Cisco IP Switched Networks (CCNP Switch), Part 7 of 7: Security

page 1

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 7 in the series.

Runtime: 01:39:53

Course description: This courses discusses the importance of layer 2 security to the integrity of your network. Topics include: best practices, rogue devices, port security and ARP Spoofing.

Course outline:

Security Best Practices
- Introduction
- OSI Layers Security
- Layer 2 Security
- Best Practices
- Best Practices Continued
- Rogue Devices
- Layer 2 Attacks
- Summary

Port Security
- Introduction
- MAC Flooding eNotes
- Port Security eNotes
- Demo: Create Network
- Demo: Port Security
- Port Errors
- Port-Based ACL
- Storm Control
- Demo: Storm Control
- AAA Framework
- Authentication
- RADIUS and TACACS
- Summary

RADIUS and TACACS
- Introduction
- RADIUS and TACACS+
- RADIUS and TACACS+ eNotes
- Demo: AAA Configuration Options
- Demo: AAA Groups
- Limitations
- Physical Security
- 802.1x
- 802.1x eNotes
- 802.1x Configuration
- Summary

DHCP Spoofing
- Introduction
- DHCP Spoofing Attacks eNotes
- Cisco DHCP Spoofing eNotes
- IP Source Guard
- ARP Spoofing eNotes
- DAI
- Dynamic Trunking Protocol
- VLAN Hopping
- VACLs
- Why PVLANs eNotes
- Isolated Ports
- Protected Ports
- Summary