Cisco Networking Academy CCNA Semester 3

Chapter 1: The OSI Reference Model and Routing
Chapter 2: LAN Switching
Chapter 3: VLANS
Chapter 4: LAN Design
Chapter 5: Routing Protocols: IGRP
Chapter 6: ACLs
Chapter 7: Novell IPX
Chapter 8: Network Management

Cisco Networking Academy CCNA Semester 3

Chapter 1: The OSI Reference Model and Routing

1.1 The OSI Reference Model and the Problems It Solves
1.2 The Physical Layer of the OSI Reference Model
1.3 The Data Link Layer of the OSI Reference Model
1.4 Network Layer Functions
1.5 Routing and the Different Classes of Routing Protocols
1.6 The Transport Layer of the OSI Reference Model

Chapter 2: LAN Switching

2.1 Various LAN Communication Problems
2.2 Full-Duplex Transmitting, Fast Ethernet Standard and LAN Segmentation
2.3 Switching and VLANs
2.4 The Spanning-Tree Protocol

Chapter 3: VLANS

3.1 VLANs
3.2 Segmentation with switching architectures
3.3 VLAN Implementation
3.4 Benefits of VLANs

Chapter 4: LAN Design

4.1 LAN Design Goals and Components
4.2 Network Design Methodology
4.3 Layer 1 Design
4.4 Layer 2 Design
4.5 Layer 3 Design

Chapter 5: Routing Protocols: IGRP

5.1 The Network Layer Basics
5.2 Routed and Routing Protocols
5.3 IP Routing Protocols
5.4 IGRP Operation

Chapter 6: ACLs

6.1 Access Control Lists (ACLs)
6.2 ACL Configuration Tasks
6.3 Standard ACLs
6.4 Extended ACLs
6.5 Named ACLs
6.6 Using ACLs with protocols
6.7 Placing ACLs
6.8 Verifying ACLs

Chapter 7: Novell IPX

7.1 Cisco Routers in Netware Networks
7.2 Novell Encapsulation
7.3 Novell Routing
7.4 Novell IPX Configuration
7.5 Monitoring and Managing an IPX Network

Chapter 8: Network Management

8.1 Network Documentation
8.2 Network Security
8.3 Environmental Factors
8.4 Network Performance
8.5 Server Administration
8.6 Network troubleshooting

Cisco Networking Academy CCNA Semester 3

Chapter 1: The OSI Reference Model and Routing

1.1 The OSI Reference Model and the Problems It Solves

1.1.1 The layered network model: The OSI reference model
1.1.2 The OSI model layers
1.1.3 Peer-to-peer communication
1.1.4 Encapsulation

1.2 The Physical Layer of the OSI Reference Model

1.2.1 Three categories of Ethernet
1.2.2 Three varieties of 10Mbps Ethernet

1.3 The Data Link Layer of the OSI Reference Model

1.3.1 Lock analogy for NICs
1.3.2 Data transport across the physical link connecting hosts, routers, and other devices

1.4 Network Layer Functions

1.4.1 Layer 3 protocols of the TCP/IP stack
1.4.2 Network and subnetwork addresses in the IP
1.4.3 Path determination in the contexts of packets and routers
1.4.4 Why Layer 3 addresses must contain both path and host information
1.4.5 Types of ICMP messages
1.4.6 ping command
1.4.7 ARP

1.5 Routing and the Different Classes of Routing Protocols

1.5.1 Routing in a mixed LAN-media environment
1.5.2 Two basic operations a router performs
1.5.3 Static and dynamic routes
1.5.4 Default route
1.5.5 Routed and routing protocols
1.5.6 Information that routers use to perform their basic functions
1.5.7 IP routing protocols
1.5.8 Network convergence
1.5.9 Distance vector routing
1.5.10 Link-state routing
1.5.11 Distance vector and link state routing
1.5.12 Enabling an IP routing process
1.5.13 Configuring RIP

1.6 The Transport Layer of the OSI Reference Model

1.6.1 "Reliable" transport
1.6.2 Layer 4 segmentation
1.6.3 The three-way handshake
1.6.4 Why is a buffer used in data communications
1.6.5 Windowing
1.6.6 Explain reliability via acknowledgment

Chapter 2: LAN Switching

2.1 Various LAN Communication Problems

2.1.1 Factors that impact on network performance
2.1.2 Elements of Ethernet/802.3 networks
2.1.3 Half-duplex Ethernet
2.1.4 Network congestion
2.1.5 Network latency

2.1.6 Ethernet 10BASE-T transmission time
2.1.7 The benefit of using repeaters

2.2 Full-Duplex Transmitting, Fast Ethernet Standard and LAN Segmentation
2.2.1 Full-duplex Ethernetl
2.2.2 LAN segmentationl
2.2.3 LAN segmentation with bridges
2.2.4 The pros and cons of LAN segmentation with routers
2.2.5 Pros and cons of LAN segmentation with switches

2.3 Switching and VLANs
2.3.1 Describe the two basic operations of a switch
2.3.2 Ethernet switch latency
2.3.3 Layer 2 and Layer 3 switching
2.3.4 Microsegmentation
2.3.5 How a switch learns addresses
2.3.6 Benefits of LAN switching
2.3.7 Symmetric and asymmetric switching
2.3.8 Memory buffering
2.3.9 Two switching methods
2.3.10 How to set up VLANs

2.4 The Spanning-Tree Protocol
2.4.1 Overview of the spanning-tree protocol
2.4.2 Describe the five spanning-tree protocol states

Chapter 3: VLANS

3.1 VLANs
3.1.1 Existing shared LAN configurations

3.2 Segmentation with switching architectures
3.2.1 Grouping geographically separate users into network-wide virtual topologies
3.2.2 Differences between traditional switched LAN and VLANs
3.2.3 The transport of VLANs across backbones
3.2.4 The role of routers in VLANs
3.2.5 How frames are used in VLANs

3.3 VLAN Implementation
3.3.1 The relationship between ports, VLANs, and broadcasts
3.3.2 Why port-centric VLANs make an administrator's job easier
3.3.3 Static VLANs
3.3.4 Dynamic VLANs

3.4 Benefits of VLANs
3.4.1 How VLANs make additions, moves, and changes easier
3.4.2 How VLANs help control broadcast activity
3.4.3 How VLANs can improve network security
3.4.4 How VLANs can save money

Chapter 4: LAN Design

4.1 LAN Design Goals and Components
4.1.1 LAN design goals
4.1.2 Critical components of LAN Design
4.1.3 The function and placement of servers when designing a network
4.1.4 Intranet
4.1.5 Why contention is an issue with Ethernet

4.1.6 How broadcast domains relate to segmentation
4.1.7 The difference between bandwidth and broadcast domains

4.2 Network Design Methodology
4.2.1 Gathering and analyzing requirements
4.2.2 Factors that affect network availability
4.2.3 Physical topologies used in networking

4.3 Layer 1 Design
4.3.1 Designing the Layer 1 Topology : signaling method, medium type, and maximum length
4.3.2 Diagramming a standards-based Ethernet cable run from the workstation to the HCC, including distances
4.3.3 HCC, VCC, MDF, IDF, and POP
4.3.4 10BASE-T and 100BASE-TX Ethernet
4.3.5 Elements of a logical topology diagram

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

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

Chapter 5: Routing Protocols: IGRP

5.1 The Network Layer Basics
5.1.1 Explain path determination
5.1.2 Path determination
5.1.3 The operation of routing tables
5.1.4 Metrics
5.1.5 Router forwarding decisions

5.2 Routed and Routing Protocols
5.2.1 Routing Protocols
5.2.2 Multiprotocol routing

5.3 IP Routing Protocols
5.3.1 Differentiating one routing protocol from another
5.3.2 The goals of routing protocols
5.3.3 Routing loops
5.3.4 Static and dynamic routing
5.3.5 Classifications of routing protocols
5.3.6 IP Routing Configuration: Choosing a routing protocol

5.4 IGRP Operation
5.4.1 IGRP's Metrics

5.4.2 Differentiating from interior, system, and exterior routes
5.4.3 Write out a correct command sequence for enabling IGRP on arouter
5.4.4 Describe three features of IGRP which enhance its stability
5.4.5 IGRP metrics and routing updates
5.4.6 The maximum hop count of IGRP

Chapter 6: ACLs

6.1 Access Control Lists (ACLs)
6.1.1 What are ACLs
6.1.2 Reasons to create ACLs
6.1.3 Testing packets with ACLs
6.1.4 How ACLs work
6.1.5 Flowchart of the ACL test matching process

6.2 ACL Configuration Tasks
6.2.1 Creating ACLs
6.2.2 The purpose and function of wildcard mask bits
6.2.3 The any command
6.2.4 The host command

6.3 Standard ACLs
6.3.1 What are standard ACLs
6.3.2 Writing a valid standard ACL command using all available parameters
6.3.3 How to verify access lists
6.3.4 Writing a standard ACL to permit traffic from a source network
6.3.5 Writing a standard ACL to deny a specific host
6.3.6 Writing a standard ACL to deny a specific subnet

6.4 Extended ACLs
6.4.1 What are extended ACLs
6.4.2 Extended ACL parameters
6.4.3 UDP and TCP port numbers
6.4.4 Writing an ACL for denying FTP on an Ethernet interface
6.4.5 Writing an ACL that denies Telnet out of an Ethernet port and permits all other traffic

6.5 Named ACLs
6.5.1 Configuring named ACLs
6.5.2 The deny command
6.5.3 The permit command

6.6 Using ACLs with protocols
6.6.1 Protocols for which ACLs can be created

6.7 Placing ACLs
6.7.1 Rule: "Putting the extended ACL as close as possible to the source of traffic denied"
6.7.2 Using ACLs in firewall routers
6.7.3 A firewall architecture to protect you from intruders

6.8 Verifying ACLs
6.8.1 How to verify ACLs and interpret the output

Chapter 7: Novell IPX

7.1 Cisco Routers in Netware Networks
7.1.1 The Novell IPX protocols suite
7.1.2 IPX features

7.1.3 IPX addressing

7.2 Novell Encapsulation
7.2.1 Netware Ethernet encapsulation terms
7.2.2 The IOS encapsulation names for Ethernet, FDDI, and Token Ring
7.2.3 The IPX packet format

7.3 Novell Routing
7.3.1 Novell RIP
7.3.2 Service advertising protocol
7.3.3 Get nearest server protocol

7.4 Novell IPX Configuration
7.4.1 Novell IPX configuration tasks
7.4.2 Writing a valid IOS command sequence to assign IPX network numbers to interface
7.4.3 Writing a valid IOS commands for monitoring and troubleshooting IPX

7.5 Monitoring and Managing an IPX Network
7.5.1 Writing a valid IOS commands for monitoring the status of an IPX interface
7.5.2 Writing a valid IOS command sequence to monitor IPX routing tables
7.5.3 Writing a valid IOS command sequence for monitoring Novell IPX servers
7.5.4 Writing a valid IOS command to monitor IPX traffic, and describe some of the field options for that command
7.5.5 Writing a valid IOS command for troubleshooting IPX routing
7.5.6 Writing a valid IOS command for troubleshooting IPX SAP
7.5.7 Using the privileged IPX ping command
7.5.8 Using the user IPX IPX ping command

Chapter 8: Network Management

8.1 Network Documentation
8.1.1 Cut sheet diagrams
8.1.2 MDF and IDF layouts
8.1.3 Server and workstation configuration details
8.1.4 Software listings
8.1.5 Maintenance records
8.1.6 Security measures
8.1.7 User policies

8.2 Network Security
8.2.1 Network access
8.2.2 Data recovery
8.2.3 Back up operations
8.2.4 Redundancy Techniques

8.3 Environmental Factors
8.3.1 Static, Dust, Dirt and Heat
8.3.2 Power conditioning
8.3.3 EMI and RFI
8.3.4 Software Viruses

8.4 Network Performance

8.4.1 Network Baseline, updates and change verification

8.5 Server Administration

8.5.1 Peer-to-Peer
8.5.2 Client-Server
8.5.3 Network Control

8.6 Network troubleshooting

8.6.1 Scientific method
8.6.2 Analyze Network Troubleshooting