Interconnecting Cisco Networking Devices (CCENT), Part 3 of 4: Network Device Security

Meet the expert: As a certified Microsoft Instructor, Ken has focused his career on various security aspects of computer and network technology since the early 1980s. He has offered a wide variety of IT training and high level consulting projects for Fortune 500 companies globally. Through the course of his extensive career, he has taught a full line of Microsoft, CompTIA, Cisco, and other high level IT Security curricula.

Prerequisites: This is part 3 in the series.

Runtime: 03:52:34

Course description: Interconnecting Cisco Networking Devices Part 1 is the exam associated with the Cisco Certified Entry Network Technician (CCENT) certification or the first half of the Cisco Certified Network Associate Routing and Switching (CCNA Routing and Switching). Managing Network device security is important. This course will cover, passwords, securing administrative access, hardening devices, access control lists and traffic filtering.

Course outline:

Securing Administative Access
- Introduction
- Securing Administrative Access
- Securing Remote Access
- Service Password Encryption
- Securing Physical Access
- Securing VTY Lines
- Using SSH
- Verify SSH Configuration
- Remote Access Reply
- SSH
- Encryption Process
- Configuration Steps
- Using ACL for Remote Access Security
- Other Authentication Options
- Using the Login Banner
- Summary
- Summary

Implementing Device Hardening
- Introduction
- Implementing Device Hardening
- How to Disable a Port
- Port Security
- How to Configure Port Security
- Verify Port Security
- Verify Port Security Continued
- Turning off Unused Services
- Turning off Unused Services Continued
- NTP
- How to Configure NTP
- Verify NTP
- AAA
- Authentication
- Authentication Continued
- AAA Configuration
- Authentication Servers
- AAA Configuration Continued
- Summary
- Summary

Implementing Traffic Filtering with ACLs
- Introduction
- Filtering Traffic with ACLs
- How an Outbound ACL Functions
- How to Apply an ACL to an Interface
- Introducing the Extended ACL
- Creating a Numbered Extended ACL
- Using a Named ACL
- Configuration Guidelines
- Monitoring ACLs
- Troubleshooting ACL Take 1 and 2
- Troubleshooting ACL Take 3 and 4
- Troubleshooting ACL Take 5 and 6
- Troubleshooting ACL Take 7
- Summary
- Demo: Configure CLI
- Demo: Sessions
- Demo: Encrypt Passwords
- Summary

Traffic Filtering Demo Part 1
- Introduction
- Demo: Enable SSH
- Demo: Repeat SSH Enabling
- Demo: Limit Remote Access
- Demo: Add Login Banner
- Demo: Banner of the Day
- Demo: Shut Down Ports
- Demo: Repeat Shut Down Ports
- Demo: Port Security
- Demo: Port Security Options
- Demo: Disable Unused Services
- Demo: NTP Connection
- Summary

Traffic Filtering Demo Part 2
- Introduction
- Demo: Extended ACL
- Demo: Troubleshoot ACL
- Demo: SSH
- Demo: Local User
- Demo: NTP
- Demo: Authenticate NTP
- Demo: RADIUS
- Demo: Locate DHCP Servers
- Demo: Locate DHCP Servers Continued
- Summary