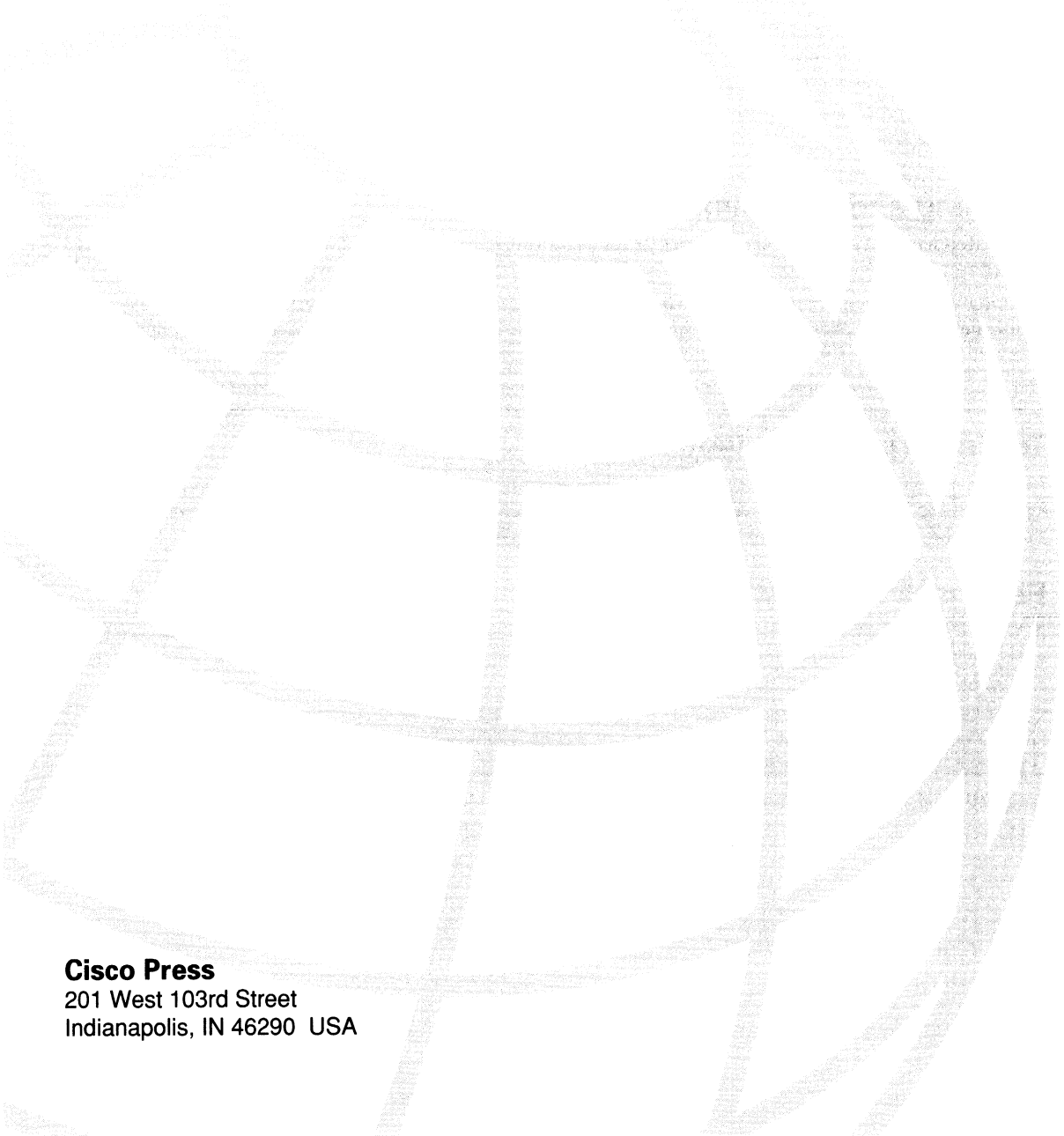
Cisco Press Certification Folio



Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

Cisco Press Certification Folio

Published by:
Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

ISBN: 1-58720-049-X

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	John Wait
Executive Editor	John Kane
Cisco Systems Program Manager	Bob Anstey
	Bill Warren
Managing Editor	Patrick Kanouse
Production Editor	Marc Fowler
Compositor	Steve Gifford

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
http://www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
http://www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Contents at a Glance

Contents

Excerpt from Interconnecting Cisco Network Devices

Excerpt from Cisco CCNA Exam #640-507 Certification Guide

Excerpt from Designing Cisco Networks

Excerpt from CCDA Exam Certification Guide

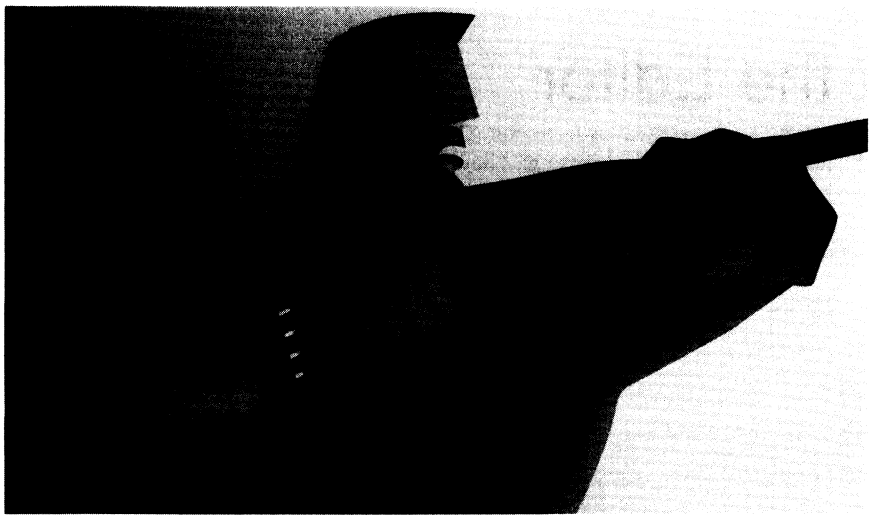
Excerpt from Building Scalable Cisco Networks

Excerpt from CCNP Routing Exam Certification Guide

Excerpt from CCNP Switching Exam Certification Guide

Excerpt from CCNP Remote Access Exam Certification Guide

Excerpt from CCNP Support Exam Certification Guide



from Interconnecting Cisco Network Devices
by Steve McQuerry

(1-57870-111-2)

Cisco Press

About the Editor

Steve McQuerry is a Certified Cisco Systems Instructor (CCSI) who works as a contract instructor and consultant throughout the U.S., teaching networking professionals how to configure and integrate Cisco equipment into their networks. Steve also holds CNE, MCSE, MCT, CCNP, and CCNA certifications. He has worked in the networking industry for over 10 years and has experience with multiple protocols in small and large networks, including TCP/IP and IPX. Steve currently teaches the Cisco courses ICND, ACRC, CIT, and CLSC with Global Knowledge.

Contents at a Glance

Bold chapters are elements included in this folio

Upon completion of this chapter, you will be able to perform the following tasks:

- Identify what a VLAN is and how it operates.
- Configure a VLAN to improve network performance.
- Identify what role the switch plays in the creation of VLANs.
- Identify how network devices communicate about VLANs.
- Configure the Catalyst 1900 for VLAN operation.

CHAPTER 6

Extending Switched Networks with Virtual LANs

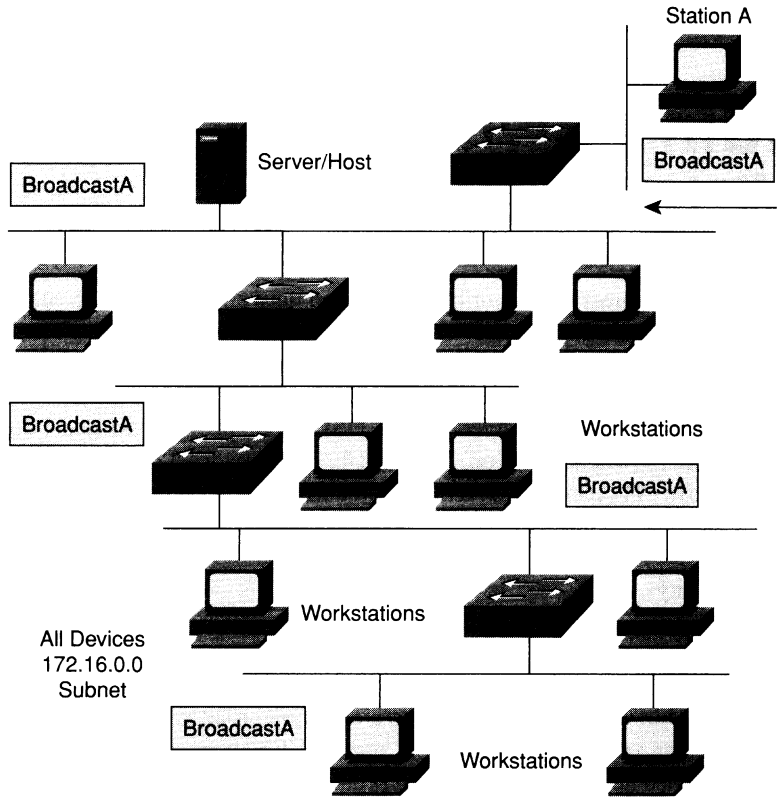
The nature and function of a bridged/switched network is to provide enhanced network services by segmenting the network into multiple collision domains. The fact remains, however, that without any other mechanism, the bridged/switched network is still a single broadcast domain. It is important to control broadcast propagation throughout the network. Routers, which operate at Layer 3 of the OSI model, provide broadcast domain segmentation. Switches also provide a method of broadcast domain segmentation called *virtual LANs* (VLANs). A VLAN is defined as a broadcast domain.

The benefits of VLANs include the following:

- Security
- Segmentation
- Flexibility

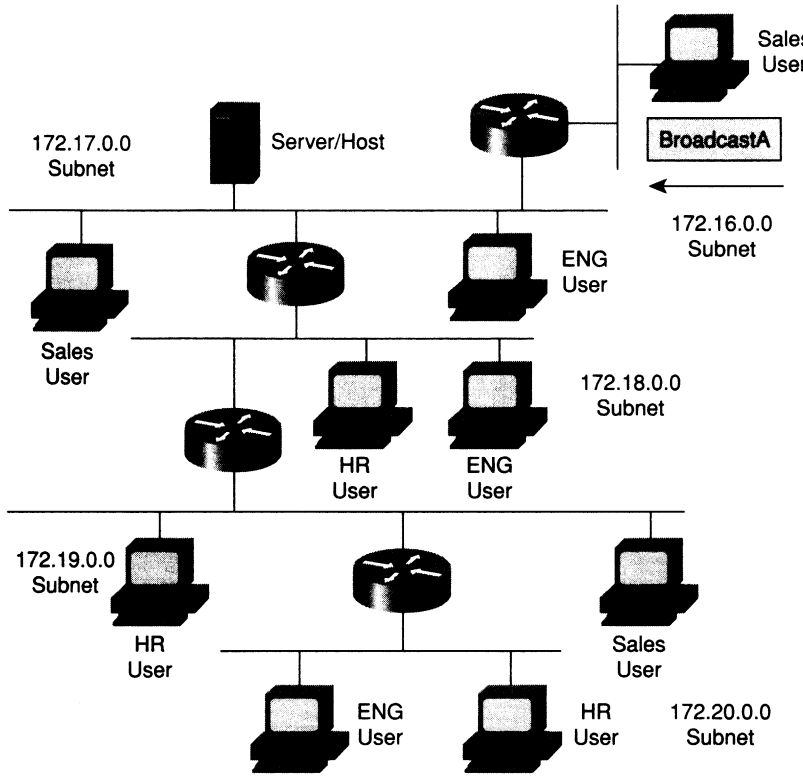
VLANs enable you to group users into a common broadcast domain regardless of their physical location in the internetwork. Creating VLANs improves performance and security in the switched network by controlling broadcast propagation. In a broadcast environment, a broadcast sent out by a host on a single segment would propagate to all segments, saturating the bandwidth of the entire network, as shown in Figure 6-1. Also, without forcing some method of checking at an upper layer, all devices in the broadcast domain would be able to communicate via Layer 2. This severely limits the amount of security that could be enforced on the network.

Figure 6-1 *Broadcast Propagation*



Before the introduction of switches and VLANs, networks were divided into multiple broadcast domains by connectivity through a router. Because routers do not forward broadcasts, each interface is in a different broadcast domain. Figure 6-2 shows a network broken into multiple broadcast domains using routers. Notice that each segment is an individual IP subnet and that regardless of a workstation's function, its subnet is defined by its physical location.

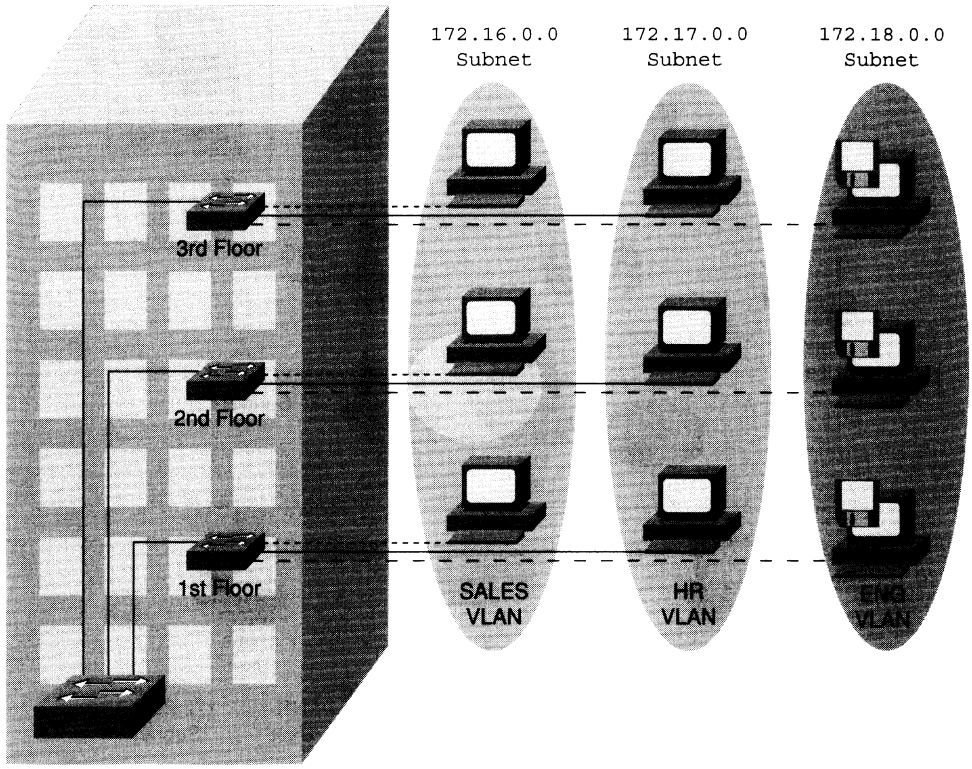
Figure 6-2 *Multiple Broadcast Domains Using Routers*



A VLAN is a logical broadcast domain that can span multiple physical LAN segments. A VLAN can be designed to provide independent broadcast domains for stations logically segmented by functions, project teams, or applications without regard to the physical location of users. Each switch port can be assigned to only one VLAN. Ports in a VLAN share broadcasts. Ports that do not belong to the same VLAN do not share broadcasts. This control of broadcast improves the network's overall performance.

VLANs enable switches to create multiple broadcast domains within a switched network, as illustrated in Figure 6-3. Notice that now all users in a given group (department in this example) are defined to be in the same VLAN. Any user in this VLAN would receive a broadcast from any other member of the VLAN, users of other VLANs would not receive these broadcasts. Each of the users in a given VLAN would also be in the same IP subnet. This is different from the broadcast domains of Figure 6-2, in which the physical location of the device determines the broadcast domain.

Figure 6-3 *VLAN Overview*



Within the switched internetwork, VLANs provide segmentation and organizational flexibility. Using VLAN technology, you can group switch ports and their connected users into logically defined communities of interest, such as coworkers in the same department, a cross-functional product team, or diverse user groups sharing the same network application.

A VLAN can exist on a single switch or span multiple switches. VLANs can include stations in a single building or multiple-building infrastructures. In rare and special cases, they can even connect across wide-area networks (WANs).

VLAN Concepts

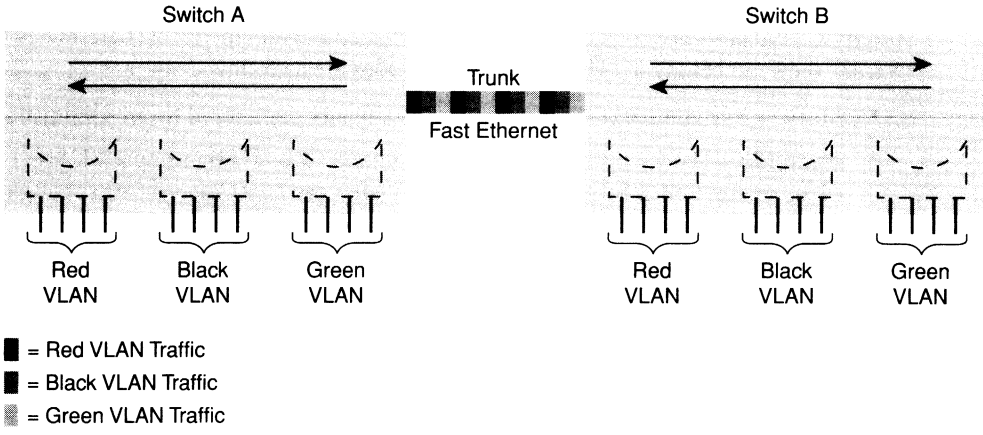
As mentioned previously, prior to the VLAN, the only way to control broadcast traffic was through segmentation using routers. VLANs are an extension of the switched network. By having the ability to place segments (ports) in individual broadcast domains, you can

control where a given broadcast will be forwarded. The following sections expand on these concepts. Basically, each switch acts independently of other switches in the network. With the concept of VLANs, a level of interdependence is built into the switch fabric. The characteristics of a typical VLAN setup are as follows:

- Each logical VLAN is like a separate physical bridge.
- VLANs can span multiple switches.
- Trunks carry traffic for multiple VLANs.

Now each switch can distinguish traffic from different broadcast domains. Each forwarding decision is based on which VLAN the packet came from; therefore, each VLAN acts like an individual bridge within a switch. In order to bridge/switch between switches, you must either connect each VLAN independently (that is, dedicate a port per VLAN) or have some method of maintaining and forwarding the VLAN information with the packets. A process called *trunking* allows this single connection. Figure 6-4 illustrates a typical VLAN setup in which multiple VLANs span two switches interconnected by a Fast Ethernet trunk.

Figure 6-4 *Multiple VLANs Can Span Multiple Switches*



How VLANs Operate

A Catalyst switch operates in your network like a traditional bridge. Each VLAN configured on the switch implements address learning, forwarding/filtering decisions, and loop avoidance mechanisms as if it were a separate physical bridge. This VLAN might include several ports.

Internally, the Catalyst switch implements VLANs by restricting data forwarding to destination ports in the same VLAN as originating ports. In other words, when a frame arrives on a switch port, the Catalyst must retransmit the frame only to a port that belongs

to the same VLAN. The implication is that a VLAN operating on a Catalyst switch limits transmission of unicast, multicast, and broadcast traffic. Flooded traffic originating from a particular VLAN floods out only other ports belonging to that VLAN. This means that each VLAN is an individual broadcast domain.

Normally, a port carries traffic only for the single VLAN it belongs to. In order for a VLAN to span multiple switches on a single connection, a trunk is required to connect two switches. A trunk carries traffic for all VLANs, as demonstrated earlier in Figure 6-4. A trunk port can only be configured on the Fast Ethernet ports on the Catalyst 1900 switches.

VLAN Membership Modes

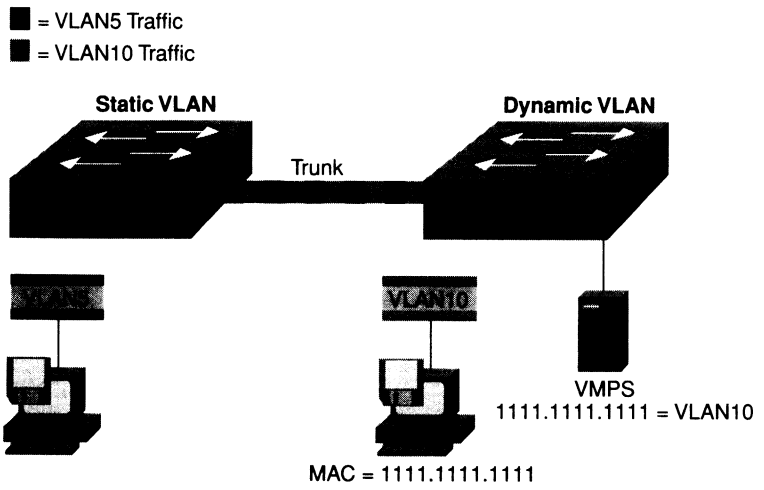
VLANs are a Layer 2 implementation in the switch fabric of your network. Because they are implemented at the data link layer, they are protocol-independent. In order to put a given port (segment) into a VLAN, you must assign that membership on the switch. After you define a port to a given VLAN, broadcast and unicast traffic from that segment will be forwarded by the switches only to ports in the same VLAN. If you need to communicate between VLANs, you need to add a router and a Layer 3 protocol to your network.

Catalyst 1900 ports are configured with a VLAN membership mode that determines which VLAN they can belong to. The membership modes are as follows:

- **Static**—Assignment of VLAN to port is statically configured by an administrator.
- **Dynamic**—The Catalyst 1900 supports dynamic VLANs by using a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 5000 or an external server. The Catalyst 1900 cannot operate as the VMPS. The VMPS contains a database that maps MAC addresses to VLAN assignment. When a frame arrives on a dynamic port at the Catalyst 1900, the Catalyst 1900 queries the VMPS for the VLAN assignment based on the source MAC address of the arriving frame.

A dynamic port can belong to only one VLAN at a time. Multiple hosts can be active on a dynamic port only if they all belong to the same VLAN. Figure 6-5 demonstrates the static and dynamic VLAN membership modes.

Figure 6-5 *VLAN Membership Modes*



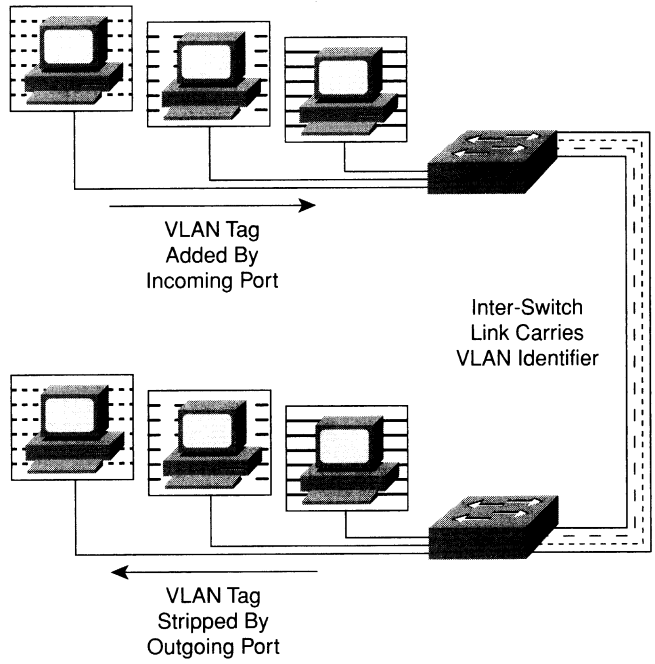
Inter-Switch Links

This chapter discusses the functionality of Inter-Switch Link (ISL) tagging and how it is used to intercommunicate VLAN information between switches. ISL trunks enable VLANs across a switched network backbone. The fundamental characteristics of ISLs include the following:

- Performed with ASIC.
- Not intrusive to client stations; client does not see the ISL header.
- Effective between switches, routers and switches, and switches and servers with ISL network interface cards.

Figure 6-6 illustrates how an ISL functions across switches.

Figure 6-6 *ISL Tagging*



The following sections address ISL tagging and ISL encapsulation.

ISL Tagging

ISL is a Cisco proprietary protocol used to interconnect multiple switches and to maintain VLAN information as traffic goes between switches. ISL provides VLAN capabilities while maintaining full wire-speed performance over Fast Ethernet links in full- or half-duplex mode. ISL operates in a point-to-point environment. The purpose of ISL is to maintain VLAN information. This function allows a switch to forward information about which VLAN traffic originated from as it is being passed from one switch to another.

The ISL frame tagging used by the Catalyst series of switches is a low-latency mechanism for multiplexing traffic from multiple VLANs on a single physical path. It has been implemented for connections between switches, routers, and network interface cards used on nodes such as servers. To support the ISL feature, each connecting device must be ISL-capable. A router that is ISL-configured is used to allow inter-VLAN communications. This is discussed in more detail in the next chapter. A non-ISL device that receives ISL-encapsulated Ethernet frames might consider them to be protocol errors if the size of the header plus the data frame exceeds the maximum transmission unit (MTU) size

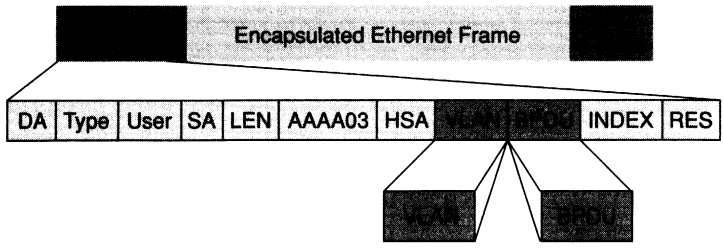
(1500 bytes) of a normal Ethernet frame. Devices that understand and can decode ISL packets do not have a problem with the size or format of these frames.

ISL Encapsulation

ISL functions at OSI Layer 2 by encapsulating a data frame with a new (ISL) header and cyclic redundancy check (CRC). ISL encapsulated frames are passed over trunk lines. ISL is protocol-independent because the data frame might carry any upper-layer protocol. Administrators use ISL to maintain redundant links and load-balance traffic between parallel links using the Spanning-Tree Protocol.

Ports configured as ISL trunks encapsulate each frame with a 26-byte ISL header and a 4-byte CRC before sending it out the trunk port. Because ISL technology is implemented in ASICs, frames are tagged at wire speed. The number of VLANs supported by a switch depends on the switch hardware. The Catalyst 1900 supports 64 VLANs with a separate Spanning Tree instance per VLAN. The ISL header supports 10 bits for ISL identification, allowing for the 1024 unique VLANs. Although a Catalyst 1900 can pass information for 1024 VLANs across a trunk line, it can support Spanning Tree for only the first 64 VLANs (1 through 64). Because there are only 27 ports on a Catalyst 1900, it could have ports in only 27 different VLANs, but it could pass traffic for any VLAN because it supports all 10 fields of the ISL header. You could create and add a port to a VLAN numbered above 65, but it would not support a Spanning Tree instance for that VLAN. This could cause bridge loops, which would cause serious network problems. It is therefore stated that the switch supports 64 active VLANs. Figure 6-7 illustrates a typical ISL encapsulated data frame.

Figure 6-7 *ISL Encapsulation*



As illustrated in Figure 6-7, the ISL frame header contains the following information fields:

- **DA**—48-bit multicast destination address.
- **Type**—4-bit descriptor of the encapsulated frame types—Ethernet (0000), Token Ring (0001), FDDI (0010), and ATM (0011).
- **User**—4-bit descriptor used as the type field extension or to define Ethernet priorities. This is a binary value from 0, the lowest priority, to 3, the highest priority.

- **SA**—48-bit source MAC address of the transmitting Catalyst switch.
- **LEN**—16-bit frame-length descriptor minus DA type, user, SA, LEN, and CRC.
- **AAAA03**—Standard SNAP 802.2 LLC header.
- **HSA**—First 3 bytes of SA (manufacturer's ID or organizational unique ID).
- **VLAN**—15-bit VLAN ID. Only the lower 10 bits are used for 1024 VLANs.
- **BPDU**—1-bit descriptor identifying whether the frame is a Spanning Tree BPDU. Also set if the encapsulated frame is a CDP frame.
- **INDEX**—16-bit descriptor that identifies the transmitting port ID. Used for diagnostics.
- **RES**—16-bit reserved field used for additional information, such as FDDI frame FC field.

VLAN Trunking Protocol

In order to provide VLAN connectivity throughout the switch fabric, VLANs must be configured on each switch. Cisco's VLAN Trunking Protocol (VTP) provides an easier method for maintaining consistent VLAN configuration throughout the switched network.

NOTE Because the focus of this book is the Catalyst 1900 Ethernet switch, we have concentrated on ISL trunking. It is important to mention, however, that there are other trunking mechanisms, such as ATM LANE and FDDI 802.10. Because VTP operates over a trunk line, it can operate on these topologies also.

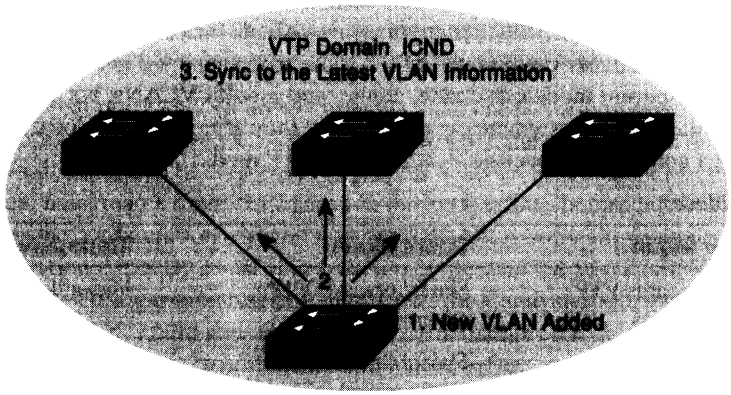
VTP is a protocol used to distribute and synchronize identifying information about VLANs configured throughout a switched network. Configurations made to a single VTP server are propagated across trunk links to all connected switches in the network. VTP enables switched network solutions to scale to large sizes by reducing the network's manual configuration needs.

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency throughout a common administration domain by managing the additions, deletions, and name changes of VLANs across networks. VTP minimizes misconfigurations and configuration inconsistencies that can cause problems, such as duplicate VLAN names or incorrect VLAN-type specifications.

A VTP domain is one switch or several interconnected switches sharing the same VTP environment. A switch is configured to be in only one VTP domain.

Figure 6-8 illustrates how VLAN configuration information is propagated from switch to switch.

Figure 6-8 *VTP Operation*



In Figure 6-8, we add a VLAN to our switched network. The steps illustrated in the figure are as follows:

Step 1 A new VLAN is added. At this point, VTP makes your job easier.

Step 2 The VTP advertisement is sent to the other switches in the VTP domain.

Step 3 The new VLAN is added to the other switch configurations. The result is consistent VLAN configuration.

By default, a Catalyst switch is in the no-management-domain state until it receives an advertisement for a domain over a trunk link, or until you configure a management domain.

VTP Modes

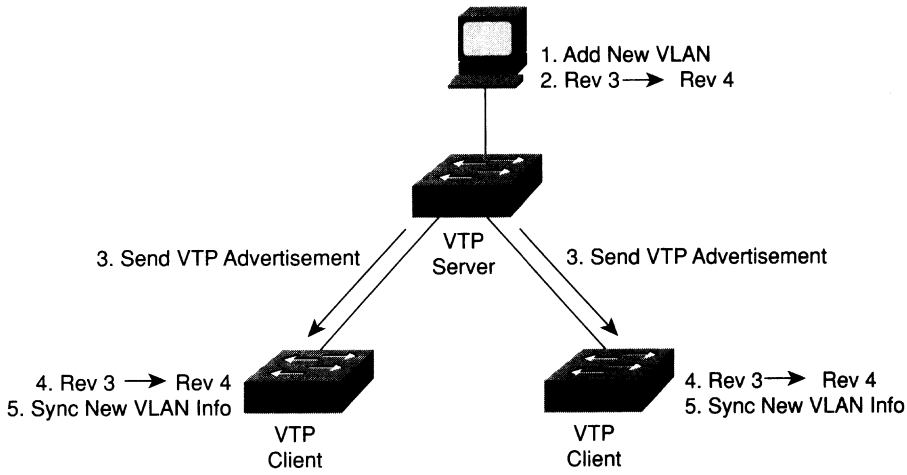
VTP operates in one of three modes: server mode, client mode, or transparent mode. The default VTP mode is server mode, but VLANs are not propagated over the network until a management domain name is specified or learned. A Catalyst switch operating in the VTP server mode can create, modify, and delete VLANs and other configuration parameters for the entire VTP domain. In server mode, VLAN configurations are saved in the Catalyst nonvolatile random-access memory (NVRAM). When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP messages are transmitted out all trunk connections, such as ISL.

A device operating as a VTP client cannot create, change, or delete VLANs. A VTP client does not save VLAN configurations in nonvolatile memory.

NOTE After you answer **Yes** to reset the VTP parameters, the switch will return you to the console menu.

One of the most critical components of VTP is the configuration revision number. Each time a VTP server modifies its VLAN information, it increments the configuration revision number by one. The VTP server then sends out a VTP advertisement with the new configuration revision number. If the configuration revision number being advertised is higher than the number stored on the other switches in the VTP domain, the other switches will overwrite their VLAN configurations with the new information that is being advertised. Figure 6-9 illustrates how VTP operates in a switched network.

Figure 6-9 *VTP Operation*



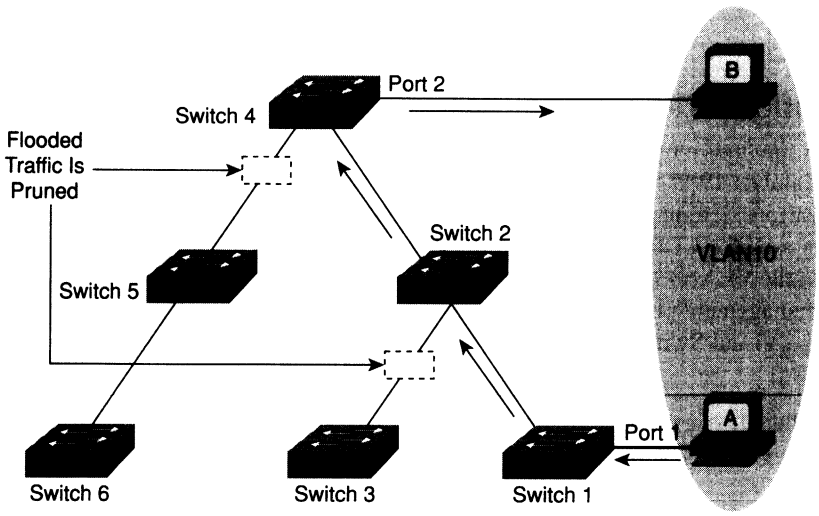
CAUTION The overwrite process would mean that the VTP server with the highest revision number determines the overall VLAN configuration for the domain. For example, if you deleted all VLANs on a VTP server and that server had the higher revision number, the other devices in the VTP domain would also delete their VLANs. This could create a loss of connectivity.

VTP Pruning

Because ISL trunk lines carry VLAN traffic for all VLANs, some traffic might be needlessly broadcast across links that do not need to carry that traffic. VTP pruning uses VLAN advertisements to determine when a trunk connection is flooding traffic needlessly.

By default, a trunk connection carries traffic for all VLANs in the VTP management domain. Commonly, some switches in an enterprise network do not have local ports configured in each VLAN. In Figure 6-10, Switches 1 and 4 support ports statically configured in VLAN10. As illustrated, with VTP pruning enabled, when Station A sends a broadcast, the broadcast is flooded only toward any switch with ports assigned to VLAN10. As a result, broadcast traffic from Station A is not forwarded to Switches 3, 5, and 6 because traffic for VLAN10 has been pruned on the links indicated on Switches 2 and 4.

Figure 6-10 *VTP Pruning*



VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

NOTE Because VLAN1 is the management VLAN and is used for administrative functions such as VTP advertisements, VLAN1 cannot be pruned from a trunk line.

VLAN Configuration

This chapter discusses the guidelines for configuring VLANs on the Cisco 1900 switch. You will learn the steps to configure VLANs, how to enable VTP domains, how to define a trunk, how to create a VLAN, and how to verify proper VLAN operation.

There are several facts you should remember before you begin VLAN configuration:

- The maximum number of VLANs is switch-dependent. The Catalyst 1900 supports 64 VLANs with a separate Spanning Tree per VLAN.
- VLAN1 is one of the factory default VLANs.
- CDP and VTP advertisements are sent on VLAN1.
- The Catalyst 1900 IP address is in the VLAN1 broadcast domain.
- The switch must be in VTP server mode or transparent mode to create, add, or delete VLANs.

VLAN Configuration Guidelines

A maximum of 64 VLANs can be active on most desktop Catalyst switches, such as the Catalyst 1900. The Catalyst 1900 switches have a factory default configuration in which various default VLANs are preconfigured. One of the default VLANs is VLAN1, which is used for CDP and VTP advertisements. The Catalyst 1900 IP address must also be in the VLAN1 broadcast domain. As you'll recall, the switch requires an IP address for management purposes—for example, to allow Telnet connections into the switch, or to use the Visual Switch Manager (VSM) via an HTTP browser to configure the switch.

Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If you want to propagate the VLAN to other switches in the domain, use server mode. If the VLAN should only be added to the local switch, use transparent mode.

VLAN Configuration Steps

Before you create VLANs, you must decide whether to use VTP to maintain global VLAN configuration information for your network.

To allow VLANs to span multiple Catalyst 1900 switches on a single link, you must configure Fast Ethernet trunks to interconnect the switches.

By default, a switch is in VTP server mode so that VLANs can be added, changed, or deleted. If the switch is set to VTP client mode, VLANs cannot be added, changed, or deleted.

VLAN membership on the switch ports is assigned manually on a port-by-port basis. When you assign switch ports to VLANs using this method, it is known as port-based, or static, VLAN membership.

The following sections elaborate on the details of the steps to configure VLANs.

VTP Configuration Guidelines

The default VTP configuration parameters for the Catalyst 1900 switch are as follows:

- VTP domain name: None
- VTP mode: Server
- VTP password: None
- VTP pruning: Disabled
- VTP trap: Enabled

The VTP domain name can be specified by the administrator or learned across a configured trunk line from a server with a domain name configured. By default, the domain name is not set.

By default, the switch is set to the VTP server mode.

A password can be set for the VTP management domain. The password entered must be the same for all switches in the domain. If you configure a VTP password, VTP does not function properly unless you assign the same password to each switch in the domain.

VTP pruning eligibility is one VLAN parameter advertised by the VTP protocol. Enabling or disabling VTP pruning on a VTP server propagates the change throughout the management domain. Enabling or disabling VTP pruning on a VTP server affects the entire management domain.

VTP trap is enabled by default. This will cause an SNMP message to be generated every time a new VTP message is sent.

CAUTION When adding a new switch to an existing domain, you should add the new switch in client mode to prevent the new switch from propagating incorrect VLAN information. Another method of preventing this is to use the **delete vtp** command, shown earlier in Example 6-1, to reset the VTP revision number on the new switch.

Configuring VTP

Use the **vtp** global configuration command to specify the operating mode, domain name, password, generation of traps, and pruning capabilities of VTP. The syntax for this command is as follows:

```
switch(config)# vtp {[server | transparent | client] [domain domain-name]
  [trap (enable | disable)] [password password] [pruning {enable | disable}]}
```

To verify a recent configuration change, or to just view the VTP configuration information, use the **show vtp** privileged EXEC command, as demonstrated in Example 6-2. Also displayed is the IP address of the device that last modified the configuration and a time

stamp showing when the modification was made. VTP has two versions. VTP version 1 only supports Ethernet. VTP version 2 supports Ethernet and Token Ring.

Example 6-2 *show vtp Output*

```
switch# show vtp
VTP version: 1
Configuration revision: 4
Maximum VLANs supported locally: 1005
Number of existing VLANs: 6
VTP domain name:switchdomain
VTP password:
VTP operating mode: Transparent
VTP pruning mode: Enabled
VTP traps generation: Enabled
Configuration last modified by: 10.1.1.40 at 00-00-0000 00:00:00
```

Trunk Line Configuration

Use the **trunk** interface configuration command to set a Fast Ethernet port to trunk mode. On the Catalyst 1900, the two Fast Ethernet ports are interfaces fa0/26 and fa0/27. The Catalyst 1900 supports the Dynamic Inter-Switch Link (DISL) protocol. DISL manages automatic ISL trunk negotiation. The syntax for the **trunk** interface configuration command is as follows:

```
switch(config)# trunk [on | off | desirable | auto | nonnegotiate]
```

The options for the **trunk** command are as follows:

- **on**—Configures the port to permanent ISL trunk mode and negotiates with the connected device to convert the link to trunk mode.
- **off**—Disables port trunk mode and negotiates with the connected device to convert the link to nontrunk.
- **desirable**—Triggers the port to negotiate the link from nontrunk to trunk mode. The port negotiates to a trunk port if the connected device is in the **on**, **desirable**, or **auto** state. Otherwise, the port becomes a nontrunk port.
- **auto**—Enables the port to become a trunk only if the connected device has the state set to **on** or **desirable**.
- **nonnegotiate**—Configures the port to permanent ISL trunk mode. No negotiation takes place with the partner.

Verifying Trunk Line Configuration

To verify a trunk configuration, use the **show trunk** privileged EXEC command to display the trunk parameters, as demonstrated in Example 6-3. The syntax for the **show trunk** privileged EXEC command is as follows:

```
switch(config)# show trunk [a | b]
```

The parameters **a** and **b** represent the Fast Ethernet ports:

- Port a represents Fast Ethernet 0/26
- Port b represents Fast Ethernet 0/27

Example 6-3 *show trunk Output*

```
switch# show trunk a
DISL state: On, Trunking: On, Encapsulation type: ISL
```

Adding a VLAN

Use the **vlan** global configuration command to configure a VLAN. The syntax for the **vlan** global configuration command is as follows:

vlan *vlan#* [**name** *vlan_name*]

Each VLAN has a unique four-digit ID that can be a number from 0001 to 1005. To add a VLAN to the VLAN database, assign a number and name to the VLAN. VLAN1, VLAN1002, VLAN1003, VLAN1004, and VLAN1005 are the factory default VLANs. These VLANs exist on all Catalyst switches and are used as default VLANs for other topologies, such as Token Ring and FDDI. No default VLAN can be modified or deleted.

To add an Ethernet VLAN, you must specify at least a VLAN number. If no VLAN name is entered for the VLAN, the default is to append the VLAN number to the word VLAN. For example, VLAN0004 could be a default name for VLAN4 if no name is assigned.

Remember, to add, change, or delete VLANs, the switch must be in VTP server or transparent mode.

Verifying a VLAN/Modifying VLAN Parameters

When the VLAN is configured, the parameters for that VLAN should be confirmed to ensure validity. To verify the parameters of a VLAN, use the **show vlan** *vlan#* privileged EXEC command to display information about a particular VLAN. Use **show vlan** to show all configured VLANs.

The **show vlan** command output in Example 6-4 also shows which switch ports are assigned to the VLAN.

Example 6-4 *show vlan Output*

```
switch# sh vlan 9

VLAN Name              Status     Ports
---------------------------------------------
9   switchlab2          Enabled
---------------------------------------------
```

continues

Example 6-4 *show vlan Output (Continued)*

```
VLAN Type           SAID   MTU    Parent RingNo BridgeNo Stp  Trans1 Trans2
------------------------------------------------------------------------------
9   Ethernet       100009 1500       0     1       1     Unkn     0         0
------------------------------------------------------------------------------
```

Other VLAN parameters shown in Example 6-4 include the type (default is Ethernet), SAID (used for FDDI trunk), MTU (default is 1500 for Ethernet VLAN), Spanning-Tree Protocol (the 1900 supports only the 802.1D Spanning-Tree Protocol standard), and other parameters used for Token Ring or FDDI VLANs.

To modify an existing VLAN parameter (such as the VLAN name), use the same command syntax used to add a VLAN.

In Example 6-5, the VLAN name for VLAN9 is changed to switchlab90.

Example 6-5 *Change VLAN Name*

```
switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z
switch(config)# vlan 9 name switchlab90
```

Use the **show vlan 9** command as demonstrated in Example 6-6 to verify the change.

Example 6-6 *Verify VLAN Change*

```
wg_sw_a# show vlan 9

VLAN Name              Status     Ports
-------------------------------------------------
9   switchlab90        Enabled
-------------------------------------------------
```

Assigning Ports to a VLAN

After creating a VLAN, you can statically assign a port or a number of ports to that VLAN. A port can belong to only one VLAN at a time.

Configure the VLAN port assignment from the interface configuration mode using the **vlan-membership** command. Here is the syntax:

```
vlan-membership {static {vlan#} | dynamic}
```

dynamic means that the Catalyst 1900 queries a VMPS for VLAN information based on a MAC address.

By default, all ports are members of the default VLAN—VLAN1.

Use the **show vlan-membership** privileged EXEC command to display the VLAN assignment and membership type for all switch ports as demonstrated in Example 6-7, where Port 1 refers to Ethernet 0/1, Port 2 refers to Ethernet 0/2, and so on.

Example 6-7 *Displaying VLAN Assignments and Membership for All Switch Ports*

```
Switch#show vlan-membership

Port  VLAN    Membership Type       Port    VLAN    Membership Type
---------------------------------------------------------------------------
1        5          Static           13       1          Static
2        1          Static           14       1          Static
3        1          Static           15       1          Static
4        1          Static           16       1          Static
5        1          Static           17       1          Static
6        1          Static           18       1          Static
7        1          Static           19       1          Static
8        9          Static           20       1          Static
```

Displaying Spanning-Tree Protocol Configuration Status

Use the **show spantree** privileged EXEC command to display the Spanning-Tree Protocol configuration status of the switch, as demonstrated in Example 6-8. The basic syntax for the **show spantree** privileged EXEC command is as follows:

```
switch# show spantree [vlannumber]
```

Example 6-8 ***show spantree*** *Output*

```
switch# show spantree 1
VLAN1 is executing the IEEE compatible Spanning Tree Protocol
   Bridge Identifier has priority 32768, address 0050.F037.DA00
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 0, address 00D0.588F.B600
   Root port is FastEthernet 0/26, cost of root path is 10
   Topology change flag not set, detected flag not set
   Topology changes 53, last topology change occured 0d00h17m14s ago
   Times:  hold 1, topology change 8960
           hello 2, max age 20, forward delay 15
   Timers: hello 2, topology change 35, notification 2
Port Ethernet 0/1 of VLAN1 is Forwarding
   Port path cost 100, Port priority 128
   Designated root has priority 0, address 00D0.588F.B600
   Designated bridge has priority 32768, address 0050.F037.DA00
   Designated port is Ethernet 0/1, path cost 10
   Timers: message age 20, forward delay 15, hold 1
```

Example 6-8 displays various Spanning Tree information for VLAN1, including the following:

- Port e0/1 is in the forwarding state for VLAN1.

- The root bridge for VLAN1 has a bridge priority of 0 with a MAC address of 00D0.588F.B600.
- The switch is running the IEEE 802.1d Spanning-Tree Protocol.

Recall that a Catalyst switch can support a separate Spanning Tree per VLAN. This allows for load balancing between switches. For example, one switch can be the root for VLAN1, and another switch can be the root for VLAN2. This idea is explained further in the Cisco Press title *CLSC Exam Certification Guide*.

VLAN Command Summary

Table 6-2 lists the commands covered in this chapter and briefly describes each command's function.

Table 6-2 *VLAN Command Summary*

Command	Description
delete vtp	Resets the VTP revision number and resets all VTP parameters to factory defaults.
vtp domain *name* **transparent**	Assigns a VTP domain name and sets transparent mode.
show vtp	Displays VTP status.
interface *interfacenumber* **trunk on**	Configures a trunk interface.
show trunk	Displays trunk status.
vlan *vlan# name vlanname*	Defines a VLAN and VLAN name.
show vlan	Displays VLAN information.
interface *interfacenumber* **vlan-membership static** *vlan#*	Assigns a port to a VLAN.
show vlan-membership	Displays VLAN membership.
show spantree *vlan#*	Displays Spanning Tree information for a VLAN.

Summary

This chapter discussed how VLANs operate to provide more effective networks by controlling broadcasts in your network. In order to configure VLANs on a Catalyst switch, you must first configure VTP to administer VLANs. Therefore, you learned how VTP operates and how it is configured. You also learned how to create a trunk link to carry all VLAN traffic, and how to configure a VLAN. Finally, this chapter discussed the verification of Spanning Tree operations, including the following:

- How VLANs operate
- How to configure VTP
- How to configure a trunk
- How to configure a VLAN
- How to verify Spanning Tree operations

Review Questions

1 VLANs allow for the creation of what in switched networks?

2 What are the two types of VLANs?

3 What type of port is capable of carrying all VLAN traffic?

4 What mechanism is used by switches to provide inter-switch communication between devices about which VLAN a packet originated from?

5 What is the purpose of VTP?

6 What is the default VTP mode for the Catalyst 1900?

7 Assume that a Catalyst 1900 is being added to your network. The switch needs to learn VLANs from the other switches in the network. You are not sure of the current VTP configuration and are fearful that it might overwrite your current VLAN information. How could you prevent the switch from accidentally overwriting the VLANs in your VTP domain?

8 What is the maximum number of VLANs that can be active on a Catalyst 1900?

9 List all the steps required to configure a VLAN on a Catalyst 1900 switch port.

10 Which command would you use to view the Spanning Tree configuration for VLAN9 on a Catalyst 1900 switch?

from Cisco CCNA Exam #640-507 Certification Guide

by Wendell Odom

(0-73570-971-8)

Cisco Press

About the Author

Wendell Odom has worked with networking technology for 15 years. He is currently a Cisco Systems Senior Systems Engineer in the Atlanta, Georgia office, assigned to several large Cisco customers. Prior to joining Cisco in 1999, Wendell provided consulting services on large networks as well as training services. He spent his first eight years in networking working for IBM, helping customers evolve their SNA networks into multiprotocol networks. Wendell is CCIE #1624, is a Certified Cisco Systems Instructor, is Cisco CIP-certified, and is a CCNA-WAN. He has taught various Cisco-certified courses, including Introduction to Cisco Router Configuration (ICRC), Advanced Cisco Router Configuration (ACRC), Cisco SNA for Multiprotocol Administrators (SNAM), Cisco Channel Interface Processor (CIP), MPLS over Cisco WAN Switches, and Cisco ATM (CATM). Wendell is one of the first Cisco instructors certified without a probationary testing period and is the first non-Cisco instructor in the United States to teach Cisco's SNAM, CIP, and DLSw courses.

Contents at a Glance

Bold chapters are elements included in this folio.

This chapter covers the following topics that you will need to master as a CCNA:

- **The IOS and Its User Interface** This section examines the types of memory used by the IOS, in addition to the commands used to examine and change the contents. This section also describes the basic functions and help for the command-line interface (CLI), and discusses how syslog messages are treated.
- **Configuration Processes and the Configuration File** The configuration file used for a router contains all the configuration for that router. This section covers all commands used to change the configuration and manipulate the configuration file.
- **Managing IOS Images** This section covers in detail the processes for upgrading the IOS in Flash memory, as well as the commands used to tell the router which IOS image to use. Password recovery is included as well.

CHAPTER 2

Cisco Internetwork Operating System (IOS) Fundamentals

The CCNA exam requires that you understand the basics of the Cisco Internetwork Operating System (IOS). In fact, the only operating system and user interface covered on the CCNA exam is the IOS and its user interface. The omission of other user interfaces, in particular the Catalyst 5000/5500 series user interface, is one of the most important facts to note when determining what to study for the CCNA exam.

The IOS runs on some Cisco switch models and provides the familiar IOS command-line interface (CLI). This chapter is geared toward the IOS CLI on a router. Chapter 4, "Bridges/ Switches and LAN Design," covers some details of IOS CLI on LAN switches. The user interface is the same, but some commands are different.

The exam also includes questions on both router and LAN switch usage of the IOS. No one should be surprised that the CCNA exam covers IOS running on routers. Also covered on the exam is the use of IOS running on Cisco 1900 series switches. User interfaces on other switch platforms might seem to be like IOS and have similar features, but these details are not covered on the exam. That should be particularly helpful for those of you with less hands-on experience.

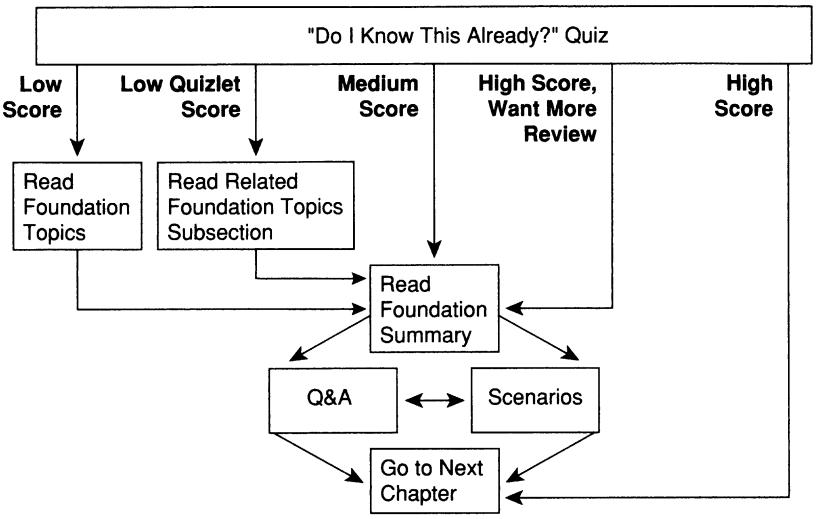
Cisco requires that CCNAs exhibit a solid recollection of the many details of the CLI. Of course, the best way to learn about any user interface is to use it. If you can spend time using a Cisco router, the knowledge and recall you gain will be of significant value. This chapter is designed to remind you of details you might not notice when practicing and will provide a reference for those of you who do not have access to routers for practice. Still, there is no substitute for hands-on practice.

How to Best Use This Chapter

By taking the following steps, you can make better use of your study time:

- Keep your notes and the answers for all your work with this book in one place, for easy reference.
- Take the "Do I Know This Already?" quiz, and write down your answers. Studies show that retention is significantly increased through writing down facts and concepts, even if you never look at the information again.
- Use the diagram in Figure 2-1 to guide you to the next step.

Figure 2-1 *How to Use This Chapter*



"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide what parts of this chapter to use. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

This 12-question quiz helps you determine how to spend your limited study time. The quiz is sectioned into three smaller four-question "quizlets," which correspond to the three major topic headings in the chapter. Figure 2-1 outlines suggestions on how to spend your time in this chapter based on your quiz score. Use Table 2-1 to record your scores.

Table 2-1 *Scoresheet for Quiz and Quizlets*

Quizlet Number	Foundation Topics Section Covering These Questions	Questions	Score
1	The IOS and Its User Interface	1 to 4	
2	Configuration Processes and the Configuration File	5 to 8	
3	Managing IOS Images	9 to 12	
All questions		1 to 12	

1 What are the two different names for the router's mode of operation that, when accessed, enables you to issue commands that could be disruptive to router operations?

2 What command would you use to receive command help if you knew that a **show** command option begins with a **c**, but you cannot recall the option?

3 After typing **show ip route**, which is the only command you issued since logging in to the router, you now want to issue the **show ip arp** command. What steps would you take to execute this command by using command recall keystrokes?

4 What is the name of the user interface mode of operation used when you cannot issue disruptive commands?

5 What configuration command causes the router to require a password from a user at the console? What configuration mode context must you be in—that is, what command(s) must be typed before this command after entering configuration mode? List the commands in the order in which they must be typed while in config mode.

6 What does CDP stand for?

7 What does the NV stand for in NVRAM?

8 Name two commands used to view the configuration that is currently used in a router. Which one is a more recent addition to the IOS?

9 What two methods could a router administrator use to cause a router to load the IOS stored in ROM?

10 What is the process used to update the contents of Flash memory so that a new IOS in a file called c4500-d-mz.120-5.bin, on TFTP server 128.1.1.1, is copied into Flash memory?

11 Two different IOS files are in a router's Flash memory: one called c2500-j-l.111-3.bin and one called c2500-j-l.112-14.bin. Which one does the router use when it boots up? How could you force the other IOS file to be used? Without looking at the router configuration, what command could be used to discover which file was used for the latest boot of the router?

12 What are the primary purposes of Flash memory in a Cisco router?

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections," on page 701. The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. This includes the "Foundation Topics" and "Foundation Summary" sections, the Q&A section, and the scenarios at the end of the chapter.
- **2 or less on any quizlet**—Review the subsection(s) of the "Foundation Topics" part of this chapter, based on Table 2-1. Then move into the "Foundation Summary" section, the Q&A section, and the scenarios at the end of the chapter.
- **7, 8, or 9 overall score**—Begin with the "Foundation Summary" section and then go to the Q&A section and the scenarios at the end of the chapter.
- **10 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the Q&A section and the scenarios at the end of the chapter. Otherwise, move to the next chapter.

Foundation Topics

The IOS and Its User Interface

IOS, a registered trademark of Cisco Systems, is the name of the operating system found in most of Cisco's routers. The majority of Cisco routers run the IOS, with its familiar command-line interface (CLI). Also, some routing cards in other devices run IOS. For example, the Route/Switch Module (RSM) card for the Catalyst 5000 series LAN switches performs routing functions and executes the IOS.

Fixes and code updates to the IOS can include new features and functions. To learn more about the code release process, features added at particular IOS revision levels, and other terminology that will help you talk to the Cisco Technical Assistance Center (TAC), check out a current Cisco Product Bulletin describing the Software Release Process. One such example is Product Bulletin #537 (http://www.cisco.com/warp/public/cc/cisco/mkt/ios/rel/prodlit/537_pp.htm).

The exam topics covered in this section will become second nature to you as you work with Cisco routers and switches more often. In fact, because this book purposefully was written for an audience that already has some training and experience with Cisco routers, several of the details in this chapter might already be ingrained in your memory. If you would like more review, or if you are still new to the IOS, read on—the details in this section are important to using Cisco routers and switches. This chapter reviews such topics as router components, the CLI, and how to navigate the IOS command set using Help and key sequences for command edit and recall.

Router Components

Before examining the IOS, a review of hardware and hardware terminology is useful. In addition to handling the logic of routing packets, the IOS controls the use of different physical components, which includes memory, processor, and interfaces. This section of the book reviews common hardware details.

All Cisco routers have a console port, and most have an auxiliary port. The console port is intended for local administrative access from an ASCII terminal or a computer using a terminal emulator. The auxiliary port, missing on a few models of Cisco routers, is intended for asynchronous dial access from an ASCII terminal or terminal emulator; the auxiliary port is often used for dial backup.

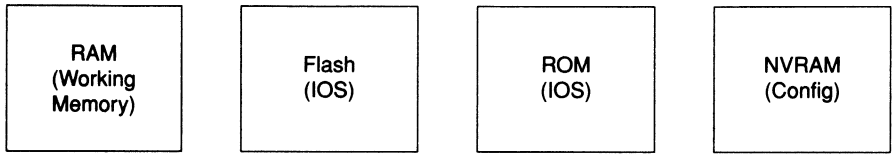
Each router has different types of memory, as follows:

- **RAM**—Sometimes called DRAM for *dynamic* random-access memory, RAM is used by the router just as it is used by any other computer: for working storage.

- **ROM**—This type of memory (read-only memory) stores a bootable IOS image, which is not typically used for normal operation. ROM contains the code that is used to boot the router until the router knows where to get the full IOS image.
- **Flash memory**—Either an EEPROM or a PCMCIA card, Flash memory stores fully functional IOS images and is the default where the router gets its IOS at boot time. Flash memory also can be used to store configuration files on Cisco 7500 series platforms.
- **NVRAM**—Nonvolatile RAM stores the initial or *startup* configuration file.

All these types of memory are permanent memory except RAM. No hard disk or diskette storage exists on Cisco routers. Figure 2-2 summarizes the use of memory in Cisco routers.

Figure 2-2 *Cisco Router Memory Types*



The processors in the routers vary from model to model. Although they are not specifically listed as requirements for the CCNA exam, some reference to terminology is useful. In most routers, only one processor option is available; thus, you would not order a specific processor type or card. The exception to this is the 7200 and 7500 families of routers. For instance, on the 7500 series, you choose either a Route Switch Processor 1 (RSP-1), RSP-2, or RSP-4 processor. In any case, all 7200 and 7500 routers, as well as most of the other Cisco router families, run IOS. This commonality enables Cisco to formulate exams, such as CCNA, that cover the IOS features without having to cover many hardware details.

Interfaces are used by a router for routing packets and bridging frames through a router. The types of interfaces available change over time due to new technology. For example, packet-over-SONET and voice interfaces are relatively recent additions to the product line. However, some confusion exists about what to call the actual cards that house the physical interfaces. Table 2-2 summarizes the terminology that might be referred to on the test.

Table 2-2 *Samples of Router Interface Terminology*

Model Series	What the IOS Calls Interfaces	What the Product Catalog Calls the Cards with the Interfaces on Them
2500	Interface	Modules and WAN interface cards
3600	Interface	Network modules and WAN interface cards
4500	Interface	Network processor modules
7200	Interface	Port adapters and service adapters
7500	Interface	Interface processors, and versatile interface processors with port adapters

Physical interfaces are referred to as *interfaces* by the IOS commands, as opposed to *ports* or *plugs*. IOS commands familiar on one platform will be familiar on another. Some nuances are involved in numbering the interfaces, however. In some smaller routers, the interface number is a single number. However, with some other families of routers, the interface is numbered first with the slot in which the card resides, followed by a slash and then the port number on that card. For example, port 3 on the card in slot 2 would be interface 2/3. Numbering starts with 0 for card slots and 0 for ports on any card. In some cases, the interface is defined by three numbers: first the card slot, then the daughter card (typically called a port adapter), and then a number for the physical interface on the port adapter. The 2600 and 3600 families also use a slot/port numbering scheme.

In this book, the single-digit interface numbers are used simply for consistency and readability.

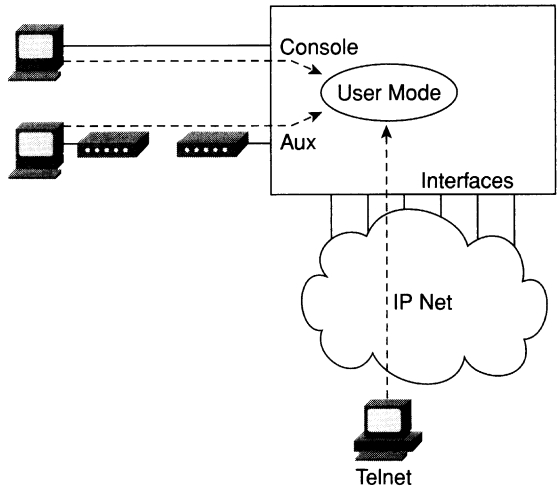
If you want to dig deeper, you might want to read about processors and interfaces in the Cisco Product Catalog (http://www.cisco.com/univercd/cc/td/doc/pcat/).

Command-Line Interface

Cisco uses the acronym CLI to refer to the terminal user command-line interface to the IOS. The term CLI implies that the user is typing commands at a terminal, terminal emulator, or Telnet connection. Although you can pass the CCNA exam without ever having used the CLI, actually using the CLI will greatly enhance your chances.

To access the CLI, use one of three methods, as illustrated in Figure 2-3.

Figure 2-3 *CLI Access*



Regardless of which access method is used, a CLI user initially is placed in user mode, or user EXEC mode, after logging in. *EXEC* refers to the fact that the commands typed here are executed, and some response messages are displayed onscreen. The alternative mode is *configuration mode*, which is covered in the next section.

Passwords can be required when accessing the CLI. In fact, the default configuration at IOS 12.x requires a password for Telnet and auxiliary port access, but no password is set—therefore, you must configure passwords from the console first. Table 2-3 reviews the different types of passwords and the configuration for each type.

Table 2-3 *CLI Password Configuration*

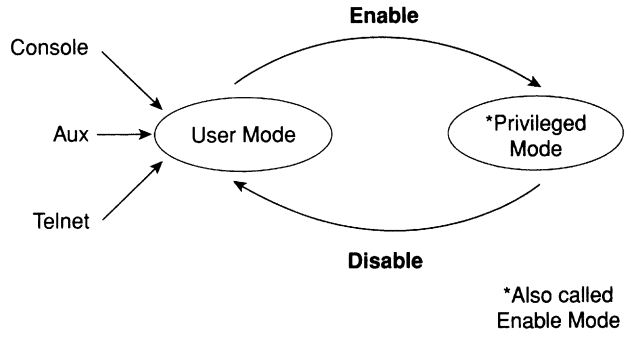
Access From . . .	Password Type	Configuration
Console	Console password	**line console** *0* **login** **password** *faith*
Auxiliary	Auxiliary password	**line aux** *0* **login** **password** *hope*
Telnet	vty password	**line vty** *0 4* **login** **password** *love*

The **login** command actually tells the router to display a prompt. The **password** commands specify the text password to be typed by the user to gain access. The first command in each configuration is a context-setting command, as described in the section "Configuration Processes and the Configuration File," later in this chapter. Typically, all three passwords have the same value.

Several concurrent Telnet connections to a router are allowed. The **line vty *0 4*** command signifies that this configuration applies to vtys (virtual teletypes—terminals) 0 through 4. Only these five vtys are allowed by the IOS unless it is an IOS for a dial access server, such as a Cisco AS5300. All five vtys typically have the same password, which is handy because users connecting to the router via a Telnet cannot choose which vty they get.

User EXEC mode is one of two command EXEC modes in the IOS user interface. *Enable* mode (also known as *privileged* mode or *privileged EXEC* mode) is the other. Enable mode is so named because of the command used to reach this mode, as shown in Figure 2-4; privileged mode earns its name because powerful, or privileged, commands can be executed there.

Figure 2-4 *User and Privileged Modes*



Navigating the IOS CLI

Several references are available for help when you are using the IOS. IOS documentation is available on CD and is free from Cisco if you own one router or switch under a current maintenance agreement. Paper documentation is also available from Cisco. If you prefer, Cisco Press offers the Cisco Documentation series (more information at www.ciscopress.com). In addition, all Cisco documentation is available online at Cisco's Web site (www.cisco.com/univercd/home/home.htm); the IOS command reference is found at www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/index.htm.

No matter which documentation you use, it is incredibly unlikely that you will remember all IOS commands. (The command reference manuals stack 14 inches high.) Therefore, you will find tools and tricks to recall commands particularly useful. Table 2-4 summarizes command recall help options available at the CLI. Note that in the first column, "Command" represents any command. Likewise, "parm" represents a command's parameter. For instance, the third row lists "command ?," which means that commands such as **show ?** and **copy ?** would list help for the **show** and **copy** commands, respectively.

Table 2-4 *IOS Command Help*

What You Type	The Help You Get
?	Help for all commands available in this mode.
help	Text describing how to get help. No actual command help is given.
command ?	Text help describing all the first parameter options for the command **command**.
com?	A list of commands that start with "com."
command parm?	This style of help lists all parameters beginning with "parm." (Notice, no spaces exist between "parm" and the ?.)

Table 2-4 *IOS Command Help (Continued)*

What You Type	The Help You Get
command parm<Tab>	If the user presses the Tab key midword, the CLI will either spell the rest of this parameter at the command line for the user, or do nothing. If the CLI does nothing, it means that this string of characters represents more than one possible next parameter, so the CLI does not know which to spell out.
command parm1 ?	If a space is inserted before the question mark, the CLI lists all next parameters and gives a brief explanation of each.

* When you type the ?, the IOS's CLI reacts immediately; that is, you don't need to press the Enter key or any other keys. The router also redisplays what you typed before the ? to save you some keystrokes. If you press Enter immediately after the ?, the IOS tries to execute the command with only the parameters you have typed so far.

** "Command" represents any command, not the word "command." Likewise, "parm" represents a command's parameter, not the word "parameter."

The context in which help is requested is also important. For example, when **?** is typed in user mode, the commands allowed only in privileged EXEC mode are not displayed. Also, help is available in configuration mode; only configuration commands are displayed in that mode of operation.

Commands you use at the CLI are stored in a command history buffer that retains the last 10 commands you typed. You can change the history size with the **terminal history size** *x* command, where *x* is the number of commands for the CLI to recall; this can be set to a value between 0 and 256.

Of course, most people want to use a previously typed command (perhaps with a different parameter). Commands you have previously used during the current console/aux/Telnet can be retrieved and then edited to save you some time and effort. This is particularly useful when you are typing long configuration commands. Table 2-5 lists the commands used to manipulate previously typed commands.

Table 2-5 *Key Sequences for Command Edit and Recall*

Keyboard Command	What the User Gets
Up-arrow or Ctrl+p	This displays the most recently used command. If pressed again, the next most recent command appears, until the history buffer is exhausted. (The p stands for *previous*.)
Down-arrow or Ctrl+n	If you have gone too far back into the history buffer, these keys will go forward, in order, to the more recently typed commands. (The n is for *next*.)
Left-arrow or Ctrl+b	This moves the cursor backward in the currently displayed command without deleting characters. (The b stands for *back*.)

continues

Table 2-5 *Key Sequences for Command Edit and Recall (Continued)*

Keyboard Command	What the User Gets
Right-arrow or Ctrl+f	This moves the cursor forward in the currently displayed command without deleting characters. (The f stands for *forward.*)
Backspace	This moves the cursor backward in the currently displayed command, deleting characters.
Ctrl+a	This moves the cursor directly to the first character of the currently displayed command.
Ctrl+e	This moves the cursor directly to the end of the currently displayed command.
Esc+b	This moves the cursor back one word in the currently displayed command.
Esc+f	This moves the cursor forward one word in the currently displayed command.
Ctl+r	This creates a new command prompt, followed by all the characters typed since the last command prompt was written. This is particularly useful if system messages confuse the screen and it is unclear what the user has typed so far.

NOTE One goal of this book is to help you learn more and solidify your understanding of the materials on the CCNA exam. Hopefully, Table 2-5 will further your understanding. Beware—these details are covered on the exam questions.

Syslog and Debug

The IOS creates messages when different events occur and, by default, sends them to the console. These messages are called *syslog* messages. If you have used the console of a router for any length of time, you likely have noticed these messages—and when they are frequent, you probably became a little frustrated.

The **debug** command is one of the key diagnostic tools for troubleshooting difficult problems on a router. **debug** enables monitoring points in the IOS and generates messages that describe what the IOS is doing and seeing. When any debug command option is enabled, the router processes the messages with the same logic as other syslog messages. Beware—some **debug** options create so many messages that the IOS cannot process them all, possibly crashing the IOS.

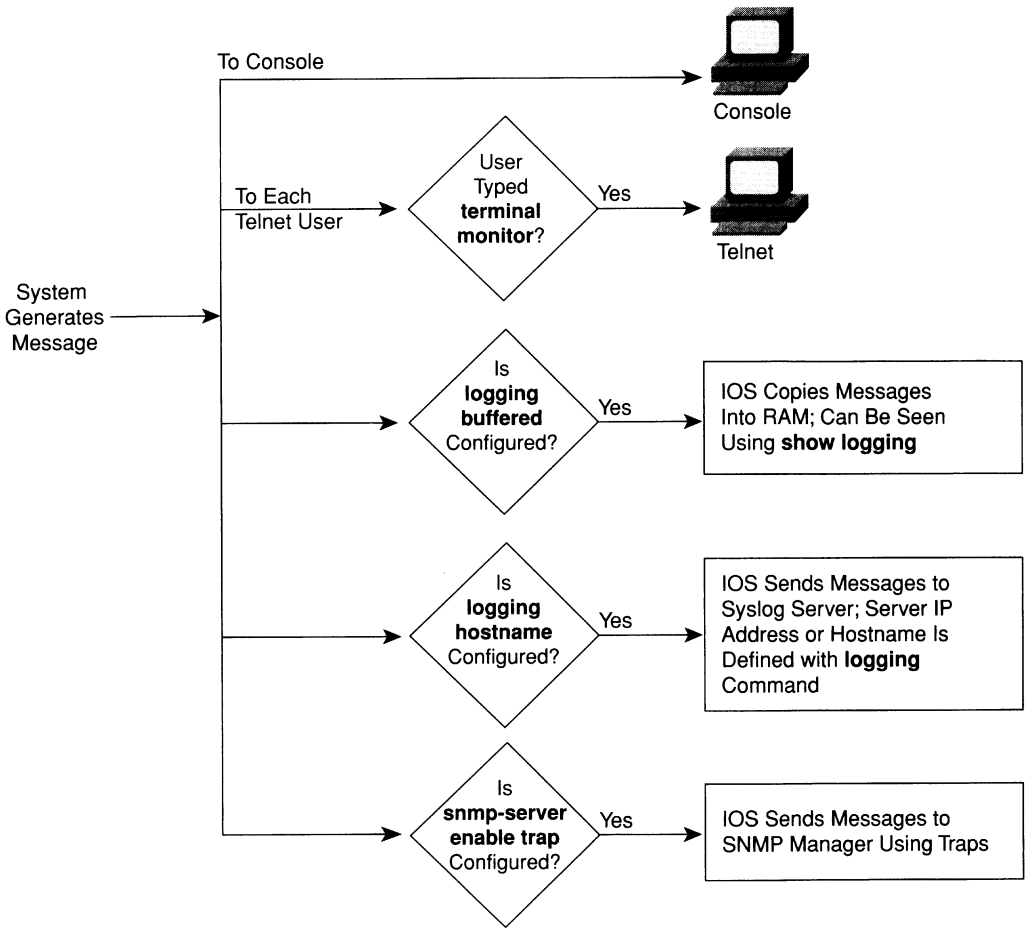
NOTE The **no debug all** command disables all debugs. Before enabling an unfamiliar **debug** command option, issue a **no debug all** and then issue the **debug** you want to use; then, quickly retrieve the **no debug all** command. If the messages are voluminous, press Enter immediately to try to prevent the router from crashing by immediately disabling all debugs.

Users might or might not be interested in seeing the messages as they occur. The console port always receives syslog messages. When a user telnets to the router, however, no syslog messages are seen unless the user issues the **terminal monitor** command. This command simply means that this terminal is monitoring syslog messages. Another alternative for viewing syslog messages is to have the IOS record the syslog messages in a buffer in RAM, and then use the **show logging** command to display the messages. For Telnet users, having the messages buffered using the global config command **logging buffered** is particularly useful. Because Telnet users do not get syslog messages by default anyway, these users can wait and look at syslog messages when desired. Finally, the **logging synchronous** line configuration subcommand can be used for the console and vtys to tell the router to wait until the user's last command output is displayed before showing any syslog messages onscreen. That provides a little less interruption for the user.

Syslog messages also can be sent to another device. Two alternatives exist: sending the messages to a syslogD server, and sending the messages as SNMP traps to a management station. The **logging** *host* command, where *host* is the IP address or host name of the syslog server, is used to enable sending messages to the external server. After SNMP is configured, the **snmp-server enable trap** tells the IOS to forward traps, including syslog messages.

Figure 2-5 summarizes the flow of syslog messages, including debug messages. For a more detailed view of syslog messages, including restricting messages based on message severity, refer to the IOS documentation CD manual called "Troubleshooting Commands."

Figure 2-5 *Syslog Message Flows*

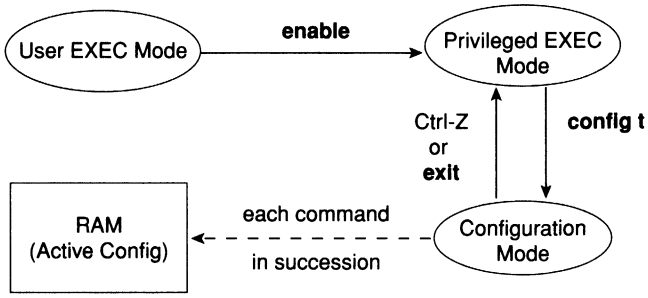


Configuration Processes and the Configuration File

Cisco requires that CCNAs master the process of changing and manipulating the configuration files in the IOS. This includes initially setting up an IOS device, handling ongoing configuration, and moving configuration files.

As mentioned in Chapter 1, "All About the Cisco Certified Network Associate Certification" configuration mode is another mode for the Cisco CLI. Changing the configuration of the router by typing various configuration commands is the purpose of configuration mode. Figure 2-6 illustrates the relationships among configuration mode, user EXEC mode, and priviledged EXEC mode.

Figure 2-6 *CLI Configuration Mode Versus EXEC Modes*



Commands typed in configuration mode update the active configuration file. Changes are moved into the active configuration file each time the user presses the Enter key and are acted upon immediately by the router.

In configuration mode, context-setting commands are used before most configuration commands. These context-setting commands tell the router the topic about which you will type commands. More importantly, they tell the router what commands to list when you ask for help. After all, the whole reason for these contexts is to make online help more convenient and clear for you.

NOTE *Context setting* is not a Cisco term—it's just a term used here to help make sense of configuration mode.

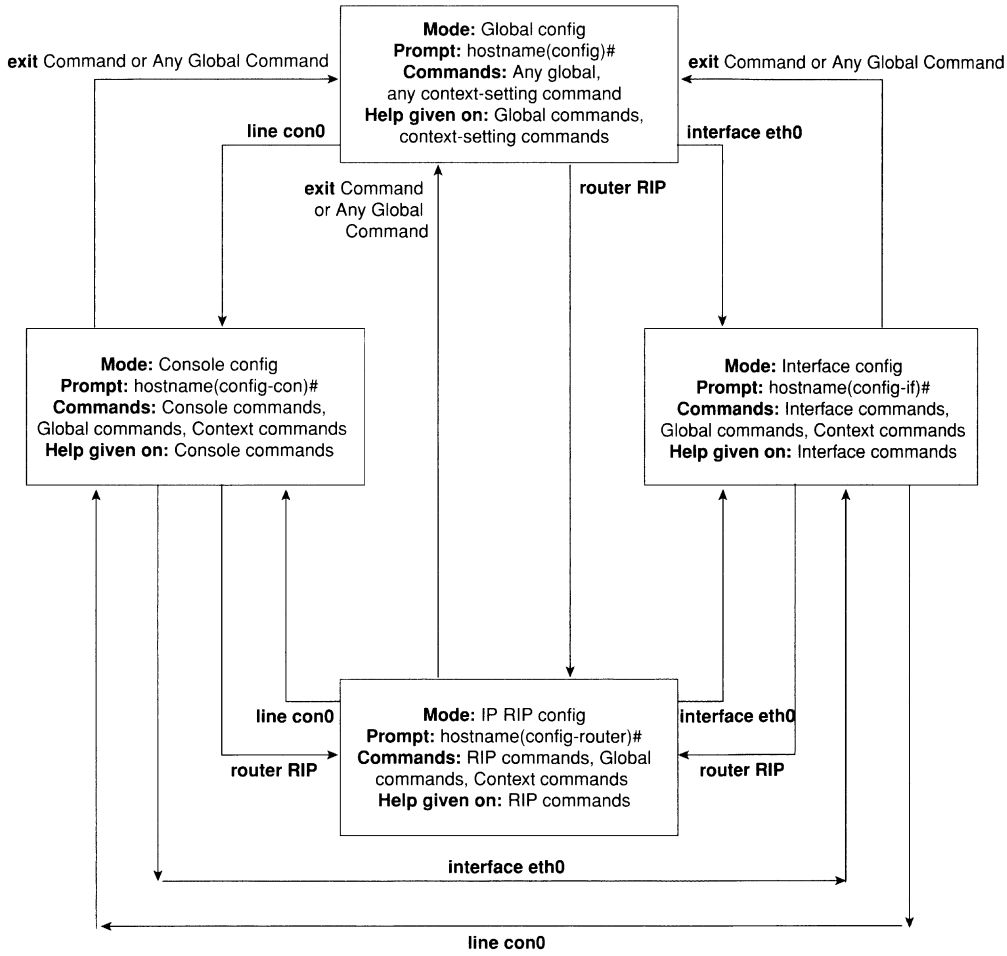
The **interface** command is the most commonly used context-setting configuration command. As an example, the CLI user could enter interface configuration mode after typing the **interface ethernet 0** configuration command. Command help in Ethernet interface configuration mode displays only commands that are useful when configuring Ethernet interfaces. Commands used in this context are called *subcommands*—or, in this specific case, *interface subcommands*. Figure 2-7 shows several different configuration mode contexts, including *interface configuration mode*, and illustrates the relationships and methods of moving among them.

The labels on the lines in Figure 2-7 represent the action or command that moves the user from one mode to another. For example, from console configuration mode (left box), the **interface ethernet 0** command could move you to the box on the right, which represents interface configuration mode.

If you have significant experience using the CLI in configuration mode, much of this will be second nature. From a CCNA exam perspective, recalling whether popular commands are global commands or subcommands will be useful. No set rules exist for what commands are global or subcommands, but generally, when multiple instances of a parameter can be set in

a single router, the command used to set the parameter is likely to be a configuration subcommand. Items that are set once for the entire router are likely to be global commands. For instance, the **hostname** command is a global command because there is only one host name per router. The **interface ethernet 0** command is a global configuration command because there is only one such interface in this router. Finally, the **ip address** command is an interface subcommand that sets the IP address on the interface; each interface will have a different IP address.

Figure 2-7 *Relationships Among Context-Setting Commands*



Use Ctrl+z from any part of configuration mode (or use the **exit** command from global configuration mode) to exit configuration mode and return to privileged EXEC mode. The configuration mode **end** command also exits from any point in the configuration mode back to privileged EXEC mode. The **exit** commands from submodes or contexts of configuration mode back up one level toward global configuration mode.

Example Configuration Process

Example 2-1 illustrates how the console password is defined; provides banner, host name, prompt, and interface descriptions; and shows the finished configuration. The lines beginning with "!" are comment lines that highlight significant processes or command lines within the example. The **show running-config** command output also includes comment lines with just a "!" to make the output more readable—many comment lines in the examples in this book were added to explain the meaning of the configuration.

Example 2-1 *Configuration Process Example*

```
This Here's the Rootin-est Tootin-est Router in these here Parts!

User Access Verification

Password:
Yosemite>enable
Password:
Yosemite#configure terminal
Yosemite(config)#enable password lu
Yosemite(config)#line console 0
Yosemite(config-line)#login
Yosemite(config-line)#password cisco
Yosemite(config-line)#hostname Critter
Critter(config)#prompt Emma
Emma(config)#interface serial 1
Emma(config-if)#description this is the link to Albuquerque
Emma(config-if)#exit
Emma(config)#exit
Emma#
 Emma#show running-config
Building configuration...

Current configuration:
!
version 11.2
! Version of IOS on router, automatic command


no service udp-small-servers
no service tcp-small-servers
!
```

continues

Example 2-1 *Configuration Process Example (Continued)*

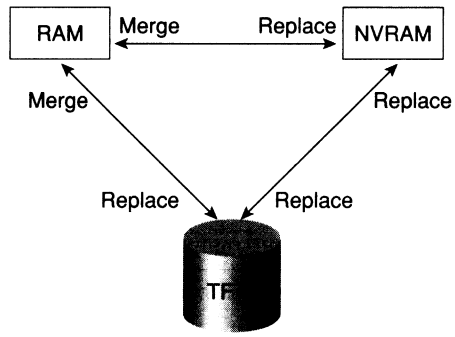
```
hostname Critter
prompt Emma
! Prompt overrides the use of the hostname as the prompt
!
enable password lu


! This sets the priviledge exec mode password
!
no ip domain-lookup
! Ignores all names resolutions unless locally defined on the router.
!
ipx routing 0000.3089.b170
! Enables IPX rip routing
!
interface Serial0
 ip address 137.11.12.2 255.255.255.0
 ipx network 12
!
interface Serial1
 description this is the link to Albuquerque
 ip address 137.11.23.2 255.255.255.0
 ipx network 23
!
interface TokenRing0
 ip address 137.11.2.2 255.255.255.0
 ipx network CAFE
 ring-speed 16
!
router rip
 network 137.11.0.0
!
no ip classless
!
!
!
banner motd ^C This Here's the Rootin-est Tootin-est Router in these here Parts! ^C
! Any text between the Ctl+C keystrokes is considered part of the banner, including
!the Enter key.!


line con 0
 password cisco
 login
! login tells the router to supply a prompt; password defines what the user must ,
!type!
!
line aux 0
line vty 0 4
 password cisco
 Login
!
End
```

Managing Configuration Files

The CCNA exam requires that you be able to distinguish between the configuration file used at startup and the active configuration file. The startup configuration file is in NVRAM; the other file, which is in RAM, is the one the router uses during operation. The router copies the stored configuration file from NVRAM into RAM as part of the boot process. Exterior to the router, configuration files can be stored as ASCII text files anywhere using TFTP.

Cisco provides several methods of manipulating configuration files. CiscoWorks and other management products let you create configurations for one or many routers without logging on to those routers. NetSys Connectivity Tools actually check all the configuration files in your network, make suggestions for improvements, and uncover errors. The most basic method for manipulating configuration files and moving them into and out of a router, however, is by using a TFTP server. The **copy** command is used to move configuration files among RAM, NVRAM, and a TFTP server. The files can be copied between any pair, as Figure 2-8 illustrates.

Figure 2-8 *Locations for Copying and Results from Copy Operations*



The commands can be summarized as follows:

```
copy {tftp | running-config | startup-config} {tftp | running-config | startup-config}
```

The first parameter is the "from" location; the next one is the "to" location. (Of course, choosing the same option for both parameters is not allowed.)

Confusion about what these commands actually do is pervasive. Any **copy** command option moving a file into NVRAM or a TFTP server replaces the existing file. Any **copy** command option moving the file into RAM, however, is effectively an *add* or *merge* operation. For example, only one host name *Siberia* configuration command is allowed. Therefore, a config file copied into RAM with **hostname *Siberia*** in it replaces the previous **hostname** command (if any). However, if the file being copied has the **access-list *1* permit host *1.1.1.1*** command in it, and if an access list number 1 already exists in the RAM configuration file, then **access-list *1* permit host *1.1.1.1*** is placed at the end of that existing access list (access lists are comprised of a list of configuration commands referencing the same list number or name). The

old entries in **access- list *1*** are not deleted. This is because many **access-list *1*** commands are allowed in the same access list. Effectively, any copy into RAM works just as if you typed the commands in the order listed in the config file.

So, why did Cisco not include a replace action, similar to the action used to copy to NVRAM or TFTP? Who knows? A replace action probably would require you to empty all routing tables, which might cause an outage. Possibly, this particular nuance is a result of some Cisco programmer who decided years ago to take the loaded gun out of users' hands. However, advanced users can accomplish the effect of a replace action by entering configuration mode and issuing commands until the running config is changed as desired. This requires that the user know whether each command will replace another that is like it in the RAM configuration file, or whether each command will simply be added to the configuration, as with an **access-list** command.

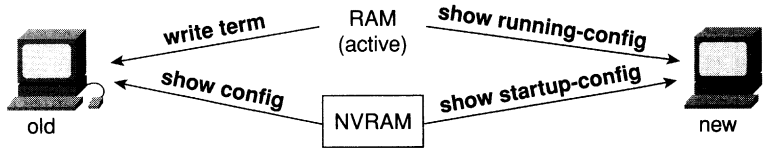
Two key commands can be used to erase the contents of NVRAM. The **write erase** command is the older command, and the **erase startup-config** command is the newer command. Both simply erase the contents of the NVRAM configuration file. Of course, if the router is reloaded at this point, there will be no initial configuration.

Viewing the Configuration and Old-Style Configuration Commands

Once upon a time, commands that were used to move configuration files among RAM, NVRAM, and TFTP did not use easy-to-recall parameters such as **startup-config** and **running-config**. In fact, most people could not remember the commands or got the different ones confused.

Figure 2-9 shows both the old and new commands used to view configurations.

Figure 2-9 *Configuration **show** Commands*



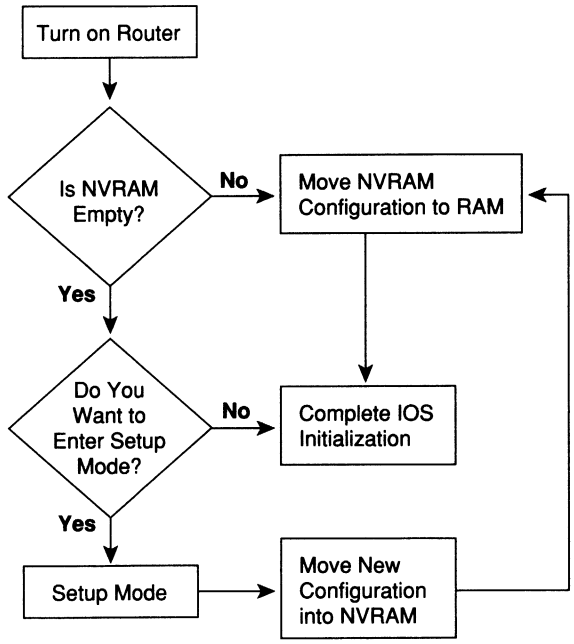
Initial Configuration (Setup Mode)

To pass the CCNA exam, you will need to be familiar with the differences between configuration mode and setup mode. Setup mode is a router configuration mode that prompts the user for basic configuration parameters. A Cisco router can be configured using the CLI in configuration mode without using setup mode. Some users like to use setup mode, however, particularly until they become more familiar with the CLI.

NOTE If you plan to work with Cisco routers much, you should become accustomed with the CLI configuration mode discussed earlier. Setup mode allows only basic configuration.

Setup mode is a topic covered on the CCNA exam, so regardless of whether you plan to use it, you must remember how it works. Figure 2-10 and Example 2-2 describe the process. Setup mode is most frequently used when the router comes up with no configuration in NVRAM; setup mode can be entered by using the **setup** command from privileged mode.

Figure 2-10 *Getting into Setup Mode*



Example 2-2 shows a screen capture of using setup mode after booting a router with no configuration in NVRAM.

Example 2-2 *Router Setup Configuration Mode*

```
Notice: NVRAM invalid, possibly due to write erase.
        --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use Ctrl+C to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.Would you
like to enter the initial configuration dialog? [yes]:
```

continues

Example 2-2 *Router Setup Configuration Mode (Continued)*

```
First, would you like to see the current interface summary? [yes]:
Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
Serial0                unassigned      NO  unset  down                  down
Serial1                unassigned      NO  unset  down                  down

Ethernet0              unassigned      NO  unset  reset                 down

Configuring global parameters:

  Enter host name [Router]: fred
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.
  Enter enable secret: cisco
The enable password is used when there is no enable secret
and when using older software and some boot images.
  Enter enable password: cisco2

Enter virtual terminal password: cisco
Configure SNMP Network Management? [yes]: n
Configure IP? [yes]:
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]: n
Configuring interface parameters:
Configuring interface Serial0:
  Is this interface in use? [yes]:
Configure IP on this interface? [yes]:
IP address for this interface: 163.4.8.3
Number of bits in subnet field [0]: 0
Class B network is 163.4.0.0, 0 subnet bits; mask is /16

Configuring interface Serial1:
  Is this interface in use? [yes]: n
Configuring interface Ethernet0:
  Is this interface in use? [yes]: y

Configure IP on this interface? [yes]:
IP address for this interface: 163.5.8.3
Number of bits in subnet field [0]: 0
Class B network is 163.5.0.0, 0 subnet bits; mask is /16



The following configuration command script was created:

hostname fred
enable secret 5 $1$aMyk$eUxp9JmrPgK.vQ.nA5Tge.
enable password cisco2
line vty 0 4
password cisco
no snmp-server
!
```

Example 2-2 *Router Setup Configuration Mode (Continued)*

```
ip routing
!
interface Serial0
ip address 163.4.8.3 255.255.0.0
!
interface Serial1
shutdown
no ip address
!
interface Ethernet0
ip address 163.5.8.3 255.255.0.0
!
end

Use this configuration? [yes/no]: y


Building configuration...[OK]
Use the enabled mode 'configure' command to modify this configuration.


Press ENTER to get started!
```

As Example 2-2 illustrates, you can use two methods to get into setup mode. First, if you are at the console and you power up the router, and if there is no configuration file in NVRAM, the router asks whether you want to enter the "initial configuration dialog." Answering **y** or **yes** puts you in setup mode. Alternatively, the **setup** privileged EXEC command puts you in setup mode.

When you are finished with setup, you are asked whether you want to use this configuration. If you answer **yes**, the configuration you created is placed in RAM and NVRAM. This is the only operation in the IOS that changes both files to include the same contents based on a single action.

As of IOS version 12.0, the setup mode prompts no longer ask for the number of subnet bits. Instead, the subnet mask used is requested, which is probably a lot better for most people. Other fine details of the setup mode prompts have changed as well. Example 2-3 shows an example using IOS version 12.0 and is simply shown here for reference.

Example 2-3 *Router Setup Configuration Mode—Version 12.0*

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use Ctrl+c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

continues

Example 2-3 *Router Setup Configuration Mode—Version 12.0 (Continued)*

```
Would you like to enter basic management setup? [yes/no]: no

First, would you like to see the current interface summary? [yes]:

Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
Serial0                unassigned      NO  unset  down                  down
Serial1                unassigned      NO  unset  down                  down
TokenRing0             unassigned      NO  unset  reset                 down

Configuring global parameters:

  Enter host name [Router]: fred

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: cisco

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: cisco2

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: cisco
Configure SNMP Network Management? [yes]: n
Configure DECnet? [no]:
Configure AppleTalk? [no]:
Configure IPX? [no]:
Configure IP? [yes]:
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]:
Configure bridging? [no]:
Configuring interface parameters:
Do you want to configure Serial0  interface? [yes]: y
Configure IP on this interface? [yes]:
IP address for this interface: 163.4.8.3
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 163.4.0.0, 24 subnet bits; mask is /24
Do you want to configure Serial1  interface? [yes]: n
Do you want to configure Ethernet0 interface? [yes]: y
Configure IP on this interface? [yes]:
IP address for this interface: 163.5.8.3
Subnet mask for this interface [255.255.0.0] : 255.255.255.0
Class B network is 163.5.0.0, 24 subnet bits; mask is /24
The following configuration command script was created:

hostname fred
enable secret 5 $1$Qxix$Fi3buBVGTpEig9AIPgzxC.
enable password cisco2
```

Example 2-3 *Router Setup Configuration Mode—Version 12.0 (Continued)*

```
line vty 0 4
password cisco
no snmp-server
!
no decnet routing
no appletalk routing
no ipx routing
ip routing
no bridge 1
!
interface Serial0
ip address 163.4.8.3 255.255.255.0
no mop enabled
!
interface Serial1
shutdown
no ip address
!
interface Ethernet0
ip address 163.5.8.3 255.255.255.0
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]Use the enabled mode 'configure' command to modify this configuration._


Press ENTER to get started!
```

In the example, notice that an early prompt gives you the choice of performing a simpler configuration for basic management. For instance, you may have the configuration editing in a file on your PC, and all you need is enough IP working so that you can Telnet into the router to copy the configuration. Also note that you have an option to start over after answering the questions, which is very convenient for those of us who are poor typists.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is used by Cisco routers and switches to ascertain basic information about neighboring routers and switches. You can use this information to learn addresses quickly for easier Simple Network Management Protocol (SNMP) management, as well as learn the addresses of other devices when you do not have passwords to log in to the other device.

CDP is a Cisco proprietary protocol; to support forwarding CDP messages over an interface, that interface must support SNAP headers. Any LAN interface, HDLC, Frame Relay, and ATM all support CDP. The router or switch can discover Layer 3 addressing details of neighboring routers—without even configuring that Layer 3 protocol—because CDP is not dependent on any particular Layer 3 protocol.

CDP discovers several useful details from the neighboring device:

- **Device Identifier**—Typically the host name.
- **Address list**—Network and data link addresses.
- **Port Identifier**—Text that identifies the port, which is another name for an interface.
- **Capabilities list**—Information on what the device does—for instance, a router or switch.
- **Platform**—The model and OS level running in the device.

CDP is enabled in the configuration by default. The **no cdp run** global command disables CDP for the entire device, and the **cdp run** global command re-enables CDP. Likewise, the **no cdp enable** interface subcommand disables CDP just on that interface, and the **cdp enable** command switches back to the default state of CDP being enabled.

A variety of **show cdp** command options are available. Example 2-4 lists the output of the commands, with some commentary following.

Example 2-4 ***show cdp*** *Command Options*

```
Seville#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
fred               Ser 1           172          R        2500      Ser 1
Yosemite           Ser 0.2         161          R        2500      Ser 0.2

Seville#show cdp entry fred
-------------------------
Device ID: fred
Entry address(es):
  IP address: 163.5.8.3
Platform: cisco 2500,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Serial1
Holdtime : 168 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Seville#show cdp neighbor detail
-------------------------
Device ID: fred
Entry address(es):
```

Example 2-4 *show cdp Command Options (Continued)*

```
  IP address: 163.5.8.3
Platform: cisco 2500,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Serial1
Holdtime : 164 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

-------------------------
Device ID: Yosemite
Entry address(es):
  IP address: 10.1.5.252
  Novell address: 5.0200.bbbb.bbbb
Platform: cisco 2500,  Capabilities: Router
Interface: Serial0.2,  Port ID (outgoing port): Serial0.2
Holdtime : 146 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Seville#show cdp interface
Ethernet0 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0.2 is up, line protocol is up
  Encapsulation FRAME-RELAY
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial1 is up, line protocol is up
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Seville#show cdp traffic
CDP counters :
    Packets output: 41, Input: 21
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
    No memory: 0, Invalid packet: 0, Fragmented: 0
```

The commands provide information about both the neighbors and the behavior of the CDP protocol itself. In the **show cdp entry** *fred* command in Example 2-4, all the details learned by CDP are shown and highlighted. To know that fred is the device identifier of a neighbor, the **show cdp neighbor** command can be used to summarize the information about each neighbor. **Show cdp neighbor detail** lists the detail of all neighbors, in the same format as **show cdp entry**. In addition, **show cdp traffic** lists the overhead that CDP introduces to perform its functions.

Managing IOS Images

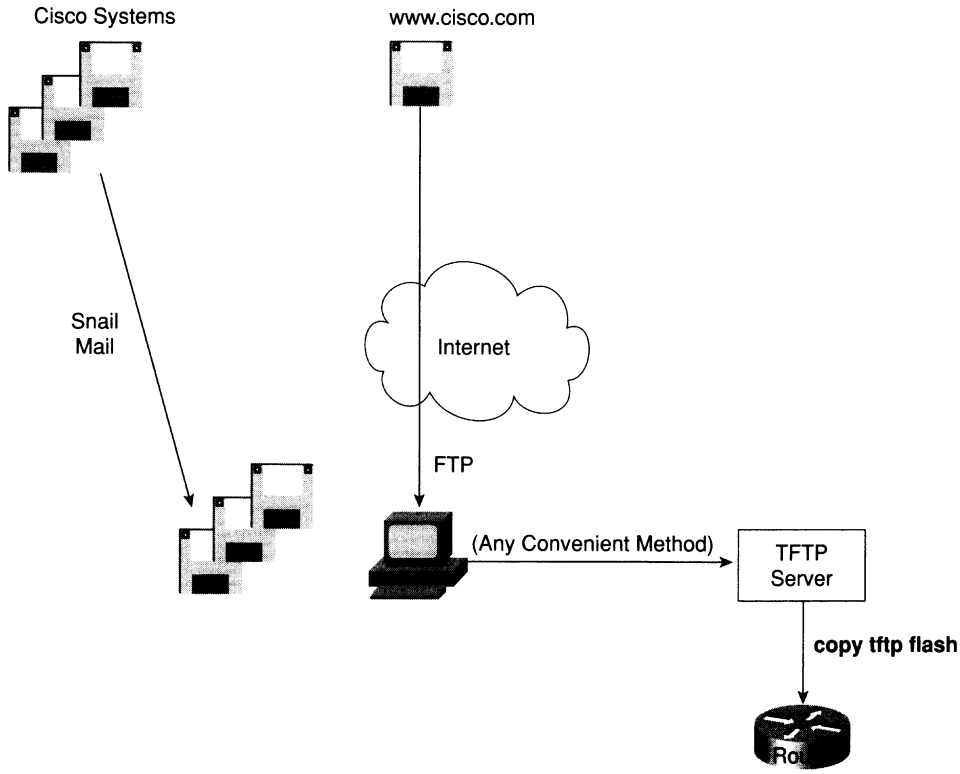
One common task that CCNAs run into is migrating to a new level of IOS. *IOS image* is simply a term referring to the file containing the IOS. Managing image files entails getting new IOS images from Cisco; backing up the currently used, older version from your routers; updating your routers with the new image; and testing. Also included in IOS image management is how to tell a router to use a particular IOS the next time it boots.

IOS files are typically stored in Flash memory. Flash memory is rewritable, permanent storage, which is ideal for storing files that need to be retained when the router loses power. Also, because there are no moving parts, there is a smaller chance of failure as compared with disk drives, which provides better availability.

Upgrading an IOS Image into Flash Memory

As Figure 2-11 illustrates, to upgrade an IOS image into Flash memory, you first must obtain the IOS image from Cisco. Then, you must place the IOS image into the default directory of a TFTP server. Finally, you must issue the **copy** command from the router, copying the file into Flash memory.

Figure 2-11 *Complete IOS Upgrade Process*



Example 2-5 provides an example of the final step, copying the IOS image into Flash memory.

Example 2-5 ***copy tftp flash*** *Command Copies the IOS Image to Flash Memory*

```
R1#copy tftp flash

System flash directory:
File  Length   Name/status
  1   7530760   c4500-d-mz.120-2.bin
[7530824 bytes used, 857784 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 134.141.3.33
Source file name? c4500-d-mz.120-5.bin
Destination file name [c4500-d-mz.120-5.bin]?
Accessing file c4500-d-mz.120-5.bin ' on 134.141.3.33...
Loading c4500-d-mz.120-5.bin from 134.141.3.33 (via TokenRing0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'c4500-d-mz.120-5.bin ' from server
  as 'c4500-d-mz.120-5.bin ' into Flash WITH erase? [yes/no]y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading c4500-d-mz.120-5.bin  from 134.141.3.33 (via TokenRing0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!
[OK - 7530760/8388608 bytes]

Verifying checksum...  OK (0xA93E)
Flash copy took 0:04:26 [hh:mm:ss]
R1#
```

During this process of copying the IOS image into Flash memory, the router will need to discover several important facts:

1. What is the IP address or host name of the TFTP server?
2. What is the name of the file?
3. Is space available for this file in Flash memory?
4. If not, will you let the router erase the old files?

The router will prompt you for answers, as necessary. Afterward, the router erases Flash memory as needed, copies the file, and then verifies that the checksum for the file shows that no errors occurred in transmission. The **show flash** command then can be used to verify the contents of Flash memory (see Example 2-6). (The **show flash** output can vary between router families.) Before the new IOS is used, however, the router must be reloaded.

Example 2-6 *Verifying Flash Memory Contents with the **show flash** Command*

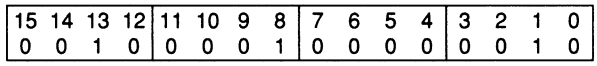
```
fred#show flash

System flash directory:
File  Length   Name/status
  1   6181132 c4500-d-mz.120-5.bin
[4181196 bytes used, 4207412 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

In some cases, Flash memory could be in read-only mode. That is the case when a router loads only part of the IOS into RAM, to conserve RAM. Other parts of the IOS file are kept in Flash memory (Flash memory access time is much slower than RAM). In this case, if Flash memory must be erased to make room for a new image, the IOS could not continue to run. So, if the router is running from a portion of the IOS in Flash memory, the router first must be booted using the IOS in ROM. Then the Flash memory will be in read/write mode, and the erase and copy processes can be accomplished. The **copy tftp flash** command in later releases of the IOS actually performs the entire process for you. In earlier releases, you had to boot the router from ROM and then issue the **copy tftp flash** command.

Choosing Which IOS Image to Load

The CCNA exam requires you to be proficient in configuring a router to load an IOS image from many sources. Two methods are used by a router to determine where it tries to obtain an IOS image to execute. The first is based on the value of the *configuration register*, which is a 16-bit software register in Cisco's more recently developed routers. (Some older routers had a hardware configuration register, with jumpers on the processor card, to set bits to a value of 0 or 1.) The second method used to determine where the router tries to obtain an IOS image is through the use of the **boot system** configuration command. Figure 2-12 shows an example binary breakdown of the default value for the configuration register.

Figure 2-12 *Binary Version of Configuration Register, Value Hex 2102*



The *boot field* is the name of the low-order 4 bits of the configuration register. This field can be considered a 4-bit value, represented as a single hexadecimal digit. Cisco represents hexadecimal values by preceding the hex digit(s) with *0x*—for example, *0xA* would mean a single hex digit *A*.

The router chooses the IOS image to load based on the boot field and the *boot system* commands in the configuration. Table 2-6 summarizes the use of the configuration register and the **boot system** command at initialization time. (If the files referred to in the boot system commands are not found, then the router will never complete the boot process. The password recovery process must be used to change the config register to 0x2161 so that the NVRAM configuration is ignored and the **boot** commands can be repaired to point to a valid IOS file name. Refer to the section "Password Recovery," later in this chapter, for more details.)

Table 2-6 ***boot system*** *Command*

Value of Boot Field	Boot System Commands	Result
0x0	Ignored if present	ROM monitor mode, a low-level problem determination mode, is entered.
0x1	Ignored if present	IOS from ROM is loaded.
0x2-0xF	No **boot** command	The first IOS file in flash is loaded; if that fails, the router broadcasts looking for an IOS on a TFTP server. If that fails, IOS from ROM is loaded.
0x2-0xF	**boot system ROM**	IOS from ROM is loaded.
0x2-0xF	**boot system flash**	The first file from Flash memory is loaded.
0x2-0xF	**boot system flash** *filename*	IOS with name *filename* is loaded from Flash memory.
0x2-0xF	**boot system tftp 10.1.1.1** *filename*	IOS with name *filename* is loaded from TFTP server.
0x2-0xF	Multiple boot system commands, any variety	An attempt occurs to load IOS based on the first boot command in configuration. If that fails, the second boot command is used, and so on, until one is successful.

Password Recovery

Several additional concepts related to loading the IOS must be understood before password recovery can be performed. First, software called the *ROM monitor* (rommon) is held in ROM on all routers and actually provides the code that is first used to boot each router. rommon has a rudimentary command structure that is used as part of the password recovery process. A limited-function IOS is also held in either ROM or in additional Flash memory called *bootflash*; in either case, the IOS in bootflash or ROM is used mainly in cases where the IOS in flash is not available for some reason. Finally, bit 6 of the configuration register set to binary 1 means that the router should ignore the NVRAM configuration when booting.

Password recovery revolves around the process of getting the router to boot while ignoring the NVRAM configuration file. The router will be up, but with a default configuration; this enables a console user to log in, enter privileged mode, and change any encrypted passwords or view any unencrypted passwords. To cause the router to ignore NVRAM at boot time, the configuration register must be changed. To do that, you must be in privileged mode—and if you were already there, you could reset any encrypted passwords or view any unencrypted ones. It seems to be a viscious circle.

The two keys to password recovery are knowing that rommon enables you to reset the configuration register and that a console user can get into rommon mode by pressing the Break key during the first 60 seconds after power-on of the router. Knowing how to reset the config register enables you to boot the router (ignoring NVRAM), allowing the console user to see or change the unencrypted or encrypted passwords, respectively.

The process is slightly different for different models of routers, although the concepts are identical. Table 2-7 outlines the process for each type of router.

Table 2-7 *Password Recovery*

Step	Function	How to Do This for 1600, 2600, 3600, 4500, 7200, 7500	How to Do This for 2000, 2500, 3000, 4000, 7000
1	Turn router off and then back on again.	Use the power switch.	Same as other routers.
2	Press the Break key within the first 60 seconds.	Find the Break key on your console devices keyboard.	Same as other routers.
3	Change the configuration register so that bit 6 is 1.	Use the rommon command **confreg**, and answer the prompts.	Use the rommon command **o/r 0x2142**.
4	Cause the router to load an IOS.	Use the rommon **reload** command or, if unavailable, power off and on.	Use rommon command **initialize**.
5	Avoid using setup mode, which will be prompted for at console.	Just say no.	Same as other routers.

Table 2-7 *Password Recovery (Continued)*

Step	Function	How to Do This for 1600, 2600, 3600, 4500, 7200, 7500	How to Do This for 2000, 2500, 3000, 4000, 7000
6	Enter privileged mode at console.	Press Enter and use **enable** command (no password required).	Same as other routers.
7	View startup config to see unencrypted passwords.	Use exec command **show startup-config**.	Same as other routers.
8	Use appropriate config commands to reset encrypted commands.	For example, use **enable secret xyz123** command to set enable secret password.	Same as other routers.
9	Change config register back to original value.	Use config command **Config-reg 0x2102**.	Same as other routers.
10	Reload the router after saving the configuration.	Use the **copy running-config startup-config** and **reload** commands.	Same as other routers.

A few nuances need further explanation. First, the **confreg** rommon command prompts you with questions that correspond to the functions of the bits in the configuration register. When the prompt asks, "Ignore system config info[y/n]?", it is asking you about bit 6. Entering **yes** sets the bit to 1. The rest of the questions can be defaulted. The last **confreg** question asks, "Change boot characteristics[y/n]?", which asks whether you want to change the boot field of the config register. You don't really need to change it, but the published password recovery algorithm lists that step, which is the only reason that it is mentioned here. Just changing bit 6 to 1 is enough to get the router booted and you into privileged mode to find or change the passwords.

The original configuration is lost through this process, but you can overcome that. When you save the configuration in Step 10, you are overwriting the config in NVRAM. There was no configuration in the running config except default and the few things you configured. So, before Step 8, you might want to perform a **copy startup-config running-config** command and then proceed with the process.

Foundation Summary

The Foundation Summary is a collection of tables and figures that provide a convenient review of many key concepts in this chapter. For those of you already comfortable with the topics in this chapter, this summary could help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final preparation before the exam, these tables and figures will be a convenient way to review the day before the exam.

Table 2-8 reviews the different types of passwords and the configuration for each type.

Table 2-8 *CLI Password Configuration*

Access from . . .	Password Type	Configuration
Console	Console password	**line console** *0* **login** **password** *faith*
Auxiliary	Auxiliary password	**line aux** *0* **login** **password** *hope*
Telnet	vty password	**line vty** *0 4* **login** **password** *love*

Table 2-9 lists the commands used to manipulate previously typed commands.

Table 2-9 *Key Sequences for Command Edit and Recall*

Keyboard Command	What the User Gets
Up-arrow or Ctrl+p	This calls up the most recently used command. If pressed again, the next most recent command appears, until the history buffer is exhausted. (The p stands for *previous.*)
Down-arrow or Ctrl+n	If you have gone too far back into the history buffer, these keys will go forward, in order, to the more recently typed commands. (The n stands for *next.*)
Left-arrow or Ctrl+b	This moves the cursor backward in the currently displayed command without deleting characters. (The b stands for *back.*)
Right-arrow or Ctrl+f	This moves the cursor forward in the currently displayed command without deleting characters. (The f stands for *forward.*)

Table 2-9 *Key Sequences for Command Edit and Recall (Continued)*

Keyboard Command	What the User Gets
Backspace	This moves the cursor backward in the currently displayed command, deleting characters.
Ctrl+a	This moves the cursor directly to the first character of the currently displayed command.
Ctrl+e	This moves the cursor directly to the end of the currently displayed command.
Esc+b	This moves the cursor back one word in the currently displayed command.
Esc+f	This moves the cursor forward one word in the currently displayed command.
Ctrl+r	This creates a new command prompt, followed by all the characters typed since the previous command prompt. This is particularly useful if system messages confuse the screen and it is unclear what the user has typed so far.

Table 2-10 summarizes the use of the configuration register and the **boot system** command at initialization.

Table 2-10 ***boot system*** *Command*

Value of Boot Field	Boot System Commands	Result
0x0	Ignored if present	ROM monitor mode, a low-level problem determination mode, is entered.
0x1	Ignored if present	IOS from ROM is loaded.
0x2-0xF	No **boot** command	The first IOS file in flash is loaded; if that fails, IOS from ROM is loaded. If that fails, the router broadcasts looking for an IOS on a TFTP server.
0x2-0xF	**boot system ROM**	IOS from ROM is loaded.
0x2-0xF	**boot system flash**	The first file from Flash memory is loaded.
0x2-0xF	**boot system flash** *filename*	IOS with name *filename* is loaded from Flash memory.
0x2-0xF	**boot system tftp 10.1.1.1** *filename*	IOS with name *filename* is loaded from the TFTP server.
0x2-0xF	Multiple boot system commands, any variety	An attempt occurs to load IOS based on the first boot command in configuration. If that fails, the second boot command is used, and so on, until one is successful.

Figure 2-13 summarizes the use of memory in Cisco routers.

Figure 2-13 *Cisco Router Memory Types*

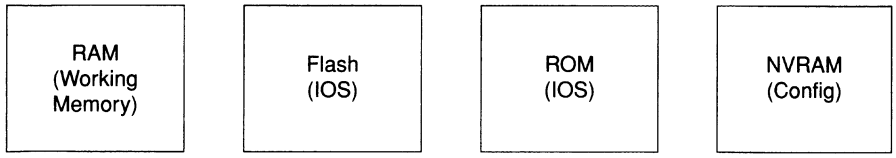
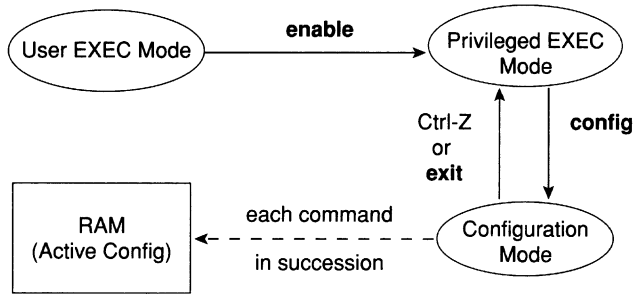


Figure 2-14 illustrates the relationships among configuration mode, user EXEC mode, and priviledged EXEC mode.

Figure 2-14 *CLI Configuration Mode Versus EXEC Modes*



The **copy** command is used to move configuration files among RAM, NVRAM, and a TFTP server. The files can be copied between any pair, as Figure 2-15 illustrates.

Figure 2-15 *Locations for Copying and Results from Copy Operations*

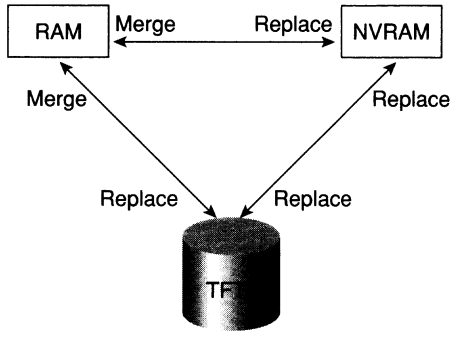


Figure 2-16 shows both the old and new commands used to view configurations.

Figure 2-16 *Configuration **show** Commands*

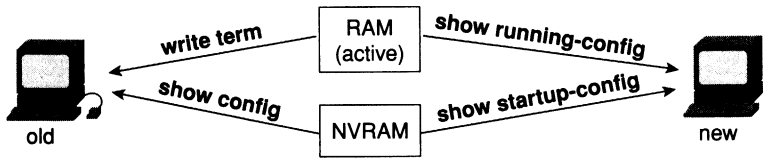
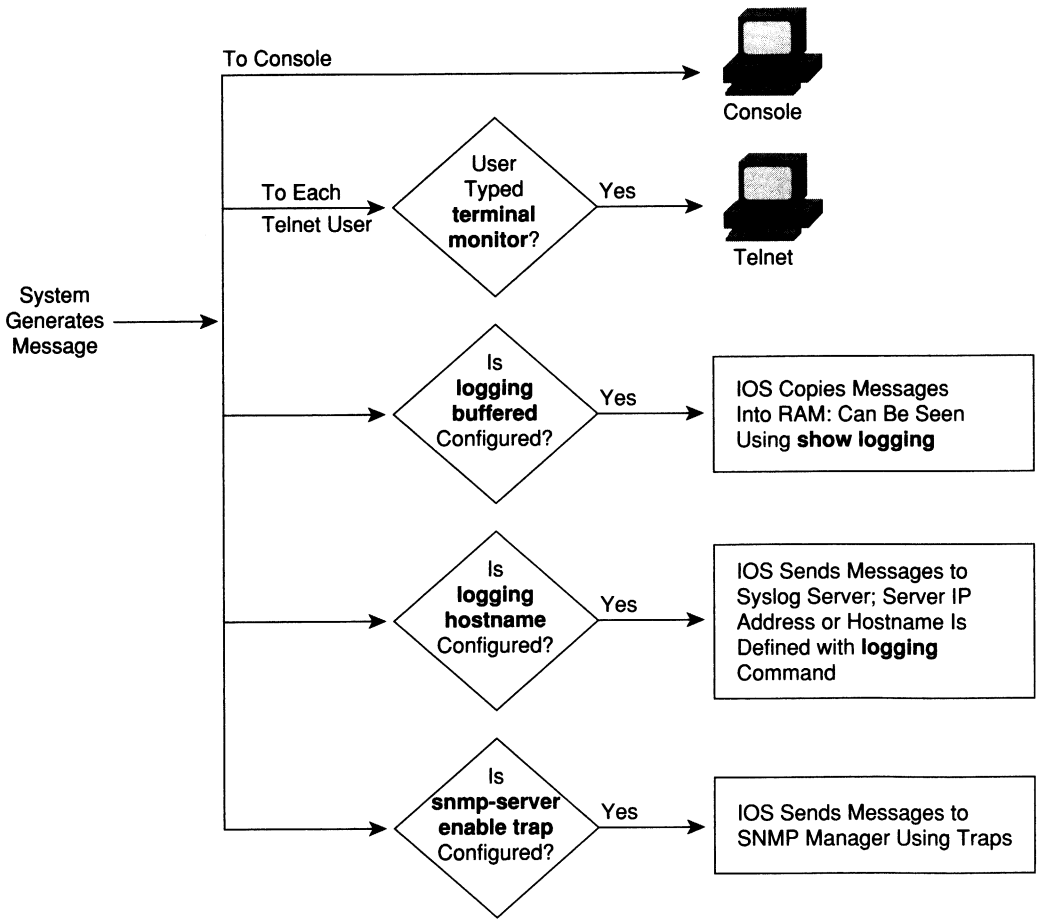


Figure 2-17 summarizes the flow of syslog messages, including debug messages.

Figure 2-17 *Syslog Message Flows*



Q&A

As mentioned in Chapter 1, the questions and scenarios in this book are more difficult than what you should experience on the actual exam. The questions do not attempt to cover more breadth or depth than the exam; however, they are designed to make sure that you know the answer. Rather than allowing you to derive the answer from clues hidden inside the question itself, the questions challenge your understanding and recall of the subject. Questions from the "Do I Know This Already?" quiz from the beginning of the chapter are repeated here to ensure that you have mastered the chapter's topic areas. Hopefully, these questions will help limit the number of exam questions on which you narrow your choices to two options and then guess. Make sure to use the CD and take the simulated exams.

The answers to these questions can be found in Appendix A, on page 703.

1 What are the two names for the router's mode of operation that, when accessed, enables you to issue commands that could be disruptive to router operations?

2 What are three methods of logging on to a router?

3 What is the name of the user interface mode of operation used when you cannot issue disruptive commands?

4 Can the auxiliary port be used for anything besides remote modem user access to a router? If so, what other purpose can it serve?

5 How many console ports can be installed on a Cisco 7500 router?

6 What command would you use to receive command help if you knew that a **show** command option begins with a **c**, but you cannot recall the option?

7 While you are logged in to a router, you issue the command **copy ?** and get a response of "Unknown command, computer name, or host." Offer an explanation as to why this error message appears.

8 Is the number of retrievable commands based on the number of characters in each command, or is it simply a number of commands, regardless of their size?

9 How can you retrieve a previously used command? (Name two ways.)

10 After typing **show ip route**, which is the only command you typed since logging in to the router, you now want to issue the **show ip arp** command. What steps would you take to execute this command by using command recall keystrokes?

11 After typing **show ip route 128.1.1.0**, you now want to issue the command **show ip route 128.1.4.0**. What steps would you take to do so, using command recall and command editing keystrokes?

12 What configuration command causes the router to require a password from a user at the console? What configuration mode context must you be in—that is, what command(s) must be typed before this command after entering configuration mode? List the commands in the order in which they must be typed while in config mode.

13 What configuration command is used to tell the router the password that is required at the console? What configuration mode context must you be in—that is, what command(s) must you type before this command after entering configuration mode? List the commands in the order in which they must be typed while in config mode.

14 What are the primary purposes of Flash memory in a Cisco router?

15 What is the intended purpose of NVRAM memory in a Cisco router?

16 What does the NV stand for in NVRAM?

17 What is the intended purpose of RAM in a Cisco router?

18 What is the main purpose of ROM in a Cisco router?

19 What configuration command would be needed to cause a router to use an IOS image named c2500-j-l.112-14.bin on TFTP server 128.1.1.1 when the router is reloaded? If you forgot the first parameter of this command, what steps must you take to learn the correct parameters and add the command to the configuration? (Assume that you are not logged in to the router when you start.)

20 What command sets the password that would be required after typing the **enable** command? Is that password encrypted by default?

21 To have the correct syntax, what must you add to the following configuration command:

```
banner This is Ivan Denisovich's Gorno Router – Do Not Use
```

22 Name two commands that affect the text used as the command prompt.

23 When using setup mode, you are prompted at the end of the process as to whether you want to use the configuration parameters you just typed in. Which type of memory is this configuration stored into if you type yes?

24 What two methods could a router administrator use to cause a router to load the IOS stored in ROM?

25 What could a router administrator do to cause a router to load file xyz123.bin from TFTP server 128.1.1.1 upon the next reload? Is there more than one way to accomplish this?

26 What is the process used to update the contents of Flash memory so that a new IOS in a file called c4500-d-mz.120-5.bin on TFTP server 128.1.1.1 is copied into Flash memory?

27 Name three possible problems that could prevent the command **boot system tftp c2500-j-l.112-14.bin 128.1.1.1** from succeeding.

28 Two different IOS files are in a router's Flash memory: one called c2500-j-l.111-3.bin and one called c2500-j-l.112-14.bin. Which one does the router use when it boots up? How could you force the other IOS file to be used? Without looking at the router configuration, what command could be used to discover which file was used for the latest boot of the router?

29 What does CDP stand for?

30 On what type of interfaces is CDP enabled by default? (Assume IOS versions 11.0 and later.)

31 What command can be used to provide as much detailed information as possible with CDP?

32 Is the password required at the console the same one that is required when Telnet is used to access a router?

33 How could a router administrator disable CDP?

34 Which IP routing protocols could be enabled using setup?

35 Name two commands used to view the configuration to be used at the next reload of the router. Which one is a more recent addition to the IOS?

36 Name two commands used to view the configuration that is currently used in a router. Which one is a more recent addition to the IOS?

37 True or False: The **copy startup-config running-config** command always changes the currently used configuration for this router to exactly match what is in the startup configuration file. Explain.

Scenarios

Scenario 2-1

Compare the following output in Example 2-7 and Example 2-8. Example 2-7 was gathered at 11:00 a.m., 30 minutes earlier than Example 2-8. What can you definitively say happened to this router during the intervening half hour?

Example 2-7 *11:00 a.m.* ***show running-config***

```
hostname Gorno
!
enable password cisco
!
interface Serial0
 ip address 134.141.12.1 255.255.255.0
!
interface Serial1
 ip address 134.141.13.1 255.255.255.0
!
interface Ethernet0
 ip address 134.141.1.1 255.255.255.0
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
```

Example 2-8 *11:30 a.m.* ***show running-config***

```
hostname SouthernSiberia
prompt Gorno
!
enable secret $8df003j56ske92
enable password cisco
!
interface Serial0
 ip address 134.141.12.1 255.255.255.0
!
interface Serial1
 ip address 134.141.13.1 255.255.255.0
!
interface Ethernet0
 ip address 134.141.1.1 255.255.255.0
 no cdp enable
```

continues

Example 2-8 *11:30 a.m.* ***show running-config*** *(Continued)*

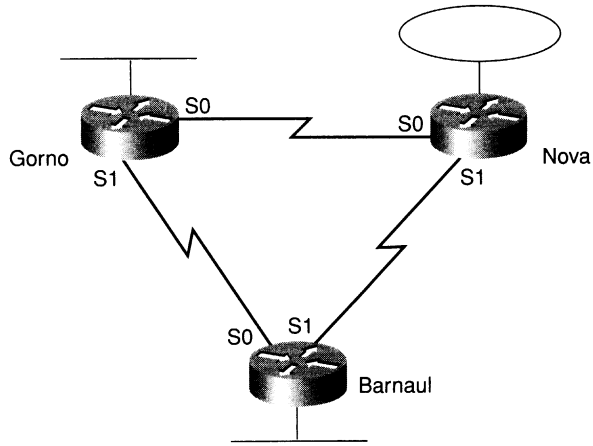
```
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 Login
```

Questions on Scenario 2-1

1 During the process of changing the configuration in Scenario 2-1, the command prompt temporarily was **SouthernSiberia(config)#**. What configuration commands, and in what order, could have changed the configuration as shown and allowed the prompt to temporarily be **SouthernSiberia(config)#**?

2 Assuming that Figure 2-18 is complete, what effect does the **no cdp enable** command have?

Figure 2-18 *Siberian Enterprises' Sample Network*



3 What effect would the **no enable password cisco** command have at this point?

Scenario 2-2

Example 2-9 shows that the **running-config** command was executed on the Nova router.

Example 2-9 *Configuration of Router Nova*

```
hostname Nova
banner # This is the router in Nova Sibiersk; Dress warmly before entering! #
!
boot system tftp c2500-js-113.bin 134.141.88.3
boot system flash c2500-j-l.111-9.bin
boot system rom
!
enable password cisco
!
interface Serial0
 ip address 134.141.12.2 255.255.255.0
!
interface Serial1
 ip address 134.141.23.2 255.255.255.0
!
interface TokenRing0
 ip address 134.141.2.2 255.255.255.0
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
```

Questions on Scenario 2-2

1 If this is all the information that you have, what IOS do you expect will be loaded when the user reloads Nova?

2 Examine the following command output in Example 2-10, taken immediately before the user is going to type the **reload** command. What IOS do you expect will be loaded?

Example 2-10 ***show ip route*** *on Nova*

```
Nova#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set
```

continues

Example 2-10 *show ip route on Nova (Continued)*

```
     134.141.0.0/24 is subnetted, 6 subnets
C       134.141.2.0 is directly connected, TokenRing0
R       134.141.3.0 [120/1] via 134.141.23.3, 00:00:15, Serial1
R       134.141.1.0 [120/1] via 134.141.12.1, 00:00:20, Serial0
C       134.141.12.0 is directly connected, Serial0
R       134.141.13.0 [120/1] via 134.141.12.1, 00:00:20, Serial0
                     [120/1] via 134.141.23.3, 00:00:15, Serial1
C       134.141.23.0 is directly connected, Serial1
```

3 Now examine the following **show flash** command in Example 2-11, which was issued immediately after the **show ip route** command in Example 2-10, but before the user issued the **reload** command. What IOS do you think would be loaded in this case?

Example 2-11 *show flash on Router Nova*

```
Nova#show flash
4096K bytes of flash memory sized on embedded flash.
File   name/status
 0 c2500-j-l.111-3.bin
[682680/4194304 bytes free/total]
```

4 Now examine the configuration in Example 2-12. Assume that there is now a route to 134.141.88.0 and that the file c2500-j-l.111-9.bin is an IOS image in Flash memory. What IOS do you expect will be loaded now?

Example 2-12 *show running-config on Router Nova*

```
 hostname Nova
banner # This is the router in Nova Sibiersk; Dress warmly before entering! #
!
boot system tftp c2500-js-113.bin 134.141.88.3
boot system flash c2500-j-l.111-9.bin
!
enable password cisco
!
interface Serial0
 ip address 134.141.12.2 255.255.255.0
!
interface Serial1
 ip address 134.141.23.2 255.255.255.0
!
interface Ethernet0
 ip address 134.141.2.2 255.255.255.0
!
router rip
 network 134.141.0.0
!
line con 0
 password cisco
 login
```

Example 2-12 ***show running-config*** *on Router Nova (Continued)*

```
line aux 0
line vty 0 4
 password cisco
 login
!
config-register 0x2101
```

Answers to Scenarios

Scenario 2-1 Answers

In Scenario 2-1, the following commands were added to the configuration:

- **enable secret** as a global command.
- **prompt** as a global command.
- **no cdp enable** as an Ethernet0 subcommand.
- The **hostname** command also was changed.

The scenario questions' answers are as follows:

1 If the host name was changed to *SouthSiberia* first and the **prompt** command was added next, the prompt would have temporarily been *SouthSiberia*. Configuration commands are added to the RAM configuration file immediately and are used. In this case, when the **prompt** command was added, it caused the router to use "Gorno," not the then-current host name "SouthernSiberia," as the prompt.

2 No practical effect takes place. Because no other Cisco CDP-enabled devices are on that Ethernet, CDP messages from Gorno are useless. So, the only effect is to lessen the overhead on that Ethernet in a very small way.

3 No effect takes place other than cleaning up the configuration file. The **enable password** is not used if an **enable secret** is configured.

Scenario 2-2 Answers

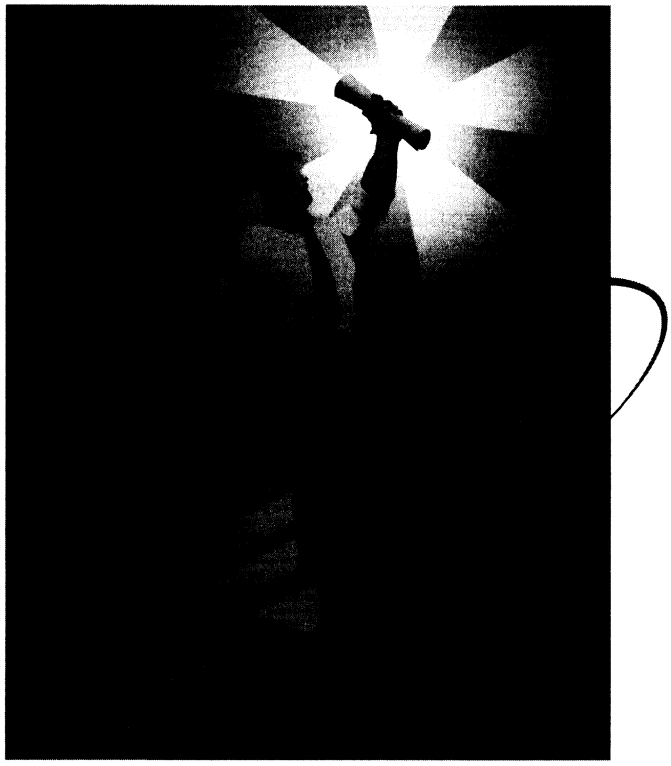
The answers to the questions in Scenario 2-2 are as follows:

1 The first boot system statement would be used: **boot system tftp c2500-js-113.bin 134.141.88.3**.

2 The **boot system flash** command would be used. The TFTP boot would presumably fail because there is not currently a route to the subnet of which the TFTP server is a part. It is reasonable to assume that a route would not be learned 2 minutes later when the router had reloaded. So, the next **boot system** command (**flash**) would be used.

3 The **boot system ROM** command would be used. Because there is no file in Flash called c2500-j-l.111-9.bin, the boot from Flash memory would fail as well, leaving only one **boot** command.

4 The IOS from ROM would be loaded due to the configuration register. If the configuration register boot field is set to 0x1, **boot system** commands are ignored. So, having a route to the 134.141.88.0/24 subnet and having c2500-j-l.111-9.bin in Flash memory does not help.



from Designing Cisco Networks

by Diane Teare

(1-57870-105-8)

Cisco Press

About the Editor

Diane Teare is a Senior Network Architect with GeoTrain Corporation, Cisco's largest worldwide training partner, where she provides training and consulting services to customers in North America and Europe. Diane is a Cisco Certified Systems Instructor with more than 14 years experience in teaching; course design; design, implementation, and troubleshooting of network hardware and software; and project management. She is the Master Instructor for the ICRC, ACRC, and DCN courses at GeoTrain. Diane has a Bachelors of Applied Science in Electrical Engineering and a Masters of Applied Science in Management Science.

Contents at a Glance

Bold chapters are elements included in this folio.

You will need approximately three hours to read this chapter and complete its exercises. Upon completion of this fourth chapter in Part IV, you will be able to do the following:

- Propose an addressing model for the customer's areas, networks, subnetworks, and end stations that meets scalability requirements.
- Propose a plan for configuring addresses.
- Propose a naming scheme for servers, routers, and user stations.

CHAPTER 8

Designing a Network Layer Addressing and Naming Model

This chapter includes some tables and other job aids you will find useful when completing the case studies at the end of the chapter. References to some WWW sites are also included; relevant information has been extracted from these sites and is provided in the chapter. If you have access to the Internet, you might want to access the sites mentioned to obtain detailed information related to specific topics. All the sites referenced in this chapter are also listed in Appendix C, "Interesting WWW Links and Other Suggested Readings."

Follow these steps to complete this chapter:

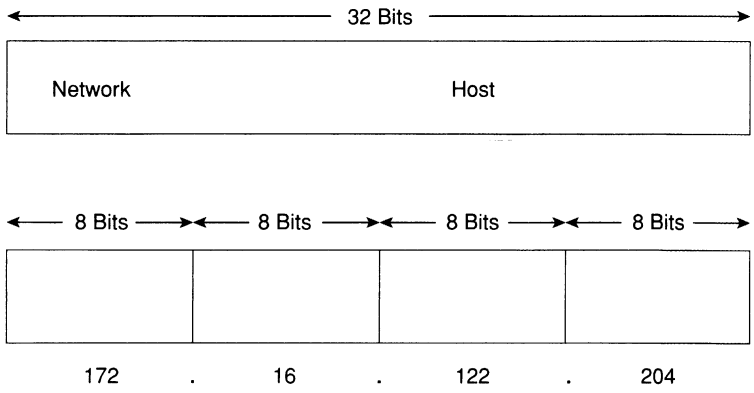
1. Study the chapter content, including any tables and job aids that appear.
2. Review the case studies at the end of this chapter.
3. Complete the questions in each case study.
4. Review the answers provided by our internetworking experts in Appendix B, "Answers to Chapter Questions, Case Studies, and Sample CCDA Exam."

Designing network layer addressing and naming is one of the most important tasks in internetwork design. It is closely linked with selecting a routing protocol, which is discussed in the next chapter, "Selecting Routing and Bridging Protocols." This chapter discusses some specifics for IP addressing, including variable-length subnet masking, route summarization, private addressing, and address translation, and some specifics for IPX addressing. The steps to follow when designing this aspect of your network are then identified.

IP Addressing

Recall that IP addresses are 32 bits, as shown in Figure 8-1. The 32 bits are grouped into four sets of eight bits (octets), separated by dots, and represented in decimal format; this is known as dotted decimal notation. As in all network layer addresses, part of a device's address represents the network, and part identifies the host number that this device is on that network. IP networks can also be subdivided into subnetworks.

Figure 8-1 *IP Addresses Are 32 Bits, Written in Dotted Decimal Format*



IP addressing defines five address classes: A, B, C, D, and E. Only Classes A, B, and C are available for addressing devices; Class D is used for multicast groups, and Class E is reserved for experimental use.

The first octet of an address defines its class, as illustrated in Table 8-1. The bits that represent network and subnet information in an IP address are known as the *prefix*; the number of such bits is known as the *prefix length*. The *Prefix Length* column in Table 8-1 indicates the default prefix lengths for the three classes of addresses.

Table 8-1 *IP Address Classes A, B, and C Are Available for Addressing Devices*

Class	Format (N= network number, H= host number)	Prefix Length	Higher-Order Bit(s)	Address Range
Class A	N.H.H.H	8 bits	0	1.0.0.0 to 126.0.0.0
Class B	N.N.H.H	16 bits	10	128.0.0.0 to 191.255.0.0
Class C	N.N.N.H	24 bits	110	192.0.0.0 to 223.255.255.0

Reference: RFC 1700, available at http://info.internet.isi.edu/in-notes/rfc/files/rfc1700.txt

A prefix identifies a block of host numbers and is used for routing to that block. According to RFC 1518, *An Architecture for IP Address Allocation with CIDR*, available at http://info.internet.isi.edu/in-notes/rfc/files/rfc1518.txt, a prefix is "an IP address and some indication of the leftmost contiguous significant bits within that address." The indication of the leftmost contiguous bits has traditionally been done with an indication of the address class and a subnet mask. More recently, a length indication has followed a network number and slash. For example, 172.16.168.0/21 indicates that the most significant 21 bits are the prefix; this is equivalent to the address 172.16.168.0 with the subnet mask of 255.255.248.0.

Further information about IP addressing is available in Chapter 1, "Internetworking Technology Review," and in the *Basic IP Addressing and Troubleshooting Guide*, available at http://www.cisco.com/warp/public/779/smbiz/service/troubleshooting/ts_ip.htm.

Classful and Classless Routing Protocols, and Variable-Length Subnet Masking

A *major network* is a Class A, B, or C network; usually, major networks are subnetted to allow the IP addresses to be allocated more efficiently. Traditional *classful routing protocols* (for example, RIP and IGRP) do not transmit any information about the prefix length. When receiving information about routes within the same major network, hosts and routers assume the same prefix length as that on the incoming interface of the route information. Classful routing protocols therefore do not accommodate different prefix lengths being used within a major network.

When receiving information about routes in a different major network, hosts and routers running a classful routing protocol calculate the prefix length by looking at the first few bits of the address to determine the class of the address, as specified in Table 8-1. The prefix length associated with that class of address is then assumed.

Classless routing protocols (for example, OSPF), on the other hand, do include the prefix length with routing updates; routers running classless routing protocols do not have to determine the prefix themselves. Therefore, different prefix lengths within a major network are allowed; this is called variable-length subnet masking (VLSM).

VLSM relies on providing prefix length information explicitly with each use of an address. The length of the prefix is evaluated independently at each place it is used. The capability to have a different prefix length at different points supports more efficient use of the IP address space and reduces routing traffic. Efficient addressing of large subnets (for example, an Ethernet with many hosts) and small subnets (for example, a point-to-point serial line with only two hosts) are allowed. If the small subnets are grouped, routing information can be summarized (aggregated) into fewer routing table entries.

Designing IP Addressing to Facilitate Route Summarization

Whether using VLSM or not, when designing IP addressing it is important to design route summarization, also referred to as *route aggregation* or *supernetting*.

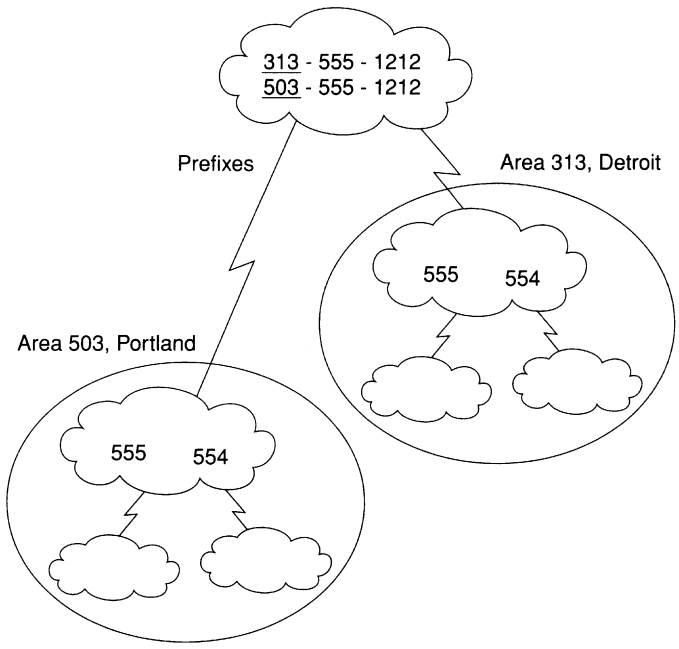
With route summarization, one route in the routing table represents many other routes. Summarizing routes reduces the number of routes in the routing table, the routing update traffic, and overall router overhead.

Reducing routing update traffic can be very important on low-speed lines. If the Internet had not adapted route summarization by standardizing on classless interdomain routing (CIDR), it would not have survived.

NOTE Classless interdomain routing (CIDR) is a mechanism developed to help alleviate the problem of exhaustion of IP addresses. The idea behind CIDR is that multiple Class C addresses can be combined, or aggregated, to create a larger (that is, more hosts allowed) classless set of IP addresses. CIDR is described in RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*, available at: http://info.internet.isi.edu/in-notes/rfc/files/rfc1519.txt.

The telephone architecture has handled *prefix routing*, or routing based only on the prefix part of the address, for many years. For example, as shown in Figure 8-2, a telephone switch in Detroit, Michigan does not need to know how to reach a specific line in Portland, Oregon. It just needs to recognize that the call is not local. A long-distance carrier needs to recognize that 503 is for Oregon but does not need to know the details of how to reach the specific line in Oregon.

Figure 8-2 *The Telephone Network Uses Prefix Routing; a Switch Does Not Need to Know How to Reach Every Specific Line*



Prefix routing is not new in the IP environment either. A router needs to know only how to reach the next hop. It does not need to know the details of how to reach an end node that is not local. Much as in the telephone example, IP routers make hierarchical decisions. Recall that an IP

address is comprised of a prefix part and a host part. Routers use the prefix to determine the path for a destination address that is not local. The host part is used to reach local hosts.

For summarization to work correctly, the following requirements must be met:

- Multiple IP addresses must share the same leftmost bits.
- Routers must base their routing decisions on a 32-bit IP address and a prefix length that can be up to 32 bits.
- Routing protocols must carry the prefix length with the 32-bit IP address.

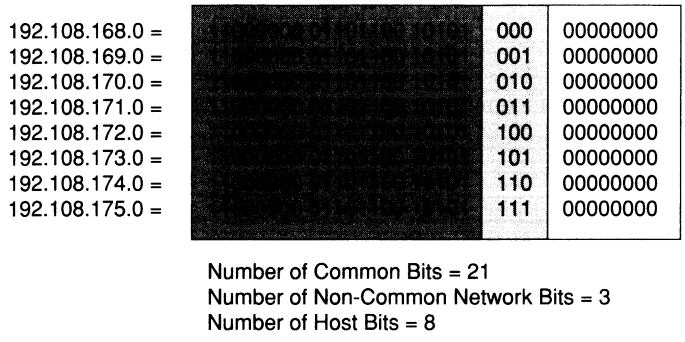
As an example, assume that a router has the following networks behind it:

192.108.168.0
192.108.169.0
192.108.170.0
192.108.171.0
192.108.172.0
192.108.173.0
192.108.174.0
192.108.175.0

Each of these networks could be advertised separately; however, this would mean advertising eight routes. Instead, this router can summarize the eight routes into one route, and advertise 192.108.168.0/21. By advertising this one route, the router is saying, "*Route packets to me if the destination has the first 21 bits the same as the first 21 bits of 192.108.168.0.*"

Figure 8-3 illustrates how this summary route is determined. The addresses all have the first 21 bits in common and include all the combinations of the other 3 bits in the network portion of the address; therefore, only the first 21 bits are needed to determine if the router can route to one of these specific addresses.

Figure 8-3 *To Summarize Routes, Find the Common Bits*



Changing IP Addresses

IP addresses used by organizations are likely to undergo changes for a variety of reasons, including the following:

- Enterprise reorganization (for example, people move to different workgroups)
- Physical moving of equipment
- New strategic relationships (for example, merging with another company and merging the networks as well)
- Changing of the Internet service provider (ISP) used to connect to the Internet
- New applications
- The needs of global Internet connectivity (for example, connecting a network to the Internet that was previously standalone)
- Route summarization implementation (for example, redesigning the addressing of your network to facilitate summarization, as elaborated earlier in this chapter)

Therefore, network designers need to devise IP addressing schemes that allow for changes and growth.

Howard Berkowitz, an engineer with a Cisco Training Partner, and Paul Ferguson, a Cisco consulting engineer, have written a document on IP renumbering titled *Network Renumbering Overview: Why would I want it and what is it anyway?* This paper is available at http://info.internet.isi.edu/in-notes/rfc/files/rfc2071.txt.

Howard Berkowitz has also written a helpful draft RFC that outlines the steps for router renumbering titled *Router Renumbering Guide*. It is available at http://info.internet.isi.edu/in-notes/rfc/files/rfc2072.txt.

IP Addressing with Cisco's DNS/DHCP Manager

In IP environments, names of devices are mapped to addresses using the Domain Name Service (DNS) protocol. Addresses can be dynamically assigned using the Dynamic Host Configuration Protocol (DHCP). Cisco has a DNS/DHCP Manager that enables you to synchronize DNS names with addresses dynamically assigned by DHCP. Cisco's product catalog available at http://www.cisco.com/univercd/cc/td/doc/pcat has a section on the DNS/DHCP Manager. Excerpts from this section are reproduced here:

> The Cisco DNS/DHCP Manager is a suite of TCP/IP management applications that manage domain names and synchronize IP addresses between a Domain Name System (DNS) server and a Dynamic Host Configuration Protocol (DHCP). The Cisco DNS/DHCP Manager includes the Domain Name Manager—a graphical DNS management tool—and a DHCP server that dynamically updates DNS with IP addresses assigned to DHCP clients. The Cisco DNS/DHCP Manager also includes a DNS server, Trivial File Transfer Protocol (TFTP) server, Network Time Protocol (NTP) server, and a Syslog server.
>
> Managing a large TCP/IP network requires maintaining accurate and up-to-date IP address and domain name information. Today, organizations are forced to manage IP address and domain name information by manually

modifying several databases. Organizations maintain IP address and domain name information in DNS servers' text-based configuration files. DHCP servers further complicate the situation by dynamically assigning domain names and IP addressees to nodes on the network. Organizations are therefore forced to manually synchronize the configuration of DNS and DHCP servers. Incorrect IP addresses and domain names can cause problems for people using the World Wide Web, a Network File System (NFS), FTP, and e-mail. The Cisco DNS/DHCP Manager eliminates the need for manually configuring and synchronizing DNS and DHCP servers.

The Cisco DNS/DHCP Manager is designed for the following applications:

- Managing DNS
  - Organizations currently manage DNS by editing configuration files that have a complex syntax. This process is time-consuming and subject to error. The Domain Name Manager browser reduces common configuration errors by checking the syntax of each new entry. The Domain Name Manager is easy to learn, and more people in an organization can use it to manage DNS.
  - The Cisco DHCP server automatically updates the Domain Name Manager with the IP address and domain name of the new nodes on the network. The Domain Name Manager then propagates this information to DNS servers on the network.
  - The Domain Name Manager replaces an organization's existing primary DNS server and becomes the source of DNS information for the entire network.
- DHCP in a switched network
  - The Cisco DHCP server allows organizations to use DHCP in a large switched network. The depletion of IP addresses on the Internet has forced organizations to use classless inter-domain routing (CIDR) blocks or groups of Class C network numbers to build physical networks with more than 256 nodes. This has created a problem for network administrators who want to use DHCP on large switched networks with more than 256 nodes.
  - Organizations building large switched networks with TCP/IP assign multiple logical IP networks on a single physical switched network. At the same time, organizations want to take advantage of DHCP to dynamically configure a large number of PCs on their network. The Cisco DHCP server supports address pools that contain multiple logical networks on the same physical network.
- TCP/IP servers for Windows NT
  - The Cisco DNS/DHCP Manager has a complete range of TCP/IP services used to build and maintain a TCP/IP network. The Cisco DNS/DHCP Manager provides a DNS server for name service, an NTP server for time synchronization, TFTP to load binary images and configuration files to network devices (including Cisco routers and switches), and a syslog server for logging error messages from network devices over the network. All these services are easily configured with a graphical user interface.

Private Addresses and Network Address Translation

Private addresses are reserved IP addresses to be used only internally within a company's network. These private addresses are not to be used on the Internet and therefore must be mapped to a company's external registered address when sending anything on the Internet.

RFC 1918, *Address Allocation for Private Internets*, available at http://info.internet.isi.edu/in-notes/rfc/files/rfc1918.txt, defines the private IP addresses.

The private IP addresses are as follows:

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

Network Address Translation (NAT) is a feature in the Cisco IOS™ Release 11.2 software that enables you to translate private addresses into registered IP addresses only when needed, thereby reducing the need for registered IP addresses.

When using NAT, the terms *inside* and *outside* networks are used, as shown in the example in Figure 8-4. Table 8-2 defines the terminology for NAT, as used in Figure 8-4.

Figure 8-4 *Network Address Translation Is Used to Translate Addresses Between the* Inside *and* Outside *Networks*

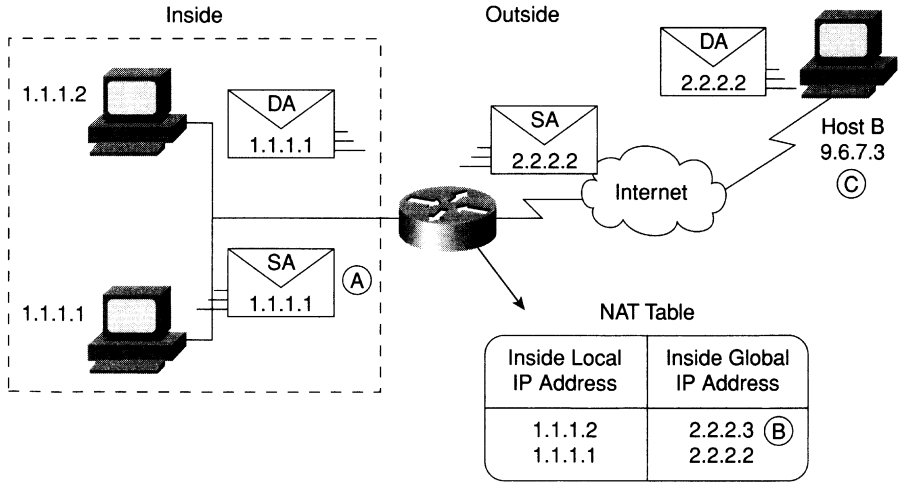


Table 8-2 *NAT Terminology*

Term	Definition
Inside Local IP Address (A)	The IP address assigned to a host on the inside network. The address was globally unique but obsolete, allocated from RFC 1918, *Address Allocation for Private Internet Space*, or randomly picked.
Inside Global IP Address (B)	A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world. The address was allocated from globally unique address space, typically provided by the ISP.
Outside Global IP Address (C)	The IP address that was assigned to a host on the outside network by its owner. The address was allocated from a globally routable address space.
Outside Local IP Address (not shown)	The IP address of an outside host as it appears to the inside network. The address was allocated from address space routable on the inside, or possibly allocated from RFC 1918, for example.

Cisco supported NAT features include the following:

- **Static address translation**—Establishes a one-to-one mapping between inside local and global addresses.
- **Dynamic source address translation**—Establishes a dynamic mapping between the inside local and global addresses. This is accomplished by describing the local addresses to be translated, the pool of addresses from which to allocate global addresses, and associating the two. The router will create translations as needed.
- **Address overloading**—Conserves addresses in the inside global address pool by allowing source ports in TCP connections or UDP conversations to be translated. When different inside local addresses map to the same inside global address, each inside host's TCP or UDP port numbers are used to distinguish between them.
- **TCP load distribution**—A dynamic form of destination translation that can be configured for some outside-to-inside traffic. Once a mapping is defined, destination addresses matching an access list are replaced with an address from a rotary pool. Allocation is done on a round-robin basis, and only when a new connection is opened from the outside to the inside. All non-TCP traffic will be passed untranslated (unless other translations are in effect).

For details of NAT operation and configuration see Appendix H, "Network Address Translation."

Dynamic Router IP Addressing

Routers usually are configured with fixed, static IP addresses, while PCs and other hosts may be assigned dynamic addresses. Easy IP is a feature available on selected routers beginning with Cisco IOS™ Release 11.3 that includes dynamic WAN interface IP address negotiation for routers, thereby reducing router configuration tasks and conserving IP addresses.

Details on the Easy IP feature are available on Cisco's web site at http://www.cisco.com/warp/customer/cc/cisco/mkt/ios/nat/tech/ezip1_wp.htm. Excerpts from this web site are reproduced here:

Cisco IOS Easy IP is a combination of the following functionality:

- Port Address Translation (PAT), a subset of Network Address Translation (NAT)
- Dynamic PPP/IPCP WAN interface IP address negotiation
- Cisco IOS DHCP Server

With Cisco IOS Easy IP, router configuration tasks are minimized: simply plug-in the router, configure the dialup number for a central access server, and connect the LAN devices to the router. With Cisco IOS Easy IP, a Cisco router automatically assigns local IP addresses to SOHO hosts via the Dynamic Host Configuration Protocol (DHCP) with the Cisco IOS DHCP Server, automatically negotiates its own registered IP address from a central server via the Point-to-Point Protocol/Internet Control Protocol (PPP/IPCP), and uses Port Address Translation (PAT) functionality to enable all SOHO hosts to access the global Internet using a single registered IP address. Because Cisco IOS Easy IP utilizes existing port-level multiplexed Network Address Translation (NAT) functionality within Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet, making the remote LAN more secure.

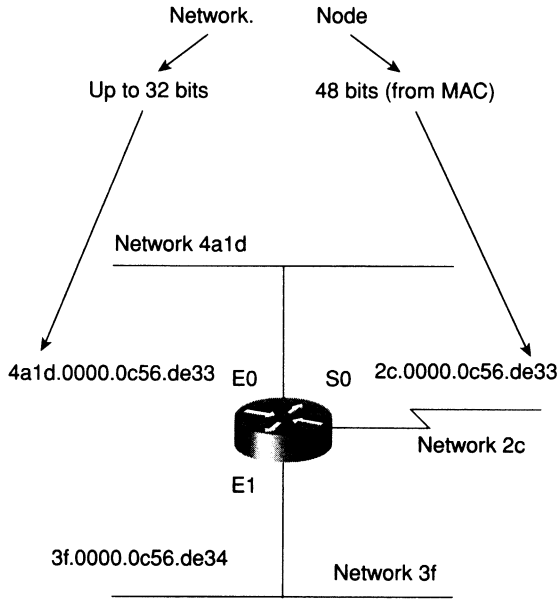
IPX Addressing

A Novell Internetwork Packet Exchange (IPX) address has two parts: the network number and the node number. An IPX address is 80 bits long, with 32 bits (4 octets, or 8 hexadecimal digits) for the network number and 48 bits (6 octets, or 12 hexadecimal digits) for the node number. The node number is typically derived from the Media Access Control (MAC) address of an interface. IPX addresses are written in hexadecimal digits.

IPX Address Example

Figure 8-5 illustrates an example of IPX addressing.

Figure 8-5 *A Novell IPX Address Has Two Parts—the Network Number and the Node Number*



In the IPX example in Figure 8-5, the following is true:

- One IPX network has an address of 4a1d. Other IPX networks shown are 2c and 3f. Note that IPX network numbers are 32 bits long (8 hexadecimal digits), but you do not have to specify leading zeros.
- The IPX node number is 48 bits (12 hexadecimal digits) in length. This number is usually the MAC address obtained from a router interface that has a MAC address.
- The example features the IPX node 0000.0c56.de33. Another node address is 0000.0c56.de34.
- The same node number appears for both the E0 and S0 interfaces of the router. Serial interfaces do not have MAC addresses, so Novell IPX obtained this node number for S0 by using the MAC address from E0.

Each interface retains its own IPX address. The use of the MAC address in the logical address eliminates the need for an Address Resolution Protocol (ARP).

Selecting IPX Addresses

You must use a valid IPX network address when you configure a Cisco router. The IPX network address refers to the *wire*. All devices on the same wire, including routers, must share the same IPX network address.

Because the Novell NetWare networks are probably already established, customers will likely have existing IPX addresses. Determine the IPX address to use for the router using the existing IPX address scheme.

The first and recommended way to find out which network address to use is to ask the NetWare administrator. Make sure that the NetWare administrator specifies the IPX network address for the same network where you want to enable IPX on your Cisco router. The Cisco router must use the same network as the NetWare file server (or other source of the address) specified by the NetWare administrator.

If you cannot obtain an IPX address to use from the NetWare administrator, you can get the neighbor's IPX address directly from a neighbor router. Use any one of the following methods to obtain the IPX address:

- If the neighbor router is another Cisco router, you can use the Cisco Discovery Protocol (CDP) to learn the neighbor's address. Use the **show cdp neighbor detail** command to view this information.
- You can Telnet to the neighbor router, enter the appropriate mode, then display the running configuration on the neighbor.
- If the neighbor router is not a Cisco router (for example, it is a NetWare PC-based router, or a NetWare file server), you may be able to attach or log in and use a NetWare utility *config* to determine the address.

Steps for Designing Network Layer Addressing and Naming

The features of IP and IPX addressing discussed in this chapter are used when designing the network layer addressing and naming of your network. This section identifies eight steps to use in this aspect of your design.

Step 1: Design a Hierarchy for Addressing

Design a hierarchy for addressing as follows:

- Autonomous systems
- Areas
- Networks
- Subnetworks
- End stations

The hierarchy that you use will depend on the network layer protocol and routing protocol that you are using.

Step 2: Design Route Summarization

Summarization, also known as *aggregation,* allows one route to represent many routes, resulting in smaller routing tables. Route summarization is discussed in detail earlier in this chapter.

Step 3: Design a Plan for Distributing Administrative Authority for Addressing and Naming at the Lower Levels of the Hierarchy

Once the high-level plan is made for the network, lower-level addressing and naming may be delegated. For example, if the client has offices in Europe and Asia, as well as North America, the authority to name devices and assign addresses, within established guidelines, could be divided along these geographical lines.

Step 4: Design a Method for Mapping Geographical Locations to Network Numbers

Assigning network numbers by geographical location will also aid in the summarization task. For example, the client who has offices in Europe, Asia, and North America could assign a range of addresses to each continent (with the authority to distribute addresses within the range resting within the appropriate continent office). The summarized address for each continent would then encompass the entire range of addresses assigned to that continent.

Step 5: Develop a Plan for Identifying Special Stations Such as Routers and Servers with Specific Node IDs

To facilitate troubleshooting, devices such as routers and servers should have fixed addresses. For example, all routers could have an IP address with the node part in the range of 1 through 19, while all servers have the node part of their addresses in the range of 20 through 29. Then, if during troubleshooting there is a problem with an address that has a node part of 25, it is immediately obvious that this address belongs to a server.

Step 6: Develop a Plan for Configuring User Station Addresses

For scalability, user station addresses should be assigned dynamically, rather than statically, if possible. Dynamic address assignment allows the automatic assignment of addresses from a pool of addresses as user stations join the network; the addresses are released back into the pool if the device leaves the network. This simplifies the network administrator's task of changing IP addresses on user stations when users move to a new location, for example.

Use the Bootstrap Protocol (BOOTP) or the newer Dynamic Host Configuration Protocol (DHCP) for dynamic IP address assignment. Cisco's DNS/DHCP Manager product, described earlier in this chapter, can be used to aid in this task.

Step 7: If Necessary, Develop a Plan for Using Gateways to Map Private Addresses to External Addresses

As noted earlier, private addresses are reserved IP addresses to be used only within a company's network. These private addresses are not to be used on the Internet and therefore must be mapped to a company's external addresses when sending anything on the Internet. Use the Cisco IOS Network Address Translation (NAT) feature described earlier in this chapter to do this mapping.

Step 8: Design a Scheme for Naming Servers, Routers, and User Stations

Names should be meaningful to facilitate troubleshooting. For example, in the company with offices in Europe, Asia, and North America, the router and server names could all start with an abbreviation of the continent: EUR, ASIA, and NA. This could be suffixed with the last octet of the device's node address—for example, ERU03 for a router. The user's PCs could all have names that start with the abbreviation for the continent, followed by the letters PC, a hyphen, and the user's first initial and last name. An example is EURPC-JSMITH.

To name devices in IP environments, install and configure DNS servers. Use Cisco's DNS/DHCP Manager, described earlier in this chapter, to synchronize DNS names with dynamically assigned IP addresses.

Summary

In this chapter you learned about IP addressing, including address classes, prefix lengths, and summarization. You also learned considerations for IPX addressing and identified steps for designing your network layer addressing and naming model. In the case studies that follow you have the opportunity to apply what you have learned to assign addresses and names for the networks.

The next chapter in Part IV reviews routing and bridging protocols and discusses how to select the right ones for your network.

Case Studies

In this section, you are asked to implement an addressing and naming scheme for the four case studies introduced in Chapter 3, "Characterizing the Existing Network," as well as for a new case study about Virtual University.

Read each case study description and complete the questions for each of the case studies.

TIP As mentioned, in working through the questions to the case studies, you may find it useful to work on some note paper in a separate binder to accommodate the depth of these exercises.

After you complete each question, you can refer to the solutions provided by our internetworking experts in Appendix B. Keep in mind that there are potentially several correct answers to each question. These case studies and their solutions will help you prepare for the Sylvan CCDA exam following the course.

Case Study: Virtual University

Read the following short case study and answer the questions that follow.

Virtual University has decided to eliminate AppleTalk and use only IP. The university will use the IP network number 172.16.0.0. The university has a North Campus, Central Campus, and South Campus. Each campus has 40 networks and each network has 150 nodes. The network administrators expect to expand to 60 networks and 200 nodes per network within the next five years.

Because of its AppleTalk heritage, Virtual University needs a simple addressing solution with very little end-node configuration. Despite its AppleTalk heritage, Virtual University has some knowledgeable IP gurus who have specified that the addressing scheme must be conducive to route summarization (aggregation).

Virtual University Case Study Questions

Question 8-1

Design and describe a model for dividing up Virtual University's IP address space that will meet the university's current needs and needs for the next five years.

Question 8-2

Explain to the IP gurus at Virtual University how the addressing model that you designed in the previous step will support route summarization. For example, what network number and prefix could a border router at one of the campuses advertise to the other areas or backbone?

Question 8-3

What is special about IP address 172.16.0.0? What will Virtual University require to connect its network to the Internet?

Question 8-4

Propose a plan for naming servers, routers, and end nodes. Describe both the names themselves and the method you will use to configure the names.

Case Study: CareTaker Publications

You might want to review the CareTaker case study description in Appendix A, "Case Studies," page 303, before proceeding to answer the questions in this section.

CareTaker Case Study Questions

Refer to the topology drawing you created for CareTaker Publications in Chapter 3 or review the topology drawing solution provided in Appendix B. In this section you will design an addressing scheme for the network.

The parent corporation, Holdings International (HI), told CareTaker that CareTaker will be protected from Internet "hackers" with a firewall at the corporate facilities. HI has informed CareTaker that it will receive only one Class C address because of the limited number of IP addresses available. CareTaker is to implement *Big Internet* addressing (that is, addressing that will not restrict it from going on the Internet) within the confines of CareTaker.

Question 8-5

Design a model for CareTaker's IP address space that will meet the current needs and needs for the next five years. Describe your model here.

Question 8-6

Propose a plan for naming servers, routers, and end nodes. Describe both the names themselves and the method to be used to configure the names.

Question 8-7

Update your topology diagram to reflect your addressing scheme.

Case Study: PH Network Services Corporation

You may wish to review the PH Network Services Corporation case study description in Appendix A, page 306, before proceeding to answer the questions in this section.

PH Network Services Corporation Case Study Questions

Refer to the topology drawing you created for Mr. Pero in Chapter 3 or review the topology drawing solution provided in Appendix B. In this section, you will design an addressing scheme for the network.

Question 8-8

The hospital system has an existing IP network with its own IP addresses. The hospital will be able to assign two Class C addresses to the PH Network: one for the WAN (202.12.27.0) and one for PH's internal use (202.12.28.0). Describe your IP addressing plans for the implementation of PH's network. You will use a Class C mask of 255.255.255.0 for the PH LAN. What mask will you use for the WAN?

Question 8-9

Update your topology diagram to reflect the new addressing scheme.

Case Study: Pretty Paper Limited

You might want to review the Pretty Paper Limited case study in Appendix A, page 307, before proceeding to answer the questions in this section.

Pretty Paper Limited Case Study Questions

Refer to the topology drawing you created for Pretty Paper in Chapter 3 or review the topology drawing solution provided in Appendix B. In this section you will design an addressing scheme for the network.

Question 8-10

The network administrator has been using the Class B IP address of 199.151.0.0. He does not know where he got it but he is sure that Pretty Paper does not own it. What are your recommendations for an IP address allocation/assignment procedure?

Question 8-11

Propose a plan for naming servers, routers, and end nodes. Describe both the names themselves and the method you will use to configure the names.

Question 8-12

Update your topology diagram to reflect the new IP addressing scheme.

Question 8-13

Recommend an addressing scheme for the IPX network.

Question 8-14

Recommend an addressing scheme for the AppleTalk network.

Case Study: Jones, Jones, & Jones

You may wish to review the Jones, Jones, & Jones case study in Appendix A, page 308, before proceeding to answer the questions in this section.

Jones, Jones, & Jones Case Study Questions

Refer to the topology drawing you created for Ms. Jones in Chapter 3 or review the topology drawing solution provided in Appendix B. In this section you will design an addressing scheme for the network.

Question 8-15

Describe your IP addressing plans for implementation of your proposed system design.

Question 8-16

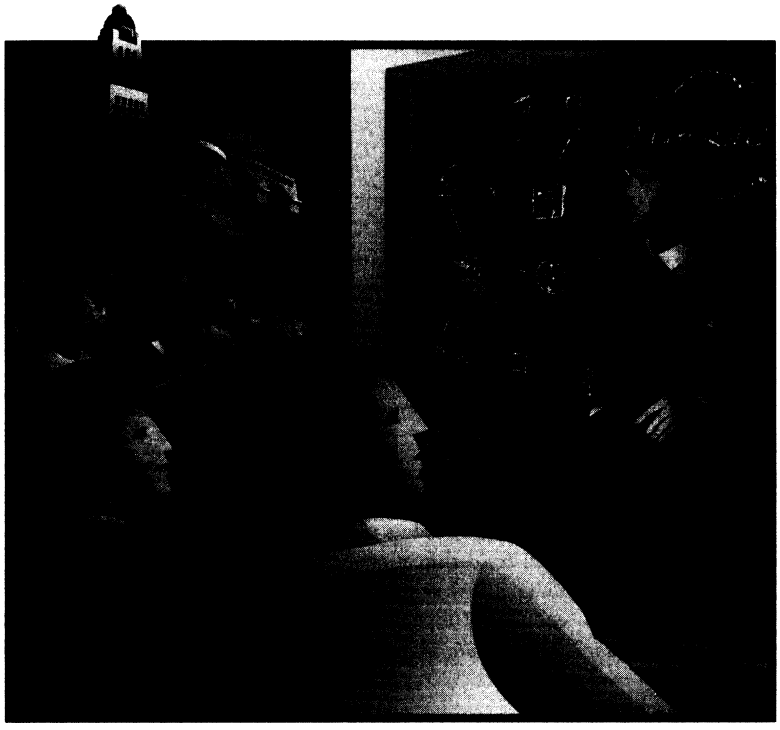
Propose a plan for naming servers, routers, and end nodes. Describe both the names themselves and the method that will be used to configure the names.

Question 8-17

The managing partner called. She wanted to emphasize that unauthorized workstations should not be allowed access to the Internet. How will you plan for this request in your design?

Question 8-18

Update your topology diagram to reflect the new addressing scheme.



from CCDA Exam Certification Guide

by A. Anthony Bruno and Jacqueline Kim

(1-57870-228-3)

Cisco Press

About the Authors

A. Anthony Bruno is a Senior Network Systems Consultant with Lucent's NetCare Professional Services Division (formerly International Network Services). His network certifications include CCIE #2738, CCDP, CCNA-WAN, Microsoft MCSE, Nortel NNCSS, Certified Network Expert (CNX) Ethernet, Certified Network Professional, and Check Point CCSE. As a consultant, he has worked with many customers in the design, implementation, and optimization of large-scale networks. Anthony has worked on the design of large company network mergers, Voice over IP/Frame Relay, and Internet access. He formerly worked as an Air Force captain in network operations and management. He completed his Master of Science degree in Electrical Engineering from University of Missouri-Rolla in 1994 and his Bachelor of Science degree in Electrical Engineering from University of Puerto Rico-Mayaguez in 1990. Anthony is a contributor and the lead technical reviewer for the Cisco Press release *CCIE Fundamentals: Network Design and Case Studies*, Second Edition.

Jacqueline Kim is the Knowledge Resource Manager with REALTECH Systems Corporation. She designed the Knowledge Exchanged Group that has the objective of providing technical instruction to clients through instructor-led classes and Web-based training tools. She staffs and manages this group within Knowledge Management and also teaches several classes. Jacqueline has various industry certifications, including Cisco CCDA, Novell CNE, and Check Point CCSA/CCSE. She has held positions in both network engineering and pre-sales engineering, during which time she presented lectures in security for Cisco Systems and Network User Groups. Jacqueline is a technical reviewer for the Cisco Press titles *Internetworking Technologies Handbook*, Second Edition, and *Cisco Systems Networking Academy: First-Year Companion Guide.*

Contents at a Glance

Bold chapters are elements included in this folio.

Objectives Covered in This Chapter

The following is a list of the objectives covered in this chapter. The list of CCDA exam design objectives and the chapters in which they are covered can be found in the Introduction of this book.

1	Design a network that meets a customer's requirements for performance, security, capacity, and scalability.
3	Upon completion of this introduction, you will be able to describe a framework you can use to simplify the complexities associated with analyzing customer network problems and creating Cisco scalable solutions.
5	Document the customer's current applications, protocols, topology, and number of users.
6	Document the customer's business issues that are relevant to a network design project.

CHAPTER 1

Design Goals

To get you started in your preparation for the CCDA exam, this chapter contains a framework for gathering customer objectives when designing a network. This chapter also covers the steps of network design and contains an overview of all the major topics of network design. The chapters that follow will cover in more detail each of the topics overviewed in this chapter.

"Do I Know This Already?" Quiz

The questions in the following quiz are designed to help you gauge how well you know the material covered in this chapter. Compare your answers with those found in Appendix A, "Answers to Quiz Questions." If you answered most or all of the questions thoroughly and correctly, you might want to skim the chapter and proceed to the "Q&A" section at the end of the chapter. If you find that you need to review only certain subject matter, search the chapter for those sections that cover the objectives you need to review, and then test yourself both with these questions and with the "Q&A" questions. If you find the following questions too difficult, read the chapter carefully until you feel that you can easily answers these and the "Q&A" questions.

1 What types of questions would you ask to determine a client's application requirements?

2 What are samples of business constraints on design?

3 What is the first step in network design?

4 In the framework of small to medium-sized network design, what should be done if there are protocol-related problems on the network?

5 What information is gathered in the logical assessment of the existing network?

6 What are the three layers of hierarchical network design?

7 If there are problems involving media contention on networks using repeaters, what should be done to resolve it?

8 What are the five areas of network management?

9 If you customer has a small network, what type of demonstration should be used?

10 If higher bandwidth is required on the network, what technologies are suggested for small to medium-sized networks?

_____

_____

_____

You can find the answers to these questions in Appendix A, "Answers to Quiz Questions."

Foundation Topics

Customer Objectives

The following CCDA objectives are covered in this section:

1	Design a network that meets a customer's requirements for performance, security, capacity, and scalability.
5	Document the customer's current applications, protocols, topology, and number of users.
6	Document the customer's business issues that are relevant to a network design project.

A CCDA should design networks based on the customer's objectives. In other words, you will need to find out what the customer wants to solve. You then must create a design that solves the networking problem or issue the customer is having.

The first step in network design is to obtain the customer's requirements. To obtain a complete picture of the customer's objectives, the engineer needs to document the client's business requirements, technical requirements, and any business and political constraints.

Business Requirements of the Customer

For this aspect of determining the customer's objectives, think about the purpose of the project. Project how the business will improve. Find out if the network is affecting the company's capability or effectiveness to develop, produce, and track products. Find out if any business applications are being affected. Determine whether the company will be audited.

Scalability is a very important consideration, and it is wise for the network designer to build a network that can scale. You should figure out how much the company will grow in one year or in five years.

Technical Requirements of the Customer

Think about the type of technical problems you are trying to solve. Consider the network's topology. For example, it may be difficult to introduce Ethernet to a customer that religiously uses Token Ring. Also consider the company's use of modern technologies. Find out whether the client is willing to experiment with the latest, bleeding-edge technologies. Keep in mind scaling issues; decide whether switched Ethernet will provide the necessary bandwidth or whether Fast Ethernet is necessary to scale the network.

Technical requirements can be divided into the following areas:

- Performance requirements
- Applications requirements
- Network management requirements
- Security requirements

Performance Requirements

Determine the following performance requirements:

- Identify any issues concerning network latency and response times.
- Find out if there is high utilization on LAN segments or WAN links.
- Determine how often the WAN links go down.

Application Requirements

Consider existing application integration. The network design will need to seamlessly accommodate the existing applications. Investigate the current application flows, and incorporate those into the network design. Determine the following application requirements:

- Find out what new applications have been introduced to the network.
- Determine the number of users using these applications.
- Find out the traffic flow for these applications.
- Identify what new protocols are being introduced to the network.
- Determine what applications are used during the daytime hours and what are used during the nighttime hours.
- Determine the time of day that represents the peak usage hours of applications.

Network Management Requirements

Determine the following network management requirements:

- Determine how the network is managed.
- Determine whether there is a network management station to view network performance and faults.
- Ascertain whether there are any accounting and security management requirements.
- Find out whether the staff is training on the network management applications.
- Find out whether there is a station for configuration management.

NOTE Remember the acronym FCAPS: fault, configuration, accounting, performance, and security management.

Security Requirements

Determine the following security requirements:

- Determine what type of security is required.
- Find out what external connections are present in the network and why they are there.
- Determine whether additional security is required on Internet connections.

Business and Political Constraints

The final aspect of determining the customer's objectives is to identify any constraints. Consider the following and ascertain whether they are constraints in your design:

- Ascertain budget or resource limitations for the project.
- Determine the timeline to complete the project.
- Determine whether any internal politics play a role in the decision-making process. Find out what different sources or groups are providing input into the requirements.
- Make sure the client's staff is able to operate and manage the new network.
- Find out whether the customer wants to reuse or trade in any existing equipment

The network design must be cost-effective and efficient. The goal is to get the best solution at a reasonable price. For example, a Catalyst 5500 may not be best solution for a remote office LAN with only 14 users.

Framework for Small- to Medium-Sized Network Design

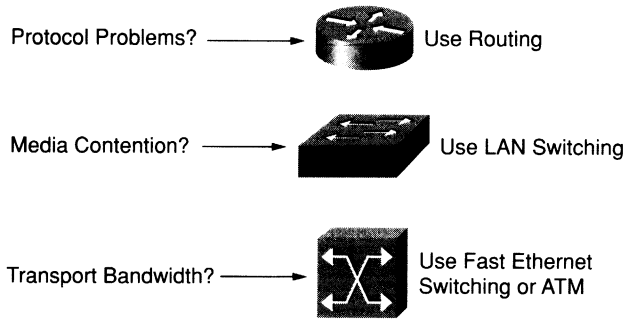
The following CCDA objective is covered in this section:

3	Upon completion of this introduction, you will be able to describe a framework you can use to simplify the complexities associated with analyzing customer network problems and creating Cisco scalable solutions.

As you gather information from the customer, keep in mind that Cisco has proposed a framework to use when designing complex small to medium-sized networks. The framework proposes the following rules (which are summarized in Figure 1-1):

- If the problems are protocol-related, use routing. Many LAN protocols use periodic broadcasts and service advertisements and do not scale well as the network size increases. Routers can be used to further subnet your network and reduce broadcast domains. Access and security policies can be applied on routers.
- If the problem involves media contention, use LAN switching. To expand on this rule, if you have too many nodes on a shared network, you will expect to have high utilization; devices will have to compete to obtain access to the network, and application response may be slow. Introducing LAN switching will help resolve the contention on the network.
- If high bandwidth is required, consider switched Fast Ethernet. Switched Fast Ethernet offers a good cost-to-performance ratio for small to medium-sized networks. For larger networks in which high bandwidth and low latency is required, use ATM. Gigabit Ethernet now provides another option in the LAN for the backbone and for bandwidth-intensive application servers.

Figure 1-1 *Small to Medium-Sized Network Design Framework*



Steps for Network Design

The following CCDA objectives are covered in this section:

1	Design a network that meets a customer's requirements for performance, security, capacity, and scalability.
5	Document the customer's current applications, protocols, topology, and number of users.
6	Document the customer's business issues that are relevant to a network design project.

The steps for designing a network are as follows:

1. Gather information to support the business and technical requirements.
2. Assess the current network.
3. Consider the applications involved.
4. Design the local-area networks.
5. Design the wide-area network.
6. Design for specific network protocols.
7. Create the design document and select Cisco network management applications.
8. Test the design.

This section provides an overview of these steps. The remainder of the book fills in the details of these steps.

Gather Information to Support the Business and Technical Requirements

The section "Customer Objectives," earlier in this chapter, covers step 1. Chapter 2, "Assessing the Existing Network and Identifying Customer Objectives," covers this step in much more detail.

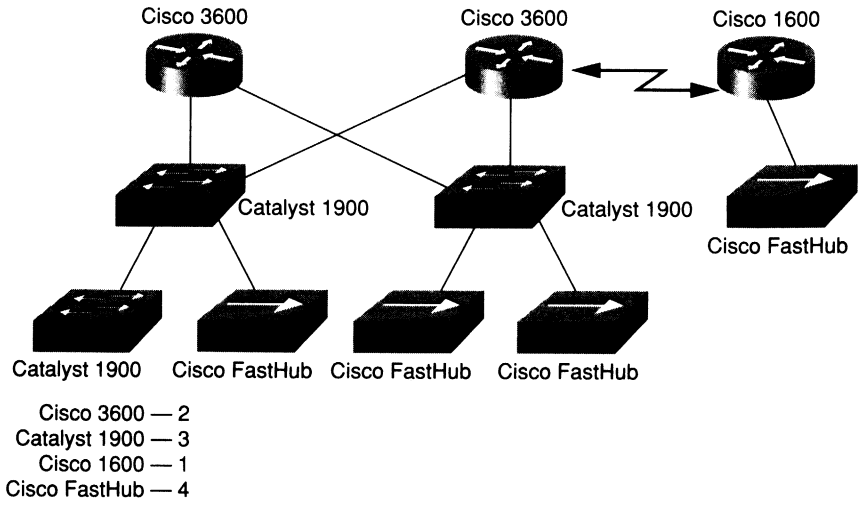
Assess the Current Network

This is the step during which you collect all data pertaining to physical, logical, traffic, and management information of the network. Chapter 2 covers this step in more detail. This section contains an overview of this step.

Physical Assessment

To perform a physical assessment, you need to document the physical topology of the network. Create a diagram with all routers, switches, and hubs. For example, in Figure 1-2, a list of network devices is created and the type and amount of devices is documented. Physical connectivity between devices should also be documented; also list the speed and type of media used between devices.

Figure 1-2 *Physical Assessment*



You will also need to list the LAN technologies being used. The following is a list of possible LAN technologies:

- Ethernet
- Token Ring
- FDDI
- Fast Ethernet
- Gigabit Ethernet

Finally, document the WAN circuit information and list the WAN technologies being used. The following is a list of possible WAN technologies used:

- Frame Relay
- Private lines
- ATM
- ISDN
- X.25

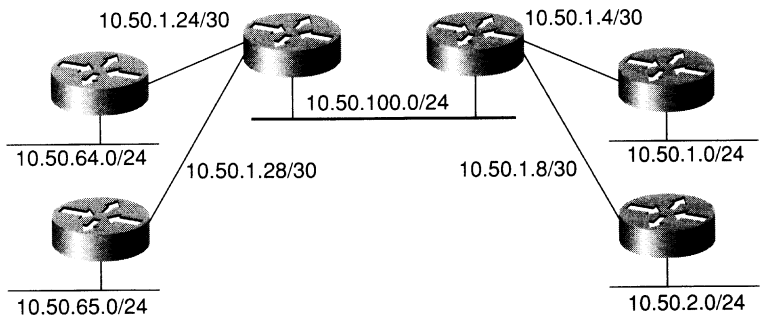
Logical Assessment

To perform the logical assessment, determine the following:

- The protocols that are being routed
- The IP address assignment scheme
- The Novell IPX address assignment
- The AppleTalk address assignment
- Whether any access list is used to filter addresses or broadcasts
- The Layer 3 architecture

Figure 1-3 provides an example of a logical assessment. Here, the IP address subnet information is documented. The figure shows five Ethernet segments with 24-bit subnet masks that can support up to 254 nodes each. This figure also shows four point-to-point links with 30-bit masks. With this mask, two IP addresses are used for each router on the link.

Figure 1-3 *Logical Assessment*



Traffic Assessment

To perform the traffic assessment, determine the following:

- Document the traffic flows on the network.
- Determine how much traffic is on each segment.
- Locate the servers.
- Determine how much traffic is local to the segment and how much traffic is external.

Management Assessment

Determine the current tools used for network management:

- Determine whether the customer has the necessary tools to manage the network.
- Determine whether there is a management station
- Find out whether CiscoWorks is being used to manage routers and switches.
- Verify whether there are capacity or performance monitoring tools.
- Determine whether a network protocol analyzer is available for LAN segment troubleshooting.
- Find out whether any RMON probes are in use.

Consider the Applications Involved

A good designer needs to take into consideration the applications that the network supports. The only reason the network is there is to provide a highway on which application information can flow. Never ignore the applications in use. Chapter 3, "Application Considerations," covers this step in more detail. This section contains an overview of the applications to consider in this step.

Microsoft Workgroups

MS Networking uses the session-layer NetBIOS protocol for file and print sharing. NetBIOS over NetBEUI is not routable and must be bridged for all devices to communicate on the network. For this reason, NetBIOS over NetBEUI does not scale well. NetBIOS over TCP (NBT) scales better because it relies on TCP/IP for transport, thus enabling NetBIOS traffic to be routed.

Novell Application Services

Novell uses the Service Advertising Protocol (SAP) for devices to announce their services to the network. SAP broadcasts are generated by fileservers, print servers, and so on. These broadcasts are sent every minute. As required by the protocol, a router adds all SAP broadcasts to its SAP table and broadcasts it every 60 seconds to its IPX interfaces. On larger networks, these broadcasts can overwhelm the network. Consider using access lists to filter SAP broadcasts from LAN segments.

IBM Networking

Traditional SNA networking involves the use of SDLC for WAN connectivity and Token Ring for LANs. Communication between hosts and terminals is bridged. The designer needs to document the Source-Route Bridging (SRB) requirements and consider Data-Link Switching Plus (DLSw+) for transporting SNA and NetBIOS traffic over WAN links in the IP network.

Multimedia Services

The network designer should investigate requirements to support multimedia services such as video and voice. Use techniques such as multicast routing to multicast video streams to reduce the total bandwidth used on the network. Multicast routing can transmit video streams to preselected end stations and reduce bandwidth consumption when compared to broadcasting. On networks supporting Voice over IP, use techniques such as RTP header compression on WAN links to reduce overhead. RSVP, policy routing, and tag switching are techniques used in the design of these time-sensitive applications.

Design the Local-Area Network

The Cisco Certified Design Associate must be able to design local-area networks that meet the customer's objectives on performance and scalability. A CCDA must design networks in a hierarchical manner to provide scalable solutions. A CCDA also must decide where to use hubs, switches, and routers to separate broadcast and collision domains. Know the differences between Layer 2 and Layer 3 switching as well. Chapter 4, "Network Topologies and LAN Design," covers this step in more detail. This section contains an overview of this step.

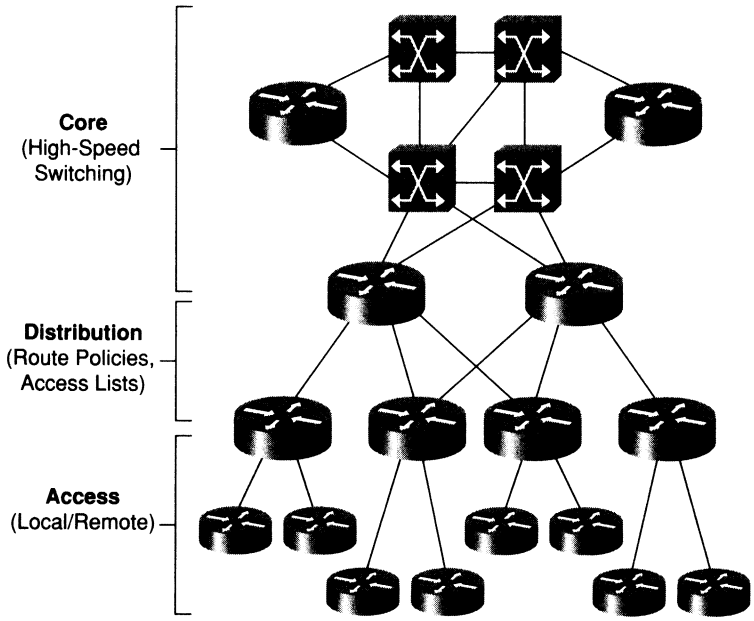
Hierarchical versus Flat Designs

The CCDA should understand that there is a limit on the number of nodes in flat network designs. Network broadcasts can overcome slow serial links. Build the network in a hierarchical manner with subnetting to reduce the amount of traffic on WAN links.

The CCDA must understand the three layers of the hierarchical model for network design: the core, distribution, and access layers. Figure 1-4 provides an example of these three layers.

At the core layer, high-speed switching is used with high availability and redundancy. Apply access and distribution lists at the distribution layer, which is where the security policies are applied. Address summarization and media translations are applied in the distribution layer as well. The access layer consists of the remote office sites using ISDN, Frame Relay, and DDR, and private lines accessing the corporate network. Local-area networks end segments are also part of the access layer.

Figure 1-4 *Hierarchical Design Model*



LAN Protocols

You need to understand the characteristics of LAN protocols, including physical distance limitations of LAN technologies: Ethernet (10Base2, 10Base5, and 10BaseT), Fast Ethernet, Gigabit Ethernet, Token Ring, and FDDI. Use these technologies to satisfy requirements ranging from user workstations to high-bandwidth servers.

LAN Physical Design

Select the equipment to be used, keeping in mind the LAN technologies and the number of ports required for the network.

Cisco LAN solutions include repeaters and switches.

Repeaters:

- Cisco 1500 hubs
- FastHub 100, 200, and 300 families

Switches:

- Catalyst 3000 Switch family
- Catalyst 5000 Switch family
- Catalyst 5500 family
- Catalyst 1900 family
- Catalyst 2800 family
- Catalyst 2900 family

Design the Wide-Area Network

The CCDA must design WAN networks that meet the customer's objectives of performance and scalability. Design networks in a hierarchical manner. and plan for bandwidth capacity to provide scalable solutions. Determine the WAN technologies to use, and plan for Cisco router solutions. Chapter 5, "WAN Design," covers this step in more detail. This section contains an overview of this step.

Transport Selection

Decide on the WAN technology to use. The following list will help you make this decision:

- Use leased lines where traffic flows are constant between point-to-point locations.
- Use ISDN for on-demand access to remote offices and for backup for another link type.
- Use Frame Relay as a high-bandwidth, cost-effective transport. This very popular WAN protocol provides permanent virtual circuits (PVC) between routers. Frame Relay provides characteristics such as congestion notification, discard eligibility (DE) bit, bursting, and the capability to have several PVCs on a physical port. These and other features (such as cost) made Frame Relay a very popular WAN technology in the 1990s.
- Use X.25 when the reliability of the WAN links is suspect. X.25 is an older WAN technology that is still widely in use and can be found running over low-speed (9600 to 64000 bps) lines. Throughput using X.25 suffers in comparison to Frame Relay due to X.25's additional error checking.
- Use ATM when high bandwidth (155+ Mbps) is required on the core. ATM offers different Quality of Service (QoS) types, allowing traffic with varying tolerances for bandwidth and latency to travel over the same network.

Bandwidth Planning

The CCDA must look at the applications being deployed at remote sites and decide on the sizing of WAN circuits. Rely on the analysis of existing traffic flows and past experience to help determine an appropriate bandwidth size for a circuit. If WAN circuit utilization is more than 70 percent for a long period of time, the circuit bandwidth should be increased. When planning bandwidth allocation, consider the following:

- The type of servers that are located at the remote site
- Whether the applications in the hub site will be accessed remotely and whether the intranet Web sites will be accessed remotely
- Whether there are Microsoft Domain controllers or MS Exchange servers at the remote sites
- Whether there are any database applications

Physical Design

Select the equipment to be used, keeping in mind the technologies and the number of interfaces required for the network. Take into consideration that the CCDA is focused on Cisco small to medium-sized network solutions.

The small to medium-sized network solutions include the following router series:

- Cisco 760/770 series
- Cisco 1000 series
- Cisco 1600 series
- Cisco 2500 series routers
- Cisco 3600 series routers
- Cisco MC3810 router
- Cisco 4500/4700 series routers
- Cisco 5200/5300 access servers
- Cisco 7200 series router

Design for Specific Network Protocols

In this step, take into consideration the type of protocols to be used on the network. Chapter 6, "Designing for Specific Protocols," covers this step in more detail. This section contains an overview of this step.

IP

The CCDA needs to design an IP address assignment scheme based on a hierarchical model. Use VLSMs to assign networks based on the number of devices and areas on the network. A hierarchical model for address assignment with VLSMs allows the network to take advantage of routing summary features supported by protocols such as EIGRP and OSPF. Choose routing protocols that will not add significant traffic to the network. Understand the differences between distance vector and link-state routing protocols.

Novell

Create IPX addressing schemes. Consider the broadcast characteristics of Novell's distance vector Routing Information Protocol (RIP) and Service Advertising Protocol (SAP). RIP broadcasts its table every 60 seconds; SAP also broadcasts the SAP table every 60 seconds. Use access lists to filter specific SAP broadcasts. Consider the design of the distance vector IPX RIP versus NetWare Link-Services Protocol (NLSP). EIGRP can be used on WAN links to reduce IPX traffic.

AppleTalk

Consider the AppleTalk cable ranges to assign to each interface and the zones for each area. To overcome the limitations of the AppleTalk routing protocol RTMP, use methods such as AURP or EIGRP on the WAN.

Bridging

Transparent and source-route bridged networks have size limitations and do not scale well. To reduce the traffic of bridged protocols, limit the size of bridged networks.

Create the Design Document and Select Cisco Network Management Applications

After working with the LAN, WAN, and protocol design, incorporate the solutions into one design during this step. Verify that the total solution meets the customer's objectives on performance, scalability, and cost. Incorporate a proactive network management solution that satisfies the customer's network service goals. Chapter 7, "The Design Document and Cisco Network Management Applications," covers this step in more detail. This section contains an overview of this step.

The Design Document

The design document helps the designer explain how the solution meets the requirements of the project. It consists of the following primary sections:

- Executive Summary
- Design Requirements
- Design Solution
- Summary
- Appendixes
- Cost of Proposed Design (optional)

Management Applications

A CCDA must be able to select the appropriate management applications for the designed network. Chapter 7 covers several management applications with which the CCDA must be familiar and discusses which are appropriate for various networks.

Test the Design

After a design has been proposed, the next step is to verify that the design will work. For large networks, a prototype can be built; for smaller networks a pilot can be devised. Chapter 8, "Building a Prototype or Pilot," covers the steps of building prototype and pilot test networks.

Q&A

The following questions are designed to test your understanding of the topics covered in this chapter. When you have answered the questions, look up the answers in Appendix A, "Answers to Quiz Questions." After you identify the subject matter you missed, review those sections in the chapter until you feel comfortable with this material.

1 During which assessment do you find out what type of IP addressing scheme is used on the network?

2 What would help solve a network with a high amount of broadcasts?

3 What are the four sections of the design document, and what goes into each section?

4 In network management, what does FCAPS stand for?

5 You would do a prototype for what type of networks?

6 Which section of the design document contains topology diagrams of the existing network?

7 Briefly describe Frame Relay.

8 Give three examples of bridged protocols.

9 What does SAP stands for? What is it used for?

10 List the nine steps for network design.

11 If higher bandwidth is required on the network, what technologies are suggested for small to medium-sized networks?

12 How often is the Novell SAP table broadcasted onto the network?

13 What are examples of business constraints?

Case Studies

Because passing the CCDA exam requires you to answer design questions about an ongoing case study, "Case Studies" and "Case Study Answers" sections will appear at the end of each body chapter in this book. Each "Case Studies" section asks questions based on one or more of the case studies presented in this section. Each "Case Study Answers" section answers those questions with detailed explanations. Each chapter's questions in the "Case Studies" section deal with the subject matter covered in that chapter. In some chapters, other case study background information will be presented in the question in addition to the general case study information here. This is so that you can answer that chapter's specific questions.

The remainder of this section introduces the three case studies that will be referred to at the end of each chapter. When you come across a question on a particular case study, refer back to these sections so that you can go about answering the questions on that case study.

Case Study #1: GHY Resources

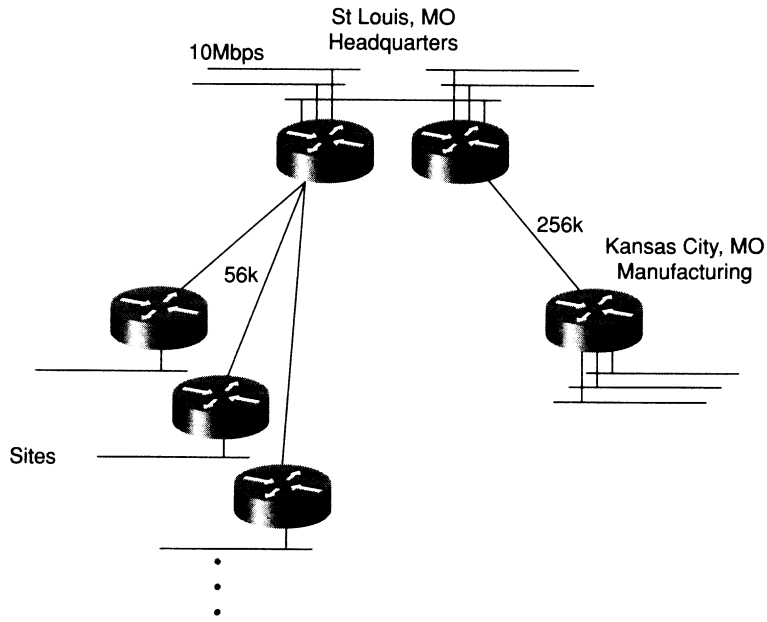
Mr. Martin of GHY Resources is responsible for the company's network. He has invited you to a meeting to discuss some issues.

GHY Resources is a manufacturing company with its headquarters based in St. Louis. In the past 10 years, GHY has grown from 10 employees to more than 400. It now has a manufacturing site in Kansas City, and a new site is opening in Nashville, Tennessee, in three months. The manufacturing sites connect back to St. Louis via a 256 K circuit. Sales offices exist in more than seven cities throughout the United States. Each sales office connects back to the headquarters via a 56 K leased line. These leased lines run at more than 70 percent utilization at certain times during the day. The company currently uses a mix of routers from different vendors and wants to standardize on Cisco's if the price is right. The current routing protocol is RIPv1. Figure 1-5 shows the current topology of GHY Resources.

Novell NetWare fileservers are used throughout the company, with one server at each of the sales offices. Local offices have print servers also. The headquarters' local-area network consists of Ethernet using 10BaseT hubs. These Ethernet segments constantly run at about 45 percent utilization. There are around 10 segments connecting to a pair of Cisco 4000 routers. One of the network analysts mentioned that the protocol analyzer reported broadcast storms on some of the Ethernet segments.

Business applications run on an HP 3000 machine located on one of the segments at the headquarters. An HP 3000 is located at the manufacturing site. The manufacturing site has two NetWare file servers. Mr. Martin expects the new manufacturing site to have the same business applications. The LAN in Kansas City consists of three Ethernet segments with 30 stations each. Network utilization is at 35 percent on each segment.

Figure 1-5 *GHY Resources Logical Diagram*



Mr. Martin has mentioned that he is interested in Frame Relay as an alternative for his WAN links. He would like to upgrade his LANs as well. He has requested a LAN/WAN solution that would help reduce the utilization problems he is having on the network. He also would like a solution to reduce the SAP traffic on the network. In addition, he wants to find a way to conserve IP addresses on his network. Mr. Martin needs to get a proposal in one week to have his managers approve the money. The design needs to be installed before the new manufacturing site becomes operational.

Look for questions on the GHY Resources case study at the end of some of the book's chapters.

Case Study #2: Pages Magazine, Inc.

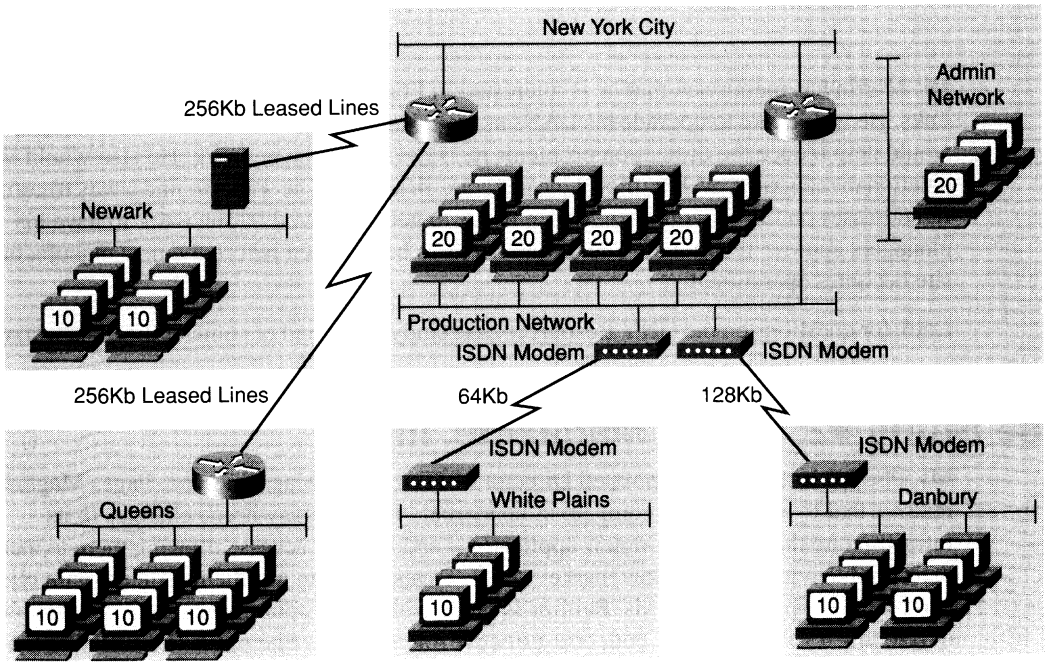
Ms. Phillips is the newly appointed Director of IT at Pages Magazine, Inc. Pages Magazine realizes that to aggressively compete in its market, this company needs changes to its infrastructure that will support new applications and Internet access, allowing them to increase their productivity and to follow market trends. Pages wants to use the Internet to gain clients and find new opportunities. Ms. Phillips is faced with many options but needs your help in developing a solution that is both cost-effective and scalable. She needs to make sure that the solution will address her immediate needs and also be scalable enough to support future applications.

Pages Magazine, Inc., is a conglomerate of four periodicals. Pages Magazine is expecting at least two periodical acquisitions per year for the next three years. Each magazine acts independently and has a mix of both small and medium-sized offices throughout the continental United States. Each magazine has various access methods back to the corporate headquarters located in New York City. Table 1-1 summarizes the current layout of the Pages Magazine, Inc., offices as they are presented in Figure 1-6.

Table 1-1 *Pages Magazine, Inc., Office Layout*

Office Location	Description	# of Nodes	Access Back to HQ
New York City, New York	Corporate headquarters	100	
Newark, New Jersey	Fashion magazine	20	256 K leased line
White Plains, New York	Entertainment news magazine	10	64 K ISDN
Queens, New York	Fashion magazine	30	256 K leased line
Danbury, Connecticut	Home improvement magazine	20	128 K ISDN

Figure 1-6 *Pages Magazine, Inc., Logical Diagram*



These leased lines have provided enough bandwidth to support basic e-mail and file transfer services. Each office has its own Novell servers that are currently managed independently, running on a flat 10BaseT Ethernet environment. A T1 will be installed at the NYC office to provide Internet access to the remote offices. Internet access and e-mail are the first critical applications that need to be addressed. Currently, the offices use CC:mail as their e-mail platform.

Pages Magazine has not standardized on MS Office applications and currently uses a mix of Apple and Microsoft application products. All the routers route IPX, AppleTalk, and IP; however, Pages Magazine wants to migrate to a purely IP environment with Novell GroupWise as the e-mail platform. Each office will have a GroupWise server that needs to be synchronized with the NYC office for Internet e-mail. After the two new offices go online, every office will slowly migrate to Netware 5, using native IP for transport. Until then, AppleTalk still needs to be supported as a routed protocol. The new Novell servers will also have a synchronized NDS directory structure that will manage the user access and login process.

Network manageability has been difficult since different vendor products are being used to provide WAN access. Ms. Phillips is looking for a single vendor solution that can be managed more effectively with her limited staff.

The additional offices for the new network are another concern, and she is looking to implement a network management solution that will support her staff. She has three remote IT support people in addition to three NYC-based people. One support person is located in Danbury and the other is in White Plains. The third supports Queens. Most of her staff have desktop and moderate networking skills.

The network used RIPv1, but Ms. Phillips plans to use DHCP to readdress her network so that she can conserve the valid IP address and to create a more scalable IP addressing scheme. Pages Magazine, Inc., will require a new routing protocol that will support subnetting and possible VLSM. Ms. Phillips is also interested in finding a more cost-effective WAN solution that will support the additional two offices that will go online within two months.

Ms. Phillips must present an infrastructure upgrade and Internet access plan to the CEO and CFO in three weeks. The presentation will include a network design to show how the network will scale to support new offices and to address any return on investment issues.

Look for questions on the Pages Magazine, Inc., case study at the end of some of the book's chapters.

Case Study #3: MediBill Services, Inc.

MediBill Services, Inc., started out providing billing support and services for a small community of independent medical offices. These offices used MediBill to service medical claims and provide patient data storage. After five years of service, MediBill has decided to grow and provide online medical information and Internet access to service its expanding client

base. The company also is looking to provide the security for file transfers for disaster recovery purposes. MediBill is looking to ensure that the integrity of the information transferred will not going be in question.

MediBill's CIO, Mr. Lee, is responsible for approving a design strategy that would support MediBill's future goals of providing secured remote storage of medical files, as well as Internet/ e-mail services and desktop support to the small to medium-sized medical offices.

MediBill currently has a T1 out to the Internet but isn't sure whether this is enough bandwidth to support its client base. The company has just acquired eight more offices that will need access within three months. MediBill has already begun the PC installation process and is waiting to coordinate the installation of the WAN connections. Prior to the WAN installations, Mr. Lee will need to purchase routers and security equipment for the Internet access.

Mr. Lee has asked several consultants to respond to the following information provided in a Request for Proposal (RFP).

MediBill has maintained an NT SQL database in its main office, which connects to the six remote doctors offices via 56 kbps dialup connections. These connections will have to be upgraded to support new services provided by the Internet. The connections will have to support Internet Web, e-mail, and file transfers as well as network management traffic. Mr. Lee is looking to implement the Microsoft Systems Management Server (SMS) for remote monitoring and management. MediBill has decided to standardize on the Microsoft platform to simplify IT management issues. MediBill has already implemented Microsoft Exchange and Outlook as the e-mail system.

MediBill is going to start by providing its clients with basic Web access, FTP, and e-mail.

After the Internet access and WAN upgrades, Mr. Lee wants to roll out a full network management solution that includes the management of each of the company's customers as well as its own network. Currently, each remote office must provide its own PC equipment, but with MediBill's new services, the company has decided to provide the PCs and all the customer premise equipment (CPE) necessary. Each office will have five to ten PCs per office, all running Microsoft Windows 98.

MediBill also won a contract with the MetroCenter Hospital, where the company will provide Internet services as well as secured disaster recovery services for data and files. The hospital will be connected to MediBill via a dedicated T1 circuit. The hospital has contracted MediBill to manage the 50 Internet workstations that will be distributed throughout the hospital, as well as the 10 data-transfer stations.

The client needs to review its WAN strategy and provide a design plan to upgrade the WAN network to support its growing client base. The client wants a demonstration of the security that his network will provide so that he can use that information in MediBill's marketing strategy.

Mr. Lee wants a proposal that will provide a baseline of the existing network and WAN connections as a comparison to a new network. Due to the large scale of changes that need to be made with MediBill, Mr. Lee is looking for a proposal that will outline how the company will migrate from its previous network to the new, more scalable network.

Additional Case Studies

Chapter 9, "Additional Case Studies," consists entirely of case studies that cover an array of CCDA topics. When you have completed all the chapters in the book, work on these case studies to fine tune your CCDA case study skills.

from Building Scalable Cisco Networks

by Catherine Paquet and Diane Teare

(1-58720-228-3)

Cisco Press

About the Authors

Catherine Paquet and **Diane Teare** are senior network architects with Global Knowledge Network (Canada) Inc., Cisco's largest worldwide training partner. There, they provide consulting and training services to customers in North America and Europe. Catherine and Diane are both Cisco Certified Systems Instructors (CCSIs) and Cisco Certified Network Professionals (CCNPs), and both have authored and edited networking books and articles. Catherine and Diane also were members of the team at Cisco Systems that developed the Building Scalable Cisco Networks (BSCN) instructor-led course.

Catherine has in-depth knowledge of routing technologies and access services, mainly in the area of Frame Relay, ISDN, and asynchronous connections. Catherine's internetworking career started as a LAN manager; she was promoted to MAN manager and eventually became the nationwide WAN manager for a federal department. She currently is the course director/master instructor for the Building Cisco Remote Access Networks (BCRAN) and Managing Cisco Networks Security (MCNS) courses at Global Knowledge Network (Canada) Inc. She has a master's degree in business administration, with a major in management information systems. Catherine edited *Building Cisco Remote Access Networks* from Cisco Press (ISBN 1-57870-091-4).

Diane has more than 15 years of experience in design, implementation, and troubleshooting of network hardware and software. She also has been involved in teaching, course design, and project management. Diane is the course director/master instructor for the BSCN and Designing Cisco Networks (DCN) courses at Global Knowledge Network (Canada) Inc. She is also a Cisco Certified Design Associate (CCDA). Diane has a bachelor's degree in applied science in electrical engineering and a master's degree in applied science in management science. She edited *Designing Cisco Networks* from Cisco Press (ISBN 1-57870-105-8).

Contents at a Glance

Bold chapters are elements included in this folio.

This chapter discusses various aspects of Internet Protocol (IP) addressing. This chapter covers the following topics:

- Current Challenges in IP Addressing
- IP Addressing Solutions
- Hierarchical Addressing
- Variable-Length Subnet Masks
- Route Summarization
- Classless Interdomain Routing
- Using IP Unnumbered Serial Interfaces
- Using Helper Addresses
- Summary
- Review Questions

CHAPTER 2

Extending IP Addresses

After reading this chapter, you will be able to use variable-length subnet masks to extend the use of the IP addresses when given an IP address range, explain whether route summarization is possible when given a network plan that includes IP addressing, and configure an IP helper address to manage broadcasts.

Current Challenges in IP Addressing

IP addressing was first defined in 1981. An IP address consists of a 32-bit number with two components: a network address and a node (host) address. Classes of addresses are also defined—originally, only Classes A, B, and C were defined, and later Classes D and E were added. Since then, the growth of the Internet has been incredible. Two addressing challenges have resulted from this explosion:

- **IP address exhaustion**—This has largely been due to the random allocation of IP addresses by the Network Information Center (NIC). Address exhaustion also has occurred because subnetting with one subnet mask may not be suitable for a typical network topology, as you will see in the "Variable-Length Subnet Masks" section later in this chapter.
- **Routing table growth and manageability**—One source indicates that in 1990, only about 5000 routes were tracked to use the Internet. This number had grown to more than 70,000 routes by the end of 1999. In addition to the exponential growth of the Internet, the random assignment of IP addresses throughout the world has contributed to the exponential growth of routing tables.

Next-generation IP (IP version 6) tries to respond to these problems by introducing a 128-bit address. In the meantime, Internet Requests For Comments (RFCs) have been introduced to enable the current IP addressing scheme to continue to be useful.

IP Addressing Solutions

Since the 1980s, solutions have been developed to slow the depletion of IP addresses and to reduce the number of Internet route table entries by enabling more hierarchical layers in an IP address. These solutions include the following:

- **Subnet masking**—Covered by RFCs 950 (1985) and 1812 (1995). Developed to add another level of hierarchy to an IP address. This additional level allows for extending the number of network addresses derived from a single IP address. (Subnet masking is reviewed in the "IP Addressing and Subnetting" section in this chapter and in Appendix A, "Job Aids and Supplements"; this subject also is discussed in detail in the Cisco Press *Interconnecting Cisco Network Devices* coursebook and Cisco ICND course.)

NOTE RFC 1812 also contains a lot of information on how IP routing protocols should work.

- **Address allocation for private internets**—Covered by RFC 1918 (1996). Developed for organizations that do not need much access to the Internet. The only reason to have a NIC-assigned IP address is to interconnect to the Internet. Any and all companies can use the privately assigned IP addresses within their organization rather than using a NIC-assigned IP address unnecessarily. The private addresses are 10.0.0.0 through 10.255.255.255, 172.16.0.0 through 172.31.255.255, and 192.168.0.0 through 192.168.255.255. (Private addresses are discussed in the Cisco Press *Building Cisco Remote Access Networks* coursebook and in the Cisco BCRAN course.)
- **Network address translation (NAT)**—Covered by RFC 1631 (1994). Developed for those companies that use private addressing or use IP addresses not assigned by NIC. This strategy enables an organization to access the Internet with a NIC-assigned address, without having to reassign the private addresses (sometimes called *illegal* addresses) that are already in place. (NAT is discussed in the Cisco Press *Building Cisco Remote Access Networks* coursebook and in the Cisco BCRAN course.)
- **Hierarchical addressing**—Applying a structure to addressing so that multiple addresses share the same left-most bits. Hierarchical addressing is discussed in this chapter in the section "Hierarchical Addressing."
- **Variable-length subnet masks (VLSMs)**—Covered by RFC 1812 (1995). Developed to allow multiple levels of subnetworked IP addresses within a single network. This strategy can be used only when it is supported by the routing protocol in use, such as the Open Shortest Path First (OSPF) protocol and the Enhanced Interior Gateway Routing Protocol (EIGRP). VLSMs are discussed later in this chapter in the section "Variable-Length Subnet Masks."
- **Route summarization**—Covered by RFC 1518 (1993). A way of having a single IP address represent a collection of IP addresses when you employ a hierarchical addressing plan. Route summarization is discussed later in this chapter in the section "Route Summarization."

- **Classless Interdomain Routing (CIDR)**—Covered by RFCs 1518 (1993), 1519 (1993), and 2050 (1996). Developed for Internet service providers (ISPs). This strategy suggests that the remaining IP addresses be allocated to ISPs in contiguous blocks, with geography being a consideration. CIDR is discussed later in this chapter in the section "Classless Interdomain Routing."

IP Addressing and Subnetting

This section is an overview of IP subnetting and addresses. Appendix A includes a more detailed review of these topics.

When contiguous ones are added to the default mask, making the all-ones field in the mask longer, the definition of the network part of an IP address is extended to include subnets. Adding bits to the network part of an address decreases the number of bits in the host part. Thus, creating additional networks (subnets) is done at the expense of the number of host devices that can occupy each network segment.

The number of bits added to a default routing mask creates a counting range for counting subnets. Each subnet is a unique binary pattern.

The number of subnetworks created is calculated by the formula 2^n, where n is the number of bits by which the default mask was extended. Subnet 0 (where all the subnet bits are 0) must be explicitly allowed using the **ip subnet-zero** global configuration command in Cisco IOS releases prior to 12.0. In Cisco IOS Release 12.0 and later, subnet zero is enabled by default.

NOTE This book describes the formula for obtaining the number of subnets differently than previous Cisco courses and books. Previously, the same formula that was used to count hosts, $2^n - 2$, was used to count subnets. Now 2^n subnets and $2^n - 2$ hosts are available. The 2^n rule for subnets has been adopted because the all-ones subnet has always been a legal subnet according to the RFC, and subnet zero can be enabled by configuration commands on the Cisco routers (and, in fact, is on by default in Cisco IOS Release 12.0 and later). Note, however, that not all vendor equipment supports the use of subnet zero.

The remaining bits in the routing mask form a counting range for hosts. Host addresses are selected from these remaining bits and must be numerically unique from all other hosts on the subnetwork.

The number of hosts created is calculated by the formula $2^n - 2$ where n is the number of bits available in the host portion. In the host counting range, the all 0s bit pattern is reserved as the subnet identifier (sometimes called *the wire*), and the all 1s bit pattern is reserved as a broadcast address, to reach all hosts on that subnet.

Both the IP address and the associated mask contain 32 bits. Routers are similar to computers in that both use the binary numbering scheme to represent addresses. Network administrators, however, typically do not use binary numbers on a daily basis and therefore have adopted other formats to represent 32-bit IP addresses. Some common formats include decimal (base 10) and hexadecimal (base 16) notations.

The generally accepted method of representing IP addresses and masks is to break the 32-bit field into four groups of 8 bits (octets) and to represent those 8-bit fields in a decimal format, separated by decimal points. This is known as 32-bit *dotted decimal notation.*

NOTE Although the dotted decimal notation is commonly accepted, this notation means nothing to the routing device because the device internally uses the 32-bit binary string. All routing decisions are based on the 32-bit binary string.

IP addresses belong to classes, defined by the decimal value represented in the first octet. The class definition is referred to as the *First Octet Rule*. As shown in Table 2-1, Classes A through E are defined. Of the five available addressing spaces, Classes A, B, and C are the best known and most commonly used because they are used to identify devices connected to the Internet.

Table 2-1 *Determining IP Address Class by the First Octet Rule*

First Octet of Address (Decimal)	Address Class
1 to 126	Class A
128 to 191	Class B
192 to 223	Class C
224 to 239	Class D
240 to 255	Class E

NOTE The first octet for Class A ranges from 1 (not 0) to 126 (not 127). The 0 address is a reserved address, meaning *this network*, and can be used only as a source address. The 127 address is reserved for the local loopback address.

Class D addresses are not as widely used. Class D addresses are multicast addresses; some Class D multicast addresses used by routing protocols are as follows:

- **OSPF**—224.0.0.5 and 224.0.0.6
- **Routing Information Protocol version 2 (RIPv2)**—224.0.0.9
- **EIGRP**—224.0.0.10

Videoconferencing and other applications use other Class D multicast addresses. In videoconferencing applications, users subscribe to a group service and are issued a special group address that allows them access to the data created for that special event. This approach enables many users to subscribe and unsubscribe to a service as their needs and schedules permit.

Class E addresses are used for experimental purposes.

Hierarchical Addressing

This section discusses hierarchical addressing and the benefits of using it. The following topics are covered:

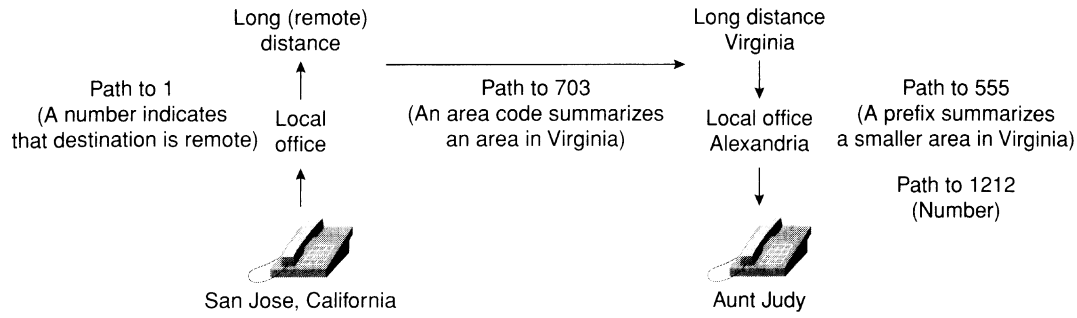
- Planning an IP address hierarchy
- Benefits of hierarchical addressing

Planning an IP Address Hierarchy

Perhaps the best-known addressing hierarchy is the telephone network. The telephone network uses a hierarchical numbering scheme that includes country codes, area codes, and local exchange numbers. For example, if you are in San Jose, California, and call someone else in San Jose, you dial the San Jose local exchange number, 528, and the person's telephone number—for example, 7777. Upon seeing the number 528, the central office recognizes that the destination telephone is within its area, so it looks for number 7777 and transfers the call.

In another example, as shown in Figure 2-1, to call Aunt Judy in Alexandria, Virginia, from San Jose, you dial 1, then the area code 703, then the Alexandria prefix 555, and then Aunt Judy's local number, 1212. The central office first sees the number 1, indicating a remote call, and then looks up the number 703. The central office immediately routes the call to a central office in Alexandria. The San Jose central office does not know exactly where 555-1212 is in Alexandria, nor does it have to. It needs to know only the area codes, which summarize the local telephone numbers within an area.

Figure 2-1 *The Telephone Network Uses an Addressing Hierarchy*



If there were no hierarchical structure, every central office would need to have every telephone number worldwide in its locator table. Instead, the central offices have summary numbers, such as area codes and country codes. A summary number (address) represents a group of numbers. For example, an area code such as 408 is a summary number for the San Jose area. That is, if you dial 1-408 from anywhere in the United States, followed by a seven-digit telephone number, the central office will route the call to a San Jose central office. This is the type of addressing strategy that the Internet gurus are trying to work toward and that you as a network administrator should implement in your own internetwork.

Benefits of Hierarchical Addressing

Imagine if the telephone network did not use a hierarchy—each central office would need to keep track of all the phone numbers in the phone network. This would obviously be unacceptable. Instead, the telephone network uses the area code and prefix to represent a collection of phone numbers—that is, they *summarize* the phone numbers within an area. Similarly, a routed network can employ a hierarchical addressing scheme to take advantage of those same benefits.

The benefits of hierarchical addressing include these:

- **Reduced number of routing table entries**—Whether it is with your Internet routers or your internal routers, you should try to keep your routing tables as small as possible by using route summarization. Route summarization is a way of having a single IP address represent a collection of IP addresses when you employ a hierarchical addressing plan. By summarizing routes, you can keep your routing table entries manageable, which offers the following benefits:
  - More efficient routing
  - Reduced number of CPU cycles when recalculating a routing table or sorting through the routing table entries to find a match

  - — Reduced router memory requirements
  - — Faster convergence after a change in the network
  - — Easier troubleshooting
- **Efficient allocation of addresses**—Hierarchical addressing enables you to take advantage of all possible addresses because you group them contiguously. With random address assignment, you may end up wasting groups of addresses because of addressing conflicts. For example, recall that classful routing protocols automatically create summary routes at a network boundary. Therefore, these protocols do not support discontiguous addressing (as you will see later in this chapter in the section "Summarizing Routes in a Discontiguous Network"), so some addresses would be unusable if not assigned contiguously.

Variable-Length Subnet Masks

This section introduces VLSMs, gives some examples, and discusses VLSM use with classless routing protocols. The section covers the following:

- VLSM overview
- Calculating VLSMs
- A working VLSM example

VLSM Overview

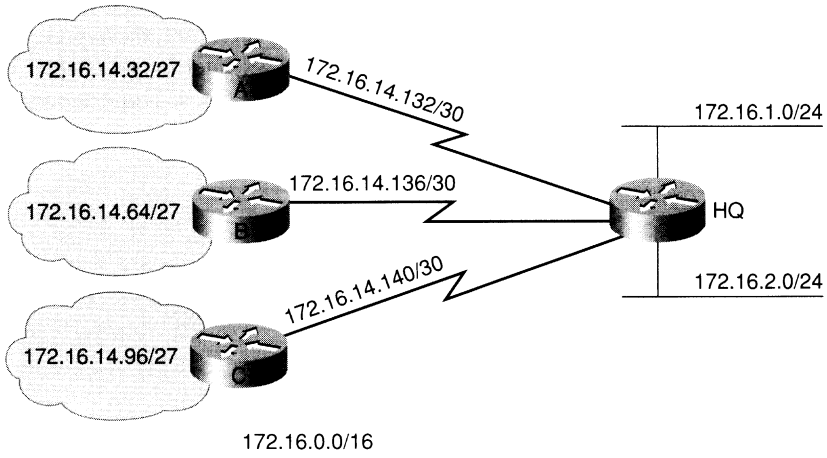
VLSMs provide the capability to include more than one subnet mask within a major network and the capability to subnet an already subnetted network address. The benefits of VLSMs include these:

- **Even more efficient use of IP addresses**—Without the use of VLSMs, companies are locked into implementing a single subnet mask within an entire Class A, B, or C network number.

  For example, consider the 172.16.0.0/16 network address divided into subnets using /24 masking, and one of the subnetworks in this range, 172.16.14.0/24, further divided into smaller subnets with the /27 masking, as shown in Figure 2-2. These smaller subnets range from 172.16.14.0/27 to 172.16.14.224/27. In Figure 2-2, one of these smaller subnets, 172.16.14.128, is further divided with the /30 prefix, creating subnets with only two hosts, to be used on the WAN links. (The details of the subnets used are shown following Figure 2-2.)

- **Greater capability to use route summarization**—VLSMs allow for more hierarchical levels within your addressing plan and thus allow for better route summarization within routing tables. For example, in Figure 2-2, address 172.16.14.0/24 could summarize all the subnets that are further subnets of 172.16.14.0, including those from subnet 172.16.14.0/27 and from 172.16.14.128/30.

Figure 2-2 *VLSMs Allow More Than One Subnet Mask Within a Major Network*



In Figure 2-2, the subnets available are as follows:

From 172.16.0.0/24:	172.16.0.0/24 (not used in this example) 172.16.1.0/24 172.16.2.0/24 and so on 172.16.14.0/24 (not used, was further subnetted to 172.16.14.0/27)
From 172.16.14.0/27:	172.16.14.0/27 (not used in this example) 172.16.14.32/27 172.16.14.64/27 172.16.14.96/27 and so on 172.16.14.128/27 (not used, but was further subnetted to 172.16.14.128/30)
From 172.16.14.128/30:	172.16.14.128/30 (not used in this example) 172.16.14.132/30 172.16.14.136/30 172.16.14.140/30 and so on

Calculating VLSMs

With VLSMs, you can subnet an already subnetted address. Consider, for example, that you have a subnet address 172.16.32.0/20, and you need to assign addresses to a network that has ten hosts. With this subnet address, however, you have $2^{12} - 2 = 4094$ host addresses, so you would be wasting more than 4000 IP addresses. With VLSMs, you can further subnet the address 172.16.32.0/20 to give you more subnetwork addresses and fewer hosts per network, which would work better in this network topology. For example, if you subnet 172.16.32.0/20 to 172.16.32.0/26, you gain 64 (2^6) subnets, each of which could support 62 ($2^6 - 2$) hosts.

NOTE The "Decimal-to-Binary Conversion Chart" in Appendix A may be helpful when you are calculating VLSMs.

To further subnet 172.16.32.0/20 to 172.16.32.0/26, do the following, as illustrated in Figure 2-3:

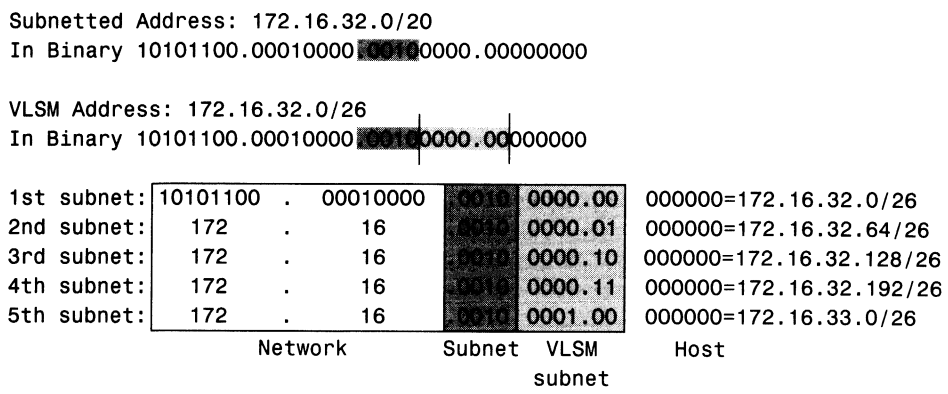
Step 1 Write 172.16.32.0 in binary form.

Step 2 Draw a vertical line between the 20th and 21st bits, as shown in Figure 2-3.

Step 3 Draw a vertical line between the 26th and 27th bits, as shown in Figure 2-3.

Step 4 Calculate the 64 subnet addresses using the bits between the two vertical lines, from lowest to highest in value. Figure 2-3 shows the first five subnets available. If necessary, refer to the "Decimal-to-Binary Conversion Chart," in Appendix A.

Figure 2-3 *An Example of Further Subnetting a Subnetted Address*



NOTE VLSM calculators are available on the Web. The following URL is for the one offered by Cisco: www.cisco.com/techtools/ip_addr.html. (Note that you need to have an account to use this calculator; you can see it but cannot use it without logging in.)

A Working VLSM Example

VLSMs are commonly used to maximize the number of possible addresses available for a network. For example, because point-to-point serial lines require only two host addresses, you can use a subnetted address that has only two host addresses and therefore will not waste scarce subnet numbers.

In Figure 2-4, the addresses used on the local-area networks (LANs) are those generated in the previous section, "Calculating VLSMs."

Figure 2-4 *A Working VLSM Example Using Ethernet and Point-to-Point WAN Links*

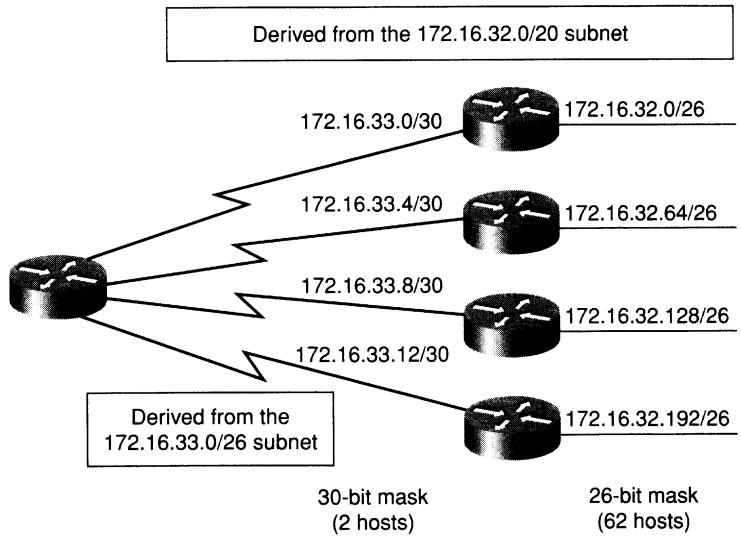


Figure 2-4 illustrates where the addresses can be applied, depending on the number of hosts anticipated at each layer. For example, the wide-area network (WAN) links use addresses with a prefix of /30 (corresponding to a subnet mask of 255.255.255.252). This prefix allows for only two hosts—just enough hosts for a point-to-point connection between a pair of routers. To calculate the addresses used on the WAN links, further subnet one of the unused subnets. In this case, you can further subnet 172.16.33.0/26 with a prefix of /30. This provides 4 more subnet bits and therefore $2^4 = 16$ subnets for the WANs.

The WAN addresses derived from the 172.16.33.0/26 subnet are as follows:

- 172.16.33.00**000000** = 172.16.33.0/30
- 172.16.33.00**000100** = 172.16.33.4/30
- 172.16.33.00**001000** = 172.16.33.8/30
- 172.16.33.00**001100** = 172.16.33.12/30

NOTE It is important to remember that only subnets that are unused can be further subnetted. In other words, if you use any addresses from a subnet, that subnet cannot be further subnetted. In the example in Figure 2-4, four subnet numbers are used on the LANs. Another, as yet unused subnet, 172.16.33.0/26, is further subnetted for use on the WANs.

Route Summarization

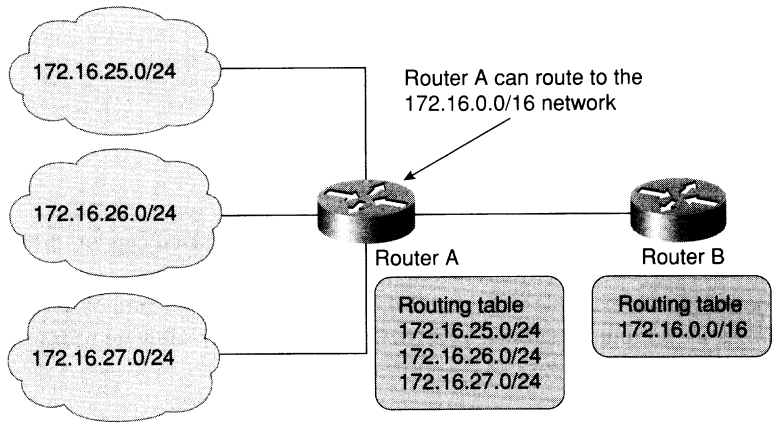
This section describes and gives examples of route summarization, including implementation considerations. This section covers the following topics:

- Route summarization overview
- Summarizing within an Octet
- Summarizing addresses in a VLSM-designed network
- Route summarization implementation
- Route summarization operation in Cisco routers
- Summarizing routes in a discontiguous network
- Route summarization summary

Route Summarization Overview

In large internetworks, hundreds or even thousands of networks can exist. In these environments, it is often not desirable for routers to maintain all these routes in their routing table. Route summarization (also called *route aggregation* or *supernetting*) can reduce the number of routes that a router must maintain because it is a method of representing a series of network numbers in a single summary address. For example, in Figure 2-5, Router A either can send three routing update entries or can summarize the three addresses into a single network number.

Figure 2-5 *Routers Can Summarize to Reduce the Number of Routes*



NOTE Router A in Figure 2-5 is advertising that it can route to the network 172.16.0.0/16, including all subnets of that network. However, if there were other subnets of 172.16.0.0 elsewhere in the network (for example, if 172.16.0.0 were discontiguous), summarizing in this way might not be valid. Discontiguous networks and summarization are discussed in the "Summarizing Routes in a Discontiguous Network" section, later in this chapter.

Another advantage to using route summarization in a large, complex network is that it can isolate topology changes from other routers. That is, if a specific link in the 172.16.27.0/24 domain were *flapping* (going down and up rapidly), the summary route would not change, so no router external to the domain would need to keep modifying its routing table due to this flapping activity.

NOTE A summary route will be announced by the summarizing router as long as at least one specific route matches the summary route in its routing table.

Route summarization is most effective and possible only when a proper addressing plan is in place. Route summarization is most effective within a subnetted environment when the network addresses are in contiguous blocks in powers of two. For example, 4, 16, or 512 addresses can be represented by a single routing entry because summary masks are binary masks—just like subnet masks—so summarization must take place on binary boundaries

(powers of two). If the number of network addresses is not contiguous or a power of two, you can divide the addresses into groups and try to summarize the groups separately.

Routing protocols summarize or aggregate routes based on shared network numbers within the network. Classless routing protocols—such as OSPF, and EIGRP—support route summarization based on subnet addresses, including VLSM addressing. Classful routing protocols—RIPv1 and IGRP—automatically summarize routes on the classful network boundary and do not support summarization on any other bit boundaries. Classless routing protocols support summarization on any bit boundary.

Summarization is described in RFC 1518, "An Architecture for IP Address Allocation with CIDR."

Summarizing Within an Octet

Figure 2-5 illustrated a summary route based on a full octet—172.16.25.0/24, 172.16.26.0/24, and 172.16.27.0/24 could be summarized into 172.16.0.0/16. However, this is not always the case.

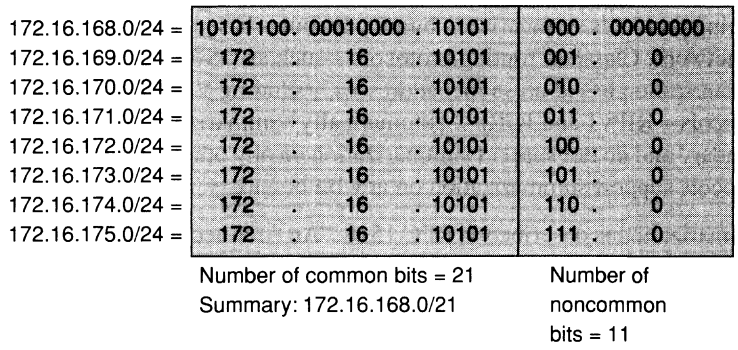
A router could receive updates for the following routes:

- 172.16.168.0/24
- 172.16.169.0/24
- 172.16.170.0/24
- 172.16.171.0/24
- 172.16.172.0/24
- 172.16.173.0/24
- 172.16.174.0/24
- 172.16.175.0/24

In this case, to determine the summary route, the router determines the number of highest-order (left-most) bits that match in all the addresses. As shown in Figure 2-6, the left-most 21 bits match in all these addresses. Therefore, the best summary route is 172.16.168.0/21 (or 172.16.168.0 255.255.248.0).

To allow the router to aggregate the most IP addresses into a single route summary, your IP addressing plan should be hierarchical in nature. This approach is particularly important when using VLSMs, as illustrated in the next section.

Figure 2-6 *An Example of Summarizing Within an Octet*



Summarizing Addresses in a VLSM-Designed Network

A VLSM design allows for maximum use of IP addresses as well as more efficient routing update communication when using hierarchical IP addressing. In Figure 2-7 for example, route summarization occurs at two levels:

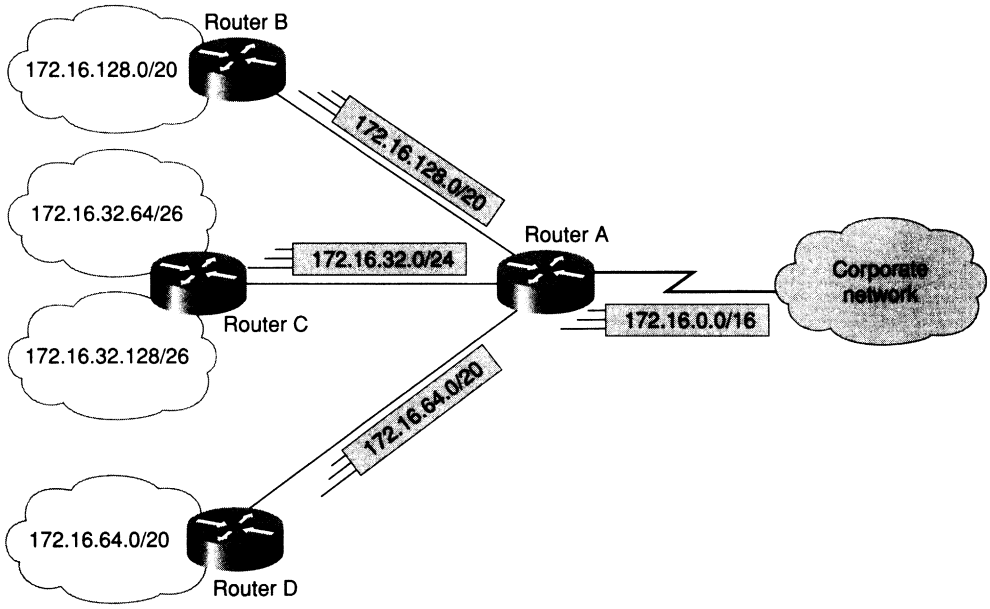
- Router C summarizes two routing updates from networks 172.16.32.64/26 and 172.16.32.128/26 into a single update, 172.16.32.0/24.
- Router A receives three different routing updates but summarizes them into a single routing update before propagating it to the corporate network.

Route Summarization Implementation

Route summarization reduces memory use on routers and routing protocol network traffic, due to less entries in the routing table. For summarization in a network to work correctly, the following requirements must be met:

- Multiple IP addresses must share the same high-order bits.
- Routing protocols must base their routing decisions on a 32-bit IP address and a prefix length that can be up to 32 bits.
- Routing updates must carry the prefix length (the subnet mask) along with the 32-bit IP address.

Figure 2-7 *An Example of Summarizing in a Network Using VLSM*



Route Summarization Operation in Cisco Routers

This section discusses generalities of how Cisco routers handle route summarization. Details about how route summarization operates with a specific protocol are discussed in the specific protocol chapter of this book. For example, route summarization for OSPF is discussed in Chapter 4, "Interconnecting Multiple OSPF Areas."

Cisco routers manage route summarization in two ways:

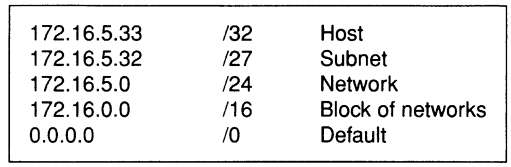
- **Sending route summaries**—Routing information advertised out an interface is automatically summarized at major (classful) network address boundaries by RIP, IGRP, and EIGRP. Specifically, this automatic summarization occurs for those routes whose classful network address differs from the major network address of the interface to which the advertisement is being sent. For OSPF, you must configure summarization.

  Route summarization is not always a solution. You would not want to use route summarization if you needed to advertise all networks across a boundary, such as when you have discontiguous networks (discussed in the next section). When using EIGRP and RIPv2, you can disable this automatic summarization.

- **Selecting routes from route summaries**—If more than one entry in the routing table matches a particular destination, the longest prefix match in the routing table is used. Several routes might match one destination, but the longest matching prefix is used.

  For example, if a routing table has the paths shown in Figure 2-8, packets addressed to destination 172.16.5.99 would be routed through the 172.16.5.0/24 path because that address has the longest match with the destination address.

Figure 2-8 *Routers Will Use the Longest Match When Selecting a Route*



NOTE When running classful protocols (RIPv1 and IGRP), you must enable **ip classless** if you want the router to select a default route when it must route to an unknown subnet of a network for which it knows some subnets. For example, consider a router's routing table that has entries for subnets 10.5.0.0/16 and 10.6.0.0/16, and a default route of 0.0.0.0. If a packet arrives for a destination on the 10.7.0.0/16 subnet, and if **ip classless** is not enabled, then the packet will be dropped. Classful protocols assume that if they know some of the subnets of network 10.0.0.0, then they must know all the existing subnets of that network. Enabling **ip classless** indicates to the router that it should follow the best supernet route or the default route for unknown subnets of known networks, as well as for unknown networks.

Note that **ip classless** is enabled by default in Release 12.0 of the Cisco IOS software; in previous releases, it is disabled by default.

Summarizing Routes in a Discontiguous Network

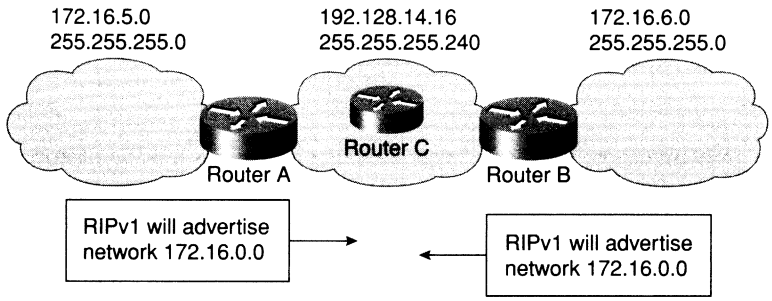
Discontiguous subnets are subnets of the same major network that are separated by a different major network.

Recall that RIP, IGRP, and EIGRP summarize automatically at network boundaries. This behavior, which cannot be changed with RIPv1 and IGRP, has important results:

- Subnets are not advertised to a different major network.
- Discontiguous subnets are not visible to each other.

In the example shown in Figure 2-9, Routers A and B do not advertise the 172.16.5.0 255.255.255.0 and 172.16.6.0 255.255.255.0 subnets because RIPv1 cannot advertise subnets across a different major network; both Router A and Router B advertise 172.16.0.0. This leads to confusion when routing across network 192.168.14.0. For example, Router C receives routes about 172.16.0.0 from two different directions; therefore, it might not make a correct routing decision.

Figure 2-9 *Classful Routing Protocols Do Not Support Discontiguous Subnets*



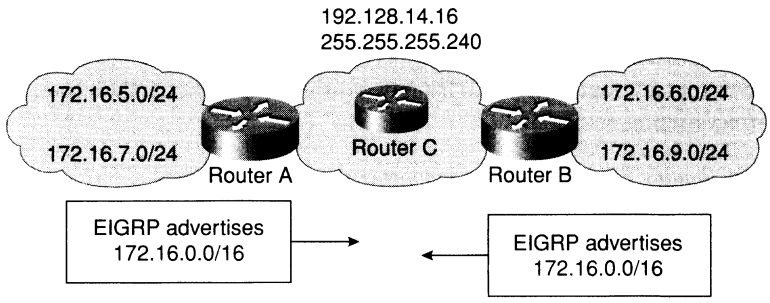
This situation can be resolved by using RIPv2, OSPF, or EIGRP and not using summarization because the subnet routes would be advertised with their actual subnet masks. Advertisements are configurable when using OSPF and EIGRP, but not RIPv2.

The Cisco IOS software also provides an IP unnumbered feature that permits noncontiguous subnets to be separated by an unnumbered link; this feature is discussed in the section "Using IP Unnumbered Serial Interfaces," later in this chapter.

Route Summarization Cautions in Discontiguous Networks

Be careful when using route summarization in a network that has discontiguous subnets, or if not all the summarized subnets are reachable via the advertising router. If a summarized route indicates that certain subnets are reachable via a router, when those subnets actually are discontiguous or are not reachable via that router, the network may have problems similar to those shown in Figure 2-9 for a RIPv1 network. For example, in Figure 2-10, EIGRP is being used, and both Router A and Router B are advertising a summarized route to 172.16.0.0/16. Therefore, Router C receives two routes to 172.16.0.0/16 and has no knowledge of which subnets are attached to which router.

Figure 2-10 *Care Is Also Needed When Summarizing with Classless Routing Protocols*



This problem can be resolved if you are using a classless routing protocol because automatic summarization can be turned off (if it is on by default). Because routers running classless routing protocols use the longest prefix match when selecting a route from the routing table, if one of the routers advertised without summarizing, other routers would see subnet routes as well as the summary route. The other routers could then select the longest prefix match and follow the correct path. For example, in Figure 2-10, if Router A continues to summarize to 172.16.0.0/16, and Router B was configured to not summarize, then Router C would receive explicit routes for 172.16.6.0/24 and 172.16.9.0/24 along with the summarized route to 172.16.0.0/16. All traffic for Router B's subnets would then be sent to Router B, while all other traffic for the 172.16.0.0 network would be sent to Router A. This would be true for any other classless protocol.

Route Summarization Summary

Table 2-2 provides a summary of the route summarization support available in the various IP routing protocols discussed.

Table 2-2 *Routing Protocol Route Summarization Support*

Protocol	Automatic Summarization at Classful Network Boundary?	Capability to Turn Off Automatic Summarization?	Capability to Summarize at Other Than Classful Network Boundary?
RIPv1	Yes	No	No
RIPv2	Yes	Yes	No
IGRP	Yes	No	No
EIGRP	Yes	Yes	Yes
OSPF	No	—	Yes

Classless Interdomain Routing

CIDR is a mechanism developed to help alleviate the problem of exhaustion of IP addresses and growth of routing tables. The idea behind CIDR is that blocks of multiple Class C addresses can be combined, or aggregated, to create a larger classless set of IP addresses (that is, with more hosts allowed). Blocks of Class C network numbers are allocated to each network service provider. Organizations using the network service provider for Internet connectivity are allocated subsets of the service provider's address space as required.

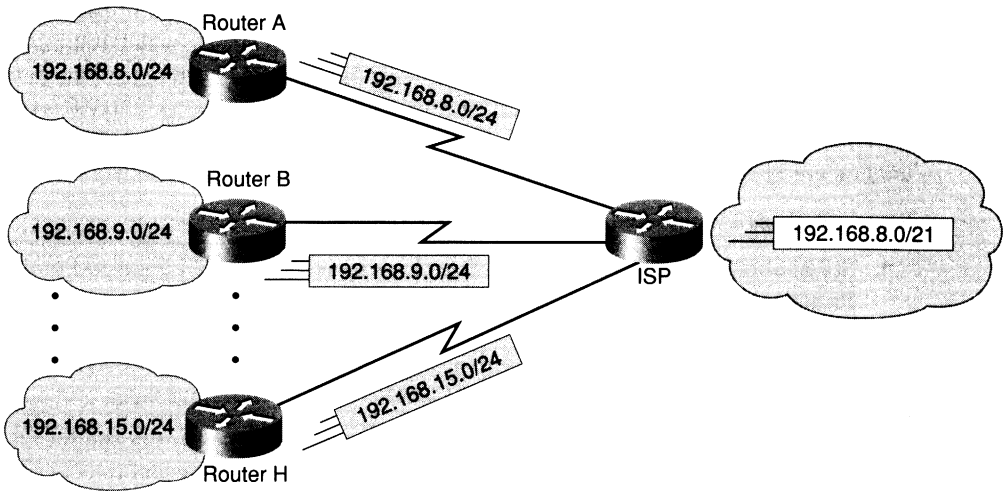
These multiple Class C addresses can then be summarized in routing tables, resulting in fewer route advertisements.

CIDR is described further in RFCs 1518 and 1519. RFC 2050, "Internet Registry IP Allocation Guidelines," specifies guidelines for the allocation of IP addresses.

CIDR Example

Figure 2-11 shows an example of CIDR and route summarization. The Class C network addresses 192.168.8.0/24 through 192.168.15.0/24 are being used and are being advertised to the ISP router. When the ISP router advertises the networks available, it can summarize these into one route instead of separately advertising the eight Class C networks. By advertising 192.168.8.0/21, the ISP router indicates that it can get to all destination addresses that have the first 21 bits the same as the first 21 bits of the address 192.168.8.0.

Figure 2-11 *CIDR Allows a Router to Summarize Multiple Class C Addresses*



NOTE The mechanism used to calculate the summary route to advertise is the same as shown in the "Route Summarization" section, earlier in this chapter. The Class C network addresses 192.168.8.0/24 through 192.168.15.0/24 are being used and are being advertised to the ISP router. To summarize these addresses, find the common bits as shown here:

192.168.8.0 192.168.**00001**000.00000000
192.168.9.0 192.168.**00001**001.00000000
192.168.10.0 192.168.**00001**010.00000000
. . .
192.168.14.0 192.168.**00001**110.00000000
192.168.15.0 192.168.**00001**111.00000000

The route 192.168.00001*xxx.xxxxxxxx* or 192.168.8.0/21 (also written as 192.168.8.0 255.255.248.0) summarizes these eight routes.

Using IP Unnumbered Serial Interfaces

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** *type number* interface configuration command. In the command, *type number* indicates the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface. To disable the IP processing on the interface, use the **no** form of this command.

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. The router also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. (For example, if the **network** command configured for the RIP routing protocol indicates that network 10.0.0.0 is running RIP, then all interfaces with an address in network 10.0.0.0 will be running RIP, as will all unnumbered interfaces that specify an interface that has an address in network 10.0.0.0.)

Restrictions on unnumbered interfaces include the following:

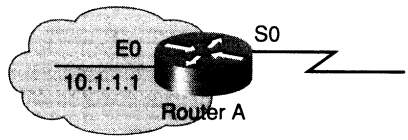
- Serial interfaces using High-Level Data Link Control (HDLC); Point-to-Point Protocol (PPP); Link Access Procedure, Balanced (LAPB); and Frame Relay encapsulations, as well as Serial Line Internet Protocol (SLIP) and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor the interface status.

The interface you specify (by the type and number parameters) must be enabled; in other words, it must be listed as up in the **show interfaces** command display.

NOTE Using an unnumbered serial line between different major networks requires special care. If at each end of the link different major networks are assigned to the interfaces you specified as unnumbered, then any routing protocol running across the serial line must not advertise subnet information. (For example, Router A and Router B are connected via an unnumbered serial line. Router A has all its interfaces in network 172.16.0.0, and therefore the serial line specifies an interface in network 172.16.0.0. Router B has all its interfaces in network 172.17.0.0, so the serial line specifies an interface in network 172.17.0.0. If OSPF is configured to run on the unnumbered serial line, it must be configured to summarize the subnet information and not send it across the link.)

In the example network in Figure 2-12, interface Serial 0 uses Ethernet 0's address. The configuration for the router in this figure is provided in Example 2-1.

Figure 2-12 *An Example of Using the ip unnumbered Command*



Example 2-1 *Configuration of the Router in Figure 2-12*

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
!
interface Serial0
 ip unnumbered Ethernet0
```

A loopback interface is often used as the interface from which unnumbered interfaces get their IP address. Loopback interfaces are virtual interfaces, so after they are defined, they are always active and cannot go down like a real interface.

Using Helper Addresses

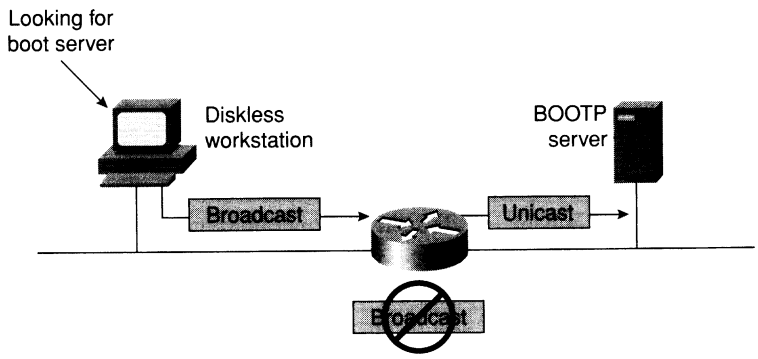
This section covers the use of helper addresses to forward selected broadcasts beyond a router. Routers do not forward broadcasts by default. By doing this, routers prevent broadcast storms—a situation in which a single broadcast triggers an onslaught of other broadcasts, ultimately leading to a disruption in network services. Large, flat networks are notorious for their bouts of broadcast storms.

However, a client might need to reach a server and might not know the server's address. In this situation, the client broadcasts to find the server. If there is a router between the client and server, the broadcast will not get through, by default. Helper addresses facilitate connectivity by forwarding these broadcasts directly to the target server.

Client hosts interact with a variety of network-support servers such as a Domain Name System (DNS) server, a Bootstrap protocol (BOOTP)/Dynamic Host Configuration Protocol (DHCP) server, or a Trivial File Transfer Protocol (TFTP) server. At startup time, the clients often do not know the IP address of the server, so they send broadcast packets to find it. Sometimes the clients do not know their own IP address, so they use BOOTP or DHCP to obtain it. If the client and server are on the same network, the server will respond to the client's broadcast request. From these replies, the client can glean the IP address of the server and use it in subsequent communication.

However, the server might not be on the same physical medium as the client, as shown in Figure 2-13. Remember that a destination IP address of 255.255.255.255 is sent in a link-layer broadcast (FFFFFFFFFFFF). By default, routers will never forward such broadcasts, and you would not want them to. A primary reason for implementing routers is to localize broadcast traffic. However, you do want clients to be capable of reaching the appropriate servers. Use helper addresses for this purpose.

Figure 2-13 *Routers Do Not Forward Broadcasts by Default*



Helper address commands change destination broadcasts addresses to a unicast address (or a directed broadcast—a local broadcast within a particular subnet) so that the broadcast message can be routed to a specific destination rather than everywhere. It is important to note that every broadcast (with the default port numbers, or with the port numbers that you specify) gets sent to all helper addresses, regardless of whether the server will actually be capable of helping for a certain port.

NOTE Helper addresses assist devices in locating necessary services within the network. It is more efficient administratively to allow a client device to broadcast for a service than to hard-code (in the client machines) the IP addresses for devices that may not always be online and available.

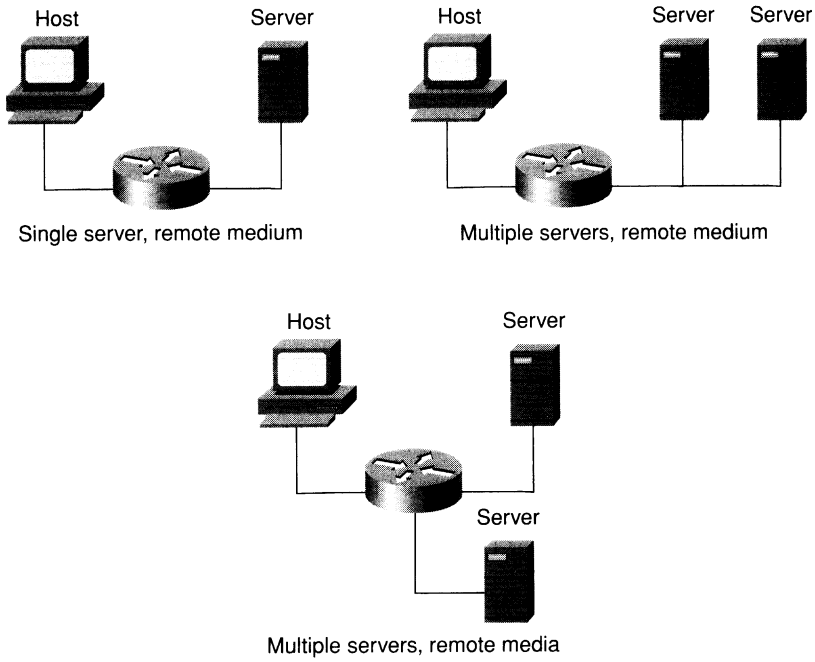
Server Location

It is important to consider how you want to get the broadcast, in a controlled way, to the appropriate servers. Such considerations depend on the location of the servers. In practice, server location is implemented in several ways, as shown in Figure 2-14:

- **A single server on a single remote medium**—Such a medium may be directly connected to the router that blocks the broadcast, or it might be several routing hops away. In any case, the all-ones broadcast needs to be handled at the first router it encounters and then sent to the server.
- **Multiple servers on a single remote medium, sometimes called a server farm**—Different kinds of servers (for example, DNS and TFTP servers used in the automatic install process [AutoInstall] for Cisco routers), could exist on the same medium. Or, perhaps redundant servers of the same type are installed on the same medium. In either case, a directed broadcast can be sent on the server farm subnet so that the multiple devices can see it.
- **Multiple servers on multiple remote media**—In this case, for example, a secondary DNS server could exist on one subnet and the primary DNS server could exist on another subnet. For fault tolerance, client requests need to reach both servers.

NOTE In Cisco IOS Release 12.0 and later, the **no ip directed-broadcast** command is on by default, which means that all received IP directed broadcasts are dropped. To enable the translation of directed broadcasts to physical broadcasts, use the **ip directed broadcast** interface configuration command.

Figure 2-14 *Servers May Be in Many Locations*



IP Helper Address Configuration

Use the **ip helper-address** *address* interface configuration command to configure an interface on which broadcasts are expected or can be received. In the command, *address* indicates the destination address to be used when forwarding User Datagram Protocol (UDP) broadcasts. The specified address can be the unicast address of a remote server or a directed broadcast address.

If an **ip helper-address** command is defined, forwarding for eight default UDP ports is enabled automatically. The default ports are TFTP (port 69), DNS (port 53), Time (port 37), Network Basic Input/Output System (NetBIOS) name service (port 137), NetBIOS datagram service (port 138), BOOTP server (port 67), BOOTP client (port 68), and Terminal Access Controller Access Control System (TACACS) (port 49).

These same eight UDP ports are automatically forwarded if you define an **ip helper-address** and the **ip forward-protocol udp** command with the same ports specified.

Use the **ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**} global configuration command to specify which type of broadcast packets are forwarded, as described in Table 2-3.

Table 2-3 ***ip forward-protocol** Command Description*

ip forward-protocol Command	Description
udp	UDP—the transport layer protocol
port	(Optional) When **udp** is specified, UDP destination port numbers or port names may be specified
nd	Network disk; an older protocol used by diskless Sun workstations
sdns	Network Security Protocol

To forward only one UDP port (whether a default-forwarded port, another UDP port, or a custom port), you must use **ip forward-protocol udp** *port* command for the ports that you want to forward, and then specify **no ip forward-protocol udp** *port* for the default ports that you do *not* want forwarded.

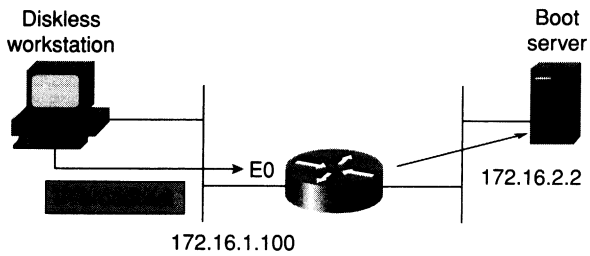
NOTE There is no easy way to forward all UDP broadcasts; you would need to specify all the UDP ports in the **ip forward-protocol** command.

DHCP and BOOTP use the same port—port 68—but it is always referred to as the BOOTP port.

IP Helper Address Examples

In the example shown in Figure 2-15, a single server is on a single remote medium. A helper address allows the router to perform the desired function of forwarding a client request to a server.

Figure 2-15 *IP Helper Address with a Single Server on a Remote Medium*



The configuration for the router in this example is shown in Example 2-2.

Example 2-2 *Configuration of the Router in Figure 2-15*

```
interface ethernet 0
   ip address 172.16.1.100 255.255.255.0
   ip helper-address 172.16.2.2
!
ip forward-protocol udp 3000
no ip forward-protocol udp tftp
```

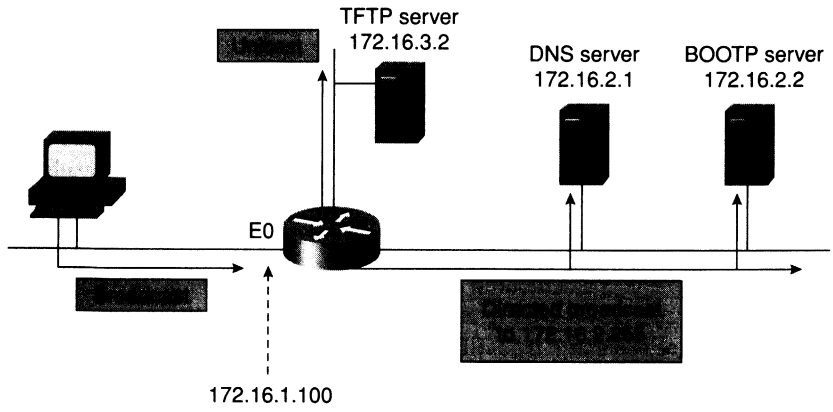
The **ip helper-address** command must be placed on the router interface that receives the original client broadcast. It causes the router to convert the 255.255.255.255 (all-ones) broadcast to a unicast or a directed broadcast. In Example 2-2, the **ip helper-address** command placed on interface Ethernet 0 would cause the default eight UDP broadcasts sent by all hosts to be converted into unicasts with a destination address of the boot server, 172.16.2.2. These unicasts would then be forwarded to the boot server.

You may not want to forward all default UDP broadcasts to the server, but only those of a protocol type supported on that server. To do this, use the **ip forward-protocol** command followed by the keyword **udp** and a port number or protocol name for those UDP broadcasts that are not automatically forwarded. Turn off any automatically forwarded ports with the **no ip forward-protocol udp** *port* or *port name* command. In Example 2-2, in addition to the default UDP broadcasts, the configuration has enabled the forwarding of a custom application using UDP port 3000. Because the server does not support TFTP requests, the automatic forwarding of TFTP, port 69, is disabled.

NOTE Additional helper addresses are not required on any routers in the middle of a series of routers in the path from the client to the server. This is because the first router has modified the destination address. The modification of the destination address from broadcast to unicast or directed broadcast allows the packet to be routed—over several hops, if necessary—to its final destination.

To handle forwarding broadcasts to multiple servers on the same remote medium, you can use a directed broadcast into the subnet instead of using several unicast helper addresses. The most general case is where multiple servers are located on different remote media. This case can be handled by a combination of multiple helper statements, some with a unicast and some with a directed-broadcast address. An example of this case is shown in Figure 2-16; the configuration for the router in this figure is shown in Example 2-3.

Figure 2-16 *IP Helper Address With Multiple Servers on a Remote Medium*



Example 2-3 *Configuration of the Router in Figure 2-16*

```
interface ethernet 0
  ip address 172.16.1.100 255.255.255.0
  ip helper-address 172.16.2.255
  ip helper-address 172.16.3.2
```

As Example 2-3 illustrates, a combination of helper addresses can be used on the same interface. Broadcasts arriving on Ethernet 0 will be forwarded to all servers on the 172.16.2.0 subnet and to the designated server (172.16.3.2) on the 172.16.3.0 subnet.

NOTE All broadcast traffic for the specified UDP ports (the default ports in Example 2-3) will be forwarded to both the 172.16.2.0 subnet and the 172.16.3.2 server. This will occur even for traffic that cannot be handled by the servers on that subnet. For example, DNS requests will be sent to the 172.16.3.2 TFTP server. Assuming that the DNS service is not enabled on the 172.16.3.2 device, this DNS request will be ignored and an ICMP "port unreachable" message will be generated. This sequence consumes bandwidth on the network.

Summary

In this chapter, you learned about IP addressing issues—address exhaustion and routing table growth—and solutions to these problems.

Hierarchical addressing can result in smaller routing tables and efficient allocation of addresses.

Using VLSMs can result in even more efficient use of IP addresses by allowing the use of multiple subnet masks within the same major network. VLSM addresses can then be summarized to reduce the routing table size.

Route summarization is a method of representing a series of network numbers in a single summary address. Summarizing of discontiguous subnets—subnets of the same major network that are separated by a different major network—requires care. Classful routing protocols do not support discontiguous subnets. Classless routing protocols do support discontiguous subnets.

CIDR is a solution developed to allow multiple Class C addresses to be combined into a larger classless set of IP addresses.

The use of an unnumbered interface in IP allows IP processing on a serial interface without using an explicit IP address.

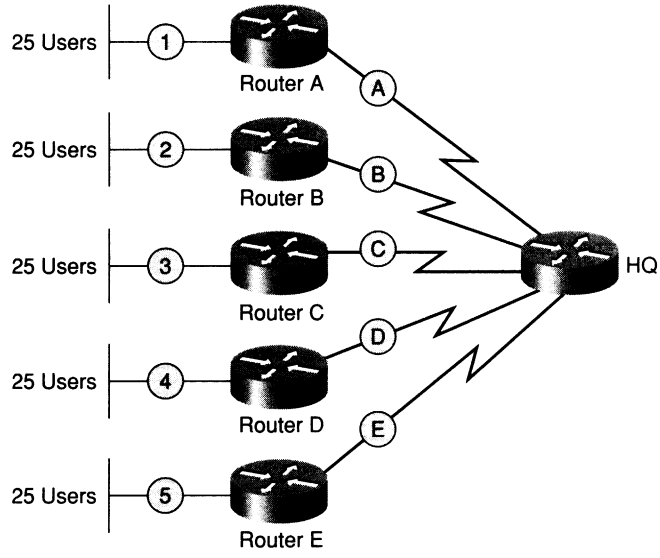
Helper addresses facilitate connectivity on networks by forwarding selected broadcasts to specified servers.

The next section of this book is Part II, "Scalable Routing Protocols." Part II discusses details of the OSPF, EIGRP, and BGP routing protocols.

Review Questions

Answer the following questions, and then refer to Appendix G, "Answers to the Review Questions," for the answers.

1 You are in charge of the network in the following figure. It consists of 5 LANs with 25 users on each LAN, and 5 serial links. You have been assigned the IP address 192.168.49.0/24 to allocate addressing for all links.



Write the addresses that you would assign to each of the LANs and the serial links in the following spaces.

LAN 1

LAN 2

LAN 3

LAN 4

LAN 5

WAN A

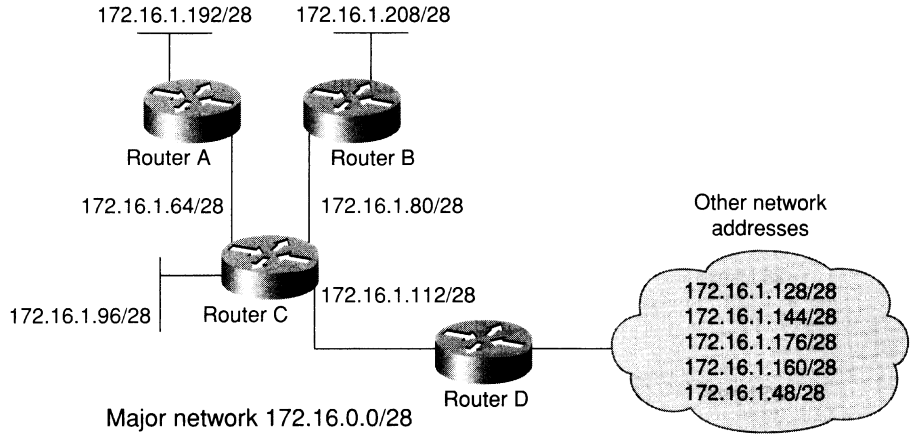
WAN B

WAN C

WAN D

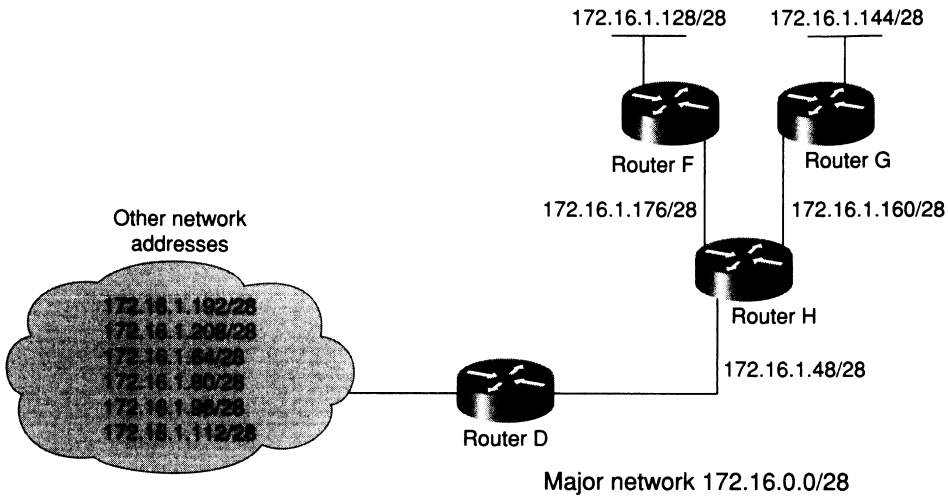
WAN E

2 The following figure shows a network with subnets of the 172.16.0.0 network configured. Indicate where route summarization can occur in this network and what the summarized addresses would be in the spaces that follow.



Router C Routing Table Entries	Summarized Routes That Can Be Advertised to Router D from Router C

3 The following figure shows a network with subnets of the 172.16.0.0 network configured. Indicate where route summarization can occur in this network and what the summarized address would be in the spaces that follow.



Router H Routing Table Entries	Summarized Routes That Can Be Advertised to Router D from Router H

4 What are some of the advantages of using a hierarchical IP addressing model?

5 Given an address with a prefix of /20, how many additional subnets are gained when subnetting with a prefix of /28?

6 When selecting a route, which prefix match is used?

from CCNP Routing Exam Certification Guide

by Clare Gough

(1-58720-001-5)

Cisco Press

About the Author

Clare Gough is a Cisco Certified Internetworking Engineer(CCIE #2893) and was a Cisco Certified Systems Instructor for the ICRC, ACRC, CIT, CLSC, and CID courses. She holds a master's degree in education and a master's degree in information systems. Over the last 15 years, she has developed and taught a variety of networking and internetworking courses throughout the world for Digital Equipment Co. and various Cisco training partners. She moved from England in 1991 and now lives in San Francisco with her family.

Contents at a Glance

Bold chapters are elements included in this folio.

This chapter covers the following topics that you will need to master to pass the CCNP/CCDP Routing exam:

- The features and operation of EIGRP.
- How EIGRP discovers chooses and maintains routes.
- How EIGRP supports the use of VLSM and summarization.
- How EIGRP functions in an NBMA environment.
- How EIGRP supports large networks.
- How to configure EIGRP, both in an enterprise network and in an NBMA network.
- How to verify an EIGRP configuration.
- Cisco defaults in EIGRP, the Cisco commands for implementing EIGRP, and the Cisco commands for reviewing the configuration of EIGRP.

CHAPTER 7

Using EIGRP in Enterprise Networks

This chapter covers in detail the Enhanced Interior Gateway Routing Protocol (EIGRP). Although EIGRP has the capability of supporting IP, AppleTalk, and IPX, the Routing exam will deal with only the mechanics of the IP routing protocol. This chapter expands on the understanding of routing within large enterprise networks that is covered in the previous chapter on OSPF within a large multiarea network.

This chapter is also broken into two topics. The first part of the chapter deals theoretically with how EIGRP works. How to implement and manage an EIGRP network is described at the end of the chapter. The operation of EIGRP, some of the options available, and design considerations are explained in this chapter, particularly in reference to scaling EIGRP and its use over a nonbroadcast multiaccess (NBMA) WAN environment. Both the network communication that the protocol uses and its configuration are explained in this chapter.

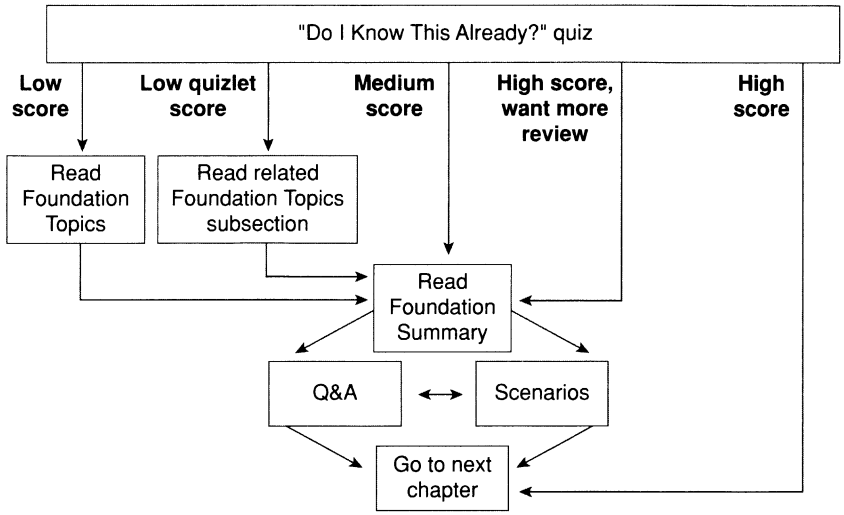
The topics in this chapter directly reflect questions on the Routing exam. EIGRP is designed for use in large networks. As a proprietary routing protocol for Cisco, it is therefore an obligatory subject in a Cisco exam on IP routing protocols. The BSCN course devotes 15 percent of its material to configuring EIGRP, and you can expect approximately 10 questions on the Routing exam to be directly related to this subject.

How to Best Use This Chapter

By taking the following steps, you can make better use of your study time:

- Keep your notes and the answers for all your work with this book in one place, for easy reference.
- When you take a quiz, write down your answers. Studies show that retention significantly increases by writing down facts and concepts, even if you never look at the information again.
- Use the diagram in Figure 7-1 to guide you to the next step.

Figure 7-1 *How to Use This Chapter*



If you skip to the Foundation Summary, Q&A, and scenarios sections and have trouble with the material there, you should go back to the Foundation Topics section.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide what parts of this chapter to use. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

This 16-question quiz helps you determine how to spend your limited study time. The quiz is sectioned into four smaller four-question "quizlets," which correspond to four major topics in the chapter. Figure 7-1 outlines suggestions on how to spend your time in this chapter. Use Table 7-1 to record your scores.

Table 7-1 *Score Sheet for Quiz and Quizlets*

Quizlet Number	Topic	Questions	Score
1	Features and operation of EIGRP, including NBMA networks	1 to 4	
2	How EIGRP discovers, chooses, and maintains routes	5 to 8	
3	How EIGRP supports large networks, including VLSM, summarization, and design	9 to 12	
4	How to configure and verify EIGRP (including NBMA networks)	13 to 16	
All questions	All	1 to 16	

1 EIGRP may be used to send information about which three routing protocols?

2 Which EIGRP packets are sent reliably?

3 In what instances will EIGRP automatically redistribute?

4 How long is the holdtime, by default?

5 What is an EIGRP topology table, and what does it contain?

6 What is the advertised distance in EIGRP, and how is it distinguished from the feasible distance?

7 What EIGRP algorithm is run to create entries for the routing table?

8 When does EIGRP place a network in active mode?

9 By default, EIGRP summarizes at which boundary?

10 What is Stuck in Active?

11 What is the **variance** command used for?

12 State two factors that influence EIGRP scalability.

13 What command is used to display which routes are in passive or active mode?

14 What command is used in EIGRP to perform manual summarization?

15 For Frame Relay, when would you configure the physical interface (as opposed to a subinterface) with the **bandwidth** command?

16 Which command is used to display all types of EIGRP packets that are both received and sent by a router?

The answers to this quiz are found in Appendix A, "Answers to Quiz Questions." The suggested choices for your next step are as follows:

- **2 or less on any quizlet**—Review the appropriate sections of the "Foundation Topics" portion of this chapter, based on Table 7-1. Then move on to the "Foundation Summary" section, the "Q&A" section, and the "Scenarios" at the end of the chapter.
- **8 or less overall score**—Read the entire chapter. This includes the "Foundation Topics" and "Foundation Summary" sections, the "Q&A" section, and the "Scenarios" at the end of the chapter.

- **9 to 12 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section and the "Scenarios" at the end of the chapter. If you have trouble with these exercises, read the appropriate sections in "Foundation Topics."
- **13 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section and the "Scenarios" at the end of the chapter. Otherwise, move to the next chapter.

Foundation Topics

Introduction: EIGRP in an Enterprise Network

EIGRP is an enhanced version of IGRP, hence the name. It uses the same distance vector technology. The changes were effected in the convergence properties and the operating efficiency of the protocol. It has some characteristics similar to those of a link-state routing protocol. Therefore, it is sometimes referred to as a hybrid routing protocol, although Cisco calls it an advanced distance vector protocol. It is an efficient, although proprietary, solution to networking large environments as it scales well. Its ability to scale is, like OSPF, dependent on the design of the network.

Case Study

The company Gargantuan, Inc., is a large multinational. It has its main offices in London, New York, San Francisco, and Tokyo. As a manufacturing company that produces cleaning products, it has plants in England, Mexico, and Japan. It has an extensive network that is running EIGRP. The network is used for local administrative purposes as well as coordinating the product movement from the manufacturing plant to the grocery store. There have been complaints during the past year about poor response times on the network. This has reached critical proportions because the problems are no longer simply irritations for the users, but they are now potentially devastating delays in shipping orders and transfers in electronic funds and manufacturing details.

A careful analysis of the network is required to identify the problem. A consultant has said that the entire organization needs to be readdressed and that configuration changes need to be made to the network. This involves an analysis of the network topology and data flow to appropriately design a new TCP/IP addressing scheme for the organization.

The CIO recently left, and there is very little documentation, so the network administrators have been charged with creating a network diagram and presenting some immediate solutions. This means that they have to thoroughly understand the operation of EIGRP in large environments. This chapter deals with the concepts of EIGRP and explains how it works within an enterprise. It considers design issues, particularly in reference to NBMA networks, and discusses the configuration and verification of the operation of the protocol.

EIGRP Defined

The focus of this chapter is on how EIGRP works so that those networks can be designed to maximize efficiency and truly scale the network.

The major concern in scaling an organizational network is controlling the network overhead that is sent, in particular over slow WAN links. The less information about the network, its

services, and networks that need to be sent, the greater the capacity available for the data between clients and servers. Although sending less routing information relieves the network, it gives the routers less information with which to make decisions. Every designer of routing protocols and every network administrator must deal continually with this trade-off. As seen with summarization, static and default routes can lead to poor routing decisions and loss of connectivity.

OSPF was the first protocol to attempt to address these problems. Alternatives to OSPF that offer the capability to scale to the size of modern networks are few. Static routing is one possibility, but it demands so much from the network administrator that it would never scale. IGRP offers another alternative; as a proprietary distance vector protocol, IGRP has solved many of the problems. However, it does face some issues with regard to scaling because of the inherent nature of distance vector. Although still distance vector and proprietary, EIGRP addresses many of the problems related to scaling the network that IGRP never anticipated.

This chapter discusses EIGRP. As a proprietary routing protocol, EIGRP can solve many problems seen in standards-based protocols that have to please all of the devices all of the time.

Operation of EIGRP

EIGRP is a revised and improved version of IGRP. Its goal is to solve the scaling limitations that IGRP faces, using the distance vector technology from which it grew. EIGRP increases the potential growth of a network by reducing the convergence time. This is achieved by the following:

- The Diffusing Update Algorithm (DUAL)
- Loop-free networks
- Incremental updates
- Multicast addressing for updates
- Holding information about neighbors as opposed to the entire network

These features depend on proprietary technology, which centers on local computation. The DUAL algorithm diffuses this computation over multiple routers, with each router responsible for its own small calculation and making requests of neighboring routers when necessary. A full understanding of the concepts and operation of EIGRP will aid you in the design, implementation, and maintenance of EIGRP networks, and will definitely help you pass an exam on the subject.

The main concepts of EIGRP are as follows:

- Advanced distance vector
- Loop-free routing tables
- Support for different topologies

- Rapid convergence
- Reduced bandwidth use
- Use of a composite metric (bandwidth and delay as the default)
- Unequal load balancing
- Neighbor discovery
- DUAL
- Successors, the selection process for a feasible successor
- Passive and active routes
- Protocol independence at Layer 3, allowing support for IP, AppleTalk, and IPX
- Reliable sending of routing updates
- VLSM, which allows efficient addressing, discontiguous networks, and the use of classless networks
- Manual summarization
- Compatibility with IGRP
- Easy-to-configure nature
- Fewer design constraints than OSPF

How EIGRP Works

Cisco identifies four main components of EIGRP:

- Protocol-dependent modules
- Reliable Transport Protocol
- Neighbor discovery/recovery
- DUAL

These components are discussed in this section. However, to understand how EIGRP works, there must be some familiarity with the terminology. Table 7-2 defines the main concepts and gives a brief synopsis of each term.

Table 7-2 *Terminology for EIGRP for IP*

Term	Definition
Neighbor	A router running EIGRP that is directly connected.
Neighbor table	A list of every neighbor, including the IP address, the outgoing interface, the holdtime, SRTT, and uptime or how long since the neighbor was added to the table. This table is built from information on hellos received from adjacent routers (neighbors).
Route table	The routing table, or list of available networks and the best paths. A path is moved from the topology table to the routing table when a feasible successor is identified.
Topology table	A table that contains all the paths advertised by neighbors to all the known networks. This is a list of all the successors, feasible successors, the feasible distance, the advertised distance, and the outgoing interface. DUAL acts on the topology table to determine successors and feasible successors by which to build a routing table.
Hello	Used to find and maintain neighbors in the topology table. They are sent periodically and are sent reliably.
Update	An EIGRP packet containing change information about the network. It is sent reliably. It is sent only when there is a change in the network to affected routers: When a neighbor first comes up When a neighbor transitions from active to passive for a destination When there is a metric change for a destination
Query	Sent from the router when it loses a path to a network. If there is no alternate route (feasible successor), it will send out queries to neighbors inquiring whether they have a feasible successor. This makes the route state change to active. The queries are sent reliably.
Reply	A response to the query. If a router has no information to send in a reply, it will send queries to all its neighbors. A unicast is sent reliably.
ACK	A hello packet with no data that is an acknowledgment of packets sent reliably.
Holdtime	Sent in the hello packet. It determines how long the router waits for hellos from a neighbor before declaring it unavailable. This information is held in the neighbor table.

Table 7-2 *Terminology for EIGRP for IP (Continued)*

Term	Definition
Smooth Round Trip Time (SRTT)	The time that the router waits after sending a packet reliably to hear an acknowledgment. This is held in the neighbor table and is used to calculate the RTO.
Retransmission Timeout (RTO)	Timer calculated in reference to the SRTT. RTO determines how long the router waits for an ACK before retransmitting the packet.
Reliable Transport Protocol (RTP)	Requirement that the packets be delivered in sequence and guaranteed.
Diffusing Update Algorithm (DUAL)	An algorithm performed on the topology table to converge the network. It is based on a router detecting a network change within a finite time, with the change being sent reliably and in sequence. As the algorithm is calculated simultaneously, in order and within a finite time frame on all affected routers, it ensures a loop-free network.
Advertised distance (AD)	The cost of the path to the remote network from the neighbor (the metric from the next-hop router).
Feasible distance (FD)	The lowest-cost distance (metric) to a remote network.
Feasible condition (FC)	When a neighbor reports a path (AD) that is lower than the router's FD to a network. The neighbor's (next-hop router's) path has a lower metric than the router's path.
Feasible successor (FS)	The neighbor reporting the AD that is lower than the router's FD becomes the feasible successor. The next-hop router that meets the FC.
Successor	The next-hop router that passes the FC. It is chosen from the FSs as having the lowest metric to the remote network.
Stuck in Active (SIA)	When a router has sent out network packets and is waiting for ACKs from all its neighbors. The route is active until all the ACKs have been received, if they do not appear after a certain time, the router is Stuck in Active for the route.
Query scoping	Another term for SIA.
Active	Route state when a network change is seen, but on interrogation of the topology table, there is no FC. The router queries its neighbors for alternative routes.
Passive	An operational route is passive. If the path is lost, the router examines the topology table to find an FS. If there is an FS, it is placed in the routing table and the router does not query the others, which would send it into active mode.

Even if the computation of the network is local, the router must know about the entire network. The explanation of the routing protocol will be given through the viewpoint of one router. When the network communication between the routers running EIGRP is understood, the operation of EIGRP will become clear; the concepts and terms will be placed in context. This facilitates the memorization of the subject; rote learning is no longer necessary.

The Hello Protocol

The router sends out a small hello packet to dynamically learn of other routing devices that are in the same broadcast domain.

NOTE A broadcast domain identifies devices that are within the same Layer 2 domain. Although they may not be directly connected to the same physical cable, if they are in a switched environment, from a logical Layer 2 or Layer 3 perspective, they are on the same link. If a broadcast is sent out, all the devices within the broadcast domain will hear the message and expend resources determining whether it is addressed to them. A Layer 3 device is a broadcast firewall, in that a router does not forward broadcasts.

Becoming a Neighbor

The Hello protocol uses a multicast address of 224.0.0.10, and all routers periodically send hellos. On hearing hellos, the router creates a table of its neighbors. The continued receipt of these packets maintains the *neighbor table*. If a hello from a known neighbor is not heard within a predetermined amount of time, as stated in the *holdtime*, the router will decide that the neighbor is no longer operational and will take the appropriate action. The holdtime is set at the default of three times the Hello timer. Therefore, if the router misses three hellos, the neighbor is declared dead. The Hello timer on a LAN is set to 5 seconds; the holdtime, therefore, is 15 seconds. On a WAN link, the Hello timer is 60 seconds, and the holdtime correspondingly is 180 seconds.

To become a neighbor, the following conditions must be met:

- The router must hear a hello packet or an ACK from a neighbor.
- The AS number in the packet header must be the same as that of the receiving router.
- The neighbor's metric settings must be the same.

The Neighbor Table

Each Layer 3 protocol has its own neighbor table—which makes sense because the neighbor, topology, and routing tables would differ greatly. Although all the information could be held in one table, the different EIGRP processes would all have to access the same table, which would complicate and slow down the lookup.

The Contents of the Neighbor Table

The neighbor table includes the following information:

- The address of the neighbor.
- The interface through which the neighbor's hello was heard.
- The holdtime.
- The uptime, how long since the router first heard from the neighbor.
- The sequence number. The neighbor table tracks all the packets sent between the neighbors. It tracks both the last sequence number sent to the neighbor and the last sequence number received from the neighbor. Although the Hello protocol is a connectionless protocol, other protocols used by EIGRP are connection-oriented. The sequence number is in reference to these protocols.
- *Smooth Round Trip Time (SRTT)* is used to calculate the *retransmission timeout (RTO)*. This is the time in milliseconds that it takes a packet to be sent to a neighbor and a reply to be received.
- RTO, the retransmission timeout. This states how long the router will wait on a connection-oriented protocol without an acknowledgment before retransmitting the packet. If the original packet that was unacknowledged was multicast, the retransmitted packets will be unicast.
- The number of packets in a queue. This is a means by which administrators can monitor congestion on the network.

Packets from Neighbors That Build the Topology Table

After the router knows who its neighbors are, it is in a position to create a database of feasible successors. This view of the network is held in the topology table.

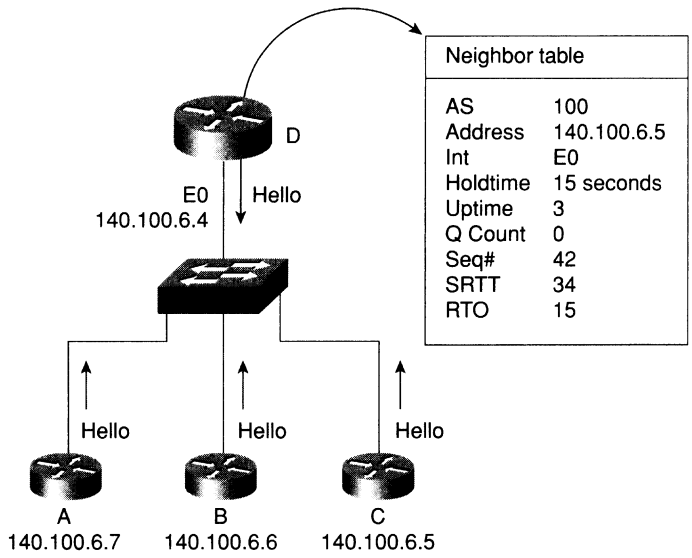
The *topology table* is created from *updates* received from the neighboring routers. The updates are exchanged between the neighbors.

Packets called *replies* will also update the topology table. Replies are sent in response to *queries* sent by the router, inquiring about suspect routes.

The queries and responses used by EIGRP for the DUAL algorithm are sent reliably as multicasts. If a router does not hear an acknowledgment within the allotted time, it retransmits the packet as a unicast. If there is no response after 16 attempts, the router marks the neighbor as dead. The window for the RTP is set as 1. The router must hear an acknowledgment from every router before it can send the next packet. The capability to send unicast retransmissions decreases the time that it takes to build the tables.

Figure 7-2 demonstrates building the neighbor table.

Figure 7-2 *Building the Neighbor Table*



The Topology Table

The topology table in EIGRP manages the selection of routes to be added to the routing table.

The topology table has a record of all known network routes within the organization. The table is built from the update packets that are exchanged by the neighbors and by replies to queries sent by the router. When the router has an understanding of the network, it runs DUAL to determine the best path to the remote network. The result is entered into the routing table.

Maintaining the Topology Table

The topology table is updated because the router either gains or loses direct connectivity with a router or hears a change through the network communication of EIGRP.

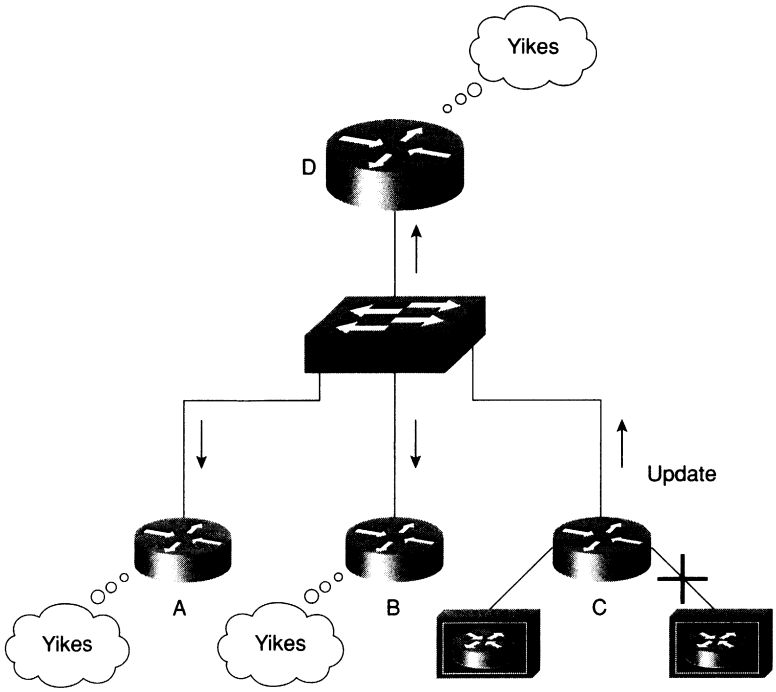
The following three reasons may cause a topology table to be recalculated:

- The router hears a change when a new network is available because of one of the following reasons:
  - — The topology table receives an update stating that there is a new remote network.
  - — The interface sees carrier sense for the network that is configured for a Layer 3 protocol supported by EIGRP, and the routing process has been configured with the appropriate network command.

- The router will change the successor in the topology table and routing table in these circumstances:
  - — The topology table receives a reply or a query from a neighbor.
  - — There is local configuration of a directly connected interface to change the cost of the link.
- The router hears a change from a neighbor when a network has become unavailable because of one of the following reasons:
  - — The topology table receives a query, reply, or update stating that the remote network is down.
  - — The neighbor table does not receive a hello within the holdtime.
  - — The network is directly connected and the router senses a loss of carrier.

Figure 7-3 illustrates the traffic flow seen when a router loses a direct connection.

Figure 7-3 *Maintaining the Topology Table—the Traffic Flow*



Just as the neighbor table tracks the receipt of the EIGRP packets, the topology table records the packets that have been sent by the router to the neighbors. It also identifies the status of the networks in the table. A healthy network is marked as *passive*; it will be labeled as *active* if the router is attempting to find an alternative path to the remote network that is believed to be down.

Because the routing table is built from the topology table, the topology table must have the information required by the routing table. This includes the next logical hop, or the address of the neighbor that sent the update with that network. The routing table will also calculate the metric to the remote network.

EIGRP Metrics

The metrics used in EIGRP are very similar to those of IGRP. The main difference is that the result of the calculation is held in a 32-bit field. This means that the decision can be much finer or detailed. The DUAL algorithm will use this metric to select the best path or paths to a destination. The computation is performed on paths held in the topology table to identify the best path to place into the routing table. There can be up to six paths held for one destination, and there can be three different types of paths. These three path types are described in Table 7-3.

Table 7-3 *EIGRP Routing Types*

Route Type	Description
Internal	Internal to the AS
Summary	Internal paths that have been summarized
External	External to the AS that have been redistributed into this EIGRP AS

The metric is the same composite metric used by IGRP, with the default being bandwidth and delay. Although it is possible to change the metric, this must be done only with great care and consideration to the network design. Any changes made must be effected on every router in the EIGRP AS.

The equation for the default metric used is this:

$$[(10000000 \div \text{smallest bandwidth kbps}) + \text{delay}] \times 256$$

Table 7-4 explains the metric values.

Table 7-4 *EIGRP Metric Values*

Metric Symbol	Metric Value	Description
K1	Bandwidth	Selects the smallest bandwidth media between the source and destination hosts. The equation used is [10000000 ÷ bandwidth kbps] × 256.
K2	Loading	Is based on the statistics held at the outgoing interface and is recorded in bits per second.
K3	Delay	Is the delay calculated on the outgoing interface. The value used is the summarization of the delay on all the interfaces between the hosts.
K4	Reliability	Is based on the statistics held on the outgoing interface gained from keepalives, and is exponentially averaged over 5 minutes.
K5	MTU	Is the smallest MTU found configured on an interface on route. This value is included although it has not been used as part of the metric calculation.

The new terminology can be very confusing and is best understood in context. It is easier to remember a concept or term when the function is understood. Given the overall understanding of how EIGRP works, a consideration of the topology table and its components will help explain the detail of EIGRP operation.

The DUAL Finite-State Machine

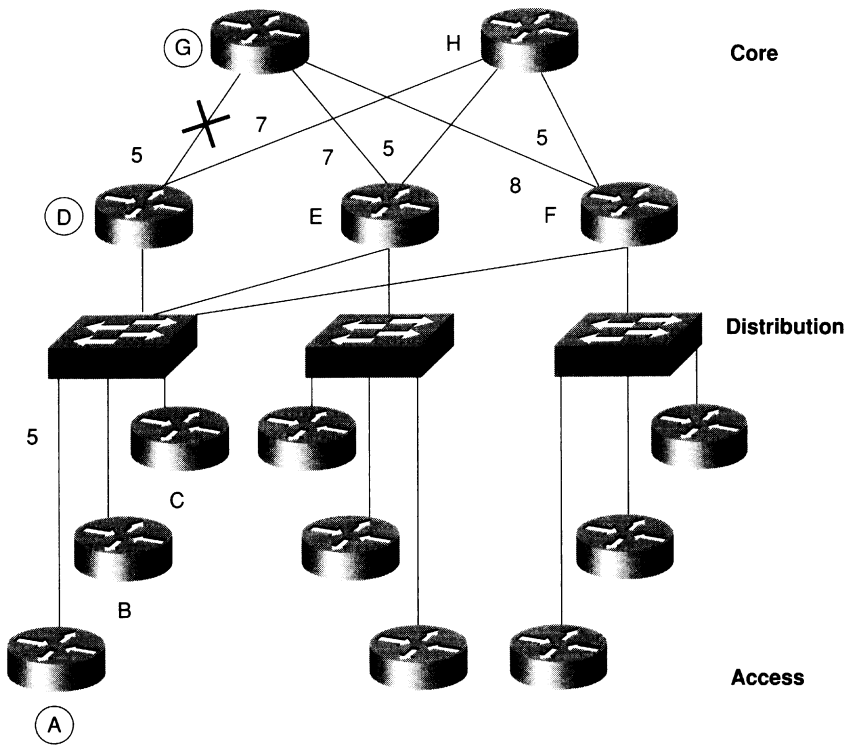
DUAL is responsible for maintenance of the topology table and the creation of the routing table. The topology table records the metric as received from the advertising router, or the next logical hop. It then adds the cost of getting to that neighbor, the one that is advertising the route.

The cost to the destination network from the advertising router, plus the cost to that router, equals the metric to the destination network from the router.

The metric or cost from the neighbor advertising the route is known as the *advertised distance*. The metric or cost from the router is referred to as the *feasible distance*. If the AD is less than the FD, then the next-hop router is downstream and there is no loop. This is fundamental to EIGRP.

Figures 7-4 and 7-5 illustrate these distances. Note that the metric shown in these figures has been simplified for the purposes of this example.

Figure 7-4 *The Use of Feasible and Advertised Distance—Passive Mode*



Updating the Routing Table in Passive Mode with DUAL

DUAL determines whether there is an acceptable route in the topology table to replace the current path in the routing table. In EIGRP terms, this is replacing a successor in the routing table with a feasible successor from the topology table.

The following actions are taken (using the network in Figure 7-4 as an example):

- In Figure 7-4, the FD from A to G is 10 (A to D to G).
- The AD from A to G is 5 (advertised from Neighbor D).
- Because 10 > 5, then FD > AD. This means that the FD is a feasible condition (FC), allowing it to become an FS. If the diagram is followed, it is very straightforward and less algebraic.
- If the link between D and G were down, A would look in its topology table.
- The alternative routes A to D to H to E to G have an AD of 19 (7 + 5 + 7).

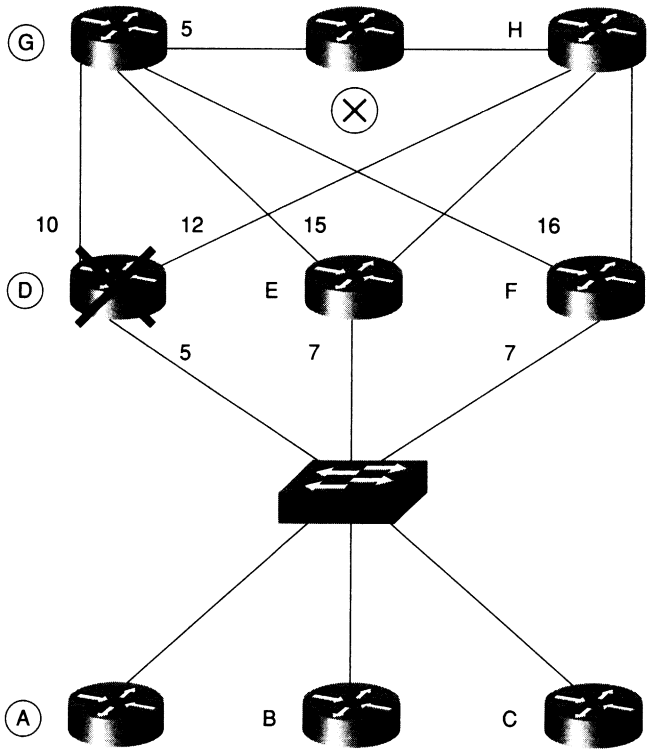
- Because 19 is greater than the original FD of 10, it does not qualify as an FS.
- The path D to H to F to G also has an AD of 19 and cannot be an FS.
- A to E to G has an AD of 7, however, which is less than the original 10. Therefore, this is an FS and can be replaced as a route without Router A changing from passive to active mode.
- The successor is Router D, while the FS is Router E.

The following example illustrates what happens when the topology table is interrogated and no feasible route is found.

Updating the Routing Table in Active Mode with DUAL

Figure 7-5 shows that the router has no acceptable route to substitute, however, and must therefore go into active mode to query its neighbors.

Figure 7-5 *The Use of Feasible and Advertised Distance—Active Mode*



When no alternative route is found in the routing table, the following actions are taken (using the network in Figure 7-5 as an example):

- In Figure 7-5, the topology table of Router A has a path (successor) of A to D to G to X.
- The FD is 20, and the AD from Neighbor D is 15.
- When Router D dies, Router A must find an alternative path to X.
- Neighbors B, C, E, and F have ADs of 27, 27, 20, and 21, respectively.
- Because all the neighbors have an AD that is the same or greater than the successor FD, none of these are acceptable as FSs.
- Router A must go into active mode and send queries to the neighbors.
- Both Routers E and F reply with an FS because both have an AD from G of 5. Remember the equation FD > AD; their FD is 20, and 20 > 5.
- This is acceptable. The topology and routing tables will be updated, DUAL will be calculated, and the network will be returned to passive mode.
- From this information received from Routers E and F in Figure 7-5, the router selects the path through E as the best route because it has the lower cost.
- The result is placed in the routing table as the valid neighboring router. EIGRP refers to this neighboring router as a *successor*.
- Router F will be stored as an FS in the topology table.

The details on how EIGRP computes successors are complex, but the concept is simple.

Choosing a Successor

To determine whether a path to a remote network is feasible, EIGRP considers the FC of the route. Essentially, each router holds a routing table that is a list of the available networks and the best or most efficient path to each of them. The term used to describe this is the *feasible distance of the successor*, otherwise known as the metric for the route. The router also holds the routing table of its neighbors, referred to as the AD. If the AD is within scope, this route may be identified as an alternative route, or an FS.

A neighbor can become an FS for a route only if its AD is less than the FD. This is DUAL's fundamental key to remaining loop-free; if a route contains a loop, the AD will be greater than the FD and therefore will fail the FC. By holding the routing tables of the neighbors, the amount of network overhead and computation is reduced. When a path to a remote network is lost, the router may well be capable of finding an alternative route with minimal fuss, computation, or network traffic. This gives the much-advertised benefit of very fast convergence.

The Topology Table Fields

The topology table includes the following information:

- Whether the route is passive or active.
- That an update has been sent to the neighbors.
- That a query packet has been sent to the neighbors. If this field is positive, at least one route will be marked as active.
- If a query packet has been sent, another field will track whether any replies have been received from the neighbors.
- That a reply packet has been sent in response to a query packet received from a neighbor.
- The remote networks.
- The prefix or mask for the remote network.
- The metric for the remote network, the FD.
- The metric for the remote network advertised by the next logical hop, the AD.
- The next logical hop.
- The outgoing interface to be used to reach the next logical hop.
- The successors, the path to the remote network stated in hops.

Adding a Network to the Topology Table

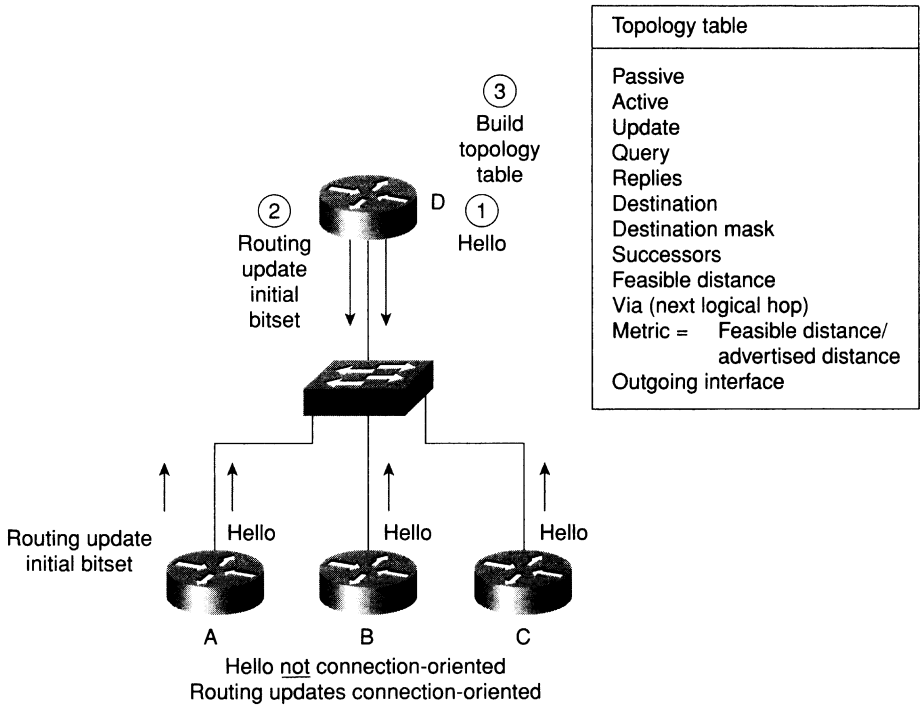
Imagine the router (Router A) that hears a new network. The administrator has plugged in another Ethernet cable to service a department that has moved into the building.

- As soon as Router A becomes aware of the new network, it starts to send Hello packets out the new interface. No one answers because this is an access router giving connectivity to the workstations and other end devices.
- There are no new entries in the neighbor table because no neighbors have responded to the Hello protocol. There is a new entry in the topology table, however, because this is a new network.
- EIGRP, sensing a change, is obliged to send an update to all its neighbors, informing them of the new network. The sent updates are tracked in the topology table and the neighbor table because the updates are connection-oriented and the acknowledgments from the neighbors must be received within a set time frame.
- Router A, having added the network to the topology table, adds the network to the routing table. The network will be marked as passive because it is operational.

- Router A's work is done. Router D's work has just begun. Router D is the backbone router in the basement of the building acting at the distribution layer. Its neighbors are routers on each floor and the routers in the other buildings.
- On hearing the update from Router A, Router D updates the sequence number in the neighbor table and adds the network to the topology table. It calculates the FD and the successor to place in the routing table. It is then in a position to send an update to all of its neighbors, except Router A. It is obeying the split horizon rule here.

In this manner, the new network is propagated to the affected routers. Figure 7-6 shows this propagation. The initial bit is set in the EIGRP header to indicate that the routes in the update represent a new neighbor relationship.

Figure 7-6 *EIGRP—Updating the Topology Table with a New Router*

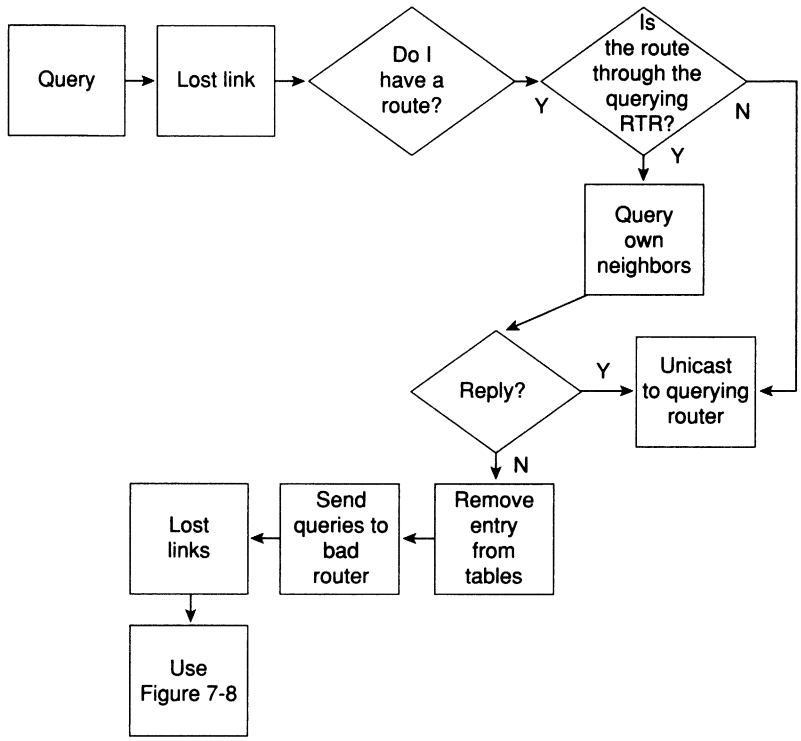


Removing a Path or Router from the Topology Table

This process is far more complex and gets to the crux of EIGRP. The following process uses Figure 7-6 and Figure 7-7 and focuses on Router D:

- If a network connected to Router A is disconnected, Router A updates its topology and routing table, and sends an update to its neighbors.

Figure 7-7 *EIGRP—Maintaining the Topology Table, Router D*



- When Router D receives the update, it updates the neighbor table and the topology table.
- As a router, it is programmed to find an alternative route to the remote network. It examines the topology table for alternatives. Because there was only one path to the remote network, no alternatives will be found.
- The router then sends out a query to the neighbors requesting that they look in their tables for paths to the remote network. The route is marked active in the topology table at this time.
- The query is tracked and, when all the replies are in, the neighbor and topology tables are updated.
- DUAL, which starts to compute as soon as a network change is registered, runs to determine the best path, which is placed in the routing table.
- Because no alternative route is available, the neighbors reply to the query stating that they have no path.

- Before they respond, they have queried their own neighbors; in this way, the search for an alternative path extends throughout the organization.
- When no router can supply a path to the network, all the routers remove the network from their routing and topology tables.

Life becomes more interesting when a neighbor does have an alternative route.

Figure 7-7 shows the actions taken when a router receives a query from another router asking for an alternative route to a destination. Note that if the queried router has no route to offer, it is still obliged to respond to the querying router.

Figure 7-8 illustrates the logic flow in a router that realizes a link has been lost, which may occur because a directly connected interface has lost a carrier signal or because the router has received an update or query.

Finding an Alternative Path to a Remote Network

When the path to a network is lost, EIGRP goes to a lot of trouble to find an alternative path. This process is one of the major benefits of EIGRP. The method it has chosen is very reliable and very fast. Figure 7-9 and the following list describe the process.

NOTE Note that the metric shown in Figure 7-9 has been simplified for the purposes of this example.

Using Figure 7-9 as reference for the topology of the network, follow the sequence of events:

- Router D marks the routes that were reached by sending the traffic to Router G.
- It looks in the topology table, which has every network and path of the network, to determine whether there is an alternative route. It is looking for an FS.
- An FS is determined by a clear equation. The topology table has listed for every route or successor an AD and an FD. This comprises the metric by which the route was selected.
- Router D adds the alternative route to X via B, found in the topology table, without moving into active mode because the AD is still less than the original FD. The AD is 5; the original FD was 15. It needs to send updates to its neighbors because the distance has changed.
- If the router did not have an FS, it would have placed the route into an active state while it actively queried other routers for an alternative path.
- After interrogating the topology table, if a feasible route is found, the neighbor replies with the alternative path.

Figure 7-8 *Maintaining the Topology Table—Choosing a Feasible Successor*

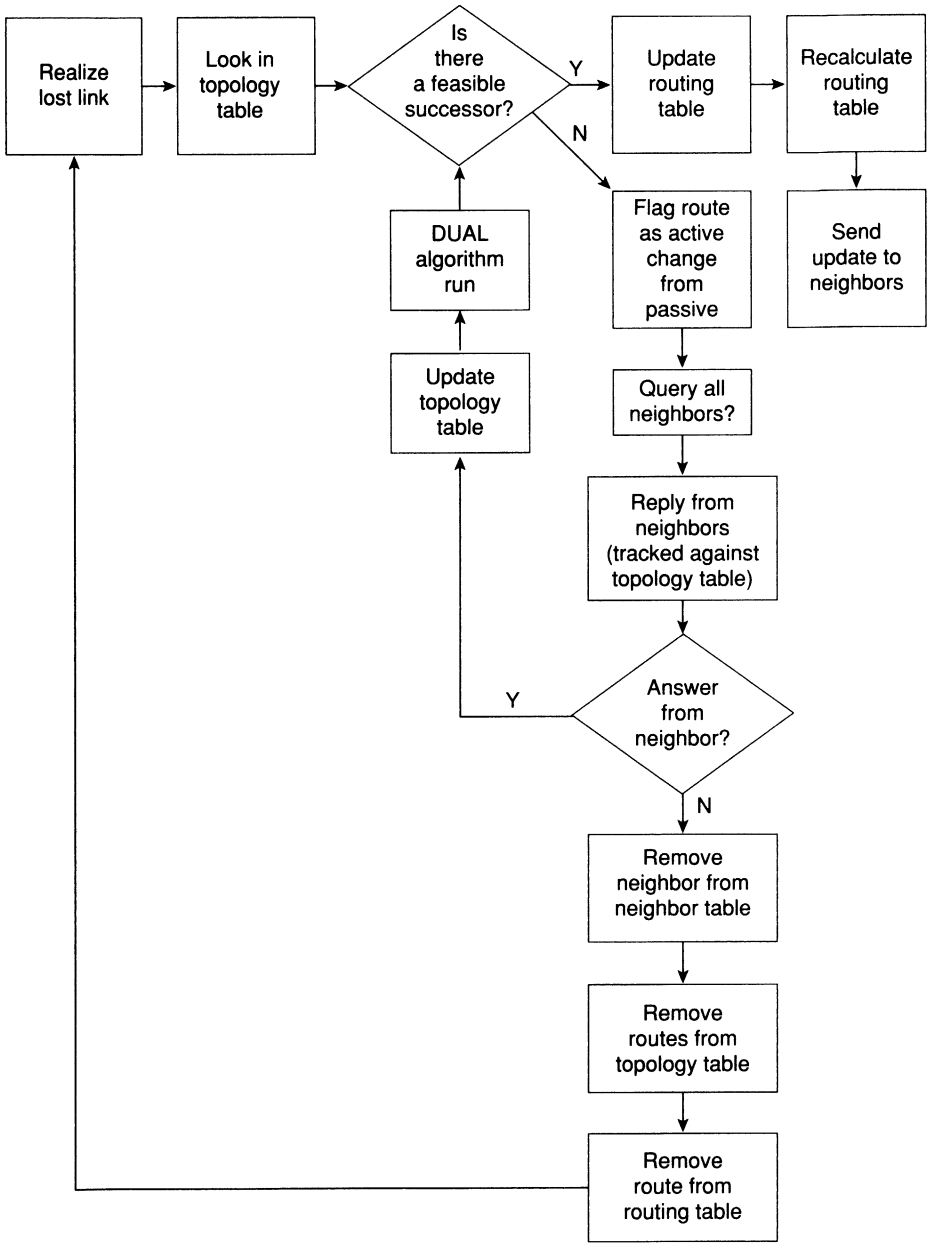
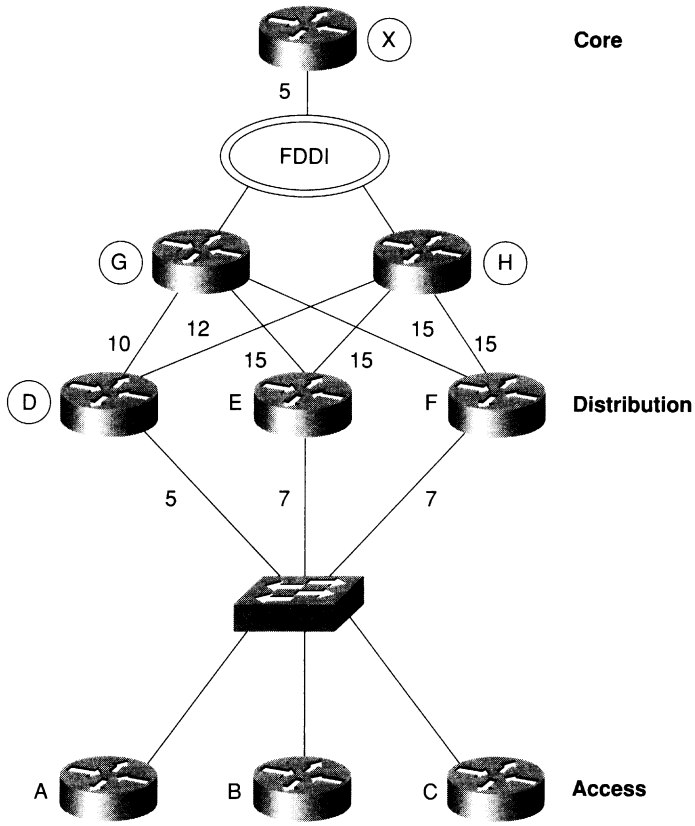


Figure 7-9 *Campus Topology Map Showing Alternative Path Selection*

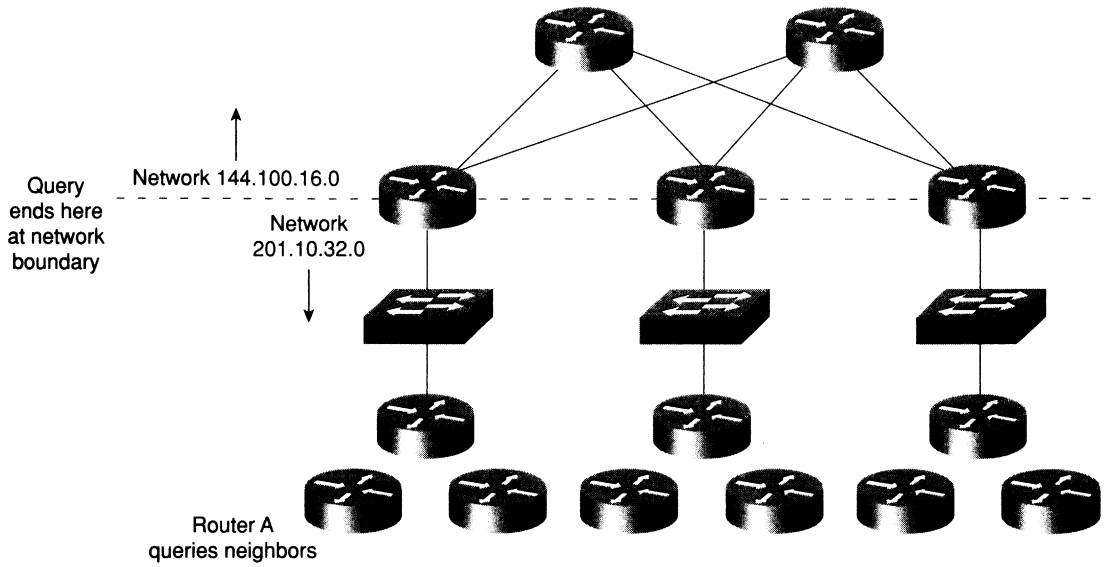


- This alternative path is then added to the topology table.
- Next, in the last steps of the DUAL algorithm, the routing table is updated.
- The network is placed back into a passive state as the router returns to sleep until the next change in the network.
- If a neighbor that has been queried has no alternative path or FS, it places the network into active mode and queries its neighbors.
- If no answer is heard, the messages are propagated until they hit a network or autonomous system boundary.

NOTE Figures 7-4 and 7-5 illustrate the process described in the previous sections, "Updating the Routing Table in Passive Mode with DUAL," and "Updating the Routing Table in Active Mode with DUAL."

Figure 7-10 illustrates the boundary for the propagation of query packets.

Figure 7-10 *The Propagation of Query Packets*



When the router sends a query packet, it is recorded in the topology table. This to ensure a timely reply. If the router does not hear a reply, the neighbor is removed from the neighbor table; all the networks held in the topology table for that neighbor are seen as suspect, and the networks are queried. Occasionally, because of slow links and burdened routers in a large network, problems can occur. In particular, a router may not receive a reply from all the queries that it sent out. This leads to the route being declared *Stuck in Active (SIA)*; the neighbor that failed to reply will be removed from the neighbor table, and DUAL will assume a reply giving an infinite metric.

As can be seen in the explanation for finding an FS, queries can be sent throughout the organization's network. This is the design key to ensuring that EIGRP scales.

Scaling EIGRP

EIGRP is designed to work in very large networks. However, as with OSPF, this is design-sensitive. Scaling a network—or, in other words, its capability to grow in size and complexity—are major concerns in today's organizations. New demands are constantly driving the networks into using applications that require more bandwidth and other resources from the network. Simply consider the need for every desktop and every user to be able to attach to centralized resources as well as the Internet. The need to understand the complications that arise from this need to grow networks is dealt with in detail in Chapter 2, "Managing Scalable Network Growth." Although it is not within the scope of the exam, it is the goal of much of its content.

Reasons for a Poorly Scaled EIGRP Network

The factors that can affect the scaling of EIGRP are these:

- The amount of information sent between neighbors
- The number of routers that are sent updates
- How far away the routers are that have to send updates
- The number of alternative paths to remote networks

Symptoms of a Poorly Scaled EIGRP Network

Poorly scaled EIGRP networks can result in the following:

- A route being SIA
- Network congestion
  - — Delays
  - — Routing information being lost
  - — Flapping routes
  - — Retransmission
- Router memory running low
- Router CPU overutilized
- Unreliable circuit or unidirectional link

Some of these symptoms are caused by other factors, such as poor design, with resources overwhelmed by the tasks assigned. Often many of these symptoms will be characterized by a route being flagged as SIA, as the router waits for a reply from a neighbor across a network that cannot handle the demands made upon it.

Careful design and placement of network devices can remedy many of the problems seen in a network.

Solutions to EIGRP Scaling Issues

The design of the network is very important to the ability to scale any network. The following solutions all revolve around a carefully thought-out network.

- Contiguous allocation of addresses, to allow summarization
- A hierarchical tiered network design, to allow summarization
- Summarization
- Sufficient network resources (both H/W and S/W) on network devices

- Sufficient bandwidth on WAN links
- Appropriate EIGRP configuration on WAN links (detailed later in this chapter)
- Filters
- Network monitoring

Design Issues Particular to EIGRP

It should be remembered that the queries must be limited to ensure that EIGRP can properly scale. If the queries are allowed to traverse the entire organization, then the problems and symptoms described will ravage your network.

Many believe that dividing the organization's network into different EIGRP autonomous systems is a good way of limiting the query range. This is true because EIGRP does not share updates with another AS. However, many organizations that created the autonomous systems to replicate OSPF areas naturally redistribute between them so that the entire organization can share routing information. At this point, the query is propagated into the new AS, and the problem continues. Summarization is the best way to limit the query range of EIGRP networks.

If redistribution is used, then it should be accompanied by route filters to ensure that feedback loops are not generated.

Certain topologies, although valid in most instances, pose problems for the EIGRP network. This is true in particular for the hub-and-spoke design often seen implemented between the remote sites and the regional offices. The popular dual-homed configuration, while providing redundancy, also allows the potential for routers to reflect queries back to one another. Summarization and filters make this network design work well while also allowing queries to be managed effectively.

The Routing Table

The routing table is built from the topology table after DUAL has been run. The topology table is the foundation of EIGRP: This is where all the routes are stored, even after DUAL has been run. It is in the routing table that the best paths are stored and accessed by the routing process.

Now that the tables have been built, the router can make routing decisions (a process explained in the preceding chapter).

Having built the appropriate tables, the technology holds one more secret: how to maintain the tables as current and accurate.

If you understand the principles of EIGRP functionality, configuring it is straightforward. The following section deals with the commands required to configure EIGRP. Before effective configuration can be achieved, the entire network should be analyzed from a design perspective, particularly with regard to summarization. Refer to Chapter 3, "IP Addressing," for a review of summarization.

Configuring EIGRP

The commands for EIGRP are consistent with the other IP routing protocols. Although IP routing is on automatically, the chosen routing protocol must be configured and the participating interfaces must be identified.

EIGRP allows for VLSM and, therefore, summarization because the mask is sent in the update packets. Although summarization is automatic, EIGRP summarizes at the NIC or major network boundary. To summarize within the NIC number, it must be manually configured. Unlike OSPF that can only summarize at the Area Border Router (ABR), EIGRP can summarize at any router.

WARNING EIGRP is a new protocol and has evolved over the past few years. It is essential that, in a practical situation, the commands and configuration be researched for the IOS code level that is installed in your network.

This section covers the following:

- Required configuration commands of EIGRP
- Optional configuration commands of EIGRP
- What each configuration command achieves
- An example of how the configuration command achieves its goal

The Required Commands for Configuring EIGRP

The router needs to understand how to participate in the EIGRP network. Therefore, it requires the following:

- **The EIGRP process**—The routing protocol needs to be started on the router.
- **The EIGRP autonomous system number**—All routers sharing routing updates and participating in the larger network must be identified as part of the same autonomous system. A router will not accept an update from a router configured with a different AS number.
- **Participating router interfaces**—The router may not want to have all its interfaces to send or receive EIGRP routing updates. A classic example is a dialup line to a remote office. If there were only one subnet at the remote office, it would be more efficient to use default and static route commands because any updates would dial the line.

By default (unless the **SETUP** script is used), there is no IP routing protocol running on the Cisco router. This is not true of other protocols, however. If an IPX network address is configured on an interface, for example, the IPX RIP process will be automatically started.

To configure EIGRP as the routing protocol, the following command syntax is used:

```
router eigrp autonomous system number
```

Although EIGRP has been turned on, it has no information on how to operate. The connected networks that are to be sent in the EIGRP updates and the interfaces that participate in the EIGRP updates must be defined. If the EIGRP information is not specified, the process with insufficient configuration will never start.

WARNING Most versions of the IOS do not offer an error message, and this can make troubleshooting more difficult. Refer to the section titled "Verifying the EIGRP Operation," later in this chapter, for more information.

The following command syntax shows the use of the **network** command prior to IOS 12.0(4)T:

```
network network number
```

The **network** command plays a similar role to that of the **network** command in RIP or IGRP. Unlike OSPF, in which it is possible to identify the specific address of an interface, the **network** command for EIGRP is stated at the class level. EIGRP does not have the design specification of areas and, therefore, has no need for granularity.

WARNING A common error is to configure the **network** command with an inappropriate wildcard mask when you're confused as to which class of address is being used.

From Cisco IOS 12.0(4)T, there have been some significant changes to the **network** command. It is now possible to identify which interfaces are running EIGRP by stating a wildcard mask. This is similar to the use of the **network** command in OSPF. However, OSPF has the added parameter, which defines the area for the interface.

The new syntax is as follows:

```
network network-number [wildcard network-mask]
no network network-number [wildcard network-mask]
```

The following syntax illustrates the use of the **network** command (the router has two Ethernet interfaces):

```
interface  e1
ip address 155.16.1.1 255.255.255.0
!
interface e2
ip address 155.16.2.2 255.255.255.0
```

The following command indicates that EIGRP will run on interface e1 only:

```
router eigrp 100
network 155.16.1.1 0.0.0.0
```

In earlier versions, as soon the first part of the command was configured, the operating system corrected the address to the NIC or major network number, 155.16.0.0, which would include both e1 and e2:

```
network 155.16.1.1
```

After the network has been defined to EIGRP, it will identify the interfaces directly connected to the routers that share that network address.

Having identified the interfaces on the router that are participating in the EIGRP domain, the following will happen:

- Updates will be received on the interface.
- Updates will be sent out the interfaces.
- The network will be advertised out all EIGRP interfaces.
- If appropriate, the Hello protocol will be propagated.

The Optional Commands for Configuring EIGRP

These commands are used to tune the way EIGRP works within your network. They should be used in reference to the design of the network and its technical requirements.

This section considers the following optional EIGRP commands:

- no auto-summary
- variance
- ip summary address
- bandwidth
- bandwidth-percent

Summarization with EIGRP

This subject has been dealt with in depth in several other locations within this book. References are given to those sections in the interests of brevity. These should be referred to for revision purposes because summarization in EIGRP solves the same problems of scaling as seen in other networks.

For more information, refer to the sections, "Design Considerations in Multiple-Area OSPF," in Chapter 6, "Using OSPF Across Multiple Areas," and, "Summarization," in Chapter 3.

The difference in the configuration between EIGRP and OSPF is that the OSPF is summarized only at the area boundary. Because EIGRP does not use the concept of areas, it may be configured on any router in the network. Consideration in where to summarize is determined by the hierarchical structure of the network. If summarization is not configured, EIGRP will automatically summarize at the class boundary.

There are two commands for summarization with EIGRP. The first command is **no auto-summary**. This command is IOS-specific, and research should be done on your IOS code level before configuring your live network.

The command applies to the entire router. This is very important because if there are slow serial interfaces or congested links, they will transmit all the subnets known on the router. This may significantly increase the overhead for the link. The solution is to configure the **summary** command on all interfaces, which in turn demands careful deployment of addresses.

Manual summarization is configured at the interface level, as shown here:

```
interface S0
ip summary address eigrp autonomous-system-number address mask
```

Load Balancing in EIGRP

EIGRP automatically load-balances across links of equal cost. Whether the traffic is sent on a per-destination or round-robin basis depends on the internal switching within the router. It is possible to configure EIGRP to load-balance across unequal paths using the **variance** command. This command allows the administrator to identify by the use of the multiplier parameter the metric scope for including additional paths.

The command structure is shown here:

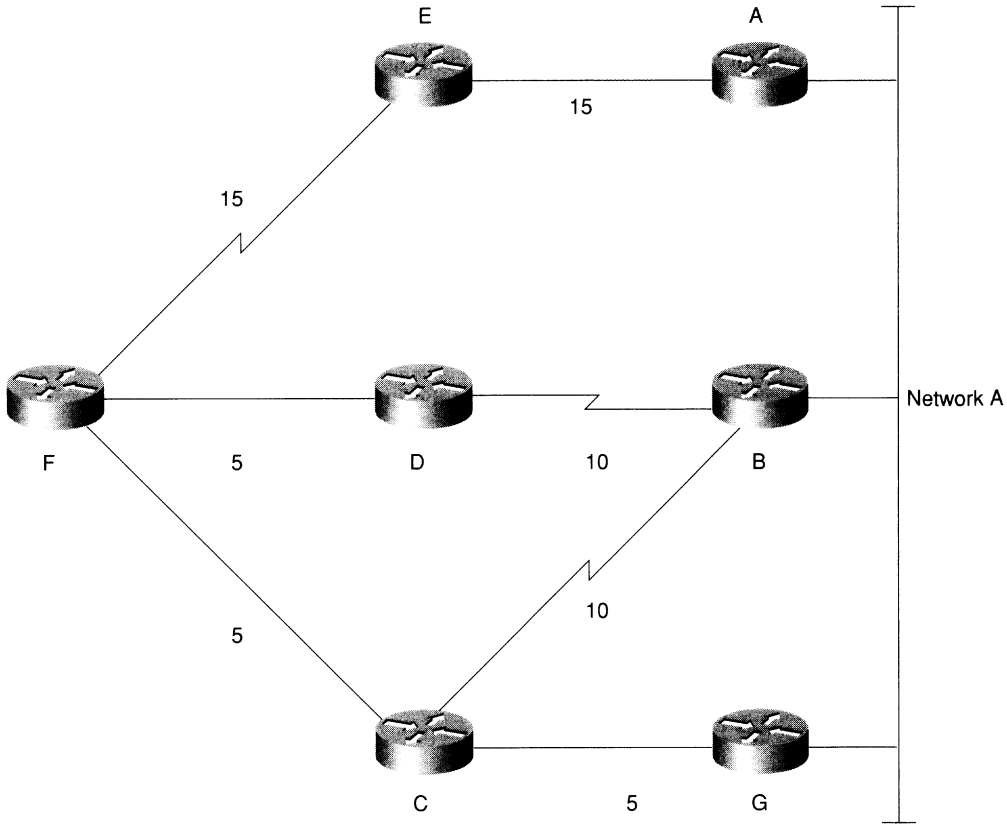
```
variance multiplier
```

The multiplier is a number that ranges from 1 to 128. The default is 1, which allows for equal-cost load balancing. If the number is higher, it will multiply the best cost or metric value for a path by the number stated as the multiplier. All paths to the same destination that have metrics within this new range are now included in load balancing. The amount of traffic sent over each link is proportional to the metric for the path.

For example, the route to network A has four paths to it from router F and the best path gave a metric value of 10. The available routes shown in Figure 7-11 reflect these paths:

F to E to A = 30
F to D to B = 15
F to C to B = 15
F to C to G = 10

Figure 7-11 *The* **variance** *Command*



If the **variance** command was configured with a variance (multiplier) of 2; then the best metric is $10 \times 2 = 20$.

These paths would all load-balance traffic from Router F to Network A:

F to D to B = 15
F to C to B = 15
F to C to G = 10

One and a half packets would be sent across the path F to C to G for every one packet sent across the other two available paths.

NOTE The router cannot really send only one and a half packets and then switch the link, because the routers can't stop transmitting after they've started sending a packet. From a practical perspective, two packets are transmitted. This the same case for custom queuing.

NOTE Only those paths that are in the topology table as FS are eligible to be included in the **variance** command. Also, appreciate that the example and figure shown are highly simplified for the purpose of explanation.

Bandwidth Control

A perennial concern of network administrators is the amount of bandwidth used for overhead traffic. Administrators want to minimize the amount of network control traffic sent through the network, to maximize the bandwidth available for user data. One of the major benefits of both EIGRP and OSPF is that they send as little network traffic as possible. This has the advantage of decreasing the convergence time of the network and ensuring that the network traffic that is sent arrives at the destination.

EIGRP Defaults in Bandwidth Utilization

EIGRP will not use more than 50 percent of the stated bandwidth on a link. The **bandwidth** command used on the interfaces of a Cisco router allows the default settings on links to be overridden. This is often necessary on serial links because the default bandwidth is 1.544 Mbps or a T1. If in reality the link is 56 kbps, it is easy to see how EIGRP could saturate the link. EIGRP will try to use 50 percent of a T1 link (772 kbps), far exceeding the real bandwidth of the line. This will mean not only the dropping of data packets due to congestion, but also the dropping of EIGRP packets. This will cause confusion in the network, not to mention miscalculated routes, retransmission, and user irritation as the network slows.

It is essential to configure all interfaces to reflect the true speed of the line.

NOTE Other technologies on a Cisco router will use this value to make decisions. Therefore, ensure that the bandwidth stated is indeed the speed of the link. When you issue the **show interface** command, the configured bandwidth of the link will be shown along with a field identifying the load on the line. The load is the amount of traffic sent out of the interface, proportional to the bandwidth of the link, in which the bandwidth is the stated bandwidth and not the speed of the interface.

If it is necessary to artificially lower the **bandwidth** command, this should be done in consideration of the other network applications.

The bandwidth is a logical construct whose value can have wide-reaching implications on the functioning of your network. It does not affect the actual speed of the link.

EIGRP and the Use of the bandwidth Command in WANs

The developers of EIGRP have provided configurations to suit the three different WAN environments. The three WAN environments are as follows:

- Point-to-point
- NBMA, such as Frame Relay, X25, or ATM
- Multipoint
  - — Point-to-point
  - — NBMA hybrid (this is a combination of the point-to-point and multipoint designs)

When configuring the **bandwidth** command, it is important to consider the actual speed of the link. It is practical to configure this only on serial lines, where the speed of the link will vary considerably. However, do not confuse the speed of the interface or access line with the bandwidth or committed information rate (CIR) of the virtual circuit (VC).

Rules in Configuring Bandwidth over an NBMA Cloud

Cisco identifies three rules that should be followed when configuring EIGRP over an NBMA cloud:

- EIGRP traffic should not exceed the CIR capacity of the VC.
- EIGRP's aggregated traffic over all the VCs should not exceed the access line speed of the interface.
- The bandwidth allocated to EIGRP on each VC must be the same in both directions.

If these rules are understood and followed, EIGRP works well over the WAN. If care is not taken in the configuration of the WAN, EIGRP can swamp the network.

Configuring Bandwidth over a Multipoint Network

The configuration of the **bandwidth** command in an NBMA cloud depends on the design of the VCs. If the serial line has many VCs in a multipoint configuration, then EIGRP will evenly distribute its overhead between the VCs, without the use of subinterfaces. The **bandwidth** command should therefore reflect the access link speed into the Frame Relay cloud. If the serial interface is accessing an NBMA environment such as Frame Relay, the situation is straightforward. Your company may have five VCs from your router's serial interface. Each VC is 56 kbps. The access link will need a capacity of 5×56 kbps, or at least 2046 kbps. Remember, the aggregate configured bandwidth cannot exceed the access speed of the interface.

Configuring Bandwidth over a Hybrid Multipoint Network

If the multipoint network has differing speeds allocated to the VCs, a more complex solution is needed. There are two main approaches.

- To take the lowest CIR and to simply multiply this by the number of circuits. This is applied to the physical interface. The problem with this configuration is that the higher-bandwidth links will be underutilized for some things.
- If possible, it is much easier to configure and manage an environment that has used subinterfaces, where a VC is logically treated as if it were a separate interface or point-to point. The **bandwidth** command may be configured on each subinterface, which allows different speeds on each VC. In this second solution, subinterfaces are configured for the links with the differing CIRs. The links that have the same configured CIR are presented as a single subinterface with a bandwidth, which reflects the aggregate CIR of all the circuits.

  Cisco recommends this as the preferred solution.

The following syntax shows the structure of the **bandwidth** command:

```
interface S0
bandwidth speed of line
```

The Configuration of the Pure Point-to-Point Network

If there are many VCs, there may not be enough bandwidth at the access speed of the interface to support it. The subinterfaces should be configured with a bandwidth that is much lower than the real speed of the circuit. In this case, it is necessary to use the **bandwidth-percent** command to indicate to the EIGRP process that it can still function.

The Use of The bandwidth-percent Command

Another command specific to EIGRP is the **bandwidth-percent** command. It is easier and simpler to use the **bandwidth** command than the **bandwidth-percent** command.

The **bandwidth-percent** command interacts with the **bandwidth** command on the interface. The reason for using this command is primarily because in your network, the **bandwidth** command does not reflect the true speed of the link. The **bandwidth** command may have been altered to manipulate the routing metric and path selection of a routing protocol, such as IGRP or OSPF. It might be better to use other methods of controlling the routing metric and return the bandwidth to a true value. Otherwise, the **bandwidth-percent** command is available. It is possible to set a bandwidth percent that is larger than the stated bandwidth. This is in the

understanding that although the bandwidth may be stated to be 56 kbps, the link is in fact 256 kbps. The following shows the structure of the **bandwidth-percent** command:

```
interface S0
ip bandwidth-percent eigrp autonomous-system-number percent
```

EIGRP can also be configured as a routing protocol for IPX and AppleTalk. The next section discusses this.

Configuring EIGRP for IPX

NOTE This section is included to place EIGRP in context. *The exam will test only on topics pertaining to EIGRP using IP.* Therefore, this section should be read only for interest and should not be studied in depth in preparation for the Routing exam.

The configuration of IPX is very similar to IP. The difference is that IPX is a client/server-based protocol that was originally designed to operate in a LAN environment. Although Novell has improved its technology over the past few years to allow the networks to scale across the enterprise domain, IPX can still prove both a design and an implementation headache for the administrator. Typically, the amount of overhead generated in a client/server network is greater than that of a peer-to-peer network. This overhead becomes problematic when slower WAN links are used and bandwidth is at a premium. In this environment, EIGRP is a powerful tool.

EIGRP offers the following main features to an IPX enterprise network:

- Incremental updates for both RIP and SAP traffic
- Faster convergence of the network
- An increased diameter of the network, through the use of the metric and hop count
- A more complex and sophisticated routing metric
- Automatic redistribution of networks among IPX RIP, NLSP, and EIGRP

The operation of EIGRP for IPX is the same as that of IP, although the EIGRP metric uses both bandwidth and delay in calculating the best path.

EIGRP for IPX uses the same major components:

- Reliable transport mechanism for updates
- DUAL
- Neighbor discovery/recovery
- Protocol-dependent modules

It is important to remember that IPX is still designed as a proprietary LAN client/server protocol. EIGRP is also a proprietary protocol, and although there are some devices on the market that support EIGRP, it cannot be assumed that these include IPX systems. In the design of the network using EIGRP, IPX RIP/SAP or NLSP will be running. These protocols are found on the LAN in the traditional client/server domain.

In the design of IPX in an enterprise network, EIGRP is used between Cisco routers when bandwidth is a precious commodity. Therefore, EIGRP is configured in the WAN, where it is unlikely that there are any clients or servers requiring RIP/SAP updates.

When IPX is configured on a Cisco router, it is necessary to turn on IPX routing and to allocate network addresses to the appropriate interfaces. This allows the router to route IPX traffic through those interfaces and to send and receive RIP/SAP updates.

Configuring EIGRP for IPX requires some additional commands. An additional routing protocol must be identified along with the interfaces that it supports. These interfaces are then removed from the RIP/SAP update schedule.

Example 7-1 is a sample configuration of a network that has both RIP/SAP and EIGRP running.

Example 7-1 *Configuring EIGRP for IPX*

```
Router(config)# ipx routing
Router(config)# ipx router eigrp 100
Router(config-router)# network FADED
Router(config)# ipx router rip
Router(config-router)#no network FADED
Router(config)#interface E0
Router(config-if)#ipx network FAB
Router(config)#interface E1
Router(config-if)#ipx network CAB
Router(config)#interface E2
Router(config-if)#ipx network DAB
Router(config)#interface s0
Router(config-if)#ipx network FADED
```

NOTE The autonomous system number used in the configuration of EIGRP for IPX must be the same on every router that wants to share routing updates. This is the same as the configuration for IP. The IPX autonomous system number is completely independent of the IP autonomous system number.

It is important to remember to remove the **network** command in IPX RIP routing configuration, as shown in the previous example. Otherwise, the system will continue sending IPX RIP updates in addition to IPX EIGRP updates, thus further affecting performance in the serial link.

EIGRP will automatically redistribute its routing information into RIP/SAP. It will also send only incremental updates through serial interfaces and will send periodic updates through LAN interfaces. EIGRP can be manually configured to send incremental updates out of the LAN interface, if required. Incremental updates might apply to networks that form a backbone in the network design—for example, where an FDDI ring or Fast Ethernet segments are connecting the distribution layer and forming the campus backbone.

The following is the command syntax to force a LAN interface to send incremental updates:

```
interface f0
ipx sap-incremental eigrp autonomous-system-number
```

Configuring EIGRP for AppleTalk

NOTE This section is included to place EIGRP in context. *The exam will test only on topics pertaining to EIGRP using IP.* Therefore, this section should be read only for interest and should not be studied in depth in preparation for the Routing exam.

EIGRP also supports the client/server protocol AppleTalk. Conceptually, the use of EIGRP is the same, although the configuration details differ. The main difference in configuration is that, whereas in configuring IP or IPX the autonomous system number must be the same for all routers sharing routing information, with AppleTalk, every router must have a unique process ID.

The configuration details of EIGRP for AppleTalk are beyond the scope of this book. Refer to the Cisco web site and documentation for details and design and configuration guidelines.

Moving Toward IP

In reality, most organizations are porting all their client/server platforms into IP, with the support of the vendors of the client/server products. EIGRP for either IPX or AppleTalk is most powerful when transitioning your organization to IP. If you are using EIGRP, be aware of the fast development of the technology, and ensure compatibility between the IOS versions by researching the Cisco web site.

Verifying the EIGRP Operation

The set of commands in this section is invaluable. These commands are crucial in the configuration, maintenance, and troubleshooting of a live network. As such, they are a necessary set of tools for use on a daily basis as well as on the CCIE lab exam.

For the preparation of the routing exam, understanding the output of these commands is important, not just because they may constitute questions on the exam, but because they reflect your conceptual understanding of the subject. The ability to analyze what is happening on the network demands a thorough understanding of the concepts explained in this chapter. This skill is required in interpreting the output of a **show** command.

This section deals with the following commands:

- **show ip eigrp neighbors**—Gives detailed information on the neighbors. This command records the communication between the router and the neighbors as well as the interface and address by which they communicate.
- **show ip eigrp topology**—Gives details about the routes held in the topology table and for detailed information on the networks that the router is aware of and the preferred paths to those networks, as well as the next logical hop as the first step in the path. The router will track the EIGRP packets that have been sent to neighbors in this table.
- **show ip eigrp topology all**—Gives details about all the routes and alternative paths held in the topology table. The router will track the EIGRP packets that have been sent to neighbors in this table.
- **show ip eigrp traffic**—Gives information on the aggregate traffic sent to and from the EIGRP process.
- **show ipx route**—Shows the routing table for IPX and is the source of the information on how to reach the remote destination network.

The EIGRP **show** commands are highly detailed and give a comprehensive understanding of the state of the network. The other commands generic to IP—**show IP route** and **show IP protocols**, as described in Chapter 5, "Using OSPF in a Single Area,"—are also useful in the maintenance of EIGRP.

The show ip eigrp neighbors Command

This command shows the neighbor table. The syntax is as follows:

show ip eigrp neighbors *type number*

Example 7-2 shows the output of this command.

Example 7-2 **show ip eigrp neighbors** *Output*

```
Router# show ip eigrp neighbors
IP-EIGRP Neighbors for process 100
Address          interface     Holdtime   Uptime     Q      Seq      SRTT      RTO
                               (secs)     (h:m:s)    Count  Num      (ms)      (ms)
140.100.48.22    Ethernet1     13         0:00:41    0      11       4         20
140.100.32.22    Ethernet0     14         0:02:01    0      10       12        24
140.100.32.31    Ethernet0     12         0:02:02    0      4        5         2
```

Table 7-5 explains the meaning of the important fields in Example 7-2.

Table 7-5 *Explanation of the* **show ip eigrp neighbors** *Command Results*

Field	Explanation
process 100	The autonomous system number used to identify routers from whom to accept routing updates.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the router is receiving hello packets from the neighbor.
Holdtime	Length of time, in seconds, that the router will wait to hear from the neighbor before declaring it down. The default is 15 seconds.
Uptime	Time, measured in hours, minutes, and seconds, since the router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the router has queued and is waiting to send.
Seq Num	The sequence number of the last packet that was received from the neighbor.
SRTT	Smooth Round Trip Time. The time is measured in milliseconds and is from the sending of the packet to the receipt of an acknowledgment from the neighbor.
RTO	Retransmission timeout, in milliseconds. This shows how long the router will wait before it retransmits the packet.

The show ip eigrp topology Command

This command shows the topology table. It allows for the analysis of DUAL. It will show whether the successor or the route is in an active or passive state. The syntax is as follows:

```
show ip eigrp topology [autonomous-system-number | [[ip-address] mask]]
```

Example 7-3 shows the output of this command.

Example 7-3 **show ip eigrp topology** *Output*

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for process 100
Codes:P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status
P 140.100.56.0 255.255.255.0, 2 successors, FD is 0
via 140.100.32.22 (46251776/46226176), Ethernet0
via 140.100.48.22 (46251776/46226176), Ethernet1
via 140.100.32.31 (46277376/46251776), Ethernet0
P 140.100.48.0 255.255.255.0, 1 successors, FD is 307200
via Connected, Ethernet1
via 140.100.48.22 (307200/281600), Ethernet1
140.100.32.22 (307200/281600), Ethernet0
via 140.100.32.31 (332800/307200), Ethernet0
```

Table 7-6 explains the meaning of the important fields in Example 7-3.

Table 7-6 *Explanation of the* **show ip eigrp topology** *Command Results*

Field	Explanation
P	Passive—The router has not received any EIGRP input from a neighbor, and the network is assumed to be stable.
A	Active—When a route or successor is down, the router attempts to find an alternative path. After local computation, the router realizes that it must query the neighbor to see whether it can find a feasible successor or path.
U	Update—A value in this field identifies that the router has sent an update packet to a neighbor.
Q	Query—A value in this field identifies that the router has sent a query packet to a neighbor.
R	Reply—A value here shows that the router has sent a reply to the neighbor.
r	This is used in conjunction with the query counter; the router has sent out a query and is awaiting a reply.
140.100.48.0	This is the destination IP network number.
255.255.255.0	This is the destination subnet mask.
Successors	These are the number of routes or the next logical hop. The number stated here is the same as the number of routes in the routing table.
FD	Feasible distance—This is the metric or cost to the destination from the router.
Replies	These are the number of replies that the router is still waiting for from this neighbor. This is relevant only when the route is in an active state.
State	This is the EIGRP state of the route. It can be the number 0, 1, 2, or 3. This is relevant when the destination is active.
Via	This is the address of the next logical hop, or the neighbor that told the router about this route. The first *N* of these entries are the current successors. The remaining entries on the list are feasible successors.
(46251776/46226176)	The first number is the EIGRP metric that represents the feasible distance, or the cost to the destination. The number after the slash is the EIGRP metric that the peer advertised, or the advertised distance.
Ethernet0	This is the interface through which the EIGRP packets were received and, therefore, the outgoing interface.

The show ip eigrp traffic Command

The command shows the EIGRP traffic received and generated by the router. The following is the command syntax:

```
show ip eigrp traffic [autonomous-system-number]
```

Example 7-4 shows the output of this command.

Example 7-4 **show ip eigrp traffic** *Output*

```
Router# show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 100
Hellos sent/received: 218/205
Updates sent/received: 7/23
Queries sent/received: 2/0
Replies sent/received: 0/2
Acks sent/received: 21/14
```

Table 7-7 explains the meaning of the important fields in Example 7-4.

Table 7-7 *Explanation of the* **show ip eigrp traffic** *Command Output*

Field	Explanation
process 100	The autonomous system number, used to identify routers from whom to accept routing updates
Hellos sent/received	Number of hello packets sent and received by the router
Updates sent/received	Number of update packets sent and received by the router
Queries sent/received	Number of query packets sent and received by the router
Replies sent/received	Number of reply packets sent and received by the router
Acks sent/received	Number of acknowledgment packets sent and received by the router

NOTE The **show ip route eigrp** command is also an extremely useful command. In fact, the **show ip route** command is one of the primary troubleshooting tools available to the network administrator, especially in conjunction with the **show ip protocols** command. This command shows the configuration of the routing protocols on the system and is an immediate way of spotting conflicts and misconfiguration. Both of these commands are dealt with extensively in Chapter 5, in the section, "Checking the Configuration of OSPF on a Single Router."

The ability to interpret these screens in conjunction with the physical and logical topology diagrams of your organization will ensure your understanding of the operation of EIGRP.

The debug Commands

An excellent although dangerous tool in troubleshooting and monitoring the network is the **debug** command. Care should be exercised in the use of this command because it can be very greedy in terms of the resources that it consumes. It should be used only for a specific option and a finite time.

The options available for monitoring EIGRP are covered in Table 7-8.

Table 7-8 **debug** *Command Options for EIGRP*

Command Option	Description
debug eigrp packet	Shows the packets sent and received by the router. The packet types to be monitored can be selected. Up to 11 types are available.
debug eigrp neighbors	Shows the hello packets sent and received by the router and the neighbors discovered by this process.
debug ip eigrp route	Is the default if the command **debug ip eigrp** is issued. Shows dynamic changes made to the routing table.
debug ip eigrp summary	Shows a summary of the EIGRP activity, including neighbors, distance, filtering, and redistribution.
show eigrp events	Shows the types of packets sent and received and statistics on routing decisions.

Conclusion

EIGRP is an IP routing protocol that attempts to solve many of the problems experienced by standards-based solutions. As a proprietary protocol, it has the freedom to create a very specific product that works well with the technology that the company produces. After a troubled childhood, EIGRP has proved itself an excellent solution for large corporations that need a routing protocol that will scale. With the use of redistribution, which will be dealt with in a future chapter, it can be integrated into a multivendor network. The functionality of using EIGRP as the routing protocol for desktop networks, such as AppleTalk or IPX, has diminished in importance as IP has risen in popularity as the protocol of choice.

Foundation Summary

The "Foundation Summary" is a collection of quick reference information that provides a convenient review of many key concepts in this chapter. For those of you who already feel comfortable with the topics in this chapter, this summary will help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final preparations before the exam, these tables and figures will be a convenient way to review the day before the exam.

Table 7-9 summarizes the EIGRP packet types sent between neighbors.

Table 7-9 *Summary of Packet Types*

Packet Type	Address	Reliable	Unreliable	Purpose
Hello	Multicast		X	To find and maintain neighbors for the neighbor table. The packet has a 0 in the Acknowledgment field.
ACK	Unicast	X		A hello packet with no data. It has a positive number in the Acknowledgment field.
Update	Unicast and multicast (Reply to a single router is unicast, but a change in topology table is multicast.)	X		Route information sent to affected routers.
Query	Multicast	X		A part of the DUAL algorithm. Queries are sent out when a route in the topology table goes down and there is no FS.

NOTE Any packet sent as a reliable multicast will be sent as a unicast if the neighbor does not acknowledge the packet. The packet will be retransmitted up to 16 times. This will speed up convergence and is an attempt to prevent the route being SIA. For this reason, some documentation will state that queries and hellos are sent both multicast and unicast. Because unicasts in this situation are used as a backup in case of failure, the answer in the exam would be multicast.

Table 7-10 summarizes the commands covered in this chapter.

Table 7-10 *Summary of Commands*

Command	Function
router eigrp *autonomous system number*	Starts the EIGRP processes on the router with the specified autonomous system number.
network *network number*	Shows the networks to be advertised.
no auto-summary	Given a hierarchical addressing design, disables the automatic summarization to the Internet NIC network address.
ip summary address eigrp *autonomous system number address mask*	Enables you to manually summarize the networks, having disabled automatic summarization.
bandwidth *speed of line*	Is issued at the interface level and is a logical construct to manually determine the real bandwidth. This command is used mainly on serial lines. Bandwidth will influence some routing decisions and dial-on-demand implementations.
ip bandwidth-percent eigrp *autonomous-system-number* [*percent*]	Enables you to change the bandwidth percentage. EIGRP by default will only take up to 50 percent of bandwidth.
variance *multiplier number*	Allows unequal paths to load-balance. Paths included in the equation will send a proportional amount of traffic across the unequal links.
ipx router eigrp *autonomous system number*	Configures EIGRP for IPX.
ipx sap-incremental eigrp *autonomous system number*	States to EIGRP that incremental updates should be used. By default, the process will send periodic updates out LAN interfaces and incremental updates through WAN interfaces. If an FDDI ring were used as a backbone, it would be advantageous to use incremental updates if all the devices on the ring were Cisco systems.
show ip eigrp neighbors	Displays information drawn from the neighbor table.
show ip eigrp topology	Displays information drawn from the topology table.
show ip eigrp traffic	Shows the EIGRP traffic passing through the router.

Chapter Glossary

This glossary provides an official Cisco definition for key words and terms introduced in this chapter. I have supplied my own definition for terms that the Cisco glossary does not contain. The words listed here are identified in the text by italics. A complete glossary, including all the chapter terms and additional terms, can be found in Appendix C, "Glossary."

ACK—A hello packet with no data that is an acknowledgment of packets sent reliably.

active—Route state in which when a network change is seen, but on interrogation of the topology table, there is no FC. The router queries its neighbors for alternative routes.

advertised distance (AD)—The cost of the path to the remote network from the neighbor (the metric from the next-hop router).

Diffusing Update Algorithm (DUAL)—An algorithm performed on the topology table to converge the network. It is based on a router detecting a network change within a finite time, with the change being sent reliably and in sequence. Because the algorithm is calculated simultaneously, in order and within a finite time frame on all effected routers, it ensures a loop-free network.

feasible condition (FC)—When a neighbor reports a path (AD) that is lower than the router's FD to a network, the neighbor's (next-hop router's) path has a lower metric than the router's path.

feasible distance (FD)—The lowest-cost distance (metric) to a remote network.

feasible successor (FS)—The neighbor reporting the AD that is lower than the router's FD becomes the feasible successor. This is the next-hop router that meets the FC.

hello—Used to find and maintain neighbors in the topology table. They are sent periodically and are sent reliably.

holdtime—Sent in the hello packet. It determines how long the router waits for hellos from a neighbor before declaring it unavailable. This information is held in the neighbor table.

neighbor—A router running EIGRP that is directly connected.

neighbor table—A list of every neighbor, including the IP address, the outgoing interface, the holdtime, the SRTT, and the uptime, or how long since the neighbor was added to the table. The table is built from information on hellos received from adjacent routers (neighbors).

passive—An operational route is passive. If the path is lost, the router examines the topology table to find an FS. If there is an FS, it is placed in the routing table, and the router does not query the others, which would send it into active mode.

query—Message sent from the router when it loses a path to a network. If there is no alternate route (feasible successor), the router will send out queries to neighbors inquiring whether they have a feasible successor. This makes the route state change to active. The queries are sent reliably.

query scoping—Another term for SIA.

Reliable Transport Protocol (RTP)—Requires that the packets be delivered in sequence and be guaranteed.

reply—A response to the query. If a router has no information to send in a reply, it will send queries to all its neighbors. A unicast is sent reliably.

Retransmission Timeout (RTO)—Timer that is calculated in reference to the SRTT. RTO determines how long the router waits for an ACK before retransmitting the packet.

route table—The routing table, or list of available networks and the best paths. A path is moved from the topology table to the routing table when a feasible successor is identified.

Smooth Round Trip Time (SRTT)—The time that the router waits after sending a packet reliably to hear an acknowledgment. This is held in the neighbor table and is used to calculate the RTO.

Stuck in Active (SIA)—State in which a router has sent out network packets and is waiting for ACKs from all its neighbors. The route is active until all the ACKs have been received. If they do not appear after a certain time, the router is Stuck in Active for the route.

successor—The next-hop router that passes the FC. It is chosen from the FSs as having the lowest metric to the remote network.

topology table—Table that contains all the paths advertised by neighbors to all the known networks. This is a list of all the successors, feasible successors, the feasible distance, the advertised distance, and the outgoing interface. DUAL acts on the topology table to determine successors and feasible successors by which to build a routing table.

update—An EIGRP packet containing change information about the network. It is sent reliably. It is sent only when there is a change in the network to affected routers:

- When a neighbor first comes up
- When a neighbor transitions from active to passive for a destination
- When there is a metric change for a destination

Q&A

The following questions test your understanding of the topics covered in this chapter. The final questions in this section repeat of the opening "Do I Know This Already?" questions. These are repeated to enable you to test your progress. After you have answered the questions, find the answers in Appendix A. If you get an answer wrong, review the answer and ensure that you understand the reason for your mistake. If you are confused by the answer, refer to the appropriate text in the chapter to review the concepts.

1 If a router does not have a feasible successor, what action will it take?

2 When does EIGRP need to be manually redistributed into another EIGRP process?

3 Which timers are tracked in the neighbor table?

4 What is the difference between an update and a query?

5 When does EIGRP recalculate the topology table?

6 EIGRP has a default limit set on the amount of bandwidth that it can use for EIGRP packets. What is the default percentage limit?

7 State two rules for designing a scalable EIGRP network.

8 What is the preferred configuration for a hybrid multipoint NBMA network when one VC has a CIR of 56 kbps and the other five VCs each have a CIR of 256 kbps?

9 With four Frame Relay circuits in a multipoint solution and a bandwidth configuration of 224, what is the allocation per circuit, and where would the **bandwidth** command be configured?

10 Explain the purpose of the command **no auto-summary**.

11 Explain the meaning of the command **ip bandwidth-percent eigrp 63 100.**

12 EIGRP may be used to send information about which three routing protocols?

13 Which EIGRP packets are sent reliably?

14 In what instances will EIGRP automatically redistribute?

15 How long is the holdtime, by default?

16 What is an EIGRP topology table, and what does it contain?

17 What is the advertised distance in EIGRP, and how is it distinguished from the feasible distance?

18 What EIGRP algorithm is run to create entries for the routing table?

19 When does EIGRP place a network in active mode?

20 By default, EIGRP summarizes at which boundary?

21 What is Stuck in Active?

22 What is the **variance** command used for?

23 State two factors that influence EIGRP scalability.

24 What command is used to display which routes are in passive or active mode?

25 What command is used in EIGRP to perform manual summarization?

26 For Frame Relay, when would you configure the physical interface (as opposed to a subinterface) with the **bandwidth** command?

27 Which command is used to display all types of EIGRP packets that are both received and sent by a router?

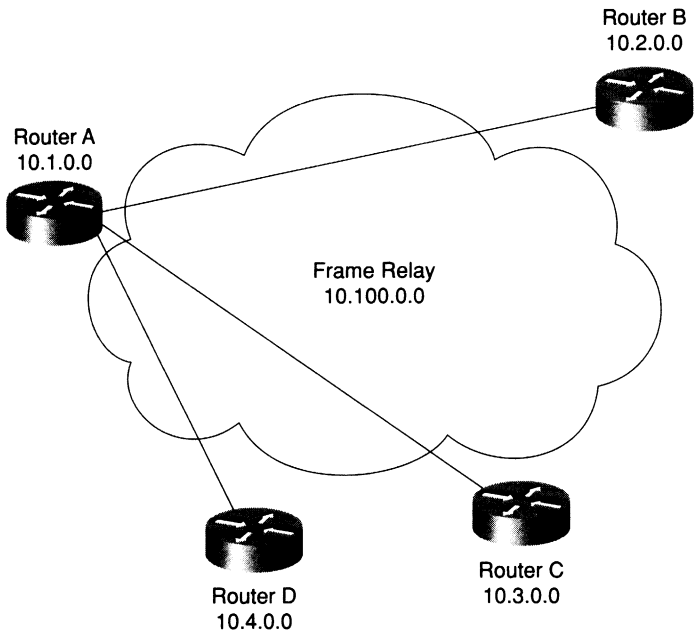
Scenarios

The following scenarios and questions are designed to draw together the content of the chapter and to exercise your understanding of the concepts. There is not necessarily a right answer. The thought process and practice in manipulating the concepts are the goals of this section. The answers to the scenario questions are found at the end of this chapter. The information used in these scenarios was adapted from the Cisco web page, "Cisco Configuration Guidelines."

Scenario 7-1

The multinational company Gargantuan, Inc., from the introduction of this chapter, has had a consultant completely readdress the company. The company has used the private network 10.0.0.0 and has created a very hierarchical addressing structure. Refer to Figure 7-12 to see this addressing scheme.

Figure 7-12 *Diagram for Scenario 7-1*



The addressing of the network was a major project, with all the necessary pitfalls that attend such a major exercise. The network is now stable, and it is time to solve the problems that are being experienced in timeouts and network crashes.

The consultant assured the company that the resolution to the delays was the addressing scheme, but although the network is easier to manage, there has been no change in the congestion on the network. In addition, EIGRP appears to be losing routes from its routing tables, which is adding to the problem.

The consultant was correct: The network needed to be readdressed to allow EIGRP to function effectively. Unfortunately, the company did not read the report carefully and missed the other part of the solution.

1 What needs to be done in addition to solve the problems caused by EIGRP? Give the configuration commands necessary to activate this solution on Router A.

   The WAN is a Frame Relay cloud, and Router A is the hub in the hub-and-spoke configuration. Each VC is 56 kbps.

2 Give the commands to configure Router A for EIGRP over this NBMA cloud.

3 Give the commands to configure Router B for EIGRP over this NBMA cloud.

Scenario 7-2

Given the configuration of EIGRP in Example 7-5, perform the tasks and answer the questions listed. The WAN has light user traffic and is a hub-and-spoke configuration, as shown in Figure 7-13.

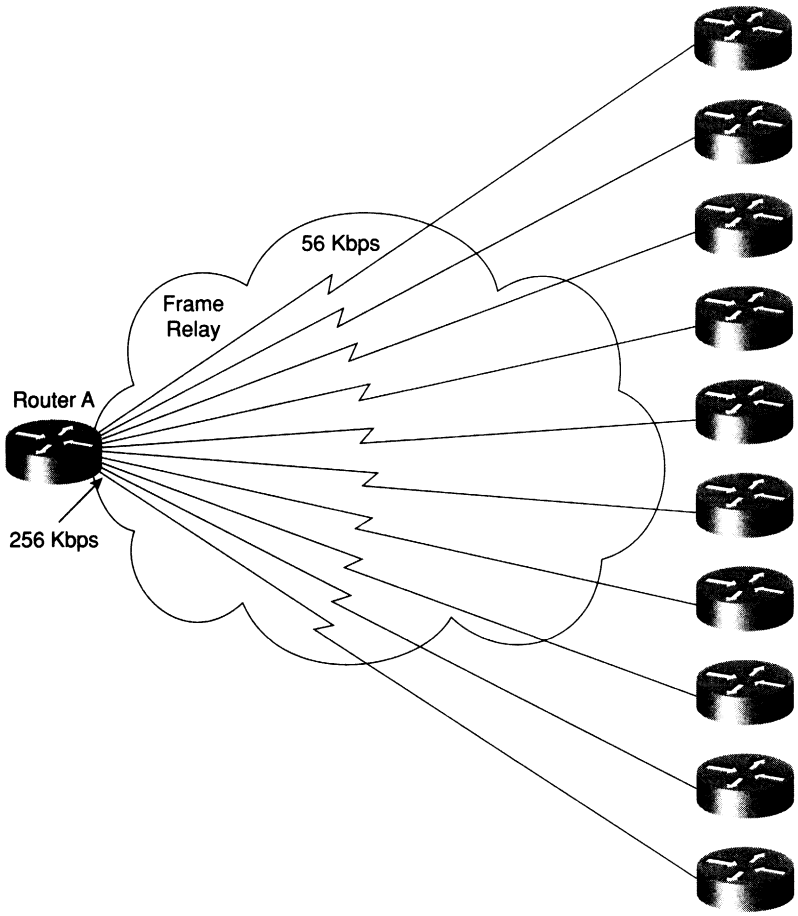
Example 7-5 *Scenario 7-2 Configuration*

```
interface Serial 0
   encapsulation frame-relay

   interface Serial 0.1 point-to-point
   bandwidth 25
   ip bandwidth-percent eigrp 123 90

   interface Serial 0.2 point-to-point
   bandwidth 25
   ip bandwidth-percent eigrp 123 90

        ...
```

The 256 kbps access line to the hub has 56 kbps access lines to each of 10 spoke sites. Each link has a Frame Relay CIR of 56 kbps. The access line to each router reflects the CIR. The access line to the hub router, Router A, is 256 kbps, but the CIR of the hub is the same as its access line.

From a Frame Relay perspective, it is said that a circuit is oversubscribed when the sum of CIRs of the remote circuits is higher than the CIR of the hub location. With 10 links, each with a CIR of 56 kbps, this circuit is clearly oversubscribed.

Figure 7-13 *Diagram for Scenario 7-2*



1 How much bandwidth has each circuit been allocated? Why was this value chosen by the administrator?

2 What bandwidth utilization is available to EIGRP? Why was this value chosen by the administrator?

3 If Router A died, what would the effect be on the network?

4 Is summarization possible only on the routers entering the WAN cloud, or is it possible on the networks not shown in the figure, but on the other side of the routers? Give reasons for your answers.

Scenario Answers

The answers are in **bold**. The answers provided in this section are not necessarily the only possible answers to the questions. The questions are designed to test your knowledge and to give practical exercise in certain key areas. This section is intended to test and exercise skills and concepts detailed in the body of this chapter.

If your answer is different, ask yourself whether it follows the tenets explained in the answers provided. Your answer is correct not if it matches the solution provided in the book, but rather if it has included the principles of design laid out in the chapter.

In this way, the testing provided in these scenarios is deeper: It examines not only your knowledge, but also your understanding and ability to apply that knowledge to problems.

If you do not get the correct answer, refer back to the text and review the subject tested. Be certain to also review your notes on the question to ensure that you understand the principles of the subject.

Scenario 7-1 Answers

1 What needs to be done in addition to solve the problems caused by EIGRP? Give the configuration commands necessary to activate this solution on Router A.

The WAN is a Frame Relay cloud, and Router A is the hub in the hub-and-spoke configuration. Each VC is 56 kbps.

The other solution that the consultant suggested was to perform summarization to limit the query range of the routers. This would prevent the routes in the topology table being SIA, which seriously affects the performance of the network.

The commands required are as follows:

```
router(config)# router eigrp 63
router(config)# no auto-summary
router(config)# network 10.0.0.0
router(config)# int s0
router(config-if)# ip summary-address 10.1.0.0 255.255.0.0
```

2 Give the commands to configure Router A for EIGRP over this NBMA cloud.

The configuration on Router A is as follows:

```
router(config)# serial 0
router(config-if)# frame relay encapsulation
router(config-if)# bandwidth 178
```

3 Give the commands to configure Router B for EIGRP over this NBMA cloud.

The configuration on Router B is as follows:

```
router(config)# serial 0
router(config-if)# frame relay encapsulation
router(config-if)# bandwidth 56
```

Scenario 7-2 Answers

1 How much bandwidth has each circuit been allocated? Why was this value chosen by the administrator?

Because a maximum of 256 kbps is available, you cannot allow any individual PVC to handle more than 25 kbps (256/10). Note that EIGRP will not use more than 22.5 kbps (90 percent of 25 kbps) on this interface, even though its capacity is 56 kbps. This configuration will not affect user data capacity, which will still be able to use the entire 56 kbps.

2 What bandwidth utilization is available to EIGRP? Why was this value chosen by the administrator?

Because this data rate is low, and because you don't expect very much user data traffic, you can allow EIGRP to use up to 90 percent of the bandwidth.

3 If Router A died, what would the effect be on the network?

If Router A died, there would be no communication between the routers in the WAN because Router A is the hub. Each site would function, but they all would be isolated from each other. The neighbor tables would fail to hear the hellos from the other routers connecting to the WAN and would time out all routes that they had heard from these routers. The topology table would be updated, and the routers would send updates to all their other neighbors.

4 Is summarization possible only on the routers entering the WAN cloud, or is it possible on the networks not shown in the figure, but on the other side of the routers? Give reasons for your answers.

Summarization is possible on all interfaces in EIGRP, as long as the addressing scheme allows for it to be implemented. This is one of the major advantages of EIGRP over OSPF. OSPF can summarize only at Area Boundary Routers (ABRs).

from CCNP Switching Exam Certification Guide

by Tim Boyles and David Hucaby

(1-58720-000-7)

Cisco Press

About the Authors

Tim Boyles is the Director of Network Architecture for @Link Networks, a national CLEC which specializes in broadband data and communications solutions for small- and medium-sized businesses. Prior to that he worked as a Senior Consultant at Lucent Networkcare, formerly known as INS, where he was responsible for the design and implementation of large switch-based networks as well as multiple service provider projects. Tim has been in the networking business for 16 years with multiple vendor certifications, including CCNP. He holds an engineering undergraduate degree from the University of Missouri-Rolla and an MBA from California State University. Tim is a co-author of the *CLSC Exam Certification Guide.*

David Hucaby, CCIE #4594, is a Lead Network Engineer for the University of Kentucky, where he designs, implements, and maintains campus networks using Cisco products. Prior to his current position, David was a senior network consultant, where he provided design and implementation consulting, focusing on Cisco-based VPN and IP telephony solutions. David has a B.S. and M.S. in Electrical Engineering from the University of Kentucky.

Contents at a Glance

Bold chapters are elements included in this folio.

This chapter covers the following topics that you will need to master for the CCNP Switching Exam:

- **Overview of Multilayer Switching**—This section outlines an overview of Multilayer Switching (MLS). Also described are the components that make up MLS and the concepts of caching and advertisements.
- **Configuring Multilayer Switching**—This sections deals with how to configure Multilayer Switching on the various network devices that make up MLS.
- **Flow Masks**—This section discusses the application of flow masks, including input and output lists.
- **Configuring the Multilayer Switching Switch Engine**—This section discusses the configuration of the Switch Engine in the role of Multilayer Switching.

CHAPTER 8

Multilayer Switching

Switching technologies have matured over the years and now are a standard part of the campus network. Switching has solved a couple of problems, namely a lack of bandwidth and the inability to have disparate physical groups logically connected. Recently we've taken switching to a higher level, incorporating a routing function within the switch itself. Add some new software that allows true Layer 3 switching, and you have a recipe for success in the campus network. The performance levels are unprecedented and the ability to scale is quite different than even a few years ago. The Internet is quickly driving this industry as web server farms and their associated switching fabrics are popping up around the world.

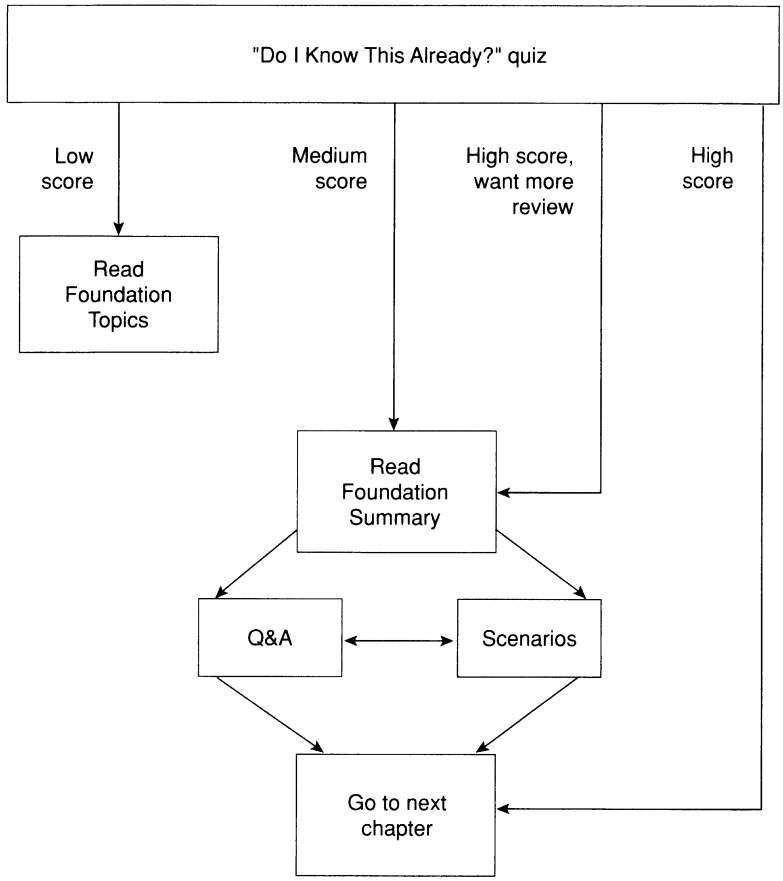
CCNP's are expected to be able to understand what multilayer switching can do for a campus network.

How to Best Use This Chapter

By taking the following steps, you can make better use of your study time:

- Keep your notes and answers for all your work with this book in one place for easy reference.
- Take the "Do I Know This Already?" quiz and write down your answers. Studies show retention is significantly increased through writing facts and concepts down, even if you never look at the information again.
- Use the diagram in Figure 8-1 to guide you to the next step.

Figure 8-1 *How To Use This Chapter*



"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide what parts of this chapter to use. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The ten-question quiz helps you make good choices of how to spend your limited study time. The quiz is sectioned into four areas that correspond to the four major headings in the Foundation Topics section of the chapter. Use the scoresheet in Table 8-1 to record your score.

Table 8-1 *Scoresheet for Quiz*

Quizlet Number	Foundation Topics Section Covering These Questions	Questions	Score
1	Overview of Multilayer Switching	1–3	
2	Configuring Multilayer Switching	4–6	
3	Flow Masks	7–8	
4	Configuring the MLS-SE	9–10	
All questions		1–10	

1 What devices make up the basis for Layer 3 switching as it relates in a Cisco environment?

2 What device is the definition of a Multilayer Switching Switch Engine (MLS-SE)?

3 What devices can be used as a Multilayer Switch Route Processor (MLS-RP)?

4 What is the command for enabling MLS on an RP?

5 What two things are required to make an interface on an RP MLS-enabled?

6 What command is used to verify the MLS configuration for an MLS-RP ?

7 What are the three types of flow masks modes supported on a MLS-SE?

8 What is the command to add an input access list to a MLS flow?

9 When using an external RP to a switch, is this configured automatically or manually?

10 What is the command to enable multilayer switching for a Catalyst switch?

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections," on page 477. The suggested choices for your next step are as follows:

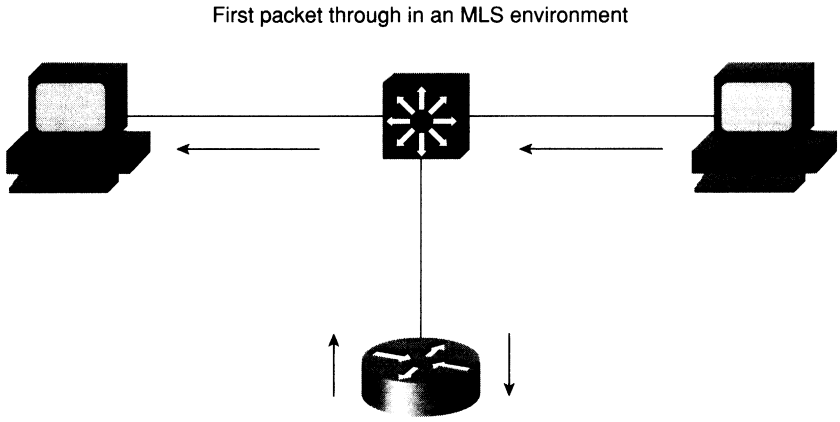
- **6 or fewer overall score**—Read the chapter. This includes the "Foundation Topics", the "Foundation Summary", Q&A, and scenarios at the end of the chapter.
- **7–8 overall score**—Begin with the "Foundation Summary" and then follow with the Q&A and scenarios at the end of the chapter.
- **9 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary", and then go to the Q&A and scenarios at the end of the chapter. Otherwise, move to the next chapter.

Foundation Topics

Overview of Multilayer Switching

Catalyst switches are the basis for Layer 3 switching in the Cisco environment. Multilayer Switching (MLS) performs IP data (also IPX and IP multicast) packet flows at a much higher level of performance than traditional routing. This preserves the CPU of an upstream router without compromising functionality. Figure 8-2 shows that the first packet through enters and exits the router illustrated. Subsequent packets would be switched.

Figure 8-2 *Multilayer Switching Flow: First Packet Through*



Strictly defined, a flow is a specific conversation, consisting of multiple packets, between a network source and destination within a specific time sequence. Let's take a user that is pulling down a web page from a specific web server. This example would be one flow. The same user could be performing a File Transfer Protocol (FTP) file transfer at the same time from an FTP server. This example would be a completely different flow. Two different applications—two different protocols—two different flows; however, only one host is performing two flows. In terms of flows, there is no distinction between unicasts or multicasts.

MLS was conceived in an effort to increase the performance of a router by combining the functionality in hardware with a switch. The frame forwarding and the rewrite function is moved to hardware and then Layer 3 switching takes over the task formerly done by the router.

MLS should not be confused with NetFlow switching supported by Cisco routers. MLS uses the Route Switch Module (RSM), a directly attached external router, and the engine. With MLS,

you are not required to use NetFlow switching on the RSM or directly attached external router; any switching path on the RSM or directly attached external router will work.

MLS can be implemented by using a Layer 3 switch or an external router topology. The Layer 3 switch contains an RSM and the NetFlow Feature Card (NFFC). MLS requires the following software and hardware:

- Catalyst 2926G, 5000, or 6000 series switch with Supervisor Engine software Release 4.1(1) or later.
- Cisco IOS Release 11.3(2)WA4(4) or later.
- Supervisor Engine III or III F with the NFFC II, or Supervisor Engine II G or III G.
- Route Switch Feature Card (RSFC).
- Multilayer Switch Feature Card (MSFC).

MLS is also supported on the following software and hardware:

- Catalyst 5000 series switch with Supervisor Engine software Release 4.1(1) or later.
- Cisco IOS Release 12.0W5 or later.
- Supervisor Engine IIG or IIIG with an RSFC daughter card.

You can also implement MLS with an external router and Catalyst switch combination. The following equipment is necessary when implementing MLS with an external router and Catalyst switch combination:

- Catalyst 2926G, 5000, or 6000 series switch with Supervisor Engine software Release 4.1(1) or later.
- Supervisor Engine III or III F with the NFFC II, or Supervisor Engine II G or III G.
- Cisco high-end routers, such as Cisco 7500, 7200, 4500, 4700, or 8500 series.
- Cisco IOS Release 11.3(2)WA4(4) or later.

The connection between the external router and the switch can be multiple Ethernet links or Fast Ethernet with the Inter-Switch Link (ISL), 802.1Q, or ATM LANE.

Multilayer Switching Components

The Cisco MLS implementation includes the following components:

- **Multilayer Switching Switch Engine (MLS-SE)**—The switching entity that handles the function of moving and rewriting the packets. The MLS-SE is an NFFC residing on a Supervisor Engine III card in a Catalyst switch. It can also be a Supervisor I and the PFC on the 6000 series.

- **Multilayer Switching Route Processor (MLS-RP)**—An RSM, RSFC, MSFC, or an externally connected Cisco 7500, 7200, 4500, 4700, or 8500 series router with software that supports multilayer switching. The MLS-RP sends MLS configuration information and updates, such as the router Media Access Control (MAC) address, virtual LAN (VLAN) number flow mask, and routing and access list changes.
- **Multilayer Switching Protocol (MLSP)**—This protocol operates between the MLS-SE and MLS-RP to enable multilayer switching. MLSP is the method in which the RSM or router advertises routing changes and the VLANs or MAC addresses of the interfaces that are participating in MLS.

MLS-RP Advertisements

As soon as an MLS-RP is enabled in the campus network, MLS-RP advertisements begin. The MLS-RP sends out multicast Hello messages every 15 seconds to all switches in the network. The advertisement message consists of the following:

- The MAC addresses used by the MLS-RP on its interfaces that are participating in MLS.
- Access list information.
- Additions and deletions of routes.

MLSP uses the Cisco Group Management Protocol (CGMP) multicast address as the destination address of the Hello message. This address ensures interoperability with the Cisco switches in the network. Although this address is the same as that used by CGMP, the message contains a different protocol type so the switch can distinguish these messages from other multicast packets.

Hello Messages

All switches in the network receive the Hello message. Only Layer 3 switches actually process the message. Any switches that are not Layer 3 capable simply pass the frames through to any downstream switches.

When an MLS-SE receives the frame, the device extracts all the MAC addresses received in the frame, along with the associated interface or VLAN ID for that address. The MLS-SE records the addresses of the MLS-RPs in the MLS-SE content-addressable memory (CAM) table.

XTAGs

XTAGs are assigned by the MLS-SE to each and every MLS-RP attached to a switch. The XTAG is a one-byte value attached to the MAC address of each attached MLS-RP. These values are instrumental in differentiating between MLS-RPs when there are more than one MLS-RP available.

The XTAG is useful for deleting a specific set of Layer 3 entries from the Layer 3 table when an MLS-RP fails or exits the network.

MLS Caching

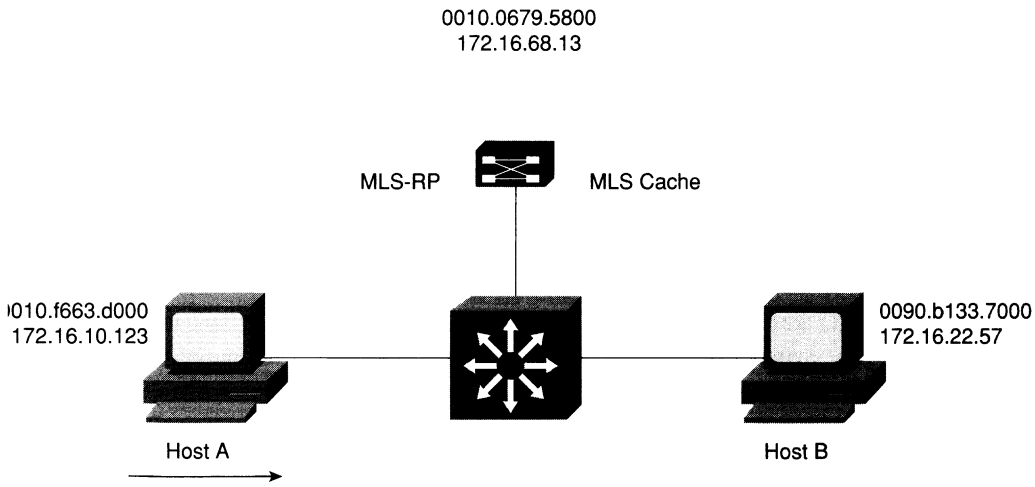
MLS caching is a process that occurs based on individual flows. In this section, we will walk through the process, step by step, in order to gain an intimate knowledge of just what occurs.

The Switching Engine (SE) is involved in the process to maintain the cache for MLS flows. Packets in a flow are compared to the cache.

Cache entries are based on one-way flows. In other words, a flow from Host A to Host B would be one flow and a flow in the reverse direction would be another flow. This action would yield two cache entries.

Here's the part of the equation that yields the payoff. In the event that the cache has an entry that is a match for the packet, the SE switches the packet instead of passing it to the router. If it does not match an entry in the cache, a process occurs that goes on to make an entry in the cache. This concept is illustrated in Figure 8-3.

Figure 8-3 *MLS Cache*



Host A sends a frame to Host B. If there is a match in the MLS cache, the packet would never go to the router but simply be switched using the sequence that follows.

Step 1 The switch receives an incoming frame and looks at the destination MAC address in the frame.

Step 2 The switch recognizes the destination MAC address of the frame as the address of the MLS-RP because the switch initially received this destination MAC address in a Layer 3 Hello message and programmed that destination MAC address in the CAM table.

Step 3 The MLS-SE then checks the MLS cache to determine if an MLS flow is already established for this flow. If the frame is the first in a flow, there will not be an entry in the cache. Because the frame contained a route processor destination address, the switch recognizes the potential for Layer 3 switching for that frame.

Step 4 On the initial packet, the switch does not have all the information for a Layer 3 switch for the frame. The switch, therefore, forwards the frame to the addressed route processor. This process of sending the frame to the addressed route processor creates a "candidate" entry in the MLS cache.

Step 5 The route processor receives the frame and consults the routing table to determine if, in fact, the route processor has knowledge of a route for the destination address.

Step 6 If the route processor finds the destination address in the routing table, the route processor constructs a new Layer 2 header, which now contains the route processor's own MAC address as the source MAC address.

The route processor also enters the MAC address of the destination host or next-hop route processor in the destination MAC address field of the Layer 2 frame.

Step 7 The route processor then forwards the frame back to the MLS-SE.

When the switch receives the frame, the switch knows which port needs to forward the frame, based on the CAM table (displayed in Example 8-1). Moreover, the switch also recognizes the MAC address in the source field and knows that that this destination belongs to the route processor.

Example 8-1 *Displaying the CAM Table*

```
Console> (enable) show cam 00-10-29-8a-4c-00
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
----  -----------------  ---------------------------------------------------
10    00-10-29-8a-4c-00R  9/1                          IP
51    00-10-29-8a-4c-00R  9/1                          IP
52    00-10-29-8a-4c-00R  9/1                          IP
53    00-10-29-8a-4c-00#  9/1                          IP
54    00-10-29-8a-4c-00#  9/1                          IP
Total Matching CAM Entries Displayed = 5
Console> (enable)
```

This recognition triggers the process of checking the MLS cache to see if there is an entry for this route processor. The switch compares the XTAGs for both the candidate entry in the MLS cache and the returned frame. If the two XTAGs match, the frame came from the same route processor for the same flow.

The switch records the information from the returned frame in the MLS cache. The switch forwards the frame out the appropriate port using the destination MAC address. This second frame becomes the "enable" entry in MLS cache and the partial entry for that flow is completed.

Remembering that the MLS-SE must see both sides of the flow going from the source to the destination in order to perform Layer 3 switching is important. In other words, you can't do Layer 3 switching by just knowing the source or destination.

When the switch receives subsequent packets in the flow, the switch recognizes that the frames contain the MAC address of the route processor. The switch checks the MLS cache and finds the entry matching the flow in question.

The switch rewrites the Layer 2 frame header, changing the destination MAC address to the MAC address of Host B and the source MAC address to the MAC address of the MLS-RP. The Layer 3 IP addresses remain the same, but the IP header Time to Live (TTL) is decremented and the checksum is recomputed. The MLS-SE rewrites the switched Layer 3 packets so that they appear to have been routed by a route processor.

The switch rewrites the frame to look exactly as if the route processor processed the frame. The final destination sees the frame exactly as if the router processed the frame.

After the MLS-SE performs the packet rewrite, the switch forwards the rewritten frame to the destination MAC address.

The state and identity of the flow are maintained while traffic is active; when traffic for a flow ceases, the entry ages out. Partial, or candidate, entries will remain in the cache for five seconds with no enabled entry before timing out. Cache entries that are complete, where the switch captures both the candidate and the enabling packet, will remain in the cache as long as packets in that flow are detected.

Disabling MLS

Actually the title of this section should read, "What not to do if you want your MLS to keep running." Believe it or not, there are a few commands that, if entered, will have the undesirable effect of disabling MLS.

The basic guideline to follow is that if you enter any command that forces the router to examine the packet, MLS will be disabled. That includes a whole host of commands, but I thought I'd list a few of the most common here:

- ip tcp header-compression
- no ip routing
- ip security

Configuring Multilayer Switching

The basic tasks for configuring multilayer switching include the following:

1. Enabling MLSP.
2. Assigning a VLAN ID to a route processor interface.
3. Adding the interfaces to the same VLAN Trunking Protocol (VTP) domain as the switch.
4. Enabling MLS on every interface.
5. Configuring the MLS Management interface.
6. Verifying MLS on an MLS-RP.

Before you can configure MLS for a specific VLAN or interface, you must globally enable the MLSP that operates between the route processor and the switch.

To enable MLSP on the route processor, enter the following command in global configuration mode:

```
Router(config)#mls rp ip
```

Example 8-2 states that the MLS-RP is configured to multilayer switch routed IP packets using MLSP. As of 12.0, MLS also routes Internetwork Packet Exchange (IPX) packets.

Example 8-2 *Determining the MLS-RP Is Configured*

```
Router#show run
Building configuration...
Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
mls rp ip
!
```

To disable MLS on the route processor/RSM, enter the **no mls rp ip** command in global configuration mode.

In Cisco's MLS implementation, Layer 3 switches IP IPX, and IP multicast packets. Any other packets are routed as in a non-Layer 3 switched network.

MLS is interVLAN routing. Multilayer switches make forwarding decisions based upon which ports are configured for which VLANs. Internal route processors and ISL-configured links inherently use VLAN IDs to identify interfaces. External route processor interfaces have

knowledge regarding subnets but not VLANs. Therefore, MLS requires that each external route processor interface have a VLAN ID assigned to it.

To assign a VLAN ID to a route processor interface, enter the following commands in interface configuration mode:

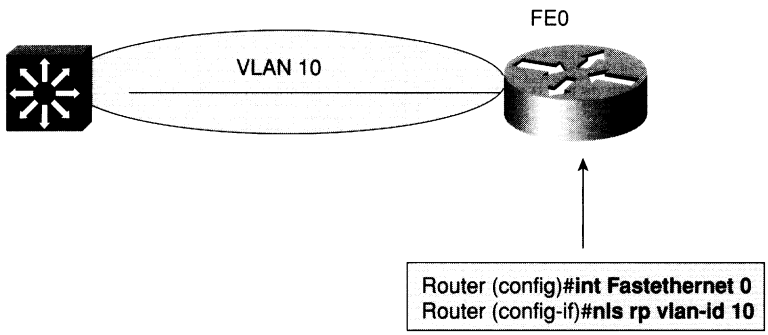
```
Router (config)#interface interface number
Router (config-if)#mls rp vlan-id vlan-id-num
```

where *vlan-id-num* represents the VLAN assigned to this interface.

To remove an interface from a VLAN, enter the **no mls rp vlan-id** *vlan-id-num* command.

Removing the VLAN ID from an interface disables MLS for that interface. Figure 8-4 demonstrates how to use these commands to assign a VLAN ID to a route processor interface.

Figure 8-4 *Assigning a VLAN ID*



After you determine which route processor interfaces will be MLS interfaces, you must add the interfaces to the same VTP domain as the switch. Both the switch and the MLS interfaces must be in the same domain. If the switch is not assigned to a VTP domain, you do not need to perform this task.

To place an external route processor interface in the same VTP domain as the switch, enter the following commands in interface configuration mode:

```
Router(config) interface interface number
Router(config-if)# mls rp vtp-domain domain-name
```

where *domain-name* is the name of the VTP domain in which the switch resides.

For an ISL interface, enter the **mls rp vtp-domain** command only on the primary interface. All subinterfaces that are part of the primary interface inherit the VTP domain of the primary interface.

The running configuration in Example 8-3 states that the VLAN41 interface of the MLS-RP is configured to reside in the Rigel2 VTP domain.

Example 8-3 *Determining the VTP Domain of the MLS-RP VLAN Interface*

```
Router#show run
Building configuration...
(Text deleted)
mls rp ip
!
!
interface Vlan1
 ip address 172.16.1.168 255.255.255.0
!
interface Vlan41
 ip address 172.16.41.168 255.255.255.0
 mls rp vtp-domain Rigel2
```

To remove the MLS interface from a VTP domain, enter the **no mls rp vtp-domain** *domain-name* command.

Displaying VTP Domain Information

Sometimes seeing VTP domain information is useful. The **show mls rp vtp-domain** command allows you to see domain information for a specific VTP domain:

```
Router#show mls rp vtp-domain vtp domain name
```

The display resulting from this command (see Example 8-4) shows a subset of the **show mls rp** command display. The following information is a result of issuing the **show mls rp vtp-domain** command:

- The name of the VTP domain(s) in which the MLS-RP interfaces reside.
- Statistical information for each VTP domain.
- The number of management interfaces defined for the MLS-RP.
- The number of VLANs in this domain configured for MLS.
- The ID of each VLAN configured for this domain MAC address.
- The number of MLS-SEs of which the router or RSM has knowledge of in this domain.
- The MAC address of each switch in this domain.

Example 8-4 *Displaying VTP Domain Information*

```
router# show mls rp vtp-domain WBU

vlan domain name: WBU
   current flow mask: ip-flow
   current sequence number: 80709115
   current/maximum retry count: 0/10
   current domain state: no-change
   current/next global purge: false/false
   current/next purge count: 0/0
   domain uptime: 13:07:36
   keepalive timer expires in 8 seconds
   retry timer not running
   change timer not running
   fcp subblock count = 7

   1 management interface(s) currently defined:
      vlan 1 on Vlan1

   7 mac-vlan(s) configured for multi-layer switching:

      mac 00e0.fefc.6000
         vlan id(s)
         1    10   91   92   93   95   100

   router currently aware of following 1 switch(es):
      switch id 0010.1192.b5ff
```

Enabling MLS

MLS is enabled on a per-interface basis. Just because you put an interface into a particular VTP domain doesn't mean that you've activated MLS. MLS must be enabled on every interface that you desire to participate in Layer 3 switching.

On a router or RSM interface, enter the following command in interface configuration mode in order to enable MLS:

```
Router (config-if)#mls rp ip
```

The running configuration in Example 8-5 shows that the VLAN19 interface of the MLS-RP is enabled to participate in MLS.

To disable MLS on an interface, enter the **no mls rp ip** command.

Example 8-5 *Determining that the MLS-RP VLAN Interface is Enabled for Multilayer Switching*

```
Router#show run
Building configuration...
(Text Deleted)
mls rp ip
!
!
interface Vlan1
 ip address 172.16.1.168 255.255.255.0
!
interface Vlan19
 ip address 172.16.41.168 255.255.255.0
 mls rp vtp-domain san-fran
 mls rp ip
```

VTP Domain Issues

When a route processor resides in a VTP domain other than the domain in which the switch resides, the switch cannot multilayer switch frames for that router. There are several ways in which a route processor and switch can end up in different VTP domains as follows:

- You can purposely place both devices in separate domains.
- You can misname or mistype the VTP domain when configuring either the switch or route processor.
- You can enter the MLS interface command prior to putting the interface in a VTP domain.

Configuring an interface for MLS by assigning the interface to a VTP domain prior to assigning it to a VTP domainplaces that interface in the null domain. When the interface resides in a null domain, it cannot participate in MLS with the switch.

To remove the MLS interface from a null VTP domain, disable MLS on the interface.

MLS Management Interface

When a RSM or router is configured to participate in MLS, the device uses the MLSP to send Hello messages, advertise routing changes, and announce the VLANs or MAC addresses of those interfaces on the devices participating in MLS. One interface on the MLS-RP must be identified as the management interface through which MLSP packets are sent and received. The MLSP management interface can be any MLS interface connected to the switch.

Only one management interface needs to be specified. If no management interface is configured, however, MLSP messages will not be sent.

Multiple interfaces on the same route processor can be configured as a management interface; however, this action increases the management overhead per route processor. Cisco does not recommend this practice.

To identify a management interface on an RSM or router, enter the following command in interface configuration mode:

```
Router(config-if)#mls rp management-interface
```

To disable the management interface, enter the **no mls rp management-interface** command in interface configuration mode.

The running configuration in Example 8-6 states that the VLAN41 interface on the MLS-RP is configured as the management interface.

Example 8-6 *Determining if the MLS-RP VLAN Interface Is Configured as the Management Interface*

```
Router#show run
Building configuration...

(Text Deleted)
mls rp ip
!
!
interface Vlan1
 ip address 172.16.1.168 255.255.255.0
!
interface Vlan41
 ip address 172.16.41.168 255.255.255.0
 mls rp vtp-domain bcmsn
 mls rp management-interface
 mls rp ip
```

Verifying MLS-RP

To verify the MLS configuration for an MLS-RP, enter the following command in privileged EXEC mode:

```
Router#show mls rp
```

The display resulting from this command (see Example 8-7) shows the following information:

- Whether MLS is globally enabled or disabled.
- The MLS ID for this MLS-RP.
- The MLS IP address for this MLS-RP.
- The MLS flow mask.
- The name of the VTP domain(s) in which the MLS-RP interfaces reside.
- Statistical information for each VTP domain.

- The number of management interfaces defined for the MLS-RP.
- The number of VLANs configured for MLS.
- The ID of each VLAN configured for this MAC address.
- The number of MLS-SEs to which the router or RSM is connected.
- The MAC address of each switch.

Example 8-7 *Displaying MLS RP Information*

```
router# show mls rp

multilayer switching is globally enabled
mls id is 00e0.fefc.6000
mls ip address 10.20.26.64
mls flow mask is ip-flow
vlan domain name: WBU
   current flow mask: ip-flow
   current sequence number: 80709115
   current/maximum retry count: 0/10
   current domain state: no-change
   current/next global purge: false/false
   current/next purge count: 0/0
   domain uptime: 13:03:19
   keepalive timer expires in 9 seconds
   retry timer not running
   change timer not running
   fcp subblock count = 7

   1 management interface(s) currently defined:
      vlan 1 on Vlan1

   7 mac-vlan(s) configured for multi-layer switching:

      mac 00e0.fefc.6000
         vlan id(s)
         1    10   91   92   93   95   100

   router currently aware of following 1 switch(es):
      switch id 0010.1192.b5ff
```

Each MLSP-RP is identified to the switch by both the MLS ID and MLS IP address of the route processor. The MLS ID is the MAC address of the route processor. The MLS-RP automatically selects the IP address of one of its interfaces and uses that IP address as its MLS IP address.

The MLS-SE uses the MLS ID as a determining factor for establishing entries in the MLS cache.

This MLS IP address is used in the following situations:

- By the MLS-RP and the MLS-SE when sending MLS statistics to a data collection application.
- In the included MLS route processor list on the switch.

To verify the MLS configuration for a specific interface, enter the following command in privilege EXEC mode:

```
Router#show mls rp interface interface number
```

The display resulting from this command shows the following information:

- Whether MLS is configured on the interface.
- The VTP domain in which the VLAN ID resides.
- Whether this interface is configured as the management interface for the MLS-RP.

If the interface is not configured for MLS, the **show mls rp ip** command displays the following message:

```
Router#show mls rp ip interface Vlan41
mls not configured on Vlan41
```

Flow Masks

The MLS-SE uses flow mask modes to determine how packets are compared to MLS entries in the MLS cache. The flow mask mode is based on the access lists configured on the MLS router interfaces. The MLS-SE learns the flow mask through MLSP messages from each MLS-RP for which the MLS-SE is performing Layer 3 switching.

MLS-SE supports only one flow mask for all MLS-RPs that are serviced by the MLS-SE. If the MLS-SE detects different flow masks from different MLS-RPs for which the MLS-SE is performing Layer 3 switching, the MLS-SE changes its flow mask to the most specific flow mask detected. However, if a more specific flowmask is in effect, a less specific flow mask then is applied.

The MLS-SE supports three flow mask modes as follows:

- **Destination-IP**—The default flow mask mode, Destination-IP represents the least-specific flow mask. The MLS-SE maintains one MLS entry for each destination IP address. All flows to a given destination IP address use this MLS entry. This mode is used if no access lists are configured on any of the MLS router interfaces.
- **Source-Destination-IP**—The MLS-SE maintains one MLS entry for each source and destination IP address pair. All flows between a given source and destination use this MLS entry regardless of the IP protocol ports. This mode is used if a standard access list is on any of the MLS interfaces.

- **IP-Flow**—This mode represents the most specific flow mask. The MLS-SE creates and maintains a separate MLS cache entry for every IP flow. An IP-Flow entry includes the source IP address, destination IP address, protocol, and protocol ports. This mode is used if there is an extended access list on any MLS interface.

When the MLS-SE flow mask changes, the entire MLS cache is purged.

You can set a flow mask on the MLS-SE without applying an access list on the route processor. You use the **set mls flow** command when you want to cache entries on a specific set of criteria to export flow statistics but not to set an access list on an interface. To set the flow mask on the MLS-SE without setting an access list on a route processor interface, enter the following command in privilege mode:

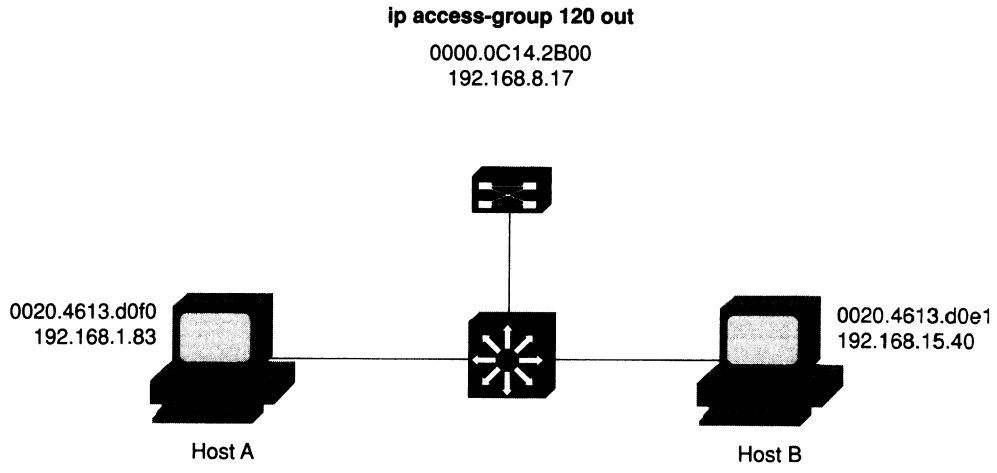
```
set mls flow [destination | destination-source | full].
```

The keywords **destination** means that you are applying the IP-Destination mode, **destination-source** means that you are applying Source-Destination-IP mode, and **full** means that you are applying IP-Flow mode. These different modes were explained earlier.

Output Lists

Figure 8-5 illustrates an output access list applied to the interface. In this case, the MLS-SE learns of this change through the MLSP process and then enforces security for the flow. Enforcement of the access list would purge any entries for flows on that interface from the MLS cache.

Figure 8-5 *Output Access Lists*



Any new flows would then be created based on the restrictions imposed by the access list. The next packet in the flow becomes a candidate packet and the process of establishing a MLS cache entry is initiated.

New entries are placed in the MLS cache once the initial packet in the flow passes the test conditions in the output access control list (ACL).

Using options like **log**, **reflexive**, or **established** forces the router to examine every packet before routing. Under MLS, the router does not examine every packet; therefore, these options are not allowed.

Input Access Lists

As with output access lists, placing an input access list on an MLS-enabled interface purges the MLS cache of all existing flows for that interface.

Because the default behavior for the input access list is to examine and route all incoming packets, however, all subsequent packets in the flow between Hosts A and B are routed.

Most input access lists can be implemented as output access lists to achieve the same effect.

Routers configured with Cisco IOS Release 11.3 or later will not automatically support input access lists on an interface configured for MLS. If an interface is configured with an input access list, all packets for a flow that are destined for that interface go through the router. Even if the router allows that flow, the flow is not Layer 3 switched.

To enable MLS to cooperate with input access lists, enter the following command in global configuration mode:

```
Router(config)#mls rp ip input-acl
```

The running configuration in Example 8-8 states that input ACLs on the MLS-RP are configured to work in a MLS environment.

Example 8-8 *Determining if Input Access Lists on the MLS-RP Can Operate in an MLS Environment*

```
Router#show run
Building configuration...

Current configuration:
!
version 11.3
(Text Deleted)
mls rp nde-address 172.16.31.113
mls rp ip input-acl
mls rp ip
```

To remove support for input access lists in an MLS environment, enter the **no mls rp ip input-acl** command in global configuration mode.

Configuring the MLS-SE

This section deals with topics involved in configuration of the switching engine or MLS-SE. Topics covered include enabling MLS, MLS caching, verifying MLS, external router support, and switch inclusion lists.

MLS is enabled by default on Catalyst series switches that support Layer 3 switching—in other words, if an RSM is on the switch. There are, however, a couple of cases where configuring the switch is necessary. The first is obvious, when the MLS-RP happens to be an external router. Because an external router is not an integral part of the switch, no knowledge of Layer 3 switching exists. The other case is when the aging time of MLS cache entries is different than the default, hence, requiring some configuration to change this parameter.

In the event that a switch has been disabled for Layer 3 switching, enter the following command in privilege EXEC mode on the switch to re-enable it:

```
Switch(enable)#set mls enable
```

The running configuration in Example 8-9 shows the entry that shows the MLS-SE is configured to support MLS.

Example 8-9 *Determining if the MLS-SE Is Configured to Support MLS*

```
Switch(enable)#show config
(Text Deleted)
#mls
set mls enable
```

Enter the **set mls disable** command to disable MLS on the MLS-SE. This command stops the MLS-SE from processing the MLSP messages from the MLS-RP and purges all existing MLS cache entries in the switch.

MLS Caching

Because the MLS cache has a size limitation, MLS entries will be deleted from the cache if certain conditions are met. This deletion, or aging, process takes into effect for the following reasons:

- Candidate entries remain in the cache for five seconds with no enabled entry before timing out.
- An MLS entry is deleted from the cache if a flow for that entry has not been detected for the specified aging time. The default aging time is 256 seconds.
- Other events, such as applying access lists, routing changes, or disabling MLS on the switch, can cause MLS entries to be purged.

The amount of time an MLS entry remains in the cache is user modifiable. To alter the value of the aging time, enter the following command in privileged EXEC mode:

```
Switch(enable)#set mls agingtime agingtime
```

where *agingtime* is the amount of time an entry remains in the cache before the entry is deleted. The range of the aging time value is from 8 to 2032 seconds. The default value is 256 seconds.

The running configuration in Example 8-10 states that entries in which no packets have been detected for a period of six minutes will be deleted from the cache.

Example 8-10 *Configuring Cache Aging*

```
Switch(enable)show config
(Text Deleted)
#mls
set mls enable
set mls agingtime 272
```

The values for *agingtime* are entered in eight-second increments. Any *agingtime* value that is not a multiple of eight seconds is adjusted to the closest one.

Some MLS flows are sporadic or short-lived. An example of a sporadic or short-lived flow would be packets that are sent to or received from a Domain Name System (DNS) or Trivial File Transfer Protocol (TFTP) server. Because the connection may be closed after one request and one reply cycle, that MLS entry in the cache is used only once. However, that MLS entry still consumes valuable cache space until the entry is aged out. Detecting and aging out these entries quickly can save MLS entry space for real data traffic.

To solve the problem of short-lived entries in the cache, a different type of aging mechanism, called fast aging, is available. This type of aging states that if the MLS-SE does not detect a specified number of packets in a certain time period, then that entry is removed from the cache.

To configure the fast aging option, enter the following command in privilege EXEC mode:

```
Switch(enable)# set mls agingtime fast fastagingtime pkt_threshold
```

where *fastagingtime* indicates the amount of time an entry remains in the cache before the entry is deleted. Allowable configuration values are 32, 64, 96, or 128 seconds. The default is 0 seconds.

The *pkt_threshold* argument indicates the number of packets that must be detected within the specified amount of time. Allowable configuration values are 0, 1, 3, 7, 15, 31 or 63 packets. The default is 0 packets.

In the configuration in Example 8-11, we have configured a *fastagingtime* of 96 and a *pkt_threshold* of 15. So for this example, any cache entries in which no more than 15 packets have been detected for a period of 96 seconds will be deleted from the cache.

Example 8-11 *Determining Entries to Be Deleted from the Cache*

```
Switch (enable)show config
(Text Deleted)
#mls
set mls enable
set mls agingtime 272
set mls agingtime fast 96 15
```

Verifying MLS Configurations

To display information about MLS on a MLS-SE, enter the following command in privileged EXEC mode:

```
Switch (enable) show mls
```

The following information is displayed as result of executing the above command (see Example 8-12):

- Status of MLS.
- Aging time, in seconds, for an MLS cache entry.
- Fast aging time, in seconds, and the packet threshold for a flow.
- Flow mask.
- Total packets switched.
- Number of active MLS entries in the cache.
- Whether Netflow data export is enabled and, if so, for which port and host.
- MLS-RP IP address, MAC address, XTAG, and supported VLANs.

Example 8-12 *Displaying Information about MLS on an MLS-SE*

```
Switch (enable) show mls

Multilayer switching enabled
Multilayer switching aging time = 110 seconds
Multilayer switching fast aging time = 64 seconds, packet threshold = 7
Full flow
Total packets switched = 87128
Active shortcuts = 1298
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0

MLS-RP IP        MLS-RP ID     XTAG      MLS-RP MAC-Vlans
---------        ----------    ----      ----------------------
192.168.1.127    0010f6fe12a3  28         00-10-f6-fe-12-a3  1,21-22
```

If you want to display information about a specific MLS-RP, enter the **show mls rp** command and designate the IP address of the target MLS-RP.

where you execute the command does make a difference. You can execute this command on both the MLS-SE and the MLS-RP. In this case, we are talking about the MLS-SE

External Router Support

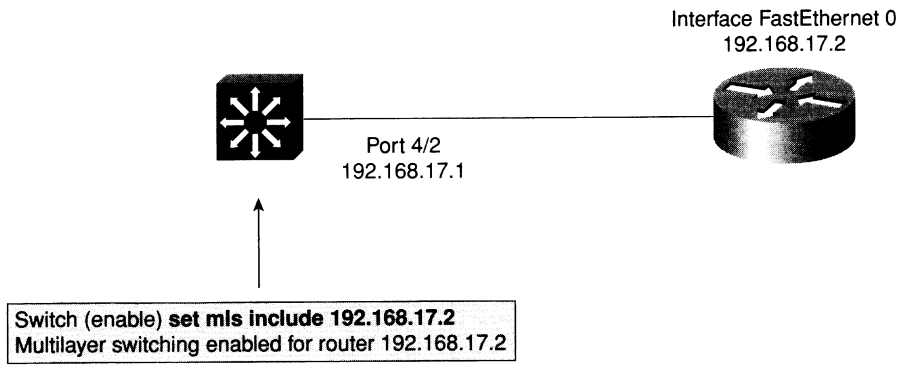
If the switch supports an externally attached MLS-RP, the switch must be manually configured to recognize that MLS-RP. To manually include an external MLS-RP, enter the following command in privilege EXEC mode on the switch:

```
Switch (enable) set mls include ip-addr
```

where *ip-addr* is the MLS IP address of the external router. To determine the IP address of the MLS-RP, enter the **show mls rp** command on the MLS-RP.

Perform this command *only* for external routers. The MLS-SE automatically includes the IP address of co-resident RSMs in the switch inclusion list. When the RSM is physically removed from the switch chassis or MLS is disabled on an RSM, the RSM IP address is removed from the inclusion list. The auto-included RSM cannot be cleared using the **clear mls include** command. Figure 8-6 demonstrates implementing the **set mls include** command to support MLS for external routers.

Figure 8-6 *Including External Routers*



The running configuration in Example 8-13 states that an external MLS-RP with the IP address of 172.16.41.168 has been added to the MLS include list.

To remove the MLS-RP from the switch inclusion list, enter the **clear mls include** command. A single MLS-RP can be removed by entering the IP address of a specific MLS-RP. All externally connected MLS-RPs can be removed from the switch inclusion list by entering the **clear mls include all** command.

Example 8-13 *Including External Routers in Multilayer Switching*

```
Switch (enable)show config
(Text Deleted)
#mls
set mls enable
set mls agingtime 256
set mls agingtime fast 0 0
set mls include 172.16.41.168
```

Switch Inclusion Lists

To display the contents of the switch inclusion list to determine which MLS-RPs are participating in MLS with the MLS-SE, enter the following command in privilege EXEC mode:

```
Switch (enable) show mls include
```

The resulting display returns the IP addresses of *all* MLS-RPs that are participating in MLS with the MLS-SE.

If the IP address of an MLS-RP does not appear in the switch inclusion list, the MLS-SE will not perform Layer 3 switching for the MLS-RP. If the MLS-SE is supposed to be performing Layer 3 switching for a specific router and its IP address is not listed in the inclusion list, check the following:

- Is the router for which you manually entered the MLS IP address external?
- If the router is an RSM, is there an RSM resident and is it functional?
- Is MLS globally enabled on the MLS-RP?

Displaying MLS Cache Entries

To display the MLS cache entries, enter the following command in privilege EXEC mode:

```
Switch (enable) show mls entry.
```

This command might be used as a troubleshooting tool or just to check the status of a particular flow that you're interested in.

This command can be further defined to show MLS cache entries for the parameters defined in Table 8-2.

To remove entries from the MLS cache, enter the **clear mls entry** command in privilege EXEC mode. Table 8-3 lists how to remove MLS cache entries based on given criteria.

Table 8-2 *Displaying Specific MLS Cache Entries*

MLS Cache Entry Based On	Command to Use
Specific destination IP address	**show mls entry destination** *ip-address*
Specific source IP address	**show mls entry source** *ip-address*
Specific MLS_RP ID	**show mls entry rp** *ip-address*
Specific IP flow	**show mls entry flow** *protocol source-port destination-port*

Table 8-3 *Removing MLS Cache Entries*

Remove MLS Cache Entry Based On	Command to Use
Specific source IP address	**clear mls entry source** *ip-address*
Specific destination IP address	**clear mls entry destination** *ip-address*
Specific flow	**clear mls entry flow** *protocol src-port dst-port*

Refer to the "Configuring Multilayer Switching" section of the *Catalyst Series Switch Configuration Guide (4.3)*, available online at www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_3/config/mls.htm#41001 for details on how to format this command for each of the above instances.

Foundation Summary

The Foundation Summary is a collection of tables and figures that provide a convenient review of many key concepts in this chapter. For those of you already comfortable with the topics in this chapter, this summary could help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final prep before the exam, these tables and figures will hopefully be a convenient way to review the day before the exam.

Table 8-4 *Components of Multilayer Switching*

Component	Description
Multilayer Switching Switch Engine (MLS-SE)	The MLS-SE is a NetFlow Feature Card residing on a Supervisor Engine III card in a Catalyst switch. It can also be a Supervisor I and the PFC on the 6000 series.
Multilayer Switching Route Processor (MLS-RP)	An RSM, RSFC, MSFC or an externally connected Cisco 7500, 7200, 4500, 4700, or 8500 series router with software that supports multilayer switching.
Multilayer Switching Protocol (MLSP)	This protocol operates between the MLS-SE and MLS-RP to enable multilayer switching.

Table 8-5 *MLS Router Commands*

Command	Description
access-list *access-list-number*	Creates an access list.
ip access-group *access-list-number*	Assigns an access list to an interface.
mls rp input-acl	Supports the creation of MLS flow entries from interfaces with input ACLs.
mls rp ip	Enables multilayer switching on an MLS-RP and on a specific interface.
mls rp management-interface	Establishes a management interface through which MLSP messages are sent.
mls rp vtp-domain *vtp-domain-name*	Assigns an interface to a VTP domain.
show mls rp	Displays the MLS configuration on the MLS-RP.
show run	Displays the current configuration on the router.

Table 8-6 *MLS Switch Commands*

Command	Description
set mls agingtime *seconds*	Alters the time in which MLS entries are maintained in the MLS cache.
set mls enable	Enables multilayer switching on the MLS-SE.
show mls	Displays the MLS configuration on the MLS-SE.
show mls include	Displays the switch MLS-RP inclusion list.
show mls entry	Displays the MLS cache.
show mls rp	Displays the MLS configuration on the MLS-RP.

Q&A

The questions and scenarios in this book are more difficult than what you should experience on the actual exam. The questions do not attempt to cover more breadth or depth than the exam; however, they are designed to make sure that you know the answer. Rather than allowing you to derive the answer from clues hidden inside the question itself, the questions challenge your understanding and recall of the subject. Questions from the "Do I Know This Already?" quiz from the beginning of the chapter are repeated here to ensure that you have mastered the chapter's topic areas. Hopefully, these questions will help limit the number of exam questions on which you narrow your choices to two options and then guess. If you get an answer wrong, review the appropriate section of this chapter to make sure you understand the reason for your mistake.

The answers to these questions can be found in Appendix A, on page 477.

1 What devices are the basis for Layer 3 switching as it relates in a Cisco environment?

2 What device is the definition of a Multilayer Switch Engine (MLS-SE)?

3 What devices can be used as a Multilayer Switch Route Processor (MLS-RP)?

4 What is the command for enabling MLS on an RP?

5 What two things are required to make an interface on an RP MLS-enabled?

6 What command is used to verify the MLS configuration for an MLS-RP ?

7 What are the three types of flow masks modes supported on a MLS-SE?

8 What is the command to add an input access list to a MLS flow?

9 When using an external RP to a switch, is this configured automatically or manually?

10 What is the command to enable Multilayer Switching for a Catalyst switch?

11 Assuming that MLS is running, what effect does the command **clear ip route** do on an MLS-RP?

12 What three components are required in a Cisco implementation of MLS?

13 Define a Destination-IP flow mask.

14 What is the command to display MLS entries in the cache?

Scenarios

Scenario 8-1

Refer to Figure 8-7, which depicts a simple router and switch setup for this scenario.

Figure 8-7 *Scenario 8-1 Network Setup*

We've decided that we need to support MLS on these two devices due to performance issues.

1. What commands would be necessary to implement MLS on these two devices?
2. Assume we are going to use the Interface VLAN12 on the RP. Also, the domain is called SJC-1. Configure accordingly.
3. Interface VLAN12 is also the management interface. Activate this feature.
4. We need to activate an input access list for VLAN12. Configure this accordingly.
5. On the MLS-SE, we want the MLS cache to timeout after 224 seconds. Configure this on the switch.
6. The RP pictured is to be included and has an IP address of 172.16.48.113. Configure accordingly.
7. Type the command to display included RPs.

Scenario 8-2

Refer to the output in Example 8-14 and 8-15 from **show** commands on a Catalyst switch acting as an MLS-SE, and then answer the questions that follow.

Example 8-14 *Scenario 8-2* **show mls** *Command Output*

```
Switch (enable) show mls
Multilayer switching enabled
Multilayer switching aging time = 192 seconds
Multilayer switching fast aging time = 56 seconds, packet threshold = 12
Full flow
Total packets switched = 81391
Active shortcuts = 1115
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0

MLS-RP IP        MLS-RP ID     XTAG      MLS-RP MAC-Vlans
---------        ----------    ----      -----------------------
172.16.30.15     0010f6ad4cb2  28         00-10-f6-ad-4c-b2  1,4-5
```

Example 8-15 *Scenario 8-2* **show mls include** *Command Output*

```
Switch (enable) show mls include
Included MLS-RP
---------------------
172.16.30.15
```

1. Use the output from Example 8-14 and 8-15 to generate a configuration of the switch as it relates to MLS.
2. How many VLANs are involved in MLS? What are they?
3. What is the XTAG for the MLS-RP?
4. Is the MLS-RP an RSM or an external attached router?
5. What type of flow is being used here?

Scenarios Answers

Scenario 8-1 Answers

1. To configure MLS on the RP, the command is **mls rp ip** while in global configuration mode. On the SE, in enable mode, the command is **set mls enable**.
2. Under the interface VLAN12, enter the command **mls rp vtp-domain sjc-1**.
3. Again, under the interface VLAN12, enter the command **mls rp management-domain**.
4. Also, under the interface VLAN12, enter the command **mls rp ip input-acl**.
5. On the switch, in enable mode, enter the command **set mls agingtime 224**.
6. On the switch, in enable mode, enter the command **set mls include 172.16.48.113**.
7. In order to display included RPs, enter the following command on the switch: **show mls include**.

Router Configuration for Scenario 8-1

```
Router#show run
Building configuration...

(Text Deleted)
mls rp ip
!
!
interface Vlan1
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan12
 ip address 172.16.48.113 255.255.255.0
 mls rp vtp-domain sjc-1
 mls rp management-interface
 mls rp ip input-acl
 mls rp ip
```

Switch Configuration for Scenario 8-1

```
Switch (enable)show config
(Text Deleted)
#mls
set mls enable
set mls agingtime 224
set mls agingtime fast 96 15
set mls include 172.16.48.113
```

Display for show mls include Command (Question 7)

```
Switch (enable) show mls include
Included MLS-RP
--------------------
172.16.48.113
```

Scenario 8-2 Answers

1 Example 8-16 shows the correct configuration for Scenario 8-2.

Example 8-16 *Scenario 8-2 Configuration*

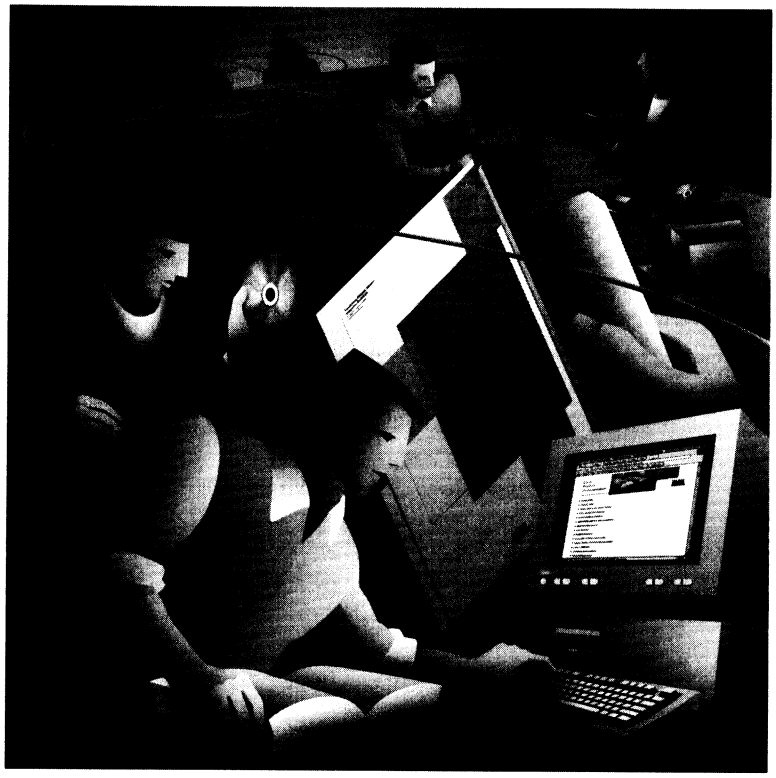
```
 Switch (enable)show config
(Text Deleted)
#mls
set mls enable
set mls agingtime 192
set mls agingtime fast 56 12
set mls include 172.16.30.15
```

2 There are three VLANs and they are VLAN 1, VLAN 4, and VLAN5.

3 The XTAG for the RP is 28.

4 Because there is an included router, this is the sign that the RP is an external router, rather than an RSM.

5 This is a full flow.



from CCNP Remote Access Exam Certification Guide

by Brian Morgan
and Craig Dennis

(1-58720-003-1)

Cisco Press

About the Authors

Brian Morgan, CCIE #4865, is a CCSI for Mentor Technologies (formerly Chesapeake Network Solutions) teaching the ICRC, ACRC, ICND, BSCN, CVOICE, and CATM courses.

Brian has been an instrutor for nearly four years and in the networking industry for over ten years. During that time he's been teaching Cisco Dial Access Solutions boot camp classes for the Service Provider Solutions Tiger Team, the upper echelon of Cisco's technical support structure.

Prior to teaching, Brian spent a number of years with IBM in Network Services where he attained MCNE and MCSE certifications. He was involved with a number of larger LAN/WAN installations for many of IBM's Fortune 500 clients.

Brian is the proud father of five year-old fraternal twin girls (Emma and Amanda) and husband to Beth. His greatest hobby is spending time with the family.

Craig Dennis is an instructor for Mentor Technologies and lives in Fairfax, Virginia. He is a CCSI and CCDP. Craig has taught CMTD and then BCRAN over the last two years. Craig is an avid, but not good, golfer and is currently working toward his CCIE certification. Craig worked for Texaco, Inc., in their Houston Research Lab for 11 years and as a consultant for the Marine Corps for four years as a Network Administrator. He spent about three years as an independent consultant and has taught Cisco classes for the last four years.

Contents at a Glance

Bold chapters are elements included in this folio.

This chapter covers the following topics that you need to master as a CCNP:

- **Modem signaling**—This section covers the transfer of data, the flow control for the signal and the modem, and the call termination methods that are defined by the modem signal pins.
- **Modem configuration using reverse Telnet**—This section describes reverse Telnet, which provides a method to communicate with a device that is attached to an asynchronous port on the router.
- **Router line numbering**—In this section, each router asynchronous interface has an associated line number where the physical and datalink parameters are configured. The line numbering is different between the fixed and nonfixed configuration router models.
- **Basic asynchronous configuration**—This section covers the configuration of the physical interface so that it can communicate with the attached device. In the same way that you configure a COM port to talk to a modem on a PC, you must declare to a router the parameters that match the modem settings.
- **Configuration of the attached modem**—In this section, you learn that a modem must be configured to answer a call and to provide the correct signalling for the telephone company. This is done using the modem command language, which uses the AT command set.
- **Chat scripts to control modem connections**—This section covers chat scripts, which provide a way to dictate to the modem how to place a call, answer an incoming call, and handle a current connection.

CHAPTER 4

Configuring Asynchronous Connections with Modems

To successfully configure an asynchronous modem connection, the following must occur:

1. The modem itself must be configured to respond correctly to the telephone company circuit.
2. The physical aspects of the router link to the modem must be correctly defined to match the modem parameters.
3. The logical parameters must be established to provide a network-layer end-to-end connection.

The modem must be configured so that it understands the signalling on both the telephone-line side and the router-connection side. This information includes the line rate and the number of bits used for data and other physical settings for the modem. The particulars for the modem are discussed in the body of this chapter.

The second and third pieces of an asynchronous modem connection are configured on the router and provide both physical and logical aspects for a connection. The physical properties are configured on the *line*. These parameters include the line rate, the data link-layer protocols supported on the line, and so on. These parameters are needed for the router line to communicate with the attached modem.

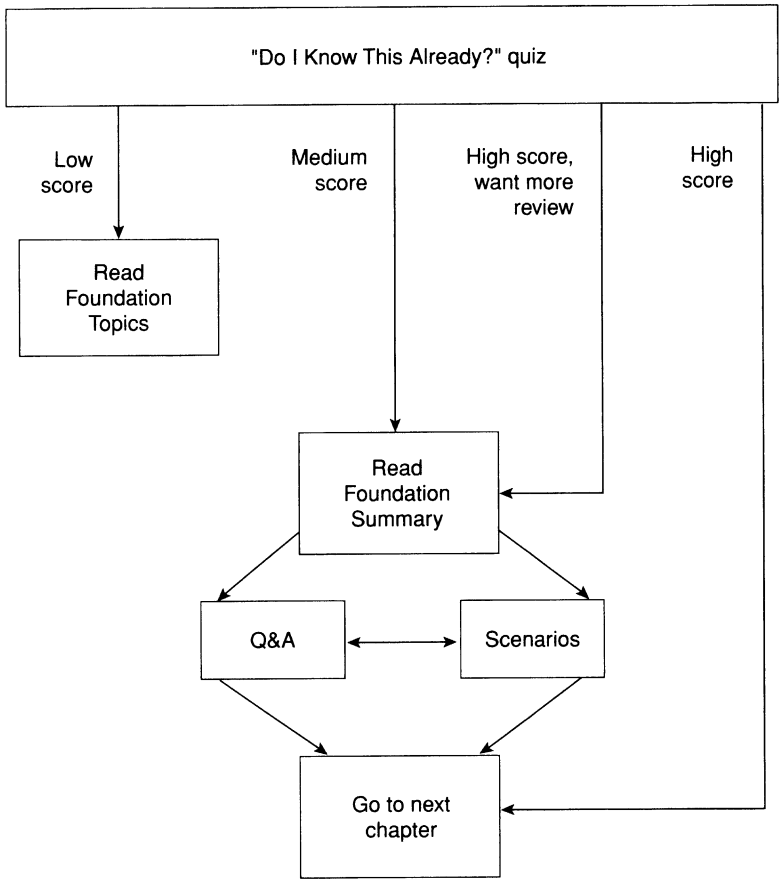
The last piece of an asynchronous modem connection is configuring the logical information on the router *interface*. The logical information includes the Layer 3 addresses, the network-layer protocol, the authentication methods, and so forth.

How to Best Use This Chapter

By taking the following steps, you can make better use of your study time:

- Keep your notes and answers for all your work with this book in one place for easy reference.
- Take the "Do I Know This Already?" quiz and write down your answers. Studies show retention is significantly increased through writing facts and concepts down, even if you never look at the information again.
- Use the diagram in Figure 4-1 to guide you to the next step.

Figure 4-1 *How to Use This Chapter*



"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide what parts of this chapter to use. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The twelve-question quiz helps you determine how to spend your limited study time. The quiz is sectioned into smaller, two-question "quizlets," each of which corresponds to the six major topic headings in the chapter. Use the scoresheet in Table 4-1 to record your scores.

Table 4-1 *Scoresheet for Quizlets and Quiz*

Quizlet Number	Foundation Topics Section Covered by These Questions	Questions	Score
1	Modem Signaling	1–2	
2	Modem Configuration Using Reverse Telnet	3–4	
3	Router Line Numbering	5–6	
4	Basic Asynchronous Configuration	7–8	
5	Configuration of the Attached Modem	9–10	
6	Chat Scripts to Control Modem Connections	11–12	
All questions		1–12	

1 What pins are used for modem control?

2 What is the standard for DCE/DTE signaling?

3 In character mode using reverse Telnet, what is the command to connect to the first async port on a 2509 router that has a loopback interface of 192.168.1.1?

4 What port range is reserved for accessing an individual port using binary mode?

5 If a four-port serial (A/S) module is in the second slot on a 3640 router, what are the line numbers for each port?

6 What is the AUX port line number on a 3620 series router?

7 What does the **physical-line async** command do and on what interfaces would you apply it?

8 In what configuration mode must you be to configure the physical properties of an asynchronous interface?

9 When should **modem autoconfigure discovery** be used? What happens when you use it?

10 Which of the following commands would you use to add an entry to a modemcap database called newmodem?

a. **edit modemcap newmodem**

b. **modemcap edit newmodem**

c. **modemcap edit type newmodem**

d. **modemcap add newmodem**

11 List four reasons why you would use a chat script.

_____

_____

_____

_____

12 Which of the following would trigger a chat script start?

a. Line reset

b. DDR

c. Line activation

d. Manual

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A," on page 397. The suggested choices for your next step are as follows:

- **6 or fewer overall score**—Read the chapter. This includes the "Foundation Topics," the "Foundation Summary," Q&A, and scenarios at the end of the chapter.
- **7, 8, or 9 overall score**—Begin with the "Foundation Summary," then go to the Q&A and scenarios at the end of the chapter.
- **10 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary," then go to the Q&A and scenarios at the end of the chapter. Otherwise, move to the next chapter.

Foundation Topics

Modem Signaling

This chapter covers the signaling of the modem and the configurations for a Remote Access Server (RAS) connection. The successful CCNP or CCDP candidate should be able to describe the signaling and pins used by the cabling and not just the syntax that is required for the connection. The signaling is just as important because it provides the basis for the physical-layer troubleshooting that can be needed to establish a connection.

Asynchronous data communications technology occurs when an end device, such as a PC, calls another end device, such as a server, to exchange data. In asynchronous data communications, end devices are called data terminal equipment (DTE). These devices communicate through data circuit-terminating equipment (DCE). DCE devices clock the flow of information. In our case, the modem provides the DCE function to the PC and server.

The Electronic Industries Association/Telecommunications Industry Association (EIA/TIA) defines a standard for the interface between DCE and DTE devices. This standard is the EIA/TIA-232 and was previously referred to as the RS-232-C standard (where the RS stood for "recommended standard").

It is unwise to think of a PC-to-server connection that uses asynchronous communications as a single circuit. The PC using a modem is one DTE to DCE path end. The far end DCE to DTE (modem to server) is another path. Each DTE–DCE or DCE–DTE connection must be made prior to data transfer.

With asynchronous communication, eight pins are used in a DB25 to transfer data and control the modem, as listed in Table 4-2. The table shows the pins and their definitions. As you read the table, note the direction of the signal and whether DCE or DTE controls or signals on the pin.

Table 4-2 *Standard EIA/TIA-232 Definitions and Codes*

Pin Number	Designation	Definition	Description
2	TD	Transmits data	DTE-to-DCE data transfer
3	RD	Receives data	DCE-to-DTE data transfer
4	RTS	Request to send	DTE signal buffer available
5	CTS	Clear to send	DCE signal buffer available
6	DSR	Data set ready	DCE is ready.
7	GRD	Signal ground	
8	CD	Carrier detect	DCE senses carrier.
20	DTR	Data terminal ready	DTE is ready.

Pins 2, 3, and 7 enable data transfer, pins 4 and 5 enable flow control of data, and pins 6, 8, and 20 provide modem control.

Data Transfer

The pins used for data transfer are pin 2, 3, and 7. The DTE device raises the voltage on the RTS when it has buffer space available to receive from the DCE device. Once a call is established and the DTE device sees the DCE raise the voltage on the CTS, the DTE device transmits data on pin 2. Conversely, the DTE device will raise the voltage on the RTS when it has buffer space available to receive from the DCE device. The need for the ground pin is such that a positive or negative voltage can be discerned.

Data Flow Control

The RTS pin and the CTS pin control the flow of information. The DTE device controls the RTS pin (as shown in Tabel 4-2), which, when seen by the DCE, alerts the DCE that it can receive data. It might help you to think of the RTS as the ready-to-receive pin. The DCE device controls the CTS pin, which in turn signals the DTE that it has buffer available. These definitions are critical to a CCNP or CCDP candidate.

Modem Control

DSR and DTR are signal pins used to control how the modem operates. The DSR pin is raised when the modem is powered on. This raising lets the DTE device know that the modem is ready for use. The DTR pin is raised when the DTE device is powered and ready to receive information from the DCE.

In most cases, when the DTE device is powered on, the DTR pin is raised; however, there are cases in which the DTR pin is raised only if a software package begins to run. This might sound like a minor point, but when you are troubleshooting, it is important to know if the DTE has signaled the modem that it is ready. In fact, just because the PC is on does not necessarily mean that DTR is asserted, and whether your DTE device raises the DTR when powering up or when you turn on your communication software, DTR is needed for a two-way conversation between the DCE and DTE device.

Note that the CD pin is also a signal pin. When two DCE devices establish a connection, the CD pin is asserted to indicate that a carrier signal has been established between the DCE devices. Note also that because two devices constitute the DTE (PC) and DCE (modem) connection, either must be allowed to terminate the connection.

DTE Call Termination

When the DTE is ready to terminate the connection because the user has completed the call and signaled the PC to go back on-hook, the DTR is dropped. For this to happen, the modem must be configured to interpret the loss of the DTR as the end of a conversation. When the DTE drops the DTR, the modem is alerted that the carrier is no longer needed.

This configuration is done when the modem is first installed. This can be manually done for each call, or it can be scripted in a chat script that is sent to the modem each time a call is terminated. Each time a call is terminated, the router resets (rescripts) the modem. This low level configuration is done on the modem to prepare the modem for reuse. In many cases, accepting the default configuration for a modem allows it to function properly.

Even accepting the default configuration provides a "configuration" to the modem. The details of each modem parameter are discussed in the section, "Configuration of an Attached Modem," later in this chapter.

DCE Call Termination

If a far-end modem drops the CD because the remote DTE has ended the transmission, the near-end modem must signal the near-end DTE that the transmission has been terminated. The modem must be programmed to understand and signal this termination. In other words, the modem must be told how to handle the loss of carrier detection. By default, most modems understand that this signal loss is an indication that the call is to be terminated. However, it is a configuration parameter that the modem must understand.

Modem Configuration Using Reverse Telnet

In order to configure a modem, a router must be set up to talk to it. Cisco refers to this as a *reverse Telnet connection.* A host that is connected to a router can Telnet to a Cisco reserved port address on the router and establish an 8-N-1 connection to a specific asynchronous port. An *8-N-1* connection declares the physical signaling characteristics for a line.

Table 4-3 shows reserved port addresses. The router must have a valid IP address on an interface and an asynchronous port. To establish a connection to the modem connected to the asynchronous port, you can Telnet to any valid IP address on the router and declare the Cisco reserved port number for the asynchronous interface. You can do this only, however, from the router console or a remote device that has Telnet access to the router.

Most modem consoles operate using eight data bits, zero parity bits, and one stop bit. In addition, the use of reverse Telnet enables the administrator to configure locally attached devices. For example, suppose you want to set up an 8-N-1 connection to the first asynchronous interface on a router, which has the 123.123.123.123 address assigned to its E0 port. To connect in character mode using Telnet, you would issue the following command:

```
telnet 123.123.123.123 2001
```

where **123.123.123.123** is the router's E0 port and **2001** is the Cisco reserved port number for the first asynchronous port on the router. Table 4-3 shows the Cisco reserved port numbers for all port ranges.

Table 4-3 *Reverse Telnet Cisco Reserved Port Numbers*

Connection Service	Reserved Port Range For Individual Ports	Reserved Port Range For Rotary Groups
Telnet (character mode)	2000–2*xxx*	3000–3*xxx*
TCP (line mode)	4000–4*xxx*	5000–5*xxx*
Telnet (binary mode)	6000–6*xxx*	7000–7*xxx*
Xremote	9000–9*xxx*	10000–10*xxx*

The use of the rotary group reserved port number connects to the first available port that is in the designated rotary group. If a specific individual port is desired, the numbers from the first column of Table 4-3 are used.

You can establish a session with an attached modem using reverse Telnet and the standard **AT** command set (listed later in Table 4-4) to set the modem configuration. This, however, is the hard way because once a modem connection has been established using reverse Telnet, you must disconnect from the line for the modem to be usable again. In addition, to exit the connection, you would have to press Ctrl+Shift+6 and then x to suspend the session, and then issue the **disconnect** command from the router prompt. It is important to remember this simple sequence because the modem does not understand the **exit** command as does a router!

Router Line Numbering

The line numbers on a router are obtained in a methodical manner. The console port is line 0. Each asynchronous (TTY) port is then numbered 1 through the number of TTY ports on the router. The auxiliary port is given the line number LAST TTY + 1, and the virtual terminal (vty) ports are numbered starting at LAST TTY + 2.

Example 4-1 has the **show line** output for a Cisco 2511 router, which has eight asynchronous ports available. Notice that the AUX port is labeled in line 17 and the vty ports are labeled in lines 18–22.

Example 4-1 **show line** *Output for Cisco 2511 Router*

```
2511Router>show line
  Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*   0 CTY              -    -      -    -    -      0       1     0/0       -
*   1 TTY   9600/9600  -    -      -    -    -      7      23     0/0       -
*   2 TTY   9600/9600  -    -      -    -    -      5       1     0/0       -
*   3 TTY   9600/9600  -    -      -    -    -     14      63     0/0       -
*   4 TTY   9600/9600  -    -      -    -    -      4       3     0/0       -
```

continues

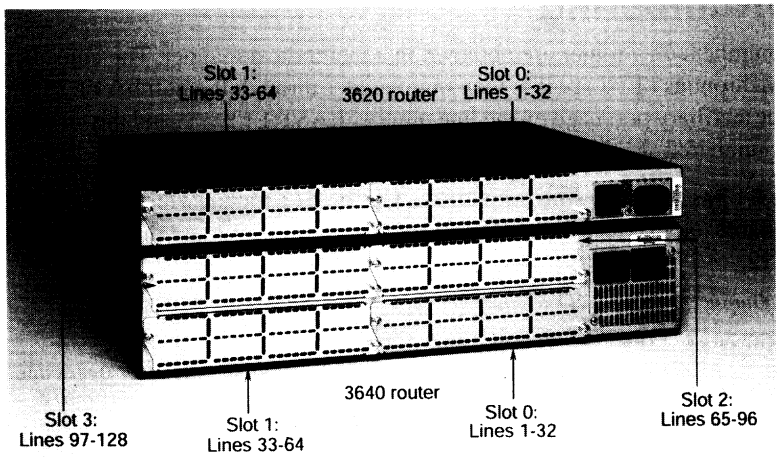
Example 4-1 **show line** *Output for Cisco 2511 Router (Continued)*

```
*  5 TTY   9600/9600  -    -    -    -    -    16    6    0/0   -
*  6 TTY   9600/9600  -    -    -    -    -    12    7    0/0   -
   7 TTY   9600/9600  -    -    -    -    -    3     1    0/0   -
   8 TTY   9600/9600  -    -    -    -    -    0     9    0/0   -
*  9 TTY   9600/9600  -    -    -    -    -    12    0    0/0   -
* 10 TTY   9600/9600  -    -    -    -    -    16    0    0/0   -
* 11 TTY   9600/9600  -    -    -    -    -    25    2    0/0   -
* 12 TTY   9600/9600  -    -    -    -    -    5     0    0/0   -
* 13 TTY   9600/9600  -    -    -    -    -    0     0    0/0   -
  14 TTY   9600/9600  -    -    -    -    -    0     2    0/0   -
  15 TTY   9600/9600  -    -    -    -    -    0     0    0/0   -
  16 TTY   9600/9600  -    -    -    -    -    3     0    0/0   -
  17 AUX   9600/9600  -    -    -    -    -    0     0    0/0   -
  18 VTY              -    -    -    -    -    0     0    0/0   -
  19 VTY              -    -    -    -    -    0     0    0/0   -
  20 VTY              -    -    -    -    -    0     0    0/0   -
  21 VTY              -    -    -    -    -    0     0    0/0   -
  22 VTY              -    -    -    -    -    0     0    0/0   -
```

The numbering scheme for interfaces was expanded for the 3600 series routers. The console is still line 0 and the vty ports are similarly counted after the TTYs. However, Cisco chose to use reserved numbering for the available slots. Thus, slot 0 has reserved lines 1–32, slot 1 has reserved lines 33–64, slot 2 has reserved lines 65–97, and so on. Each slot is given a range of 32 line numbers, whether they are used or not.

Figure 4-2 shows the rear of the chassis for a 3620 and 3640 router and the line numbers associated with each slot.

Figure 4-2 *Line Numbers for 3620 and 3640 Routers*



The line-numbering scheme is important when configuring a router. In the case of the 3600 and 2600 routers with the new modular interfaces, the line numbers are based on the slot that the feature card is in. For illustration, consider the output in Example 4-2, which is from a 3640 series router with a modem card in slot 2. Notice that the line numbers for the internal modems are 65–70 because only one MICA card is installed in the slot.

Example 4-2 **show line** *Output from a 3640 Series Router with a Modem Card in Slot 2*

```
router#show line
  Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*   0 CTY              -    -      -    -    -      0       0     0/0       -
I  65 TTY              - inout      -    -    -      0       0     0/0       -
I  66 TTY              - inout      -    -    -      0       0     0/0       -
I  67 TTY              - inout      -    -    -      0       0     0/0       -
I  68 TTY              - inout      -    -    -      0       0     0/0       -
I  69 TTY              - inout      -    -    -      0       0     0/0       -
I  70 TTY              - inout      -    -    -      0       0     0/0       -
I  97 TTY 115200/115200- inout      -    -    -      0       0     0/0       Se3/0
*129 AUX   9600/9600   -    -      -    -    -      0       0     0/0       -
 130 VTY               -    -      -    -    -      0       0     0/0       -
 131 VTY               -    -      -    -    -      0       0     0/0       -
 132 VTY               -    -      -    -    -      0       0     0/0       -
 133 VTY               -    -      -    -    -      0       0     0/0       -
 134 VTY               -    -      -    -    -      0       0     0/0       -
The following lines are not in asynchronous mode or are without hardware support:
1-64, 71-96, and 98-128.
```

To properly configure a router, you must know the association between the line and interface numbers. The AUX port on the modular routers is the last line number, which would be the number of slots multiplied by 32, plus 1. In the case of the 3640 router shown in Example 4-2, the AUX port number is 129, and the vty ports are 130–134 by default.

In Example 4-3, the configuration for a 3640 router has physical characteristics configured on line 97 for the asynchronous interface in slot 3/0. The remaining IOS commands are discussed in detail later in this chapter, but are presented here for completeness.

Example 4-3 *3640 Router Configuration*

```
interface Serial3/0
 physical-layer async
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 encapsulation ppp
 async mode interactive
 peer default ip address pool TESTPOOL
 no cdp enable
 ppp authentication chap
!
line 97
 password cisco
```

continues

Example 4-3 *3640 Router Configuration (Continued)*

```
 autoselect during-login
 autoselect ppp
 login local
 modem InOut
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 login local
!
```

Basic Asynchronous Configuration

To configure the modem (the DCE) from the router (the DTE), you must set up the logical and physical parameters for the connection. The logical parameters include the protocol addressing, the authentication method, and the encapsulation, all of which are configured on the asynchronous interface. The physical configuration is done on the line. The physical parameters include the flow control, the DTE-DCE speed, and the login request. It is important for the successful CCNP or CCDP to be aware of the command mode needed for configuration.

The configuration in Example 4-4 demonstrates which commands are used on each line or interface.

Example 4-4 *Configuration for a Serial Interface in Asynchronous Mode*

```
interface Serial3/0     !logical parameters go on the interface
    physical-layer async
     ip unnumbered Ethernet0/0
      no ip directed-broadcast
      encapsulation ppp
      async mode interactive
      peer default ip address pool remaddpool
      no cdp enable
      ppp authentication chap
line 97   !physical parameters go on the line
      autoselect during-login
      autoselect ppp
      login
      modem InOut
      modem autoconfigure type usr_sportster
      transport input all
      stopbits 1
      rxspeed 115200
```

Example 4-4 shows the distinction between the physical and logical parameters and where they are defined in the router configuration file.

Three types of router interfaces can be configured for serial communication:

- Asynchronous interfaces
- Synchronous/asynchronous interfaces (A/S)
- Synchronous interfaces

Router interfaces that are synchronous only cannot be used for modem or asynchronous communication. On the router models with A/S ports, the serial ports default to synchronous, and the interface must be declared for asynchronous usage using the **physical-layer async** command.

The configuration in Example 4-4 is for the first (port 0) synchronous/asynchronous interface on a four-port A/S card in the third slot of a 3600. The **physical-layer async** is needed because this device has A/S ports. Hence, the **physical-layer async** command is entered at the **router(config-if)#** prompt for Serial 3/0. On the other hand, in the case of those routers that have ports designated as asynchronous, only the **physical-layer async** command is not used.

Logical Considerations on the Router

Logical considerations are configured on the interface of the router. These include the network-layer addressing, the encapsulation method, the authentication, and so on. The configuration in Example 4-5 is for a serial interface that is used to receive an inbound call.

Example 4-5 *Router Configuration for Serial Interface Receiving Inbound Calls*

```
interface Serial2
  physical-layer async
  ip unnumbered Ethernet0
  ip tcp header-compression passive
   encapsulation ppp
   bandwidth 38
   async mode interactive
   peer default ip address pool remaddpool
   no cdp enable
   ppp authentication chap
```

In Example 4-5, the **physical-layer async** command places the serial 2 interface in asynchronous mode. Once this command is issued, the router treats the interface as an asynchronous port. This can be done on ONLY those interfaces that are defined as A/S.

The **ip unnumbered Ethernet0** command declares that the interface assume the address of the E0 interface. This enables the saving of IP addresses but makes the interface non-SNMP manageable. This command could be replaced with the desired IP address of the interface (refer

to the discussion in this section that covers **ip address pool**). Note that it is quite common for a large number of asynchronous interfaces to a common physical interface to be unnumbered and to use an address pool to assign the network-layer addresses to the dial-up users.

The **ip tcp header-compression passive** command states that if the other DCE device sends packets with header-compression, the interface understands and sends in kind but does not initiate the compression.

The **encapsulation ppp** command declares the encapsulation method for the interface.

The **bandwidth 38** command tells the routing protocol and the router (for statistics) the speed of the line. This command has no affect on the actual negotiated speed of the modem or the speed at which the DTE talks to the modem.

The **async mode interactive** command enables, once a connection is made, the dial-up user access to the EXEC prompt.

The **peer default ip address pool remaddpool** command specifies that the IP address assigned to the dial-up user be from the address grouping or pool defined by the label **remaddpool**. The syntax for the pool definition, defined in global configuration mode, is as follows:

```
ip local pool remaddpool low-ip-pool-address high-ip-pool-address.
```

A unique address from the pool of addresses is given to a dial-up user for the duration of the session. The address is returned to the pool when the dial-up user disconnects the session. In this fashion, it is not necessary to associate an IP address with each asynchronous interface. Each asynchronous interface to another interface on the router is unnumbered and the pool is created from part of that interface's subnet. For more information and examples on the use of address pools and unnumbering, refer to Chapter 6, "Using ISDN and DDR Technologies."

The **no cdp enable** command turns off the Cisco Discovery Protocol for the interface. By default, this protocol is on, and because the interface is likely connected to a dial-up user who does not understand CDP, the bandwidth it would use is saved.

The **ppp authentication chap** command specifies that the Challenge Handshake Authentication Protocol (CHAP) be used on this link. Failure of the client to honor CHAP results in the link not being established.

Physical Considerations on the Router

Physical characteristics are configured in line mode. These include the speed, the direction of the call, modem setup, and so on. Example 4-6 shows a configuration used to connect to a USR Sportster modem on physical line 2.

Example 4-6 *Router Configuration Connecting USR Sportster Modem on Physical Line 2*

```
line 2
      autoselect during-login
      autoselect ppp
      login local
      modem InOut
      modem autoconfigure type usr_sportster
      transport input all
      stopbits 1
      rxspeed 115200
      txspeed 115200
      flowcontrol hardware
```

The **login local** command is the same for this line as it is for the console and AUX ports. The **Login local** command tells the physical line to request a username/password pair when a connection is made and to look locally on the router for a matching **username** *xxxx* **password** *yyyy* pair that has been configured in global mode (*xxxx* and *yyyy* represent a freely chosen username and password combination).

The **autoselect during-login** and **autoselect ppp** commands automatically start the PPP protocol and issue a carriage return so that the user is prompted for the login. This feature became available in IOS Software Release 11.0. Prior to this "during-login" feature, the dial-up user was required to issue an exec command or press the Enter key to start the session.

The **modem InOut** command enables both incoming and outgoing calls. The alternative to this command is the default **no modem inout** command, which yields no control over the modem.

The **modem autoconfigure type usr_sportster** command uses the **modemcap database usr_sportster** entry to initialize the modem. We further discuss this initialization later in the chapter.

The **transport input all** command enables the processing of any protocols on the line. This command defines which protocols to use to connect to a line. The default command prior to 11.1 was **all**; the default with 11.1 is **none**.

In the router configuration, the number of **stopbits** must be the same for both communicating DCE devices. Remember that the physical-layer parameters must match for the physical layer to be established. Failure to do so prevents the upper layers from beginning negotiation.

In Example 4-6, **rxspeed** and **txspeed** are shown as separate commands. The **speed** command, however, sets both transmit and receive speeds and locks the speed between the modem and the DTE device. Failure to lock or control the DTE-to-DCE speed allows the speed of local communication to vary with the line speed negotiated between the DCE devices. This limits the capability of the DTE-to-DCE flow control.

The **flowcontrol hardware** command specifies that the RTS and CTS be honored for flow control.

Example 4-6 provides the basic configuration for an asynchronous line. Once the DTE device has been configured, you must set the DCE device to communicate with the modem by using the AT commands.

Configuration of the Attached Modem

In the early modem days, the Hayes command set was the de facto standard; however, there was never a ratified industry command set. Today, rather than converging to a general standard, the modem industry has actually diverged. Nonetheless, the AT commands documented in Table 4-4 are considered "standard" and should work on most modems.

Table 4-4 *Standard* AT *Commands*

COMMAND	Result
AT&F	Loads factory default settings
ATS0=n	Auto answers
AT&C1	CD reflects the line state
AT&D2	Hangs up on low DTR
ATE0	Turns off local echo
ATM0	Turns off the speaker

A CCNP or CCDP should be familiar with these commands. For many modems on the market today, commands not in this table are used to configure the modem fall into the category of not standard.

The correct initialization string must be sent to the modem for proper operation. You can do this by using a chat script or the **modem autoconfigure** command. The former method is the most common.

Modem Autoconfiguration and the Modem Capabilities Database

Modem autoconfiguration is a Cisco IOS software feature that enables the router to issue the modem configuration commands, which frees the administrator from creating and maintaining scripts for each modem. The general syntax for modem autoconfiguration is as follows:

```
modem autoconfigure [discovery | type modemcap-entry-name]
```

The two command options for the **modem autoconfigure** command are as follows:

- **type**—This option configures modems without using modem commands, or so it is implied. The **type** argument declares the modem type that is defined in the modem capabilities database so that that the administrator does not have to create the modem commands.

- **discovery**—Autodiscover modem also uses the modem capabilities database, but in the case of **discover**, it tries each modem type in the database as it looks for the proper response to its query.

As you can see, the **modem autoconfigure** command relies on the modem capabilities database, also known as the *modemcap*. The modem capabilities database has a listing of modems and a generic initialization string for the modem type. The discovery of a modem using the **autoconfigure** feature uses the initialization strings from each modem in the modem capabilities database to discover the installed modem. If the modem is not in the database, it fails, and the administrator has to manually add the modem to the database.

The use of the discovery feature is not recommended because of the overhead on the router. Each time the line is reset, the modem is rediscovered. However, the discovery feature can be used to initially learn the modem type if you are not geographically near the router and cannot gather the information any other way. After discovery has taken place, the administrator should use the **type** option to specify the entry in the modem capabilities database to use.

To discover a modem, the syntax would be as follows:

```
modem autoconfigure discovery
```

Again, once the modem type is determined, the final configuration for the router interface should be as follows:

```
modem autoconfigure type entry_name_from_modemcap
```

This configuration eliminates unnecessary overhead on the router.

Use the **show modemcap** command to see the entries in the modemcap database. Example 4-7 demonstrates the output from the **show modemcap** command.

Example 4-7 **show modemcap** *Command Output Reveals Modemcap Database Entries*

```
BCRANrouter#show modemcap

default
codex_3260
usr_courier
usr_sportster
hayes_optima
global_village
viva
telebit_t3000
microcom_hdms
microcom_server
nec_v34
nec_v110
nec_piafs
cisco_v110
mica
```

To view the detailed settings for a particular entry in the modem capabilities database, the entry name is added as an argument to the **show modemcap** command. The database has most models of modems. If your entry is not in the database, it can be added by editing the database.

Editing the database requires creating your own entry name and specifying the AT commands for the initialization string. This must be done for any modem that is not in the database. This might sound time-consuming or tedious, but it has to be done only once. The added information to the database is stored in NVRAM as part of the router configuration and can be copied to other routers that have the same modems.

Common practice dictates that multiple modem types not be used at a single RAS facility. Instead, the administrator should use a single modem type and maintain spares of that particular type so that constant manipulation of the modem capabilities database is not necessary.

Let's take a look at how a modem is added to the database. If an attached modem is a Viva plus that is not listed in the database, but another Viva modem is in the database, you could create a new entry and name it whatever you want. The AT commands that are unique to the Viva plus modem would be added to the local configuration in NVRAM and the additional AT commands that are the same for all Viva modems would be obtained from the database.

To add the modem, you would use the following global commands:

```
modemcap edit viva_plus speed &B1
modemcap edit viva_plus autoanswer s0=2
modemcap edit viva_plus template viva
```

These commands use the initialization string from the entry **viva** and enable the administrator to alter the newly created **viva_plus**. All changes and additions to the modemcap are stored in the configuration file for the router. Because of this, Cisco can add to the modemcap at any release because the local NVRAM changes override the modemcap.

The overview of all this is that you bought some modems that you, as the administrator, feel are the best for your application. The modemcap database may, or may not, have these particular modems defined. If the modem is defined in the modemcap then you can simply use the **type** option to the **modem autoconfigure** command. If the modem is not in the database then it must be added. Once it is added, all future modem connections on this router can simply point to the added entry.

Chat Scripts to Control Modem Connections

Chat scripts enable us to talk to or through a modem to a remote system using whatever character strings or syntax is needed. A chat script takes the form of

Expect-string - send-string - expect-string - send-string

where the *expect* strings are character strings sent from or through the modem to the DTE device and the *send* strings are character strings sent from the DTE device to or through the modem.

Reasons for Using a Chat Script

As a CCNP or CCDP, you should be aware that chat scripts are used for the following goals:

- **Initialization**—To initialize the modem
- **Dial string**—To provide the modem with a dial string
- **Logon**—To log in to a remote system
- **Command execution**—To execute a set of commands on a remote system

Reasons for a Chat Script Starting

A chat script can be manually started on a line using the **start-chap** command; they can also be configured to start for the following events:

- **Line activation**—CD trigger (incoming traffic)
- **Line connection**—DTR trigger (outgoing traffic)
- **Line reset**—Asynchronous line reset
- **Startup of an active call**—Access server trigger
- **Dialer startup**—From a dial-on-demand trigger

Using a Chat Script

The primary use of a chat script is to provide the dial number for the connection. The following line shows an example of this chat script:

```
Router(config)#chat-script REMDEVICE ABORT ERROR ABORT BUSY "" "ATZ" OK "ATDT \T"
TIMEOUT 30 CONNECT \c
```

Care should be taken with the character case used in this command. **ABORT ERROR** and **ABORT BUSY** cause the modem to abort if it sees **ERROR** or **BUSY**. Both arguments might be easier understood if read as "abort if you see ERROR" and "abort if you see BUSY," respectively. If **error** or **abort** are entered in lowercase, the modem never sees these conditions because its search is case-sensitive. The **\T** inserts the called number from the **dial string** or **map** command into the chat script. A **\t** causes the script to look for a "table character"; hence, case is important here as well.

NOTE Detailed information on the **dial string** and **map** commands are provided in Chapter 6.

The **REMDEVICE** chat script has been configured to drop the connection if the modem declares a busy or error condition. If no busy or error condition is declared, the router does not

wait for anything except string = " ". The router then issues the **ATZ**, or modem reset, command, using a send string. The router waits for the modem to respond OK, which is the normal modem response to **ATZ**. The router then sends the **ATDT** command and replaces the **\T** with the phone number to make the call. Last, the **TIMEOUT 30** declares that the call is considered "not answered" if no carrier is obtained in 30 seconds. Once the connection is made, the chat script sends a **c**, which is a carriage return.

Provided that the router, the modem, and the phone number are correct, the physical layer should now be established! Congratulations! You can now move on to the upper layer protocols, such as PPP (see Chapter 5, "Configuring PPP and Controlling Network Access") and advanced uses (see Chapter 6).

Foundation Summary

The Foundation Summary is a collection of tables and figures that provides a convenient review of many key concepts in this chapter. For those of you already comfortable with the topics in this chapter, this summary could help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final preparation before the exam, these tables and figures will hopefully be a convenient way to review the day before the exam.

Table 4-5 *Standard EIA/TIA-232 Definitions and Codes*

Pin Number	Designation	Definition	Description
2	TD	Transmits data	DTE-to-DCE data transfer
3	RD	Receives data	DCE-to-DTE data transfer
4	RTS	Request to send	DTE signal buffer available
5	CTS	Clear to send	DCE signal buffer available
6	DSR	Data set ready	DCE is ready.
7	GRD	Signal ground	
8	CD	Carrier detect	DCE senses carrier.
20	DTR	Data terminal ready	DTE is ready.

Table 4-6 *Cisco Reserved Port Numbers Used with Reverse Telnet*

Connection Service	Reserved Port Range for Individual Ports	Reserved Port Range for Rotary Groups
Telnet (character mode)	2000–2*xxx*	3000–3*xxx*
TCP (line mode)	4000–4*xxx*	5000–5*xxx*
Telnet (binary mode)	6000–6*xxx*	7000–7*xxx*
Xremote	9000–9*xxx*	10000–10*xxx*

Figure 4-3 *3600 Line Numbers*

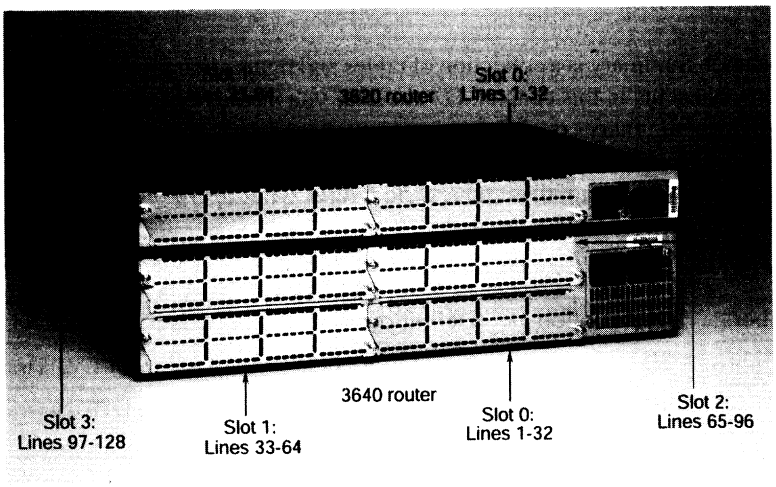


Table 4-7 **modem autoconfigure** *Commands*

Command	What It Does
modem autoconfigure discovery	Discovers the modem
modem autoconfigure type *entry_name_from_modemcap*	Creates the final configuration for the router interface, which eliminates unnecessary overhead on the router
show modemcap	Displays the entries in the modemcap database

Table 4-8 *Standard* AT *Commands*

Command	Result
AT&F	Loads factory default settings
ATS0=n	Auto answers
AT&C1	CD reflects the line state
AT&D2	Hangs up on low DTR
ATE0	Turns off local echo
ATM0	Turns off the speaker

Reasons for using a chat script:

- **Initialization**—To initialize the modem
- **Dial string**—To provide the modem with a dial string
- **Logon**—To log in to a remote system
- **Command Execution**—To execute a set of commands on a remote system

A chat script can be manually started on a line using the **start-chap** command; they can also be configured to start for the following events:

- **Line activation**—CD trigger (incoming traffic)
- **Line connection**—DTR trigger (outgoing traffic)
- **Line reset**—Asynchronous line reset
- **Startup of an active call**—Access server trigger
- **Dialer startup**—From a dial-on-demand trigger

Q&A

The questions and scenarios in this book are more difficult than what you will experience on the actual exam. The questions do not attempt to cover more breadth or depth than the exam; however, they are designed to make sure that you know the answer. Rather than enabling you to derive the answer from clues hidden inside the question itself, the questions challenge your understanding and recall of the subject.

Questions from the "Do I Know This Already?" quiz from the beginning of the chapter are repeated here to ensure that you have mastered the chapter's topic areas. Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options and then guess.

The answers to these questions can be found in Appendix A, on page 397.

1 What pins are used for modem control?

2 What is the standard for DCE/DTE signaling?

3 If the user wants to terminate a call, what pin does the DTE device drop to signal the modem?

4 What must be done to terminate a reverse Telnet session with an attached modem?

5 In character mode using reverse Telnet, what is the command to connect to the first async port on a 2509 router that has a loopback interface of 192.168.1.1?

6 Which interface is line 97 on a 3640 series router?

a. S 0/97

b. S 3/1

c. S 2/1

d. S 097

7 What port range is reserved for accessing an individual port using binary mode?

8 When flow control is enabled, which pins are used?

9 If a four-port serial (A/S) module is in the second slot on a 3640 router, what are the line numbers for each port?

10 What is the **AT** command to return a router to factory default settings?

a. **AT Default**

b. **AT@F**

c. **AT&F**

d. **ATZ**

11 What is the AUX port line number on a 3620 series router?

12 Which of the following commands configure a router for use with a Viva modem?

a. **modem autoconfigure viva**

b. **modem configure type viva**

c. **modem autoconfigure type viva**

d. **modem autoconfigure discovery type viva**

13 What does the **physical-line async** command do and on what interfaces would you apply it?

14 In what configuration mode must you be to configure the physical properties of an asynchronous interface?

15 What does it mean when the signal pin RTS is asserted?

16 What is the command to manually begin a chat script named remcon?

17 When should **modem autoconfigure discovery** be used, and what are the ramifications of doing so?

18 What command would you use to add an entry to the modemcap database called newmodem?

19 Which interface type provides clocking for a line?

20 List four reasons why you would use a chat script.

21 What command can be used to determine whether Serial 0 is the DCE or DTE?

22 What command lists the transmit and receive speeds for the asynchronous ports on the router?

_____

_____

_____

23 On which pins does the DTE device send and receive?

_____

_____

_____

24 Which of the following would trigger a chat script start?

a. Line reset

b. DDR

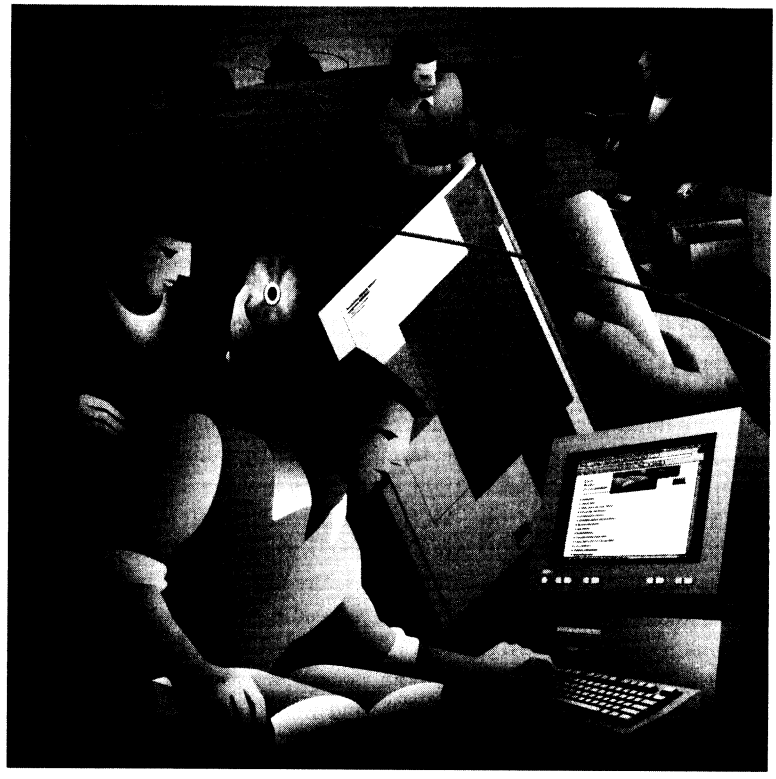
c. Line activation

d. Manual

Scenarios

There are no scenarios for this particular chapter. The key issues and concepts here are syntax, syntax, and syntax. For further review, you should practice creating a configuration for a router and include all parts necessary for an asynchronous setup. The parts should include:

- Line configuration (physical)
- Interface configuration (logical)
- A new modemcap entry (your choice)
- An alias to address the modem locally (Reverse Telnet)
- A chat script for the connection (no phone number needed!)



from CCNP Support Exam Certification Guide

by Amir S. Ranjibar

(0-73570-995-5)

Cisco Press

About the Author

Amir S. Ranjbar (CCNP) is an instructor and senior network architect for Global Knowledge, Cisco's largest training partner. He is a Certified Cisco Systems Instructor (CCSI) who teaches the Cisco Internetwork Troubleshooting course on a regular basis. Born in Tehran, Iran, Amir moved to Canada in 1983 and obtained his Bachelors degree in Computing and Information Science (1988) and Master of Science degree in Knowledge Based Systems (1991) from the University of Guelph (Guelph, Ontario). After graduation, Amir developed software applications in the areas of statistical analysis and systems simulation for a number of institutes such as Statistics Canada, University of Waterloo, and University of Ottawa. Amir started his training career by joining Digital Equipment Corporation's Learning Services in 1995, and after a few years of working exclusively as a Microsoft Certified Trainer (MCSE, MCT), he decided to shift his focus to Cisco Systems' internetworking products. In 1998, Amir joined Geotrain Corporation, which was acquired by Global Knowledge in 1999. Currently, Amir, already a CCNP, is preparing for the CCIE examinations and is a full-time instructor for Global Knowledge. Among the courses Amir teaches are Interconnecting Cisco Network Devices (ICND), Building Scalable Cisco Networks (BSCN), Building Cisco Remote Access Networks (BCRAN), Cisco Internetwork Troubleshooting (CIT), OSPF, and BGP. You can contact Amir by email at amir.ranjbar@globalknowledge.com.

Contents at a Glance

Bold chapters are elements included in this folio.

This chapter covers the following topics that you will need to master to pass the CCNP Support exam:

Objective	Description
1	Troubleshooting Cisco IOS configuration.
2	VLAN design issues for troubleshooting.
3	Switch/router configuration consistency.
4	Router VLAN diagnostic tools: **show** commands.
5	Router VLAN diagnostic tools: **debug** commands.
6	Problem isolation in router/switch VLAN networks.

CHAPTER 9

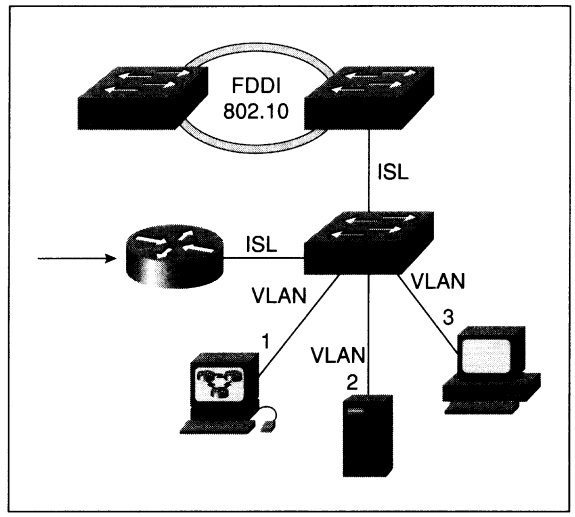
Troubleshooting VLANS on Routers and Switches

This chapter's focus is on routers used in switched internetworks to provide communication between VLANs and access to remote sites across wide area networks. In this context, routers not only facilitate integration of switching products, but they also make VLAN-based architectures scalable and flexible. This chapter discusses how VLANs must be implemented on Cisco routers, what the key configuration issues are, and which commands can help diagnose related errors and faults.

A router may play different roles in a switched internetwork. A router may be connected to a switch through a trunk connection, in which case the router interface that is on the trunk connection will have one subinterface for each VLAN that goes through the trunk. The router is typically used to route packets between the VLANs and the other networks (including wide-area connections) to which it connects. This setup is usually referred to as the router on a stick (see Figure 9-1). The term "router on a stick" is used for a scenario in which an external router is connected to a LAN switch via trunk connection(s) and performs routing between the VLANs that belong to the trunk connection(s). On the other hand, a Router Switch Module (RSM), sometimes referred to as a "router on a blade," is also commonly used in Catalyst switches for the purpose of routing between VLANs.

In certain scenarios the router may be configured to perform bridging between certain ports, including the subinterfaces of the interface that is configured for trunking. This function is called VLAN switching. Naturally the router's Spanning-Tree Protocol must then match and communicate with the Spanning-Tree Protocols of the other devices (switches and bridges) on the network. Finally, if a router has multiple trunk connections via different media (ISL over Fast Ethernet, 802.1Q over Fast Ethernet, 802.10 over FDDI, LANE over ATM) it can also provide transparent connectivity between them. This function, called VLAN translation, was introduced as of Cisco IOS Release 11.1 and it is fast switched. In summary, a router may perform VLAN routing, VLAN switching, and VLAN translation in a network.

Figure 9-1 *Router on a Stick*



"Do I Know This Already?" Quiz

If you wish to evaluate your knowledge of the contents of this chapter before you get started, answer the following questions. The answers are provided in Appendix A, "Answers to Quiz Questions." If you are having difficulty providing correct answers, you should thoroughly review the entire chapter. If all or most of your answers are correct, you might want to skim this chapter for only those subjects you need to review. You can also use the "Foundation Summary" section to quickly review topics. Once you have completed the chapter, you should reevaluate yourself with the questions in the "Q&A" section at the end. Finally, use the companion CD-ROM to evaluate your knowledge of the topics and see if you need a review.

1 Name three of the functions routers perform in a VLAN switching environment.

_____

_____

_____

2 Which type of router interface is used for ISL trunking?

3 How many VLANs can a subinterface of an interface used for trunking correspond to?

4 Which command functions are configured on the main interface of the (Fast Ethernet) interface for the purpose of trunking?

5 What is the general recommendation for the bridged networks in terms of the number of hops?

6 How many default VLANs are preconfigured on a Catalyst 5000 switch?

7 What is the recommended usage of VLAN number 1?

8 What role can a Cisco router play in a VTP domain?

9 What information can one obtain from the output of the **show vlans** command?

_____

_____

_____

Foundation Topics

Troubleshooting Cisco IOS Configuration

The Fast Ethernet interface of a router is used to connect a router to a switch for trunking purpose. Example 9-1 shows a sample configuration for the Fast Ethernet interface of a router for this case.

Example 9-1 *Sample Configuration of Fast Ethernet Interface for Trunking*

```
interface FastEthernet0
 no ip address
 full-duplex
!
interface FastEthernet0.1
 encapsulation isl 1
 ip address 10.1.1.44 255.255.0.0
 ipx network 36dd
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.1.40 255.255.0.0
 bridge-group 60
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.1.40 255.255.0.0
  bridge-group 60
!
interface FastEthernet0.100
 encapsulation isl 100
 ip address 144.251.100.40 255.255.255.0
!
```

If a Fast Ethernet interface is used for trunking purposes, it should not have any Layer 3 (OSI network layer) address or any bridging commands configured on the main interface. These types of commands must be appropriately entered on the subinterfaces. Each subinterface will correspond to one VLAN member of the trunk.

The main interface configuration commands that may be necessary on the Fast Ethernet interface are **media-type** and **full-duplex**. Those router interfaces that have multiple connectors for different types of connections (such as MII and100BaseTx) consider one of the media as the default media. If you connect your cable to the default connector (for example, MII), then you do not need to enter the media-type command. However, if the 100BaseTx connection is used, then you have to enter the **media-type 100basetx** command on the main (Fast Ethernet) interface. Because a trunk connection is point-to-point, it is possible and very advantageous to configure the trunk connection with the full-duplex command (also done on the main interface).

If you forget to configure, or misconfigure, the media type on an interface, the symptom will be easy to spot. If the interface is not administratively shut down, then the physical layer will show as UP, but the link layer will show as DOWN, since the router's keepalive will fail. If an interface is configured with the **no keepalive** command, both the physical and link layers will show as UP, even though the cable is connected to the wrong connector! This makes troubleshooting more difficult. Fortunately, there are three methods to discover that. You may enter the **show controller fastethernet** *interface-number* command and find out the media type from its output. Some interfaces (for instance, the FASTETHERNET cards of the Cisco 4500 routers) have a LED that tells you the media type the router is configured for. You may also look at the running-config of a router to find out the media type configured on an interface. Keep in mind that the default media type is not shown on the running-config and startup-config.

The duplexing configuration of a trunk port can be tricky. Catalyst switches are supposed to autosense the duplexing (full versus half) and Cisco routers have a default setting. If you are troubleshooting a trunk connection between a router and a switch, it is best if you decide on the duplexing mode and do a manual configuration on both devices. Relying on the auto-sensing feature is usually discouraged.

As mentioned earlier, each subinterface of a Fast Ethernet interface used for trunking corresponds to one VLAN. On each subinterface you need to enter the **encapsulation isl** *vlan-number* command. A subinterface may have a Layer 3 (OSI network layer) address such as an IP address, and it may have a **bridge-group** *bridge-group-number.*

The interface shown in Example 9-1 has four subinterfaces, each with an IP address (for each interface you may configure up to 255 subinterfaces). The subinterfaces correspond to VLANs 1, 2, 3, and 100, and each VLAN matches one IP subnet. Note that the fa0.2 and fa0.3 subinterfaces are configured to bridge any packet other than IP. When the router receives an ISL frame on its Fast Ethernet interface, it first recognizes the VLAN number of the frame from the ISL header. It then de-encapsulates the original frame from the ISL frame and processes it based on the assumption that the original frame was received from the subinterface that corresponds to the VLAN ID of the ISL frame.

You must now realize why it is important to have one subinterface for each VLAN that belongs to the trunk. After the router selects the subinterface the frame corresponds to, it will then route, bridge, or drop the received packet. For example, assume that the router (using Example 9-1 as the guide) receives an ISL frame with VLAN ID of 100 encapsulating an Ethernet frame, which in turn encapsulates an IPX packet. The router processes the de-encapsulated Ethernet frame as if it has arrived from a real Ethernet interface. However, because the Fast Ethernet 0.100 interface shown in Example 9-1 does not have an IPX address and is not configured to bridge IPX either, the frame will be dropped.

There are some important facts you need to remember about the limitations of VLAN processing and trunking on a router. For example, the ISL encapsulation is available only on the Fast Ethernet interfaces of certain routers (4500 and 7000 series Cisco routers). IP

and IPX routing between VLANs is only allowed by specific IOS releases (and the IPX frame-type must be Novell-Ethernet). Some IOS releases, in addition to transparent bridging, support integrated routing and bridging (IRB) between the VLANs, for IPX (with SAP and SNAP frame types) and AppleTalk.

VLAN Design Issues for Troubleshooting

One important topic of interest in switched internetworks is the convergence time of the spanning tree. Two factors, the diameter of a network measured in terms of the number of hops (bridges/switches), and the values of the spanning tree timers, affect the time it takes for the bridged/switched internetwork to converge. The general rule for the bridged networks is that the number of hops (bridges/switches) should not exceed seven.

When a port that is in the Forwarding state fails, the other ports (of the other devices) on that segment wait for a period equal to three times the HELLO period before they consider that port gone (dead). Because the spanning tree may have to be reexecuted, the change notification BPDU must first be sent to ALL of the switches. This notification might have to traverse through all of the network segments hop by hop via BPDUs that are released as often as the HELLO period (the default HELLO period is 2 seconds).

Hence, from the instant that a port fails to the moment that all switches are notified of the change can take up to 20 seconds (assuming the maximum of 7 hops). The default value of the MAX_AGE parameter of the spanning tree is set to 20 (seconds) for this reason. Next, the spanning tree is executed for a period equal to the fwddelay parameter, which is equal to 15 seconds by default. During this period the ports are in the Listening state and are NOT forwarding received frames.

After completion of the spanning tree, each port spends a period equal to the fwddelay parameter in the Learning mode during which it builds the initial MAC table and does not forward received frames. Hence, the convergence of a switched internetwork (seven hops assumed) can take up to 50 seconds (20 + 15 + 15). The values of the HELLO, MAX_AGE, and Forward Delay (fwddelay) parameters are imposed on all other switches by the root device. In other words, changing any of these parameters on any device other than the root device is not practical, as the non-root device will revert to the values imposed by the root device. Changing these parameters on the root device, on the other hand, practically means changing the parameters on all of the devices.

Switch/Router Configuration Consistency

There are five default VLANs preconfigured on a Catalyst 5000 switch for different media types. Table 9-1 shows these VLANs along with their associated MTU, ISL VLAN ID, and 802.10 Security Association Identifier (SAID). Numbers 1 though 1000 may be used for the VLANs created on a Catalyst 5000 family switch. You are encouraged to leave VLAN

number 1 for management and troubleshooting and use VLANs 2 through 1000 for user (traffic) VLANs. When you connect a router and a switch via a trunk connection, you must make sure that the Media type and MTU of each VLAN are consistent between these devices.

Table 9-1 *Default VLANs on a Catalyst 5000 Family Switch*

VLAN Name	Type	MTU	ISL VLAN-id	802.10 SAID
Default	Ethernet	1500	0001	100001
Fddi-default	Fddi	4352	1002	101002
Token-ring-default	Token-ring	2048	1003	101003
Fddinet-default	Fddi-net	4352	1004	101004
Trnet-default	Tr-net	2048	1005	101005

As mentioned earlier, on a (an ISL-capable) Cisco router, you have the option to bridge between the subinterfaces of the ISL (trunk) interface. This may very well be necessary; however, you must realize that this action combines the spanning trees associated with the VLANs of those subinterfaces that you bridge. Moreover, when you do bridging on a router, you must also ensure that the Spanning-Tree Protocol used on the router (IEEE or DEC) is identical to the Spanning-Tree Protocol used on your switches. Usage of incompatible Spanning-Tree Protocols has serious implications, including loss of BPDUs (drops), loops, broadcast storms, and ultimately network meltdown.

An important factor in management and troubleshooting of switched internetworks is having a map of the network showing the connections (loops), bridge and port priorities, and the root bridge. In most cases automatic election of root device, designated port, and root port, as per the Spanning-Tree Protocol's algorithm, does not yield the most efficient and effective topology. You must make use of manual bridge priority, port priority, and port cost configuration for the most desirable Layer 2 topology.

Keep in mind that spanning tree timers are dictated by the root device to all of the other participating members of the spanning tree (the non-root devices). In periods of instability it is wise to reduce the spanning tree activities of the devices. One way of achieving this is by setting the spanning tree timers at their maximum values on the root device. The forward delay (fwddelay) parameter can be set to the maximum value of 30 seconds, and the maximum age (MAX_AGE) parameter can be set to the maximum value of 40 seconds. In a stable network, on the other hand, using shorter timer values assist in swift detection of a failure and a faster network convergence.

Cisco routers do not yet support VTP (VLAN Trunking Protocol). Positioning a router between a bunch of switches segregates a VTP domain. If there is only one switch behind a router, it is probably wise to configure that switch in a VTP transparent mode. If there is

more than one switch behind a router, however, it is probably easier to have them configured with a different VTP domain (name).

Router VLAN Diagnostic Tools: show Commands

In this section a few of the Cisco router IOS **show** commands that help diagnose VLAN-related cases are presented. You need to know the syntax of each command and what information each command's output makes available. The following sections each provide a sample output for the presented **show** command to help you better understand the usage and benefits of it.

show vlans

The **show vlans** command lists all the VLANs configured on a router. Example 9-2 shows a sample output of this command. For each VLAN, the corresponding subinterface and its configured addresses (for instance, IP and IPX) are displayed. For each protocol configured on a subinterface, this command also shows the number of packets sent and received.

Example 9-2 *A Sample Output for the* ***show vlans*** *Command*

```
D_BackR#show vlans

Virtual LAN ID:  1 (Inter Switch Link Encapsulation)

 vLAN Trunk Interface:   FastEthernet0.1
 Protocols Configured:   Address:            Received:   Transmitted:
 IP                      10.1.1.44           67          104

Virtual LAN ID:  2 (Inter Switch Link Encapsulation)

 vLAN Trunk Interface:   FastEthernet0.2
 Protocols Configured:   Address:            Received:   Transmitted:
 IP                      10.2.1.40           134         87
 IPX (NOVELL-ETHER)      2000.00e0.1454.cf19 10          10

Virtual LAN ID:  3 (Inter Switch Link Encapsulation)

 vLAN Trunk Interface:   FastEthernet0.3
 Protocols Configured:   Address:             Received:  Transmitted:
 IP                      10.3.1.40            20         44
 IPX (NOVELL-ETHER)      3000.00e0.1454.cf19  14         13

Virtual LAN ID:  100 (Inter Switch Link Encapsulation)

 vLAN Trunk Interface:   FastEthernet0.100
 Protocols Configured:   Address:              Received: Transmitted:
 IP                      144.251.100.40        367       98

D_BackR#
```

show span [*vlan-number*]

This command first appeared in Cisco IOS Release 10.3 and it shows the Spanning-Tree Protocol information known to the router (see Example 9-3). The first part of this command's output shows the type of Spanning-Tree Protocol in use, the bridge ID (priority and address) of the local device (the router), the ID of the root device, and the timer parameters of the spanning tree. Next, the interfaces that participate in the spanning tree (associated to the VLAN number typed in) are listed. For each interface, its associated state (for example, Forwarding), priority, cost, timers, as well as the ID of the designated root and bridge are displayed. It is noteworthy that the Catalyst switch's IOS command counterpart for displaying information about Spanning Tree is **show spantree**; the **show span** command on a Catalyst switch displays SPAN (switched port analyzer) information.

Example 9-3 *A Sample Output for the* ***show span*** *[vlan-number] Command*

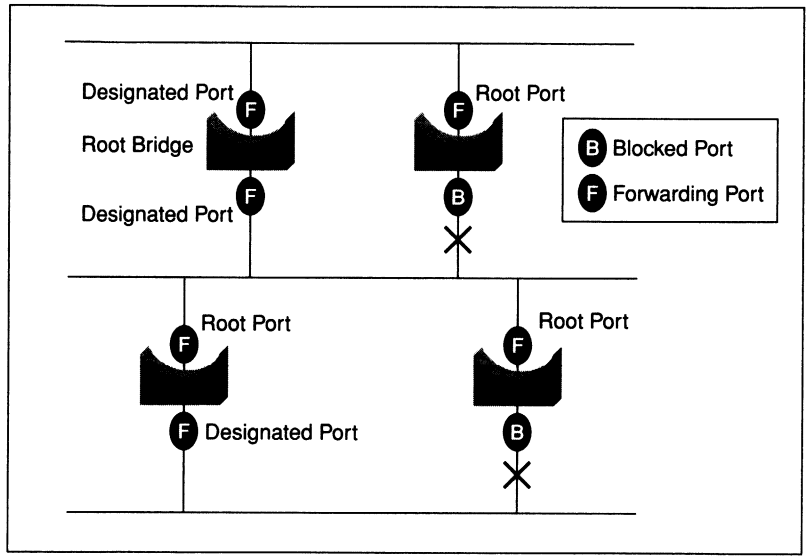
```
D_BackR_J#show span 1

Bridge Group 1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00e0.1454.cf1b
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag set, detected flag set
  Times:  hold 1, topology change 30, notification 30
          hello 2, max age 20, forward delay 15, aging 300
  Timers: hello 2, topology change 25, notification 0

Port 3 (Ethernet1) of bridge group 1 is forwarding
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 00e0.1454.cf1b
   Designated bridge has priority 32768, address 00e0.1454.cf1b
   Designated port is 3, path cost 0
   Timers: message age 0, forward delay 0, hold 0

Port 19 (FastEthernet0.100 ISL) of bridge group 1 is forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 32768, address 00e0.1454.cf1b
   Designated bridge has priority 32768, address 00e0.1454.cf1b
   Designated port is 19, path cost 0
   Timers: message age 0, forward delay 0, hold 0
```

You can construct a map of your Spanning-Tree Protocol network from the key information displayed by the **show span** command. A network map is one of the essential parts of the set of facts you need to support and troubleshoot a network (see Figure 9-2). When you read the output of this command, you need to be aware of the following facts:

- When the MAC address of the designated bridge is the same as the MAC address of the root bridge, the port or interface of the bridge being examined and the root bridge are attached to the same network.

- When the MAC address of the designated bridge is different from the MAC address of the bridge being examined, the designated bridge is in the path to the root bridge.
- When the MAC address of the designated bridge is the same as the bridge identifier of the bridge being examined, the port or interface points away from the root bridge.
- The bridge port value specified for a particular port belongs to the bridge associated with the designated bridge shown in the port listing.

Figure 9-2 *Spanning-Tree Map of a Network*



show bridge [*bridge-number*]

The **show bridge** command displays the contents of your router's bridge forwarding database for all the bridge groups defined (see Example 9-4). If you specify a bridge number, then of course the output will show only the information pertaining to the bridge group specified.

Example 9-4 *A Sample Output for the* ***show bridge*** *Command*

```
D_BackR_J#show bridge

Total of 300 station blocks, 295 free
Codes: P - permanent, S - self

Bridge Group 1:
```

continues

Example 9-4 *A Sample Output for the* ***show bridge*** *Command (Continued)*

```
Address          Action    Interface     Age   RX count  TX count
0010.7b2c.5b1b   forward   Ethernet1       0      6          0
00e0.fe80.bbff   forward   Ethernet1       0    119          0
00e0.1ee8.86e3   forward   Ethernet1       0      2          0
00e0.1454.cf49   forward   Ethernet1       0      4          0
0080.c885.54a2   forward   Ethernet1       0      5          0
D_BackR_J#
```

show interface fastethernet 0

The Fast Ethernet interface can be used to build a trunk connection to a switch or another router with ISL. The **show interfaces fastethernet 0** command displays information about this interface's state (up, down, administratively down) and other information that you see when you issue this command for any interface. However, when you observe the output of this command, pay special attention to the duplexing mode, speed, and the media reported. Example 9-5 provides a sample output of this command. As you can see, the sixth line of the output shows Full-duplex, 100 Mbps, and 100BaseTX/FX, which is a common configuration for a trunk/ISL connection between a router and a Catalyst switch.

Example 9-5 *A Sample Output of the* ***show interfaces fastethernet 0*** *Command*

```
D_BackR_J#show interfaces fastethernet 0
FastEthernet0 is up, line protocol is up
  Hardware is DEC21140, address is 00e0.1454.cf19 (bia00e0.1454.cf19)
  Description: For ISL trunking
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 2000 bits/sec, 4 packets/sec
     1651 packets input, 126990 bytes, 0 no buffer
     Received 1194 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     2536 packets output, 272626 bytes, 0 underruns
     41 output errors, 41 collisions, 7 interface resets
     0 babbles, 0 late collision, 0 deferred
     41 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
D_BackR_J#
```

Router VLAN Diagnostic Tools: debug Commands

There are two **debug** commands particularly useful for troubleshooting VLANs on a router. The **debug VLAN packets** command helps diagnose a trunk/ISL connection on a Fast Ethernet interface, and the **debug span** command with the **tree** or **events** option is helpful for diagnosing spanning tree issues.

debug vlan packets

The **debug vlan packet** command displays messages about virtual LAN (VLAN) packets that the router receives (off the trunk connection) but is not configured to support (see Example 9-6). In other words, if an ISL packet with a VLAN ID of 6 is received, but none of the subinterfaces of the input interface are configured for VLAN 6, the router cannot process the encapsulated frame and the debug process displays a message indicating what has just happened. As mentioned earlier, you may use the **show vlans** command to see the list of all the VLANs configured on your router.

Example 9-6 *A Sample Output of the **debug vlan packets** Command*

```
D_BackR#debug vlan packets
Virtual LAN packet information debugging is on
D_BackR#
05:20:45: vLAN: Received ISL encapsulated UNKNOWN packet bearing colour ID 100
      on interface FastEthernet0.100 which is not configured to
      route or bridge this packet type.

05:20:45: vLAN: Received ISL encapsulated UNKNOWN packet bearing colour ID 3
      on interface FastEthernet0.3 which is not configured to
      route or bridge this packet type.

05:20:45: vLAN: ISL packet received bearing colour ID 4 on FastEthernet0
      which has no subinterface configured to route or bridge ID 4.

05:20:45: vLAN: ISL packet received bearing colour ID 5 on FastEthernet0
      which has no subinterface configured to route or bridge ID 5.

05:20:45: vLAN: ISL packet received bearing colour ID 6 on FastEthernet0
      which has no subinterface configured to route or bridge ID 6.

05:20:45: vLAN: ISL packet received bearing colour ID 7 on FastEthernet0
      which has no subinterface configured to route or bridge ID 7.

05:20:45: vLAN: Received ISL encapsulated UNKNOWN packet bearing colour ID 100
      on interface FastEthernet0.100 which is not configured to
      route or bridge this packet type.
```

The first entry in the output of Example 9-6 notifies you that an ISL frame was received from the fastethernet 0.100 subinterface. That ISL frame's VLAN ID was 100, but it

encapsulated a frame that in turn encapsulated a packet that the fastethernet 0.100 subinterface is not configured to route or bridge.

The third entry in the output of Example 9-6 tells you that an ISL frame was received from the fastethernet 0 interface. The ISL frame's VLAN ID was 4, and the fastethernet 0 interface does not have a subinterface to handle this VLAN's frames. In scenarios like this, it is usually wise to configure the device on the other side of the trunk not to send certain VLANs' frames in this direction. On the Catalyst 5000 switch, you may use the **clear trunk** command to take a VLAN out of a trunk port.

debug span tree and debug span events

The **debug span** command can be used with either the **tree** or the **events** parameter. The **events** option is more user-friendly because it tells you in words the meaning of the BPDU packets that the router is receiving (see Example 9-7). The **tree** option, on the other hand, displays each BPDU received from each interface in its raw format.

For instance, the first entry in the output of the debug span tree (Example 9-7) shows the following line: 00:15:42: ST: Fa0.100 00000080. This line tells you that at 3:42 p.m. a spanning-tree packet was received from the fastethernet 0.100 subinterface. This BPDU packet starts with four zeros (field A), which means that this packet is an IEEE spanning-tree BPDU. The following two zeros (field B) indicate the version, and the 80 at the end (field C) indicates that the received BPDU is a Topology Change Notification (TCN). As you can see, either of these commands can be used to track and verify the operation of the spanning tree.

Example 9-7 *Sample Output of* ***debug span ?****,* ***debug span tree****, and* ***debug span events***

```
D_BackR_J#debug span ?
  events  Spanning-tree topology events
  tree      Spanning-tree protocol data units

D_BackR_J#debug span tree
Spanning Tree BPDU debugging is on
D_BackR_J#
00:15:42: ST: Fa0.100 00000080
00:16:19: ST: Ethernet1 00000080
00:16:27: ST: Fa0.100 00000080
00:16:37: ST: Ethernet1 00000080

D_BackR_J#debug span events
Spanning Tree event debugging is on
D_BackR_J#
00:16:57: ST: Topology Change rcvd on FastEthernet0.100
00:16:57: ST: Topology Change rcvd on FastEthernet0.100
00:17:19: ST: Topology Change rcvd on Ethernet1
00:17:29: ST: Topology Change rcvd on FastEthernet0.100

D_BackR_J#
```

Problem Isolation in Router/Switch VLAN Networks

To ensure that a router is properly connected to a switch through a trunk and that it is receiving the desired data units and processing them, you need to do the following:

- Check the physical link between the router and the switch. For instance, make sure that the cable between the router and switch is straight-through, is of the correct type/category, and is properly connected using proper connectors. The LEDs and the output of appropriate **show** commands can help you determine the state of the physical link between a switch port and a router's Fast Ethernet interface. Also make sure that the correct media type is specified (if applicable).
- Make sure that the router and the switch are both configured for the same speed and duplexing mode.
- Make sure that the router's Fast Ethernet interface has the correct subinterfaces and VLANs configured on it. On each subinterface, make sure that the network layer addressing or any bridging commands are appropriately configured.
- Those VLANs that do not need to be relayed to the router should be taken out of the trunk (with the **clear trunk** command).
- Make sure that the Spanning-Tree Protocol configured on the router matches the spanning tree of the connected switch.

Foundation Summary

The Foundation Summary is a collection of quick reference information that provides a convenient review of many key concepts in this chapter. For those of you who already feel comfortable with the topics in this chapter, this summary helps you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For any of you doing your final prep before the exam, these tables and figures are a convenient way to review the day before the exam.

Example 9-8 *Sample Configuration for the Fast Ethernet Interface of a Router*

```
interface FastEthernet0
 no ip address
 media-type mii
 full-duplex
!
interface FastEthernet0.1
 encapsulation isl 1
 ip address 10.1.1.44 255.255.0.0
 ipx network 36dd
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.1.40 255.255.0.0
 bridge-group 60
 !
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.1.40 255.255.0.0
  bridge-group 60
!
```

Table 9-2 *Default Values for the IEEE Spanning-Tree Protocol Timers*

Parameter	Default Value
HELLO	2
MAX_AGE	20
Fwddelay	15
Convergence	50
MAX_AGE + Listening (fwddelay) + Learning (fwddelay)	

Table 9-3 *Default VLANs on a Catalyst 5000 Family Switch*

VLAN Name	Type	MTU	ISL VLAN-id	802.10 SAID
Default	Ethernet	1500	0001	100001
Fddi-default	FDDI	4352	1002	101002
Token-ring-default	Token Ring	2048	1003	101003
Fddinet-default	FDDI-net	4352	1004	101004
Trnet-default	Tr-net	2048	1005	101005

Table 9-4 *Router VLAN Diagnostic Tools: **show** Commands*

Command	Description
show vlans	Lists all the VLANs configured on a router. For each VLAN, the corresponding subinterface and its configured addresses are displayed.
show span [*vlan-number*]	Shows the Spanning-Tree Protocol information known to the router. The first part of this command's output shows the type of Spanning-Tree Protocol in use, the bridge ID (priority and address) of the local device (the router), the ID of the root device, and the timer parameters of the spanning tree. Next, the interfaces that participate in the spanning tree (associated with the VLAN number typed in) are listed.
show bridge [*bridge-number*]	Displays contents of your router's bridge forwarding database for all the bridge groups defined.

Table 9-5 *Router VLAN Diagnostic Tools: **debug** Commands*

Command	Description
debug vlan packets	The **debug vlan packet** command displays messages about virtual LAN (VLAN) packets that the router receives (off the trunk connection) but is not configured to support.
debug span tree	Displays messages about the BPDU packets that the router is receiving (in text format).
debug span events	Displays the BPDU packets that the router is receiving (in its raw format).

Q&A

The answers to the following questions can be found in Appendix A. Some of the questions in this section are repeated from the "Do I Know This Already" Quiz so that you can gauge the advancement of your knowledge of this subject matter.

1 Name three of the functions routers perform in a VLAN switching environment.

2 Which type of router interface is used for ISL trunking?

3 True or false: If a Fast Ethernet interface is used for trunking purposes, it should not have any Layer 3 address or any bridging commands configured on the main interface.

4 How many VLANs can a subinterface of an interface used for trunking correspond to?

5 Which command functions are configured on the main interface of the interface used for trunking?

6 What IOS command configures a multiport Fast Ethernet interface to operate from its RJ45 (100BaseTX) connector?

7 What IOS command configures a multi-port Fast Ethernet interface to operate in full-duplex mode?

8 Which command shows the media type configured on a Fast Ethernet interface?

9 Which command would configure a subinterface of a Fast Ethernet interface to be in VLAN number 10 (in ISL format)?

10 Routing between VLANs is supported for which protocols on Cisco 4500 and 7000 series routers running IOS Release 11.3?

11 What is the general rule for the bridged networks in terms of the number of hops?

12 What is the default HELLO interval in the IEEE Spanning-Tree Protocol?

13 What is the default MAX_AGE interval in the IEEE Spanning-Tree Protocol?

14 What is the default fwddelay interval in the IEEE Spanning-Tree Protocol?

15 What is the maximum convergence time of the IEEE Spanning-Tree Protocol in a network with a seven-hop diameter and default IEEE spanning tree timer values?

16 How many default VLANs are preconfigured on a Catalyst 5000 switch?

17 What is the recommended usage of VLAN number 1?

18 What are the possible implications of using different (inconsistent) Spanning-Tree Protocols for a VLAN in the same network?

19 What is the suggested setting for the spanning tree timers during periods of instability?

20 What role can a Cisco router play in a VTP domain?

21 What information can one obtain from the output of the **show vlans** command?

22 Describe the output of the **show span** ***vlan-number*** command.

23 Discuss the output of the **show bridge** [*bridge-number*] command.

24 What messages does the **debug vlan packets** command display?

25 What are the two forms of the Cisco IOS's **debug span** command?

Cisco Interactive Mentor

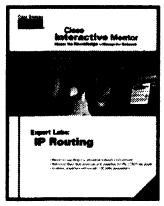
The Cisco Interactive Mentor (CIM) product line is a series of e-learning solutions designed to provide entry-level networking professionals with the opportunity to gain practical, hands-on experience through self-paced instruction and network lab simulation exercises. This combination of computer-based training with lab exercises offers users a unique learning environment that eliminates the cost overhead necessary with the actual network devices, while offering the same degree of real-world experience. Current releases include the following:

Internetworking Basics
1-58720-034-1
$99.95
AVAILABLE JUNE 2001

LAN Switching
1-58720-021-X
$199.95
AVAILABLE NOW

IP Routing: Distance-Vector Protocols
1-58720-012-0
$149.95
AVAILABLE NOW

Access ISDN
1-58720-025-2
$199.95
AVAILABLE NOW

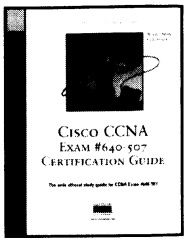


Expert Labs: IP Routing
1-58720-010-4
$149.95
AVAILABLE NOW

Voice Internetworking: Basic Voice over IP
1-58720-023-6
$149.95
AVAILABLE NOW

For an online demo of the CIM product line, go to www.ciscopress.com/cim today!

Cisco Career Certifications

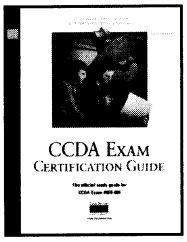


Cisco CCNA Exam #640-507 Certification Guide

Wendell Odom

0-7357-0971-8 • **AVAILABLE NOW**

Although it's only the first step in Cisco Career Certification, the Cisco Certified Network Associate (CCNA) exam is a difficult test. Your first attempt at becoming Cisco certified requires plenty of study and confidence in your networking knowledge. When you're ready to test your skills, complete your knowledge of the exam topics, and prepare for exam day, you need the preparation tools found in *Cisco CCNA Exam #640-507 Certification Guide.*

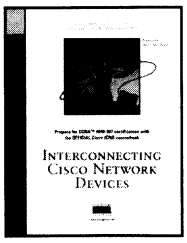


CCDA Exam Certification Guide

Anthony Bruno

0-7357-0074-5 • **AVAILABLE NOW**

CCDA Exam Certification Guide is a comprehensive study tool for DCN Exam #640-441. Written by a CCIE and a CCDA, and reviewed by Cisco technical experts, CCDA Exam Certification Guide helps you understand and master the exam objectives. In this solid review on the design areas of the DCN exam, you learn to design a network that meets a customer's requirements for performance, security, capacity, and scalability.

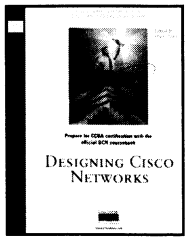


Interconnecting Cisco Network Devices

Edited by Steve McQuerry

1-57870-111-2 • **AVAILABLE NOW**

Based on the Cisco course taught worldwide, Interconnecting Cisco Network Devices teaches you how to configure Cisco switches and routers in multiprotocol internetworks. ICND is the primary course recommended by Cisco Systems for CCNA #640-507 preparation. If you are pursuing CCNA certification, this book is an excellent starting point for your study.



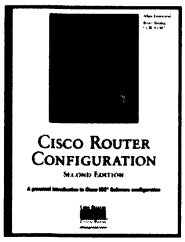
Designing Cisco Networks

Edited by Diane Teare

1-57870-105-8 • **AVAILABLE NOW**

Based on the Cisco Systems instructor-led and self-study course available worldwide, *Designing Cisco Networks* teaches you how to become proficient in network design methodologies. Created for those seeking to attain CCDA certification, this book focuses on small- to medium-sized networks and provides a step-by-step process to follow when designing internetworks to ensure that all the important issues are considered, resulting in optimal network design.

Cisco Press Solutions

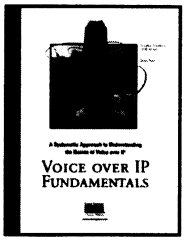


Cisco Router Configuration, Second Edition

Allan Leinwand and Bruce Pinsky

1-57870-241-0 • AVAILABLE NOW

Cisco Router Configuration, Second Edition, takes an example-oriented and chronological approach to helping you implement and administer your internetworking devices. Starting with the configuration of devices out of the box, this book moves to configuring the Cisco IOS for the three most popular networking protocols used today: Transmission Control Protocol/Internet Protocol (TCP/IP), AppleTalk, and Novell InterPacket eXchange (IPX). You also learn basic administrative and management configuration, including access control with TACACS+ and RADIUS, network management with SNMP, logging of messages, and time control with NTP. *Cisco Router Configuration*, Second Edition, is updated from the previous edition for many new features and configuration commands in Cisco IOS 12.1T. Updated in this edition are solutions for configuring Cisco IOS software for Gigabit Ethernet LANs, Digital Subscriber Line (DSL) networks, DHCP services and Secure Shell (SSH) access IOS devices.

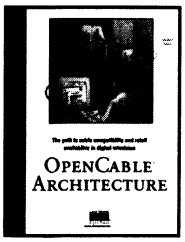


Voice over IP Fundamentals

Jonathan Davidson and Jim Peters

1-57870-168-6 • AVAILABLE NOW

This book provides you with a thorough introduction to the voice and data technology. You learn how the telephony infrastructure was built and how it works today. You also gain an understanding of the major concepts concerning voice and data networking, transmission of voice over data, and IP signaling protocols used to interwork with current telephony systems.



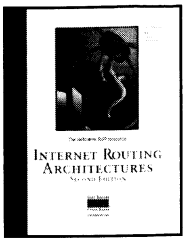
OpenCable Architecture

Michael Adams

1-57870-135-X • AVAILABLE NOW

This award-winning book explains key concepts in practical terms. It describes the digital headend, optical transport, distribution hub, hybrid-fiber coax, and set-top terminal equipment and how these components are interconnected. Whether you are a television, data communications, or telecommunications professional, or an interested layperson. *OpenCable Architecture* helps you understand the technical and business issues surrounding interactive television services. It provides you with an inside look at the combined efforts of the cable, data, and consumer electronics industries to develop those new services.

Cisco Press Solutions

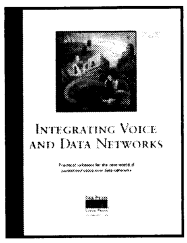


Internet Routing Architectures, Second Edition

Sam Halabi and Danny McPherson

1-57870-233-x • Available Now

Internet Routing Architectures, Second Edition, explores the ins and outs of interdomain routing network designs with emphasis on BGP-4—the de facto interdomain routing protocol. The comprehensive resource provides you with real solutions for ISP connectivity issues. You learn how to integrate your network on the global Internet and discover how to build large-scale autonomous systems. You also learn to control expansion of interior routing protocols using BGP-4, design sound and stable networks, configure the required policies using Cisco IOS Software, and explore routing practices and rules on the Internet.

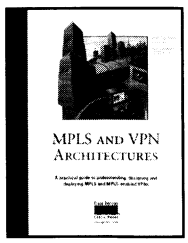


Integrating Voice and Data Networks

Scott Keagy

1-57870-196-1 • **AVAILABLE NOW**

Integrating Voice and Data Networks is both a conceptual reference and a practical how-to book that bridges the gap between existing telephony networks and the new world of packetized voice over data networks. Underlying technologies are explained in a context that gives a holistic understanding of voice/data integration. You then follow a complete process to design and implement a variety of network scenarios, leveraging author Scott Keagy's extensive experience with real voice/data networks. This book focuses on the implementation of Voice over Frame Relay, Voice over ATM, and Voice over IP using Cisco IOS voice gateways, including the Cisco MC3810, Cisco 2600/3600/7200/7500 series routers, and AS5300/AS5800 Access Servers.



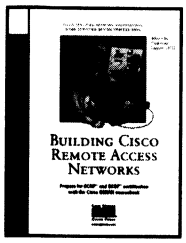
MPLS and VPN Architectures

Ivan Pepelnjak and Jim Guichard

1-57870-002-1 • **AVAILABLE NOW**

This book provides an in-depth study of MPLS technology, including MPLS theory and configuration, network design issues, and case studies. The MPLS/VPN architecture and all its mechanisms are explained with configuration examples and suggested deployment guidelines. MPLS and VPNs provides the first in-depth discussion particular to Cisco's MPLS architecture. Multiprotocol Label Switching and Virtual Private Networks covers MPLS theory and configuration, network design issues, and case studies as well as one major MPLS application: MPLS-based VPNs. The MPLS/VPN architecture and all its mechanisms are explained with configuration examples, suggested design and deployment guidelines, and extensive case studies.

Cisco Career Certifications

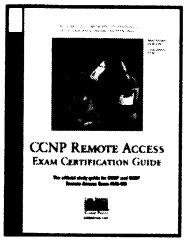


Building Cisco Remote Access Networks

Cisco Systems, Inc., Edited by Catherine Paquet

1-57870-091-4 • AVAILABLE NOW

Based on the Cisco Systems instructor-led course available worldwide, *Building Cisco Remote Access Networks* teaches you how to design, set up, configure, maintain, and scale a remote access network using Cisco products. In addition, *Building Cisco Remote Access Networks* provides chapter-ending questions to help you assess your understanding of key concepts and start you down the path for attaining your CCNP certification.

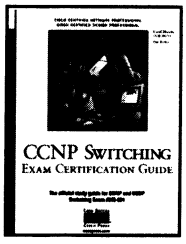


CCNP Remote Access Exam Certification Guide

Brian Morgan, CCIE #4865, and Craig Dennis

1-58720-003-1 • AVAILABLE NOW

CCNP Remote Access Exam Certification Guide is a comprehensive study tool for the Cisco Certified Network Professional Remote Access Exam #640-505. The exam evaluates your ability to build a remote access network to interconnect central sites to branch offices and home office/telecommuters, control access to the central site, as well as maximize bandwidth utilization over the remote links. This book provides you with concise reviews of all the major topics covered on the Remote Access Exam. You gain full mastery of all the concepts and technologies upon which you will be tested, including selecting the proper equipment, assembling and cabling WAN components, configuring asynchronous connections with modems, configuring PPP and controlling network access, using ISDN and DDR, establishing X.25 and Frame Relay connections, managing network performance, scaling IP addresses with NAT, and monitoring the access and use of the network with AAA. The book also includes a comprehensive testing engine on CD-ROM.



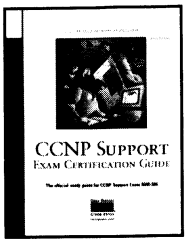
CCNP Switching Exam Certification Guide

David Hucaby, CCIE #4594, and Tim Boyles

1-58720-000-7 • AVAILABLE NOW

CCNP Switching Exam Certification Guide is a comprehensive study tool for the Cisco Certified Network Professional Switching Exam #640-504. The exam evaluates your ability to build campus networks using multilayer switching technologies and to manage campus network traffic. This book provides you with concise reviews of all the major topics covered on the Switching Exam. You gain full mastery of all the concepts and technologies upon which you will be tested, including switched Ethernet, trunking, multicasting, multilayer switching, VLANs, ATM, LANE, interVLAN routing, HSRP, network traffic control, and monitoring and troubleshooting techniques. This book also includes a comprehensive testing engine on CD-ROM.

Cisco Career Certifications

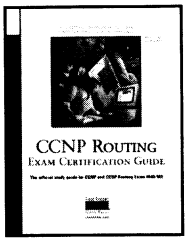


CCNP Support Exam Certification Guide

Amir Ranjbar

0-7357-0995-5 • AVAILABLE NOW

Cisco Support Exam Certification Guide is a comprehensive study tool for the Cisco Certified Network Professional Support Exam #640-506. The exam evaluates your ability to diagnose, isolate, and correct network problems in a variety of environments. This book provides you with concise reviews of all the major topics covered on the Support Exam. You gain full mastery of all the concepts and technologies upon which you will be tested, including troubleshooting resources, tools, and methodology, understanding data-link layer troubleshooting, fast switching methods, and buffering technologies, network layer protocol troubleshooting, troubleshooting Catalyst 5000 switches, and troubleshooting WAN connections. This book also includes a comprehensive testing engine on CD-ROM.

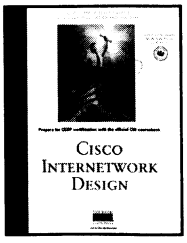


CCNP Routing Exam Certification Guide

Clare Gough

1-58720-001-5 • AVAILABLE NOW

CCNP Routing Exam Certification Guide is a comprehensive study tool for the Cisco Certified Network Professional Routing Exam #640-503. The exam evaluates you ability to support and implement scalable routed internetworks for any size environment. This book provides you with concise reviews of all the major topic areas and objectives for the Routing exam. You gain full mastery of all the concepts and technologies upon which you will be tested, including principles of scalable internetworks, scalable routing protocols, managing traffic and access, and optimizing scalable internetworks. This book also includes a comprehensive testing engine on CD-ROM.



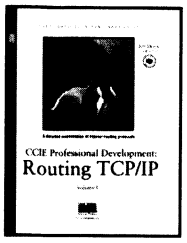
Cisco Internetwork Design

Cisco Systems, Inc., Edited by Matthew H. Birkner, CCIE

1-57870-171-6 • AVAILABLE NOW

Based on the Cisco Systems instructor-led course available worldwide, *Cisco Internetwork Design* teaches you how to plan and design a network using various internetworking technologies. Created for those seeking to attain CCDP certification, this book presents the fundamental, technical, and design issue associated with campus LANs; TCP/IP networks; IPX, AppleTalk, and Windows-based networks; WANs, and SNA networks.

CCIE Professional Development

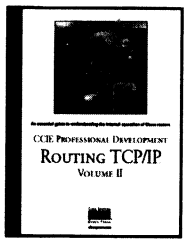


Routing TCP/IP, Volume I

Jeff Doyle, CCIE

1-57870-041-8 • AVAILABLE NOW

Routing TCP/IP, Volume I, takes the reader from a basic understanding of routers and routing protocols through a detailed examination of each of the IP interior routing protocols. Learn techniques for designing networks that maximize the efficiency of the protocol being used. Exercises and review questions provide core study for the CCIE Routing and Switching exam.

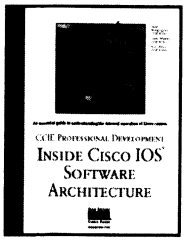


Routing TCP/IP, Volume II

Jeff Doyle, CCIE

1-57870-089-2 • AVAILABLE NOW

Routing TCP/IP, Volume II, presents a detailed examination of exterior routing protocols (EGP and BGP) and advanced IP routing issues, such as multicast routing, quality of service routing, IPv6, and router management. Readers learn IP design and management techniques for implementing routing protocols efficiently. Network planning, design, implementation, operation, and optimization are stressed in each chapter. Cisco-specific configurations for each routing protocol are examined in detail. Plentiful review questions and configuration and troubleshooting exercises make this an excellent self-study tool for CCIE exam preparation.



Inside Cisco IOS Software Architecture

Vijay Bollapragada, CCIE; Curtis Murphy, CCIE; and Russ White, CCIE

1-57870-181-3 • AVAILABLE NOW

Part of the Cisco CCIE Professional Development Series, *Inside Cisco IOS Software Architecture* offers crucial and hard-to-find information on Cisco's Internetwork Operating System (IOS) Software. This book begins with an overview of operating system concepts and the IOS software infrastructure, then delves into the intricate details of the design and operation of platform specific features, including the 1600, 2500, 4x00, 3600, 7200, 7500, and GSR Cisco Routers, and ends with an overview of IOS quality of service.

Cisco Press

Cisco Press books are available at your local bookstore, computer store, and online booksellers.