CISCO NETWORKING ACADEMY PROGRAM CURRICULUM
SCOPE & SEQUENCE

Semester 3 version 2.1

Course Description:

The Cisco Networking Academy Program consists of four semesters. The program is designed to teach students the skills they will need to design, build, and maintain small to medium size networks. This provides them with the opportunity to enter the workforce and/or further their education and training in the computer networking field.

CHAPTER 1

Upon completion of this chapter, students will be able to perform tasks related to:

The OSI Reference Model and the Problems It Solves

- The layered network model: the OSI Reference Model
- The OSI Model layers
- Peer-to-peer communication

The Physical Layer of the OSI Reference Model

- Three categories of Ethernet
- Three varieties of 10 Mbps Ethernet

The Data Link Layer of the OSI Reference Model

- Lock analogy for NICs
- Data transport across the physical link connecting hosts, routers, and other devices
- Network Layer Functions
- Layer 3 protocols of the TCP/IP stack
- Network and subnetwork addresses in the IP
- Path determination in the contexts of packets and routers
- Why Layer 3 addresses must contain both path and host information
- Types of ICMP messages
- ping command
- ARP

Routing and the Different Classes of Routing Protocols

- Routing in a mixed LAN-media environment
- Two basic operations a router performs
- Static and dynamic routes
- Default route
- Routed and routing protocols
- Information that routers use to perform their basic functions
- IP routing protocols
- Network convergence
- Distance-vector routing
- Link-state routing
- Distance-vector and link-state routing
- Enabling an IP routing process
- Configuring RIP

The Transport Layer of the OSI Reference Model

- Routing in a mixed LAN-media environment
- Layer 4 segmentation
- The three-way handshake
- Why is a buffer used in data communications
- Windowing
- Explain reliability via acknowledgment

CHAPTER 2

Upon completion of this chapter, students will be able to perform tasks related to:

Various LAN Communication Problems

- Factors putting pressure on network performance
- Elements of Ethernet/802.3 networks
- Half-duplex Ethernet
- Network congestion
- Network latency
- Ethernet 10BaseT transmission time
- The benefits of using repeaters

Full-Duplex Transmitting, the Ethernet Standard, and LAN Segmentation

- Full-duplex Ethernet
- LAN segmentation
- LAN segmentation with bridges
- The pros and cons of LAN segmentation with routers
- The pros and cons of LAN segmentation with switches

Switching and VLANs

- Describe the two basic operations of a switch
- Ethernet switch latency
- Layer 2 and Layer 3 switching
- Microsegmentation
- How a switch learns addresses
- Benefits of LAN switching
- Symmetric and asymmetric switching
- Memory buffering
- Two switching methods
- How to set up VLANs

The Spanning-Tree Protocol

- Overview of the Spanning-Tree Protocol
- Describe the five Spanning-Tree Protocol states

CHAPTER 3

Upon completion of this chapter, students will be able to perform tasks related to:

VLANs

- Existing Shared LAN Configurations

Segmentation with Switching Architecture

- Grouping geographically separate users into networkwide virtual topologies
- Differences between traditional switched LANs and VLANs
- The transport of VLANs across backbones
- The role of routers in VLANs
- How frames are used in VLANs

VLAN Implementation

- The relationship between ports, VLANs, and broadcasts
- Why port-centric VLANs make an administrator's job easier
- Static VLAN
- Dynamic VLAN

Benefits of VLANs

- How VLANs make adds, moves, and changes easier
- How VLANs help control broadcast activity

- How VLANs can improve network security
- How VLANs can save money

CHAPTER 4

Upon completion of this chapter, students will be able to perform tasks related to:

LAN Network Design Goals and Components
- LAN Design goals
- Critical components of LAN Design
- The function and placement of servers when designing a network
- Intranet
- Why contention is an issue with Ethernet
- How broadcast domains relate to segmentation
- The difference between bandwidth and broadcast domains

Network Design Methodology
- Gathering and analyzing requirements
- Factors that affect network availability
- Physical topologies used in networking

Layer 1 Design
- Designing the Layer 1 topology: signaling method, medium type, and maximum length
- Diagramming a standards-based Ethernet cable run from the workstation to the HCC, including distances
- HCC, VCC, MDF, IDF and POP
- 10BaseT and 100BaseT Ethernet.
- Elements of a logical topology diagram

Layer 2 Design
- Common Layer 2 devices and their impact on network domains
- Asymmetric switching
- The effect microsegmentation can have on a network
- Determining the number of cable runs and drops
- Determining the size of collision domains in hubbed and switched networks
- Diagramming hub placement in a standards-based extended star topology
- Migrating a network from 10 Mbps to 100 Mbps

Layer 3 Design
- Using routers as the basis for Layer 3 network design
- How VLANs can create smaller broadcast domains
- Explain how a router provides structure to a network
- Why large, scalable LANs need to incorporate routers
- Diagramming a standards-based LAN that uses routers
- Logical and physical network maps

CHAPTER 5

Upon completion of this chapter, students will be able to perform tasks related to:

The Network Layer Basics
- Explain path determination
- Path determination
- The operation of routing tables
- Metrics
- Router forwarding decisions

Routed and Routing Protocols
- Routing protocols

- Multiprotocol routing

IP Routing Protocols
- Differentiating one routing protocol from another
- Describe five goals of routing protocols
- Routing loops
- Static and dynamic routing
- Classifications of routing protocols
- IP routing configuration: choosing a routing protocol

IGRP Operation
- IGRPs metrics
- Differentiating amongst interior system and exterior routes
- Write out a correct command sequence for enabling IGRP on a router
- Describe three features of IGRP which enhance its stability
- IGRP metrics and routing updates
- The maximum hop count of IGRP

CHAPTER 6

Upon completion of this chapter, students will be able to perform tasks related to:

Access Control Lists (ACLs)
- What are ACLs
- Reasons to create ACLs
- Testing packets with ACLs
- How ACLs work
- Flowchart of the ACL test matching process

ACL Configuration Tasks
- Creating ACLs
- The purpose and function of wildcard mask bits
- The any command
- The host command

Standard ACLs
- What are standard ACLs
- Writing a valid standard ACL command using all available parameters
- How to verify access control lists
- Writing a standard ACL to permit traffic from a source network
- Writing a standard ACL to deny a specific host
- Writing a standard ACL to deny a specific subnet

Extended ACLs
- What are extended ACLs
- Extended ACL parameters
- UDP and TCP port numbers
- Writing an ACL for denying FTP on an Ethernet interface
- Writing an ACL which denies Telnet out of an Ethernet port and permits all other traffic

Named ACLs
- Configuring named ACLs
- The deny command
- The permit command

Using ACLs with Protocols
- Protocols for which ACLs can be created

Placing ACLs
- Rule: "Putting the ACL as close as possible to the source of the traffic denied"

- Using ACLs in firewall routers
- A firewall architecture to protect you from intruders

Verifying ACLs
- How to verify ACLs and interpret the output

CHAPTER 7

Upon completion of this chapter, students will be able to perform tasks related to:

Cisco Routers in Netware Networks
- The Novell IPX protocol suite
- IPX features
- IPX addressing

Novell Encapsulation
- NetWare Ethernet encapsulation terms
- The IOS encapsulation names for Ethernet, FDDI, and Token Ring
- The IPX packet format

Novell Routing
- Novell RIP
- Service advertising protocol
- Get nearest Server protocol

Novell IPX Configuration
- Novell Configuration Tasks
- Writing a valid IOS command sequence to assign IPX network numbers to interfaces
- Writing a valid IOS command for monitoring and troubleshooting IPX

Monitoring and Managing an IPX Network
- Writing a valid IOS command for monitoring the status of an IPX interface
- Writing a valid IOS command sequence to monitor IPX routing tables
- Writing a valid IOS command sequence for monitoring Novell IPX servers
- Writing a valid IOS command to monitor IPX traffic, and describe some of the field options for that command
- Writing a valid IOS command for troubleshooting IPX routing
- Writing a valid IOS command for troubleshooting IPX SAP
- Using the privileged IPX ping command
- Using the user IPX IPX ping command

CHAPTER 8

Upon completion of this chapter, students will be able to perform tasks related to:

Network Documentation
- Cut sheet diagrams
- MDF & IDF layouts
- Server and workstation configuration details
- Software listings
- Maintenance records
- Security measures
- User policies

Network Security
- Network access
- Data recovery
- Backup operations
- Redundancy techniques

Planning Structured Cabling: Identifying Potential Wiring Closets

- Static, dust, dirt, and heat
- Power conditioning
- EMI and FRI
- Software viruses

Network Performance

- Network baseline, updates, and change verification

Server Administration

- Peer-to-peer
- Clilent-srver
- Network control

Network Troubleshooting

- Scientific method
- Analyze network troubleshooting