Contents

1 Training Description

1.1 H3C Certification Training

1.1.1 Constructing Secure Optimized WANs V2.0 (V7)

Training Object

- Personnel who are interested in network technologies and H3C certification
- H3C's agent engineers
- H3C training partner's trainers
- H3C product O&M personnel and technical support personnel

Entry Requirements

- Trainees have participated in and passed the H3C Certified Network Engineer (H3CNE) examination.
- It is advisable to complete the Building H3C High-Performance Campus Network V2.0 (V7 Version) and H3C Large-Scale Network Routing Technology V2.0 (V7 Version) courses.

Objectives

Upon completing this training, trainees will be able to:

- Understand the general WAN structure and related technologies.
- Master common broadband access technologies and understand their applications.
- Be proficient in common VPN principles, configurations, and applications such as GRE and L2TP.
- Be proficient in IPsec VPN principles, configurations, and applications.
- Understand SSL VPN working principles.
- Be proficient in BGP/MPLS VPN principles and configurations.
- Understand the technologies and means involved in enhancing network security.
- Be proficient in basic QoS principles, configurations, and applications.
- Understand basic concepts of the open system architecture.

Courses

Course ID	Course Name	Total Duration of Course (Working Days)	Practical Operation Duration (Working Days)
HM-050	Secure Optimized WAN Overview	0.15	
HM-051	Broadband Access Technologies	0.5	
HM-052	Conventional VPN Technologies	0.8	0.25
HM-053	Secure VPN Technologies	1	0.5

HM-054	BGP/MPLS VPN	1.1	0.5
HM-055	Network Security	0.3	
HM-057	Quality of Service	1	0.35
HM-058	Open Application Architecture	0.15	
Total		5	1.6

Training Content

- Enterprise network architecture and common technologies involved in WANs
- Principles of common broadband access technologies such as Ethernet, ADSL, and EPON
- Principles, configurations, and maintenance of VPN technologies such as GRE VPN, L2TP VPN, IPSec VPN, and SSL VPN
- BGP/MPLS VPN principles, configurations, and maintenance
- Technologies used to enhance network security, such as access control, authentication and authorization, and security protection
- QoS concepts, principles, configurations, and maintenance
- Open application architecture concepts

Training Mode

Class teaching and practical operation

Training Duration

5 working days, including 1.6 working days of practical operation

2 Course Description

HM-050 Secure Optimized WAN Overview

Prerequisites

Personnel who have passed H3C Certified Network Engineer (H3CNE) certification, or have a comparable level of technology

It is advisable to complete the Building H3C High-Performance Campus Network V2.0 (V7 Version) and H3C Large-Scale Network Routing Technology V2.0 (V7 Version) courses.

Course Objectives

- Master the enterprise network models.
- Master secure and optimized WAN technologies.

Course Content

- Enterprise network model
- Secure and optimized WAN technologies

Training Mode

Class teaching

Maximum Number of Trainees

12

Course Duration

0.15 working days

HM-051 Broadband Access Technologies

Prerequisites

Personnel who have completed course HM-050 or have a comparable level of technology

Course Objectives

- Master basic concepts of broadband access.
- Master principles of common broadband access technologies such as Ethernet, ADSL, EPON, and EPCN.

Course Content

- Basic concepts of broadband access
- PPPoE principles and configurations
- PON technology introduction
- Key EPON technologies and configurations
- Overview of cable TV network and bidirectional reconstruction
- EPCN technology introduction
- DSL technology introduction and comparisons of major DSL technologies
- ADSL principles and configurations
- ADSL2/2+ technology introduction

Training Mode

Class teaching

Maximum Number of Trainees

12

Course Duration

0.5 working days

HM-052 Conventional VPN Technologies

Prerequisites

Personnel who have completed course HM-051 or have a comparable level of technology

Course Objectives

- Master basic principles and configurations of GRE VPN.
- Master working principles and configurations of L2TP VPN.

Course Content

- VPN classification and common VPN technologies
- GRE encapsulation format
- GRE tunnel encapsulation and decapsulation processes
- GRE VPN deployment
- Basic concepts of L2TP VPN
- L2TP VPN data encapsulation and working process
- L2TP VPN configuration for an independent LAC
- Client LAC implemented through iNode clients
- Common faults and troubleshooting methods of L2TP VPN

Training Mode

Class teaching and practical operation

Maximum Number of Trainees

12

Course Duration

0.8 working days, including 0.25 working days of practical operation

HM-053 Secure VPN Technologies

Prerequisites

Personnel who have completed course HM-052 or have a comparable level of technology

Course Objectives

- Understand basic data security concepts.
- Master principles and configurations of IPsec VPN.
- Understand SSL VPN working principles.

Course Content

- Data encryption and decryption
- Data integrity and digital signature
- Digital certificate and PKI
- IPSec VPN system architecture
- AH and ESP
- IKE
- IPSec VPN configuration
- Common faults of IPSec VPN
- Tunnel nesting technologies such as GRE over IPSec
- SSL working principles
- SSL VPN functions and implementation

Training Mode

Class teaching and practical operation

Maximum Number of Trainees

12

Course Duration

1 working day, including 0.5 working days of practical operation

HM-054 BGP/MPLS VPN

Prerequisites

Personnel who have completed course HM-053 or have a comparable level of technology

Course Objectives

- Master basic MPLS principles.
- Master BGP/MPLS VPN principles and configurations.
- Master common troubleshooting methods of BGP/MPLS VPN.

Course Content

- MPLS label and label distribution
- MPLS data forwarding
- Multi-VRF technology
- Private route and private label transfer of BGP/MPLS VPN
- Data forwarding process of BGP/MPLS VPN
- BGP/MPLS VPN deployment and configurations

Training Mode

Class teaching and practical operation

Maximum Number of Trainees

12

Course Duration

1.1 working days, including 0.5 working days of practical operation

HM-055 Network Security

Prerequisites

Personnel who have completed course HM-054 or have a comparable level of technology

Course Objectives

- Understand network security content.
- Understand service separation, access control, and network attack defense means
- Application state detection firewall technology
- Security hardening for network devices

Course Content

- Network threat sources and concerns for building secure networks
- Major means for service separation and access control
- Configurations of firewalls with stateful inspection and packet filtering functions
- Typical attacks and security defense
- Equipment security hardening methods and configurations

Training Mode

Class teaching

Maximum Number of Trainees

12

Course Duration

0.3 working days

HM-057 Quality of Service

Prerequisites

Personnel who have completed course HM-055 or have a comparable level of technology

Course Objectives

- Understand basic concepts of Quality of Service and major Quality of Service models.
- Master the technical principles and configuration methods of DiffServ service models such as traffic policing, congestion management, and congestion avoidance.
- Master link validity enhancement technologies and configuration methods such as IP header compression, PPP payload compression, and LFI.

Course Content

- Basic concepts ofQuality of Service and majorQuality of Service models
- Configuration of Quality of Service boundary behaviors, including flag, shaping, and rate limiting
- Relationship between congestion management and queue scheduling
- Various queue scheduling technologies of routers
- Configurations of priority mapping, SQP, and WRR on switches
- Tail drop and TCP global synchronization
- RED and WRED
- CBQ and QoS Policy
- IP header compression and PPP payload compression
- LFI configurations

Training Mode

Class teaching and practical operation

Maximum Number of Trainees

12

Course Duration

1 working day, including 0.35 working days of practical operation

HM-058 Open Application Architecture

Prerequisites

Personnel who have completed course HM-057 or have a comparable level of technology

Course Objectives

- Understand OAA system architecture, components, and relationships.
- Master four OAA working modes and respective application scenarios.
- Understand associations between OAP and RSM and management methods.

Course Content

- Challenges that devices on traditional networks face
- Major components of the OAA system
- Four OAA working modes and respective application scenarios
- Association and management
- Typical OAA cases

Training Mode

Class teaching

Maximum Number of Trainees

12

Course Duration

0.15 working days