all cases, traffic counters on the Spirent test instrument verified that **HP and Cisco switches correctly forwarded VLAN traffic that was intended to be forwarded, and did not carry VLAN traffic that was not intended to be forwarded.**

L2/L3 Jumbo Frame Handling

Jumbo Ethernet frames – those larger than the standard maximum length of 1,518 bytes – are commonly used for bulk data-transfer applications such as backups, storage, and disaster recovery. To validate the ability of HP and Cisco switch/routers to exchange jumbo frames, Network Test offered these frames in both switching and routing modes.

In the switching tests, Spirent TestCenter offered 9,216-byte jumbo Ethernet frames using a "partially meshed" topology, meaning all traffic offered to HP devices was destined to Cisco ports and vice-versa. **All HP and Cisco devices correctly switched traffic consisting of jumbo frames.**

In the routing assessment, Network Test enabled OSPF on both HP and Cisco devices. The OSPF protocol will not exchange traffic unless routers agree on the same maximum transmission unit (MTU). In this case, with 9,198-byte IP packets inside 9,216-byte Ethernet frames, **all HP and Cisco devices successfully established OSPF adjacencies as expected, and successfully routed traffic consisting of jumbo frames.**

Link Aggregation

Network Test evaluated the ability of HP and Cisco devices to bundle multiple physical ports into one logical port using the IEEE 802.3ad link aggregation protocol.

Engineers configured the HP and Cisco devices to set up link aggregation groups (LAGs) between the access, distribution, and core layers. Specifically for this test, engineers then disabled any redundant paths through the network, forcing traffic to be forwarded across each LAG. Spirent TestCenter offered bidirectional traffic to eight ports on each access and distribution switch/router, emulating 32 hosts on

each port to encourage distribution of flows across the multiple LAG members. **In all cases, the HP and Cisco switches correctly forwarded traffic using link aggregation.**

To validate that link aggregation can supply additional bandwidth by bundling multiple physical ports, engineers configured Spirent TestCenter to offer traffic at an aggregate rate in excess of 1 Gbit/s in each direction, the nominal capacity of a single link. In all cases, the aggregated links carried the additional traffic with zero frame loss.

Spanning Tree Protocol (STP)

The spanning tree protocol serves as a key loop prevention and redundancy mechanism in enterprise networks. Over the years it has been refined with updates such as rapid spanning tree (RSTP) to speed convergence and multiple spanning tree (MSTP) to form a separate spanning tree instance for each VLAN. In addition to these standards-based methods, Cisco switches use proprietary variants called per-VLAN spanning tree plus (PSVT+) and Rapid PVST+.

Network Test verified HP-Cisco interoperability using four variations of spanning tree:

1. RSTP (HP) / PVST+ (Cisco)
2. MSTP (HP and Cisco, using the IEEE 802.1s specification)
3. MSTP (HP) / PVST+ (Cisco)
4. MSTP (HP) / Rapid PVST+ (Cisco)

For each variation, engineers set up redundant connections between all devices, thus forcing spanning tree to select a root bridge and place device ports in either blocked or forwarding states. Engineers then offered traffic to each device using Spirent TestCenter and verified that traffic was received only from an intended port in forwarding state.

While continuing to offer traffic, engineers then tested spanning tree convergence by administratively disabling a port in forwarding state, forcing the spanning tree to bring up ports formerly in blocked state. Engineers verified correct spanning tree operation by observing Spirent TestCenter port counters and by examining the command-line interface (CLI) output for spanning tree on each device. **In all four test cases, spanning tree delivered loop-free operation and seamless failover.**

OSPFv2 for IPv4/OSPFv3 for IPv6

IP routing is a given in enterprise networks, and by far the most commonly used interior gateway protocol is Open Shortest Path First (OSPF).

To validate OSPF interoperability between HP and Cisco devices, engineers enabled OSPF on all switch/routers on the test bed, and then configured Spirent TestCenter to emulate OSPF routers

attached to each device. This is a more rigorous and stressful topology than is commonly found in most enterprise networks, where IP routing often is found only on core devices. Here, all switch/routers, including those at the distribution and access layers, brought up OSPF routing sessions and forwarded traffic to and from networks advertised using OSPF.

Engineers conducted these routing tests twice, with IPv4 and IPv6 variations. In IPv4 testing, engineers configured OSPF version 2, while IPv6 testing used the newer OSPFv3 variant of the protocol.[1]

In these tests, Spirent TestCenter emulated OSPF routers attached to each switch/router. After bringing up an OSPF session, these emulated routers used OSPF to advertise networks "behind" them, and then offered traffic to and from these networks.

For this interoperability test to work successfully, HP and Cisco switch/routers would need to share routing information to forward traffic to these emulated networks. That is exactly what happened: **All HP and Cisco devices not only established OSPF sessions over IPv4 and IPv6, but also forwarded all traffic to all networks with zero frame loss observed.**

These results validate OSPF routing interoperability between all HP and Cisco devices, both on IPv4 and IPv6 networks.

Multicast Switching and Routing

Streaming media, conferencing, financial quote services and many other applications are making increasing use of IP multicast. Network Test validated the ability of HP and Cisco equipment to share information about multicast topology both in purely switched and switched/routed environments.

In the switched scenario, engineers configured all HP and Cisco devices in layer-2 mode and enabled IGMP snooping. In the routed scenario, all devices used the Protocol Independent Multicast-Sparse Mode (PIM-SM) routing protocol and OSPF to carry multicast and unicast routing information, respectively.

In both scenarios, a Spirent TestCenter port attached to the Cisco Catalyst 3750-E offered traffic destined to 10 multicast groups while other test ports emulated multicast subscribers to all 10 groups on the HP A5800 and HP E5406zl. Engineers also attached one additional monitor port to each of the HP devices to verify they did not flood multicast frames to non-subscriber ports.

The HP and Cisco devices correctly delivered multicast traffic to subscribers in both switched and routed configurations, and did not flood traffic to non-subscribers.

In addition, Network Test evaluated IGMP snooping support while multicast routing was enabled. When operating in Ethernet switching mode, the HP and Cisco devices use IGMP reports to determine which

[1] IETF RFC 2328 describes OSPFv2 and RFC 5340 describes OSPFv3. While the basic mechanics of OSPF are identical in both versions, OSPFv3 introduces new link-state advertisement (LSA) types; removes addressing semantics from OSPF headers; generalizes flooding; and removes OSPF-layer authentication, among other changes.

switch ports have subscribers attached. Working with IGMPv2, engineers verified the HP and Cisco switches correctly populated IGMP snooping tables and forwarded multicast traffic in all cases.

Virtual Router Redundancy Protocol (VRRP)

Network Test verified the ability of HP and Cisco devices to provide router failover using the Virtual Router Redundancy Protocol (VRRP). As defined by the Internet Engineering Task Force (IETF) in RFC 5798, VRRP provides a standard method by which multiple routers select Master and Backup roles, with a Backup router taking over from a Master in the event of a router or link failure.

Testing involved all six HP and Cisco devices as shown in Figure 1 above, with VRRP running on the HP A9505, the HP EE5406zl, and the Cisco Catalyst 6509. The devices running VRRP agreed on a virtual IP (VIP) addresses, verified by examining their respectively CLIs.

Initially, the HP A9505 acted in the Master role and the Cisco Catalyst 6509 acted as Backup. Then engineers configured the Cisco device to take over as Master by changing its priority to force VRRP failover. Again, the two sides agreed on VRRP settings, and traffic counters on Spirent TestCenter showed devices forwarding traffic after the failover.

Engineers then repeated this exercise using the HP EE5406zl and the Cisco Catalyst 6509, and again failover worked as expected.

The results demonstrate that upon failure of an active router or link, HP and Cisco devices work together using VRRP to reroute traffic onto a backup link, with minimal interruption to users and applications.

Conclusion

Interoperability testing was successful in every case where both HP and Cisco devices supported a given protocol. This provides assurance to network professionals considering design or deployment of networks comprised of a mix of HP and Cisco switch/routers.

Appendix A: About Network Test

Network Test is an independent third-party test lab and engineering services consultancy. Our core competencies are performance, security, and conformance assessment of networking equipment and live networks. Our clients include equipment manufacturers, large enterprises, service providers, industry consortia, and trade publications.

Appendix B: Software Releases Tested

This appendix describes the software versions used on the test bed. All tests were conducted in March 2011 at Network Test's facility in Westlake Village, CA, USA.

Component	Version
HP A9505	5.20, Release 1238P08
HP EE5406zl	K.15.03.0007
HP A5800	5.20, Release 1206
Cisco Catalyst 6509	12.2(33)SXI2a
Cisco Catalyst 4506	12.2(20)EWA
Cisco Catalyst 3750-E	12.2(55)SE1
Spirent TestCenter	3.55.5086.0000

Appendix C: Disclaimer

Network Test Inc. has made every attempt to ensure that all test procedures were conducted with the utmost precision and accuracy, but acknowledges that errors do occur. Network Test Inc. shall not be held liable for damages which may result for the use of information contained in this document. All trademarks mentioned in this document are property of their respective owners.

Network Test Inc.
31324 Via Colinas, Suite 113
Westlake Village, CA 91362-6761
USA
+1-818-889-0011
http://networktest.com
info@networktest.com

networktest

HP/Cisco Switching and Routing Interoperability Cookbook

May 2011

TABLE OF CONTENTS

ILLUSTRATIONS

Introduction

Objective

This configuration guide aims to help networking professionals interconnect HP Networking and Cisco Catalyst switches using a variety of protocols commonly found in enterprise campus networks. By following the step-by-step procedures described in this document, it should be possible to verify interoperability and to pass traffic between the two vendors' switches.

Intended audience

This guide is intended for any network architect, administrator, or engineer who needs to interconnect HP and Cisco Ethernet switches.

This guide assumes familiarity with basic Ethernet and TCP/IP networking concepts, as well as at least limited experience with the HP Networking and Cisco IOS command-line interfaces (CLIs). No previous experience is assumed for the protocols discussed in this document.

For basic TCP/IP networking concepts, the standard references are ***Internetworking with TCP/IP, Volume 1*** by Douglas E. Comer and ***TCP/IP Illustrated, Volume 1*** by W. Richard Stevens.

For IP multicast topics, ***Deploying IP Multicast in the Enterprise*** by Thomas A. Maufer is a popular choice.

Devices under test

Using the commands given in this document, Network Test has verified interoperability between the HP A9505, HP E5406zl, and HP A5800 Ethernet switches and Cisco Catalyst 6509, Cisco Catalyst 4506, and Catalyst 3750-E Ethernet switches. Appendix B lists software versions used.

Except where specifically noted, command syntax for HP Networking and Cisco Catalyst switches does not change across product lines. In cases where HP A-series and E-series switches use different command syntax, this is explicitly noted.

Conventions used in this document

The following table lists text and syntax conventions.

Conventions	Description	Examples
Bold Type	Represents user-inputted text.	To enter configuration mode, type the **system-view** command: <HP5800> **system-view**
Fixed-width text like this	Represents output that appears on the terminal screen.	<A9505> **display stp bridge** MSTID Port Role STP State Protection 0 Bridge-Aggregation20 ROOT FORWARDING NONE 0 GigabitEthernet3/0/11 DESI FORWARDING NONE 0 GigabitEthernet3/0/16 DESI FORWARDING NONE
Italic text like this	• Introduces important new terms • Identifies book titles • Identifies RFC and Internet-draft titles	• A policy *term* is a named structure that defines match conditions and actions. • *TCP/IP Illustrated Volume 1* by W. Richard Stevens. • RFC 4814, *Hash and Stuffing: Overlooked Factors in Network Device Benchmarking*

Interoperability testing

For each protocol tested, this document uses a five-section format consisting of objective, technical background, HP configuration, Cisco configuration, and test validation.

Topology

Except where otherwise noted, engineers used the standard test bed shown in Figure 1 below to validate protocol interoperability. The test bed uses the three-tier network design commonly found in campus enterprise networks, with access, distribution, and core layers represented. In this example network, access switches (HP A5800 and Cisco Catalyst C3750-E) connect to distribution switches (HP E5406zl and Cisco Catalyst 4506), which in turn connect to core switches (HP A9505 and Cisco Catalyst 6509). For redundancy, multiple connections exist between switch layers.

Test engineers configured link aggregation between HP A5800 and HP E5406zl switches; between HP E5406zl and HP A9505 switches; between HP A9505 and Cisco Catalyst 6509 switches; between Cisco Catalyst 6509 and Cisco Catalyst 4506 switches; and between Cisco Catalyst 4506 and Cisco Catalyst 3750-E switches. The use of link aggregation is not mandatory, however.

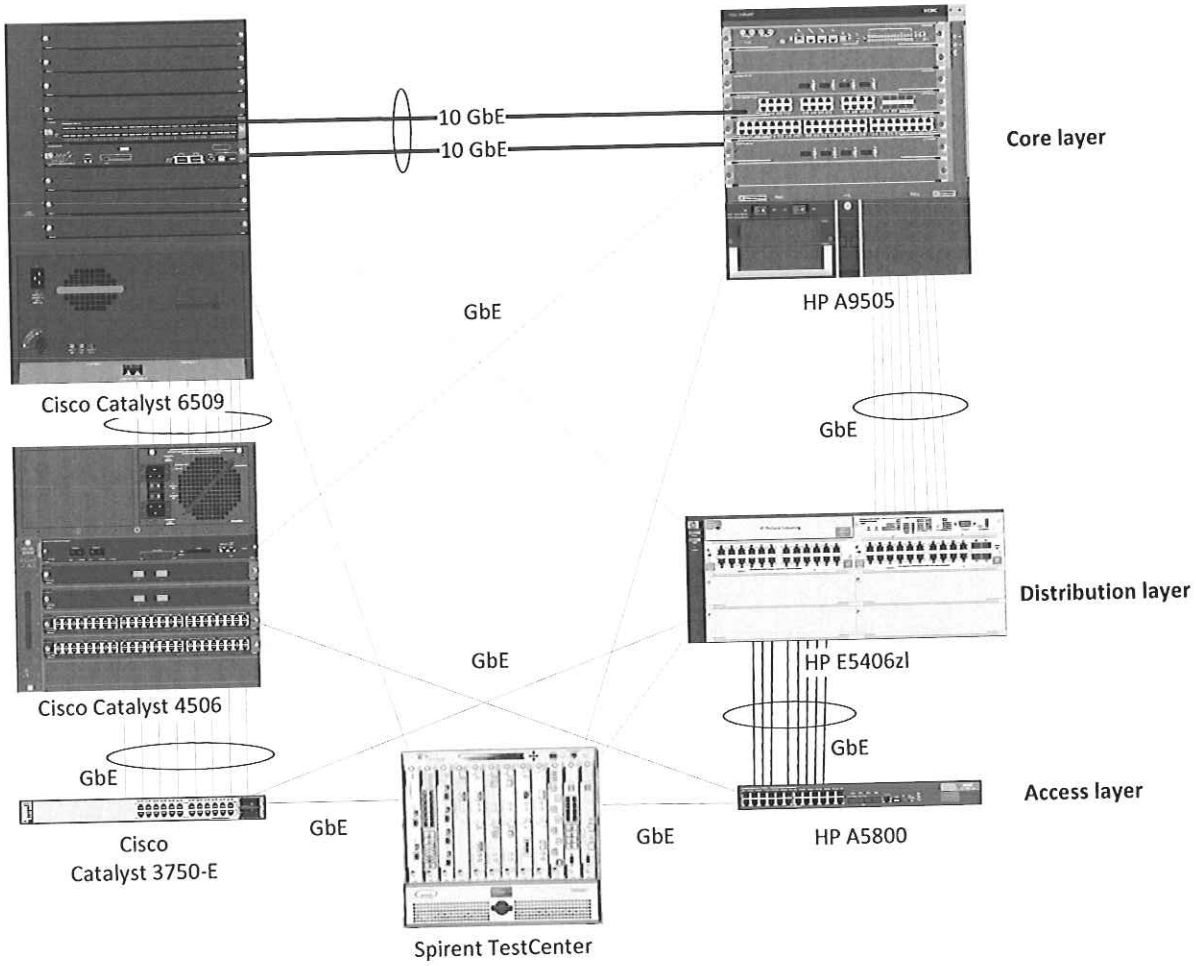


Figure 1: HP-Cisco interoperability test bed

Virtual LAN (VLAN) trunking

Objective

To verify interoperability of IEEE 802.1Q VLAN trunking between HP Networking and Cisco Catalyst switches using tagged traffic.

To verify interoperability of IEEE 802.1Q VLAN trunking between HP Networking and Cisco Catalyst switches using untagged traffic.

Background

The IEEE 802.1Q specification defines a method of defining virtual broadcast domains. A 4-byte VLAN header, usually called a "tag," allows definition of broadcast domains that may differ from physical switch topology. With VLANs, all switch ports are members of the same broadcast domain; with VLAN tagging, a network manager can set up multiple broadcast domains across switches, and restrict broadcasts for different VLANs on different ports.

Topology

This configuration example will validate VLAN trunking interoperability between HP Networking and Cisco Catalyst switches in three ways:

- The switches will forward allowed tagged traffic from multiple VLANs across a trunk port.
- The switches will forward allowed untagged traffic from a native VLAN across a trunk port.
- The switch will not forward disallowed tagged traffic across a trunk port.

The final example above is a negative test to verify that switches with VLAN trunking will forward only traffic explicitly permitted by the switch configurations.

This test used the standard test bed (see Figure 1, above). In this example, all interswitch communication is done via VLAN trunks. The trunk ports on each switch will allow tagged traffic with VLAN IDs from 301 through 303, and untagged traffic from ports with VLAN ID of 300. A fifth VLAN, with an ID of 304, is also defined by the trunk ports are configured not to allow that traffic.

HP A-series commands

First, define VLANs 300 to 304.

```
<HP5800> system-view
[HP5800] vlan 300 to 304
```

Then, define a VLAN trunk port that allows tagged traffic from VLANs 301-303, and native untagged traffic on VLAN 300.

```
[HP5800] interface GigabitEthernet1/0/23
[HP5800-gigabitethernet1/0/23]  port link-mode bridge
[HP5800-gigabitethernet1/0/23]  port link-type trunk
[HP5800-gigabitethernet1/0/23]  undo port trunk permit vlan 1
[HP5800-gigabitethernet1/0/23]  port trunk permit vlan 300 to 303
[HP5800-gigabitethernet1/0/23]  port trunk pvid vlan 300
[HP5800-gigabitethernet1/0/23]  quit
```

Next, define access-mode interfaces allowing untagged traffic for VLANs 300-304.

```
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1]  port link-mode bridge
[HP5800-Gigabitethernet1/0/1]  port access vlan 300
[HP5800-Gigabitethernet1/0/1] interface GigabitEthernet1/0/2
[HP5800-Gigabitethernet1/0/2]  port link-mode bridge
[HP5800-Gigabitethernet1/0/2]  port access vlan 301
[HP5800-Gigabitethernet1/0/2] interface GigabitEthernet1/0/3
[HP5800-Gigabitethernet1/0/3]  port link-mode bridge
[HP5800-Gigabitethernet1/0/3]  port access vlan 302
[HP5800-Gigabitethernet1/0/3] interface GigabitEthernet1/0/4
[HP5800-Gigabitethernet1/0/4]  port link-mode bridge
[HP5800-Gigabitethernet1/0/4]  port access vlan 303
[HP5800-Gigabitethernet1/0/4] interface GigabitEthernet1/0/5
[HP5800-Gigabitethernet1/0/5]  port link-mode bridge
[HP5800-Gigabitethernet1/0/5]  port access vlan 304
[HP5800-Gigabitethernet1/0/5]  quit
[HP5800]  quit
```

HP E-series commands

HP E-series switches combine trunk creation, access ports, and VLAN assignment together into a single VLAN construct. A port that is a member of a single VLAN carrying only untagged traffic is an access port (ports A1-A5 in this example). A port that is a member of multiple VLANs that carries both tagged and untagged traffic is a VLAN trunk port (ports A9-A10 in this example). Here we define VLANs 300-304 and assign ports to them.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)#    name "VLAN300"
HP5406ZL(vlan-300)#    untagged A1,A9-A10
HP5406ZL(vlan-300)#    ip address 10.1.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
```

```
HP5406ZL(config)# vlan 301
HP5406ZL(vlan-301)#    name "VLAN301"
HP5406ZL(vlan-301)#    untagged A2
HP5406ZL(vlan-301)#    ip address 10.2.2.1 255.255.0.0
HP5406ZL(vlan-301)#    tagged A9-A10
HP5406ZL(vlan-301)#    exit
HP5406ZL(config)# vlan 302
HP5406ZL(vlan-302)#    name "VLAN302"
HP5406ZL(vlan-302)#    untagged A3
HP5406ZL(vlan-302)#    ip address 10.3.2.1 255.255.0.0
HP5406ZL(vlan-302)#    tagged A9-A10
HP5406ZL(vlan-302)#    exit
HP5406ZL(config)# vlan 303
HP5406ZL(vlan-303)#    name "VLAN303"
HP5406ZL(vlan-303)#    untagged A4
HP5406ZL(vlan-303)#    ip address 10.4.2.1 255.255.0.0
HP5406ZL(vlan-303)#    tagged A9-A10
HP5406ZL(vlan-303)#    exit
HP5406ZL(config)# vlan 304
HP5406ZL(vlan-304)#    name "VLAN304"
HP5406ZL(vlan-304)#    untagged A5
HP5406ZL(vlan-304)#    ip address 10.5.2.1 255.255.0.0
HP5406ZL(vlan-304)#    exit
HP5406ZL(config)#    exit
```

Cisco commands

The following commands apply to a Cisco Catalyst 6509. The syntax is similar for the Catalyst 3750-E switches and Cisco Catalyst 4506 switches.

First, define VLANs 300 to 304.

```
Cat6509# configure terminal
Cat6509(config)# vlan 300-304
```

Then, define a VLAN trunk port that allows tagged traffic from VLANs 301-303, and native untagged traffic on 300.

```
Cat6509(config)# interface GigabitEthernet4/9
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport trunk encapsulation dot1q
Cat6509(config-if)#  switchport trunk native vlan 300
Cat6509(config-if)#  switchport trunk allowed vlan 300-303
Cat6509(config-if)#  switchport mode trunk
Cat6509(config-if)#  exit
```

Next, define access-mode interfaces allowing untagged traffic from VLANs 300-304.

```
Cat6509(config)# interface GigabitEthernet6/0/1
Cat6509(config-if)#  switchport access vlan 300
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)# interface GigabitEthernet6/0/2
```

```
Cat6509(config-if)#  switchport access vlan 301
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)# interface GigabitEthernet6/0/3
Cat6509(config-if)#  switchport access vlan 302
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)# interface GigabitEthernet6/0/4
Cat6509(config-if)#  switchport access vlan 303
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)# interface GigabitEthernet6/0/5
Cat6509(config-if)#  switchport access vlan 304
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  end
```

Validation

The Spirent TestCenter traffic generator/analyzer can be configured to offer traffic between pairs of access-mode interfaces on each switch. In all cases – involving unicast, multicast, or broadcast traffic – traffic will stay local to the VLAN in which it is defined. For example, traffic offered to VLAN 300 on the HP switches will be forwarded only to interfaces in VLAN 300 on the Cisco switches and vice-versa.

If desired, port mirroring can be enabled on either HP or Cisco switches to verify that the trunk ports carry tagged traffic VLAN IDs 301-303 and untagged traffic for VLAN ID 300. As a final verification that VLANs limit broadcast domains, Spirent TestCenter can be configured to offer traffic on access ports with VLAN 304. The trunk ports on all switches will not forward this traffic.

Jumbo frame switching

Objective

To validate the ability of HP Networking and Cisco Catalyst switches to correctly forward bidirectional traffic consisting of jumbo frames.

Background

For many years the IEEE Ethernet specification has defined the maximum length of an Ethernet frame to be 1,518 bytes (or 1,522 bytes with an 802.1Q VLAN tag). The use of jumbo frames – those larger than 1518 bytes – remains nonstandard. However, jumbo frames can improve the performance of applications involving bulk data transfer, such as backup and disaster recovery.

HP and Cisco switches both support 9,216-byte jumbo frames, including Ethernet CRC. This section explains how to configure both vendors' switches to exchange jumbo frames.

Topology

In this example, the Spirent TestCenter traffic generator offers 9,216-byte jumbo Ethernet frames using a "partially meshed" topology, meaning all traffic offered to ports on HP switches are destined to ports on Cisco switches and visa-versa. VLAN trunk ports connect the switches and VLAN access ports at the edge accept untagged jumbo frames. However, the ability to switch jumbo frames does not depend on VLAN tagging. This example would also work with all interfaces passing untagged traffic.

Figure 2 below illustrates the configuration used to validate jumbo frame switching. This test deviates from the standard test bed by the removal of the link aggregation trunks between the Cisco Catalyst 4506 and the Cisco Catalyst 3750-E as well as the link aggregation trunk between the Cisco Catalyst 4506 and the Cisco Catalyst 6509. There is also no connection between the Cisco Catalyst 4506 and the Cisco Catalyst 6509. As noted in the configuration sections below, all interfaces explicitly support switching of jumbo frames. Engineers configured all interswitch trunks to use VLAN trunking, in this case carrying traffic from VLAN 300.

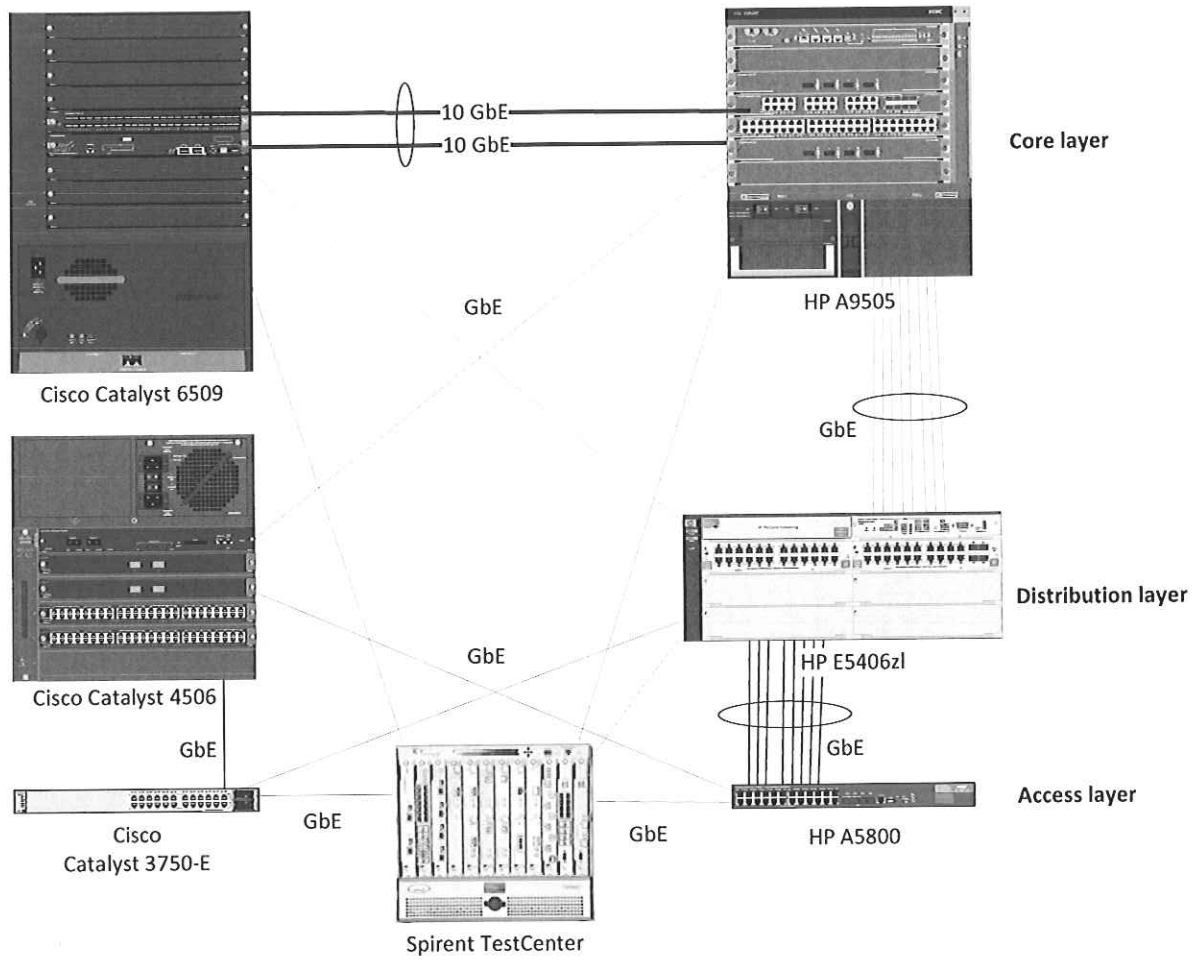


Figure 2: Jumbo frame switching test bed

HP A-series commands

HP A-series switches have jumbo frames enabled by default. The following commands are used to explicitly set the maximum transmission unit (MTU). The MTU is set in the interface configuration context.

```
<HP5800> system-view
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1] port link-mode bridge
[HP5800-Gigabitethernet1/0/1] jumboframe enable 9216
[HP5800-Gigabitethernet1/0/1] quit
[HP5800] quit
```

HP E-series commands

HP E-series switches set the MTU on a per-VLAN basis. When enabled, all ports on that VLAN will forward jumbo frames.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)#     name "VLAN306"
HP5406ZL(vlan-300)#     untagged A1-A5,A9-A10,Trk1-Trk2
HP5406ZL(vlan-300)#     ip address 10.1.2.1 255.255.0.0
HP5406ZL(vlan-300)#     jumbo
HP5406ZL(vlan-300)#       exit
HP5406ZL(config)#       exit
```

Cisco commands

On Cisco Catalyst 6509 and Cisco Catalyst 4506 switches, jumbo frame support varies by line card. For line cards that support jumbo frames, MTU is set on a per-interface basis.

```
Cat6509# configure terminal
Cat6509(config)# interface GigabitEthernet4/48
Cat6509(config-if)# switchport
Cat6509(config-if)# switchport access vlan 300
Cat6509(config-if)# switchport mode access
Cat6509(config-if)# mtu 9216
Cat6509(config-if)# end
```

On Cisco Catalyst 3750-E switches, MTU is set systemwide:

```
Cat3750E# configure terminal
Cat3750E(config)# system mtu jumbo 9216
Cat3750E(config)# end
```

Validation

Generating jumbo frames between the attached clients and servers will validate the ability of the switches to exchange jumbo traffic. All switches will forward all jumbo frames with zero frame loss.

Jumbo frame routing

Objective

To validate the ability of HP Networking and Cisco Catalyst switches to correctly route bidirectional traffic consisting of jumbo frames.

Background

Some routing protocols, such as open shortest path first (OSPF), require that both routers use the same MTU before exchanging routing information. For Ethernet interfaces, the requirement for matched MTUs applies equally to jumbo frames (those larger than 1518 bytes) as to standard-length frames.

HP Networking and Cisco Catalyst switches both support 9,216-byte jumbo frames, including Ethernet CRC. This section explains how to configure both vendors' devices to set up on an OSPF routing session using jumbo frames.

Topology

In this example, the HP A9505, HP E5406zl, and HP A5800 switches are configured as OSPF routers exchanging jumbo frames with Cisco Catalyst 6509, Cisco Catalyst 4506, and Cisco Catalyst 3750-E switches.

Figure 3 below illustrates the configuration used to validate jumbo frame routing. This test deviates from the standard test bed by the removal of the link aggregation trunks between the Cisco Catalyst 4506 and the Cisco Catalyst 3750-E, and between the Cisco Catalyst 4506 and the Cisco Catalyst 6509. There is also no connection between the Cisco Catalyst 4506 and the Cisco Catalyst 6509. In addition, all devices routed traffic at layer 3 in this test. In this example, OSPF routing sessions are established between all connected devices.

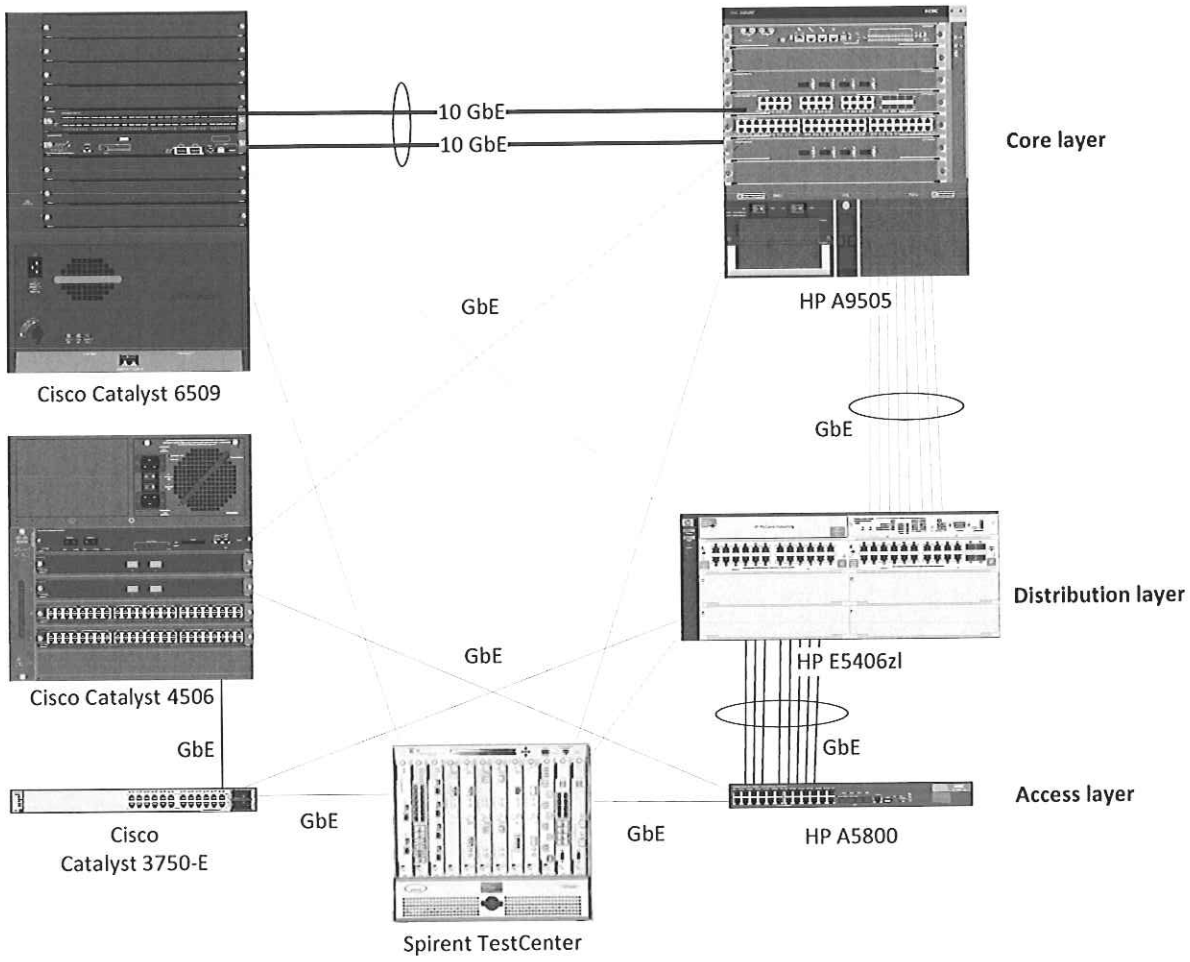


Figure 3: Jumbo frame routing test bed

HP A-series commands

HP A-series switches have jumbo frames enabled by default. The following commands are used to set the jumbo frame MTU. The frame size is set in the interface configuration context.

```
<HP5800> system-view
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1] port link-mode bridge
[HP5800-Gigabitethernet1/0/1] jumboframe enable 9216
[HP5800-Gigabitethernet1/0/1] quit
[HP5800] quit
```

Then OSPF is configured. In this example, the interface is a member of OSPF area 0.

```
[HP5800] ospf 1 router-id 10.0.0.1
[HP5800-OSPF] area 0.0.0.0
[HP5800-OSPF] network 10.0.0.0 0.0.255.255
[HP5800-OSPF] quit
```

HP E-series commands

HP E-series switches set MTU on a per-VLAN basis. When enabled, all ports on that VLAN will forward jumbo frames.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)#     name "VLAN306"
HP5406ZL(vlan-300)#     untagged A1-A5,A9-A10,Trk1-Trk2
HP5406ZL(vlan-300)#     ip address 10.1.2.1 255.255.0.0
HP5406ZL(vlan-300)#     jumbo
HP5406ZL(vlan-300)#       exit
```

Then set up OSPF routing. In our configuration, the VLAN interfaces were used as the routable interfaces. The **area backbone** command designates OSPF area 0.

```
HP5406(config)# ip routing
HP5406(config)# ip router-id 10.0.32.1
HP5406(config)# router ospf
HP5406(ospf)#    area backbone range 10.0.0.0 255.255.0.0 type summary
HP5406(ospf)#    exit
HP5406(config)# vlan 33
HP5406(vlan-33)#    ip ospf 10.0.33.1 area backbone
HP5406(vlan-33)#    exit
HP5406(config)# vlan 34
HP5406(vlan-34)#    ip ospf 10.0.34.1 area backbone
HP5406(vlan-34)#    exit
HP5406(config)# vlan 35
HP5406(vlan-35)#    ip ospf 10.0.35.1 area backbone
HP5406(vlan-35)#    exit
HP5406(config)# vlan 36
HP5406(vlan-36)#    ip ospf 10.0.36.1 area backbone
HP5406(vlan-36)#    exit
HP5406(config)# vlan 37
HP5406(vlan-37)#    ip ospf 10.0.37.1 area backbone
HP5406(vlan-37)#
HP5406(config)# vlan 38
HP5406(vlan-38)#    ip ospf 10.0.38.1 area backbone
HP5406(vlan-38)#    exit
HP5406(config)# vlan 39
HP5406(vlan-39)#    ip ospf 10.0.39.1 area backbone
HP5406(vlan-39)#    exit
HP5406(config)# vlan 40
HP5406(vlan-40)#    ip ospf 10.0.40.1 area backbone
HP5406(vlan-40)#    exit
HP5406(config)#   exit
```

Cisco commands

On Cisco Catalyst 6509 and Cisco Catalyst 4506 switches, jumbo frame support varies by line card. For those line cards that support jumbo frames, MTU is set on a per-interface basis. Cisco

IOS has separate commands for **mtu**, describing the maximum transmission unit for the *Ethernet* frame and for the **ip mtu**, describing the MTU for the *IP packet*.

Configure the interface with a jumbo frame size.

```
Cat6509# configure terminal
Cat6509(config)# interface GigabitEthernet4/9
Cat6509(config-if)# ip address 10.0.42.2 255.255.255.0
Cat6509(config-if)# ip mtu 9198
Cat6509(config-if)# exit
```

Then set up OSPF.

```
Cat6509(config)# router ospf 1
Cat6509(config-router)#  log-adjacency-changes
Cat6509(config-router)#  network 10.0.0.0 0.0.255.255 area 0
Cat6509(config-router)#  exit
```

Then set up the VLAN for jumbo frames. This is required to route jumbo frames between VLANs. All interfaces in the VLAN must be set to allow jumbo frames before this command will take effect.

```
Cat6509(config)# interface Vlan193
Cat6509(config-if)# mtu 9216
Cat6509(config-if)#  end
```

On Cisco Catalyst 3750-E switches, MTU is set systemwide:

```
Cat3750E# configure terminal
Cat3750E(config)# system mtu jumbo 9216
Cat3750E(config)# system mtu routing 9198
Cat3750E(config)# router ospf 1
Cat3750E(config-router)#  log-adjacency-changes
Cat3750E(config-router)#  network 10.0.43.2 0.0.0.0 area 0
Cat3750E(config-router)#  network 10.0.75.2 0.0.0.0 area 0
Cat3750E(config-router)#  network 10.0.128.0 0.0.127.255 area 0
Cat3750E(config-router)#  network 192.168.1.0 0.0.0.255 area 0
Cat3750E(config-router)#  network 192.168.2.0 0.0.0.255 area 0
Cat3750E(config-router)#  end
```

Validation

Unless both HP and Cisco interfaces agree on MTU size, OSPF routing adjacencies will remain in ExStart state, and will never transition to OSPF "full" state. To verify that an OSPF adjacency has entered OSPF "full" state on the HP A-series switches, use the **display ospf peer** command. To verify that an OSPF adjacency has entered OSPF "full" state on HP E-series and Cisco switches, use the **show ip ospf neighbor** command.

The fact that both routers are in Full state indicates they have agreed to exchange IP packets up to 9,198 bytes long (or 9,216 bytes, including Ethernet header and CRC). OSPF routing session establishment will not work unless both sides agree on MTU size.

Link aggregation

Objective

To validate the ability of HP Networking and Cisco Catalyst switches to correctly forward traffic over a logical connection created using IEEE 802.3ad link aggregation.

Background

The IEEE 802.3ad link specification defines a standards-based method for aggregating multiple physical Ethernet links into a single logical link. The logical link, known as a link aggregation group (LAG), is comprised of multiple *members* (pairs of physical interfaces on each switch). LAGs may be defined statically or dynamically, the latter using the link aggregation control protocol (LACP). With LACP enabled, 802.3ad-compliant switches can dynamically add or remove up to eight LAG members.

Link aggregation is useful both for increasing bandwidth beyond the limits of single physical interfaces and, especially when used with LACP, for adding redundancy to network connections.

Topology

In this example, an HP A9505 switch uses two-member LAGs to exchange traffic with a Cisco Catalyst 6509 switch and a Cisco Catalyst 4506 switch. An HP E5406zl switch uses two-member LAGs to exchange traffic with a Cisco Catalyst 6509 switch and a Cisco Catalyst 3750-E switch. An HP A5800 switch uses two-member LAGs to exchange traffic with a Cisco Catalyst 4506 switch.

Figure 4 below shows the topology used to validate link aggregation and LACP functionality. This test deviates from the standard test bed with the additional of several link aggregation groups between the HP E5406zl and the Cisco Catalyst 3750-E, between the HP 5406zl and the Cisco Catalyst 6509, between the HP A9505 and the Cisco Catalyst 4506, and between the HP 5800 and the Cisco C5406. Other connections have been removed between the HP 5406zl and the HP 5800, between the HP 5406zl and HP 9505, between the Cisco Catalyst 3750-E and the Cisco Catalyst 4506, and between the Cisco Catalyst 4506 and the Cisco Catalyst 6509.

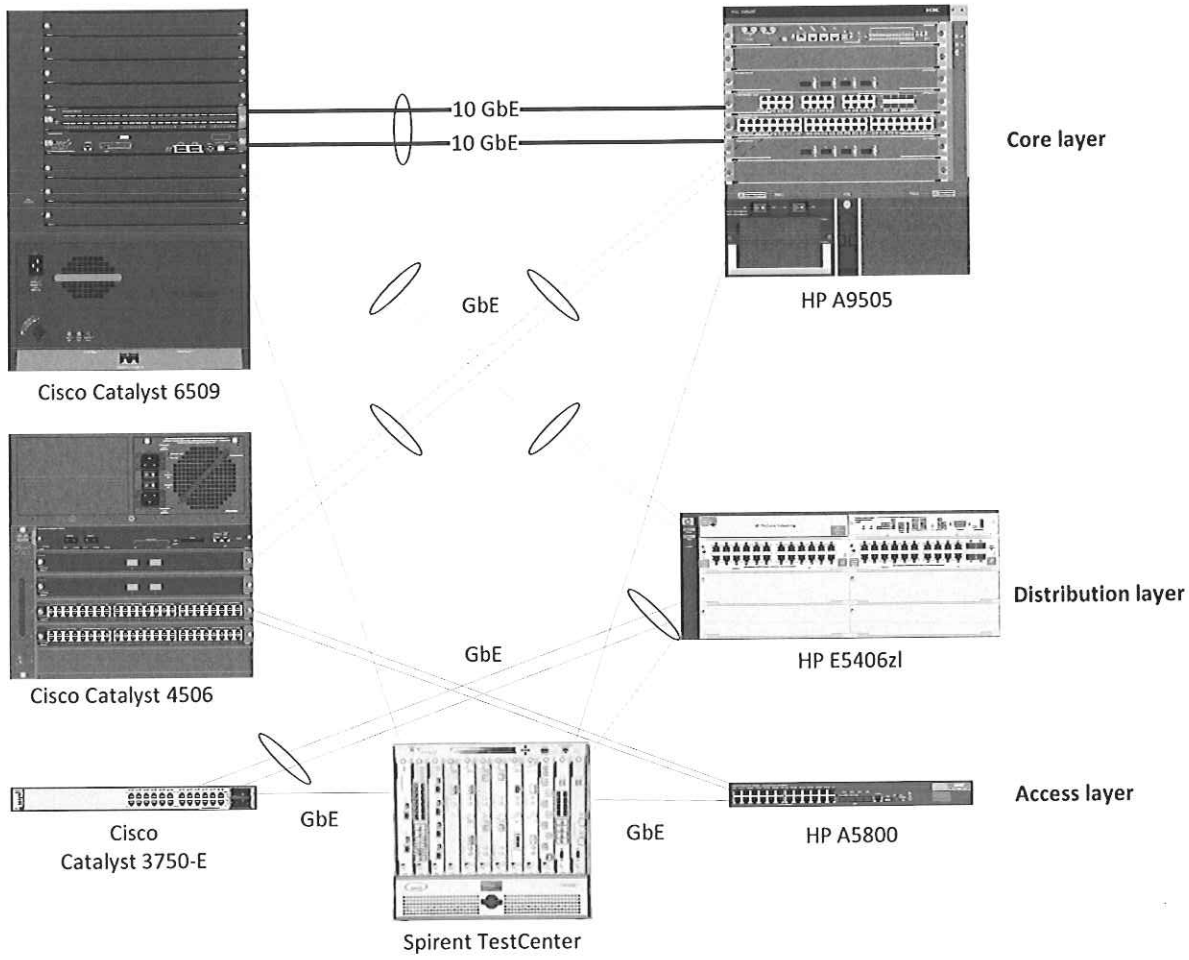


Figure 4: Link aggregation test bed

HP A-series commands

On these HP switches, link aggregation is a two-step process. First a virtual *bridge aggregation* interface is created. Then physical interfaces are associated with the virtual bridge interface. While this example involves a VLAN trunk, a common use of link aggregation, it is not a requirement.

Create the bridge aggregation interface.

```
<HP5800> system-view
[HP5800] interface Bridge-Aggregation31
[HP5800-bridge-aggregation31]  description linkagg_to_4506
[HP5800-bridge-aggregation31]  port link-type trunk
[HP5800-bridge-aggregation31]  undo port trunk permit vlan 1
[HP5800-bridge-aggregation31]  port trunk permit vlan 300 to 303
[HP5800-bridge-aggregation31]  port trunk pvid vlan 300
```

```
[HP5800-bridge-aggregation31]  link-aggregation mode dynamic
[HP5800-bridge-aggregation31]
          link-aggregation load-sharing mode destination-mac source-mac
[HP5800-bridge-aggregation31] quit
```

Then assign physical interfaces to the bridge aggregation virtual interface.

```
[HP5800] interface GigabitEthernet1/0/17
[HP5800-gigabitethernet1/0/17]  port link-mode bridge
[HP5800-gigabitethernet1/0/17]  port link-type trunk
[HP5800-gigabitethernet1/0/17]  undo port trunk permit vlan 1
[HP5800-gigabitethernet1/0/17]  port trunk permit vlan 300 to 303
[HP5800-gigabitethernet1/0/17]  port trunk pvid vlan 300
[HP5800-gigabitethernet1/0/17]  port link-aggregation group 31
[HP5800-gigabitethernet1/0/17] interface GigabitEthernet1/0/18
[HP5800-gigabitethernet1/0/18]  port link-mode bridge
[HP5800-gigabitethernet1/0/18]  port link-type trunk
[HP5800-gigabitethernet1/0/18]  undo port trunk permit vlan 1
[HP5800-gigabitethernet1/0/18]  port trunk permit vlan 300 to 303
[HP5800-gigabitethernet1/0/18]  port trunk pvid vlan 300
[HP5800-gigabitethernet1/0/18]  port link-aggregation group 31
[HP5800-gigabitethernet1/0/18]  quit
[HP5800]  quit
```

HP E-series commands

HP E-series switches create *trunks* to support LACP. A single command creates the trunk and assigns physical members to the trunk.

```
HP5406ZL# configure
HP5406ZL(config)# trunk A9,A12 Trk31 LACP
HP5406ZL(config)# exit
```

Cisco commands

Cisco Catalyst switches, like HP A-series switches, perform a two-step process to create a *Port Channel*. The following commands apply to a Cisco Catalyst 6509. The syntax is similar for the Catalyst 3750-E switches and Cisco Catalyst 4506 switches.

First, create the link aggregation group. Here we also create a VLAN trunk.

```
Cat6509# configure terminal
Cat6509(config)# interface Port-channel1
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport trunk encapsulation dot1q
Cat6509(config-if)#  switchport trunk native vlan 300
Cat6509(config-if)#  switchport trunk allowed vlan 300-303
Cat6509(config-if)#  switchport mode trunk
```

```
Cat6509(config-if)#  exit
```

Next, add interfaces to the link aggregation group. The command **channel-group 1** adds an interface to the link aggregation group created in the previous step, while **mode active** enables LACP.

```
Cat6509(config-)# interface GigabitEthernet4/1
Cat6509(config-if)# no ip address
Cat6509(config-if)# switchport
Cat6509(config-if)# switchport trunk encapsulation dot1q
Cat6509(config-if)# switchport trunk native vlan 300
Cat6509(config-if)# switchport trunk allowed vlan 300-303
Cat6509(config-if)# switchport mode trunk
Cat6509(config-if)#`channel-group 1 mode active
Cat6509(config)# interface GigabitEthernet4/3
Cat6509(config-if)# no ip address
Cat6509(config-if)# switchport
Cat6509(config-if)# switchport trunk encapsulation dot1q
Cat6509(config-if)# switchport trunk native vlan 300
Cat6509(config-if)# switchport trunk allowed vlan 300-303
Cat6509(config-if)# switchport mode trunk
Cat6509(config-if)# channel-group 1 mode active
Cat6509(config-if)# end
```

Validation

The command **display link-aggregation summary** on HP A-series switches will show the status of the bridge aggregation interfaces. On HP E-series switches, the **show lacp** command will verify correct operation.

The correct operation of a LAG can with two or more members also can be verified by offering traffic at a rate higher than any single LAG member can carry. If the switch forwards all traffic across the LAG without loss, the LAG is operating properly.

Spanning tree case 1: RSTP/Rapid-PVST+

Objective

To verify interoperability of a rapid spanning tree topology between HP Networking and Cisco Catalyst switches using RSTP and Rapid-PVST+.

To measure convergence time of a rapid spanning tree topology between HP and Cisco after a link failure.

Background

The spanning tree protocol is widely used in campus enterprise networks for loop prevention and redundancy. Rapid spanning tree, defined in IEEE 802.1w, provides much faster convergence time after a link or device failure than the original 802.1D spanning tree specification

Topology

This example uses redundant paths between HP Networking and Cisco Catalyst switches. The default spanning tree mode in Cisco Catalyst switches is that vendor's proprietary per-VLAN spanning tree plus (PVST+) mode, which is interoperable with other vendors' rapid spanning tree implementations.

Figure 1 above shows the RSTP validation test bed. All ports on all switches are access-mode members of the default VLAN. Rapid spanning is enabled on all the HP switches. Cisco's "Rapid-PVST+" is enabled on all the Cisco switches and is interoperable with standard rapid spanning tree. Traffic offered from the Spirent TestCenter generator/analysis verifies the spanning tree topology.

HP A-series commands

Assign all members to be access-mode members of the default VLAN. Here is the command for interface GigabitEthernet1/0/6; the same command would apply to all interfaces participating in the spanning tree topology.

```
<HP5800> system view
[HP5800] interface GigabitEthernet1/0/6
[HP5800-Gigabitethernet1/0/6] port link-mode bridge
[HP5800-Gigabitethernet1/0/6] quit
```

Then enable rapid spanning tree on the HP A-series switches.

```
<HP5800> system-view
[HP5800] stp mode rstp
[HP5800] stp enable
[HP5800] quit
```

HP E-series commands

On HP E-series switches, by default all members are access-mode members of the default VLAN and therefore no per-interface command needs to be done.

Enable rapid spanning tree on the HP E-series switches.

```
HP5406ZL# configure
HP5406ZL(config)# spanning-tree
HP5406ZL(config)# spanning-tree priority 9 force-version rstp-operation
HP5406ZL(config)# exit
```

Cisco commands

First, assign all members to be access-mode members of the default VLAN. The following commands apply to a Cisco Catalyst 6509. The syntax is similar for Cisco Catalyst 3750-E and Cisco Catalyst 4506 switches.

Here is the command for interface GigabitEthernet6/0/3; the same command would apply to all interfaces participating in the spanning tree topology.

```
Cat6509# configure terminal
Cat6509(config)# interface GigabitEthernet6/0/3
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  exit
```

Then enable rapid-pvst mode on the Cisco switches.

```
Cat6509(config)# spanning-tree mode rapid-pvst
Cat6509(config)# end
```

Validation

HP A-series switches can use the command **`display stp brief`** to verify the state of rapid spanning tree.

```
<A9505>display stp br
 MSTID      Port                        Role  STP State     Protection
   0        Bridge-Aggregation10        ROOT  FORWARDING    NONE
   0        Bridge-Aggregation20        DESI  FORWARDING    NONE
   0        GigabitEthernet3/0/11       ALTE  DISCARDING    NONE
   0        GigabitEthernet3/0/16       DESI  FORWARDING    NONE
```

HP E-series switches uses the command **show spanning-tree** to display spanning-tree state.

```
E5406zl# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled    : Yes
  Force Version : RSTP-operation
...

                    |            Prio                | Designated     Hello
  Port    Type      | Cost       rity State          | Bridge         Time PtP Edge
  ------ ---------- + ---------- ---- ---------- + ------------- ---- --- ----
  A1      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A2      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A3      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A4      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A5      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A6      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A7      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A8      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A9      100/1000T | 20000      128  Blocking   | 001de6-eb7001 2    Yes No
  A10     100/1000T | 20000      128  Blocking   | 002155-740000 2    Yes No
...

  E2      10GbE-CX4 | 2000       128  Forwarding | 001560-f56200 2    Yes Yes
  F1      10GbE-CX4 | 2000       128  Forwarding | 001560-f56200 2    Yes Yes
  F2      10GbE-CX4 | 2000       128  Forwarding | 001560-f56200 2    Yes Yes
  Trk1              | 20000      64   Blocking   | 002389-11d000 2    Yes No
  Trk2              | 20000      64   Forwarding | 000fe2-f3e292 2    Yes No
```

To verify all switches send traffic only over the spanning tree interfaces in forwarding state, generate a known quantity of frames from Spirent TestCenter or other source and compare switch interface packet counters with those sent and received on each interface. Interfaces in blocking state will receive spanning tree BPDU frames but should transmit no frames.

To determine convergence time, disable one of the spanning tree interfaces in forwarding state while offering a known quantity of frames from Spirent TestCenter or other traffic generator. Convergence time can be derived from frame loss. For example, if Spirent TestCenter generates traffic at a rate of 1,000 frames per second, each dropped frame is equivalent to 1 millisecond of convergence time. If the switches drop 47 frames, then rapid spanning tree convergence time is 47 ms.

Spanning tree case 2: MSTP/PVST+

Objective

To verify interoperability of multiple spanning tree protocol (MSTP) and per-vlan spanning tree protocol plus (PVST+) between HP Networking and Cisco Catalyst switches, respectively.

To measure convergence time of an MSTP-PVST+ topology between HP Networking and Cisco Catalyst switches after a link failure.

Background

As defined in IEEE specification 802.1s, the multiple spanning tree protocol (MSTP) adds loop prevention and redundancy on a per-VLAN basis. With MSTP, individual spanning tree topologies can be configured for each VLAN.

The goal of this exercise is to demonstrate interoperability in a multiple-VLAN environment when the HP Networking and Cisco Catalyst switches use different variations of spanning tree: MSTP on HP and PVST+ on a Cisco Catalyst switch.

Topology

This example uses redundant paths between the HP Networking and Cisco Catalyst switches. VLAN Ids of 300 to 304 have been defined on all switches. MSTP is enabled on all the HP switches, and Rapid PVST+ is enabled on all the Cisco switches.

Figure 1 above illustrates the MSTP-PVST+ validation test bed. The links interconnecting each switch are trunk ports that allow tagged traffic from VLAN IDs 300 to 304. Access ports were configured on the access layer switches, with one port assigned to each VLAN. Traffic offered from the Spirent TestCenter traffic generator/analyzer verifies the spanning tree topology in each VLAN.

HP A-series commands

Create VLAN IDs 300 to 304.

```
<HP5800> system-view
[HP5800] vlan 300 to 304
```

Configure access-mode ports for their respective VLANs.

```
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1]  port link-mode bridge
[HP5800-Gigabitethernet1/0/1]  port access vlan 300
[HP5800-Gigabitethernet1/0/1] interface GigabitEthernet1/0/2
[HP5800-Gigabitethernet1/0/2]  port link-mode bridge
[HP5800-Gigabitethernet1/0/2]  port access vlan 301
[HP5800-Gigabitethernet1/0/2] interface GigabitEthernet1/0/3
[HP5800-Gigabitethernet1/0/3]  port link-mode bridge
[HP5800-Gigabitethernet1/0/3]  port access vlan 302
[HP5800-Gigabitethernet1/0/3] interface GigabitEthernet1/0/4
[HP5800-Gigabitethernet1/0/4]  port link-mode bridge
[HP5800-Gigabitethernet1/0/4]  port access vlan 303
[HP5800-Gigabitethernet1/0/4] interface GigabitEthernet1/0/5
[HP5800-Gigabitethernet1/0/5]  port link-mode bridge
[HP5800-Gigabitethernet1/0/5]  port access vlan 304
```

Configure interswitch connections as trunk ports. Here is interface GigabitEthernet1/0/23 as an example.

```
[HP5800] interface GigabitEthernet1/0/23
[HP5800-Gigabitethernet1/0/23]  port link-mode bridge
[HP5800-Gigabitethernet1/0/23]  port link-type trunk
[HP5800-Gigabitethernet1/0/23]  undo port trunk permit vlan 1
[HP5800-Gigabitethernet1/0/23]  port trunk permit vlan 300 to 303
[HP5800-Gigabitethernet1/0/23]  port trunk pvid vlan 300
[HP5800-Gigabitethernet1/0/23]  quit
```

Enable multiple spanning tree. This requires enabling MSTP (the default on HP A-series switches) and configuring one multiple spanning tree instance per VLAN.

```
[HP5800] stp enable
[HP5800] stp region-configuration
[HP5800-mst-region]  instance 2 vlan 300
[HP5800-mst-region]  instance 3 vlan 301
[HP5800-mst-region]  instance 4 vlan 302
[HP5800-mst-region]  instance 5 vlan 303
[HP5800-mst-region]  instance 6 vlan 304
[HP5800-mst-region]  active region-configuration
[HP5800-mst-region]  quit
[HP5800]  quit
```

HP E-series commands

Create the VLANs and assign physical interfaces to them. Interfaces that have both untagged (access ports) and tagged VLAN IDs are VLAN trunks.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)#    name "VLAN300"
HP5406ZL(vlan-300)#    untagged A1,A9-A10
HP5406ZL(vlan-300)#    ip address 10.1.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
```

```
HP5406ZL(config)# vlan 301
HP5406ZL(vlan-300)#    name "VLAN301"
HP5406ZL(vlan-300)#    untagged A2
HP5406ZL(vlan-300)#    ip address 10.2.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(config)#    exit
HP5406ZL(vlan-300)# vlan 302
HP5406ZL(vlan-300)#    name "VLAN302"
HP5406ZL(vlan-300)#    untagged A3
HP5406ZL(vlan-300)#    ip address 10.3.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 303
HP5406ZL(vlan-300)#    name "VLAN303"
HP5406ZL(vlan-300)#    untagged A4
HP5406ZL(vlan-300)#    ip address 10.4.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 304
HP5406ZL(vlan-300)#    name "VLAN304"
HP5406ZL(vlan-300)#    untagged A5
HP5406ZL(vlan-300)#    ip address 10.5.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
```

Create the MSTP instances, and assign one VLAN to each instance.

```
HP5406ZL(config)# spanning-tree
HP5406ZL(config)# spanning-tree instance 2 vlan 300
HP5406ZL(config)# spanning-tree instance 3 vlan 301
HP5406ZL(config)# spanning-tree instance 4 vlan 302
HP5406ZL(config)# spanning-tree instance 5 vlan 303
HP5406ZL(config)# spanning-tree instance 6 vlan 304
HP5406ZL(config)# spanning-tree priority 9
HP5406ZL(config)# exit
```

Cisco commands

The following commands apply to a Cisco Catalyst 3750-E switch. The syntax is similar for the Cisco Catalyst 6509 and Cisco Catalyst 4506 switches.

Create the VLANs.

```
Cat3750E# configure terminal
Cat3750E(config)# vlan 300-304
```

Configure access-mode ports for their respective VLANs.

```
Cat3750E(config)# interface GigabitEthernet6/0/1
Cat3750E(config)#  switchport
Cat3750E(config-if)#  switchport access vlan 300
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
```

```
Cat3750E(config-if)# interface GigabitEthernet6/0/2
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 301
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/3
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 302
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/4
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 303
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/5
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 304
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)#  exit
```

Configure interswitch connections as trunk ports. Here is interface GigabitEthernet6/0/10 as an example.

```
Cat3750E(config)# interface GigabitEthernet6/0/10
Cat3750E(config-if)#  switchport trunk encapsulation dot1q
Cat3750E(config-if)#  switchport trunk native vlan 300
Cat3750E(config-if)#  switchport trunk allowed vlan 300-303
Cat3750E(config-if)#  switchport mode trunk
Cat3750E(config-if)#  exit
```

Enable PVST+. On a new switch, PVST+ already is enabled by default.

```
Cat3750E(config)# spanning-tree mode pvst
Cat3750E(config)# end
```

Validation

HP A-series switches can use the command **`display stp brief`** to verify the state of spanning tree on HP A-series switches.

```
<A9505>display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        Bridge-Aggregation10        DESI  FORWARDING    NONE
   0        Bridge-Aggregation20        ROOT  FORWARDING    NONE
   0        GigabitEthernet3/0/11       DESI  FORWARDING    NONE
   0        GigabitEthernet3/0/16       DESI  FORWARDING    NONE
   2        Bridge-Aggregation10        DESI  FORWARDING    NONE
   2        Bridge-Aggregation20        MAST  FORWARDING    NONE
   2        GigabitEthernet3/0/11       DESI  FORWARDING    NONE
   3        Bridge-Aggregation10        DESI  FORWARDING    NONE
```

```
  3        Bridge-Aggregation20          MAST  FORWARDING     NONE
  3        GigabitEthernet3/0/11         DESI  FORWARDING     NONE
  4        Bridge-Aggregation10          DESI  FORWARDING     NONE
  4        Bridge-Aggregation20          MAST  FORWARDING     NONE
  4        GigabitEthernet3/0/11         DESI  FORWARDING     NONE
  5        Bridge-Aggregation10          DESI  FORWARDING     NONE
  5        Bridge-Aggregation20          MAST  FORWARDING     NONE
  5        GigabitEthernet3/0/11         DESI  FORWARDING     NONE
```

HP E-Series uses the command **show spanning-tree** to display the state of spanning tree on HP E-Series switches.

```
E5406zl# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled    : Yes
  Force Version : MSTP-operation
…

                    |            Prio                | Designated     Hello
  Port    Type      | Cost       rity State          | Bridge         Time PtP Edge
  ------ --------- + --------- ---- ---------- + ------------- ---- --- ----
  A1      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A2      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A3      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A4      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A5      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A6      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A7      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A8      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A9      100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
  A10     100/1000T | 20000      128  Forwarding | 001560-f56200 2    Yes Yes
…
  E2      10GbE-CX4 | 2000       128  Forwarding | 001560-f56200 2    Yes Yes
  F1      10GbE-CX4 | 2000       128  Forwarding | 001560-f56200 2    Yes Yes
  F2      10GbE-CX4 | 2000       128  Forwarding | 001560-f56200 2    Yes Yes
  Trk1              | 20000      64   Forwarding | 001560-f56200 2    Yes No
  Trk2              | 20000      64   Forwarding | 000fe2-f3e292 2    Yes No
```

To verify all switches send traffic only over the spanning tree interfaces in forwarding state, generate a known quantity of frames from Spirent TestCenter or other source to each VLAN and compare switch interface packet counters with those sent and received on each interface. Interfaces in blocking state will receive spanning tree BPDU frames but should transmit no frames.

To determine convergence time, disable one of the spanning tree interfaces in forwarding state while offering a known quantity of frames from Spirent TestCenter or other traffic generator. Convergence time can be derived from frame loss. For example, if Spirent TestCenter generates

traffic at a rate of 1,000 frames per second, each dropped frame is equivalent to 1 millisecond of convergence time. If the switches drop 47 frames, then spanning tree convergence time is 47 ms.

Spanning tree case 3: MSTP/Rapid-PVST+

Objective

To verify interoperability of multiple spanning tree protocol (MSTP) and rapid per-VLAN spanning tree protocol plus (Rapid PVST+) between HP Networking and Cisco Catalyst switches, respectively.

To measure convergence time of an MSTP-Rapid PVST+ topology between HP Networking and Cisco Catalyst switches after a link failure.

Background

As defined in IEEE specification 802.1s, the multiple spanning tree protocol (MSTP) adds loop prevention and redundancy on a per-VLAN basis. With MSTP, individual spanning tree topologies can be configured for each VLAN.

The goal of this exercise is to demonstrate interoperability in a multiple-VLAN environment when the HP Networking and Cisco Catalyst switches use different variations of spanning tree: MSTP on HP switches and Rapid PVST+ on Cisco Catalyst switches.

Topology

This example uses redundant paths between the HP Networking and Cisco Catalyst switches. VLAN Ids of 300 to 304 have been defined on all switches. MSTP is enabled on all HP switches, with Rapid PVST+ defined on all Cisco switches.

Figure 1 above illustrates the MSTP-Rapid PVST+ validation test bed. The links interconnecting each switch are trunk ports that allow tagged traffic from the VLAN IDs 300 to 304. Access ports were configured on the access layer switches, with one port per vlan being configured. Traffic offered from the Spirent TestCenter traffic generator/analyzer verifies the spanning tree topology in each VLAN.

HP A-series commands

Create VLAN IDs 300 to 304.

```
<HP5800> system-view
[HP5800] vlan 300 to 304
```

Configure access-mode ports for their respective VLANs.

```
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1]  port link-mode bridge
[HP5800-Gigabitethernet1/0/1]  port access vlan 300
[HP5800-Gigabitethernet1/0/1] interface GigabitEthernet1/0/2
[HP5800-Gigabitethernet1/0/2]  port link-mode bridge
[HP5800-Gigabitethernet1/0/2]  port access vlan 301
[HP5800-Gigabitethernet1/0/2] interface GigabitEthernet1/0/3
[HP5800-Gigabitethernet1/0/3]  port link-mode bridge
[HP5800-Gigabitethernet1/0/3]  port access vlan 302
[HP5800-Gigabitethernet1/0/3] interface GigabitEthernet1/0/4
[HP5800-Gigabitethernet1/0/4]  port link-mode bridge
[HP5800-Gigabitethernet1/0/4]  port access vlan 303
[HP5800-Gigabitethernet1/0/4] interface GigabitEthernet1/0/5
[HP5800-Gigabitethernet1/0/5]  port link-mode bridge
[HP5800-Gigabitethernet1/0/5]  port access vlan 304
[HP5800-Gigabitethernet1/0/5]  quit
```

Configure interswitch connections as trunk ports. Here is interface GigabitEthernet1/0/23 as an example.

```
[HP5800] interface GigabitEthernet1/0/23
[HP5800-Gigabitethernet1/0/23]  port link-mode bridge
[HP5800-Gigabitethernet1/0/23]  port link-type trunk
[HP5800-Gigabitethernet1/0/23]  undo port trunk permit vlan 1
[HP5800-Gigabitethernet1/0/23]  port trunk permit vlan 300 to 303
[HP5800-Gigabitethernet1/0/23]  port trunk pvid vlan 300
[HP5800-Gigabitethernet1/0/23]  quit
```

Enable multiple spanning tree. This requires enable MSTP (the default on HP switches) and configuring one multiple spanning tree instance per VLAN.

```
[HP5800] stp enable
[HP5800] stp region-configuration
[HP5800-mst-region]  instance 2 vlan 300
[HP5800-mst-region]  instance 3 vlan 301
[HP5800-mst-region]  instance 4 vlan 302
[HP5800-mst-region]  instance 5 vlan 303
[HP5800-mst-region]  instance 6 vlan 304
[HP5800-mst-region]  active region-configuration
[HP5800-mst-region]  quit
[HP5800]  quit
```

HP E-series commands

Create the VLANs and assign physical interfaces to them. Interfaces that have both untagged (access ports) and tagged VLAN IDs are VLAN trunks.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)#    name "VLAN300"
HP5406ZL(vlan-300)#    untagged A1,A9-A10
HP5406ZL(vlan-300)#    ip address 10.1.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 301
HP5406ZL(vlan-300)#    name "VLAN301"
HP5406ZL(vlan-300)#    untagged A2
HP5406ZL(vlan-300)#    ip address 10.2.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(config)#    exit
HP5406ZL(vlan-300)# vlan 302
HP5406ZL(vlan-300)#    name "VLAN302"
HP5406ZL(vlan-300)#    untagged A3
HP5406ZL(vlan-300)#    ip address 10.3.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 303
HP5406ZL(vlan-300)#    name "VLAN303"
HP5406ZL(vlan-300)#    untagged A4
HP5406ZL(vlan-300)#    ip address 10.4.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 304
HP5406ZL(vlan-300)#    name "VLAN304"
HP5406ZL(vlan-300)#    untagged A5
HP5406ZL(vlan-300)#    ip address 10.5.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
```

Create the multiple spanning tree protocol instances, and assign one VLAN to each instance.

```
HP5406ZL(config)# spanning-tree
HP5406ZL(config)# spanning-tree instance 2 vlan 300
HP5406ZL(config)# spanning-tree instance 3 vlan 301
HP5406ZL(config)# spanning-tree instance 4 vlan 302
HP5406ZL(config)# spanning-tree instance 5 vlan 303
HP5406ZL(config)# spanning-tree instance 6 vlan 304
HP5406ZL(config)# spanning-tree priority 9tree instance 2 vlan 300
HP5406ZL(config)# spanning-tree instance 3 vlan 301
HP5406ZL(config)# spanning-tree instance 4 vlan 302
HP5406ZL(config)# spanning-tree instance 5 vlan 303
HP5406ZL(config)# spanning-tree instance 6 vlan 304
HP5406ZL(config)# spanning-tree priority 9
```

Cisco commands

The following commands apply to a Cisco Catalyst 3750-E switch. The syntax is similar for the Catalyst 6509 switches and Cisco Catalyst 4506 switches.

Create the VLANs.

```
Cat3750E# configure terminal
Cat3750E(config)# vlan 300-304
```

Configure access-mode ports for the respective VLANs.

```
Cat3750E(config)# interface GigabitEthernet6/0/1
Cat3750E(config)#  switchport
Cat3750E(config-if)#  switchport access vlan 300
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/2
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 301
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/3
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 302
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/4
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 303
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/5
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 304
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)#  exit
```

Configure interswitch connections as trunk ports. Here is interface GigabitEthernet6/0/10.

```
Cat3750E(config)# interface GigabitEthernet6/0/10
Cat3750E(config-if)#  switchport trunk encapsulation dot1q
Cat3750E(config-if)#  switchport trunk native vlan 300
Cat3750E(config-if)#  switchport trunk allowed vlan 300-303
Cat3750E(config-if)#  switchport mode trunk
Cat3750E(config-if)#  exit
```

Enable Rapid PVST+.

```
Cat3750E(config)# spanning-tree mode rapid-pvst
Cat3750E(config)# end
```

Validation

HP A-series switches can use the command **`display stp brief`** to verify the state of spanning tree on HP A-series switches. HP E-series uses the command **`show spanning-tree`** to display the state of spanning tree on HP E-series switches.

To verify switches send traffic only over the spanning tree interfaces in forwarding state, generate a known quantity of frames from Spirent TestCenter to each VLAN and compare switch interface packet counters with those sent and received on each interface. Interfaces in blocking state will receive spanning tree BPDU frames but should transmit no frames.

To determine convergence time, disable one of the spanning tree interfaces in forwarding state while offering a known quantity of frames from Spirent TestCenter or other traffic generator. Convergence time can be derived from frame loss. For example, if Spirent TestCenter generates traffic at a rate of 1,000 frames per second, each dropped frame is equivalent to 1 millisecond of convergence time. If the switches drop 47 frames, then spanning tree convergence time is 47 ms.

Spanning tree case 4: MSTP/MSTP

Objective

To verify interoperability of a multiple spanning tree topology between HP Networking and Cisco Catalyst switches.

To measure convergence time of a multiple spanning tree topology between HP and Cisco switches after a link failure.

Background

As defined in IEEE specification 802.1s, the multiple spanning tree protocol (MSTP) adds loop prevention and redundancy on a per-VLAN basis. With MSTP, a separate spanning tree topology can be configured for each VLAN.

MSTP is the default spanning tree protocol for HP Networking switches. MSTP is enabled by default on HP A-series switches, and disabled by default on HP E-series switches.

Topology

This example uses redundant paths between the HP Networking and Cisco Catalyst switches. VLAN IDs of 300 to 304 have been defined on all switches, and MSTP is enabled on all switches.

Figure 1 above illustrates the MSTP validation test bed. The links interconnecting each switch are trunk ports that allow tagged traffic from the VLAN IDs 300 to 304. Access ports were configured on the access layer switches, with one port per VLAN being configured. Traffic offered from the Spirent TestCenter traffic generator/analyzer verifies the spanning tree topology in each VLAN.

HP A-series commands

Create VLAN IDs 300 to 304.

```
<HP5800> system-view
[HP5800] vlan 300 to 304
```

Configure access-mode ports for their respective VLANs.

```
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1]  port link-mode bridge
[HP5800-Gigabitethernet1/0/1]  port access vlan 300
[HP5800-Gigabitethernet1/0/1] interface GigabitEthernet1/0/2
[HP5800-Gigabitethernet1/0/2]  port link-mode bridge
[HP5800-Gigabitethernet1/0/2]  port access vlan 301
[HP5800-Gigabitethernet1/0/2] interface GigabitEthernet1/0/3
[HP5800-Gigabitethernet1/0/3]  port link-mode bridge
[HP5800-Gigabitethernet1/0/3]  port access vlan 302
[HP5800-Gigabitethernet1/0/3] interface GigabitEthernet1/0/4
[HP5800-Gigabitethernet1/0/4]  port link-mode bridge
[HP5800-Gigabitethernet1/0/4]  port access vlan 303
[HP5800-Gigabitethernet1/0/4] interface GigabitEthernet1/0/5
[HP5800-Gigabitethernet1/0/5]  port link-mode bridge
[HP5800-Gigabitethernet1/0/5]  port access vlan 304
[HP5800-Gigabitethernet1/0/5]  quit
```

Configure interswitch connections as trunk ports. Here is interface GigabitEthernet1/0/23 as an example.

```
[HP5800] interface GigabitEthernet1/0/23
[HP5800-Gigabitethernet1/0/23]  port link-mode bridge
[HP5800-Gigabitethernet1/0/23]  port link-type trunk
[HP5800-Gigabitethernet1/0/23]  undo port trunk permit vlan 1
[HP5800-Gigabitethernet1/0/23]  port trunk permit vlan 300 to 303
[HP5800-Gigabitethernet1/0/23]  port trunk pvid vlan 300
[HP5800-Gigabitethernet1/0/23]  quit
```

Enable multiple spanning tree. This requires enabling MSTP (the default on HP A-series switches) and configuring one multiple spanning tree instance per VLAN.

```
[HP5800] stp enable
[HP5800] stp region-configuration
[HP5800-mst-region]  instance 2 vlan 300
[HP5800-mst-region]  instance 3 vlan 301
[HP5800-mst-region]  instance 4 vlan 302
[HP5800-mst-region]  instance 5 vlan 303
[HP5800-mst-region]  instance 6 vlan 304
[HP5800-mst-region]  active region-configuration
[HP5800-mst-region]  quit
[HP5800]  quit
```

HP E-series commands

Create the VLANs and assign physical interfaces to them. Interfaces that have both untagged (access ports) and tagged VLAN IDs are VLAN trunks.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)#    name "VLAN300"
HP5406ZL(vlan-300)#    untagged A1,A9-A10
HP5406ZL(vlan-300)#    ip address 10.1.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 301
HP5406ZL(vlan-300)#    name "VLAN301"
HP5406ZL(vlan-300)#    untagged A2
HP5406ZL(vlan-300)#    ip address 10.2.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(config)#    exit
HP5406ZL(vlan-300)# vlan 302
HP5406ZL(vlan-300)#    name "VLAN302"
HP5406ZL(vlan-300)#    untagged A3
HP5406ZL(vlan-300)#    ip address 10.3.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 303
HP5406ZL(vlan-300)#    name "VLAN303"
HP5406ZL(vlan-300)#    untagged A4
HP5406ZL(vlan-300)#    ip address 10.4.2.1 255.255.0.0
HP5406ZL(vlan-300)#    tagged A9-A10
HP5406ZL(vlan-300)#    exit
HP5406ZL(config)# vlan 304
HP5406ZL(vlan-300)#    name "VLAN304"
HP5406ZL(vlan-300)#    untagged A5
HP5406ZL(vlan-300)#    ip address 10.5.2.1 255.255.0.0
HP5406ZL(vlan-300)#    exit
```

Create the multiple spanning tree protocol instances, and assign one VLAN to each instance.

```
HP5406ZL(config)# spanning-tree
HP5406ZL(config)# spanning-tree instance 2 vlan 300
HP5406ZL(config)# spanning-tree instance 3 vlan 301
HP5406ZL(config)# spanning-tree instance 4 vlan 302
HP5406ZL(config)# spanning-tree instance 5 vlan 303
HP5406ZL(config)# spanning-tree instance 6 vlan 304
HP5406ZL(config)# spanning-tree priority 9
HP5406ZL(config)# exit
```

Cisco commands

The following commands apply to a Cisco Catalyst 3750-E. The syntax is similar for the Catalyst 6509 switches and Cisco Catalyst 4506 switches.

Create the VLANs.

```
Cat3750E# configure terminal
Cat3750E(config)# vlan 300-304
```

Configure access-mode ports for their respective VLANs.

```
Cat3750E(config)# interface GigabitEthernet6/0/1
Cat3750E(config)#  switchport
Cat3750E(config-if)#  switchport access vlan 300
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/2
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 301
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/3
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 302
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/4
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 303
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)# interface GigabitEthernet6/0/5
Cat3750E(config-if)#  switchport
Cat3750E(config-if)#  switchport access vlan 304
Cat3750E(config-if)#  switchport mode access
Cat3750E(config-if)#  spanning-tree portfast
Cat3750E(config-if)#  exit
```

Configure interswitch connections as trunk ports. Here is interface GigabitEthernet6/0/10 as an example.

```
Cat3750E(config)# interface GigabitEthernet6/0/10
Cat3750E(config-if)#  switchport trunk encapsulation dot1q
Cat3750E(config-if)#  switchport trunk native vlan 300
Cat3750E(config-if)#  switchport trunk allowed vlan 300-303
Cat3750E(config-if)#  switchport mode trunk
Cat3750E(config-if)#  exit
```

Enable multiple spanning tree. This requires enable MSTP and configuring one multiple spanning tree instance per VLAN.

```
Cat3750E(config)# spanning-tree mode mst
Cat3750E(config)# spanning-tree mst configuration
Cat3750E(config-mst)#  instance 1 vlan 300
Cat3750E(config-mst)#  instance 2 vlan 301
Cat3750E(config-mst)#  instance 3 vlan 302
Cat3750E(config-mst)#  instance 4 vlan 303
Cat3750E(config-mst)#  instance 5 vlan 304
Cat3750E(config-mst)#  end
```

Validation

HP A-series switches can use the command **`display stp brief`** to verify the state of spanning tree on HP A-series switches. HP E-series uses the command **`show spanning-tree`** to display the state of spanning tree on HP E-series switches.

To verify all switches send traffic only over the spanning tree interfaces in forwarding state, generate a known quantity of frames from Spirent TestCenter or other source to each VLAN and compare switch interface packet counters with those sent and received on each interface. Interfaces in blocking state will receive spanning tree BPDU frames but should transmit no frames.

To determine convergence time, disable one of the spanning tree interfaces in forwarding state while offering a known quantity of frames from Spirent TestCenter or other traffic generator. Convergence time can be derived from frame loss. For example, if Spirent TestCenter generates traffic at a rate of 1,000 frames per second, each dropped frame is equivalent to 1 millisecond of convergence time. If the switches drop 47 frames, then spanning tree convergence time is 47 ms.

OSPFv2 (OSPF for IPv4)

Objective

To verify that HP Networking and Cisco Catalyst switches are able to establish open shortest path first version 2 (OSPFv2) connections and exchange topology information.

Background

Intended for use on IPv4 networks, OSPFv2 supports IP subnetting and redistribution of routing information learned via other protocols. OSPF also allows session authentication and uses IP multicast for distribution of routing updates.

OSPF uses areas to segment traffic, with area 0 designated as the backbone network. OSPF typically involves coordination among multiple internal routers; area border routers (ABRs) connected to multiple areas; and autonomous system boundary routers (ASBRs).

In addition to standard areas, OSPFv2 also defines two special types of areas: Stubs are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area. A Not-So-Stubby-Area (NSSA) is like a stub area, but it can import external routes into the area for redistribution via OSPF.

Topology

This example uses multiple paths between HP and Cisco devices. Each HP and Cisco switch was configured with multiple networks, which were then advertised by OSPF to its neighbors.

Figure 1 above illustrates the OSPFv2 test bed. Access switches were connected to both distribution switches and the distribution switches were connected to both core switches. Traffic offered from the Spirent TestCenter traffic generator/analyzer verifies that traffic is indeed being passed between networks.

HP A-series commands

In this example, switched virtual interfaces (SVIs) are created using VLAN interfaces. Physical interfaces are then mapped to the VLAN interfaces. Routing is done between VLAN interfaces on each switch.

Create the VLANs.

```
<HP5800> system-view
[HP5800] vlan 1
[HP5800] vlan 2 to 9
```

Create the switched virtual interfaces.

```
[HP5800] interface Vlan-interface2
[HP5800-vlan-interface2] ip address 10.0.2.1 255.255.255.0
[HP5800-vlan-interface2] interface Vlan-interface3
[HP5800-vlan-interface3] ip address 10.0.3.1 255.255.255.0
[HP5800-vlan-interface3] interface Vlan-interface4
[HP5800-vlan-interface4] ip address 10.0.4.1 255.255.255.0
[HP5800-vlan-interface4] interface Vlan-interface5
[HP5800-vlan-interface5] ip address 10.0.5.1 255.255.255.0
[HP5800-vlan-interface5] interface Vlan-interface6
[HP5800-vlan-interface6] ip address 10.0.6.1 255.255.255.0
[HP5800-vlan-interface6] interface Vlan-interface7
[HP5800-vlan-interface7] ip address 10.0.7.1 255.255.255.0
[HP5800-vlan-interface7] interface Vlan-interface8
[HP5800-vlan-interface8] ip address 10.0.8.1 255.255.255.0
[HP5800-vlan-interface8] interface Vlan-interface9
[HP5800-vlan-interface9] ip address 10.0.9.1 255.255.255.0
[HP5800-vlan-interface9] quit
```

Associate the physical interfaces with the corresponding SVIs.

```
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1]  port link-mode bridge
[HP5800-Gigabitethernet1/0/1]  port access vlan 2
[HP5800-Gigabitethernet1/0/1] interface GigabitEthernet1/0/2
[HP5800-Gigabitethernet1/0/2]  port link-mode bridge
[HP5800-Gigabitethernet1/0/2]  port access vlan 3
[HP5800-Gigabitethernet1/0/2] interface GigabitEthernet1/0/3
[HP5800-Gigabitethernet1/0/3]  port link-mode bridge
[HP5800-Gigabitethernet1/0/3]  port access vlan 4
[HP5800-Gigabitethernet1/0/3] interface GigabitEthernet1/0/4
[HP5800-Gigabitethernet1/0/4]  port link-mode bridge
[HP5800-Gigabitethernet1/0/4]  port access vlan 5
[HP5800-Gigabitethernet1/0/4] interface GigabitEthernet1/0/5
[HP5800-Gigabitethernet1/0/5]  port link-mode bridge
[HP5800-Gigabitethernet1/0/5]  port access vlan 6
[HP5800-Gigabitethernet1/0/5] interface GigabitEthernet1/0/6
[HP5800-Gigabitethernet1/0/6]  port link-mode bridge
[HP5800-Gigabitethernet1/0/6]  port access vlan 7
[HP5800-Gigabitethernet1/0/6] interface GigabitEthernet1/0/7
[HP5800-Gigabitethernet1/0/7]  port link-mode bridge
[HP5800-Gigabitethernet1/0/7]  port access vlan 8
[HP5800-Gigabitethernet1/0/7] interface GigabitEthernet1/0/8
[HP5800-Gigabitethernet1/0/8]  port link-mode bridge
[HP5800-Gigabitethernet1/0/8]  port access vlan 9
[HP5800-Gigabitethernet1/0/8]  quit
```

Configure OSPF routing.

```
[HP5800] ospf 1 router-id 10.0.0.1
[HP5800-ospf]  area 0.0.0.0
[HP5800-ospf]   network 10.0.0.0 0.0.255.255
[HP5800-ospf]   quit
[HP5800]   quit
```

HP E-series commands

For the HP E-series switches, a single command sets up VLANs and assigns physical interfaces to those VLANs.

Enable IP routing .

```
HP5406ZL> configure
HP5406ZL(config)> ip routing
```

Define and configure VLANs.

```
HP5406ZL(config)> vlan 33
HP5406ZL(vlan-33)>    name "VLAN33"
HP5406ZL(vlan-33)>    untagged A1
HP5406ZL(vlan-33)>    ip address 10.0.33.1 255.255.255.0
HP5406ZL(vlan-33)>    exit
HP5406ZL(vlan-33)> vlan 34
HP5406ZL(vlan-34)>    name "VLAN34"
HP5406ZL(vlan-34)>    untagged A2
HP5406ZL(vlan-34)>    ip address 10.0.34.1 255.255.255.0
HP5406ZL(vlan-34)>    exit
HP5406ZL(vlan-34)> vlan 35
HP5406ZL(vlan-35)>    name "VLAN35"
HP5406ZL(vlan-35)>    untagged A3
HP5406ZL(vlan-35)>    ip address 10.0.35.1 255.255.255.0
HP5406ZL(vlan-35)>    exit
HP5406ZL(vlan-35)> vlan 36
HP5406ZL(vlan-36)>    name "VLAN36"
HP5406ZL(vlan-36)>    untagged A4
HP5406ZL(vlan-36)>    ip address 10.0.36.1 255.255.255.0
HP5406ZL(vlan-36)>    exit
HP5406ZL(vlan-36)> vlan 37
HP5406ZL(vlan-37)>    name "VLAN37"
HP5406ZL(vlan-37)>    untagged A5
HP5406ZL(vlan-37)>    ip address 10.0.37.1 255.255.255.0
HP5406ZL(vlan-37)>    exit
HP5406ZL(vlan-37)> vlan 38
HP5406ZL(vlan-38)>    name "VLAN38"
HP5406ZL(vlan-38)>    untagged A6
HP5406ZL(vlan-38)>    ip address 10.0.38.1 255.255.255.0
HP5406ZL(vlan-38)>    exit
HP5406ZL(vlan-38)> vlan 39
HP5406ZL(vlan-39)>    name "VLAN39"
HP5406ZL(vlan-39)>    untagged A7
HP5406ZL(vlan-39)>    ip address 10.0.39.1 255.255.255.0
```

```
HP5406ZL(vlan-39)>    exit
HP5406ZL(vlan-39)> vlan 40
HP5406ZL(vlan-40)>    name "VLAN40"
HP5406ZL(vlan-40)>    untagged A8
HP5406ZL(vlan-40)>    ip address 10.0.40.1 255.255.255.0
HP5406ZL(vlan-40)>    exit
```

Enable OSPF routing and configure the VLANs for OSPF.

```
HP5406ZL(config)> ip router-id 10.0.32.1
HP5406ZL(config)> router ospf
HP5406ZL(ospf)>    area backbone range 10.0.0.0 255.255.0.0 type summary
HP5406ZL(ospf)>    exit
HP5406ZL(config)> vlan 33
HP5406ZL(vlan-33)>    ip ospf 10.0.33.1 area backbone
HP5406ZL(vlan-33)>    exit
HP5406ZL(vlan-33)> vlan 34
HP5406ZL(vlan-34)>    ip ospf 10.0.34.1 area backbone
HP5406ZL(vlan-34)>    exit
HP5406ZL(vlan-34)> vlan 35
HP5406ZL(vlan-35)>    ip ospf 10.0.35.1 area backbone
HP5406ZL(vlan-35)>    exit
HP5406ZL(vlan-35)> vlan 36
HP5406ZL(vlan-36)>    ip ospf 10.0.36.1 area backbone
HP5406ZL(vlan-36)>    exit
HP5406ZL(vlan-36)> vlan 37
HP5406ZL(vlan-37)>    ip ospf 10.0.37.1 area backbone
HP5406ZL(vlan-37)>    exit
HP5406ZL(vlan-37)> vlan 38
HP5406ZL(vlan-38)>    ip ospf 10.0.38.1 area backbone
HP5406ZL(vlan-38)>    exit
HP5406ZL(vlan-38)> vlan 39
HP5406ZL(vlan-39)>    ip ospf 10.0.39.1 area backbone
HP5406ZL(vlan-39)>    exit
HP5406ZL(vlan-39)> vlan 40
HP5406ZL(vlan-40)>    ip ospf 10.0.40.1 area backbone
HP5406ZL(vlan-40)>    exit
HP5406ZL>    exit
```

Cisco commands

On Cisco Catalyst switches, like HP A-series switches, create the VLANs first and then assign physical interfaces to the VLAN interfaces. The following commands apply to a Cisco Catalyst 6509. The syntax is similar for Cisco Catalyst 3750-E switches and Cisco Catalyst 4506 switches.

First, enable routing.

```
Cat6509# configure terminal
Cat6509(config)# ip routing
```

Then, create the VLAN interfaces.

```
Cat6509(config)# interface Vlan129
Cat6509(config-if)#  ip address 10.0.129.1 255.255.255.0
Cat6509(config-if)# interface Vlan130
Cat6509(config-if)#  ip address 10.0.130.1 255.255.255.0
Cat6509(config-if)# interface Vlan131
Cat6509(config-if)#  ip address 10.0.131.1 255.255.255.0
Cat6509(config-if)# interface Vlan132
Cat6509(config-if)#  ip address 10.0.132.1 255.255.255.0
Cat6509(config-if)# interface Vlan133
Cat6509(config-if)#  ip address 10.0.133.1 255.255.255.0
Cat6509(config-if)# interface Vlan134
Cat6509(config-if)#  ip address 10.0.134.1 255.255.255.0
Cat6509(config-if)# interface Vlan135
Cat6509(config-if)#  ip address 10.0.135.1 255.255.255.0
Cat6509(config-if)# interface Vlan136
Cat6509(config-if)#  ip address 10.0.136.1 255.255.255.0
Cat6509(config-if)#  exit
```

Next, assign physical interfaces to the VLANs.

```
Cat6509(config)# interface GigabitEthernet1/0/1
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 129
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/2
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 130
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/3
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 131
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/4
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 132
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/5
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 133
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/6
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 134
Cat6509(config-if)#  switchport mode access
```

```
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/7
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 135
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)# interface GigabitEthernet1/0/8
Cat6509(config-if)#  no ip address
Cat6509(config-if)#  switchport
Cat6509(config-if)#  switchport access vlan 136
Cat6509(config-if)#  switchport mode access
Cat6509(config-if)#  spanning-tree portfast
Cat6509(config-if)#  exit
```

Finally, enable OSPF routing.

```
Cat6509(config)# router ospf 1
Cat6509(config-ospf)#  log-adjacency-changes
Cat6509(config-ospf)#  network 10.0.0.0 0.0.255.255 area 0
Cat6509(config-ospf)#  end
```

Validation

If the HP and Cisco devices are unable to complete OSPF negotiation, routing adjacencies will remain in the ExStart state. Fully functional adjacencies will be in the Full state. To verify that an OSPF adjacency has entered OSPF Full state on the HP switches, use the **`display ospf peer`** command on A-series switches and the **`show ip ospf neighbor`** command on E-series switches.

OSPFv3 (OSPF for IPv6)

Objective

To verify that HP Networking and Cisco Catalyst switches are able to establish open shortest path first version 3 (OSPFv3) connections and exchange topology information.

Background

OSPFv3 updates the routing protocol for use on IPv6 networks. In a mixed IPv4/IPv6 environment, OSPFv2 must be used in conjunction with OSPFv3.

While the basic mechanics of OSPF are identical in both versions, OSPFv3 introduces new link-state advertisement (LSA) types; removes addressing semantics from OSPF headers; generalizes

flooding; and removes OSPF-layer authentication, among other changes. RFC 5340 describes OSPFv3.

Topology

This example uses multiple paths between HP and Cisco devices. Each HP and Cisco switch was configured with multiple networks, which were then advertised by OSPF to its neighbors. The switches have been configured in dual-stack IPv4/IPv6 mode, running both OSPFv2 (to support IPv4 traffic) and OSPFv3 (to support IPv6 traffic).

Figure 1 above illustrates the OSPv3 test bed. Both access switches were connected to both distribution switches, and both distribution switches in turn were connected to both core switches. Traffic offered from the Spirent TestCenter traffic generator/analyzer verifies that traffic is correctly routed between networks.

HP A-series commands

In this example, switched virtual interfaces (SVIs) are created using VLAN interfaces. Physical interfaces are then mapped to the VLAN interfaces. Routing is done between VLAN interfaces on each switch. Unlike OSPFv2, OSPv3 configuration is done on the actual routable interface.

While not required, the configuration is using a dual-stack IPv4/IPv6 setup.

First, enable IPv6.

```
<HP9505> system-view
[HP9505] ipv6
```

Then, configure the VLAN interfaces.

```
[HP9505] vlan 65
[HP9505] vlan 75
[HP9505] interface Vlan-interface65
[HP9505-vlan-interface65]  ipv6 address 2002:9505:0:65::1/64
[HP9505-vlan-interface65]  ospfv3 1 area 0.0.0.0
[HP9505-vlan-interface65]  ip address 10.0.65.1 255.255.255.0
[HP9505-vlan-interface65] interface Vlan-interface75
[HP9505-vlan-interface75]  ipv6 address 2002:9595:4506:75::1/64
[HP9505-vlan-interface75]  ospfv3 1 area 0.0.0.0
[HP9505-vlan-interface75]  ip address 10.0.75.1 255.255.255.0
[HP9505-vlan-interface75]  quit
```

Next, assign the physical interfaces to the VLANs.

```
[HP9505] interface GigabitEthernet3/0/9
[HP9505-Gigabitethernet3/0/9]  port access vlan 65
[HP9505-Gigabitethernet3/0/9] interface GigabitEthernet3/0/11
[HP9505-Gigabitethernet3/0/11]  port access vlan 75
[HP9505-Gigabitethernet3/0/11]  quit
```

Finally, configure the OSPFv3 and OSPFv2 routing processes.

```
[HP9505] ospf 1 router-id 10.0.64.1
[HP9505-ospf]  area 0.0.0.0
[HP9505-ospf]   network 10.0.0.0 0.0.255.255
[HP9505-ospf] ospfv3 1
[HP9505-ospfv3]  router-id 10.0.64.1
[HP9505-ospfv3]  area 0.0.0.0
[HP9505-ospfv3]  quit
[HP9505]  quit
```

HP E-series commands

For HP E-series switches, a single command sets up VLANs and assigns physical interfaces to the VLANs.

First, enable routing.

```
HP5406ZL# configure
HP5406ZL(config)# ip routing
HP5406ZL(config)# ipv6 unicast-routing
```

Next, create the VLAN and assign the associated physical interfaces to it.

```
HP5406ZL(config)# vlan 42
HP5406ZL(vlan-42)#    name "VLAN42"
HP5406ZL(vlan-42)#    untagged A9
HP5406ZL(vlan-42)#    ip address 10.0.42.1 255.255.255.0
HP5406ZL(vlan-42)#    ipv6 address 2002:5406:6509:42::1/64
HP5406ZL(vlan-42)#    exit
```

Then, configure the OSPF processes.

```
HP5406ZL(config)# ip router-id 10.0.32.1
HP5406ZL(config)# router ospf
HP5406ZL(ospf)#    area backbone range 10.0.0.0 255.255.0.0 type summary
HP5406ZL(ospf)#    exit
HP5406ZL(config)# router ospf3
HP5406ZL(ospf3)#    area backbone
HP5406ZL(ospf3)#    enable
HP5406ZL(ospf3)#    exit
```

Finally, enable OSPF on the VLAN.

```
HP5406ZL(config)# vlan 42
HP5406ZL(vlan-42)#    ip ospf 10.0.42.1 area backbone
HP5406ZL(vlan-42)#    ipv6 ospf3 area backbone
HP5406ZL(vlan-42)#    exit
```

Cisco commands

On Cisco Catalyst switches, like HP A-series switches, create the VLANs first and then assign physical interfaces to the VLAN instances. The following commands apply to a Cisco Catalyst 6509. Except where noted, the syntax is similar for the Cisco Catalyst 3750-E and Cisco Catalyst 4506 switches.

First, enable IPv6 routing.

```
Cat6509# configure terminal
Cat6509(config)# ipv6 unicast-routing
```

Configuration syntax is slightly different on the Cisco Catalyst 3750-E. First, configure the system to support IPv6.

```
Cat3750E# configure terminal
Cat3750E(config)# sdm prefer dual-ipv4-and-ipv6 default
Cat3750E(config)# ip routing
Cat3750E(config)# ipv6 unicast-routing
```

Cisco Catalyst 3750-E, Cisco Catalyst 4506, and Cisco Catalyst 6509 switches use the same commands for the remaining steps.

Configure the physical interface. With OSPFv3, the primary configuration is done on the port.

```
Cat6509(config)# interface GigabitEthernet4/9
Cat6509(config-if)#  ip address 10.0.42.2 255.255.255.0
Cat6509(config-if)#  ipv6 address 2002:5406:6509:42::2/64
Cat6509(config-if)#  ipv6 ospf 1 area 0
Cat6509(config-if)#  exit
```

Finally, configure the OSPF router processes. On Cisco Catalyst switches, **`ospf`** refers to OSPFv2 while **`ipv6 ospf`** refers to OSPFv3.

```
Cat6509(config)# router ospf 1
Cat6509(config-ospf)#  log-adjacency-changes
Cat6509(config-ospf)#  network 10.0.42.2 0.0.0.0 area 0
Cat6509(config-ospf)#  network 10.0.73.2 0.0.0.0 area 0
Cat6509(config-ospf)#  network 10.0.77.2 0.0.0.0 area 0
Cat6509(config-ospf)#  network 10.0.128.0 0.0.127.255 area 0
Cat6509(config-ospf)# ipv6 router ospf 1
Cat6509(config-ipv6-ospf)#  log-adjacency-changes
Cat6509(config-ipv6-ospf)#  end
```

Validation

If the HP and Cisco devices are unable to complete OSPF negotiation, routing adjacencies will remain in the ExStart state. Fully functional adjacencies will be in the Full state. To verify that an OSPF adjacency has entered OSPF Full state on the HP switches, use the **`display ospf peer`** command on the A-series switches and the **`show ipv6 ospf neighbor`** command on the HP E-series switches.

IP multicast switching

Objective

To verify the ability of HP Networking and Cisco Catalyst switches to correctly forward multicast traffic from a multicast routed network.

Background

In IPv4 networks, Ethernet switches use Internet group management protocol (IGMP) snooping to determine where a switch should forward multicast traffic. With IGMP snooping enabled, a switch listens for IGMP reports from attached multicast subscribers. The switch then maps subscribed multicast group address(es) to the interface on which the subscriber is attached. When the switch receives traffic destined for one or more addresses, it will forward it only to those interfaces from which it has heard membership reports.

IGMP snooping requires the use of either an IGMP querier or an IGMP PIM router. An IGMP querier is useful if no router is available, and in this case acts as the multicast router (mrouter) for VLAN by issuing periodic membership queries. If an IGMP querier is being used, there should only be one querier per VLAN.

Topology

In this example, a Spirent TestCenter port attached to the Cisco Catalyst 3750-E offers traffic destined to 10 multicast groups, while other test ports emulate multicast subscribers on the HP A5800 and HP E5406zl. An IGMP querier is used instead of a multicast router.

Figure 1 above illustrates the topology used to validate IP multicast switching functionality. On HP switches, all subscriber interfaces use the same VLAN for untagged traffic, and IGMP snooping is enabled. On the Cisco Catalyst 6509 and Cisco Catalyst 4506, IGMP snooping is enabled. On the Cisco Catalyst 3750-E, IGMP snooping and IGMP querier are enabled.

HP A-series commands

In this example, all interfaces use the same VLAN for untagged traffic and IGMP snooping is enabled globally:

```
<HP5800> system-view
[HP5800] igmp-snooping
```

IGMP snooping also must be enabled on a per-VLAN basis. Only one VLAN is used in this switching example. In configurations that use additional VLANs, only one querier should be defined per VLAN.

```
[HP5800] vlan 300
[HP5800-Vlan-300] igmp-snooping enable
[HP5800-Vlan-300] igmp-snooping querier
[HP5800-Vlan-300] quit
[HP5800] quit
```

HP E-series commands

On HP E-series switches, IGMP snooping also is enabled on a per-VLAN basis:

```
HP5406ZL# configure
HP5406ZL(config)# vlan 300
HP5406ZL(vlan-300)# ip igmp
HP5406ZL(vlan-300)# exit
```

Cisco commands

The following commands apply to a Cisco Catalyst 6509. Except where noted, the syntax is similar for the Catalyst 3750-E switches and Cisco Catalyst 4506 switches.

First, enable IP multicast routing.

```
Cat6509# configure terminal
Cat6509(config)# ip multicast-routing
```

Cisco Catalyst 3750-E switches use a slightly different syntax.

```
Cat3750# configure terminal
Cat3750(config)# ip routing
Cat3750(config)# ip multicast-routing distributed
```

Cisco Catalyst 3750-E, Cisco Catalyst 4506, and Cisco Catalyst 6509 switches use the same commands for the remaining steps.

Enable IGMP snooping. IGMP snooping is enabled by default on Cisco Catalyst switches for all VLANs. In case it is disabled, it can be enabled with these commands:

```
Cat6509# configure terminal
Cat6509(config)# ip igmp snooping
```

Next, enable an IGMP querier. Only one querier should be defined across all switches that share a common VLAN ID.

```
Cat6509# configure terminal
Cat6509(config)# ip igmp snooping querier
Cat6509(config)# end
```

Validation

Once subscribers attached to the HP A5800 switches and the HP E5406zl switches have joined multicast groups by sending IGMP reports with join messages, multicast traffic for these groups will be forwarded to all subscriber ports.

The HP A-series switch command **`display igmp-snooping group`** also will verify that the HP A5800 and Cisco devices see one another and can exchange IGMP membership information.

The HP E-series switch command **`show ip igmp`** also will verify that the HP E5406zl and Cisco devices see one another and can exchange IGMP membership information.

IP multicast routing

Objective

To verify the ability of HP switches to learn multicast routing information from a Cisco device using the protocol independent multicast-sparse mode (PIM-SM) protocol.

To verify the ability of the HP Networking and Cisco Catalyst switches to correctly forward multicast traffic based on routing information learned via PIM-SM.

Background

PIM-SM is a popular choice for multicast routing. Devices running PIM-SM can learn topology information from other PIM-SM routers and make forwarding decisions based on that information.

Topology

This example is similar to that used in the "IP Multicast Switching" section, with two important changes: Routing (including OSPF) is enabled on all switches, and the HP A9505 switch also acts a PIM-SM router.

In this example, a Spirent TestCenter port attached to the Cisco Catalyst 3750-E offers traffic destined to 10 multicast groups on different subnets while other test ports emulated multicast subscribers to all 10 groups on the HP A5800 and HP E5406zl. The Cisco device uses PIM-SM to propagate subnet routing information to other subnets, including the ones on the HP switches, also running PIM-SM, as attached.

The HP switches use PIM-SM and OSPF to propagate routing information. Multicast subscribers attached to VLAN-routed interfaces, each in a different VLAN with each VLAN in a different IP subnet, receive traffic from Sprirent TestCenter. The subscriber interfaces also use IGMP to build a multicast forwarding table.

Figure 1 above illustrates the topology used to validate IP multicast routing functionality. PIM-SM and OSPF routing is enabled on all Cisco and HP devices.

HP A-series commands

First, create the necessary VLANs.

```
<HP5800> system-view
[HP5800] vlan 2 to 10
```

Next, assign IP addresses and enable IGMP on the respective VLANs.

```
[HP5800] interface Vlan-interface2
[HP5800-vlan-interface2] ip address 10.0.2.1 255.255.255.0
[HP5800-vlan-interface2]  igmp enable
[HP5800-vlan-interface2] interface Vlan-interface3
[HP5800-vlan-interface3]  ip address 10.0.3.1 255.255.255.0
[HP5800-vlan-interface3]  igmp enable
[HP5800-vlan-interface3] interface Vlan-interface4
```

```
[HP5800-vlan-interface4]  ip address 10.0.4.1 255.255.255.0
[HP5800-vlan-interface4]  igmp enable
[HP5800-vlan-interface4] interface Vlan-interface5
[HP5800-vlan-interface5]  ip address 10.0.5.1 255.255.255.0
[HP5800-vlan-interface5]  igmp enable
[HP5800-vlan-interface5] interface Vlan-interface6
[HP5800-vlan-interface6]  ip address 10.0.6.1 255.255.255.0
[HP5800-vlan-interface6]  igmp enable
[HP5800-vlan-interface6] interface Vlan-interface7
[HP5800-vlan-interface7]  ip address 10.0.7.1 255.255.255.0
[HP5800-vlan-interface7]  igmp enable
[HP5800-vlan-interface7] interface Vlan-interface8
[HP5800-vlan-interface8]  ip address 10.0.8.1 255.255.255.0
[HP5800-vlan-interface8]  igmp enable
[HP5800-vlan-interface8] interface Vlan-interface9
[HP5800-vlan-interface9]  ip address 10.0.9.1 255.255.255.0
[HP5800-vlan-interface9]  igmp enable
[HP5800-vlan-interface9]  quit
```

Then, assign the interfaces to the respective VLANs.

```
[HP5800] interface GigabitEthernet1/0/1
[HP5800-Gigabitethernet1/0/1] port link-mode bridge
[HP5800-Gigabitethernet1/0/1] port access vlan 2
[HP5800-Gigabitethernet1/0/1] interface GigabitEthernet1/0/2
[HP5800-Gigabitethernet1/0/2] port link-mode bridge
[HP5800-Gigabitethernet1/0/2] port access vlan 3
[HP5800-Gigabitethernet1/0/2] interface GigabitEthernet1/0/3
[HP5800-Gigabitethernet1/0/3] port link-mode bridge
[HP5800-Gigabitethernet1/0/3] port access vlan 4
[HP5800-Gigabitethernet1/0/3] interface GigabitEthernet1/0/4
[HP5800-Gigabitethernet1/0/4] port link-mode bridge
[HP5800-Gigabitethernet1/0/4] port access vlan 5
[HP5800-Gigabitethernet1/0/4] interface GigabitEthernet1/0/5
[HP5800-Gigabitethernet1/0/5] port link-mode bridge
[HP5800-Gigabitethernet1/0/5] port access vlan 6
[HP5800-Gigabitethernet1/0/5] interface GigabitEthernet1/0/6
[HP5800-Gigabitethernet1/0/6] port link-mode bridge
[HP5800-Gigabitethernet1/0/6] port access vlan 7
[HP5800-Gigabitethernet1/0/6] interface GigabitEthernet1/0/7
[HP5800-Gigabitethernet1/0/7] port link-mode bridge
[HP5800-Gigabitethernet1/0/7] port access vlan 8
[HP5800-Gigabitethernet1/0/7] interface GigabitEthernet1/0/8
[HP5800-Gigabitethernet1/0/8] port link-mode bridge
[HP5800-Gigabitethernet1/0/8] port access vlan 9
[HP5800-Gigabitethernet1/0/8] quit
```

Next, enable multicast routing and IGMP.

```
[HP5800] multicast routing-enable
[HP5800] igmp-snooping
```

Then, enable OSPF. Although this step is not strictly necessary for IP multicast routing, some unicast routing protocol or static routing is required.

```
[HP5800] ospf 1 router-id 10.0.0.1
[HP5800-OSPF] area 0.0.0.0
[HP5800-OSPF] network 10.0.0.0 0.0.255.255
[HP5800-OSPF] quit
```

Then, enable PIM-SM and designate a rendezvous point (RP), in this example the VLAN interface on the HP A9505 switch.

```
[HP5800] pim
[HP5800-PIM] static-rp 10.0.73.1
[HP5800-PIM] quit
```

Next, enable PIM-SM on the VLAN used for the trunk line between switches.

```
[HP5800] interface Vlan-interface41
[HP5800-vlan-interface41]  ip address 10.0.41.2 255.255.255.0
[HP5800-vlan-interface41]  igmp enable
[HP5800-vlan-interface41]  pim sm
[HP5800-vlan-interface41]  quit
```

Finally, on the HP A9505, we need to configure the rendezvous point (RP). We will also enable PIM-SM on the same VLAN interface that is being used as the rendezvous point.

```
[HP9505] interface Vlan-interface75
[HP9505-vlan-interface75]  ip address 10.0.75.1 255.255.255.0
[HP9505-vlan-interface75]  igmp enable
[HP9505-vlan-interface75]  pim sm
[HP9505] pim
[HP9505-PIM]  c-rp Vlan-interface73
[HP9505-PIM]  static-rp 10.0.73.1
[HP9505-PIM]  quit
[HP9505]  quit
```

HP E-series commands

First, setup the VLANs that will be used, and assign interfaces to them.

```
HP5406# configure
HP5406(config)# vlan 33
HP5406(vlan-33)#    name "VLAN33"
HP5406(vlan-33)#    untagged A1
HP5406(vlan-33)#    ip address 10.0.33.1 255.255.255.0
HP5406(vlan-33)#    exit
HP5406(config)# vlan 34
HP5406(vlan-34)#    name "VLAN34"
HP5406(vlan-34)#    untagged A2
HP5406(vlan-34)#    ip address 10.0.34.1 255.255.255.0
HP5406(vlan-34)#    exit
HP5406(config)# vlan 35
HP5406(vlan-35)#    name "VLAN35"
HP5406(vlan-35)#    untagged A3
HP5406(vlan-35)#    ip address 10.0.35.1 255.255.255.0
```

```
HP5406(vlan-35)#    exit
HP5406(config)# vlan36
HP5406(vlan-36)#    name "VLAN36"
HP5406(vlan-36)#    untagged A4
HP5406(vlan-36)#    ip address 10.0.36.1 255.255.255.0
HP5406(vlan-36)#    exit
HP5406(config)# vlan 37
HP5406(vlan-37)#    name "VLAN37"
HP5406(vlan-37)#    untagged A5
HP5406(vlan-37)#    ip address 10.0.37.1 255.255.255.0
HP5406(vlan-37)#    exit
HP5406(config)# vlan 38
HP5406(vlan-38)#    name "VLAN38"
HP5406(vlan-38)#    untagged A6
HP5406(vlan-38)#    ip address 10.0.38.1 255.255.255.0
HP5406(vlan-38)#    exit
HP5406(config)# vlan 39
HP5406(vlan-39)#    name "VLAN39"
HP5406(vlan-39)#    untagged A7
HP5406(vlan-39)#    ip address 10.0.39.1 255.255.255.0
HP5406(vlan-39)#    exit
HP5406(config)# vlan 40
HP5406(vlan-40)#    name "VLAN40"
HP5406(vlan-40)#    untagged A8
HP5406(vlan-40)#    ip address 10.0.40.1 255.255.255.0
HP5406(vlan-40)#    exit
```

Next, configure OSPF routing. While OSPF is not strictly necessary, some unicast routing protocol or static routing is required.

```
HP5406(config)# ip routing
HP5406(config)# ip router-id 10.0.32.1
HP5406(config)# router ospf
HP5406(ospf)#    area backbone range 10.0.0.0 255.255.0.0 type summary
HP5406(ospf)#    exit
HP5406(config)# vlan 33
HP5406(vlan-33)#    ip ospf 10.0.33.1 area backbone
HP5406(vlan-33)#    exit
HP5406(config)# vlan 34
HP5406(vlan-34)#    ip ospf 10.0.34.1 area backbone
HP5406(vlan-34)#    exit
HP5406(config)# vlan 35
HP5406(vlan-35)#    ip ospf 10.0.35.1 area backbone
HP5406(vlan-35)#    exit
HP5406(config)# vlan 36
HP5406(vlan-36)#    ip ospf 10.0.36.1 area backbone
HP5406(vlan-36)#    exit
HP5406(config)# vlan 37
HP5406(vlan-37)#    ip ospf 10.0.37.1 area backbone
HP5406(vlan-37)#
HP5406(config)# vlan 38
HP5406(vlan-38)#    ip ospf 10.0.38.1 area backbone
HP5406(vlan-38)#    exit
HP5406(config)# vlan 39
```

```
HP5406(vlan-39)#    ip ospf 10.0.39.1 area backbone
HP5406(vlan-39)#    exit
HP5406(config)# vlan 40
HP5406(vlan-40)#    ip ospf 10.0.40.1 area backbone
HP5406(vlan-40)#    exit
```

Then, enable multicast routing and set the PIM rendezvous point (RP).

```
HP5406(config)# ip multicast-routing
HP5406(config)# router pim
HP5406(pim)#   rp-address 10.0.73.1 224.0.0.0 240.0.0.0
HP5406(pim)#   exit
```

Finally, configure a VLAN to carry traffic between switches, and enable OSPF on that VLAN.

```
HP5406(config)# vlan 43
HP5406(vlan-33)#    name "VLAN43"
HP5406(vlan-33)#    untagged A10
HP5406(vlan-33)#    ip address 10.0.43.1 255.255.255.0
HP5406(vlan-33)#    ip igmp
HP5406(vlan-33)#    exit
HP5406(vlan-33)#    ip ospf 10.0.43.1 area backbone
HP5406(vlan-33)#    ip pim-sparse
HP5406(vlan-33)#       ip-addr any
HP5406(vlan-33)#       exit
HP5406(vlan-33)#    exit
HP5406#    exit
```

Cisco commands

The following commands apply to a Cisco Catalyst 6509. Except where noted, the syntax is similar for Cisco Catalyst 3750-E and Cisco Catalyst 4506 switches.

First, enable IP multicast routing.

```
Cat6509# configure terminal
Cat6509(config)# ip multicast-routing
```

Command syntax is slightly different on the Cisco Catalyst 3750-E.

```
Cat3750E# configure terminal
Cat3750E(config)# ip routing
Cat3750E(config)# ip multicast-routing distributed
```

Cisco Catalyst 3750-E, Cisco Catalyst 4506, and Cisco Catalyst 6509 switches use the same commands for the remaining steps.

Configure interswitch interfaces with an IP address and support for PIM-SM.

```
Cat6509(config)# interface TenGigabitEthernet5/4
Cat6509(config-if)#  ip address 10.0.201.1 255.255.255.0
```

```
Cat6509(config-if)#  ip pim sparse-mode
Cat6509(config-if)#  exit
```

Then, enable OSPF. Although OSPF is not strictly necessary for IP multicast forwarding, some unicast routing protocol or static routing is required.

```
Cat6509(config)# router ospf 1
Cat6509(config-router)#  log-adjacency-changes
Cat6509(config-router)#  network 10.0.0.0 0.0.255.255 area 0
Cat6509(config-router)#  exit
```

4. Configure a PIM rendezvous point (RP). In the case the RP will be on the HP A9505.

```
Cat6509(config)# ip pim rp-address 10.0.73.1
Cat6509(config)# end
```

Validation

Once subscribers attached to the HP switches have joined multicast groups by sending IGMP reports with join messages, any multicast traffic for these groups offered to Interface VLAN73 on the HP9505 will be forward to all subscriber ports on the HP switches.

The HP A-series command **`display ip multicast routing-table`** will verify that the HP A5800 and Cisco devices see one another and can exchange multicast information. The HP E-series **`command show ip mrouter`** provides the same verification for HP E5406zl Ethernet switches.

Virtual router redundancy protocol (VRRP) interoperability

Objective

To validate failover functionality of the virtual router redundancy protocol (VRRP) between HP Networking and Cisco Catalyst switches configured as routers.

Background

Two or more routers can make use of VRRP to add redundancy and enhance network availability. With VRRP, all routers share a single virtual IP address. One router acts as the master (active) device, while all others act as backups. If the master router fails (or if a link fails on the interfaces configured with the virtual IP address), one of the backup routers takes over as master.

Topology

In this example, an HP A9505 switch, HP E5406zl, and Cisco Catalyst 6509 switch are all configured to route IP traffic. The interfaces connecting the switches each have unique IP addresses. A shared virtual IP address of 10.0.41.254/24 is used for VRRP, with the HP E5406zl initially acting as the master.

Figure 5 below illustrates the VRRP validation test bed. The HP switches assign an IP address to VLAN 41, and then assign interfaces to that VLAN. However, VRRP also would work if an IP address was assigned directly to the physical interface, as it is with the Cisco Catalyst 6509.

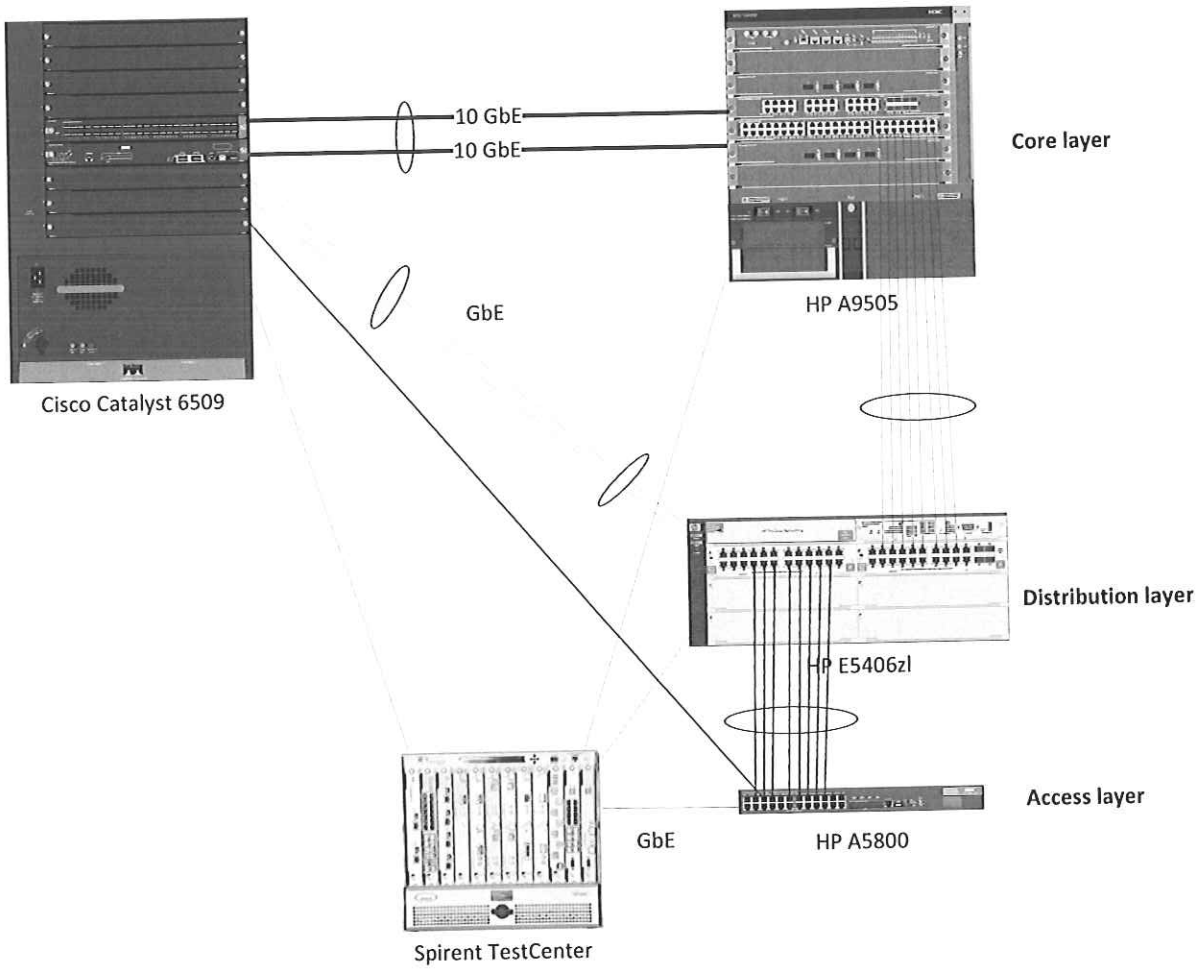


Figure 5: Virtual router redundancy protocol test bed

HP A-series commands

VRRP configuration is done in the interface configuration context. Here, it is done on the VLAN interface.

```
<HP9505> system-view
[HP9505] interface Vlan-interface41
[HP9505-Vlan-interface41]  ip address 10.0.41.1 255.255.255.0
[HP9505-Vlan-interface41]  vrrp vrid 1 virtual-ip 10.0.41.254
[HP9505-Vlan-interface41]  vrrp vrid 1 priority 254
[HP9505-Vlan-interface41]  quit
[HP9505]  quit
```

HP E-series commands

First, create and configure the VLAN interface.

```
HP5406ZL# configure
HP5406ZL(config)# vlan 41
HP5406ZL(vlan-41)#    name "VLAN41"
HP5406ZL(vlan-41)#    untagged A10
HP5406ZL(vlan-41)#    ip address 10.0.41.1 255.255.255.0
HP5406ZL(vlan-41)#    exit
```

Next, configure VRRP.

```
HP5406ZL(config)# router vrrp
HP5406ZL(config)# vlan 41
HP5406ZL(vlan-41)#    vrrp vrid 1
HP5406ZL(vlan-41-vrid-1)#       owner
HP5406ZL(vlan-41-vrid-1)#      virtual-ip-address 10.0.41.254 255.255.255.0
HP5406ZL(vlan-41-vrid-1)#      priority 255
HP5406ZL(vlan-41-vrid-1)#      enable
HP5406ZL(vlan-41-vrid-1)#      exit
HP5406ZL(vlan-41-vrid-1)#   exit
HP5406ZL(vlan-41)#   exit
HP5406ZL#   exit
```

Cisco commands

The following commands apply to a Cisco Catalyst 6509. The syntax is similar for Catalyst 3750-E and Cisco Catalyst 4506 switches.

VRRP configuration is done in the interface configuration context.

```
Cat6509# configure terminal
Cat6509(config)# interface GigabitEthernet4/21
Cat6509(config-if)#  ip address 10.0.41.3 255.255.255.0
```

```
Cat6509(config-if)#  vrrp 1 description VRRP Test
Cat6509(config-if)#  vrrp 1 ip 10.0.41.254
Cat6509(config-if)#  vrrp 1 timers learn
Cat6509(config-if)#  vrrp 1 priority 90
Cat6509(config-if)#  end
```

Validation

Both the HP E5406zl and Cisco Catalyst 6509 support the **`show vrrp`** command, which will indicate the current VRRP state on each system.

Appendix A: About Network Test

Network Test is an independent third-party test lab and engineering services consultancy. Our core competencies are performance, security, and conformance assessment of networking equipment and live networks. Our clients include equipment manufacturers, large enterprises, service providers, industry consortia, and trade publications.

Appendix B: Sample Configuration Files

This appendix lists URLs for the HP and Cisco switch files used to verify interoperability. These files are freely available for download from a public Network Test server.

A copy of this document, a brief interoperability report, and all HP and Cisco configuration files are available at http://networktest.com/hpiop.

Appendix C: Software Releases Tested

This appendix describes the software versions used on the test bed. All tests were conducted in March 2011 at Network Test's facility in Westlake Village, CA, USA.

Component	Version
HP A9505	5.20, Release 1238P08
HP E5406zl	K.15.03.0007
HP A5800	5.20, Release 1206
Cisco Catalyst 6509	12.2(33)SXI2a
Cisco Catalyst 4506	12.2(20)EWA
Cisco Catalyst 3750-E	12.2(55)SE1
Spirent TestCenter	3.55.5086.0000

Appendix D: Disclaimer

Network Test Inc. has made every attempt to ensure that all test procedures were conducted with the utmost precision and accuracy, but acknowledges that errors do occur. Network Test Inc. shall not be held liable for damages which may result for the use of information contained in this document. All trademarks mentioned in this document are property of their respective owners.

Network Test Inc.
31324 Via Colinas, Suite 113
Westlake Village, CA 91362-6761
USA
+1-818-889-0011
http://networktest.com
info@networktest.com