Hewlett Packard Enterprise

Deploying HPE FlexNetwork Core Technologies H8D06S (00832513)

Deploying HPE FlexNetwork Core Technologies provides you with a comprehensive set of networking skills which will increase your capability to simplify the journey to a unified campus network. Upon course completion, you will be able to successfully implement and troubleshoot enterprise-level HPE FlexNetwork solutions.

HPE course number	H8D06S
Course length	5 days
Delivery mode	ILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- IDC MarketScape leader 4 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and (ISC)²
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

Course description

This course includes comprehensive labs on which learners will have hands-on experience with Comware and ProVision switches, including configuring HPE switches supporting Layer 2 and Layer 3 network redundancy, dynamic routing with OSPF and BGP, network optimization via QoS, and IP multicast routing supported network systems. Additionally, you will extend your knowledge of Intelligent Resilient Framework (IRF) and how switch virtualization technology simplifies network design and operation.

HPE Intelligent Management Center (IMC), which allows network engineers and technicians to quickly and easily configure Quality of Service (QoS) and end-user authentication technologies, is featured throughout the course.

This course is approximately fifty percent lecture and learning activities and fifty percent lab activities.

The Deploying HPE FlexNetwork Core Technologies course prepares candidates for the HPE Accredited Solutions Expert (ASE)—FlexNetwork Integrator V1 certification within the HPE ExpertOne program.

Audience

IT Professionals who deploy enterprise/core solutions based on HPE products and technologies, including HPE Reseller Systems Engineers, Customer IT Staff, HPE System Engineers, and HPE Services Field and Call Center Support Engineers.

Certification(s) and Exam(s)

Certification(s)
HPE ASE—FlexNetwork Integrator V1.

Exam(s)
HPE0-Y47—Deploying HPE FlexNetwork Core Technologies.

Prerequisites

HPE ATP—FlexNetwork Solutions V2 certification or HPE AIS—Network Infrastructure (2011) is required in order to obtain the HPE ASE—Network Integrator V1 certification. The course supporting the HPE ATP—FlexNetwork Solutions V2 certification is 00870186—HPE FlexNetwork Fundamentals, Rev. 14.21.

What is new?

Deploying HPE FlexNetwork Core Technologies is a new course that combines the best of two courses, HPE Core/ Distribution Network Technologies using Comware Software, Rev. 11.41 and HPE Core/Distribution Network Technologies using ProVision Software, Rev. 10.41. The new course brings together both switch families in a single, comprehensive training. HPE Intelligent Management Center (IMC) network management software is the tool connecting it all together that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security needs. Additionally the Deploying HPE FlexNetwork Core Technologies course includes security related features and technologies such as Access Control Lists (ACLs) and port authentication.

Course objectives

The Deploying HPE FlexNetwork Core Technologies course covers the important topics a network specialist needs to know when deploying enterprise-level core networks in Campus LANs. After completing this course, you will be able to:

- Explain the HPE FlexNetwork Architecture
- Understand and configure advanced dynamic routing protocols like multi-area OSPF and BGP
- Configure and implement Router Redundancy with VRRP
- Configure and implement Data Link Layer Redundancy with Spanning Tree protocols, UDLD/DLDP and Distributed Trunking
- Configure and implement advanced network virtualization with IRF such as ISSU
- Configure and implement Network Security with ACLs and Port Authentication
- Deploy and manage the network with HPE Intelligent Management Center
- Configure and implement network optimization technologies such as Quality of Service (QoS)

Configure and implement Multicasting with IGMP, PIM Spars, and PI

Detailed course outline

Course Introduction	• Course overview • Course objectives	• Course agenda • HPE ASE—FlexNetwork Integrator V1 certification
Module 1: HPE FlexNetwork Architecture	• Objectives • Discussion topics • HPE FlexNetwork • HPE FlexCampus 2-and 3-tier reference architectures • HPE FlexCampus architecture for a smaller campus • HPE FlexFabric reference architectures – Supplemental information about BladeSystems • HPE FlexBranch solutions • HPE FlexManagement • Discussion topics • Switch planes • Modular switch planes • General forwarding plane architecture	• Crossbar fabric • CLOS fabric • Discussion topics • Enhancing resiliency in networks with HPE ProVision cores • Enhancing resiliency in networks with HPE Comware cores • Enhancing security and QoS • Implementing dynamic routing • Managing, monitoring, and troubleshooting • Meeting other business needs • Lab Activity 1 • Lab Activity 1 debrief • Summary • Learning check
Module 2: Network Management	• Objectives • Discussion topics • Port mirroring • Port mirroring on HPE Comware switches – Local port mirroring – Remote port mirroring • Port mirroring on HPE ProVision switches – Configuring local mirroring on ProVision switches – Configuring remote mirroring on ProVision switches – Enabling jumbo frames or using the truncation option • Discussion topics • sFlow – Configuring sFlow on HPE Comware switches – sFlow on HPE ProVision switches • NetFlow • NetStream • RMON – RMON support on HPE Comware switches – RMON on ProVision switches • Discussion topics • SNMP • SNMP v1 and v2c	– SNMP operations – SNMP communities • SNMP v3 – Configure SNMPv3 on HPE Comware switches – Configure SNMPv3 on HPE ProVision switches • NetConf • Discussion topics • HPE IMC: Review activity • HPE IMC recap • HPE IMC fits any organization's needs • HPE IMC add-on modules • Facilitator demonstration • IMC Deployment Monitoring Agent • SNMP, SSH, and Telnet templates • Discovery • Network Traffic Analyzer • Lab Activity 2.1 • Lab Activity 2.1 debrief • Lab Activity 2.2 • Lab Activity 2.2 debrief • Summary • Learning check

Module 3: Data Link Layer Redundancy

- Objectives
- Discussion topics
- STP review
  - Review questions
- RSTP review
  - Review questions
- MSTP review
- Discussion topics
- PVST+ spanning tree instances
  - Supplemental information: PVST
- Spanning tree and PVST+ BPDUs
  - Review of standard STP BPDUs
  - PVST+ BPDUs
- Other PVST+ enhancements
  - PortFast
  - UplinkFast
  - BackboneFast
- Introduction to RPVST+
- RPVST+ BPDUs
- Path cost differences
- Interoperation between protocols
- Configuring support for RPVST+
  - Configuring RPVST+ support on Comware switches
  - Configuring RPVST+ support on ProVision switches
- Review activity
  - Discussion question
- Discussion topics
- Detecting unidirectional links
- HPE ProVision switches: UDLD
- HPE ProVision switches: Guidelines for configuring UDLD
  - Configuring UDLD
  - Tagged or untagged UDLD frames
  - View information about UDLD-enabled ports
- HPE Comware switches: DLDP
- HPE Comware switches: DLDP states and timers
- HPE Comware switches: port shutdown modes
- HPE Comware switches: DLDP authentication
- HPE Comware switches: DLDP configuration steps
- Discussion topics
- Distributed trunking on HPE ProVision switches
- Server-to-switch distributed trunking
- Switch-to-switch distributed trunking
- InterSwitch-Connect (ISC)
- Peer-keepalive link
  - Updating switches running software versions K.14 to K.15.03
- Forwarding unicast traffic on the distributed trunk
- Forwarding multicast and broadcast traffic
- Layer 3 routing with distributed trunking
- Distributed trunking and spanning tree
- Distributed trunking topologies
- Distributed trunking topologies and IRF
- Distributed trunking with a non-HPE switch
- Preparing to configure distributed trunking
- Guidelines for ISC
- Guidelines for the peer-keepalive link
- Configuration steps
  - Configuring ISC
  - Configuring the peer-keepalive link
  - Configuring the distributed trunk
- Maximums and limitations
- HPE IMC—Monitoring data link layer redundancy
- Lab Activity 3
- Lab Activity 3 debrief
- Summary
- Learning check

Module 4: Virtual Router Redundancy Protocol (VRRP)

- Objectives
- Discussion topics
- Need for VRRP
- VRRP overview
- Controlling VRRP states
  - Controlling the states with a VRRP owner
  - Controlling the roles without a VRRP owner
- VRRP basic operation
  - Choosing the virtual router settings
- VRRP failover
  - Supplemental information on electing the new master
  - Supplemental information on controlling the failover time
- VRRP preempt and non-preempt mode
  - Effect of owner role on preemption
- Considerations for setting up VRRP
- Discussion topics
- Load-balancing routing within a subnet
- Load-balancing routing across different subnets
- Comware: Load-balancing within a subnet with one virtual router
  - Creating the VFs
  - Failing over for VF states
  - Summary of load-balancing VRRP functions
- Discussion topics
- ProVision: Combining VRRP and distributed trunking
- Combining VRRP and MSTP
- Monitoring VRRP with HPE IMC
- Lab Activity 4
- Lab Activity 4 debrief
- Learning check
- Summary

Module 5: HPE Intelligent Resilient Framework and Backplane Stacking

- Objectives
- Discussion topics
- Review activity: IRF on HPE Comware switches
- Implementing IRF at the access, distribution, or core
- Advantages of implementing IRF at the access layer
- Best practices for implementing IRF at the access layer
- Advantages of implementing IRF at the distribution layer
- Best practices for implementing IRF at the distribution layer
- Advantages of implementing IRF at the core layer
- Best practices for implementing IRF at core layer
- Configuring IRF: option 1
- Configuring IRF: option 2
- Synchronizing the configuration files
- Load sharing across physical links bound to IRF ports
- Managing the bridge MAC address for the IRF virtual device
- ISSU upgrade process
- ISSU: compatibility check
- ISSU prerequisite checklist
- MPU-based ISSU upgrade
  - Version rollback
- Member-based ISSU upgrade
- IRF split stack
- Detecting IRF split stacks with LACP MAD
  - Excluding a port from being shut down by MAD
- Detecting IRF split stacks with BFD MAD
  - Excluding a port from being shut down by MAD
- Detecting IRF splits with ARP MAD
  - Excluding a port from being shut down by MAD
- MAD: Detecting and resolving the split stack
- Activity: Comparing LACP and BFD MAD
- Using HPE IMC to monitor the IRF virtual device
- Lab Activity 5
- Lab Activity 5 debrief
- Discussion topics
- Backplane stacking on HPE 3800 and 2920 Switch Series (ProVision)
- Backplane stacking topologies
  - Activity
- Roles in the backplane stack
  - Commander
  - Standby member
  - Members
- Requirements
- Configuring a backplane stack
  - Deterministic installation method
  - Plug-and-go installation method
  - Election of the commander and standby member
- Stack operations
- Stack fragments
- Summary
- Learning check

Module 6: ACLs

- Objectives
- Discussion topics
- What is an ACL?
- Reasons to implement ACLs
- Discussion topics
- Types of ACLs
  - Basic/standard ACLs
  - Advanced/extended ACLs
  - Ethernet frame header ACLs
- Creating valid IDs for basic/standard ACLs
  - Creating and identifying a Comware basic ACL
  - Creating and identifying a ProVision standard ACL
- Creating rules for basic/standard ACLs
  - ID
  - Action
  - Matching criteria
  - Supplemental information about rule options
- Specifying IP address ranges with wildcard bits
  - Common IP addressing mask
  - Wildcard bits
  - Activity
- ProVision: Specifying IP address ranges with prefix length
  - Example
  - Activity
- Processing order and implicit permit or deny
  - Processing order
  - Implicit action
- Specifying rule IDs
  - Automatic numbering
  - Manual numbering
  - Sequence renumbering on ProVision switches
  - Sequence renumbering on Comware switches
- Comware: Matching based on logical order
- Review activity: Basic/standard ACL rules
- Creating valid IDs for advanced/extended ACLs
  - Creating and identifying a Comware advanced ACL
  - Creating and identifying a ProVision standard ACL
- Creating rules for advanced/extended ACLs
  - Supplemental information
- Comware: Matching based on logical order
- Review activity: Advanced/extended ACL rules
- Creating valid IDs for Ethernet frame header ACLs
- Creating rules for Ethernet frame header ACLs
  - Rule ID
  - Action
  - Match criteria
  - Additional options
  - Auto match order
- Discussion topics
- Applying ACLs to interfaces
  - Supplemental tips
- RACLs
- Port ACLs
  - Applying port ACLs to link aggregations (ProVision)
  - Applying port ACLs to link aggregation (Comware)
- ProVision: VACLs
- Comware: Alternative method for filtering traffic
  - Whitelist global packet filter
  - Blacklist global packet filter
- Example basic/standard ACL implementation
- Example advanced/extended ACL implementation
- Discussion topics
- HPE IMC ACL Management
- Creating rules for ACL resources manually
- Importing rules from templates with static rules
- Importing rules from templates with variables
- Creating standard rules for devices controlling different networks
- Discovering and importing ACLs
- Deploying ACLs to managed devices
- Optional Lab Activity 6.1
- Lab Activity 6.1 debrief
- Lab Activity 6.2
- Lab Activity 6.2 debrief
- Summary
- Learning check

Module 7: Port Authentication

- Objectives
- Port-based authentication use models
- Discussion topics
- 802.1X overview
  - Controlled port
  - Uncontrolled port
- 802.1X roles
  - Supplicant
  - Authenticator
  - Authentication server
- EAP framework
- Common EAP methods
  - EAP-Transport Layer Security (TLS)
  - PEAP and EAP-Tunneled TLS (TTLS)
- Complete process (EAP and RADIUS)
- 802.1X requirements
- 802.1X certificate requirements
- Defining the RADIUS server on the switch
  - ProVision
  - Comware
- Comware RADIUS schemes and domains
  - Assigning requests to domains
  - Using the domain
  - Activity
- Basic 802.1X configuration process
- Discussion topics
- HPE IMC UAM overview
- Creating service policies
- Defining access users
- Defining access devices
- Deploying AAA configurations to access devices
- Lab Activity 7.1
- Lab Activity 7.1 debrief
- Discussion topics
- Customizing authenticated users' access
  - Activity
- Process for configuring customized settings
  - More information on dynamic port ACLs
- Customizing settings with UAM
- Creating specialized requirements for access
- Defining specialized requirements and settings with UAM
- Permitting limited access for unauthorized clients
  - Guidelines for the network infrastructure setup
- Comware: Permitting limited access for unauthorized clients
- ProVision: Permitting limited access for unauthorized clients
- Supporting multiple clients on the same port at the same time
  - User-based/MAC-based versus port-based mode
- Multiple client scenario: Unmanaged switch and users in different VLANs
  - Using MAC-based VLANs to support multiple dynamic VLANs
  - Behavior when the port does not support MAC-based VLANs
  - Other scenarios with similar setup
- Multiple client scenario: Computer and VoIP phone
  - Comware setup
  - ProVision setup
- Discussion topics
- MAC-Auth overview
- RADIUS MAC-Auth
- RADIUS MAC-Auth options
  - Authentication protocol
  - Credentials
  - MAC address format
- RADIUS MAC-Auth configuration process
  - Comware steps
  - ProVision steps
- Comware: Local MAC-Auth
- Comware: Local MAC-Auth configuration process
- Lab Activity 7.2
- Lab Activity 7.2 debrief
- Discussion topics
- Web-Auth overview
  - Advantages of Web-Auth
  - Disadvantages of Web-Auth
- Overview of Web-Auth process and options
- Comware: Local Web-Auth with a RADIUS server
  - The scenario
  - How it works
- Comware: Set up local Web-Auth with a RADIUS server
- Comware: Local Web-Auth with local accounts
- Comware: Set up local Web-Auth with local accounts
- ProVision: Local Web-Auth to a RADIUS server
  - The scenario
  - How it works
- ProVision: Set up local Web-Auth to a RADIUS server
- Customizing local Web pages
- ProVision: Remote Web-Auth
  - The scenario
  - How it works
- ProVision: Set up remote Web-Auth
- Web-Auth with UAM portal services
- UAM portal authentication: Process
- UAM portal authentication: Set up UAM
- UAM portal authentication: Set up the Comware switch
  - Defining the portal server
  - Defining free rules
  - Enabling Web-Auth on the VLAN interface
  - Configuring the RADIUS settings
- UAM portal authentication: Multiple guest VLANs
- UAM portal authentication: Temporary IP addresses
- Summary of Web-Auth options
- Lab Activity 7.3
- Lab Activity 7.3 debrief
- Discussion topics
- Comware: Customizing MAC-Auth and Web-Auth connections
  - Activity
- ProVision: Customizing MAC-Auth and Web-Auth connections
- Comware: Using 802.1X and Web-Auth on the same port
- ProVision: Using 802.1X and Web-Auth on the same port
- Guidelines for using 802.1X and Web-Auth on the same port
- Using 802.1X, Web-Auth, and MAC-Auth on the same port
- Summary
- Learning check

Learn more at
hpe.com/ww/learnnetworking

Follow us:

Hewlett Packard Enterprise

c04586919, December 2016, Rev. 1