

ICND1

Interconnecting Cisco Networking Devices, Part 1

Volume 1

Version 2.0

Student Guide

Part Number: 97-3242-01



Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV
Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Welcome Students

Note Students, this letter describes important course evaluation access information.

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise that you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions; therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. Please complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL directing you to a short postcourse evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,
Cisco Systems Learning

Do Not Duplicate
Post beta, not for release

The Cisco M-Learning Test and Study App

The Cisco M-Learning Test and Study app is the ideal on-the-go study application for those preparing for Cisco certifications.

Scan the following QR code to get the free Cisco M-Learning Test and Study app along with the 20 free exam questions and free TCP/IP Architecture video.

**Scan the code to get
the iPhone M-Test app**



Do Not Duplicate
Post beta, not for release.

Table of Contents

Course Introduction	11
Overview	11
Course Goal and Objectives	12
Course Flow	13
Your Training Curriculum	14
Additional References	17
Building a Simple Network	11
Exploring the Functions of Networking	13
What Is a Network?	14
Physical Components of a Network	16
Interpreting a Network Diagram	17
Impact of User Applications on the Network	18
Characteristics of a Network	19
Physical vs. Logical Topologies	111
Summary	113
Understanding the Host-to-Host Communications Model	115
Introducing Host-to-Host Communications	116
OSI Reference Model	118
TCP/IP Protocol Suite	120
Encapsulation and De-Encapsulation	121
Peer-to-Peer Communications	123
Summary	124
Introducing LANs	125
Local Area Networks	126
LAN Components	127
Need for Switches	129
Switches	131
Summary	132
Operating Cisco IOS Software	133
Cisco IOS Software Features and Functions	134
Cisco IOS CLI Functions	135
User EXEC Mode	136
Privileged EXEC Mode	137
Help Functions in the CLI	138
CLI Error Messages	140
Managing Cisco IOS Configurations	142
Improving the User Experience in the CLI	147
Summary	150
Starting a Switch	151
Switch Installation	152
Switch LED Indicators	153
Connecting to a Console Port	154

Basic Switch Configuration	156
Verifying the Switch Initial Startup Status	159
Summary	162
Understanding Ethernet and Switch Operation	163
Ethernet LAN Connection Media	164
Ethernet Frame Structure	170
MAC Addresses	171
Switching Operation	174
Duplex Communication	176
Configuring Duplex and Speed Options	178
Summary	181
Troubleshooting Common Switch Media Issues	183
Common Troubleshooting Tools	184
Media Issues	186
Troubleshooting Switch Media Issues	188
Port Issues	192
Troubleshooting Port Issues	195
Summary	197
Module Summary	199
Module Self-Check	1101
<i>Establishing Internet Connectivity</i>	21
Understanding the TCP/IP Internet Layer	23
Internet Protocol	24
IPv4 Address Representation	26
IPv4 Header Address Fields	27
Decimal and Binary Systems	28
Decimal-to-Binary Conversion	29
IP Address Classes	211
Reserved IPv4 Addresses	213
Domain Name System	215
Verifying the IPv4 Address of a Host	216
Summary	218
Understanding IP Addressing and Subnets	219
Subnets	220
Subnet Masks	222
Octet Values of a Subnet Mask	224
Default Gateways	227
Computing Usable Subnetworks and Hosts	229
Applying Subnet Masks	231
Determining the Network Addressing Scheme	233
Example: Addressing Scheme	237
Variable-Length Subnet Mask	239
VLSM Example	241
Summary	244

Understanding the TCP/IP Transport Layer	245
TCP/IP Transport Layer Functions	247
Reliable vs. Best-Effort Transport	249
TCP vs. UDP Analogy	251
UDP Characteristics	252
TCP Characteristics	254
TCP/IP Applications	256
Summary	258
Exploring the Functions of Routing	259
Role of a Router	260
Router Characteristics	261
Router Functions	263
Path Determination	265
Routing Table	266
Types of Routes	267
Dynamic Routing Protocols	269
Summary	271
Configuring a Cisco Router	273
Initial Router Startup	274
Initial Router Setup	275
Configuring Router Interfaces	276
Configuring the Cisco Router IP Address	278
Verifying Interface Configuration and Status	279
Exploring Connected Devices	282
Cisco Discovery Protocol	283
Discovering Neighbors Using Cisco Discovery Protocol	284
Summary	286
Exploring the Packet Delivery Process	287
Layer 2 Addressing	288
Layer 3 Addressing	290
Address Resolution Protocol	292
Host-to-Host Packet Delivery	295
Role of a Switch in Packet Delivery	2104
Summary	2107
Enabling Static Routing	2109
Routing Operations	2110
Static and Dynamic Routing Comparison	2112
When to Use Static Routing	2113
Static Route Configuration	2114
Default Routes	2116
Static Route Configuration Verification	2118
Summary	2120
Managing Traffic Using ACLs	2121
Using ACLs	2122
ACL Operation	2123

ACL Wildcard Masking	2124
Wildcard Bit Mask Abbreviations	2127
Types of ACLs	2128
Testing an IP Packet Against a Numbered Standard Access List	2130
Basic Configuration of Numbered Standard IPv4 ACLs	2131
Summary	2133
Enabling Internet Connectivity	2135
The Demarcation Point	2137
Dynamic Host Configuration Protocol	2138
Options for Configuring a Provider-Assigned IP Address	2140
Configuring a Static Provider-Assigned IP Address	2141
Configuring a DHCP Client	2142
Public vs. Private IPv4 Addresses	2143
Introducing NAT	2145
Types of Addresses in NAT	2147
Types of NAT	2149
Understanding Static NAT	2150
Configuring Static NAT	2151
Verifying Static NAT Configuration	2152
Understanding Dynamic NAT	2153
Configuring Dynamic NAT	2155
Verifying Dynamic NAT Configuration	2156
Understanding PAT	2157
Configuring PAT	2159
Verifying PAT Configuration	2160
Troubleshooting NAT	2161
Troubleshooting NAT Case Study	2165
Summary	2169
Module Summary	2171
Module Self-Check	2173
<i>Managing Network Device Security</i>	<i>31</i>
Securing Administrative Access	33
Network Device Security Overview	34
Securing Access to Privileged EXEC Mode	35
Securing Console Access	37
Securing Remote Access	38
Enabling Remote Access Connectivity	311
Limiting Remote Access with ACLs	312
External Authentication Options	313
Configuring the Login Banner	314
Summary	315
Implementing Device Hardening	317
Securing Unused Ports	318
Port Security	320

Port Security Configuration	323
Port Security Verification	325
Disabling Unused Services	328
Network Time Protocol	331
Configuring NTP	333
Verifying NTP	334
Summary	335
Implementing Traffic Filtering with ACLs	337
Using ACLs to Filter Network Traffic	338
ACL Operation	339
Applying ACLs to Interfaces	340
The Need for Extended ACLs	342
Configuring Numbered, Extended IPv4 ACLs	344
Configuring Named ACLs	346
ACL Configuration Guidelines	348
Monitoring ACLs	349
Troubleshooting Common ACL Errors	350
Summary	357
Module Summary	359
Module Self-Check	361
<i>Building a Medium-Sized Network</i>	41
Implementing VLANs and Trunks	43
Issues in a Poorly Designed Network	44
VLAN Introduction	46
Trunking with 802.1Q	47
Creating a VLAN	411
Assigning a Port to a VLAN	413
Configuring an 802.1Q Trunk	416
VLAN Design Considerations	418
Physical Redundancy in a LAN	420
Summary	422
Routing Between VLANs	423
Purpose of Inter-VLAN Routing	423
Options for Inter-VLAN Routing	425
Configuring a Router with a Trunk Link	428
Summary	431
Using a Cisco Network Device as a DHCP Server	433
Need for a DHCP Server	433
Understanding DHCP	435
Configuring a DHCP Server	436
Monitoring DHCP Server Functions	438
DHCP Relay Agent	441
Summary	443
Introducing WAN Technologies	445

Introducing WANs	445
WANs vs. LANs	448
Role of Routers in WANs	450
WAN Communication Link Options	451
Point-to-Point Connectivity	452
Configuring a Point-to-Point Link	453
Summary	454
Introducing Dynamic Routing Protocols	455
Purpose of Dynamic Routing Protocols	455
Interior and Exterior Routing Protocols	458
Distance Vector and Link-State Routing Protocols	459
Understanding Link-State Routing Protocols	461
Summary	464
Implementing OSPF	465
Introducing OSPF	465
OSPF Adjacencies	467
SPF Algorithm	469
Router ID	471
Configuring Single-Area OSPF	473
Verifying OSPF Configuration	476
Summary	480
Module Summary	481
Module Self-Check	483
<i>Introducing IPv6</i>	51
Introducing Basic IPv6	53
IPv4 Addressing Exhaustion Workarounds	54
IPv6 Features	56
IPv6 Addresses	57
IPv6 Unicast Addresses	59
IPv6 Addresses Allocation	512
Basic IPv6 Connectivity	513
Summary	516
Understanding IPv6	517
IPv6 Header Changes and Benefits	518
ICMPv6	520
Neighbor Discovery	521
Stateless Autoconfiguration	522
Summary	525
Configuring IPv6 Routing	527
Routing for IPv6	528
Static Routing	530
OSPFv3	533
Summary	537
Module Summary	539

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Course Introduction

Overview

You may be asking yourself, “What do I need to know to support my network?” The answer to this question depends on the size and complexity of the network. Regardless of its size and complexity, the starting point for learning to support a network is the same. This course is intended to be that starting point. This course focuses on providing the skills and knowledge necessary to implement and operate a small- to medium-sized network.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course.

Learner Skills and Knowledge

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic Internet usage skills
- Basic IP addressing knowledge

Course Goal and Objectives

This topic describes the course goal and objectives.

Course Goal

To provide students with the knowledge and skills necessary to install, configure, and operate small- to medium-sized networks.

© 2013 Cisco Systems, Inc.

Upon completing this course, you will be able to meet these objectives:

- Describe network fundamentals and build simple LANs
- Establish Internet connectivity
- Manage network device security
- Expand small- to medium-sized networks with WAN connectivity
- Describe IPv6 basics

Course Flow

This topic presents the suggested flow of the course materials.

Course Flow					
	Day 1	Day 2	Day 3	Day 4	Day 5
AM	Course Introduction Building a Simple Network	Establishing Internet Connectivity	Managing Network Device Security	Building a Medium-Sized Network	Introducing IPv6
	LUNCH				
PM	Building a Simple Network (Cont.)	Establishing Internet Connectivity (Cont.)	Managing Network Device Security (Cont.)	Building a Medium-Sized Network (Cont.)	ICND1 Superlab

© 2013 Cisco Systems, Inc.

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Your Training Curriculum

This topic presents the training curriculum for this course.

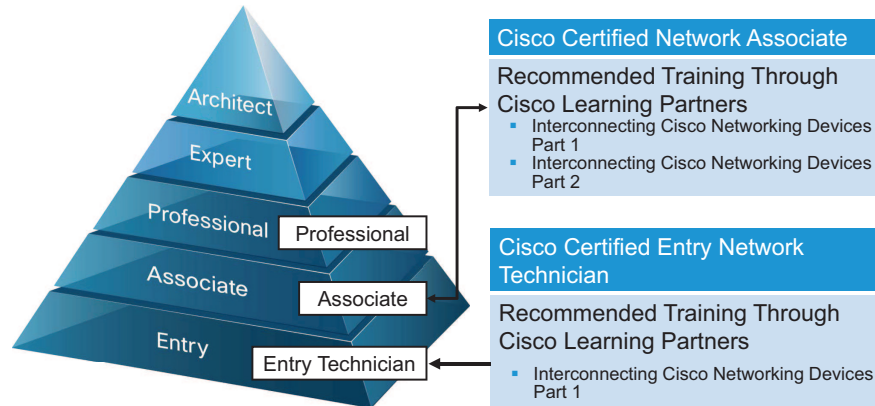
Additional information is available at <http://learningnetwork.cisco.com>.



You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE[®], CCNA R&S[®], CCDA[®], CCNP[®], CCDP[®], CCNP Security[®], and CCNP Voice[®], and others). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit <http://www.cisco.com/go/certifications>.

Cisco Career Certifications

Expand Your Professional Options, Advance Your Career.



© 2013 Cisco Systems, Inc.

CCNA Prep Center

Save on Cisco CCNA Study

Get the Cisco CCNA Premium Study Bundle and save up to 37 percent.

New to Certifications? What best describes your background?

Start a Networking Career | Military | Student | Professional

CERTIFICATIONS HIGHLIGHTS

View Certifications, review our study and practice materials or join a Study Group.

- ▶ Introducing the new CCNA Data Center and CCNP Data Center certifications.
- ▶ Schedule your CCIE Data Center lab exams now. Avoid the rush.
- ▶ Now Available On-demand - The Essentials of CCDE Webinar: Access Now.
- ▶ CCIE Security written and lab exams v4.0 now available for registration
- ▶ Review the updated score reporting process for the CCDE practical exam.
- ▶ Retirement of CCIP Certification

LEARNING NEWS

Information on the latest happenings on the site.

- ▶ What is the IT industry demanding? View this video to find out.
- ▶ Congratulations to our new Community Spotlight Award recipients!
- ▶ Check out the Games Arcade, Cisco Learning Network's November Page of the Month
- ▶ New Users Getting Started Guide and Video Tour
- ▶ Now Available on Demand: Cisco Exam Preparation - Studying for Results

Latest Poll

Is Cisco Learning Network meeting your expectations?

Strongly Agree (46%)
Votes: 58/129

Agree (35%)
Votes: 68/199

Somewhat Agree (10%)
Votes: 29/189

© 2013 Cisco Systems, Inc.

<http://learningnetwork.cisco.com>

Learner Introductions

Learner Introductions

- Your name
- Your company
- Job responsibilities
- Skills and knowledge
- Brief history
- Objective

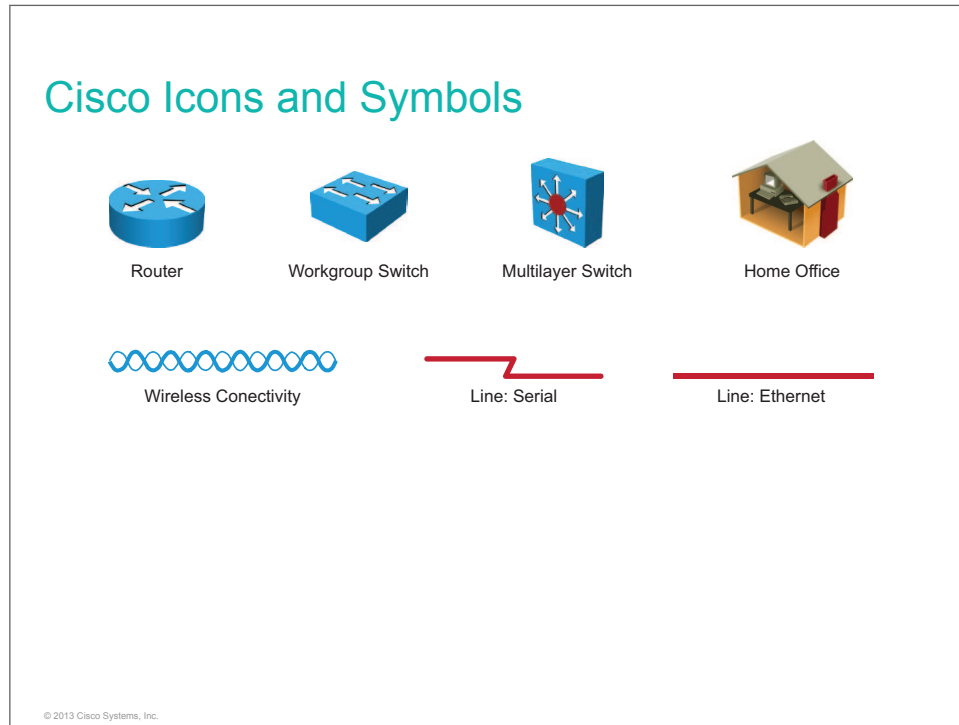


© 2013 Cisco Systems, Inc.

Do Not Duplicate
Post beta, not for

Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information on where to find additional technical references.



Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the Cisco Internetworking Terms and Acronyms glossary of terms at

[http://doewiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_\(ITA\)](http://doewiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)).

Do Not Duplicate.
Post beta, not for release.

Building a Simple Network

This module provides a high-level overview of basic networking components and their functions. The need for a communication module is explained, followed by an overview of the TCP/IP protocol stack. Cisco IOS Software is introduced, and its basic functions and features are described. Basic switch configuration is described, with configuration examples so that learners can perform switch startup and initial configuration in the associated lab. LANs are introduced, as well as the Ethernet standard. The operation and role of switches within LANs is described. Finally, the module provides an overview of common switch media issues and lists recommended troubleshooting steps.

Objectives

Upon completing this module, you will be able to meet these objectives:

- Identify the components of a computer network and describe their basic characteristics
- Understand the model of host-to-host communications
- Describe LANs and the role of switches within LANs
- Describe the features and functions of Cisco IOS Software
- Install a switch and perform the initial configuration
- Describe Ethernet as the network access layer of TCP/IP and describe the operation of switches
- Identify and resolve common switched network issues

Do Not Duplicate.
Post beta, not for release.

Exploring the Functions of Networking

Overview

Understanding the benefits of computer networks and how they function is important in maximizing communication channels among end users. This lesson describes the concept of computer networking, introduces the components of a computer network, and explains how users benefit from using networks.

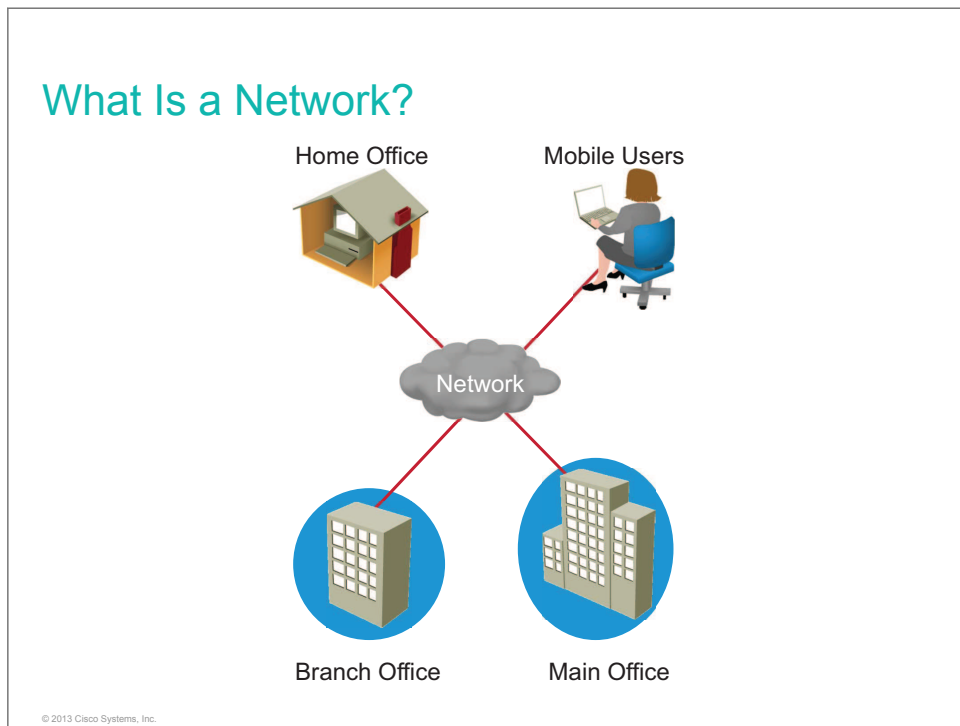
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Define a network and describe examples of networks
- Identify common networking components by function
- Interpret network diagrams
- Describe the impact of user applications on the network
- List the characteristics of a network
- Compare and contrast logical and physical topologies

What Is a Network?

This topic provides examples of networks and describes their characteristics.



A network is a connected collection of devices and end systems, such as computers and servers, which can communicate with each other. Networks carry data in many types of environments, including homes, small businesses, and large enterprises. Large enterprise networks may have a number of locations that need to communicate with each other. Based on where workers are situated, these locations are as follows:

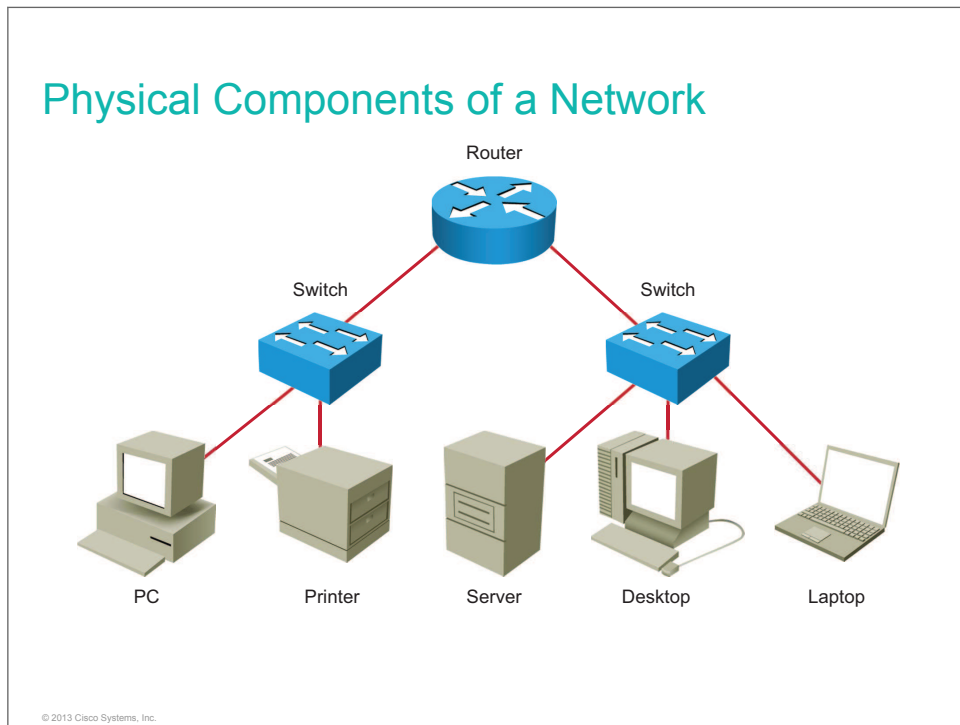
- **Main office:** A main office is a site where everyone is connected via a network and where most corporate information is located. A main office can have hundreds or even thousands of people who depend on network access to do their jobs. A main office may use several connected networks that can span many floors in an office building or cover a campus that contains several buildings.
- **Remote locations:** A variety of remote access locations use networks to connect to the main office or to each other.
 - **Branch offices:** In branch offices, smaller groups of people work and communicate with each other via a network. Although some corporate information may be stored at a branch office, it is more likely that branch offices have local network resources, such as printers, but must access information directly from the main office.
 - **Home offices:** When individuals work from home, the location is called a home office. Home-office workers often require on-demand connections to the main office or branch offices to access information or to use network resources such as file servers.
 - **Mobile users:** Mobile users connect to the main office network while at the main office, at the branch office, or traveling. The location of the mobile users determines their network access requirements.

You may use a network in your home office to communicate via the Internet to locate information, place orders for merchandise, and send messages to friends. You may also have a small office that is set up with a network that connects other computers and printers in the office. Similarly, you may work in a large enterprise with many computers, printers, storage devices, and servers that are used to communicate and store information from many departments over large geographic areas.

Do Not Duplicate.
Post beta, not for release.

Physical Components of a Network

This topic describes the typical physical components of a network, including PCs, interconnections, switches, and routers.

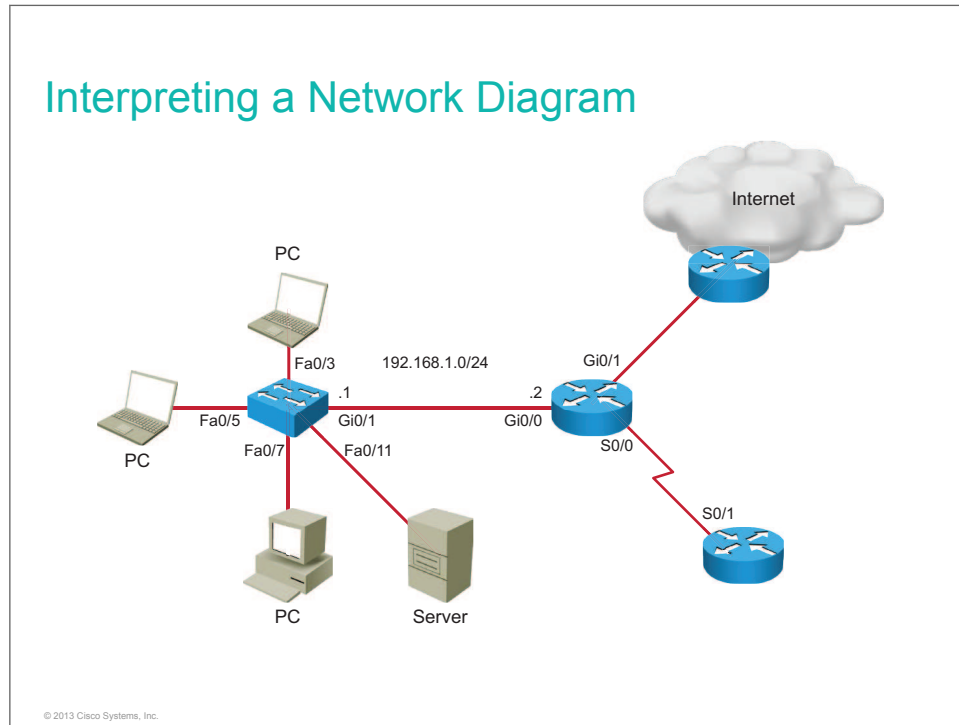


There are four major categories of physical components in a computer network:

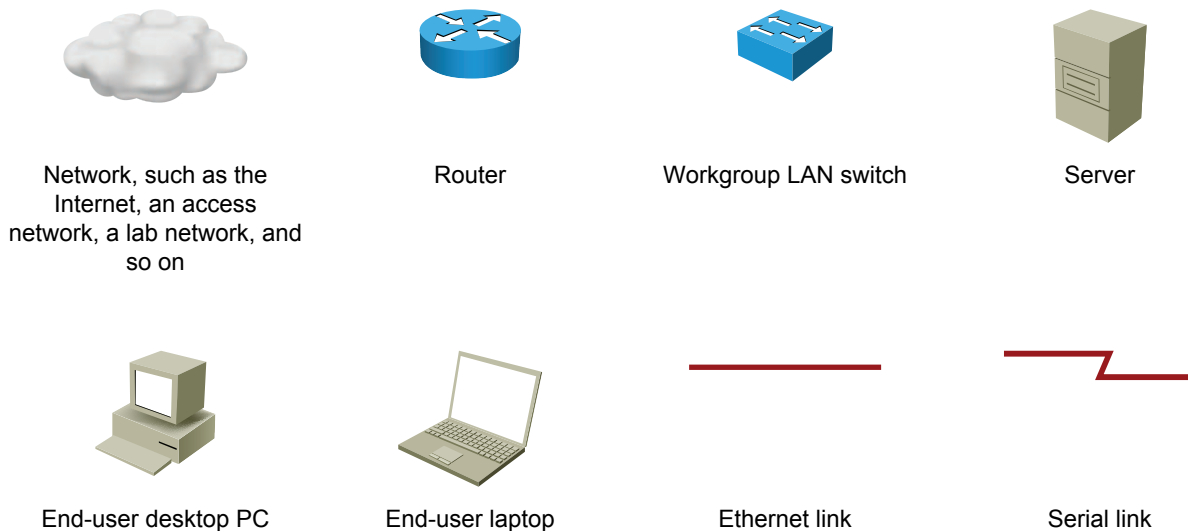
- **Endpoints:** Computers serve as endpoints in the network. They send and receive data. Printers and servers are also endpoints in the network.
- **Interconnections:** The interconnections consist of components that provide a means for data to travel from one point to another point in the network. Interconnections include components such as these:
 - NICs, which translate computer data into a format that can be transmitted over the local network
 - Network media, such as cables or wireless media, which provide the means by which signals are transmitted between networked devices
 - Connectors, which provide the connection points for the media
- **Switches:** Switches are devices that provide network attachment to the end systems and provide intelligent switching of the data within the local network.
- **Routers:** Routers interconnect networks and choose the best paths between networks.

Interpreting a Network Diagram

This topic describes the typical icons that represent the components of a network, including PCs, switches, and routers.



The network diagram captures network-related information. The amount of information and the detail differs from organization to organization. A series of lines and icons commonly represents the network topology. Some of the more common networking icons used in this diagram include the following:



Other information may be included in the network diagram if space allows. For example, it is common to identify the interface on a device in the S0/0/0 format for a serial interface, Fa0/0 for a Fast Ethernet interface, or Gi0/1 for a Gigabit Ethernet interface. It is also common to include the network address of the segment in the 192.168.1.0/24 format. In the example shown in the figure, 192.168.1.0 indicates the network address, /24 indicates the subnet mask, and .1 and .2 at the device ends indicate IP addresses on interfaces (.1 corresponds to 192.168.1.1).

Impact of User Applications on the Network

Applications can affect network performance and, conversely, network performance can affect applications. This topic describes common interactions between user applications and the network.

Impact of User Applications on the Network

- **Batch applications:**
 - FTP, TFTP, inventory updates
 - No direct human interaction
 - Bandwidth important, but not critical
- **Interactive applications:**
 - Inventory inquiry, database update
 - Human-to-machine interaction
 - Human waiting for response, response time important but not critical, unless wait becomes excessive
- **Real-time applications:**
 - VoIP, video
 - Human-to-human interaction
 - End-to-end latency critical

© 2013 Cisco Systems, Inc.

Historically, when considering the interaction between the network and applications that ran on the network, bandwidth was the main concern. Batch applications, such as FTP, TFTP, and inventory updates, were initiated by a user and then run to completion by the software, with no further direct human interaction. For batch applications, bandwidth was important but not critical, as long as the time needed for completion was not excessive. Interactive applications, such as inventory inquiries and database updates, required more human interaction. The user would request some type of information from the server and then wait for a reply. Bandwidth became more important because users became impatient with slow responses. However, because response time was more dependent on the server than on the network, bandwidth was still not critical. In most cases, QoS features could overcome bandwidth limitations by giving interactive applications preference over batch applications.

Like interactive applications, real-time applications such as VoIP and video applications involve human interaction. Because of the amount of information that is transmitted, bandwidth has become critical. In addition, because these applications are time-critical, latency (delay through the network) is critical. Variations in the amount of latency can affect the network. Not only is sufficient bandwidth mandatory, QoS is mandatory. VoIP and video applications must be given the highest priority.

Today, VoIP is promoted as a way for organizations to save money and is said to be as easy as installing a VoIP router into the network. While the benefits of VoIP are easily realized in the home network, VoIP can result in a disaster in a small-office network. Simply installing a VoIP router in a network does not ensure sufficient bandwidth, nor does it provide a proper QoS scheme. Applications that worked correctly in the past may begin to run so slowly that they are unusable when someone is on the phone. Additionally, voice quality may be poor. You can overcome both of these issues, bandwidth and QoS, with good network design.

Characteristics of a Network

This topic describes the characteristics of a network.

Characteristics of a Network

- Topology
- Speed
- Cost
- Security
- Availability
- Scalability
- Reliability

© 2013 Cisco Systems, Inc.

You can describe a network according to performance and structure:

- **Topology:** In networks, there are physical and logical topologies. The physical topology is the arrangement of the cables, network devices, and end systems. The logical topology is the path over which the data is transferred in a network. For example, a physical topology describes how the network devices are actually interconnected with wires and cables. A logical topology describes how the network devices appear connected to network users.
- **Speed:** Speed is a measure of the data rate in bits per second of a given link in the network.
- **Cost:** Cost indicates the general expense for the purchasing of network components and installation and maintenance of the network.
- **Security:** Security indicates how protected the network is, including the information that is transmitted over the network. The subject of security is important, and techniques and practices are constantly evolving. You should consider security whenever you take actions that affect the network.
- **Availability:** Availability is a measure of the probability that the network will be available for use when it is required. For networks that are meant to be used 24 hours per day, 7 days per week, 365 days per year, availability is calculated by dividing the time that it is actually available by the total time in a year and then multiplying by 100 to get a percentage.

For example, if a network is unavailable for 15 minutes per year because of network outages, you can calculate its percentage availability as follows:

$$([\text{Number of minutes in a year} - \text{down time}] / [\text{number of minutes in a year}]) * 100 = \text{percentage availability}$$

$$([525600 - 15] / [525600]) * 100 = 99.9971$$

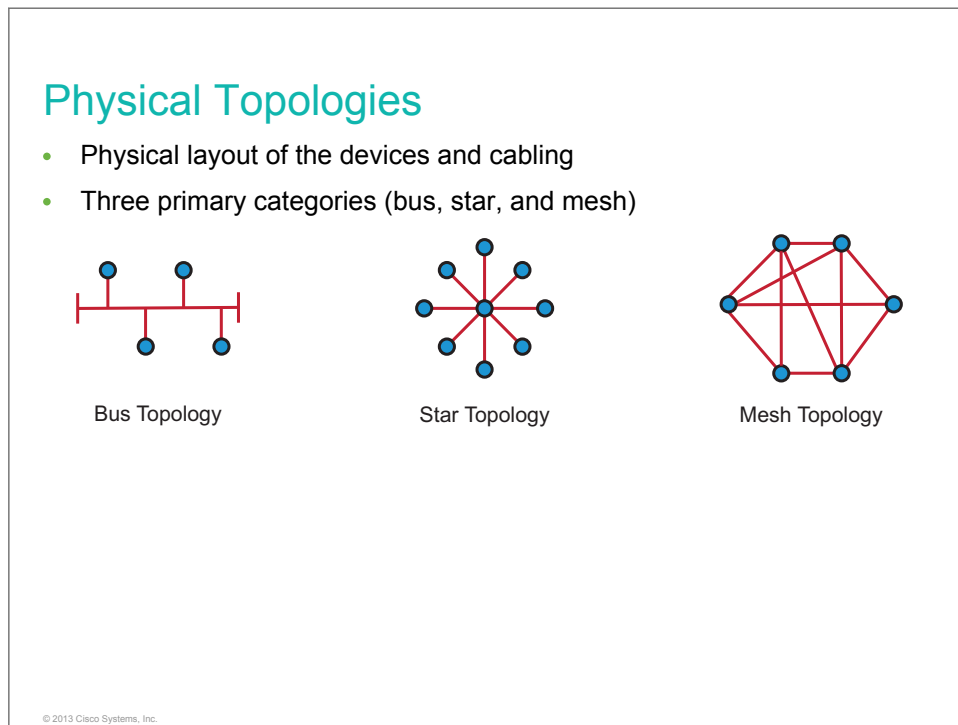
- **Scalability:** Scalability indicates how easily the network can accommodate more users and data transmission requirements. If you design and optimize a network for only the current requirements, it can be very expensive and difficult to meet new needs when the network grows.
- **Reliability:** Reliability indicates the dependability of the components that make up the network, such as the routers, switches, PCs, and servers. Reliability is often measured as a probability of failure or as MTBF.

These characteristics and attributes provide a means to compare various networking solutions.

Do Not Duplicate.
Post beta, not for release.

Physical vs. Logical Topologies

This topic describes the physical and logical topologies of networks.



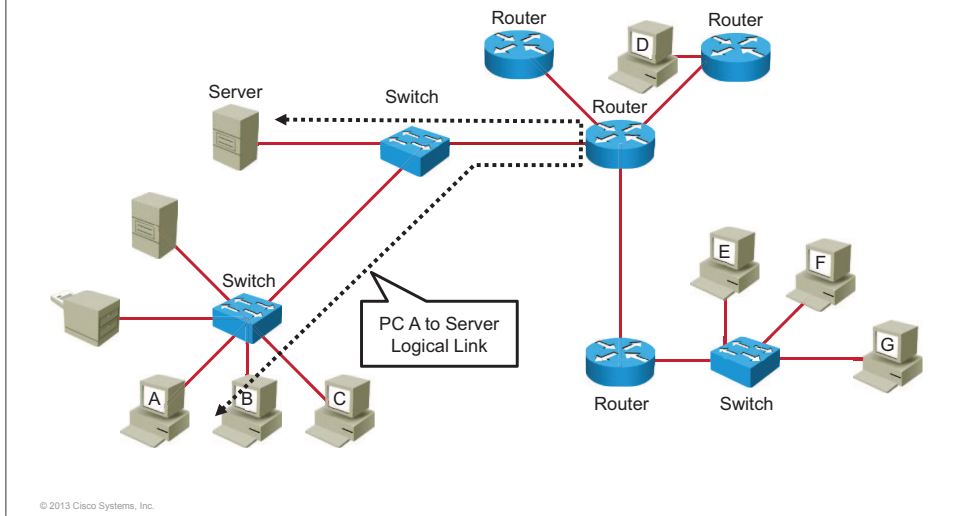
Each type of network has a physical and a logical topology.

The physical topology of a network refers to the physical layout of the devices and cabling. You must match the appropriate physical topology to the type of cabling that you will install, such as twisted pair, coaxial, or fiber. Understanding the type of cabling that is used is important in understanding each type of physical topology. These are the primary categories of physical topologies:

- **Bus:** In early bus topologies, computers and other network devices were cabled together in a line using coaxial cable. Modern bus topologies establish the bus in a hardware device and connect the host devices to the bus using twisted-pair wiring.
- **Star:** A central cabling device connects the computers and other network devices. The physical connection is commonly made using twisted-pair wiring.
- **Mesh:** Every network device is cabled with many others. Redundant links offer reliability and self-healing. The physical connection is commonly made using fiber or twisted-pair wiring.

Logical Topologies

Logical paths that the signals use to travel from one point on the network to another



The logical paths that the signals (data) use to travel between points in the network define the way in which data accesses the network media and transmits packets across it.

The physical and logical topologies of a network can be the same. For example, in a network that is physically shaped like a linear bus, the data travels along the length of the cable. Therefore, the network has both a physical bus topology and a logical bus topology.

On the other hand, a network can have physical and logical topologies that are quite different. For example, data sent from PC A to a server can take a different path from the shortest path, as indicated in the figure. It is not always possible to predict how data travels in a network simply by observing its physical layout, so engineers often document logical topologies as well as physical topologies.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- A network is a connected collection of devices that can communicate with each other.
- There are four major categories of physical components in a computer network: computers, interconnections, switches, and routers.
- Icons are used to represent the components of a network in a network diagram.
- Common network user applications can be grouped into batch, interactive, and real-time applications.
- The ways in which networks can be described include characteristics that address network performance and structure: topology, speed, cost, security, availability, scalability, and reliability.
- A physical topology describes the layout for wiring the physical devices. A logical topology describes how information flows through a network.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Understanding the Host-to-Host Communications Model

Overview

Host-to-host communications models were created to help define how network processes function, including the various components of networks and the transmission of data. Understanding the structure and purpose of the most commonly used protocol stack, TCP/IP, is important for understanding how one host communicates with another host. This lesson introduces the OSI model and describes the TCP/IP protocol stack and its layers.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Identify the requirements of a host-to-host communications model
- Define the OSI reference model
- Describe the functions of the TCP/IP layers
- Describe the processes of encapsulation and de-encapsulation
- Describe how peer-to-peer communications work


Introducing Host-to-Host Communications

Host-to-host communications require a consistent model. The model addresses hardware, software, and data transmission. This topic describes the host-to-host communications model.

Introducing Host-to-Host Communications

Two different types of host-to-host models:

- Older model:
 - Proprietary
 - Applications and combinations of software controlled by one vendor
- Standards-based model:
 - Multivendor software
 - Layered approach
 - Examples: OSI, TCP/IP



© 2013 Cisco Systems, Inc.

The network devices that people are most familiar with are called *end devices*. End devices form the interface between the human network and the underlying communications network. In the context of a network, end devices are called *hosts*. A host device is either the source or the destination of a message that is transmitted over the network. Communication begins with a message, or information, that must be sent from one device to another device. The message then flows through the network and arrives at the end device.

Successful communication between hosts on a network requires the interaction of many different protocols. A protocol is a set of rules that govern communications. Networking protocols describe the functions that occur during network communications. Protocols are implemented in the software and hardware of each host and other devices.

Original host-to-host communications models were proprietary. Each vendor controlled its own application and embedded communications software. An application that was written by one vendor would not function on a network that was developed by another vendor. In the computer industry, “proprietary” is the opposite of “open.” Proprietary means that one company or small group of companies controls all use of the technology. Open means that use of the technology is available and is free to the public.

Business drivers and technology advances led to a multivendor solution. The first step is to separate application software from communications software, which allows new communications technologies to be implemented without requiring new applications. However, it still requires a single-vendor solution for communications software and hardware.

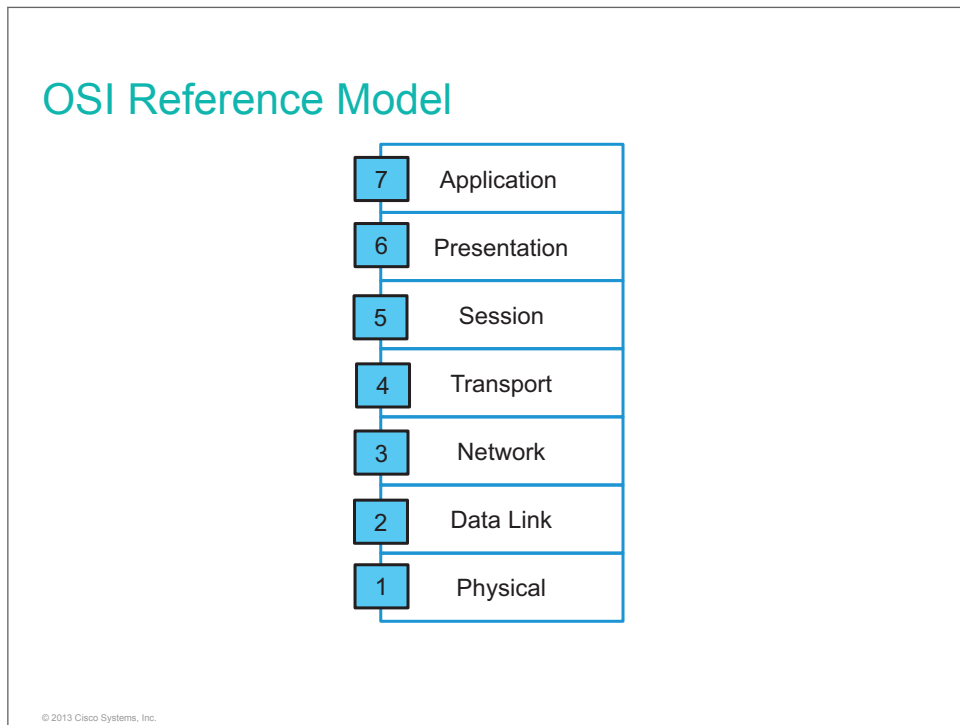
It became apparent that a multivendor solution for communications software and hardware would require a layered approach with clearly defined rules for interlayer interaction. Within a layered model, various vendors provide solutions for separate layers. Hardware vendors could design hardware and software to support emerging physical-level technologies (that is, Ethernet, Token Ring, Frame Relay, and so on). Other vendors could write software to be used by network operating systems that control host communications.

Examples of such standards-based models are TCP/IP and OSI.

Do Not Duplicate.
Post beta, not for release.

OSI Reference Model

This topic describes the OSI reference model, which provides a means of describing how data is transmitted over a network. The model addresses hardware, software, and data transmission.



To address the problem of networks being incompatible and unable to communicate with each other, the ISO researched different network schemes. As a result of this research, the ISO created a model to serve as a framework on which to build a suite of open systems protocols. The vision was that this set of protocols would be used to develop an international network that would not be dependent on proprietary systems.

As a reference, the OSI model provides an extensive list of functions and services that can occur at each layer. It also describes the interaction of each layer with the layers directly above and below it. More importantly, the OSI model facilitates an understanding of how information travels throughout a network. It provides vendors with a set of standards that ensures compatibility and interoperability between the various types of network technologies that are produced by companies around the world. It is also used for data network design, operation specifications, and troubleshooting.

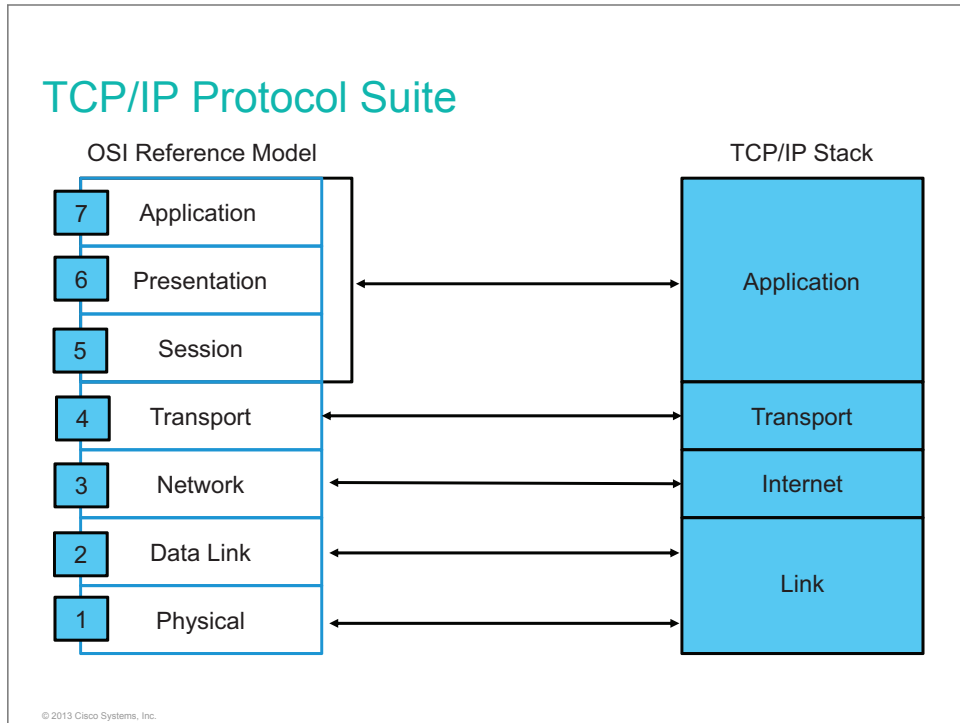
The OSI reference model separates network functions into seven categories. This separation of networking functions is called layering. The OSI reference model has seven numbered layers, each one illustrating a particular network function.

- **The physical layer (Layer 1):** The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link for bit transmission between end devices. Physical layer specifications are defining characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes.
- **The data link layer (Layer 2):** The data link layer defines how data is formatted for transmission and how access to physical media is controlled. This layer also typically includes error detection and correction to ensure reliable delivery of the data.

- **The network layer (Layer 3):** The network layer provides connectivity and path selection between two host systems that may be located on geographically separated networks. The growth of the Internet has increased the number of users that access information from sites around the world. The network layer is the layer that manages the connectivity of these users by providing logical addressing.
- **The transport layer (Layer 4):** The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices. For example, business users in large corporations often transfer large files from field locations to a corporate site. Reliable delivery of the files is important, so the transport layer breaks down large files into smaller segments that are less likely to incur transmission problems.
- **The session layer (Layer 5):** The session layer establishes, manages, and terminates sessions between two communicating hosts. The session layer also synchronizes dialog between the presentation layers of the two hosts and manages their data exchange. For example, web servers have many users, so there are many communication processes open at a given time. It is important, then, to keep track of which user communicates on which path. In addition to session regulation, the session layer offers provisions for efficient data transfer, CoS, and exception reporting of session layer, presentation layer, and application layer problems.
- **The presentation layer (Layer 6):** The presentation layer ensures that the information that is sent at the application layer of one system is readable by the application layer of another system. For example, a PC program communicates with another computer. One PC is using EBCDIC and the other PC is using ASCII to represent the same characters. If necessary, the presentation layer translates among multiple data formats by using a common format.
- **The application layer (Layer 7):** The application layer is the OSI layer that is closest to the user. This layer provides network services to the applications of the user, such as email, file transfer, and terminal emulation. The application layer differs from the other layers in that it does not provide services to any other OSI layer. It provides services only to applications outside the OSI model. The application layer establishes the availability of intended communication partners, and it synchronizes and establishes agreement on procedures for error recovery and control of data integrity.

TCP/IP Protocol Suite

Although OSI reference model layer names are often used, the OSI protocol stack is not the most commonly used reference model. The TCP/IP protocol suite, which was defined at approximately the same time as the OSI reference model, has become the most commonly used reference. Within the set of various individual communication protocols in the TCP/IP protocol suite, the two most important protocols are TCP and IP.



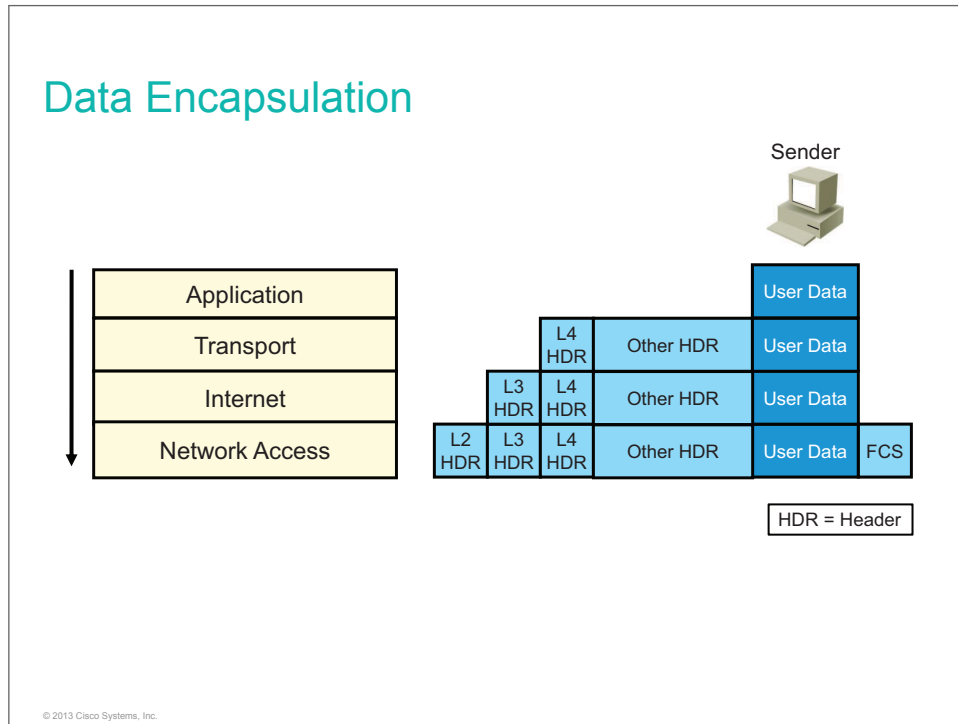
A TCP/IP protocol suite is the most popular protocol stack used in networks. It specifies end-to-end connectivity, describing how data should be formatted, addressed, routed, and transmitted. Functions are organized into the following four layers:

- **Link layer:** The link layer covers the same processes as the two lower OSI layers, the data link and physical layers. The link layer describes the physical characteristics of a link, how access is controlled, and how data is formatted for transmission.
- **Internet layer:** The internet layer provides routing of data from the source to the destination by defining the packet and the addressing schemes, moving data between the link layer and transport layers, routing packets of data to remote hosts, and performing fragmentation and reassembly of data packets.
- **Transport layer:** The transport layer is the core of the TCP/IP architecture. It provides communication services directly to the application processes that are running on network hosts.
- **Application layer:** The application layer provides applications for file transfer, network troubleshooting, and Internet activities. It also supports network APIs, which allow programs that have been created for a particular operating system to access the network.

Note Although this course refers to the TCP/IP stack, it has become common in the industry to shorten this term to "IP stack."

Encapsulation and De-Encapsulation

Information that is transmitted over a network must undergo a process of conversion at the sending and receiving ends of the communication. The conversion process is known as encapsulation and de-encapsulation of data. This topic describes the encapsulation and de-encapsulation processes.



Encapsulation

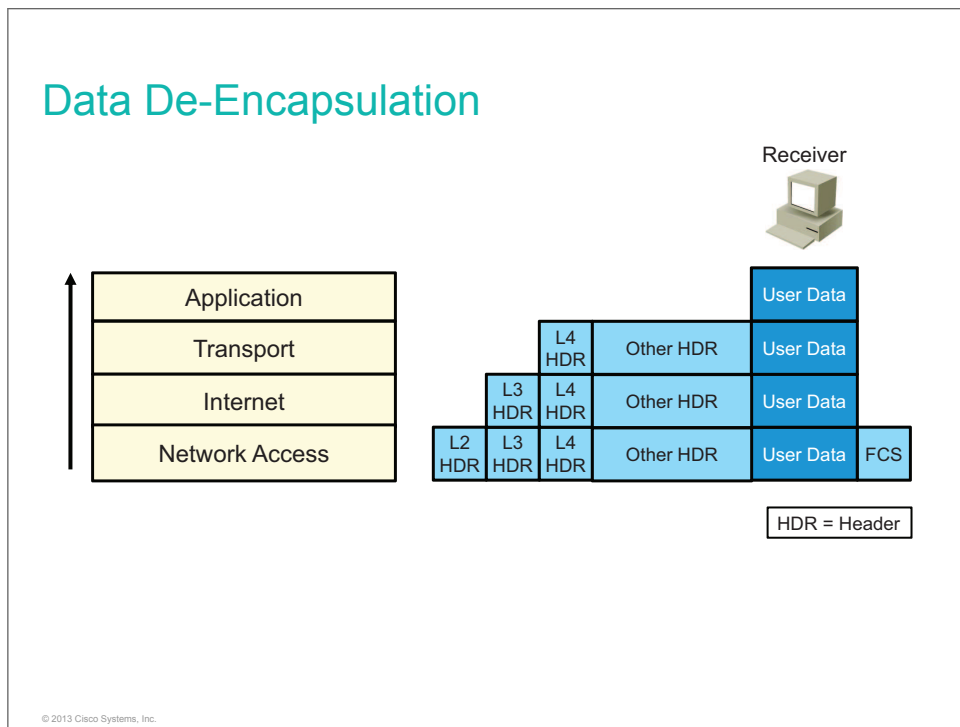
The information that is sent on a network is referred to as data or data packets. As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocols add information to it at each level. This process is commonly known as the encapsulation process. Each layer adds a header (and a trailer, if applicable) to the data before passing it down to a lower layer. The headers and trailers contain control information for the network devices and the receiver, to ensure proper delivery of the data and to ensure that the receiver can correctly interpret the data.

The figure shows how encapsulation occurs. It shows how data travels through the layers. The data is encapsulated as follows:

1. The user data is sent from an application to the application layer.
2. The transport layer adds the transport layer header (Layer 4 header) to the data. The Layer 4 header and the previous data become the data that is passed down to the internet layer.
3. The internet layer adds the internet layer header (Layer 3 header) to the data. The Layer 3 header and the previous data become the data that is passed down to the link layer.
4. The link layer adds the Layer 2 header and trailer to the data. A Layer 2 trailer is usually the FCS, which is used by the receiver to detect whether the data is in error.

Encapsulation is like sending a package through a postal service. The first step is to put the contents of the package into a container. Next, you write the address to which you want to send the package on the outside of the container. Then you put the addressed package into the postal service collection bin, and the package begins its route toward its destination.

Data De-Encapsulation



De-Encapsulation

When receiving messages on a network, the protocol stack on a host operates from the bottom to the top. The process of encapsulation is reversed at the receiving host. The data is de-encapsulated as it moves up the stack toward the end-user application.

When the remote device receives a sequence of bits, the data is de-encapsulated as follows:

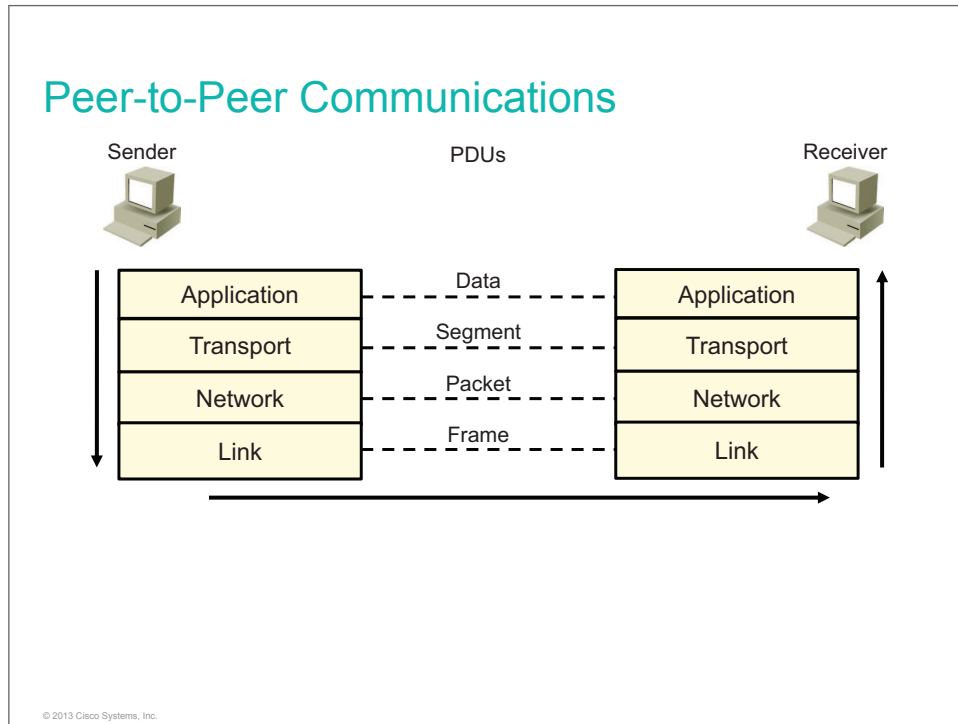
1. The link layer checks the trailer (the FCS) to see if the data is in error. The frame may be discarded or the link layer may ask for the data to be retransmitted.
2. If the data is not in error, the link layer reads and interprets the control information in the Layer 2 header.
3. The link layer strips the Layer 2 header and trailer and then passes the remaining data up to the internet layer, based on the control information in the link layer header.

Each subsequent layer performs a similar de-encapsulation process.

The de-encapsulation process is like reading the address on a package to see if it is addressed to you and then removing the contents of the package.

Peer-to-Peer Communications

Each layer of the OSI model at the source must communicate with its peer layer at the destination so that data packets can travel from the source to the destination. This topic describes the process of peer-to-peer communications.



During the process of peer-to-peer communication, the protocols at each layer exchange packets of information, called PDUs, between peer layers.

These data packets originate at a source on a network and then travel to a destination. To provide a service, each layer depends on the TCP/IP layer below it. To perform its service function, the lower layer uses encapsulation to put the PDU from the upper layer into the lower layer data field. During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above, in accordance with the protocol being used. At each stage of the process, a PDU has a different name to reflect its new appearance. Although there is no universal naming convention for PDUs, in this course, PDUs are named according to the protocols of the protocol suite:

- **Data:** The general term for the PDU used at the application layer
- **Segment:** A transport layer PDU
- **Packet:** An internet layer PDU
- **Frame:** A link layer PDU

The application layer protocol begins the process by delivering application data to the transport layer, which adds the necessary header.

The internet layer moves the data through the internetwork by encapsulating the data and attaching a header to create a packet. The header information is required to complete the transfer, and includes such information as source and destination logical addresses.

The link layer provides a service to the network layer by encapsulating the network layer packet into a frame. The frame header contains the physical addresses that are required to complete the data link functions, and the frame trailer contains the FCS.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Successful communication between hosts on a network requires the interaction of many different protocols.
- The TCP/IP protocol suite, the most commonly used protocol model, enables an understanding of how networks function.
- TCP/IP organizes the functions that must occur for communications to be successful into four layers (link, Internet, transport, and application).
- As application data within the TCP/IP suite is passed down the protocol stack on its way to be transmitted across the network media, various protocols add information to it at each level. This process is commonly known as the encapsulation process. The process is reversed at the receiving host and is known as de-encapsulation.
- During the process of peer-to-peer communication, the protocols at each layer exchange packets of information called PDUs. Protocols, which are implemented on the sending and receiving hosts, interact to provide end-to-end delivery of applications over a network.

© 2013 Cisco Systems, Inc.

Introducing LANs

Overview

LANs are a relatively low-cost way of sharing expensive resources. LANs allow multiple users in a relatively small geographic area to exchange files and messages and to access shared resources such as file servers. LANs have rapidly evolved into support systems that are critical to communications within an organization. This lesson describes LAN components and switches and explains their roles in local networks.

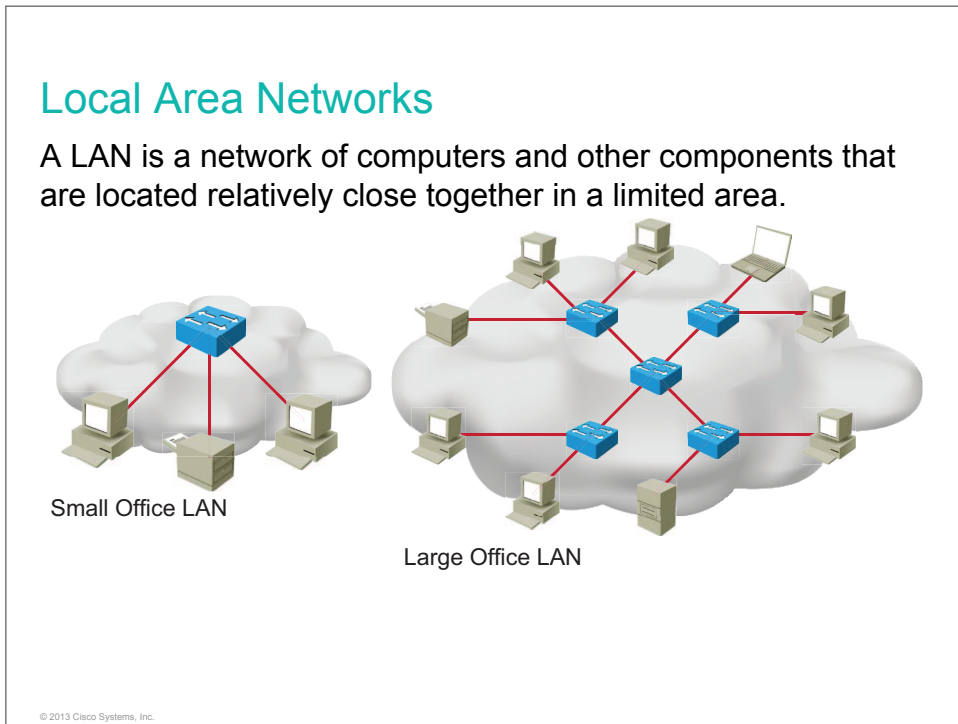
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Define a LAN
- Identify the components of a LAN
- Identify the need for switches in a LAN
- List the characteristics and features of a switch

Local Area Networks

This topic defines LANs.



LANs can vary widely in size. A LAN may consist of only two computers in a home office or small business, or it may include hundreds of computers in a large corporate office or multiple buildings.

The defining characteristics of LANs, in contrast to WANs, include their typically higher data transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

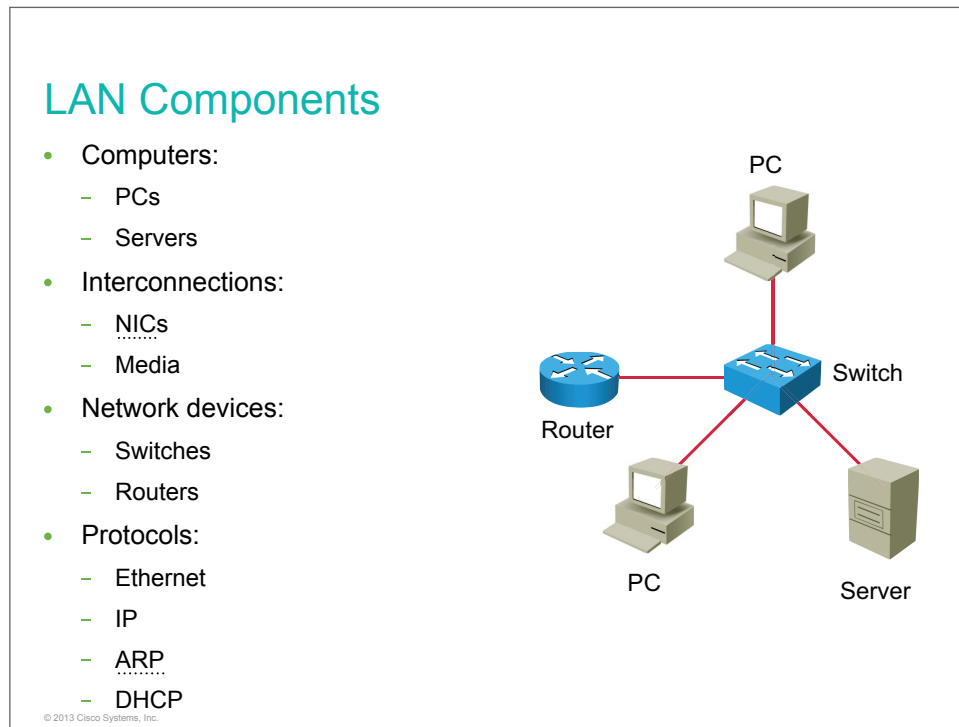
Examples: A Small-Office LAN and a Large-Office LAN

A small home business or a small-office environment can use a small LAN to connect two or more computers and to connect the computers to one or more shared peripheral devices, such as printers.

A large corporate office can use multiple LANs to accommodate hundreds of computers and shared peripheral devices, spanning many floors in an office complex.

LAN Components

Every LAN has specific components, including hardware, interconnections, and software. This topic describes the components of a LAN.



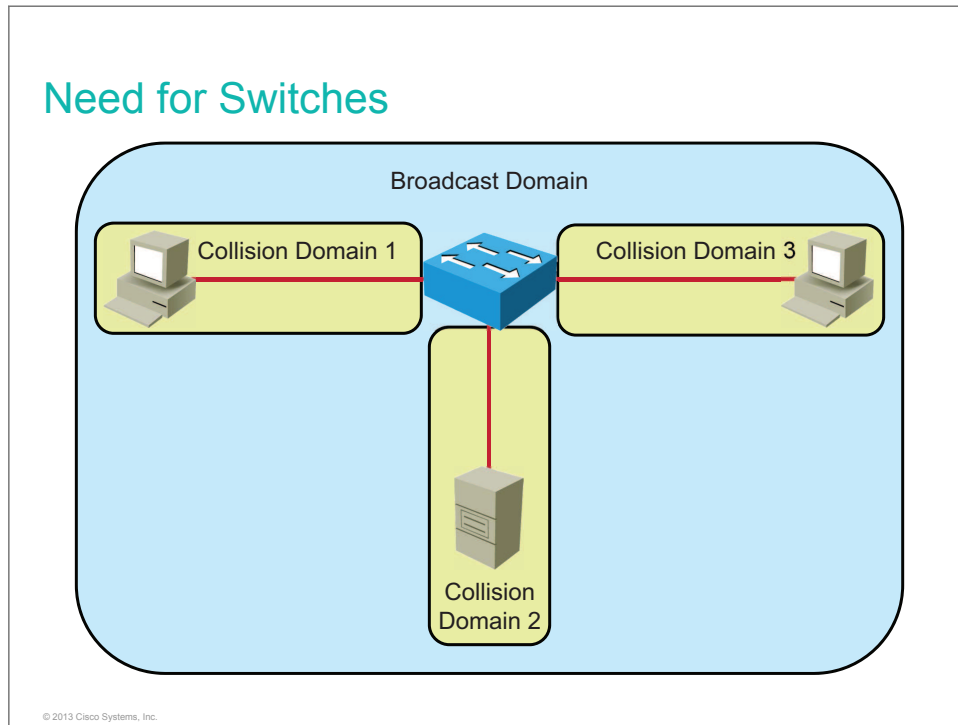
Regardless of its size, a LAN requires these fundamental components for its operation:

- **Computers:** Computers serve as the endpoints in the network. They send and receive data.
- **Interconnections:** Interconnections allow data to travel from one point to another in the network. Interconnections include these components:
 - **NICs:** NICs translate the data that is produced by the computer into a format that can be transmitted over the LAN.
 - **Network media:** Network media, such as cables or wireless media, transmit signals from one device on the LAN to another.
- **Network devices:** A LAN requires these network devices:
 - **Ethernet switches:** Ethernet switches form the aggregation point for LANs. Ethernet switches provide intelligent distribution of frames within the LAN.
 - **Routers:** Routers, sometimes called gateways, provide a means to connect LAN segments.
- **Protocols:** Protocols are sets of rules that govern data transmission over a LAN and include the following:
 - Ethernet protocols (IEEE 802.2 and IEEE 802.3)
 - IP
 - ARP
 - DHCP

Do Not Duplicate.
Post beta, not for release.

Need for Switches

This topic describes the need for switches.



When you connect three or more devices together, you need a dedicated network device to enable communication between hosts.

Historically, when network devices had few Ethernet segments, end host devices had to compete for the same bandwidth, and only one device was able to transmit data at a time. Network segments that share the same bandwidth are known as collision domains, because when two or more devices within that segment try to communicate at the same time, collisions may occur.

Today, it is common to use switches as network devices, operating at the link layer of the TCP/IP protocol suite, to divide a network into segments and reduce the number of devices that compete for bandwidth. Each new segment, then, results in a new collision domain. More bandwidth is available to the devices on a segment, and collisions in one collision domain do not interfere with the working of the other segments.

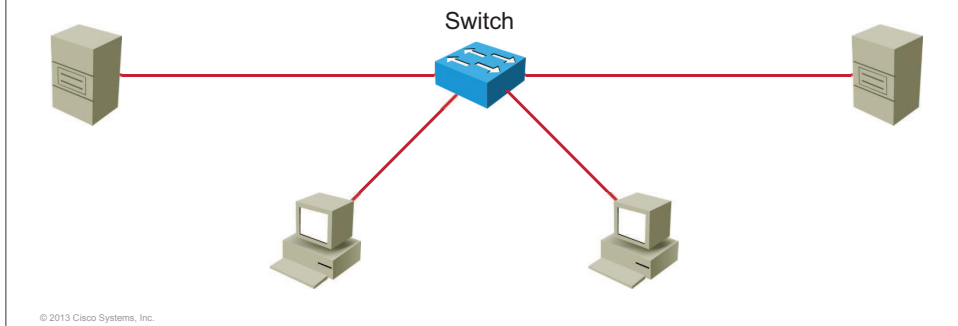
As shown in the figure, each switch port connects to a single PC or server. Each switch port represents a unique collision domain.

The broadcast domain is another key concept. The filtering of frames by switches, based on their MAC addresses, does not extend to filtering broadcast frames. By their nature, broadcast frames must be forwarded. Therefore, a port on a switch forms a single broadcast domain. It takes a Layer 3 entity, such as a router, to terminate a Layer 2 broadcast domain.

Need for Switches (Cont.)

Switches have these functions:

- Operate at the link layer of the TCP/IP protocol suite
- Forward, filter, or flood frames based on MAC table entries
- Have many full-duplex ports to segment a large LAN into many smaller segments
- Are fast and support various port speeds



Ethernet switches selectively forward individual frames from a receiving port to the port where the destination node is connected. This selective forwarding process can be thought of as establishing a momentary point-to-point connection between the transmitting and receiving nodes. The connection is made only long enough to forward a single frame. During this instant, the two nodes have a full-bandwidth connection between them and represent a logical point-to-point connection.

The switch builds and maintains a table, called a MAC table, that matches a destination MAC address with the port that is used to connect to a node. For each incoming frame, the destination MAC address in the frame header is compared to the list of addresses in the MAC table. Switches then use MAC addresses as they decide whether to filter, forward, or flood frames.

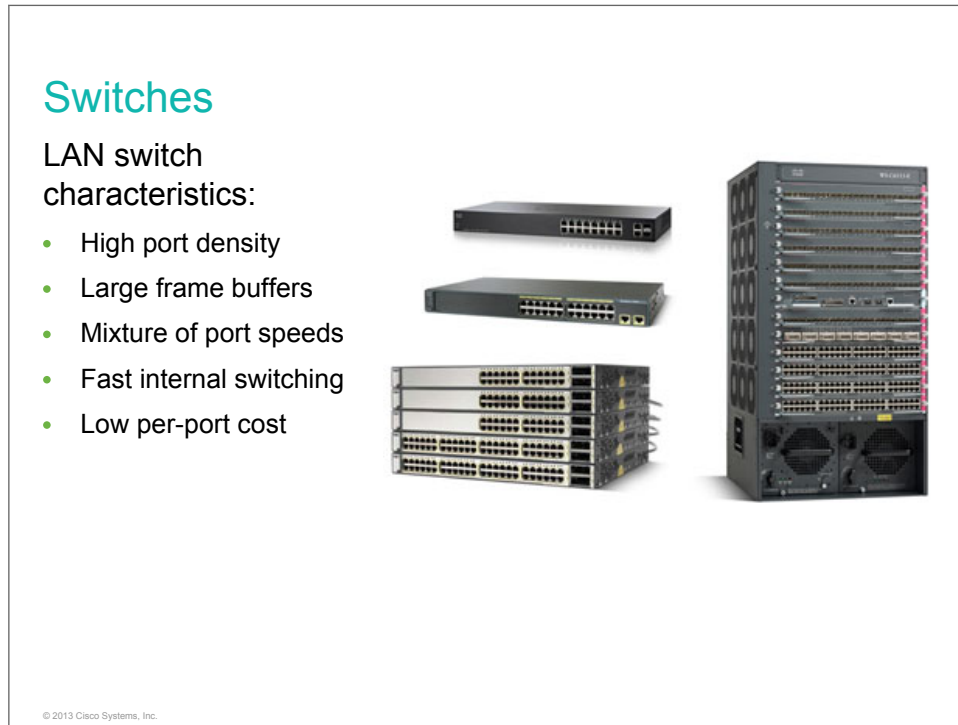
The table shows how switches process unicast frames.

How Switches Process Unicast Frames on an Ethernet LAN

Step	Action
1	When a unicast frame is received on a port, the switch compares the destination MAC address to the MAC addresses contained in its tables.
2	If the switch determines that the destination MAC address of the frame resides on the same network segment as the source, it does not forward the frame. This process is called filtering, and by performing this process, switches can significantly reduce the amount of traffic going between network segments by eliminating the unnecessary frames.
3	If the switch determines that the destination MAC address of the frame is not in the same network segment as the source, it forwards the frame to the appropriate segment.
4	If the switch does not have an entry for the destination address, it transmits the frame out of all ports except the port on which it received the frame. This process is called flooding.

Switches

LAN switches have special characteristics that make them effective in alleviating network congestion. This topic describes the characteristics of switches.



Switches have become a fundamental part of most networks. They allow the segmentation of a LAN into separate collision domains. Each port of the switch represents a separate collision domain and provides the full media to the node or nodes that are connected on that port. The introduction of full-duplex communications (a connection that can carry transmitted and received signals at the same time) has enabled 1 Gb/s Ethernet and beyond.

Switches connect LAN segments, use a table of MAC addresses to determine the segment to which the data is to be sent, and reduce network traffic. The following are some important characteristics of switches:

- **High port density:** Switches have high port densities: 24- and 48-port switches operate at speeds of 100 Mb/s, 1 Gb/s, and 10 Gb/s. Large enterprise switches may support hundreds of ports.
- **Large frame buffers:** The ability to store more received frames before needing to start dropping them is useful, particularly when there may be congested ports to servers or other parts of the network.
- **Port speed:** Depending on the cost of a switch, it may be possible to support a mixture of speeds. Ports of 100 Mb/s are expected, but switches offering ports supporting 1 or 10 Gb/s are more common.
- **Fast internal switching:** Having fast internal switching allows many speeds: 100 Mb/s, 1 Gb/s, and 10 Gb/s. The method that is used may be a fast internal bus or shared memory, which affects the overall performance of the switch.
- **Low per-port cost:** Switches provide high port density at a lower cost. For this reason, LAN switches can accommodate network designs featuring fewer users per segment, therefore increasing the average available bandwidth per user.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- A LAN is a network that is located in a limited area, with the computers and other components that are part of this network located relatively close together.
- Regardless of its size, several fundamental components are required for the operation of a LAN, including computers, interconnections, network devices, and protocols.
- Ethernet switches enable the exchange of frames between devices. They selectively forward individual frames from a receiving port to the destination port.
- Switches support high-throughput performance, high port density, and have low per-port cost.

© 2013 Cisco Systems, Inc.

Operating Cisco IOS Software

Overview

Cisco IOS Software is a feature-rich network system software that provides network intelligence to meet all current networking demands. This lesson describes Cisco IOS Software and the basic Cisco IOS CLI functions and operations. This lesson also describes how to navigate the Cisco IOS CLI configuration modes, how to use embedded keyboard help, how to manage configurations, and how to use additional Cisco IOS features to improve the user experience in the CLI.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- List the features and functions of Cisco IOS Software
- Define the functions and use of the Cisco IOS CLI
- Describe the user EXEC mode
- Describe privileged EXEC mode
- Describe CLI help functions
- Explain the role of CLI error messages
- Describe how to manage Cisco IOS configurations
- Describe how to improve the user experience in the Cisco IOS CLI

Cisco IOS Software Features and Functions

Cisco IOS Software is the industry-leading and most widely deployed network system software. This topic describes the features and functions of Cisco IOS Software.

Cisco IOS Software Features and Functions

Cisco IOS Software delivers networking services in Cisco products:

- Connectivity, for high-speed traffic between devices
- Security, to control access and prohibit unauthorized network use
- Scalability, to add interfaces and capability for network growth
- Reliability, to ensure access to networked resources
- Consistency, to experience among various device types

© 2013 Cisco Systems, Inc.

Like a computer, a switch or router cannot function without an operating system. Without an operating system, the hardware does not have any capabilities. Cisco IOS Software is the system software in Cisco devices. It is the core technology that extends across most of the Cisco product line. Cisco IOS Software is used for most Cisco devices, regardless of the size and type of the device. It is used for routers, LAN switches, small wireless access points, large routers with numerous interfaces, and many other devices.

The Cisco IOS Software operational details vary on different internetworking devices, depending on the purpose and feature set on the device.

The services that are provided by Cisco IOS Software are generally accessed using the CLI. The CLI is accessed through a console connection, a modem connection, or a Telnet or SSH session. Regardless of which connection method is used, access to the Cisco IOS CLI is generally referred to as an *EXEC session*. The look and feel of the CLI is similar among various device types, although features that are accessible through the CLI vary, based on the version of Cisco IOS Software and the type of device.

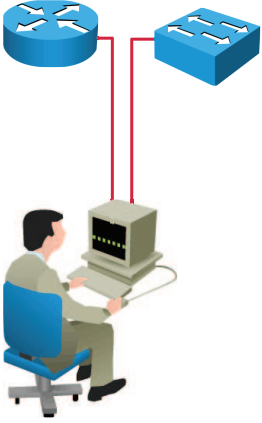
Cisco IOS CLI Functions

Cisco IOS Software uses a CLI via the console as its traditional environment to enter commands. While Cisco IOS Software is a core technology that extends across many products, the details of its operation vary on different internetworking devices. This topic describes the functions of the Cisco IOS CLI.

Cisco IOS CLI Functions

The CLI is used to enter commands.

- Operations vary on different internetworking devices.
- Users type or copy-and-paste entries in the console command modes.
- Command modes have distinctive prompts.
- Pressing **Enter** instructs the device to parse (translate) and execute the command.
- The two primary EXEC modes are user mode and privileged mode.



© 2013 Cisco Systems, Inc.

Cisco IOS Software is designed as a modal operating system. The term “modal” describes a system in which there are various modes of operation, each having its own domain of operation. The CLI uses a hierarchical structure for the modes.

To enter commands into the CLI, type or copy-and-paste the entries within one of the several console command modes. Each command mode is indicated with a distinctive prompt. The term “prompt” is used because the system is prompting you to make an entry. By default, every prompt begins with the device name. Following the name, the remainder of the prompt indicates the mode. As commands are used and modes are changed, the prompt changes to reflect the current context. Pressing Enter instructs the device to parse and execute the command.

Cisco IOS Software uses a hierarchy of commands in its command-mode structure. Each command mode supports specific Cisco IOS commands that are related to a type of operation on the device.

As a security feature, Cisco IOS Software separates EXEC sessions into two access levels:

- **User EXEC:** Allows a person to access only a limited number of basic monitoring commands
- **Privileged EXEC:** Allows a person to access all device commands, such as those used for configuration and management, and can be password-protected to allow only authorized users to access the device

User EXEC Mode

The user executive mode, or user EXEC, has limited capabilities but is useful for some basic operations. This topic describes the user EXEC mode.

User EXEC Mode

User EXEC mode allows limited examination of a switch or a router

- Command prompt: **hostname>**

```
Switch>?  
Exec commands:  
  access-enable   Create a temporary Access-List entry  
  access-profile  Apply user-profile to interface  
  clear           Reset functions  
  connect         Open a terminal connection  
  crypto          Encryption related commands  
  disable         Turn off privileged commands  
  disconnect      Disconnect an existing network connection  
  enable          Turn on privileged commands  
  exit            Exit from the EXEC  
<output omitted>
```

© 2013 Cisco Systems, Inc.

The table lists the procedure for enabling user EXEC mode on a Cisco device.

Step	Action	Results and Notes
1	Log into the device with a username and password (if a login has been configured). This action displays a user EXEC mode prompt.	A hostname> prompt appears, signifying that you have entered user EXEC mode. The right arrow (>) in the prompt indicates that the device is at the user EXEC level. Enter exit to close the session from user EXEC mode.
2	Enter the ? command at the user EXEC prompt to display the command options that are available in user EXEC mode.	The ? command in user EXEC mode reveals fewer command options than it does at privileged EXEC level. This feature is referred to as <i>context-sensitive help</i> .

User EXEC mode allows only a limited number of basic monitoring commands. This mode is often referred to as view-only mode. The user EXEC level does not allow for the execution of any commands that might change the configuration or control the operation of the device or switch. For example, user EXEC mode does not allow reloading of the device or switch.

By default, no authentication is required to access user EXEC mode from the console. It is a good practice to ensure that authentication is configured during the initial configuration.

Privileged EXEC Mode

Cisco IOS Software supports two EXEC command modes: user and privileged. This topic describes the privileged EXEC mode.

Privileged EXEC Mode

Privileged EXEC mode allows detailed examination of a switch or a router

- Enables configuration and debugging
- Prerequisite for other configuration modes
- Change from user EXEC mode to privileged EXEC mode using the **enable** command

© 2013 Cisco Systems, Inc.

Privileged EXEC Mode (Cont.)

- Command prompt: **hostname#**

```
Switch>enable
Switch#?
Exec commands:
  access-enable   Create a temporary Access-List entry
  access-profile  Apply user-profile to interface
  access-template Create a temporary Access-List entry
  archive         Manage archive files
  beep           Blocks Extensible Exchange Protocol commands
  call-home      Call-Home commands
  cd             Change current directory
  clear          Reset functions
  clock         Manage the system clock
  cns           CNS agents
<output omitted>
```

© 2013 Cisco Systems, Inc.

Critical commands, such as those related to configuration and management, require that you are logged into privileged EXEC mode.

To return to the user EXEC level, enter the **disable** command at the hostname# prompt.

Help Functions in the CLI

Cisco devices use Cisco IOS Software with extensive command-line input help functions, including context-sensitive help. This topic describes the CLI keyboard help that is available on Cisco IOS devices.

Help Functions in the CLI	
Type of CLI Help	Description
Context-sensitive help	Provides a list of commands and the arguments that are associated with a specific command
Console error messages	Identifies problems with commands that are incorrectly entered so that they can be altered or corrected

© 2013 Cisco Systems, Inc.

The Cisco IOS CLI on Cisco devices offers two types of context-sensitive help:

- **Word help:** Enter the character sequence, followed immediately by a question mark. Do not include a space before the question mark. The device will display a list of commands that start with the characters that you entered. For example, enter the **sh?** command to get a list of commands that begin with the character sequence “sh”.
- **Command syntax help:** Enter the **?** command to get help on the syntax needed to complete a command. Enter the question mark in place of a keyword or argument, following the command name. Include a space before the question mark. The network device will then display a list of available command options, with <cr> standing for carriage return. For example, enter **show ?** to get a list of the command options available for the **show** command.

Note Cisco routers and Cisco Catalyst switches have similar command-line help functions. All of the help functions that are mentioned in this section for devices also apply to Catalyst switches, unless otherwise stated.

When you submit a command by pressing Enter, the command-line interpreter parses the command from left to right to determine which action is being requested. If the interpreter understands the command, the requested action is executed and the CLI returns to the appropriate prompt. However, if the interpreter cannot understand the command being entered, it provides feedback describing what is wrong with the command.

Help Functions in the CLI (Cont.)

This sequence of commands shows how CLI context-sensitive help can be used:

```
SwitchX#cl?  
clear clock  
SwitchX#clock ?  
    set    Set the time and date  
SwitchX#clock set ?  
    hh:mm:ss Current time  
SwitchX#clock set 19:50:00 ?  
    <1-31> Day of the month  
    MONTH Month of the year  
SwitchX#clock set 19:50:00 25 June ?  
    <1993-2035> Year  
SwitchX#clock set 19:50:00 25 June 2012  
SwitchX#
```

© 2013 Cisco Systems, Inc.

Context-sensitive help provides a list of commands and the arguments that are associated with those commands within the context of the current mode. To access context-sensitive help, enter a question mark (?) at any prompt. There is an immediate response. You do not need to press Enter.

One use of context-sensitive help is to get a list of available commands. This list can be used when you are unsure of the name for a command or you want to see if Cisco IOS Software supports a particular command in a particular mode.

For example, to list the commands available at the user EXEC level, enter ? at the prompt.

Another use of context-sensitive help is to display a list of commands or keywords that start with a specific character or characters. Enter a character sequence, then immediately enter a question mark (without a space before it). Cisco IOS Software displays a list of commands or keywords for this context that start with the characters that you entered.

For example, enter **sh?** to get a list of commands that begin with the character sequence “sh”.

If the word “clock” is misspelled as it is entered, the system performs a symbolic translation of the misspelled command as parsed by Cisco IOS Software. If no CLI command matches the string that was entered, an error message is returned. Furthermore, if there is no Cisco IOS Software command that begins with the letters entered, the device interprets the command as a host name and attempts to resolve the host name to an IP address. Then the device tries to establish a Telnet session to that host.

A final type of context-sensitive help is used to determine which options, keywords, or arguments are matched with a specific command. Enter a command, followed by a space and then a question mark, to determine what can or should be entered next.

As shown in the example, after entering the command **clock set 19:50:00**, you can enter a space and then a question mark to determine the options or keywords that are available with this command.

CLI Error Messages

This topic describes CLI error messages.

CLI Error Messages

```
SwitchX#c
% Ambiguous command:'c'
```

- Not enough characters were entered.

```
SwitchX#clock set
% Incomplete command
SwitchX#clock set 19:50:00
% Incomplete command
```

- Required arguments or keywords were left off the end of the command.

```
SwitchX#>clock set 19:50:00 25 6
                        ^
% Invalid input detected at '^' marker
```

- The caret (^) indicates where the command interpreter cannot decipher the command.

© 2013 Cisco Systems, Inc.

There are three types of console error messages:

- Ambiguous command
- Incomplete command
- Incorrect command

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your device to recognize the command.	Re-enter the command, followed by ? without a space before it. The possible keywords that you can enter with the command are displayed.
% Incomplete command	You did not enter all the keywords or values that are required by this command.	Re-enter the command, followed by ? with a space before it.
% Invalid input detected at '^' marker	You entered the command incorrectly. The ^ marks the point of the error.	Enter ? to display all of the commands or parameters that are available.

The command history buffer stores the commands that have been most recently entered. To see these commands, enter the Cisco IOS **show history** command.

You can use context-sensitive help to determine the syntax of a particular command. For example, if the device clock needs to be set but you are not sure of the **clock** command syntax, the context-sensitive help provides a means to check the syntax.

Context-sensitive help supplies the whole command even if you enter just the first part of the command, such as **cl?**.

If you enter the command **clock** but an error message is displayed, indicating that the command is incomplete, enter the **?** command (preceded by a space) to determine which arguments are required for the command. In the **clock ?** example, the help output shows that the keyword **set** is required after **clock**.

If you now enter the command **clock set** but another error message appears, indicating that the command is still incomplete, press the **Up** arrow to repeat the command entry. Then, add a space and enter the **?** command to display a list of arguments that are available for the command.

The example shows that after the last command recall, the administrator used the **?** command to reveal the additional arguments, which involve entering the current time using hours, minutes, and seconds.

The figure continues to illustrate how to set the device clock.

If, after entering the current time, you still see the Cisco IOS Software error message indicating that the command entered is incomplete, recall the command, add a space, and enter the **?** command to display a list of arguments that are available for the command. In this example, enter the day, month, and year using the correct syntax and then press **Enter** to execute the command.

Syntax checking uses the caret symbol (^) as an error-location indicator. It appears at the point in the command string where an incorrect command, keyword, or argument has been entered. The error-location indicator and interactive help system provide a way to easily find and correct syntax errors. In the clock example, the caret symbol indicates that the month was entered incorrectly as a number. The parser is expecting the month to be spelled out.

Managing Cisco IOS Configurations

This topic describes various Cisco IOS Software configurations and how to save, back up, and load configurations.

Managing Cisco IOS Configurations

There are two general types of configuration:

- **Running configuration:** This state reflects the current configuration of the device.
- **Startup configuration:** This file is used to load the saved configuration after powering up. If no configuration is present, enter setup mode or load a blank configuration.

© 2013 Cisco Systems, Inc.

Cisco switches and routers have three primary types of memory:

- **RAM:** Stores routing tables (router), fast-switching cache, running configuration, and so on
- **NVRAM:** Used for writable permanent storage of the startup configuration
- **Flash:** Provides permanent storage of the Cisco IOS Software image, backup configurations, and any other files via memory cards

After the Cisco IOS Software image is loaded and started, the router or switch must be configured to be useful. If there is a saved configuration file (startup configuration) in NVRAM, it is executed. If there is no saved configuration file in NVRAM, the router or switch enters the setup utility. The setup utility prompts you at the console for specific configuration information to create a basic initial configuration on the router or switch.

You can also interrupt the setup utility and start configuring a router or switch by manually entering all the needed commands. After you enter and execute a command, the command is stored in the running configuration. The running configuration reflects the current configuration of the device. It is stored in RAM and is therefore deleted at reboot. You have to copy the running configuration to the startup configuration to preserve the configuration across a router or switch reboot.

Managing Cisco IOS Configurations (Cont.)

This is how you investigate the current running configuration (RAM):

```
Switch#show running-config
Building configuration...

Current configuration : 1707 bytes
!
! Last configuration change at 04:45:43 UTC Fri Aug 17 2012
! NVRAM config last updated at 04:45:43 UTC Fri Aug 17 2012
!
version 15.0
no service pad
service timestamps debug datetime msec
<output omitted>
```

© 2013 Cisco Systems, Inc.

Managing Cisco IOS Configuration (Cont.)

This is how you investigate the saved configuration (NVRAM):

```
Switch#show startup-config
Using 1707 out of 65536 bytes
!
! Last configuration change at 04:45:43 UTC Fri Aug 17 2012
! NVRAM config last updated at 04:45:43 UTC Fri Aug 17 2012
!
version 15.0
no service pad
service timestamps debug datetime msec
<output omitted>
```

© 2013 Cisco Systems, Inc.

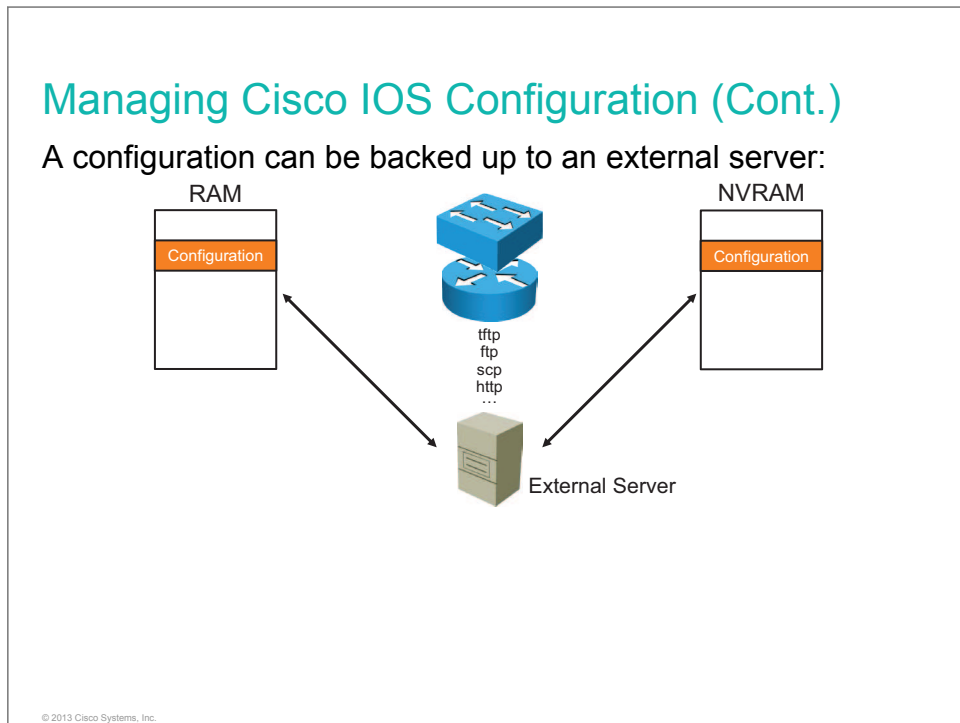
The **show running-config** command displays the current running configuration in RAM. The “Building configuration...” output indicates that the running configuration is being built from the active configurations stored in RAM.

After the running configuration is built from RAM, the “Current configuration: 1707 bytes” message appears, indicating that this is the current configuration running in RAM and the size of the current running configuration, in bytes.

The **show running-config** command also has various command options to filter the running configurations that will be displayed. For example, you can use the **show running-config interface GigabitEthernet0/1** command to display only the running configuration of interface GigabitEthernet0/1.

The **show startup-config** command displays the saved configuration in NVRAM.

The first line of the command output indicates the amount of NVRAM used to store the configuration. For example, “Using 1707 out of 65536 bytes” indicates that the total size of the NVRAM is 65536 bytes and the current configuration stored in NVRAM takes up 1707 bytes.

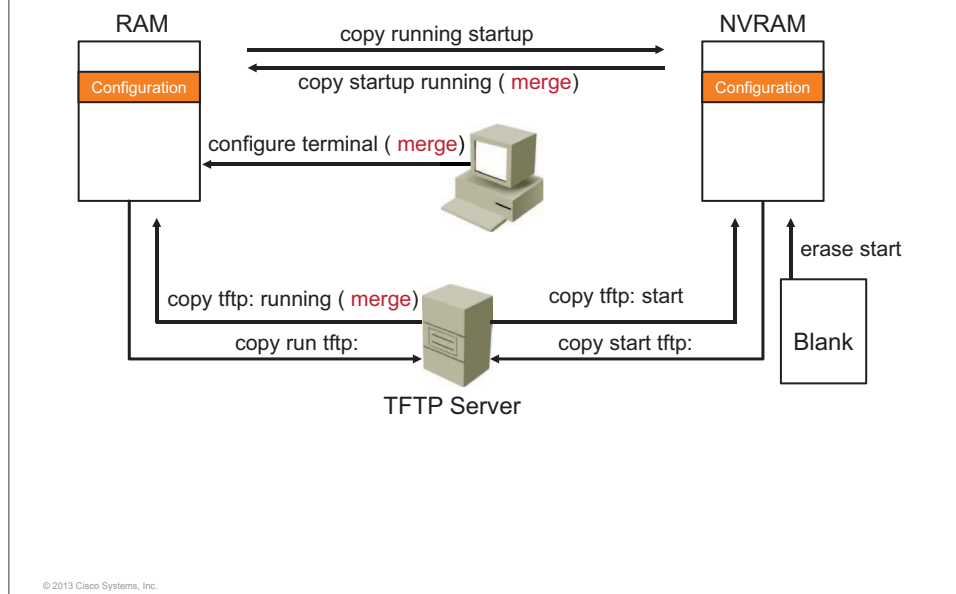


You can copy configuration files from the router or switch to a file server using FTP, SCP, HTTP, TFTP, and others. For example, you can copy configuration files to back up a current configuration file to a server before changing its contents, thereby allowing the original configuration file to be restored from the server. The protocol that is used depends on which type of server is used.

You can copy configuration files of the router or switch from an external server to the running configuration in RAM or to the startup configuration file in NVRAM for one of the following reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another router or switch. For example, you may add another router or switch to the network and want it to have a configuration similar to the original router or switch. By copying the file to the network server and making the changes to reflect the configuration requirements of the new router or switch, you can save time.
- To load the same configuration commands onto all the routers or switches in the network so that all the routers or switches have similar configurations.

Managing Cisco IOS Configuration (Cont.)



In addition to using the setup utility or the CLI to load or create a configuration, there are several other configurations that you can use.

You can use the Cisco IOS **copy** command to move configurations from one component or device to another. The syntax of the **copy** command requires that the first argument indicate the source (where the configuration is to be copied from), followed by the destination (where the configuration is to be copied to). For example, in the **copy running-config tftp:** command, the running configuration in RAM is copied to a TFTP server.

Use the **copy running-config startup-config** command after a configuration change is made in the RAM that must be saved to the startup configuration file in NVRAM. Similarly, copy the startup configuration file in NVRAM back into RAM with the **copy startup-config running-config** command. Notice that you can abbreviate the commands.

Similar commands exist for copying between a TFTP server and either NVRAM or RAM.

Use the **configure terminal** command to interactively create configurations in RAM from the console or remote terminal.

Use the **erase startup-config** command to delete the saved startup configuration file in NVRAM.

When a configuration is copied into RAM from any source, the configuration merges with the existing configuration in RAM. New configuration parameters are added, and changes to existing parameters overwrite the old parameters. Configuration commands that exist in RAM for which there is no corresponding command in NVRAM remain unaffected. Copying the running configuration from RAM into the startup configuration file in NVRAM overwrites the startup configuration file in NVRAM.

Managing Cisco IOS Configuration (Cont.)

This is how you can save a device configuration:

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

This is how you back up a configuration to the TFTP server:

```
Switch#copy running-config tftp:
Address or name of remote host []? 10.1.1.1
Destination filename [running-config]? config.cfg
!!!
1684 bytes copied in 13.300 secs (129 bytes/sec)
```

© 2013 Cisco Systems, Inc.

After the commands to configure the router or switch have been entered, you must save the running configuration to NVRAM with the **copy running-config startup-config** command. If the configuration is not saved to NVRAM and the router or switch is reloaded, the configuration will be lost and the router or switch will revert to the last configuration saved in NVRAM.

You can use the TFTP servers to store configurations in a central place, allowing centralized management and updating. Regardless of the size of the network, there should always be a copy of the current running configuration online as a backup.

The **copy running-config tftp:** command allows the current configuration to be uploaded and saved to a TFTP server. The IP address or name of the TFTP server and the destination filename must be supplied. During the copying process, a series of exclamation marks shows the progress of the upload.

The **copy tftp: running-config** command downloads a configuration file from the TFTP server to the running configuration of the RAM. Again, the address or name of the TFTP server and the source and destination filenames must be supplied. In this case, because you are copying the file to the running configuration, the destination filename should be running-config. This is a merge process, not an overwrite process.

Improving the User Experience in the CLI

The Cisco IOS Software CLI includes many features that make the configuration process easier and faster. This topic describes Cisco IOS CLI features that enhance a configuration process.

Improving the User Experience in the CLI

Command-Line Editing Key Sequence	Description
Tab	Completes the remainder of the command or keyword
Ctrl-A	Moves the cursor to the beginning of the command line
Ctrl-E	Moves the cursor to the end of the command line
Backspace	Removes one character to the left of the cursor
Ctrl-U	Erases a line
Ctrl-Shift-6	Allows the user to abort a Cisco IOS process such as ping or traceroute
Ctrl-C	Aborts the current command and exits the configuration mode
Ctrl-Z	Ends configuration mode and returns to the EXEC prompt

© 2013 Cisco Systems, Inc.

The key sequences indicated in the figure are shortcuts or hot keys that are provided by the CLI. Use these key sequences to move the cursor around on the command line for corrections or changes and to make configuring, monitoring, and troubleshooting easier.

Improving the User Experience in the CLI (Cont.)

```
Switch#terminal history size 50
```

- Sets session command buffer size to 50 lines.

```
Switch#show history
enable
terminal history size 50
show history
```

- Displays the contents of the command buffer.

© 2013 Cisco Systems, Inc.

With the command history feature, you can complete these tasks:

- Display the contents of the command buffer.
- Set the command history buffer size.
- Recall previously entered commands that are stored in the history buffer. There is a buffer for EXEC mode and another buffer for configuration mode.

By default, command history is enabled, and the system records the last 10 command lines in its history buffer.

To change the number of command lines that the system will record during the current terminal session only, use the **terminal history** command in user EXEC mode.

To recall older commands in the history buffer, press **Ctrl-P** or the **Up Arrow** key. The command output will begin with the most recent command. Repeat the key sequence to recall successively older commands.

To return to more recent commands in the history buffer (after recalling older commands with **Ctrl-P** or the **Up Arrow** key), press **Ctrl-N** or the **Down Arrow** key. Repeat the key sequence to successively recall more recent commands.

On most computers, there are additional select and copy functions available. Copy a previous command string, and then paste or insert it as the current command entry and press **Enter**.

Improving the User Experience in the CLI (Cont.)

```
Switch#show running-config
Building configuration...
Current configuration : 1707 bytes
!
! Last configuration change at 11:46:10 UTC Fri Aug 17 2012
! NVRAM config last updated at 04:45:43 UTC Fri Aug 17 2012
!
<output omitted>
!
--More--
```

- The Cisco IOS CLI pauses after a specific number of lines is displayed.

```
Switch#terminal length 100
```

- Sets the number of lines on the current terminal screen.

© 2013 Cisco Systems, Inc.

When you use **show** commands (for example, **show running-config**), Cisco IOS Software automatically pauses its display of the output after a specified number of lines and displays "--More--" text. It waits for user input to continue with the display. You must press **Spacebar** to display a set of subsequent lines, or press **Enter** to display a single line.

You can use the **terminal length** command followed by a number to control the number of lines that are displayed without pause. A value of zero prevents the router from pausing between screens of output. By default, the value is set to 24.

Improving the User Experience in the CLI (Cont.)

You can filter **show** outputs using the pipe (|) character and a filtering parameter.

Use the **include** parameter to display configuration commands that include a specific word:

```
Switch#show running-config | include hostname
hostname Switch
```

Use the **section** parameter to display a section of the configuration:

```
Switch#show running-config | section FastEthernet0/11
interface FastEthernet0/11
 switchport access vlan 100
 switchport mode access
 switchport port-security
```

© 2013 Cisco Systems, Inc.

Another useful feature that improves the user experience in the CLI is filtering of **show** outputs. Using filtering, you can display only the parts of **show** outputs that you want to display. You can filter outputs by providing the pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression.

The table describes filtering parameters that are available for output filtering:

Parameter	Description
begin	Shows all the output lines from a certain point, starting with the line that matches the filtering expression
exclude	Excludes all output lines that match the filtering expression
include	Includes all output lines that match the filtering expression
section	Shows entire section that starts with the filtering expression

Note You can use output filters in combination with any **show** command. The **show running-config** command in the example is used for the sake of simplicity only.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco IOS Software provides network services to Cisco products to perform various internetworking functions.
- The Cisco IOS CLI uses a hierarchy of commands in its command-mode structure.
- Two basic configuration modes are user EXEC mode and privileged EXEC mode.
- Context-sensitive help and console error messages are available in the Cisco IOS CLI to help you configure Cisco devices.
- Two general configurations that are used by Cisco routers and switches are the running configuration and the startup configuration.
- You can use hot keys and shortcuts, command history, and output filters to improve the CLI user experience.

© 2013 Cisco Systems, Inc.

Starting a Switch

Overview

Before you start a Cisco Catalyst switch, the physical installation must meet operational conditions. After the switch is turned on and startup is complete, you can configure the initial software settings. Verifying that the switch startup has been completed without error is the first step in deploying a Catalyst switch. The switch must start successfully and have a default configuration to operate on the network. This lesson describes switch installation and how to verify the initial operation and configuration.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Identify physical installation requirements
- Identify the conditions that are reflected by the LEDs on switches
- Connect to a switch console port
- Configure a Cisco IOS switch from the CLI
- Verify initial switch operation

Switch Installation

Before you physically install a Catalyst switch, you must have the correct power and operating environment. When the cables are correctly connected, the switch can be powered up. This topic describes the physical installation and startup of a Catalyst switch.

Switch Installation

- Before installing a switch, verify the power and cooling requirements.
- Physically install the switch:
 - Rack mount
 - Wall mount
 - Table or shelf mount
- Verify the network cabling.
- Attach the power cable plug to start the switch.
- System startup routines perform POST and initiate the switch software.

© 2013 Cisco Systems, Inc.

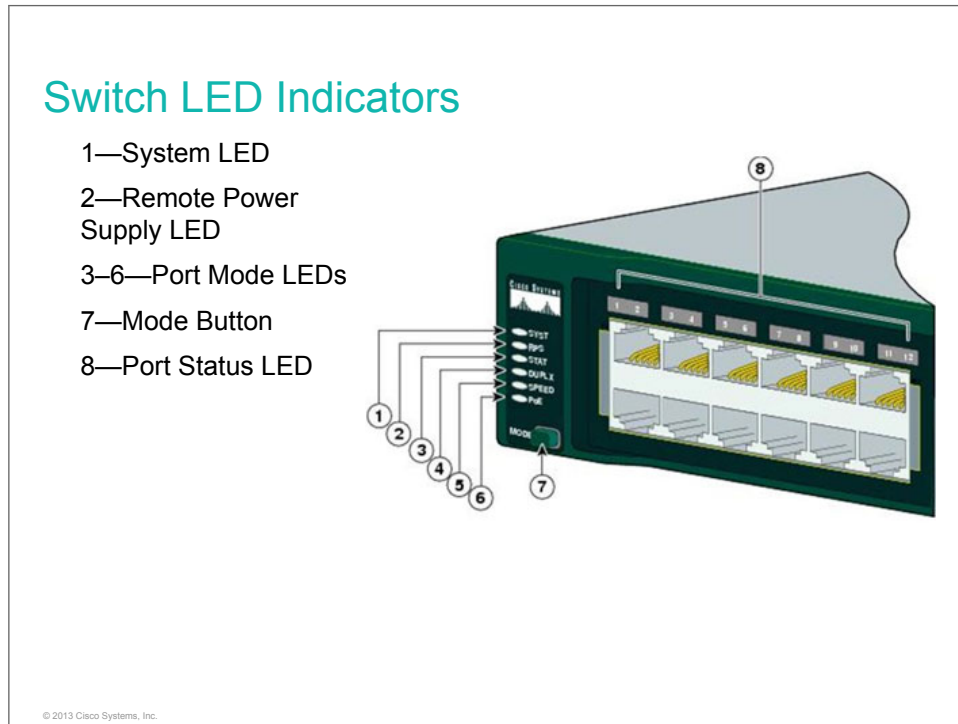
Physical installation and startup of a Catalyst switch requires completion of these steps:

1. Before performing physical installation, verify the following:
 - Switch power requirements
 - Switch operating environment requirements (operational temperature and humidity)
2. Use the appropriate installation procedures for rack mounting, wall mounting, or table or shelf mounting.
3. Before starting the switch, verify that network cable connections are secure.
4. Attach the power cable plug to the power supply socket of the switch. The switch will start. Some Catalyst switches, including the Cisco Catalyst 2960 Series, do not have power buttons.
5. Observe the boot sequence:
 - When the switch is on, POST begins. During POST, the switch LED indicators blink while a series of tests determine that the switch is functioning properly.
 - The Cisco IOS Software output text is displayed on the console.

When all startup procedures are finished, the switch is ready to configure.

Switch LED Indicators

Cisco Catalyst switches have several status LEDs that are generally lit in green when the switch is functioning normally. The LEDs are lit in amber when there is a malfunction. This topic describes the states of the LEDs on Catalyst 2960 Series Switches.



The front panel of a switch has several lights, called *LEDs*, to help monitor system activity and performance. LED indicators provide only a quick overview of the status of the switch. For a more detailed view, you can use Cisco IOS commands.

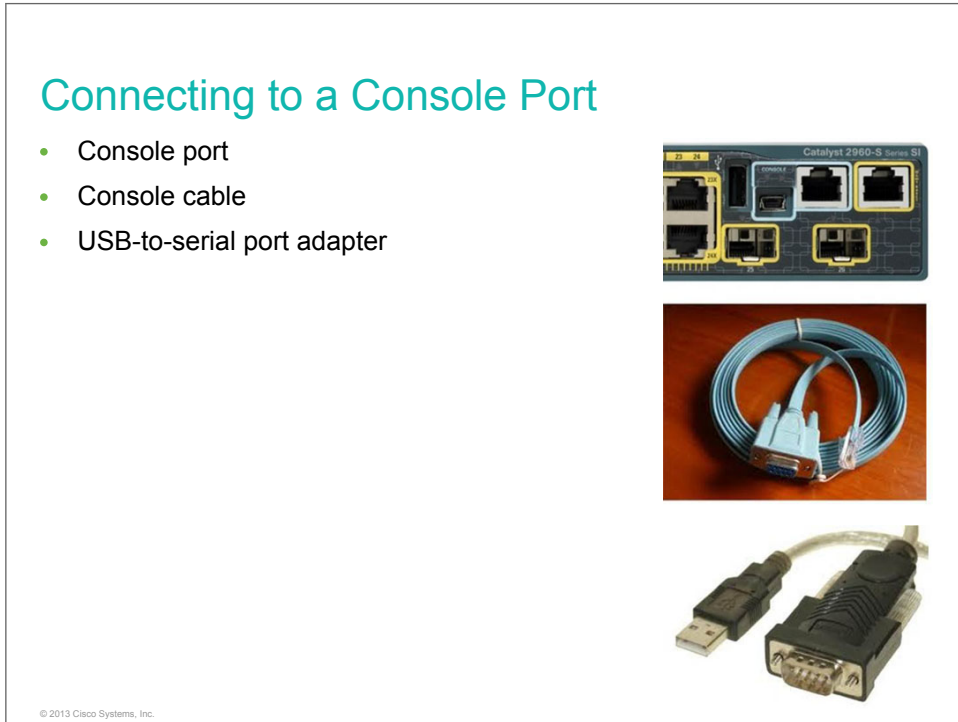
The front of the switch features these LEDs:

- **System LED:** Indicates whether the system is receiving power and functioning correctly.
- **Remote Power Supply LED:** Indicates whether the remote power supply is in use.
- **Port Mode LEDs:** Indicate the current state of the Mode button, which is used to switch between various modes. The modes are used to determine how the Port Status LEDs are interpreted.
- **Port Status LEDs:** Have various meanings, depending on the current value of the Mode LED.

For more details about LED indicators and their functions, refer to the *Cisco Switch Hardware Installation Guide*. It is recommended that you refer to the model-specific documentation. The reference for the Catalyst 2960 switches can be found at <http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/hardware/installation/guide/higover.html#wp1021241>.

Connecting to a Console Port

Upon initial installation, you can configure the switch from a PC that is connected directly through the console port on the switch. This topic describes how to connect to the console port and log in to a Cisco Catalyst switch to begin the initial configuration.



To perform initial switch configuration, connect to the switch through the console port.

This equipment is needed to access a Cisco device through the console port:

- RJ-45-to-DB-9 console cable
- PC or equivalent with serial port and communications software, such as HyperTerminal, configured with these settings:
 - Speed: 9600 b/s
 - Data bits: 8
 - Parity: None
 - Stop bit: 1
 - Flow control: None

Modern computers and notebooks rarely include built-in serial ports. Often a USB-to-RS-232-compatible serial port adapter is used instead.

On newer Cisco network devices, a USB serial console connection is also supported. A suitable USB cable (USB Type A-to-5-pin mini Type B) and operating system device driver are needed to establish connectivity.

Note Only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. When the USB cable is removed from the USB port, the RJ-45 port becomes active.

When a console connection is established, you gain access to user EXEC mode, by default. To start configuration, you must enter privileged EXEC mode by using the **enable** command.

Do Not Duplicate:
Post beta, not for release.

Basic Switch Configuration

Cisco IOS Software on a Catalyst switch has various configuration modes, including global configuration mode and interface configuration mode. This topic describes how to complete the initial switch configuration using both modes.

Basic Switch Configuration

Configuration modes:

- Global configuration mode

```
Switch#configure terminal
Switch(config)#
```

- Interface configuration mode

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
```

© 2013 Cisco Systems, Inc.

Cisco IOS Software CLI modes are hierarchically structured.

When you are in privileged EXEC mode, you can access other configuration modes. Each mode is used to accomplish particular tasks and has a specific set of commands that are available in that mode. For example, to configure a switch interface, you must be in interface configuration mode. All configurations that are entered in interface configuration mode apply only to that interface.

To begin, you will explore how to navigate two frequently used configuration modes: global configuration mode and interface configuration mode.

The example starts with the switch in privileged EXEC mode. To configure global switch parameters, such as the switch hostname or the switch IP address, which are used for switch management, use global configuration mode. To access global configuration mode, enter the **configure terminal** command in privileged EXEC mode:

```
Switch#configure terminal
```

After the command is executed, the prompt changes to show that the router is in global configuration mode.

```
Switch(config)#
```

Configuring interface-specific parameters is a common task. To access interface configuration mode for the Fast Ethernet 0/1 interface from global configuration mode, enter the **interface FastEthernet 0/1** command:

```
Switch(config)#interface FastEthernet 0/1
```

Or, you can use a shorter version of the same command:

```
Switch(config)#interface fa 0/1
```


The prompt changes:

```
Switch(config-if)#
```

To exit interface configuration mode, use the **exit** command.

Sometimes, you need to execute commands on multiple subinterfaces at the same time. Use the **interface range** command in global configuration mode for this task:

```
Switch(config)#interface range FastEthernet 0/1 - 24  
Switch(config-if-range)#
```

This example shows how to configure interfaces FastEthernet 0/1 through 0/24, all at the same time.

Basic Switch Configuration (Cont.)

Set the local identity for the switch.

```
Switch(config)#hostname SwitchX  
SwitchX(config)#
```

© 2013 Cisco Systems, Inc.

Naming the switch enables you to better manage the network by being able to uniquely identify each switch within the network. The name of the switch is considered to be the hostname and is the name that is displayed at the system prompt. The switch name is assigned in global configuration mode. In the example that is shown in the figure, the switch name is set to "SwitchX" with the use of the **hostname** command. If the hostname is not explicitly configured, a switch has the factory-assigned default hostname of "Switch."

Basic Switch Configuration (Cont.)

Assign the IP address and subnet mask for the switch.

```
SwitchX(config)#interface vlan 1
SwitchX(config-if)#ip address 172.20.137.5 255.255.255.0
SwitchX(config-if)#no shutdown
```



Note: Most software versions require use of the **no shutdown** command to make the interface operational.

© 2013 Cisco Systems, Inc.

To manage a switch remotely, you need to assign an IP address to the switch. In this example, you want to manage SwitchX from a PC, a computer that is used for managing the network, so you need to assign an IP address to SwitchX. This IP address is assigned to a virtual interface called a VLAN. The default configuration on the switch is to have switch management controlled through VLAN 1. Therefore, the IP address in the example is assigned to VLAN 1.

To configure an IP address and subnet mask for the switch, you must be in VLAN 1 interface configuration mode and then use the **ip address** configuration command.

You must use the **no shutdown** interface configuration command to make the interface operational.

The operational VLAN interface with the assigned IP address can be used, for example, in a remote management Telnet connection, or, if you use SNMP, to manage the switch.

After you enter the initial commands to configure the switch, you must save the running configuration to NVRAM with the **copy running-config startup-config** command. If the configuration is not saved to NVRAM and the switch is reloaded, the configuration is lost and the router reverts to the last configuration saved in NVRAM.

Verifying the Switch Initial Startup Status

After you log in to a Catalyst switch, you can verify the switch software and hardware status using verification commands executed from privileged EXEC mode. This topic describes the switch **show** commands that can be used to verify the initial switch operation.

Verifying the Switch Initial Startup Status

```
SwitchX#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(1)SE3,
RELEASE SOFTWARE (fc1)
<output omitted>
SwitchX uptime is 15 hours, 30 minutes
System returned to ROM by power-on
System restarted at 15:06:49 UTC Tue Aug 21 2012
System image file is "flash:/c2960-lanbasek9-mz.150-1.SE3/c2960-lanbasek9-mz.
150-1.SE3.bin"
<output omitted>
cisco WS-C2960-24TT-L (PowerPC405) processor (revision D0) with
65536K bytes of memory.
Processor board ID FOC1141Z8YW
<output omitted>
```

- Displays the configuration of the system hardware, software version, and boot images.

© 2013 Cisco Systems, Inc.

Use the **show version** EXEC command to display the configuration of the system hardware and the software version information. The table describes some of the output fields of the **show version** command.

Output	Description
Cisco IOS Software Release	Identification of the software by name and release number Always specify the complete release number when reporting a possible software problem. In this example, the switch is running Cisco IOS Release 15.0(1)SE3.
Switch uptime	Current days and time since the system was last booted In this example, the switch uptime is 15 hours and 30 minutes.
System image file is	Show location and file name of used system image
Switch platform	Hardware platform information, including revision and amount of RAM
Processor board ID	Device serial number

The information in this figure is from a Cisco Catalyst WS-C2960-24 switch with 24 Fast Ethernet ports.

Verifying the Switch Initial Startup Status (Cont.)

```
SwitchX#show interfaces FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001e.147c.bd01 (bia 001e.147c.bd01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
<output omitted>
  5 minute input rate 31000 bits/sec, 33 packets/sec
<output omitted>
--More--
```

- Displays statistics for selected interfaces on the switch.

© 2013 Cisco Systems, Inc.

The **show interfaces** command displays status and statistical information for the network interfaces of the switch. The resulting output varies, depending on the network for which an interface has been configured. Usually, this command is entered with the options *type* and *slot/number*. The *type* option allows values such as FastEthernet and GigabitEthernet, and the *slot/number* option indicates slot 0 and the port number on the selected interface (for example, fa0/1). The table shows some of the fields in the display that are useful for verifying fundamental switch details.

Output	Description
FastEthernet0/1 is up	Indicates the status of the interface hardware. In this example, it is functioning correctly. The hardware status is followed by the status of the line protocol, which in this example is also operational and active.
Full-duplex, 100 Mb/s	Shows the type and mode of connection. Other possibilities include half-duplex, 10 Mb/s.
5 minute input rate 31000 bits/sec	Reports interface traffic statistics for average input rate.

The **show interfaces** command is frequently used when you are configuring and monitoring network devices.

Verifying the Switch Initial Startup Status (Cont.)

```
SwitchX#show running-config
Building configuration...
<output omitted>
!
hostname SwitchX
!
<output omitted>
!
interface Vlan1
 ip address 172.20.137.5 255.255.255.0
!
ip default-gateway 172.20.137.1
!
<output omitted>
```

- Displays the current active configuration file of the switch.

© 2013 Cisco Systems, Inc.

The **show running-config** command displays the current running (active) configuration file of the switch. This command requires privileged EXEC mode access. The IP address, subnet mask, and default gateway settings are displayed here.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Physical switch installation must meet power and environmental requirements.
- Cisco IOS switches have several status LEDs that are generally green when the switch is functioning normally but turn amber when there is a malfunction.
- A console cable and port are needed to access the switch console and perform the initial configuration.
- Cisco IOS switches can be configured in the CLI using the global configuration mode and other configuration modes.
- You can verify switch hardware, software, and operational status using the **show version**, **show interfaces**, and **show running-config** commands.

© 2013 Cisco Systems, Inc.

Understanding Ethernet and Switch Operation

Overview

This lesson describes various Ethernet media options (copper and fiber), including the most common connectors and cable types. Ethernet frame structure and MAC addresses are discussed. In the second part of the lesson, switch operation, or switch frame processing, is described. Duplex options are described, collision domains are explained, and configuration examples for duplex settings are provided.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the types of Ethernet LAN connection media
- Describe the fields of an Ethernet frame
- Define the structure and function of MAC addresses
- Describe how switches operate
- Compare half-duplex and full-duplex operation
- Configure speed and duplex on an interface

Ethernet LAN Connection Media

This topic defines the types of Ethernet LAN connection media.

Ethernet LAN Connection Media

The mechanical properties of Ethernet depend on the type of physical medium:

- Coaxial (not used anymore)
- Copper
- Fiber-optic

Ethernet was originally based on the concept of computers communicating over a shared coaxial cable, sharing files and applications.



© 2013 Cisco Systems, Inc.

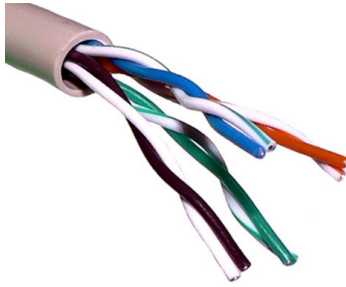
The mechanical properties of Ethernet depend on the type of physical medium in use, with coaxial, copper, fiber, and wireless media available. Although wireless is increasing in popularity for desktop connectivity, copper and fiber are the most popular physical layer media for network deployments.

Ethernet was originally based on the idea of computers communicating over a shared coaxial cable acting as a broadcast transmission medium. Originally, the shared coaxial cable of an Ethernet (the shared medium) connected every attached machine in a building or campus. A scheme known as CSMA/CD governed the way in which the computers shared the channel.

Through the first half of the 1980s, the 10BASE5 implementation of Ethernet used a coaxial cable with a diameter of 9.5 mm (0.375 inches), later called “thick Ethernet” or “thicknet.” Its successor, 10BASE2, also called “thin Ethernet” or “thinnet,” used a cable similar to the television cable of the era. The emphasis was on making installation of the cable easier and less costly. Modifying Ethernet to conform to the twisted-pair telephone wiring already installed in commercial buildings provided another opportunity to lower costs, expand the installed base, and leverage building design. Thus, twisted-pair Ethernet was the next logical development in the mid-1980s, beginning with StarLAN. UTP-based Ethernet became widely deployed with the 10BASE-T standard. This system replaced coaxial cable systems with a system of full-duplex switches linked via UTP.

Ethernet LAN Connection Media (Cont.)

- Modifying Ethernet to conform to existing twisted-pair telephone wiring enabled cost reduction.
- UTP-based Ethernet, which uses copper, became widely deployed after the 10BASE-T standard.
- Fiber-optic variants of Ethernet offer high performance, electrical isolation, and long distance (tens of kilometers with some versions).



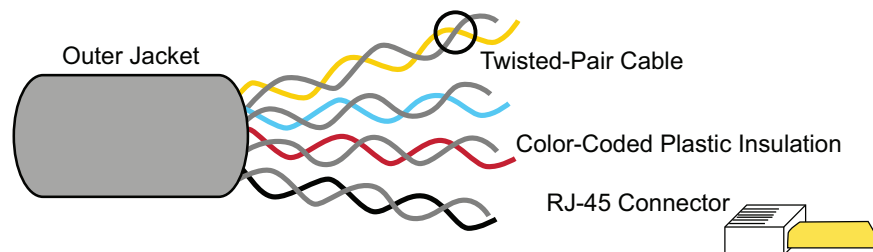
© 2013 Cisco Systems, Inc.

With the introduction of the 10BASE-T standard in 1990, Ethernet switches supplemented the half-duplex CSMA/CD scheme with a full-duplex system that offered higher performance at a lower cost than routers. With the arrival of 100BASE-T, Ethernet switches capable of mixed-speed and mixed-duplex operation were built.

The Ethernet physical layer evolved over a considerable time and now encompasses many physical media interfaces and several magnitudes of speed. Fiber-optic variants of Ethernet offer high performance, electrical isolation, and long distance (tens of kilometers with some versions). In general, network protocol stack software works similarly on all varieties.

Ethernet LAN Connection Media (Cont.)

Unshielded Twisted-Pair Cable



Characteristic	Value
Speed and throughput	From 10 Mb/s to 10 Gb/s
Average cost per node	Least expensive
Media and connector size	Small
Maximum cable length	Varies

© 2013 Cisco Systems, Inc.

Ethernet over twisted-pair technologies use twisted-pair cables for the physical layer of an Ethernet computer network. Twisted-pair cabling is a type of wiring in which two conductors (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling EMI from external sources (for example, electromagnetic radiation from UTP cables and crosstalk between neighboring pairs).

A UTP cable is a four-pair wire. Each of the eight individual copper wires in a UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other. The advantage of a UTP cable is its ability to cancel interference, because the twisted-wire pairs limit signal degradation from EMI and RFI. To further reduce crosstalk between the pairs in a UTP cable, the number of twists in the wire pairs varies. Cables must follow precise specifications regarding how many twists or braids are permitted per meter.

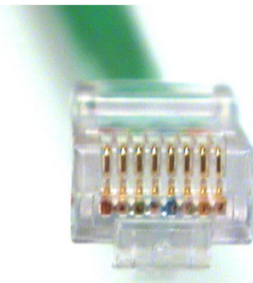
UTP cable is used in a variety of types of networks. When used as a networking medium, a UTP cable has four pairs of either 22- or 24-gauge copper wire. A UTP used as a networking medium has an impedance of 100 ohms, differentiating it from other types of twisted-pair wiring such as that used for telephone wiring. A UTP cable has an external diameter of approximately 0.43 cm (0.17 inches), and its small size can be advantageous during installation.

Several categories of UTP cable exist:

- **Category 1:** Used for telephone communications, not suitable for transmitting data
- **Category 2:** Capable of transmitting data at speeds of up to 4 Mb/s
- **Category 3:** Used in 10BASE-T networks—can transmit data at speeds up to 10 Mb/s
- **Category 4:** Used in Token Ring networks—can transmit data at speeds up to 16 Mb/s
- **Category 5:** Capable of transmitting data at speeds up to 100 Mb/s
- **Category 5e:** Used in networks running at speeds up to 1000 Mb/s (1 Gb/s)
- **Category 6:** Consists of four pairs of 24-gauge copper wires, which can transmit data at speeds of up to 1 Gb/s
- **Category 6a:** Used in networks running at speeds up to 10 Gb/s

Ethernet LAN Connection Media (Cont.)

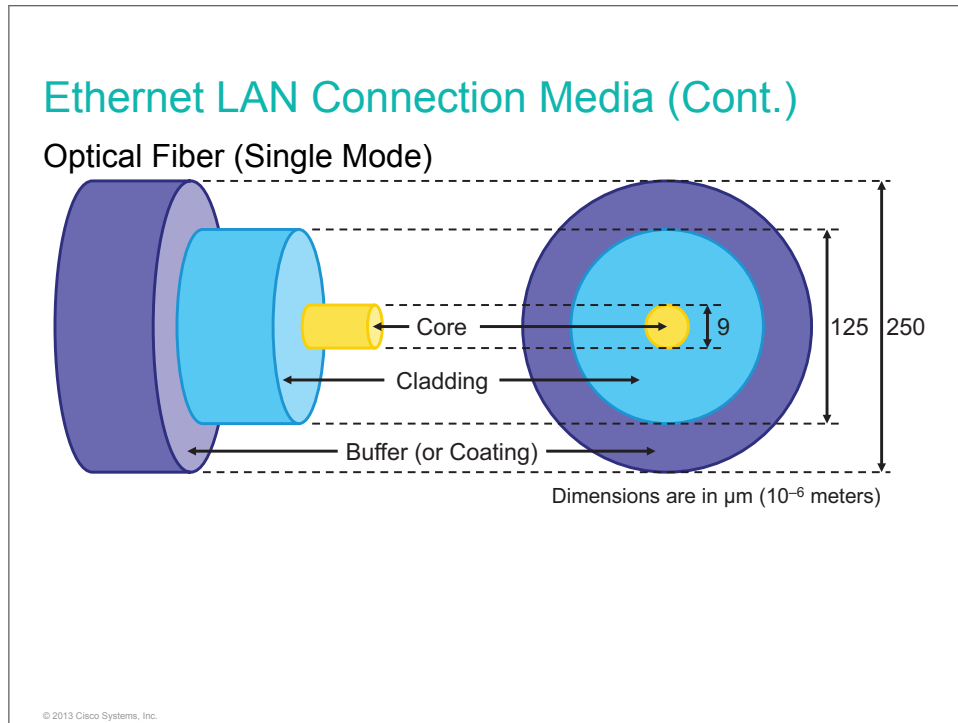
RJ-45 Connector and Jack



© 2013 Cisco Systems, Inc.

The RJ-45 plug is the male component, crimped at the end of the cable. As you look at the male connector from the front, as shown in the figure, the pin locations are numbered from 8 on the left to 1 on the right.

The jack is the female component in a network device, wall, cubicle partition outlet, or patch panel. As you look at the female connector from the front, as shown in the figure, the pin locations are numbered from 1 on the left to 8 on the right.



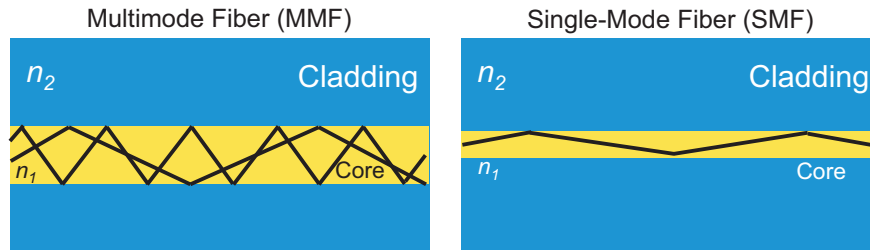
An optical fiber is a flexible, transparent fiber that is made of very pure glass (silica) and is not much larger than a human hair. It acts as a waveguide, or “light pipe,” to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communication, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and with immunity to electromagnetic interference.

The two fundamental components that allow a fiber to confine light are the core and the cladding. Most of the light travels from the beginning to the end inside the core. The cladding around the core provides confinement. The diameters of the core and cladding are shown in the figure, but the core diameter may vary for various fiber types. In this case, the core diameter of 9 µm is very small—the diameter of a human hair is about 50 µm. The outer diameter of the cladding is a standard size of 125 µm. Standardizing the size means that component manufacturers can make connectors for all fiber-optic cables.

The third element in this picture is the buffer (coating), which has nothing to do with the confinement of the light in the fiber. Its purpose is to protect the glass from scratches and moisture. The fiber-optic cable can be easily scratched and broken, like a glass pane. If the fiber is scratched, the scratch could propagate and break the fiber. Another important aspect is the need to keep the fiber dry.

Ethernet LAN Connection Media (Cont.)

Fiber Types



The most significant difference between SMF and MMF is in the ability of the fiber to send light over a long distance at high bit rates. In general, MMF is used for shorter distances at a lower bit rate than SMF. For long distance communications, SMF is preferred. There are many variations of fiber for both MMF and SMF.

The most significant physical difference is in the size of the core. The glass in the two fibers is the same, and the index of refraction change is similar. The core diameter can make a major difference. The diameter of the fiber cladding is universal for matching fiber ends.

The effect of having different-size cores in fiber is that the two fiber types will support various ways for the light to get through the fiber. MMF supports multiple ways for the light from one source to travel through the fiber (the source of the designation "multimode"). Each path can be thought of as a mode.

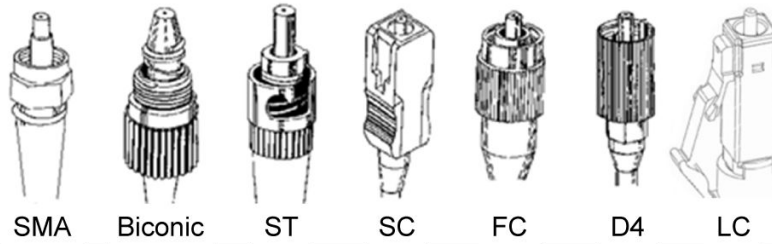
For SMF, the possible ways for light to get through the fiber have been reduced to one, a "single mode." It is not exactly one, but that is a useful approximation.

The table summarizes MMF and SMF characteristics.

MMF and SMF Characteristics

MMF Characteristics	SMF Characteristics
LED transmitter usually used	Laser transmitter usually used
Lower bandwidth and speed	Higher bandwidth and speed
Shorter distances	Longer distances
Less expensive	More expensive

Fiber Connector Types



© 2013 Cisco Systems, Inc.

An optical fiber connector terminates the end of an optical fiber. A variety of optical fiber connectors are available. The main differences among the types of connectors are dimensions and methods of mechanical coupling. Generally, organizations standardize on one type of connector, depending on the equipment that they commonly use, or they standardize per type of fiber (one for MMF, one for SMF). There are about 70 connector types in use today.

There are three types of connectors:

- Threaded
- Bayonet
- Push-pull

These materials are used for connectors:

- Metal
- Plastic sleeve

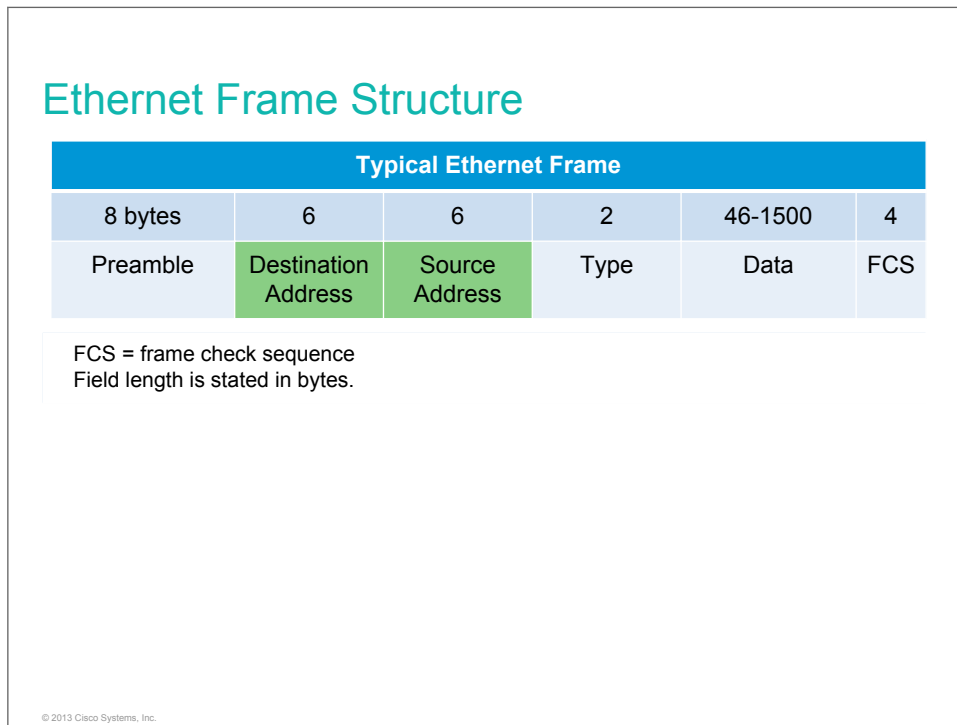
These are the most common types of connectors and their typical uses:

- ST: For patch panels (for their durability)
- FC: For patch panels, used by service providers
- SC: For enterprise equipment
- LC: For enterprise equipment, commonly used on SFP modules

In data communications and telecommunications applications today, small-form-factor connectors (for example, LCs) are replacing the traditional connectors (for example, SCs), mainly to pack more connectors on the faceplate and thus reduce system footprints.

Ethernet Frame Structure

Bits that are transmitted over an Ethernet LAN are organized into frames. This topic describes the structure of an Ethernet frame.



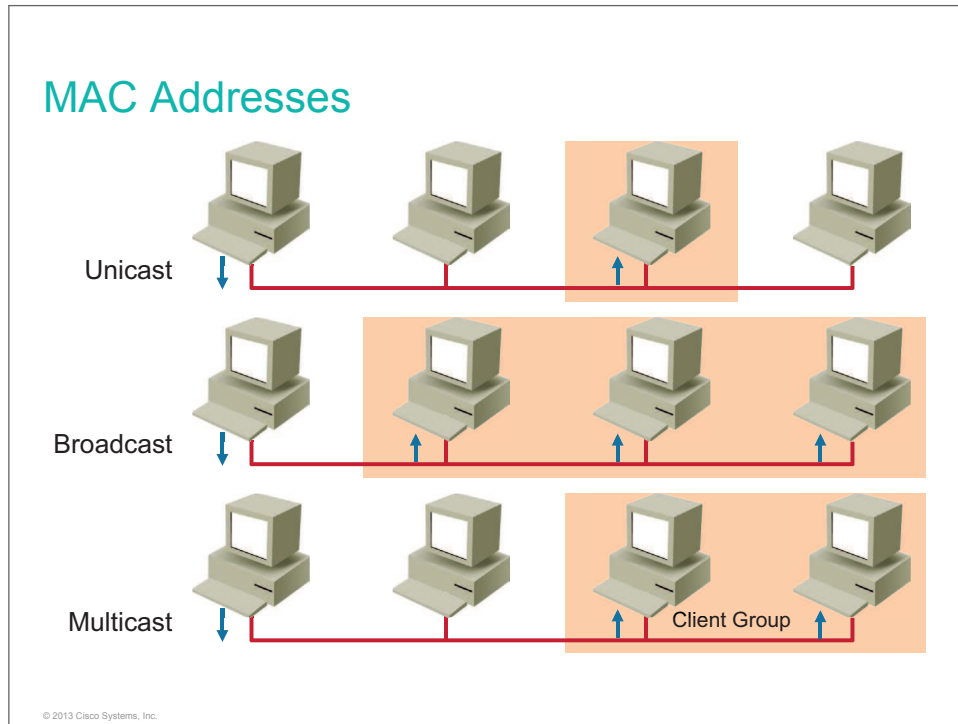
In Ethernet terminology, the container into which data is placed for transmission is called a *frame*. The frame contains header information, trailer information, and the actual data that is being transmitted.

The figure shows the most important fields of a MAC layer of the Ethernet frame:

- **Preamble:** This field consists of 8 bytes of alternating 1s and 0s that are used to synchronize the signals of the communicating computers.
- **Destination address:** This field contains the address of the NIC on the local network to which the packet is being sent.
- **Source address:** This field contains the address of the NIC of the sending computer.
- **Type or length:** In the Ethernet II standard, this field contains a code that identifies the network layer protocol. In the 802.3 standard, this field specifies the length of the data field. Therefore, the protocol information is contained in 802.2 fields, which are at the LLC layer that is contained in the 802.2 header and data field.
- **Data and pad:** This field contains the data that is received from the network layer on the transmitting computer. This data is then sent to the same protocol on the destination computer. If the data is shorter than the minimum length of 46 bytes, a string of extraneous bits is used to pad the field.
- **FCS:** The FCS field includes a checking mechanism to ensure that the packet of data has been transmitted without corruption.

MAC Addresses

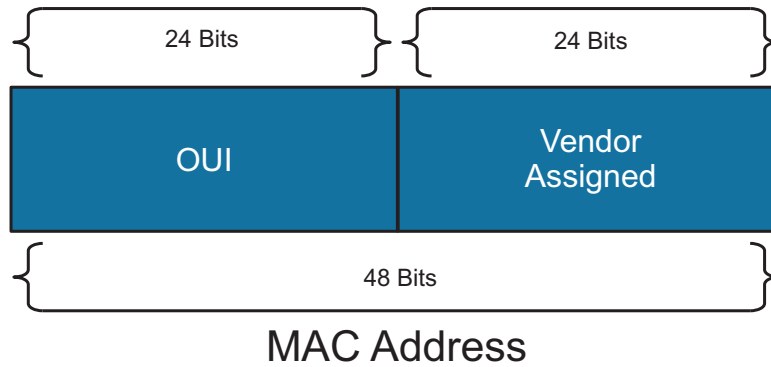
Communication in a network occurs in three ways: unicast, broadcast, and multicast. Ethernet frames are addressed accordingly. This topic describes the relationship of Ethernet frames to methods of network communications.



There are three major types of network communications:

- **Unicast:** Communication in which a frame is sent from one host and addressed to one specific destination. In a unicast transmission, there is just one sender and one receiver. Unicast transmission is the predominant form of transmission on LANs and within the Internet.
- **Broadcast:** Communication in which a frame is sent from one address to all other addresses. In this case, there is just one sender, but the information is sent to all the connected receivers. Broadcast transmission is essential for sending the same message to all devices on the LAN.
- **Multicast:** Communication in which information is sent to a specific group of devices or clients. Unlike broadcast transmission, in multicast transmission, clients must be members of a multicast group to receive the information.

MAC Addresses (Cont.)



© 2013 Cisco Systems, Inc.

The address that is on the NIC is the MAC address, which is often referred to as the BIA. Some vendors allow modification of this address to meet local needs. There are two components of a 48-bit Ethernet MAC address:

- **24-bit OUI:** The OUI identifies the manufacturer of the NIC. The IEEE regulates the assignment of OUI numbers.
- **24-bit vendor-assigned end-station address:** This portion uniquely identifies the Ethernet hardware.

MAC Addresses (Cont.)

Different display formats:

- 0000.0c43.2e08
- 00:00:0c:43:2e:08
- 00-00-0C-43-2E-08

© 2013 Cisco Systems, Inc.

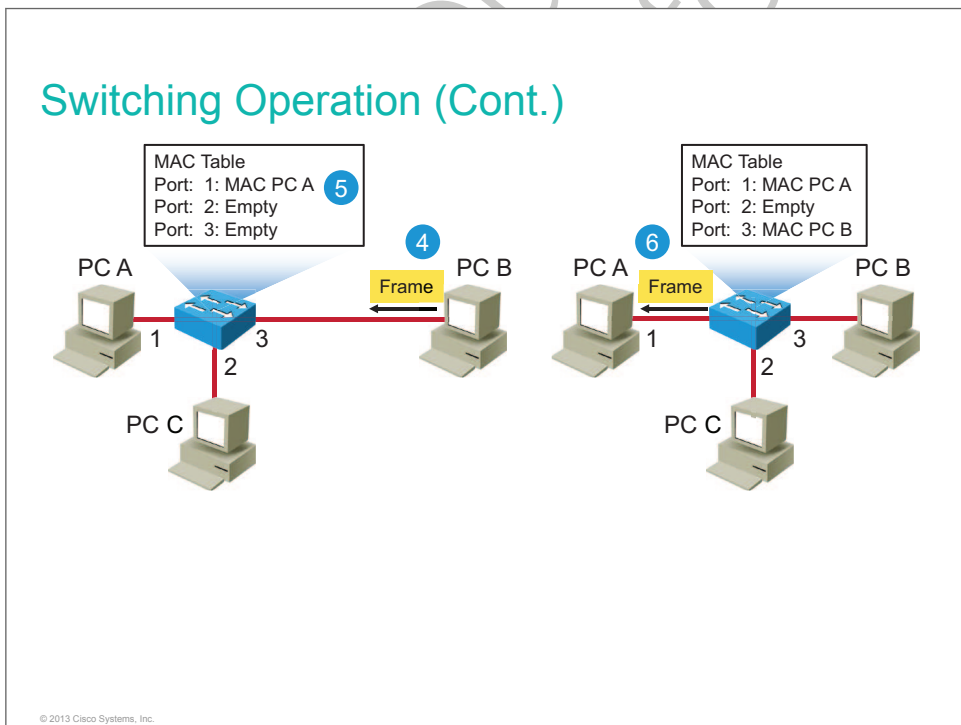
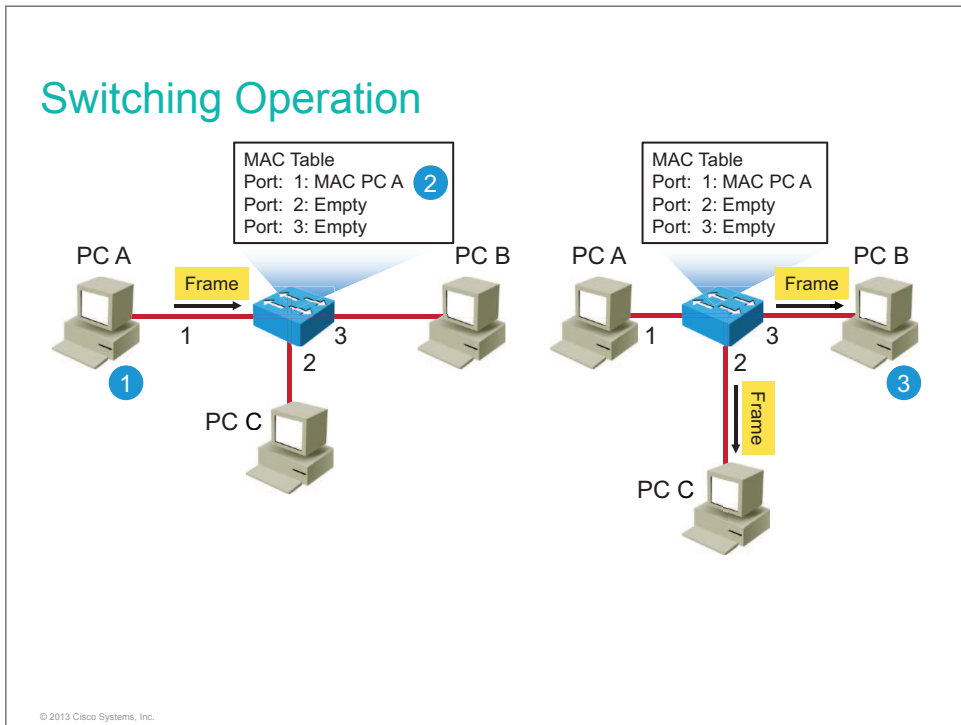
The MAC sublayer of the TCP/IP link layer processes physical addressing issues. The physical address is a number in hexadecimal format that is actually burned into the NIC. This address is referred to as the *MAC address*, and it is expressed as groups of hexadecimal digits that are organized in pairs or quads, such as 0000.0c43.2e08, 00:00:0c:43:2e:08, or 00-00-0C-43-2E-08. Note that various systems use various display formats.

Each device on a LAN must have a unique MAC address to participate in the network. The MAC address identifies the location of a specific computer on a LAN. Unlike other kinds of addresses that are used in networks, the MAC address should not be changed unless there is some specific need to do so.

Do Not Duplicate.
Post beta, not for release.

Switching Operation

This topic describes how switches process and transmit frames based on MAC addresses.



The switch builds and maintains a table, called a MAC table, that matches a destination MAC address with the port used to connect to a node. The MAC table is stored in CAM, which enables very fast lookups.

For each incoming frame, the destination MAC address in the frame header is compared to the list of addresses in the MAC table. Switches then use MAC addresses as they decide whether to filter, forward, or flood frames.

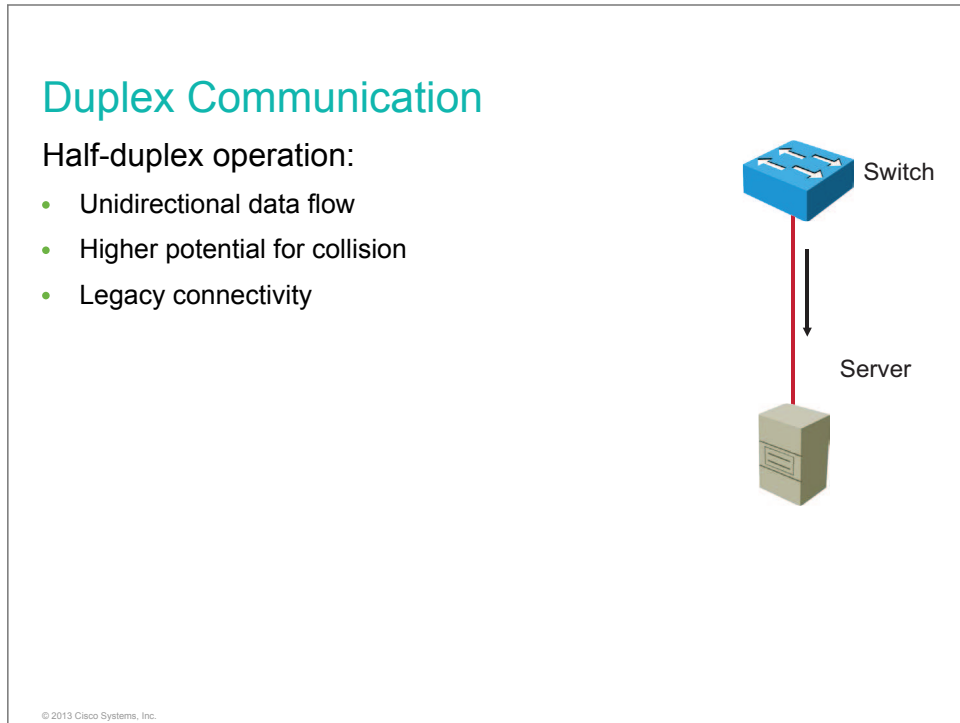
The switch creates and maintains a table using the source MAC addresses of incoming frames and the port number through which the frame entered the switch. When an address is not known, a switch learns the network topology by analyzing the source address of incoming frames from all of the attached networks. The table describes the switching process:

Switching Frames Procedure

Step	Action
1	The switch receives a frame from PC A on port 1.
2	The switch enters the source MAC address and the switch port that received the frame into the MAC table.
3	The switch checks the table for the destination MAC address. Because the destination address is not known, the switch floods the frame to all the ports except the port on which it received the frame.
4	The destination device with the matching MAC address replies to the broadcast with a unicast frame addressed to PC A.
5	The switch enters the source MAC address of PC B and the port number of the switch port that received the frame into the MAC table. The destination address of the frame and its associated port is found in the MAC table.
6	The switch can now forward frames between the source and destination devices without flooding because it has entries in the MAC table that identify the associated ports.

Duplex Communication

Full-duplex communication increases effective bandwidth by allowing both ends of the connection to transmit simultaneously. However, this method of optimizing network performance requires microsegmentation before full-duplex communication can occur. This topic describes half-duplex and full-duplex communication and illustrates how full-duplex communication can improve the performance of a switched LAN.



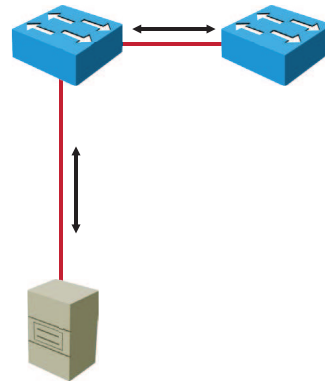
Half-duplex communication relies on a unidirectional data flow, where sending and receiving data are not performed at the same time. This behavior is similar to walkie-talkies or two-way radios in that only one person can talk at a time. If someone talks while another person is speaking, a collision occurs. As a result, half-duplex communication implements Ethernet CSMA/CD to help reduce the potential for collisions and to detect them when they do happen.

Half-duplex communication has performance issues that stem from the constant waiting, because data can flow in only one direction at a time. Half-duplex connections are typically seen in older hardware such as hubs. Nodes that are attached to hubs that share their connection to a switch port must operate in half-duplex mode because the end computers must be able to detect collisions. Nodes can operate in a half-duplex mode if the NIC cannot be configured for full-duplex operations. In this case, the port on the switch operates in half-duplex mode as well. Because of these limitations, full-duplex communication has replaced half duplex in more current hardware.

Duplex Communication (Cont.)

Full-duplex operation:

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends



© 2013 Cisco Systems, Inc.

In full-duplex communication, the data flow is bidirectional, so data can be sent and received at the same time. The bidirectional support enhances performance by reducing the wait time between transmissions. Most Ethernet, Fast Ethernet, and Gigabit Ethernet NICs offer full-duplex capability. Frames that are sent by the two connected end nodes cannot collide, because the end nodes use two separate circuits in the network cable. Each full-duplex connection uses only one port. Full-duplex connections require a switch that supports full duplex or a direct connection between two nodes that each support full duplex. Nodes that are directly attached to a dedicated switch port with NICs that support full duplex should be connected to switch ports that are configured to operate in full-duplex mode.

Configuring Duplex and Speed Options

This topic describes how to configure speed and duplex on an interface.

Configuring Duplex and Speed Options

- Setting full duplex and 100-Mb/s speed settings on the FastEthernet0/5
- Setting auto-duplex and auto-speed settings on the FastEthernet0/1

```
SwitchX(config)#interface FastEthernet0/1
SwitchX(config-if)#duplex full
SwitchX(config-if)#speed 100
SwitchX(config-if)#interface FastEthernet0/5
SwitchX(config-if)#duplex auto
SwitchX(config-if)#speed auto
```

General recommendation:

- Use manual settings on infrastructure links.
- Use auto settings on ports toward end devices.

© 2013 Cisco Systems, Inc.

The duplex parameters on the Cisco Catalyst 2960 Series Switch are as follows:

- The **auto** option sets autonegotiation of duplex mode. With autonegotiation enabled, the two ports communicate to decide the best mode of operation.
- The **full** option sets full-duplex mode.
- The **half** option sets half-duplex mode.

For Fast Ethernet and 10/100/1000 ports, the default option is **auto**. For optical 100BASE-FX ports, the default is **full**. The 10/100/1000 ports operate in either half- or full-duplex mode when they are set to 10 or 100 Mb/s, but when they are set to 1000 Mb/s, they operate only in full-duplex mode.

A general recommendation is to manually set the duplex mode and speed on ports between infrastructure devices. In the figure, ports between the switches are manually set. On ports toward users and on end devices, autonegotiation is suggested. This simplifies the administration when users frequently connect different end devices to the network. The port toward PC1 in the figure is configured with autonegotiation, which is also the default option for Fast Ethernet ports.

Configuring Duplex and Speed Options (Cont.)

Overview of duplex settings and the resulting operation

Duplex settings	Half	Full	Auto
Half	Half	Mismatch	Half
Full	Mismatch	Full	Full
Auto	Half	Full	Full

© 2013 Cisco Systems, Inc.

The table in the figure shows combinations of duplex settings on a link between two devices. A mismatch state makes a link nonoperational, while half-duplex enables low performance connectivity. If devices support it, full-duplex connectivity is preferred.

Autonegotiation can sometimes produce unpredictable results. By default, when autonegotiation fails, the Catalyst switch sets the corresponding Fast Ethernet switch port to half-duplex mode. This type of failure happens when an attached device does not support autonegotiation. If the device is manually configured to operate in half-duplex mode, it matches the default mode of the switch. However, autonegotiation errors can happen if the device is manually configured to operate in full-duplex mode. This configuration, half duplex on one end and full duplex on the other end, causes late collision errors at the half-duplex end. To avoid this situation, manually set the duplex parameters of the switch to match the attached device.

Configuring Duplex and Speed Options (Cont.)

Verify the duplex and speed settings on the FastEthernet0/5 interface.

```
SwitchX#show interfaces FastEthernet0/5
FastEthernet0/5 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
<output omitted>
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  7289 packets input, 927927 bytes, 0 no buffer
  Received 184 broadcasts (1380 multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 1380 multicast, 0 pause input
  0 input packets with dribble condition detected
  39965 packets output, 7985339 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
```

Verify the duplex settings by using the **show interfaces** command on the Cisco Catalyst 2960 Series Switch. The **show interfaces** privileged EXEC command displays statistics and the status for all interfaces or specified interfaces. The figure shows the duplex and speed settings of a Fast Ethernet interface.

If the switch port is in full-duplex mode and the attached device is in half-duplex mode, check for CRC errors on the full-duplex switch port.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Ethernet over twisted-pair technologies use twisted-pair cables for the physical layer of an Ethernet computer network. Optical fiber permits transmission over longer distances and at higher data rates.
- The Ethernet frame contains header information, trailer information, and the actual data that is being transmitted.
- An Ethernet MAC address consists of two parts: OUI and a vendor-assigned end-station address.
- The switch creates and maintains a MAC address table by using the source MAC addresses of incoming frames and the port number through which the frame entered the switch.
- Full-duplex communication increases effective bandwidth by allowing both ends of the connection to transmit simultaneously.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Troubleshooting Common Switch Media Issues

Overview

Most issues that affect a switched network are encountered during the original implementation. After a network is installed, it should continue to operate without problems. However, that is only true in theory. Cabling becomes damaged, configurations change, and new devices are connected to the switch that require switch configuration changes. Ongoing maintenance is necessary. This lesson describes the most common media and port issues and how to troubleshoot them.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe common tools for connectivity verification
- Identify common switched network media issues
- Troubleshoot switched network media issues
- Identify common access port issues
- Troubleshoot common access port issues

Common Troubleshooting Tools

This topic describes common troubleshooting tools that can be used when verifying network connectivity.

Common Troubleshooting Tools

ping command

```
Switch#ping 10.1.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
```

```
C:\>ping example.com
Pinging example.com [192.0.43.10] with 32 bytes of data:
Reply from 192.0.43.10: bytes=32 time=107ms TTL=243
Reply from 192.0.43.10: bytes=32 time=107ms TTL=243
Reply from 192.0.43.10: bytes=32 time=137ms TTL=243
Reply from 192.0.43.10: bytes=32 time=107ms TTL=243
Ping statistics for 192.0.43.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 107ms, Maximum = 137ms, Average = 114ms
```

© 2013 Cisco Systems, Inc.

The **ping** command is a utility for testing IP connectivity between hosts. It sends out requests for responses from a specified host address. The **ping** command uses a Layer 3 protocol that is a part of the TCP/IP suite called **ICMP**, and it uses the ICMP echo request and ICMP echo reply packets.

If the host at the specified address receives the ICMP echo request, it responds with an ICMP echo reply packet. For each packet sent, the **ping** command measures the time that is required to receive the response. As each response is received, the **ping** command displays the time between the request being sent and when the response is received. By using interval timing and response rates, the **ping** command estimates the **RTT**, generally in milliseconds, and the packet-loss rate between hosts. The RTT is a measure of the network performance.

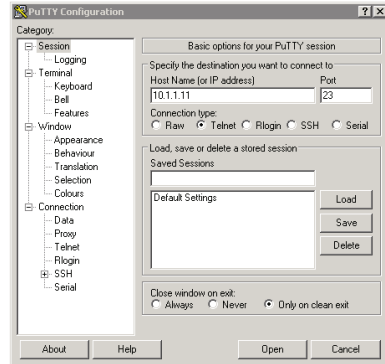
The **ping** command is supported on most devices connected to the network, including network devices such as switches and routers, and different operating systems running on a PC such as Windows, Mac, or Linux.

In the figure, the first output illustrates the use of the **ping** command on the Cisco Catalyst switch, while the second output shows **ping** verification on a PC running Windows.

Common Troubleshooting Tools (Cont.)

Telnet

```
Switch1#telnet 10.1.20.1
Trying 10.1.20.1 ... Open
Switch2>
```



Telnet provides the capability to remotely access another computer, servers, and networking devices. Telnet enables a user to log in to a remote host and execute commands. It is also used to verify connectivity with a remote host.

Cisco IOS devices can also be used as a Telnet client to connect to other devices. You can initiate a Telnet session with the **telnet** command.

Some operating systems on a PC include built-in Telnet clients. On others, you can install a client as an add-on or use a dedicated application that includes a Telnet client. An application named PuTTY, shown in the figure, is one example of a free open-source Telnet client.

Media Issues

This topic describes the methods of identifying common switched network media issues.

Media Issues – Copper

Copper media issues have several possible sources:

- Wiring becomes damaged.
- New EMI sources are introduced.
- Traffic patterns change.
- New equipment is installed.

© 2013 Cisco Systems, Inc.

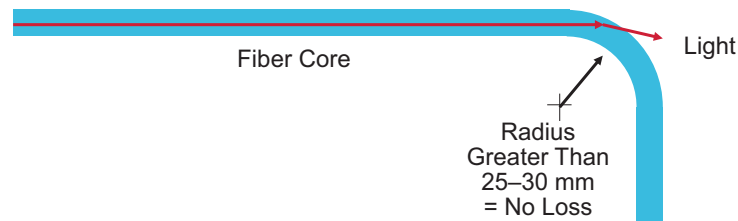
Media issues are common. Here are some examples of common situations that can cause media issues:

- In an environment using Category 3 wiring, the maintenance crew installs a new air conditioning system that introduces new EMI sources into the environment.
- In an environment using Category 5 wiring, cabling is run too close to an elevator motor.
- Poor cable management puts a strain on some RJ-45 connectors, causing one or more wires to break.
- New applications change traffic patterns.
- When new equipment is connected to a switch, the connection operates in half-duplex mode, or a duplex mismatch occurs, which could lead to an excessive number of collisions.

Media Issues – Fiber

Fiber media issues have these possible sources:

- Macrobend losses:
 - Bending the fiber in too small a radius causes light to escape.
 - Light strikes the core or cladding at less than the critical angle.
 - Total internal reflection no longer happens, and light leaks out.
- Splice losses



© 2013 Cisco Systems, Inc.

There are several ways in which light can be lost from the fiber. Some of these are manufacturing problems (for example, microbends, macrobends, and splicing fibers that do not have their cores centered), while others are physics problems (back reflections), because light reflects whenever it encounters a change in the index of refraction.

Macrobends are typically applied to the fiber during fiber installation.

There is another explanation for why light leaks out at a macrobend. Part of the traveling wave, called the evanescent wave, travels inside the cladding. Around the bend, part of the evanescent wave must travel faster than the speed of light in the material. This is not possible, so that part radiates out of the fiber.

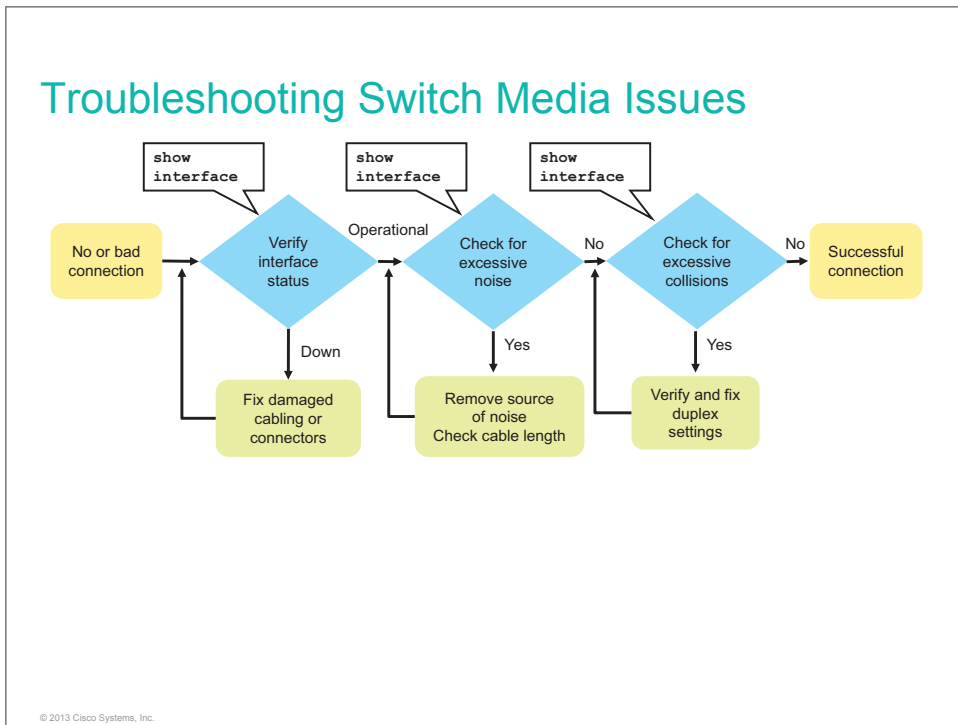
Bend losses can be minimized by designing a larger index difference between the core and the cladding. Another approach is to operate at the shortest possible wavelength and perform good installations.

Splices are a way to connect two fibers by fusing their ends. The best way to align the fiber core is by using the outside diameter of the fiber as a guide. If the core is at the center of the fiber, a good splice can be achieved. If the core is off center, then it is impossible to create a good splice. You would have to cut the fiber further upstream and test again.

Another possibility is that the fibers to be spliced could have dirt on their ends. Dirt can cause many problems, particularly if the dirt intercepts some or all of the light from the core. Recall that the core for SMF is only 9 μm .

Troubleshooting Switch Media Issues

This topic describes how to troubleshoot switched network media issues.



To troubleshoot switch media issues when you have no connection or a bad connection between a switch and another device, follow this process:

1. Use the **show interface** command to check the interface status. If the interface is not operational, check the cable and connectors for damage.
2. Use the **show interface** command to check for excessive noise. If there is excessive noise, first find and remove the source of the noise, if possible. Verify that the cable does not exceed the maximum cable length and check the type of cable that is used. For copper cable, it is recommended that you use at least Category 5.
3. Use the **show interface** command to check for excessive collisions. If there are collisions or late collisions, verify the duplex settings on both ends of the connection.

Note A counter shows excessive values when it is constantly increasing while performing sequential verification of counter values.

Troubleshooting Switch Media Issues (Cont.)

Verify interface status.

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
```

Interface Status	Line Protocol Status	Link State
Up	Up	Operational
Up	Down	Connection problem
Down	Down (not connected)	Cable unplugged; other end of the link disconnected or interface in shutdown mode
Down	Down	Interface problem
Administratively down	Down	Disabled

One of the most important elements of the **show interface** command output is the display of the line and data link protocol status. This figure highlights the key summary line to check in the command output, and the status meanings for an interface.

The first parameter (Interface Status) refers to the hardware layer and, essentially, reflects whether the interface is receiving the carrier detect signal from the other end. The second parameter (Line Protocol Status) refers to the data link layer and reflects whether the data link layer protocol keepalives are being received.

Based on the output of the **show interface** command, possible problems can be defined as follows:

- If the interface is up and the line protocol is down, a problem exists. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
- If the line protocol and the interface are both down, a cable is not attached or some other interface problem exists. For example, in a back-to-back connection, the other end of the connection may be administratively down.
- If the interface is administratively down, it has been manually disabled (the **shutdown** command has been issued) in the active configuration.

Interface Status Verification

Excessive noise:

- Presence of many CRC errors
- Inspect the cable for damage and correct length, and search for noise sources

Excessive collisions:

- Normal in half-duplex operations
- Configure the link to use full-duplex

Excessive late collisions:

- Indicates duplex mismatch
- Configure both ends of the link to use the same duplex settings

© 2013 Cisco Systems, Inc.

Based on the output of the **show interface** command, you can find, diagnose, and correct the problem.

If you see many CRC errors, there is too much noise on the link and you should inspect the cable for damage and length. You should also search for and eliminate noise sources, if possible.

Collisions will occur in networks where half duplex is being used. Collisions in half-duplex operations are normal and you should not be concerned about them, as long as you are pleased with the half-duplex operations. However, you should never see collisions in a correctly designed and configured network that uses full duplex. It is highly recommended that you use full duplex unless you have older or legacy equipment that does not support full duplex.

Late collision refers to a collision that occurs after the preamble is transmitted. Late collisions occur when you have serious problems in a switched network, such as duplex misconfiguration. For example, you could have one end of a connection configured for full duplex and the other for half duplex. You would see late collisions on an interface that is configured for half duplex. In that case, you must configure the same duplex setting on both ends.

Interface Status Verification (Cont.)

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0 throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  1935 output errors, 1790 collisions, 10 interface resets
  0 unknown protocol drops
  0 babbles, 135 late collision, 0 deferred
<output omitted>
```

- Displays interface status and statistics.

© 2013 Cisco Systems, Inc.

The figure shows an example of **show interface** command output. The example shows counters and statistics for the FastEthernet0/1 interface.

The table describes some of the parameters in the **show interface** command output.

Parameter	Description
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision. This often happens on half-duplex links when two devices transmit frames at the same time.
Late collisions	Jammed signal could not reach to ends. Caused by duplex mismatch or by exceeded Ethernet cable length limits.


Port Issues

This topic describes the methods of identifying common port access issues.


Port Issues

Most common port issues are related to duplex and speed issues.

Duplex-related issues result from a mismatch in duplex settings:



Speed-related issues result from a mismatch in speed settings:



© 2013 Cisco Systems, Inc.

A common issue with speed and duplex occurs when the duplex settings are mismatched between two switches, between a switch and a router, or between a switch and a workstation or server. This mismatch can occur when you manually hard-code the speed and duplex, or from autonegotiation issues between the two devices.

Port Issues (Cont.)

These are examples of duplex-related issues:

- One end set to full duplex and the other set to half duplex results in a mismatch.
- One end is set to full duplex and the other is set to autonegotiation:
 - Autonegotiation fails, and that end reverts to half duplex.
 - It results in a mismatch.
- One end is set to half duplex and the other is set to autonegotiation:
 - Autonegotiation fails, and that end reverts to half duplex.
 - Both ends are set to half duplex, and there is no mismatch.

© 2013 Cisco Systems, Inc.

Port Issues (Cont.)

More examples of duplex-related issues:

- Autonegotiation is set on both ends:
 - One end fails to full duplex, and the other end fails to half duplex.
 - Example: A Gigabit Ethernet interface defaults to full duplex, while a 10/100 defaults to half duplex.
- Autonegotiation is set on both ends:
 - Autonegotiation fails on both ends, and they both revert to half duplex.
 - Both ends are set to half duplex, and there is no mismatch.



© 2013 Cisco Systems, Inc.

Duplex mismatch is a situation in which the switch operates at full duplex and the connected device operates at half duplex, or vice versa. The result of a duplex mismatch is extremely slow performance, intermittent connectivity, and loss of connection. Other possible causes of data-link errors at full duplex are bad cables, a faulty switch port, or NIC software or hardware issues.

Use the **show interface** command to verify the duplex settings.

If the mismatch occurs between two Cisco devices with Cisco Discovery Protocol enabled, you will see Cisco Discovery Protocol error messages on the console or in the logging buffer of both devices. Cisco Discovery Protocol is useful to detect errors as well as to gather port and system statistics on nearby Cisco devices. Whenever there is a duplex mismatch (in this example, on the FastEthernet0/1 interface), these error messages are displayed on the switch consoles of Catalyst switches that run Cisco IOS Software:

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not half duplex)
```

Additionally, for switches with Cisco IOS Software, these messages appear for link up or down situations (in this example, on the FastEthernet0/1 interface):

```
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up  
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Port Issues (Cont.)

These are examples of speed-related issues:

- One end is set to one speed and the other is set to another speed, resulting in a mismatch.
- One end is set to a higher speed and autonegotiation is enabled on the other end:
 - If autonegotiation fails, switch senses what the other end is using and reverts to optimal speed.
- Autonegotiation is set on both ends:
 - Autonegotiation fails on both ends, and they revert to their lowest speed.
 - Both ends are set at lowest speed, and there is no mismatch.

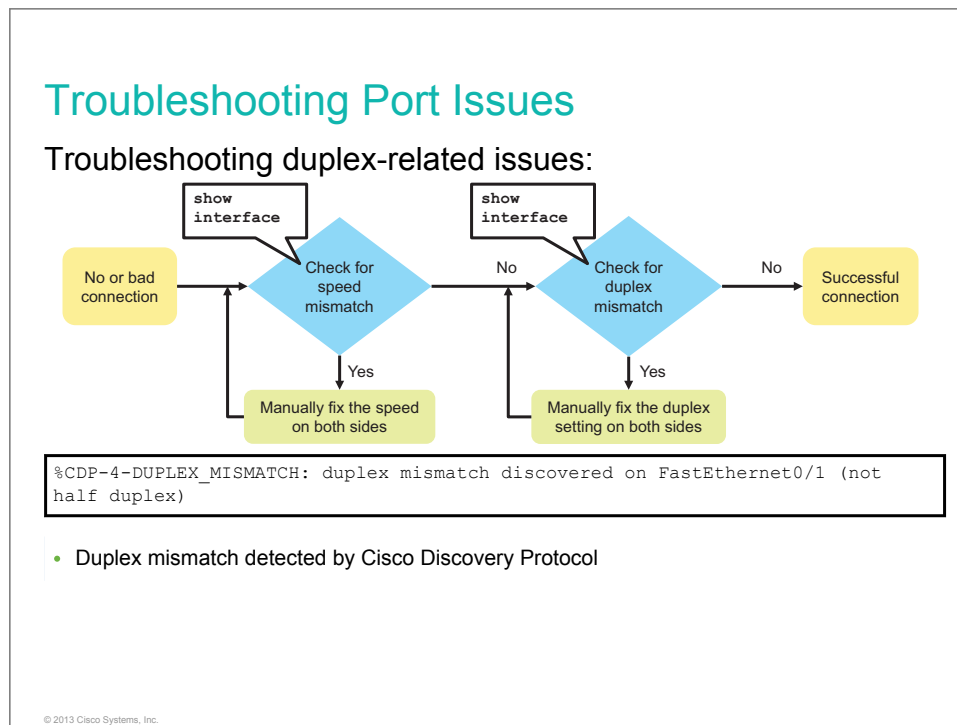


© 2013 Cisco Systems, Inc.

Use the **show interface** command to verify the speed settings.

Troubleshooting Port Issues

This topic describes how to troubleshoot common port access issues.



To troubleshoot switch port issues when you have no connection or a bad connection between a switch and another device, use this general process:

1. Use the **show interface** command to check whether there is a speed mismatch between the switch and a device on the other side (switch, router, server, and so on). If there is a speed mismatch, set the speed on both sides to the same value.
2. Use the **show interface** command to check whether there is a duplex mismatch between the switch and a device on the other side. It is recommended that you use full duplex if both sides support it.

Troubleshooting Port Issues (Cont.)

```
Switch#show interfaces FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 001e.147c.6f01 (bia 001e.147c.6f01)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:28, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
```

- Displays duplex and speed statistics.

© 2013 Cisco Systems, Inc.

The figure shows an example of **show interface** command output. The example highlights duplex and speed settings for interface FastEthernet0/1.

Based on the output of the **show interface** command, you can find, diagnose, and correct the duplex or speed mismatch between the switch and the device on the other side.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Use **ping** and **telnet** to verify connectivity.
- Switch media issues are common and have several possible sources, such as damaged copper wiring, EMI, and macrobend and splice losses in fiber media.
- Speed or duplex mismatch on a link leads to serious performance degradation.
- Use the **show interface** verification command when troubleshooting speed and duplex port issues.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- A network is a connected collection of devices (computers, interconnections, routers, and switches) that can communicate with each other, providing the means for users to share hardware and applications.
- TCP/IP defines four categories of functions that must occur for communications to be successful (the network access, Internet, transport, and application layers).
- A LAN is a network that is located in a limited area, with the computers and other components that are part of this network located relatively close together.
- Ethernet switches divide collision domains and reduce the number of devices that are competing for bandwidth. Ethernet switches selectively forward individual frames from a receiving port to the destination port.

Module Summary (Cont.)

- Cisco IOS Software provides network services to Cisco products to perform various internetworking functions.
- Ethernet over twisted-pair technologies use twisted-pair cables for the physical layer of an Ethernet computer network. Optical fibers permit transmission over longer distances and at higher data rates.
- The switch creates and maintains a MAC address table by using the source MAC addresses of incoming frames and the port number through which the frame entered the switch.
- Switch media issues are common and have several possible sources, such as damaged copper wiring, EMI sources, and macrobend and splice losses in fiber media.
- Speed or duplex mismatch on a link leads to serious performance degradation.

© 2013 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which three statements about networks are accurate? (Choose three.) (Source: Exploring the Functions of Networking)
 - A. Networks are used to transmit data in various environments, including homes, small businesses, and large enterprises.
 - B. A main office can have hundreds or even thousands of people who depend on network access to do their jobs.
 - C. A network is a connected collection of devices that can communicate with each other.
 - D. A main office usually has one large network to connect users.
 - E. The purpose of a network is to create a means to provide workers with access to all information and components that are accessible via the network.
 - F. Remote locations cannot connect to a main office through a network.

2. Match each network characteristic to its definition. (Source: Exploring the Functions of Networking)

A. scalability	<input type="checkbox"/>	indicates how fast data is transmitted over the network
B. speed	<input type="checkbox"/>	indicates the probability that the network will be available for use
C. cost	<input type="checkbox"/>	indicates the structure of the network
D. availability	<input type="checkbox"/>	indicates the general price of components, installation, and maintenance of the network
E. security	<input type="checkbox"/>	indicates the dependability of the network
F. topology	<input type="checkbox"/>	indicates how well the network can accommodate more users or data transmission requirements
G. reliability	<input type="checkbox"/>	indicates the protection level of the network itself and the data that is transmitted

3. Which two statements about the purpose of the TCP/IP model are accurate? (Choose two.) (Source: Understanding the Host-to-Host Communications Model)
- A. The TCP/IP model defines the network functions that occur at each layer.
 - B. The TCP/IP model facilitates an understanding of how information travels throughout a network.
 - C. The TCP/IP model ensures reliable data delivery through its layered approach.
 - D. The TCP/IP model defines seven layers.
4. Match each TCP/IP layer to its function. (Source: Understanding the Host-to-Host Communications Model)
- | | | |
|----------------------|--------------------------|--|
| A. application layer | <input type="checkbox"/> | supports communication between end devices across diverse networks |
| B. internet layer | <input type="checkbox"/> | provides logical addressing and determines the best path through the network |
| C. link layer | <input type="checkbox"/> | controls the hardware devices and media that make up the network |
| D. transport layer | <input type="checkbox"/> | deals with human interaction and the implementation of software applications and related protocols |
5. Which two statements about switches are accurate? (Choose two.) (Source: Introducing LANs)
- A. They operate only at the internet layer of the TCP/IP model.
 - B. They forward, filter, or flood frames based on MAC table entries.
 - C. A hub is a newer and better version of a switch.
 - D. Their three major functions are forwarding, filtering, and flooding.
6. Which CLI prompt indicates that you are working in privileged EXEC mode? (Source: Operating Cisco IOS Software)
- A. hostname#
 - B. hostname>
 - C. hostname-exec>
 - D. hostname-config
7. Which command would you enter in privileged EXEC mode to list the command options? (Source: Operating Cisco IOS Software)
- A. ?
 - B. **init**
 - C. **enable**
 - D. **login**
8. Which CLI command would you enter to display a list of commands that begin with the letter “c”? (Source: Operating Cisco IOS Software)
- A. **c?**
 - B. **c ?**
 - C. **help c**
 - D. **help C**

9. Match each step of the physical Cisco Catalyst switch startup process to its description. (Source: Starting a Switch)
- A. Step 3 Verify that all cable connections are secure, the terminal is connected to the console port, and the console terminal application is selected.
 - B. Step 2 Observe the boot sequence, including the Cisco IOS Software output text on the console.
 - C. Step 1 Attach the power cable plug to the power supply socket of the switch.
10. Which configuration mode would you use to configure a particular port on a switch? (Source: Starting a Switch)
- A. user EXEC mode
 - B. global configuration mode
 - C. interface configuration mode
 - D. controller configuration mode
11. Match the types of traffic with their description. (Source: Understanding Ethernet and Switch Operation)
- A. multicast A frame is sent from one address to all other addresses.
 - B. broadcast A frame is sent from one address to multiple addresses.
 - C. unicast A frame is sent from one address to a single address.
12. Which CLI prompt indicates the correct way to set the port duplex operation to full? (Source: Understanding Ethernet and Switch Operation)
- A. SwitchX(config-if)#**duplex half**
 - B. SwitchX>**duplex full**
 - C. SwitchX(config-if)#**duplex full**
 - D. SwitchX(config)#**full duplex**
13. Which Cisco IOS command is the most useful for troubleshooting media issues? (Source: Troubleshooting Common Switch Media Issues)
- A. **show controller**
 - B. **show troubles**
 - C. **show counters**
 - D. **show interface**

14. Issuing a **show interface FastEthernet 0/1** command resulted in output that stated "FastEthernet0/1 is up, line protocol is down." What does this message mean? (Source: Troubleshooting Common Switch Media Issues)
- A. The link is fully functional.
 - B. The interface has been manually disabled (the **shutdown** command has been issued) in the active configuration.
 - C. There could be an encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
 - D. A cable is not attached, or some other interface problem exists. For example, in a back-to-back connection, the other end of the connection may be administratively down.

Do Not Duplicate:
Post beta, not for release.

Answer Key

1. A, B, C
2. A. speed indicates how fast data is transmitted over the network
B. cost indicates the general price of components, installation, and maintenance of the network
C. security indicates the protection level of the network itself and the data that is transmitted
D. availability indicates the probability that the network will be available for use
E. scalability indicates how well the network can accommodate more users or data transmission requirements
F. reliability indicates the dependability of the network
G. topology indicates the structure of the network
3. A, B
4. A. application layer deals with human interaction and the implementation of software applications and related protocols
B. transport layer supports communication between end devices across diverse networks
C. internet layer provides logical addressing and determines the best path through the network
D. link layer controls the hardware devices and media that make up the network
5. B, D
6. A
7. A
8. A
9. A. Step 1 Verify that all cable connections are secure, the terminal is connected to the console port, and the console terminal application is selected.
B. Step 2 Attach the power cable plug to the power supply socket of the switch.
C. Step 3 Observe the boot sequence, including the Cisco IOS Software output text on the console.
10. C

- 11. A. unicast
- B. broadcast
- C. multicast

A frame is sent from one address to a single address.
A frame is sent from one address to all other addresses.
A frame is sent from one address to multiple addresses.

12. C

13. D

14. C

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate:
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Establishing Internet Connectivity

When you fully understand how a small network is built, you can more easily understand how a router connects your network to the Internet. Connectivity with the outside world is the primary function of networks. Internet access is usually provided by ISPs using various technologies, from DSL and cable to various wireless technologies such as IEEE 802.11 and 3G or 4G.

When you connect to the Internet, it is important to understand how to use ACLs for filtering and classification of traffic. IP uses packets to carry information through the network. The transport layer is responsible for the overall end-to-end transfer of application data. Networks are usually divided by administrators into subnets to provide network scalability.

NAT and PAT translate IP addresses and eliminate the need for host renumbering. This module describes their configuration.

Objectives

Upon completing this module, you will be able to meet these objectives:

- Describe IPv4 and its addressing scheme
- Describe subnets, subnetting, and the role of subnet masks
- Describe the TCP/IP transport layer
- Describe the functions of routing in the network model
- Implement basic configuration on a Cisco router
- Understand host-to-host communications across switches and routers
- Describe the operation, benefits, and limitations of static routing
- Describe the operation of ACLs and their applications in the network
- Configure Internet access using DHCP clients, NAT, and PAT on Cisco routers

Do Not Duplicate.
Post beta, not for release.

Understanding the TCP/IP Internet Layer

Overview

There are various aspects to IP addressing, including calculations for constructing an IP address, classes of IP addresses designated for specific routing purposes, and public versus private IP addresses. There are also two types of IP addresses: IPv4 and IPv6. This lesson introduces the concepts behind IPv4 addresses.

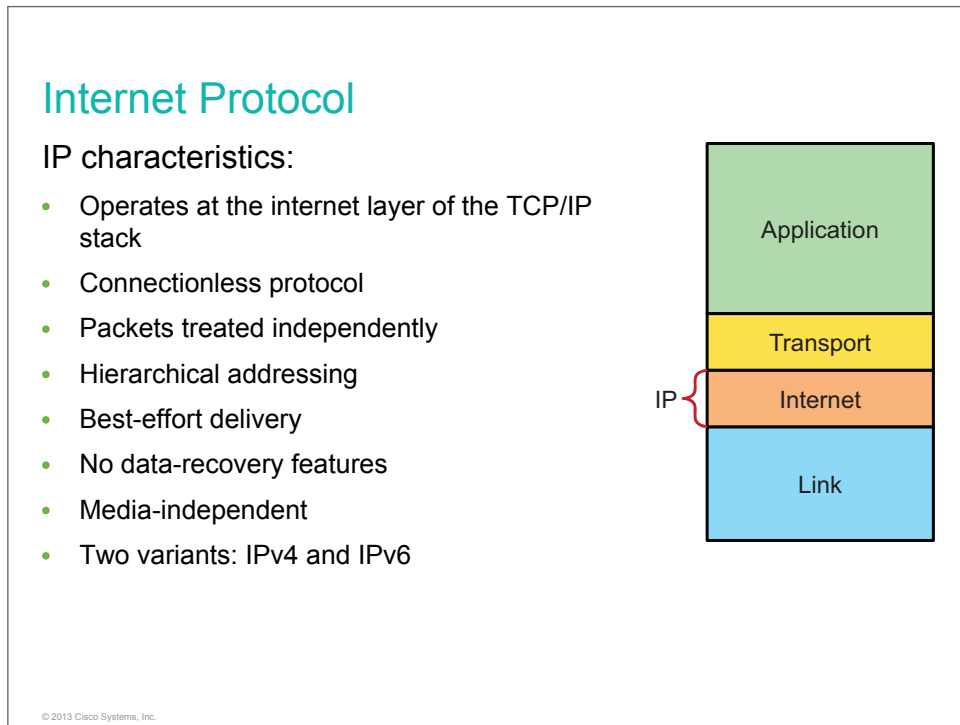
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- List the characteristics of IP
- Describe the components of an IPv4 address
- Identify the source and the destination fields within the IPv4 header
- Describe the decimal and binary number systems
- Convert a decimal number to a binary number
- List the classes of IPv4 addresses
- Describe reserved IPv4 addresses
- Define the function of DNS
- Verify the IPv4 address of a host

Internet Protocol

The IP component of TCP/IP determines where packets of data are routed, based on their destination addresses. IP has certain characteristics that are related to how it manages this function. This topic describes some of the key functions of IP.



IP uses packets to carry information through the network. A packet is a self-contained, independent entity that contains data and sufficient information to be routed from the source to the destination without reliance on earlier exchanges.

IP has these characteristics:

- IP operates at Layer 3 of the OSI model (network layer) and at the internet layer of the TCP/IP stack.
- IP is a connectionless protocol in which a one-way datagram is sent to the destination without advance notification to the destination device. The destination device receives the data and does not return any status information to the sending device.
- Each packet is treated independently, which means that each packet can travel a different way to the destination.
- IP uses hierarchical addressing, in which the network ID is the equivalent of a street and the host ID is the equivalent of a house or office building on that street.
- IP provides service on a best-effort basis and does not guarantee packet delivery. A packet can be misdirected, duplicated, or lost on the way to its destination.
- IP does not provide any special features that recover corrupted packets. These services are instead provided by the end systems of the network.
- IP operates independently of the medium that is carrying the data.
- There are two types of IP addresses: IPv4 and IPv6.

Example: Delivering a Letter Through a Postal Service

An analogy for IP services would be mail delivery by a postal service. For example, you live in San Francisco and your mother lives in New York. You write three letters to your mother. You seal each letter in a separate envelope, address each letter, and write your return address in the upper left-hand corner of each envelope.

You deposit the three letters in the outgoing mail slot at your local post office. The postal service makes its best attempt to deliver all three letters to your mother in New York. However, the postal service will not guarantee that the letters will arrive at their destination. It will not guarantee that all three letters will be processed by the same carrier or take the same route. And it will not guarantee that the letters will arrive in the order in which you mailed them.

Do Not Duplicate:
Post beta, not for release.

IPv4 Address Representation

This topic describes the components of an IPv4 address.

IPv4 Address Representation

- Every host (computer, networking device, peripheral) must have a unique address.
- An IP address consists of two parts:
 - Network ID:
 - Identifies the network of which the host is a part
 - Used by routers to maintain information about routes
 - Host ID:
 - Identifies the individual host
 - Assigned by organizations to individual devices

172.16.12.22

© 2013 Cisco Systems, Inc.

Physical street addresses are necessary to identify the locations of specific homes and businesses so that mail can reach them efficiently. In the same way, logical IP addresses are used to identify the location of specific devices on an IP network so that data can reach those network locations. Every host, computer, networking device, or peripheral device connected to the Internet has a unique 32-bit IP address that identifies it. Without a structure for allocating all of those IP addresses, it would be impossible to route packets efficiently. Learning how IP addresses are structured and how they function in the operation of a network provides an understanding of how IP packets are forwarded over networks using TCP/IP.

The IPv4 address is the most common type of address that is currently used on the Internet. IPv4 addresses are 32-bit numbers that describe the location of a network device.

An IP address is hierarchical and consists of two parts:

- The network address portion (network ID) describes the network of which this IP address is a part.
- The host address component (host ID) identifies a specific endpoint. These endpoints are the servers, computers, and other devices that are connected to the network. Host IDs are assigned to individual devices (end-user devices, printers, network devices, and so on).

IPv4 Header Address Fields

This topic identifies the source and destination address fields within the IPv4 header.

Ver.	IHL	Service Type	Total Length	
Identification			Flag	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

© 2013 Cisco Systems, Inc.

The IPv4 header has several fields. These are the two fields that are most important for you at this point:

- **Source Address:** Specifies the 32-bit binary value that represents the IP address of the sending endpoint
- **Destination Address:** Specifies the 32-bit binary value that represents the IP address of the receiving endpoint

Other fields in the header are the following:

- **Version:** Describes the version of Internet Protocol
- **IHL:** Internet Header Length, describes the length of the header
- **Service Type:** Provides information of desired quality of service
- **Total Length:** Describes the length of a packet, including header and data
- **Identification:** Used for unique fragment identification
- **Flag:** Sets various control flags regarding fragmentation
- **Fragment Offset:** Indicates where specific fragment belongs
- **Time to Live:** Limits lifetime of a packet
- **Protocol:** Indicates the protocol used in the data portion of a IP packet
- **Header Checksum:** Used for header error detection
- **Options:** Includes optional parameters
- **Padding:** Used to ensure that the header ends on a 32-bit boundary

If you would like to learn more about the IPv4 header fields, go to <http://tools.ietf.org/html/rfc791>.

Decimal and Binary Systems

The decimal (base 10) system is the numbering system that is used in everyday mathematics, and the binary (base 2) system is the foundation of computer operations. Network device addresses use the binary system to define their location on the network. The IP address is based upon a dotted-decimal notation of a binary number. Having a basic understanding of the mathematical properties of a binary system helps you to understand networking. This topic describes the decimal and binary systems.

Decimal and Binary Systems

- Decimal numbers are represented by the numbers 0 through 9.
- Binary numbers are represented by a series of 1s and 0s.

Decimal	Binary
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Decimal	Binary
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011

© 2013 Cisco Systems, Inc.

In the decimal system, the digits are 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. When quantities higher than 9 are required, the decimal system begins with 10 and continues all the way to 99. Then the decimal system begins again with 100, and so on, with each column to the left raising the exponent by 1.

The binary system uses only the digits 0 and 1. Therefore, the first digit is 0, followed by 1. If a quantity higher than 1 is required, the binary system goes to 10, followed by 11. The binary system continues with 100, 101, 110, 111, then 1000, and so on. This figure shows the binary equivalent of the decimal numbers 0 through 19.

Decimal-to-Binary Conversion

Decimal numbers can be converted to binary numbers through a specific process. This topic describes how to convert decimal numbers to binary numbers.

Base ^{Exponent}	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
Place Value	128	64	32	16	8	4	2	1
Example: Convert decimal 35 to binary	0	0	1	0	0	0	1	1
35 =	(2 ⁷ *0)+	(2 ⁶ *0)+	(2 ⁵ *1)+	(2 ⁴ *0)+	(2 ³ *0)+	(2 ² *0)+	(2 ¹ *1)+	(2 ⁰ *1)
35 =			(32*1)		+		(2*1) + (1*1)	
35 =	0 + 0 + 1 + 0 + 0 + 0 + 1 + 1							
35 = <u>0010011</u>								

© 2013 Cisco Systems, Inc.

This figure shows a simple binary conversion of the decimal number 35. The base exponent line shows base-2 numbers and their exponents ($2 * 2 = 4 * 2 = 8$ and so on). The decimal value of the base exponent number is listed in the second row, and the binary number is displayed in the third row. The table describes the steps to determine the binary number. Note that the first 2 bits of the binary number are 0s. These 0s are known as leading 0s. In reality, the decimal number 35 would only be a 6-bit binary number. Because IP addresses are laid out as four sets of octets, the binary number is made into an octet by placing 0s to the left of the 6-bit number.

The table shows the steps for converting the number 35 to a binary number.

Procedure for Converting a Decimal Number to a Binary Number

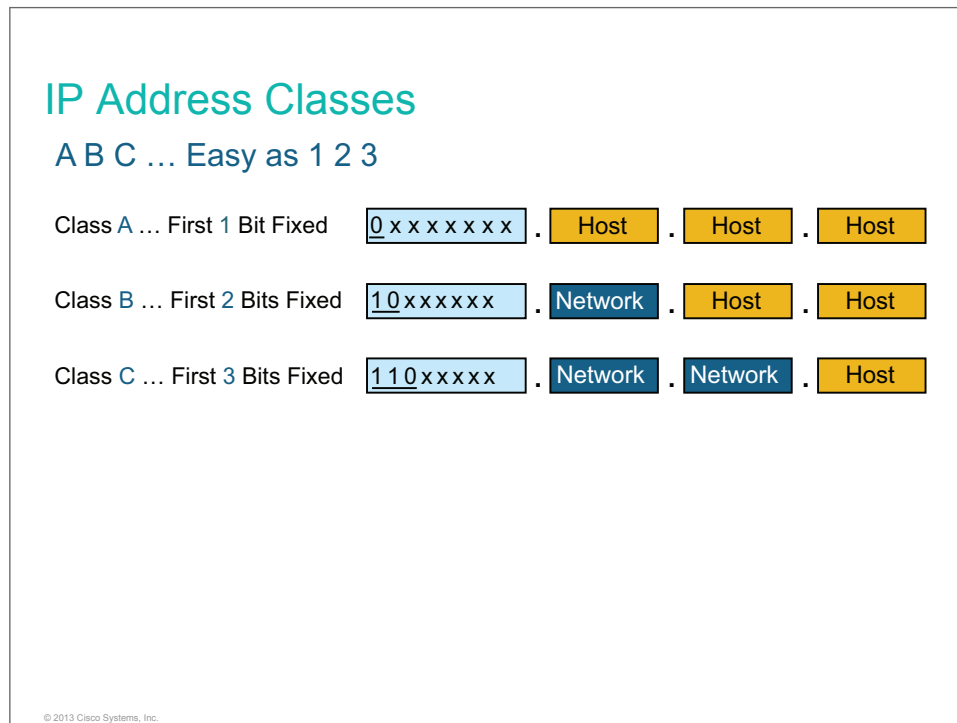
Step	Action
1.	Looking at the figure, what is the greatest power of 2 that is less than or equal to 35? 128 does not go into 35, so place a 0 in that column.
2.	64 does not go into 35, so place a 0 in that column.
3.	2 ⁵ (32) is smaller than 35. 32 goes into 35 one time. Place a 1 in that column.
4.	Calculate how much is left over by subtracting 32 from 35. The result is 3.
5.	Check to see if 16 (the next lower power of 2) fits into 3. Because it does not, a 0 is placed in that column.
6.	The value of the next number is 8, which is larger than 3, so a 0 is placed in that column also.
7.	The next value is 4, which is still larger than 3, so it, too, receives a 0.
8.	The next value is 2, which is smaller than 3. Because 2 fits into 3 one time, place a 1 in that column.

Step	Action
9.	Subtract 2 from 3, and the result is 1.
10.	The decimal value of the last bit is 1, which fits into the remaining number. Therefore, place a 1 in the last column. The binary equivalent of the decimal number 35 is 00100011.

Do Not Duplicate.
Post beta, not for release.

IP Address Classes

To accommodate networks of various sizes and to aid in classifying them, IP addresses are divided into categories that are called *classes*. This topic describes the IP address classes and the structure of the IP addresses within them.



Assigning IP addresses to classes is known as *classful addressing*. The classes were determined during the early days of the Internet by the IANA.

Each IP address is broken down into a network ID and a host ID. In addition, a bit or bit sequence at the start of each address determines the class of the address. The figure shows three of the five IP classes.

Class A

A Class A address block is designed to support extremely large networks with more than 16 million host addresses. The Class A address uses only the first octet (8 bits) of the 32-bit number to indicate the network address. The remaining three octets of the 32-bit number are used for host addresses. The first bit of a Class A address is always a 0. Because the first bit is a 0, the lowest number that can be represented is 00000000 (decimal 0), and the highest number that can be represented is 01111111 (decimal 127). However, these two network numbers, 0 and 127, are reserved and cannot be used as network addresses. Any address that starts with a value between 1 and 126 in the first octet of the 32-bit number is a Class A address.

Class B

The Class B address space is designed to support the needs of moderate to large networks with more than 65,000 hosts. The Class B address uses two of the four octets (16 bits) to indicate the network address. The remaining two octets specify host addresses. The first two bits of the first octet of a Class B address are always binary 10. Starting the first octet with binary 10 ensures that the Class B space is separated from the upper levels of the Class A space. The remaining six bits in the first octet may be populated with either 1s or 0s. Therefore, the lowest number that can be represented with a Class B address is 10000000 (decimal 128), and the highest number that can be represented is 10111111 (decimal 191). Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.

Class C

The Class C address space is the most commonly available address class. This address space is intended to provide addresses for small networks with a maximum of 254 hosts. In a Class C address, the first three octets (24 bits) of the IP address identify the network portion, with the remaining octet reserved for the host portion. A Class C address begins with binary 110. Therefore, the lowest number that can be represented is 11000000 (decimal 192), and the highest number that can be represented is 11011111 (decimal 223). If an address contains a number in the range of 192 to 223 in the first octet, it is a Class C address.

Note Additionally, there is also Class D address space, dedicated for multicast addressing and Class E address space, which is reserved for experimental use and research. The Class D address space range goes from 224.0.0.0 to 239.0.0.0, while the Class E range uses IPs from 240.0.0.0 to 254.0.0.0.

IP Address Classes (Cont.)

IP Address Ranges

IP Address Class	First Octet Decimal Value	First Octet Binary Value	Possible Number of Hosts
Class A	1–126	00000001 to 01111110*	16,777,214
Class B	128–191	10000000 to 10111111	65,534
Class C	192–223	11000000 to 11011111	254

*127 (01111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.

© 2013 Cisco Systems, Inc.

The table shows the IP address range of the first octet (in decimal and binary) for Class A, B, and C IP addresses, as well as the number of host addresses available for each class of addresses.

Each class of network allows a fixed number of hosts. In a Class A network, the first octet is assigned to the network, leaving the last three octets to be assigned to hosts. The first host address in each network (all 0s) is reserved for the actual network address, and the final host address in each network (all 1s) is reserved for broadcasts. The maximum number of hosts in a Class A network is $2^{24} - 2$ (subtracting the network and broadcast reserved addresses), or 16,777,214.

In a Class B network, the first two octets are assigned to the network. The final two octets are assigned to hosts. The maximum number of hosts in a Class B network is $2^{16} - 2$, or 65,534.

In a Class C network, the first three octets are assigned to the network. The final octet can be assigned to hosts, so the maximum number of hosts is $2^8 - 2$, or 254.

Note RFC 1700 grouped the unicast ranges into specific sizes that are called Class A, Class B, and Class C addresses, as presented in this topic. It also defined Class D (multicast) and Class E (experimental) addresses.

Reserved IPv4 Addresses

Certain IP addresses are reserved and cannot be assigned to individual devices on a network. These reserved addresses include a network address, which is used to identify the network itself, and a broadcast address, which is used for broadcasting packets to all of the devices on a network. This topic describes the types of reserved IP addresses and provides examples of each.

Reserved IPv4 Address

These are reserved IPv4 addresses:

- Network address
- Directed broadcast address
- Local broadcast address
- Local loopback address
- All zeros address

© 2013 Cisco Systems, Inc.

Network Address

The network address is a standard way to refer to a network. An IP address that has binary 0s in all of the host bit positions is reserved for the network address. For example, in a Class A network, 10.0.0.0 is the IP address of the network containing the host 10.1.2.3. All hosts in 10.0.0.0 will have the same network bits. The IP address 172.16.0.0 is a Class B network address, and 192.16.1.0 is a Class C network address. A router uses the network IP address when it searches its IP routing table for the destination network location.

The decimal numbers that constitute the first two octets in a Class B network address are assigned. The last two octets contain 0s because those 16 bits are for host numbers and are used for devices that are attached to the network. In the IP address 172.16.0.0, the first two octets are reserved for the network address and are never used as an address for any device that is attached to it. An example of an IP address for a device on the 172.16.0.0 network is 172.16.16.1. In this example, 172.16 is the network address portion and 16.1 is the host address portion.

Directed Broadcast Address

The broadcast IP address of a network is a special address for each network that allows communication to all of the hosts in that network. To send data to all of the hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network. The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portion are all 1s. For network 10.0.0.0, with 8 network bits, the broadcast address would be 10.255.255.255. This address is also referred to as the *directed broadcast*.

For the network address 172.16.0.0, the last 16 bits make up the host field (or host part of the address). The broadcast that would be sent out to all of the devices on that network would include a destination address of 172.16.255.255.

The directed broadcast address can be routed. However, for some versions of the Cisco IOS operating system, routing directed broadcasts is not the default behavior.

Local Broadcast Address

If an IP device wants to communicate with all of the devices on the local network, it sets the destination address to all 1s (255.255.255.255) and transmits the packet. For example, hosts that do not know their network number and are asking a server for it may use this address. The local broadcast is never routed.

Local Loopback Address

A local loopback address is used to let the system send a message to itself for testing. The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate with each other. A typical local loopback IP address is 127.0.0.1.

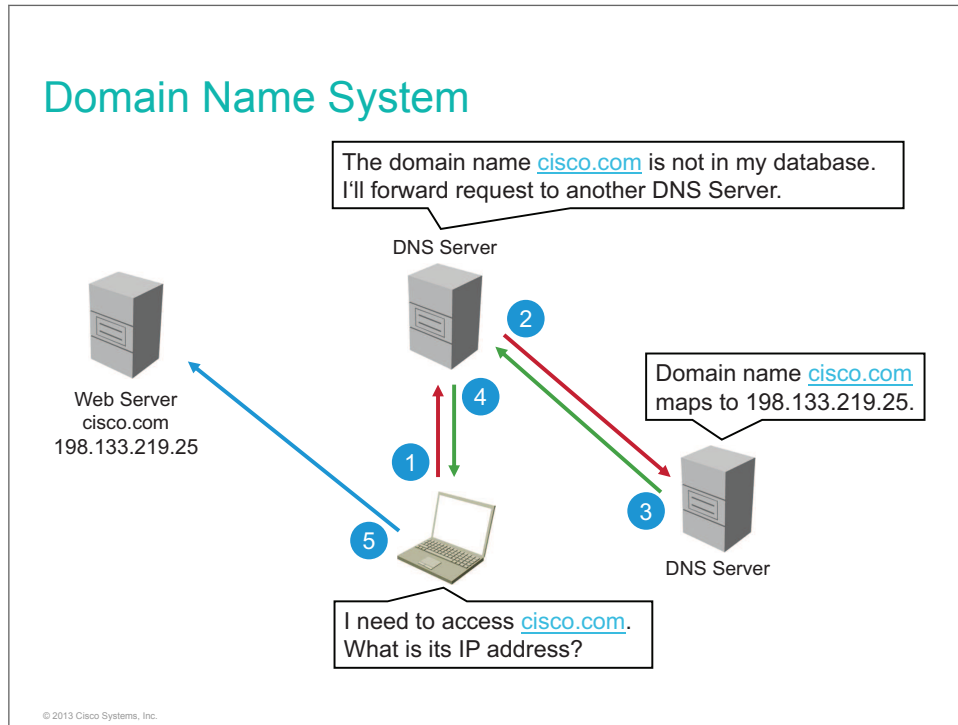
All zeros address

Address 0.0.0.0 indicates the host in "this" network and is used only as a source address. An example use case is the DHCP assignment process before the host has a valid IP address.

For more information about reserved IPv4 addresses, refer to RFC 5735, at <http://tools.ietf.org/html/rfc5735>.

Domain Name System

DNS provides an efficient way to convert human-readable names of IP end systems into machine-readable IP addresses that are necessary for routing. This topic describes the function of DNS.

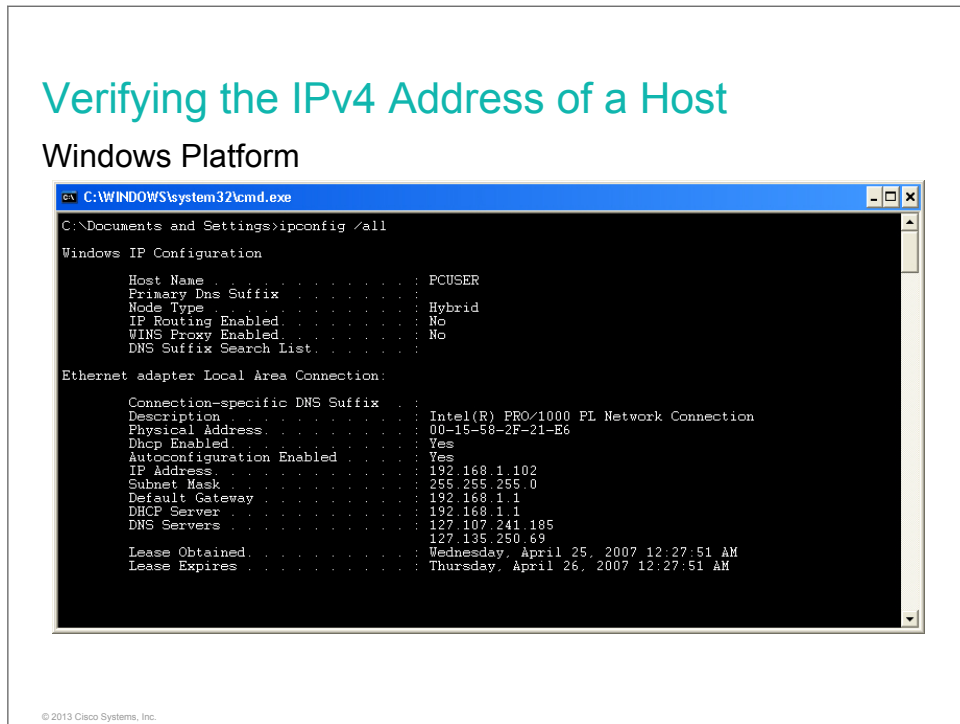


In data networks, devices are labeled with numeric IP addresses so that they can send and receive messages over the network. However, most people find it difficult to remember this numeric address. Therefore, domain names were created to convert the numeric address into a simple, recognizable name.

DNS was created for domain name-to-address resolution for networks. DNS uses a set of servers to resolve the names that are associated with numbered addresses. The DNS protocol defines an automated service that matches resource names with the required numeric network address.

Verifying the IPv4 Address of a Host

Most operating systems and devices connected to a network provide a set of tools that can be used to verify host addressing. This topic focuses on the tools available on the Microsoft Windows platform. Additionally, it also describes how to verify the IP address of a switch acting as a host.



The following describes the syntax for the **ipconfig** command:

On a PC with the Microsoft Windows operating system, the **ipconfig** command can be used to display all current TCP/IP network configuration values at the command line. Using various parameters, the command can also be used to refresh DHCP and DNS settings. Used without parameters, the **ipconfig** command displays the IP address, subnet mask, and default gateway for all adapters.

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns]
```

These parameters are commonly used:

- **/all**: Displays the complete TCP/IP configuration for all adapters. Without this parameter, the **ipconfig** command displays only the IP address, subnet mask, and default gateway values for each adapter. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.
- **/renew [*Adapter*]**: Renews the DHCP configuration for all of the adapters (if an adapter is not specified) or for a specific adapter if the *Adapter* parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use the **ipconfig** command without parameters.
- **/release [*Adapter*]**: Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all of the adapters (if an adapter is not specified) or for a specific adapter if the *Adapter* parameter is included. This parameter disables TCP/IP for adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use the **ipconfig** command without parameters.

- `/?`: Displays help at the command prompt.

Additional information and the command syntax can be found at <http://technet.microsoft.com/en-us/library/dd197434>.

Verifying the IPv4 Address of a Host (Cont.)

Verifying IP address of a switch

```
Switch#show ip interface brief
Interface      IP-Address      OK?  Method  Status  Protocol
Vlan1          10.1.1.11       YES  manual  up       up
FastEthernet0/1 unassigned      YES  unset   up       up
FastEthernet0/2 unassigned      YES  unset   down     down
FastEthernet0/3 unassigned      YES  unset   up       up
FastEthernet0/4 unassigned      YES  unset   up       up
FastEthernet0/5 unassigned      YES  unset   down     down
<output omitted>
```

© 2013 Cisco Systems, Inc.

Although a switch does not need an IP address for its operation of forwarding frames, it uses one for management purposes. You can verify the IP address settings with the **show ip interface brief** command.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- IP is a Layer 3 media-independent connectionless protocol that uses hierarchical logical addressing and provides service in a best-effort manner.
- Every node that is connected to the Internet has a unique IP address that identifies it. An IP address consists of two parts: the network ID and the host ID.
- Every packet that travels through the network contains a source address and a destination address.
- Certain IP addresses (for example, network and broadcast addresses) are reserved and cannot be assigned to individual network devices.
- DNS is an application that is specified in the TCP/IP suite. It provides a means to translate human-readable names into IP addresses.

© 2013 Cisco Systems, Inc.

Understanding IP Addressing and Subnets

Overview

Subnetworks, or subnets, are common in all but the smallest network environments, segmenting networks into smaller divisions that have their own addresses. To create subnet addresses, some of the bits that are used for the host portion of an IP address are "borrowed" to create the subnet address. This lesson describes how subnets function and how they are computed.

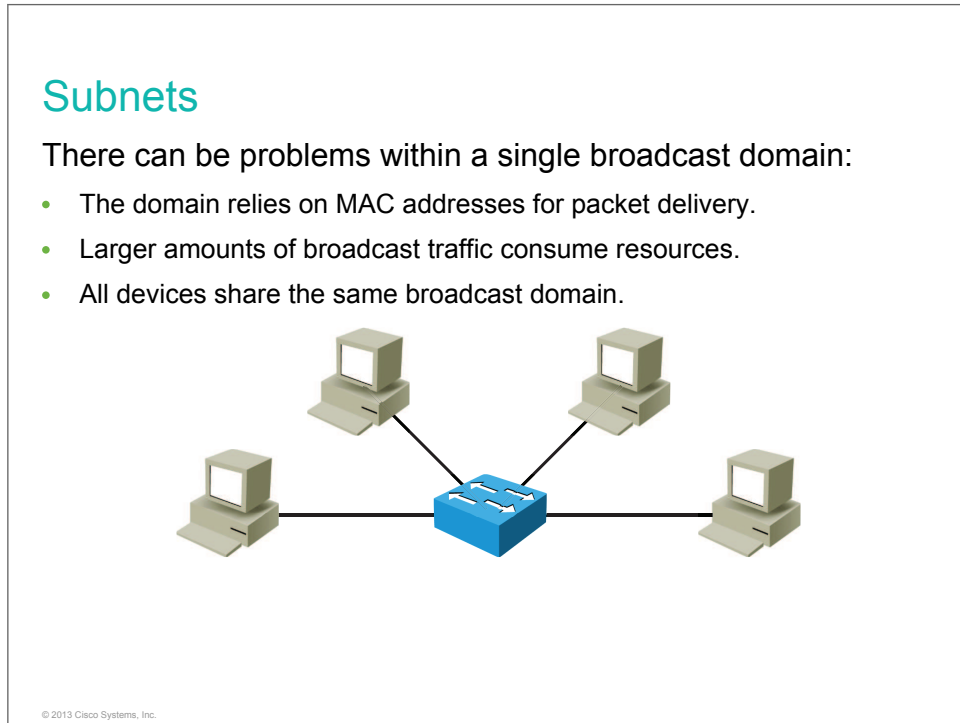
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the purposes and functions of subnets and their addressing schemes
- Explain the role of a subnet mask
- Describe the octet values of a subnet mask
- Describe how end systems use subnet masks and default gateways
- Determine the number of subnets and hosts
- Identify a procedure to determine subnet addresses
- Show how to determine a subnet address
- Determine an addressing scheme
- Describe the role of VLSM
- Use VLSM to subnet a network

Subnets

Network administrators often need to divide networks, especially large networks, into subnetworks, or subnets, to provide scalability. This topic describes the purposes and functions of subnets and their addressing schemes.



A company that occupies a three-story building might have a network that is divided by floors, with each floor divided into offices. Think of the building as the network, the floors as the three subnets, and the offices as the individual host addresses.

A subnet segments the hosts within the network. Without subnets, the network has a flat topology. A flat topology has a short routing table and relies on MAC addresses to deliver packets. MAC addresses have no hierarchical structure. As the network grows, the use of the network bandwidth becomes less efficient.

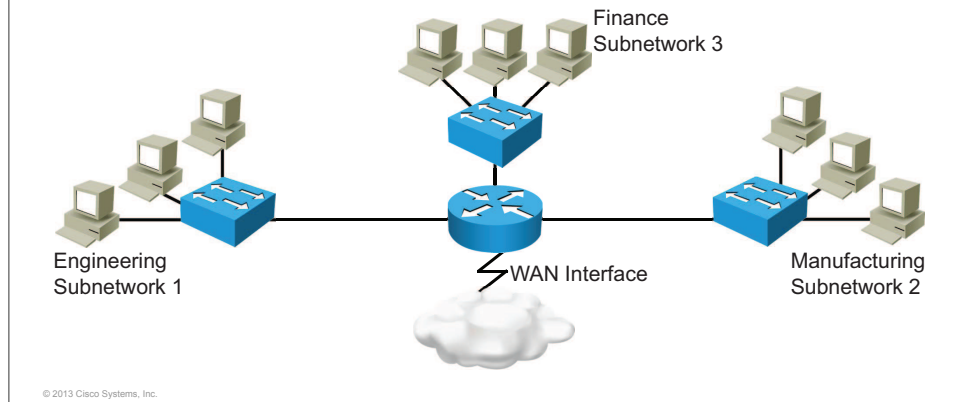
There are other disadvantages to a flat network. All devices share the same bandwidth and broadcast domain, and it is difficult to apply security policies because there are no boundaries between devices.

On a switch-connected network, the host sees all of the broadcasts in the broadcast domain. When traffic is heavy, collisions caused by two or more devices that are transmitting simultaneously may be frequent. The devices detect the collisions, stop transmitting, and then begin transmitting later, at random intervals. To users, this process is perceived as the network slowing down. The switches are improving network performance, but routers are a better choice in these situations. Routers can be used to separate networks by breaking the network into multiple subnets.

Subnets (Cont.)

Solution: Subnetworks

- Smaller networks are easier to manage.
- Overall traffic is reduced.
- You can apply network security policies more easily.



The advantages of subnetting a network are as follows:

- Smaller networks are easier to manage and map to geographical or functional requirements.
- Overall network traffic is reduced, which can improve performance.
- You can more easily apply network security measures at the interconnections between subnets than within a large single network.

In multiple-network environments, each subnetwork may be connected to the Internet by a single router. This figure shows one router connecting multiple subnetworks to the Internet. The details of the internal network environment and how the network is divided into multiple subnetworks are inconsequential to other IP networks.

The IP addressing that is used in the flat network must be modified to accommodate the required segmentation. A subnet mask identifies the network-significant portion of an IP address. The network-significant portion of an IP address is simply the part that identifies the network that the host device is on. This part is called the *network address* and defines every subnetwork. The use of segmentation is important for the routing operation to be efficient.

Subnet Masks

This topic describes the role of the subnet mask within the network.

Subnet Masks

A subnet mask:

- Defines the number of bits that represent the network and subnet part of the address
- Used by end systems to identify the destination IP address as either local or remote
- Used by Layer 3 devices to determine network path

Subnet mask: 255.255.0.0 or /16
IP Address: 172.16.55.87

© 2013 Cisco Systems, Inc.

How do you know how many bits represent the network portion of the address and how many bits represent the host portion? When you express an IPv4 network address, you add a prefix length to the network address. The prefix length is the number of bits in the address that give the network portion. For example, in 172.16.55.87 /16, /16 is the prefix length. It tells you that the first 16 bits are the network address. This leaves the remaining 16 bits, the last octet, as the host portion. The entity that is used to specify the network portion of an IPv4 address to the network devices is called the *subnet mask*. The subnet mask consists of 32 bits, just as the address does, and uses 1s and 0s to indicate which bits of the address are network bits and which bits are host bits. You express the subnet mask in the same dotted decimal format as the IPv4 address. The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion. A /16 prefix is expressed as a subnet mask of 255.255.0.0 (11111111.11111111.00000000.00000000). The remaining bits (low order) of the subnet mask are zeroes, indicating the host address within the network.

The subnet mask is configured on a host with the IPv4 address to define the network portion of that address.

Networks are not always assigned the same prefix. Depending on the number of hosts on the network, the prefix that is assigned may be different. Having a different prefix number changes the host range and broadcast address for each network.

For example, look at the host 10.1.20.70/26:

- Address:
 - 10.1.20.70
 - 00001010.00000001.00010100.01000100
- Subnet mask:
 - 255.255.255.196
 - 11111111.11111111.11111111.11000000

- Network address:
 - 10.1.20.64
 - 00001010.00000001.00010100.01000000

Do Not Duplicate.
Post beta, not for release.

Octet Values of a Subnet Mask

This topic describes the octet values of a subnet mask.

Octet Values of a Subnet Mask

- Subnet masks, like IP addresses, are represented in the dotted decimal format, such as 255.255.255.0.
- The binary 1 reflects the network and subnetwork part of the IP address.

© 2013 Cisco Systems, Inc.

Octet Values of a Subnet Mask (Cont.)

128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	=	0
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

© 2013 Cisco Systems, Inc.

Although subnet masks use the same format as IP addresses, they are not IP addresses themselves. Each subnet mask is 32 bits long, divided into four octets, and is usually represented in dotted decimal notation like IP addresses. In their binary representation, subnet masks have all 1s in the network and subnetwork portions, and have all 0s in the host portion.

Because the high-order bits of the subnet masks are contiguous 1s, there is only a limited number of subnet values within an octet. Recall that you only need to expand an octet if the network and host division falls within that octet. Therefore, the number of 8-bit patterns that are used in address masks is limited.

The subnet field always immediately follows the network number. The bits that are borrowed to create a subnet mask must be the first n bits in that octet. The borrowed bits must start with the **MSB** of the default host field. This figure shows the borrowed n bits, where value n is from 1 to 8. The subnet mask is the tool that is used by the router to determine which bits are routing (network and subnet) bits and which bits are host bits.

The last column in the figure shows the decimal representation of the subnet mask for each combination of borrowed bits. If the subnet mask for an octet is represented by 255, then all the equivalent bits in that octet of the address are network bits. Similarly, if the subnet mask for an octet is represented by 0, then all the equivalent bits in that octet of the address are host bits. In each of these cases, it is not necessary to expand this octet to binary to determine the network and host portions.

The figure shows only one octet because the decimal representation of each octet is the same. In Class A, the default subnet address is 255.0.0.0 or 11111111.00000000.00000000.00000000. If the three highest-order bits from the next highest-order host octet are borrowed, they add up to 224. This value translates to 255.224.0.0 or 11111111.11100000.00000000.00000000. The same approach applies to the other classes. The only difference is in the default subnet mask that is used for the various classes. In Class B, the default subnet address is 255.255.0.0 or 11111111.11111111.00000000.00000000. In Class C, the default subnet address is 255.255.255.0 or 11111111.11111111.11111111.00000000.

Octet Values of a Subnet Mask (Cont.)

Default Subnet Masks, Class A

Example Class A address (decimal):	10.0.0.0
Example Class A address (binary):	00001010 .00000000.00000000.00000000
Default Class A mask (binary):	11111111 .00000000.00000000.00000000
Default Class A mask (decimal):	255.0.0.0
Default classful prefix length:	/8

© 2013 Cisco Systems, Inc.

Octet Values of a Subnet Mask (Cont.)

Default Subnet Masks, Class B

Example Class B address (decimal):	172.16.0.0
Example Class B address (binary):	10101100 .00010000.00000000.00000000
Default Class B mask (binary):	11111111 .11111111.00000000.00000000
Default Class B mask (decimal):	255.255.0.0
Default classful prefix length:	/16

© 2013 Cisco Systems, Inc.

Octet Values of a Subnet Mask (Cont.)

Default Subnet Masks, Class C

Example Class C address (decimal):	192.168.42.0
Example Class C address (binary):	11000000 .10101000.00101010.00000000
Default Class C mask (binary):	11111111 .11111111.11111111.00000000
Default Class C mask (decimal):	255.255.255.0
Default classful prefix length:	/24

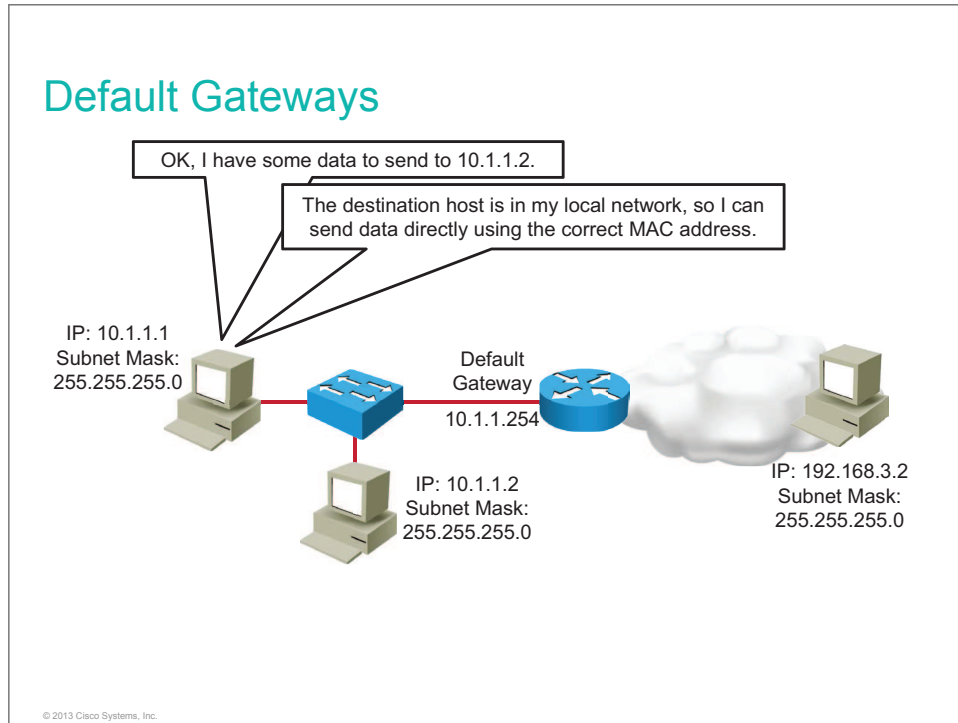
© 2013 Cisco Systems, Inc.

In IP addressing, the subnet mask identifies the addressing information that is necessary in order to send packets toward their final destinations. The subnet mask identifies which bits within the IP address are the network and subnet bits.

The figure shows the default subnet masks and the default classful prefix length for Class A, Class B, and Class C addresses. The subnet mask itself is indicated with 1s in the binary notation for the mask. All other bits are indicated as 0s.

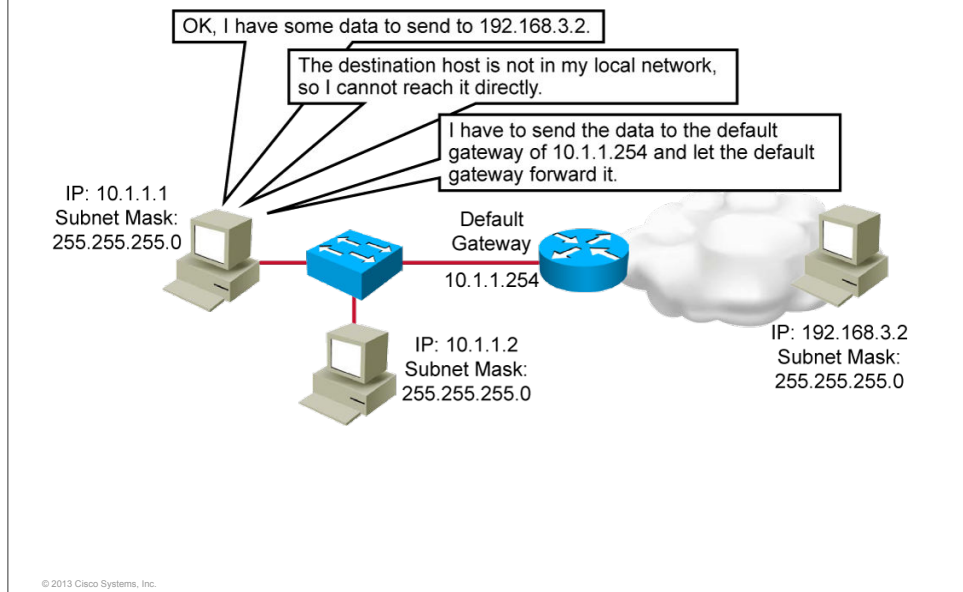
Default Gateways

The source host is able to communicate directly with the destination host only if the two hosts are on the same network. If the two hosts are on different networks, the sending host must send the data to the default gateway, which will forward the data to the destination. This topic describes the function of a default gateway.



Before an end system can send a packet to its destination, it must first determine if the destination address is in the local network. The subnet mask defines the network part of the IP address. The end system compares the network portion of the local network address with the destination network address of the packet to be sent. If the network portion of the local network address is the same as the destination network address, then the end system can deliver packets directly. If the network portion of the local network address is not the same as the destination network address, then the packets must be forwarded to some other network.

Default Gateways (Cont.)

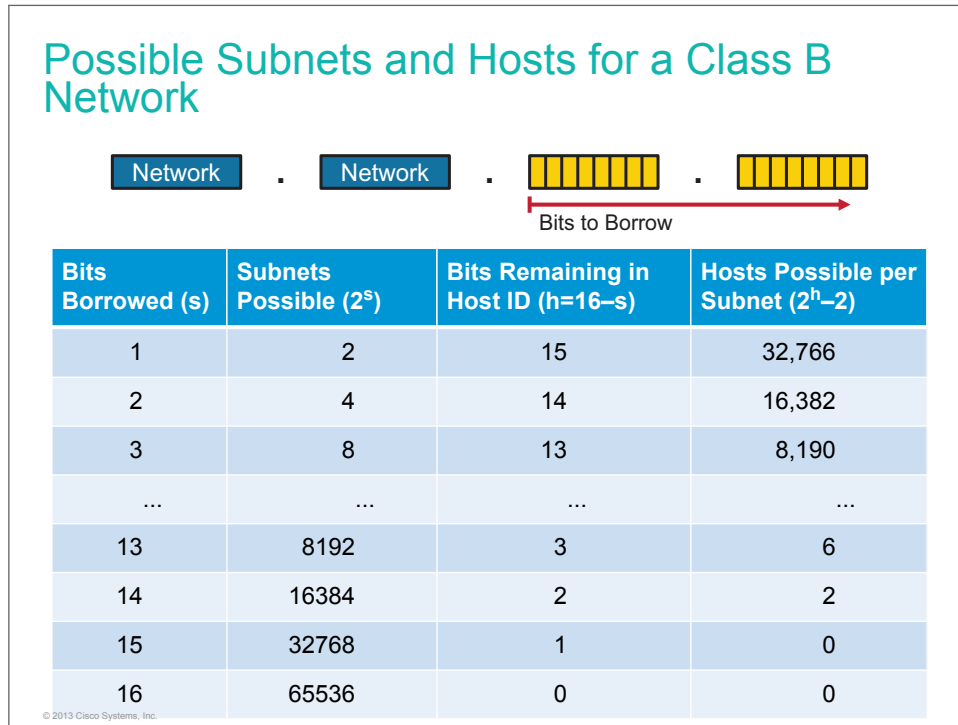


The default gateway is needed to send a packet out of the local network. If the network portion of the destination address of the packet is different from the network of the originating host, the packet has to be routed outside of the original network. To do this, the packet is sent to the default gateway. This default gateway is a router interface that is connected to the local network. The default gateway interface has a network layer address that matches the network address of the hosts. The hosts are configured to recognize that address as the default gateway.

On a Windows computer, the Internet Protocol (TCP/IP) Properties tools are used to enter the default gateway IP address. The host IP address as well as the default gateway address must have the same network portion of their respective addresses.

Computing Usable Subnetworks and Hosts

One of the decisions you must make when creating subnets is to determine the optimal number of subnets and hosts. This topic describes a process for planning subnets.



Consider a Class B network address in which 16 bits are used for the network ID and 16 bits are used for the host ID. Therefore, there are 65,536 (2^{16}) possible addresses that are available to assign to hosts. Of these, 65,534 are usable addresses after subtracting the two addresses that cannot be used—the broadcast and subnet addresses.

Now, imagine that this Class B network is divided into subnets. If 2 bits are borrowed from the default 16-bit host field, the size of the host field decreases to 14 bits. All possible combinations of 0s and 1s that could occur in the remaining 14 bits produce a total number of possible hosts that could be assigned in each subnet. Thus, the number of hosts that are assigned to each subnet is now 16,382.

In the same Class B network, if 3 bits are borrowed, the size of the host field decreases to 13 bits, and the total number of assignable hosts for each subnet decreases to 8192 (2^{13}). The number of usable host numbers decreases to 8190 ($8192 - 2$). This last example shows six ($8 - 2$) usable subnets in a Class B network. Each of these six subnets can have 8190 ($8192 - 2$) usable host addresses.

The table shows all possible subnets and hosts for a Class B network.

Subnetting a Class B Network

Number of Bits Borrowed (s)	Number of Possible Subnets 2^s	Number of Bits Remaining in Host ID ($24 - s = h$)	Number of Hosts Possible per Subnet ($2^h - 2$)
1	2	15	32766
2	4	14	16382
3	8	13	8190

Number of Bits Borrowed (s)	Number of Possible Subnets 2^s	Number of Bits Remaining in Host ID ($24 - s = h$)	Number of Hosts Possible per Subnet ($2^h - 2$)
4	16	12	4094
5	32	11	2046
6	64	10	1022
7	128	9	510
8	256	8	254
9	512	7	126
10	1024	6	62
11	2048	5	30
12	4096	4	14
13	8192	3	6
14	16384	2	2
15	32768	1	0
16	65536	0	0

Do Not Duplicate. Post beta, not for release.

Applying Subnet Masks

Most network administrators work with existing networks, complete with subnets and subnet masks in place. Network administrators need to be able to determine which part of an existing IP address is the network and which part of the address is the subnet. Subnet masks provide this information. This topic describes how to apply subnet masks.

Applying Subnet Masks

Procedure for implementing subnets:

1. Determine the IP address space.
2. Based on the organizational and administrative structure, determine the number of subnets that are required.
3. Based on the address class and required number of subnets, determine the number of bits that you need to borrow from the host ID.
4. Determine the binary and decimal value of the subnet mask.
5. Apply the subnet mask to the network IP address to determine the subnet and host addresses.
6. Assign subnet addresses to specific interfaces for all devices that are connected to the network.

© 2013 Cisco Systems, Inc.

The procedure that is described in the table explains how to select the number of subnets that you need for a particular network and then apply a mask to implement subnets.

Procedure for Implementing Subnets

Step	Action	Example
1	Determine the IP address to be used for your network.	Assume that you are assigned an address of 172.16.0.0 with a subnet mask of 255.255.0.0.
2	Based on your organizational and administrative structure, determine the number of subnets that are required for the network. Be sure to plan for growth.	Assume that you are managing a worldwide network in 25 countries. Each country has an average of eight locations. Therefore, you will need 200 subnets.
3	Based on the address class and the number of subnets that you selected, determine the number of bits that you need to borrow from the host ID.	To create 200 subnets, you need to borrow 8 bits ($2^8 = 256$).
4	Determine the binary and decimal values of the subnet mask that you select.	For an address with 16 bits in the network ID, from which you borrow 8 bits, the mask is /24. The binary value of the mask is 11111111.11111111.11111111.00000000. The decimal value of the mask is 255.255.255.0.

Step	Action	Example
5	Apply the subnet mask for the network IP address to determine the subnet and host addresses. You will also determine the network and broadcast addresses for each subnet.	The first subnet is 172.16.0.0 with a subnet mask 255.255.255.0. The network address is the first one in the subnet, the broadcast address is the last one. The network address is 172.16.0.0 while the broadcast address is 172.16.0.255. The next available subnet is 172.16.1.0 /24.
6	Assign subnet addresses to specific interfaces on all of the devices that are connected to the network.	Apply the first host address within the subnet to the selected host or interface. The first available host address within the first subnet is 172.16.0.1.

Do Not Duplicate.
Post beta, not for release.

Determining the Network Addressing Scheme

This topic describes how to determine the network addressing scheme.

Determining the Network Addressing Scheme

Example 1: The IP address with subnet mask is 172.16.36.42/24.

The following tables show the eight steps that are used to determine the subnet addresses of a given IP address. In this example, the IP address and subnet mask are as follows:

- **IP address:** 172.16.36.42
- **Subnet mask:** 255.255.255.0

© 2013 Cisco Systems, Inc.

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
1	Write down the octet that is being split and all remaining octets on the right in binary.	Third and fourth octet (36.42): 00100100.00101010
2	Write down the mask or classful prefix length in binary.	Assigned mask (/24): 11111111.11111111.11111111.00000000
3	Draw a line to delineate the subnet and host bits in the assigned IP address. Write the IP address and the mask on top of each other so that you are able to identify the significant bits in the IP address.	Split octet (binary): 00100100 00101010 Split mask (binary): 11111111 00000000

© 2013 Cisco Systems, Inc.

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
4	Copy the subnet bits four times.	00100100.00000000 (subnet address)
5	In the first line, define the network address by placing all 0s in the host bits.	00100100.00000001 (first address in subnet) 00100100.11111110 (last address in subnet)
6	In the last line, define the broadcast address by placing all 1s in the host bits.	00100100.11111111 (broadcast address)
7	In the middle lines, define the first and last host number.	
8	Increment the subnet bits by 1 to determine the next subnet.	00100101.00000000

© 2013 Cisco Systems, Inc.

When subnet addresses are defined, the host part includes two addresses that cannot be used for any host. The first address consists of all 0s in the host part. All 0s define the subnet itself. The second address that cannot be used for host addressing is all 1s in the host part of the address. All 1s define the broadcast address on that subnet.

Determining the Network Addressing Scheme (Cont.)

After converting the addresses from binary to decimal, the addresses for the subnets are as follows:

- **Subnet address:** 172.16.36.0
- **First host address:** 172.16.36.1
- **Last host address:** 172.16.36.254
- **Broadcast address:** 172.16.36.255
- **Next subnet address:** 172.16.37.0

© 2013 Cisco Systems, Inc.

Determining the Network Addressing Scheme (Cont.)

Example 2: The IP address with subnet mask is 192.168.221.37/29.

The following tables show the eight steps that are used to determine the subnet addresses of a given IP address. In this example, the IP address and subnet mask are as follows:

- **IP address:** 192.168.221.37
- **Subnet mask:** 255.255.255.248

© 2013 Cisco Systems, Inc.

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
1	Write down the octet that is being split and all remaining octets on the right in binary.	Fourth octet (37): 00100101
2	Write down the mask or classful prefix length in binary.	Assigned mask (/29): 11111111.11111111.11111111.11111000
3	Draw a line to delineate the subnet and host bits in the assigned IP address. Write the IP address and the mask on top of each other so that you are able to identify the significant bits in the IP address.	Split octet (binary): 00100 101 Split mask (binary): 11111 000

© 2013 Cisco Systems, Inc.

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
4	Copy the subnet bits four times.	00100000 (network address)
5	In the first line, define the network address by placing all 0s in the host bits.	00100001 (first address in subnet) 00100110 (last address in subnet) 00100111 (broadcast address)
6	In the last line, define the broadcast address by placing all 1s in the host bits.	
7	In the middle lines, define the first and last host number.	
8	Increment the subnet bits by 1 to determine the next subnet.	00101000

© 2013 Cisco Systems, Inc.

Determining the Network Addressing Scheme (Cont.)

After converting the addresses from binary to decimal, the addresses for the subnets are as follows:

- **Subnet address:** 192.168.221.32
- **First host address:** 192.168.221.33
- **Last host address:** 192.168.221.38
- **Broadcast address:** 192.168.221.39
- **Next subnet address:** 192.168.221.40

© 2013 Cisco Systems, Inc.

Example: Addressing Scheme

This topic provides an example of determining a network addressing scheme.

Example: Addressing Scheme

The IP address with subnet mask is 192.168.5.139/27.

IP Address	192	168	5	139
IP Address	11000000	10101000	00000101	100 01011
Subnet Mask	11111111	11111111	11111111	111 00000
Network (2)	11000000	10101000	00000101	100 00000
Network (10)	192	168	5	128
First Host	192	168	5	100 00001 = 129
Last Host	192	168	5	100 11110 = 158
Directed Broadcast	192	168	5	100 11111 = 159
Next Network	192	168	5	101 00000 = 160

© 2013 Cisco Systems, Inc.

Steps to Determine Subnet Addresses

Step	Description	Example
1	Write down the octet that is being split in binary.	10001011
2	Write down the mask or classful prefix length in binary.	11100000
3	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	100 01011 111 00000
4	Copy the significant bits four times.	100 00000 (first subnet address)
5	In the first line, define the network address by placing 0s in the remaining host bits.	100 00001 (first host address) 100 11110 (last host address)
6	In the last line, define the directed broadcast address by placing 1s in the host bits.	100 11111 (broadcast address)
7	In the middle lines, define the first and last host ID for this subnet.	
8	Increment the subnet bits by 1 to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	101 00000 (next subnet address)

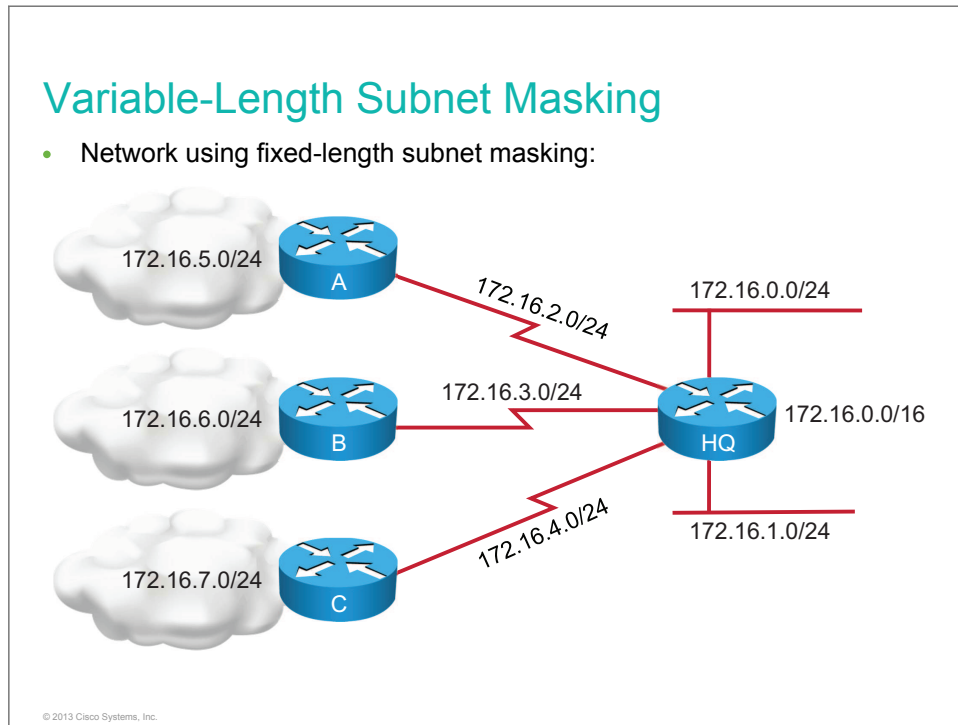
Subnet Addresses Table

Subnet Number	Subnet ID	Host Range	Broadcast Address
All 0s	192.168.5.0	192.168.5.1 to 192.168.5.30	192.168.5.31
1	192.168.5.32	192.168.5.33 to 192.168.5.62	192.168.5.63
2	192.168.5.64	192.168.5.65 to 192.168.5.94	192.168.5.95
3	192.168.5.96	192.168.5.97 to 192.168.5.126	192.168.5.127
4	192.168.5.128	192.168.5.129 to 192.168.5.158	192.168.5.159
5	192.168.5.160	192.168.5.161 to 192.168.5.190	192.168.5.191
6	192.168.5.192	192.168.5.193 to 192.168.5.222	192.168.5.223
All 1s	192.168.5.224	192.168.5.225 to 192.168.5.254	192.168.5.255

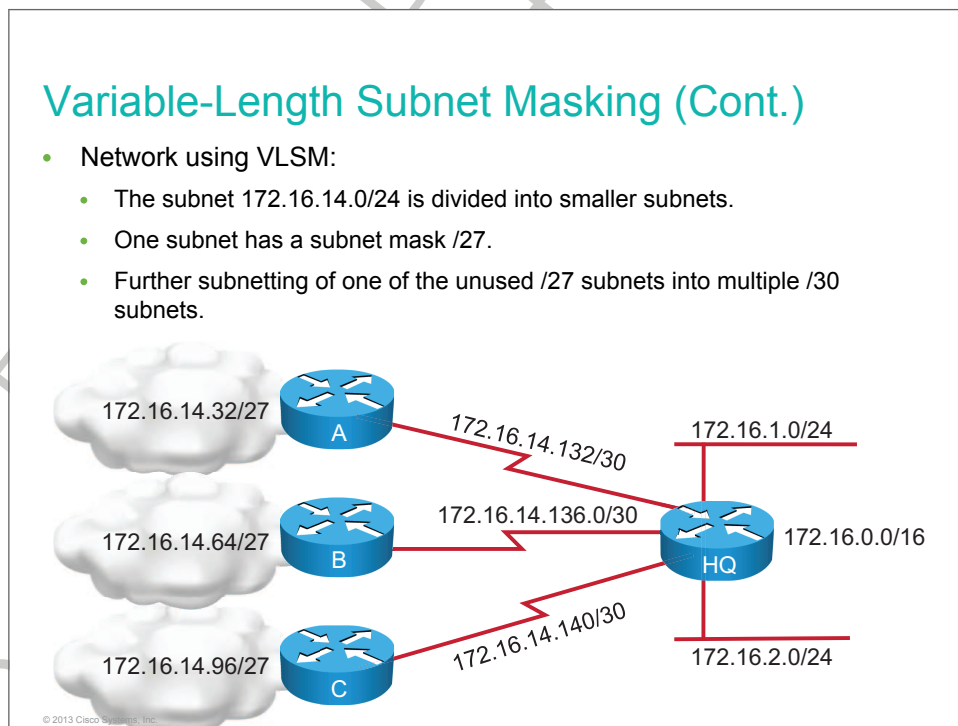
Do Not Duplicate
Post beta, not for release

Variable-Length Subnet Mask

This topic describes the purpose of a VLSM.



The figure illustrates a network that uses fixed-length prefixes to address various segments. Address space is wasted because large subnets are used for addressing point-to-point segments.



VLSM affords the options of including more than one subnet mask within a network and of subnetting an already subnetted network address. VLSM offers these benefits:

- **More efficient use of IP addresses:** Without the use of VLSM, companies must implement 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 that is divided into subnetworks using /24 masking. One of the subnetworks in this range, 172.16.14.0/24, is further divided into smaller subnetworks using /27 masking. These smaller subnetworks range from 172.16.14.0/27 to 172.16.14.224/27.

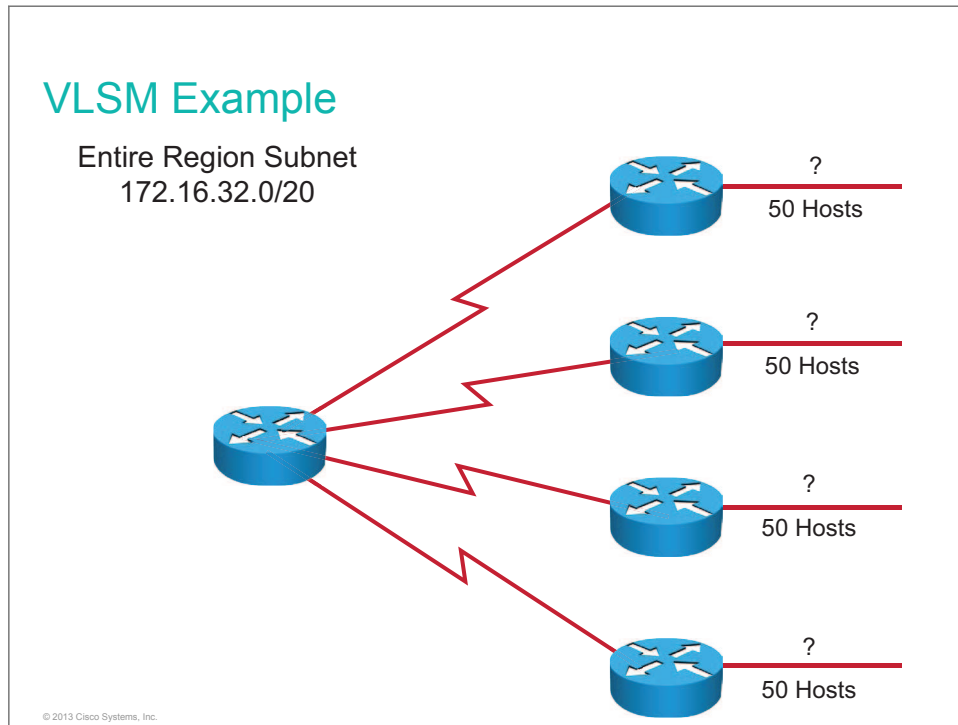
In the figure, one of these smaller subnets, 172.16.14.128/27, is further divided using the /30 prefix, which creates subnets with only two hosts, to be used on the WAN links. The /30 subnets range from 172.16.14.128/30 to 172.16.14.156/30. The WAN links used the 172.16.14.132/30, 172.16.14.136/30, and 172.16.14.140/30 subnets out of the range.

- **Better-defined network hierarchical levels:** VLSM allows more hierarchical levels within an addressing plan, which enables easier aggregation of network addresses. For example, in the figure, subnet 172.16.14.0/24 describes all of the addresses that are further subnets of 172.16.14.0, including those from subnet 172.16.14.0/27 to subnet 172.16.14.128/30.

Do Not Duplicate
Post beta, not for release

VLSM Example

This topic provides an example of VLSM.



In the figure, the subnet address 172.16.32.0/20, used for this portion of the enterprise network, is generated from subnetting the 172.16.0.0/16 network into multiple /20 subnets.

VLSM Example (Cont.)

Subnetted address: 172.16.32.0/20
 In binary: 10101100.00010000.**0010**0000.00000000

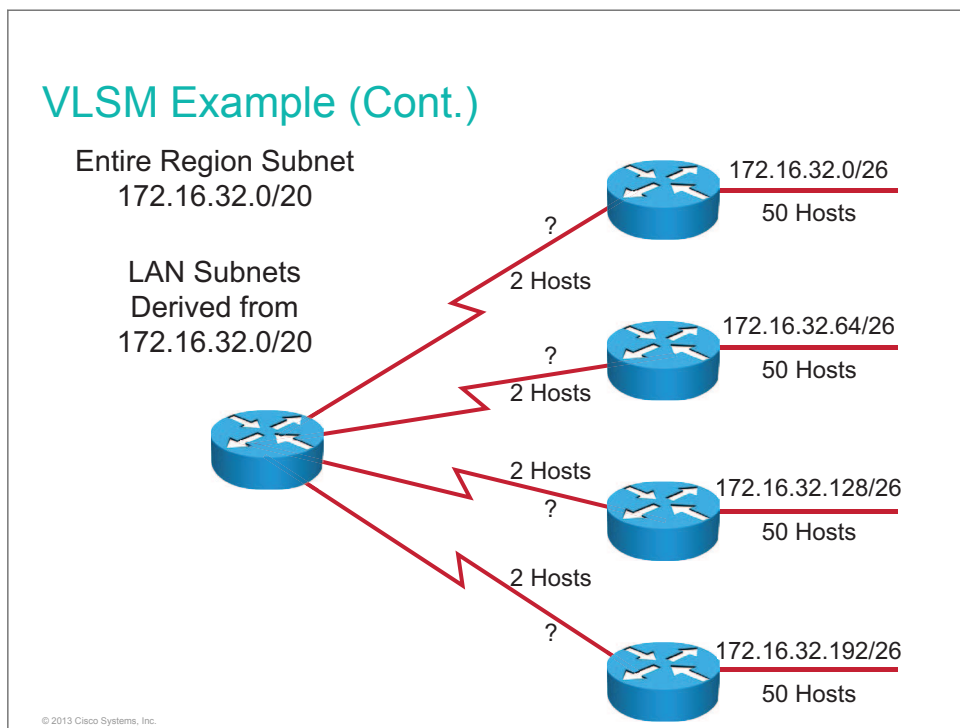
VLSM address: 172.16.32.0/26
 In binary: 10101100.00010000.**0010****0000.00**000000

	Network	Subnet	VLSM Subnet	Host	
1st subnet:	172	16	.0010	0000.00	000000 = 172.16.32.0/26
2nd subnet:	172	16	.0010	0000.01	000000 = 172.16.32.64/26
3rd subnet:	172	16	.0010	0000.10	000000 = 172.16.32.128/26
4th subnet:	172	16	.0010	0000.11	000000 = 172.16.32.192/26
5th subnet:	172	16	.0010	0001.00	000000 = 172.16.33.0/26

Note

© 2013 Cisco Systems, Inc.

By using VLSM, you can further subnet an already subnetted address. Consider, for example, that your region of the enterprise network has a subnet address of 172.16.32.0/20 and that you need to assign addresses to multiple LANs. Additionally, each LAN must have 50 hosts within your region. With VLSM, you can further subnet address 172.16.32.0/20 to give you more network addresses and fewer hosts per network. 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.



In the figure, the subnet addresses that are used on the Ethernet LANs are generated from subdividing the 172.16.32.0/20 subnet into multiple /26 subnets.

To calculate the subnet addresses that are used on the WAN links, further subnet one of the unused /26 subnets.

VLSM Example (Cont.)

Subnetted address: 172.16.33.0/26
 In binary: 10101100.00010000.00100001.00000000

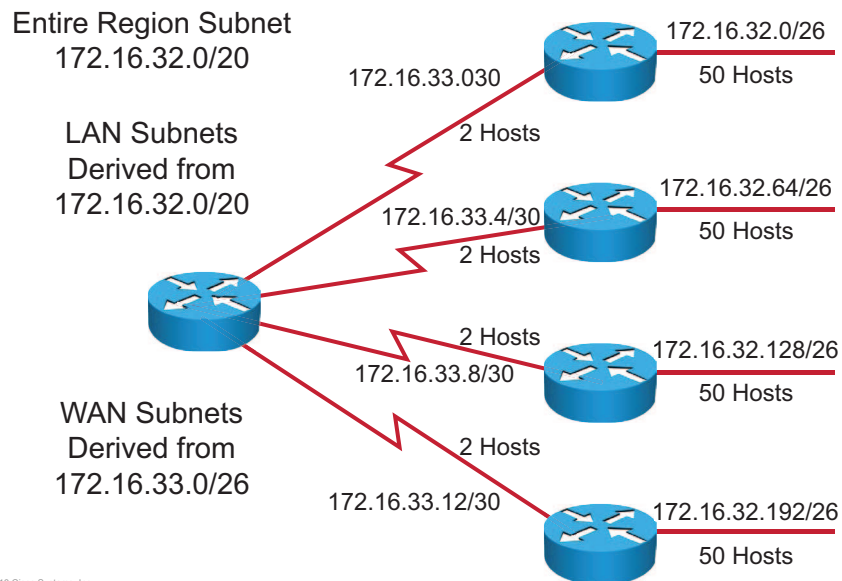
VLSM address: 172.16.33.0/30
 In binary: 10101100.00010000.00100001.00000000

	Network	Subnet	VLSM Subnet	Host
1st subnet:	172 . 16 . 33 . 0000	00	00 =	172.16.33.0/30
2nd subnet:	172 . 16 . 33 . 0000	01	01 =	172.16.33.4/30
3rd subnet:	172 . 16 . 33 . 0000	10	10 =	172.16.33.8/30
4th subnet:	172 . 16 . 33 . 0000	11	11 =	172.16.33.12/30

© 2013 Cisco Systems, Inc.

For each WAN link, you need only two IP addresses, one for each end of a connection. Therefore, only two bits are needed in the host portion of an IP address to create the appropriate subnet. Subnet mask /30 is used for each WAN subnet.

VLSM Example (Cont.)



© 2013 Cisco Systems, Inc.

In the figure, the subnet addresses that are used on the WAN links are generated from subdividing the 172.16.33.0/26 subnet into multiple /30 subnets. This mechanism provides 16 (2^4) subnets and 2 ($2^2 - 2$) hosts for each of the WANs.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Networks, particularly large networks, are often divided into smaller subnetworks, or subnets, which can improve network performance and control.
- The subnet mask defines the number of bits that represent the network part or subnet part of an IP address.
- End systems use subnet masks to identify the destination IP address as either local or remote.
- A default gateway is needed to send a packet out of the local network.
- Determining the optimal number of subnets and hosts depends on the type of network and the number of host addresses required.
- The algorithm for computing a number of subnets is 2^n , where n is the number of subnet bits.
- VLSM lets you allocate IP addresses more efficiently by adding multiple layers to the addressing hierarchy.

© 2013 Cisco Systems, Inc.

Understanding the TCP/IP Transport Layer

Overview

Data networks and the Internet provide seamless and reliable communications, locally and world-wide. Applications such as email, web browsers, and instant messaging allow you to use computers and networks to send messages and find information. Data from applications is packaged, transported, and delivered to the appropriate server or application on the destination device. The processes that are described in the TCP/IP transport layer accept data from the application layer and prepare it for addressing at the internet layer. The transport layer is responsible for the overall end-to-end transfer of application data. The transport layer also provides functions to enable multiple applications to communicate over the network at the same time on a single device. This layer uses error-processing mechanisms (if required) to ensure that all of the data is received reliably and in order by the correct application.

For the Internet and internal networks to function correctly, data must be delivered reliably. You can ensure reliable delivery of data through development of an application and by using the services that are provided by the network protocol. In the TCP/IP and OSI models, the transport layer manages the process of reliable data delivery. The transport layer hides the details of any network-dependent information from the higher layers to provide transparent data transfer. TCP/IP UDP and TCP therefore operate between the network layer and the application layer. Learning how UDP and TCP function between the network layer and the transport layer provides a more complete understanding of how data is transmitted in a TCP/IP networking environment. This lesson describes the function of the transport layer and how UDP and TCP operate.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

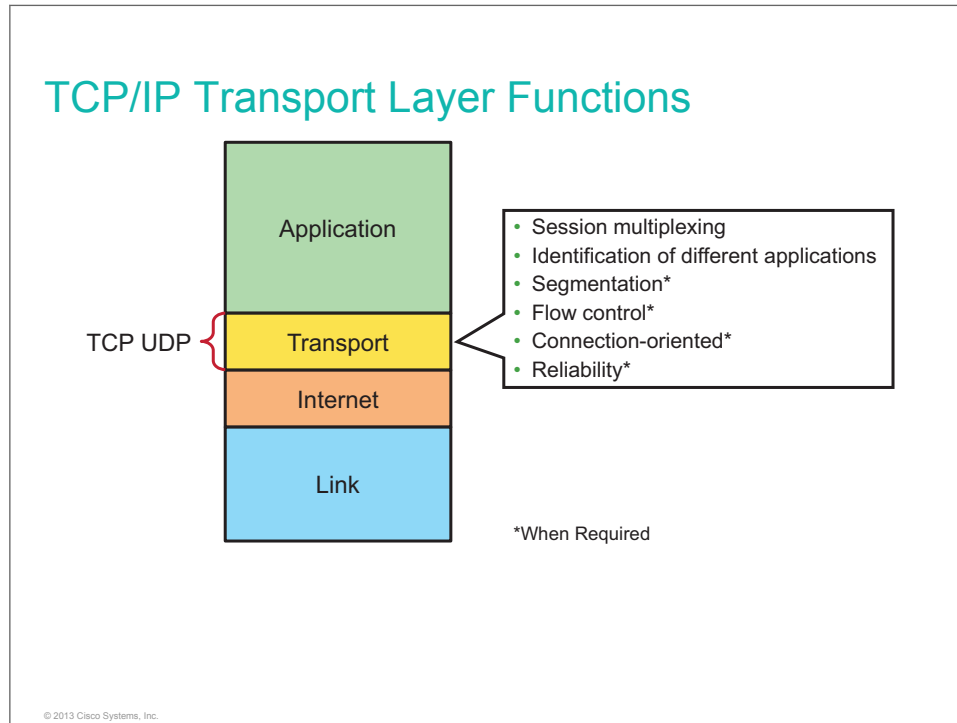
- Explain the purpose and major functions of the TCP/IP transport layer
- Contrast connection-oriented transport with connectionless transport
- Explain the basic difference between TCP and UDP

- List the characteristics of UDP
- List the characteristics of TCP
- List the common applications that are provided by TCP/IP

Do Not Duplicate.
Post beta, not for release.

TCP/IP Transport Layer Functions

Residing between the application and internet layers, the transport layer is fundamental to the operation of the TCP/IP layered network architecture. This topic describes the functions of the transport layer.



The TCP/IP internet layer directs information to its destination, but it cannot guarantee that the information will arrive in the correct order, free of errors, or even that it will arrive at all. The two most common transport layer protocols of the TCP/IP protocol suite are TCP and UDP. Both protocols manage the communication of multiple applications and provide communication services directly to the application process on the host. The basic service that is provided by the transport layer is tracking the individual communications between applications on the source and destination hosts. This service is called *session multiplexing*, and it is performed by both UDP and TCP. The premium service that is provided by the transport layer is ensuring reliable delivery, which is performed only by TCP.

The primary duty of the transport layer is to track the individual communications between applications on the source and destination hosts. This tracking is provided by both UDP and TCP. To pass data streams to the proper applications, the transport layer must identify the target application. If TCP is used, the transport layer has the further responsibilities of establishing end-to-end operations, segmenting data and managing each piece, reassembling the segments into streams of application data, managing flow control, and applying reliability mechanisms.

Session Multiplexing

Session multiplexing is an activity in which a single computer with a single IP address is able to support multiple sessions simultaneously. A session is created when a source machine needs to send data to a destination machine. Most often, this process involves a reply, but a reply is not mandatory.

Identifying the Applications

To pass data streams to the proper applications, the transport layer must identify the target application. The transport layer assigns an identifier to an application. The TCP/IP protocols call this identifier a *port number*. Each software process that needs to access the network is assigned a port number that is unique in that host. This port number is used in the transport layer header to indicate to which application that piece of data is associated.

Segmentation

TCP takes data chunks from the application layers and prepares them for shipment onto the network. Each chunk is broken up into smaller segments that will fit the MTU of the underlying network layers. UDP is simpler; it does no checking or negotiating and it expects the application process to give it data that will work.

Flow Control

If a sender transmits data faster than the receiver can receive it, the receiver drops the data and requires it to be retransmitted. Retransmission can waste time and network resources, which is why most flow control methods try to maximize the transfer rate and minimize the required retransmissions.

Basic flow implementation in TCP uses acknowledgments that are generated by the receiver. For every data chunk sent, the sender waits for this acknowledgment from the receiver before sending the next part. However, if the RTT is significant, the overall transmission rate may slow to an unacceptable level. A mechanism called *windowing* increases network efficiency when combined with basic flow control. Windowing allows a receiving computer to advertise how much data it is able to receive before transmitting an acknowledgment to the sending computer.

Connection-Oriented Transport Protocol

Within the transport layer, a connection-oriented protocol, such as TCP, establishes the session connection and then maintains the connection during the entire transmission. When the transmission is complete, the session is terminated.

Reliability

TCP reliability has these three main objectives:

- Recognition and correction of data loss
- Recognition and correction of duplicate or out-of-order data
- Avoidance of congestion in the network

Reliability is not always necessary. For example, in a video stream, if a packet is dropped and then retransmitted, it will appear out of order. That result would be frustrating and confusing to the audience and serve no useful purpose. In real-time applications, such as voice and video streaming, dropped packets can be tolerated as long as the overall percentage of dropped packets is low.

Reliable vs. Best-Effort Transport

“Reliable” and “best effort” are terms that describe two types of connections between computers. Each type has advantages and disadvantages. This topic compares the two connection types.

	Reliable	Best Effort
Protocol	TCP	UDP
Connection Type	Connection-oriented	Connectionless
Sequencing	Yes	No
Uses	<ul style="list-style-type: none">• Email• File sharing• Downloading	<ul style="list-style-type: none">• Voice streaming• Video streaming

© 2013 Cisco Systems, Inc.

Reliable (Connection-Oriented)

Applications such as databases, web pages, and email require that all of the sent data must arrive at the destination in its original condition in order for the data to be useful. Any missing data could cause a corrupt communication that is either incomplete or unreadable. Therefore, these applications are designed to use a transport layer protocol that implements reliability.

Some applications that use TCP are as follows:

- Web browsers
- Email
- File transfers

TCP is the reliable protocol at the transport layer. To support reliability, a connection is established. Establishing a connection ensures that the application is ready to receive the data. During the initial process of connection establishment, information is exchanged about the capabilities of the receiver and starting parameters are agreed to. These parameters are then used for tracking the data transfer for the duration of the connection.

When the sending computer transmits data, it gives the data a sequence number. The receiver then responds with an acknowledgment number equal to the next expected sequence number. This exchange of sequence and acknowledgment numbers allows the protocol to recognize when data has been lost or duplicated or has arrived out of order. TCP is a complex transport layer protocol.

Best Effort (Connectionless)

Other applications are more tolerant of the loss of small amounts of data. For example, if one or two segments of a video stream fail to arrive, it would only create a momentary disruption in the stream. This disruption might appear as distortion in the image, but it might not even be noticeable to the user.

Some applications that use UDP are as follows:

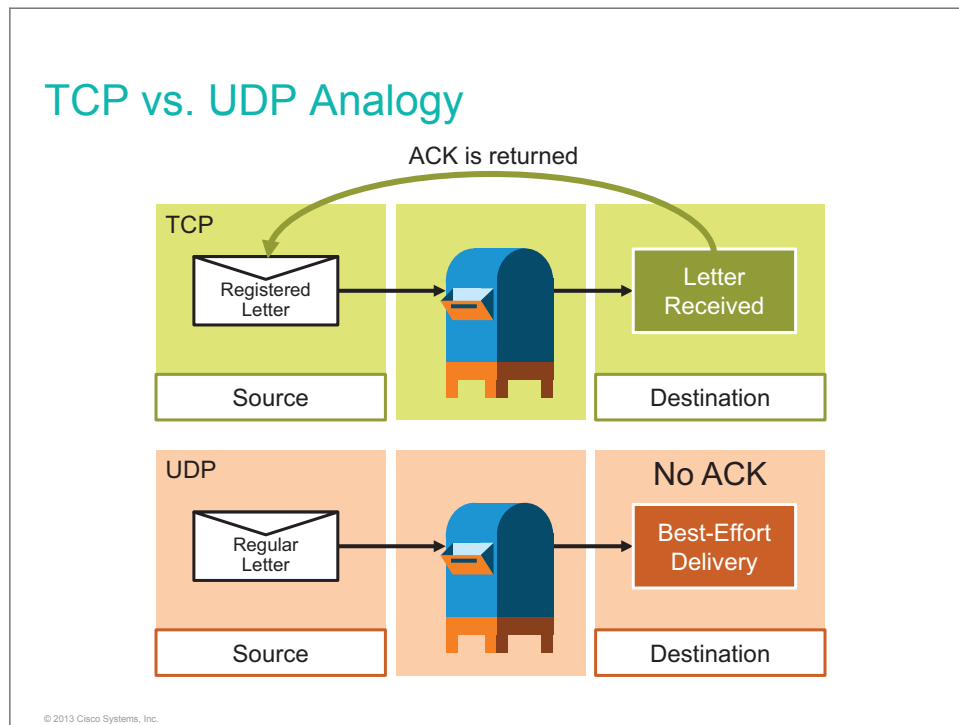
- Video streaming
- VoIP

UDP, providing best-effort delivery, does not need or want to keep information about previously sent data. Therefore, UDP does not need to establish any connection with the receiver and is termed *connectionless*. There are many situations in which best-effort delivery is more desirable than reliable delivery. A connectionless protocol is desirable for applications that require faster communication without verification of receipt.

Do Not Duplicate.
Post beta, not for release.

TCP vs. UDP Analogy

This topic describes the basic difference between TCP and UDP, using a postal service analogy.



Example: UDP—Sending Regular Mail

An analogy for UDP services is using the postal service to pay your bills. You address each bill payment to a specific company address, stamp the envelope, and include your return address. The postal service guarantees its best effort to deliver each payment. The postal service does not guarantee delivery, and it is not responsible for telling you that delivery was successful or unsuccessful. Like the postal service, UDP is a very simple protocol that provides only the most basic data-transfer services.

Example: TCP—Sending Certified Mail

An analogy for TCP services is sending certified mail through the postal service. Imagine that you live in San Francisco and that you have a book that must be sent to your mother in New York. You discover that the postal service will only process letters. You copy the pages in the book and put each page in a separate envelope. To ensure that your mother reassembles the book correctly, you number each envelope. You address the envelopes and send the first one as certified mail. The postal service delivers it by any truck and any route but, because it is certified, the carrier who delivers it must get a signature from your mother and return a certificate of delivery to you.

Sending each page separately is tedious, so you send several envelopes together. The postal service again delivers each envelope by any truck and any route. Your mother signs a separate receipt for each envelope in the batch as she receives them. If one envelope is lost in transit, you will not receive a certificate of delivery for that numbered envelope, and you would resend that page. After receiving all the envelopes, your mother puts the pages in the right order to recreate the book. Like certified mail, TCP is a complex protocol that offers precise and traceable data transfer services.

UDP Characteristics

The transport layer of the TCP/IP stack contains protocols that provide addressing information so that data can be transmitted over a network. UDP is an expansion of the early TCP/IP suite and is one of those protocols. This topic describes some of the major functions of UDP.

UDP Characteristics

- Operates at the transport layer of the TCP/IP stack
- Provides applications with access to the network layer without the overhead of reliability mechanisms
- Is a connectionless protocol
- Provides limited error-checking
- Provides best-effort delivery
- Has no data-recovery features

© 2013 Cisco Systems, Inc.

UDP is a simple protocol that provides the basic transport layer functions.

- UDP operates at the transport layer of the TCP/IP stack.
- UDP provides applications with access to the network layer without the overhead of reliability mechanisms.
- Like IP, UDP is a connectionless protocol in which a one-way datagram is sent to a destination without advance notification to the destination device.
- UDP is capable of performing very limited error-checking. The UDP datagram includes an optional checksum value, which the receiving device can use to test the integrity of the data. Additionally, the UDP datagram includes a pseudo-header that includes the destination address. If the receiving device sees that the datagram is directed to an inactive port, it returns a message that the port is unreachable.
- UDP provides service on a best-effort basis and does not guarantee data delivery, because packets can be misdirected, duplicated, or lost on the way to their destination.
- UDP does not provide any special features that recover lost or corrupted packets. This functionality does not mean that applications that use UDP are always unreliable. It simply means that these functions are not provided by the transport layer protocol.

UDP Characteristics (Cont.)

The UDP header:

16-Bit Source Port	16-Bit Destination Port
16-Bit UDP Length	16-Bit UDP Checksum
Data	

© 2013 Cisco Systems, Inc.

An analogy to UDP service is using a postal service to send flyers that notify neighbors about a garage sale. In this example, the seller creates a flyer that advertises the day, time, and location of the garage sale. The seller addresses each flyer with the specific name and address of each neighbor within a 2-mile (3.2-km) radius. The postal service delivers each flyer by any truck and any route. However, the seller does not use certified mail because it is not important if a flyer is lost in transit or if a neighbor acknowledges receipt of the flyer.

UDP has the advantage of providing low-overhead data delivery. This advantage is why the UDP header length is always only 64 bits (8 bytes). The figure shows the field definitions in the UDP segment:

- **Source Port:** Number of the calling port (16 bits)
- **Destination Port:** Number of the called port (16 bits)
- **Length:** Length of UDP header and UDP data (16 bits)
- **Checksum:** Calculated checksum of the header and data fields (16 bits)
- **Data:** ULP data (varies in size)

Application layer protocols that use UDP include DNS, SNMP, DHCP, RIP, TFTP, NFS, and online games.

TCP Characteristics

TCP is a connection-oriented protocol that provides data reliability between hosts. TCP has a number of characteristics that are related to the way in which it accomplishes this transmission. This topic describes the major characteristics of TCP.

TCP Characteristics

- Transport layer of the TCP/IP stack
- Access to the network layer for applications
- Connection-oriented protocol
- Full-duplex mode operation
- Error checking
- Sequencing of data packets
- Reliable delivery—acknowledgment of receipt
- Data-recovery features
- Flow control

© 2013 Cisco Systems, Inc.

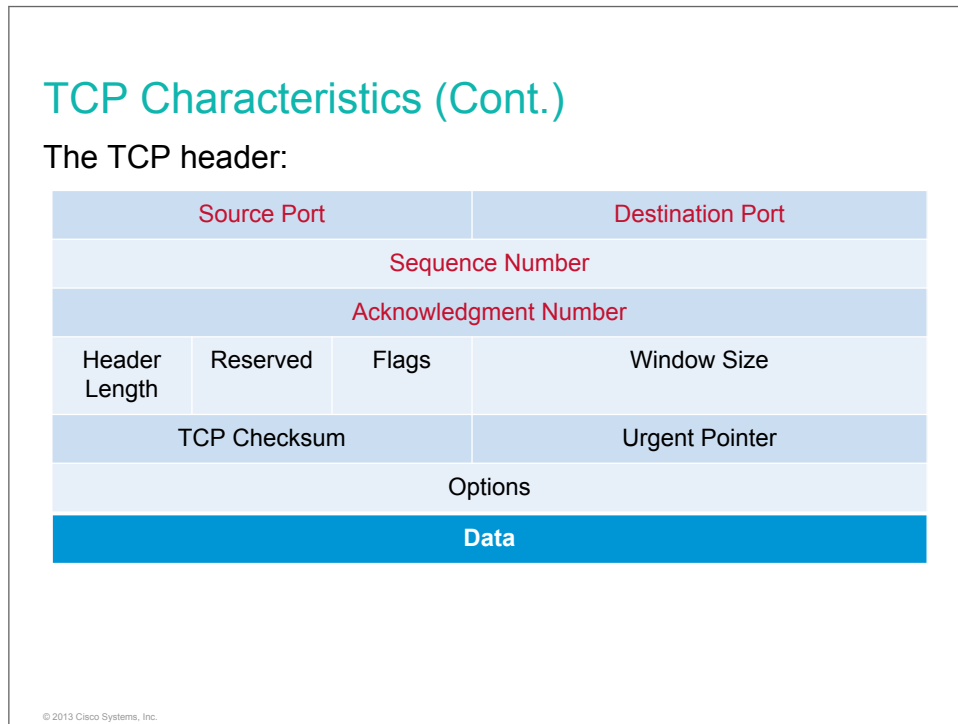
TCP is another protocol in the transport layer of the TCP/IP stack that provides addressing information so that data can be transmitted over a network.

TCP is characterized as follows:

- Like UDP, TCP operates at the transport layer of the TCP/IP stack.
- Like UDP, TCP provides a service to applications: access to the network layer.
- TCP is a connection-oriented protocol where two network devices set up a connection to exchange data. The end systems synchronize with each other to manage packet flows and adapt to congestion in the network.
- A TCP connection is a pair of virtual circuits, one in each direction, so that it operates in full-duplex mode.
- TCP provides error checking by including a checksum in the datagram to verify that the TCP header information is not corrupt.
- TCP segments are numbered and sequenced so that the destination can reorder segments and determine if data is missing.
- Upon receipt of one or more TCP segments, the receiver returns an acknowledgment to the sender to indicate that it received the segment. Acknowledgments form the basis of reliability within the TCP session. When the source receives acknowledgment, it knows that the data has been successfully delivered. If the source does not receive acknowledgment within a predetermined period, it retransmits that data to the destination. It may also terminate the connection if it determines that the receiver is no longer on the connection.
- TCP provides recovery services in which the receiver can request retransmission of a segment.

- TCP provides mechanisms for flow control. Flow control assists the reliability of TCP transmission by adjusting the effective rate of data flow between the two services in the session.

Reliable data delivery services are critical for applications such as file transfers, database services, transaction processing, and other mission-critical applications in which delivery of every packet must be guaranteed. TCP provides this reliability but sometimes sacrifices speed. UDP provides speed at the expense of reliability.

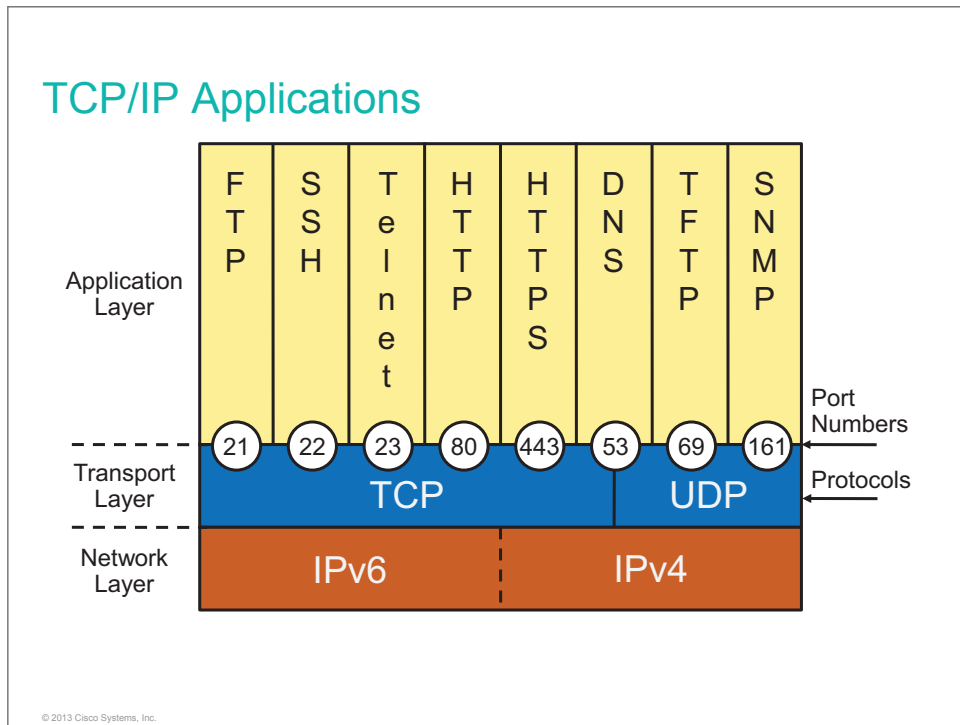


TCP segments are sent by using IP packets. The TCP header follows the IP header, and supplies information specific to the TCP protocol. Flow control, reliability, and other TCP characteristics are achieved by having fields in the TCP segment header, each with a specific function. The fields of the TCP header include the following:

- **Source port:** Number of the calling port (16 bits)
- **Destination port:** Number of the called port (16 bits)
- **Sequence number and acknowledgment number:** Tools for reliability mechanisms (each 32 bits)
- **Acknowledgment number:** The next TCP octet that is expected by the receiver (32 bits)
- **Checksum:** Calculated checksum of the header and fields that are used for error checking (16 bits)
- **Data:** Upper-layer protocol data (varies in size)
- **Header length:** Number of 32-bit words in the header (4 bits)
- **Reserved:** Set to 0 (3 bits)
- **Flags:** Used in session management and in treatment of segments (9 bits). A single bit that has a specific meaning is often referred to as a flag.
- **Window size:** Number of octets that the device is willing to accept (16 bits)
- **Urgent pointer:** Indicates the end of the urgent data (16 bits)
- **Options:** The variable-length field, which contains optional headers that you may want to use. Maximum TCP segment size is currently defined.

TCP/IP Applications

UDP and TCP use internal software ports to support multiple conversations between various network devices. To differentiate the segments and datagrams for each application, TCP and UDP both have header fields that uniquely identify these applications. These unique identifiers are the port numbers. This topic lists various applications along with their port numbers and short descriptions.



These are some of the applications that TCP/IP supports:

- **FTP (port 21, TCP):** FTP is a reliable, connection-oriented service that uses TCP to transfer files between systems that support FTP. FTP supports bidirectional binary and ASCII file transfers. In addition to port 21, which is used for exchange of control, it also uses one additional port for data transmission.
- **SSH (port 22, TCP):** SSH provides the capability to remotely access other computers, servers, and networking devices. SSH enables a user to log in to a remote host and execute commands. SSH messages are encrypted.
- **Telnet (port 23, TCP):** Telnet is a predecessor to SSH. It sends messages in unencrypted cleartext. Most organizations now use SSH for remote communications.
- **HTTP (port 80):** HTTP defines how messages are formatted and transmitted and what actions browsers and web servers take in response to various commands. It uses TCP.
- **HTTPS (port 443, TCP):** HTTPS combines HTTP with a security protocol (SSL/TLS).
- **DNS (port 53, TCP and UDP):** DNS is used to resolve Internet names to IP addresses. DNS uses a distributed set of servers to resolve names that are associated with numbered addresses.
- **TFTP (port 69, UDP):** TFTP is a connectionless service. Routers use TFTP to transfer configuration files and Cisco IOS images as well as other files between systems that support TFTP.
- **SNMP (port 161, UDP):** SNMP is an application layer protocol and facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

These are just some applications with their port numbers. Go to the Service Name and Transport Protocol Port Number Registry for a complete list at <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>.

Do Not Duplicate:
Post beta, not for release.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The purpose of the transport layer is to hide the network requirements from the application layer and to ensure end-to-end transfer of application data.
- Connection-oriented transport provides reliable transport. Connectionless transport provides best-effort transport.
- UDP is a protocol that operates at the transport layer and provides applications with access to the network layer without the overhead of the reliability mechanisms of TCP. UDP is a connectionless, best-effort delivery protocol.
- TCP is a protocol that operates at the transport layer and provides applications with access to the network layer. TCP is connection-oriented and provides reliable transport.
- Port numbers identify applications.

© 2013 Cisco Systems, Inc.

Exploring the Functions of Routing

Overview

Routing is the process that forwards data packets between networks or subnetworks, using a TCP/IP internet layer device, a router. The routing process uses network routing tables, protocols, and algorithms to determine the most efficient path for forwarding an IP packet. Routers gather routing information and update other routers about changes in the network. Routers greatly expand the scalability of networks by terminating Layer 2 collisions and broadcast domains. Understanding how routers function will help you to understand the broader topic of how networks are connected and how data is transmitted over networks. This lesson describes the operation of routing.

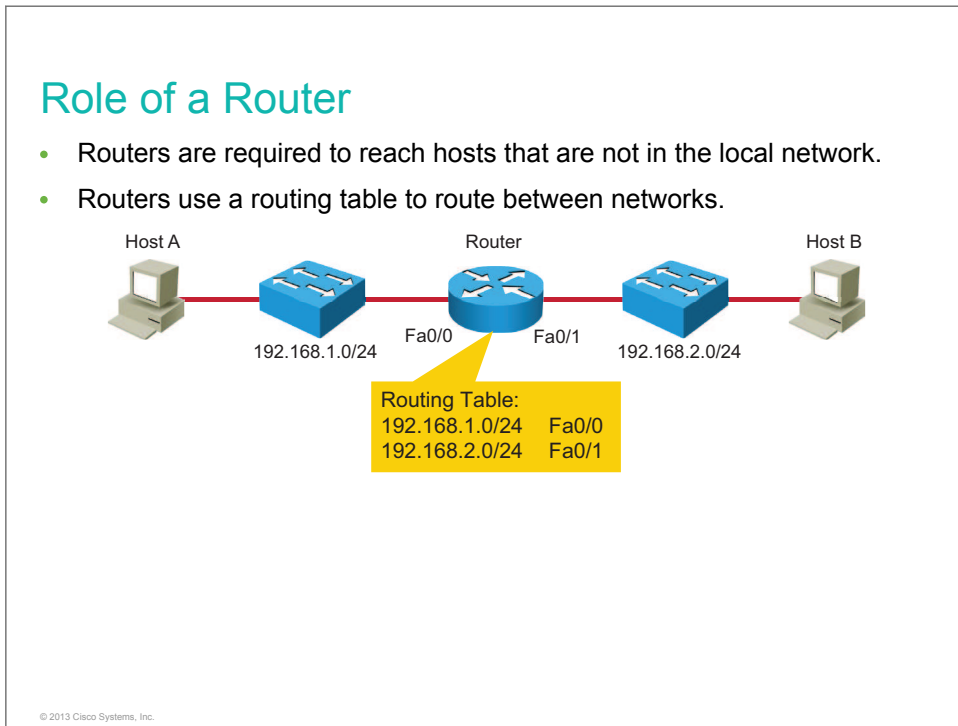
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the role of a router in the IP packet delivery process
- Describe the physical characteristics of a router
- Describe the functions of a router
- Describe the method that is used to determine the optimal path for forwarding IP packets
- Describe the functions of the routing table in the routing process
- List types of routes
- Describe the function of dynamic routing protocols

Role of a Router

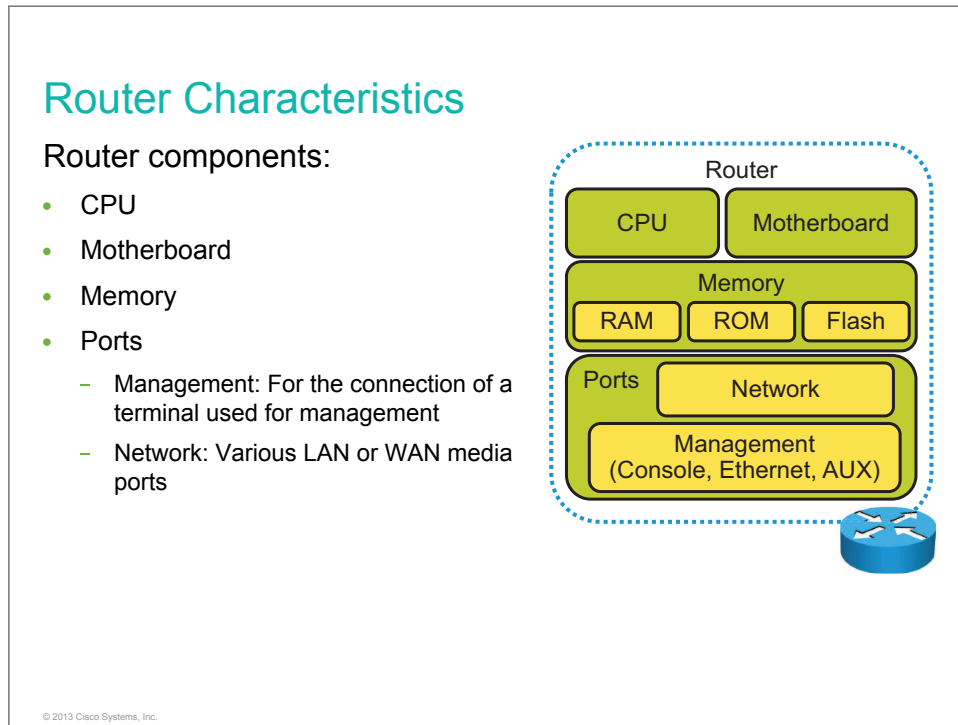
This topic describes the role of a router in internetwork communication.



While switches switch data frames between segments to enable communication within a single network, routers are required to reach hosts that are not in the local LAN. Routers enable internetwork communication by placing the interface of each router in the network of the other routers. They use routing tables to route traffic between different networks.

Router Characteristics

This topic describes common characteristics of routers.



Routers are essential components of large networks that use TCP/IP, because routers can accommodate growth across wide geographical areas. These characteristics are common to all routers:

- Routers have these components, which are also found in computers and switches:
 - **CPU:** The CPU, or processor, is the chip, that is installed on the motherboard, that carries out the instructions of a computer program. For example, it processes all of the information that is gathered from other routers or sent to other routers.
 - **Motherboard:** The motherboard is the central circuit board, which holds critical electronic components of the system. The motherboard provides connections to other peripherals and interfaces.
 - **Memory:** There are three types of memory: RAM, ROM, and flash. RAM is memory on the motherboard that stores data during CPU processing. It is a volatile type of memory in that its information is lost when power is switched off. ROM is read-only memory on the motherboard. The content of ROM is not lost when power is switched off. Data stored in ROM cannot be modified, or it can be modified only slowly or with difficulty, so it is mainly used to distribute firmware. Flash memory is a nonvolatile storage chip that can be electrically erased and reprogrammed.
- Routers have various network ports to which IP addresses are assigned. Ports are used to connect routers to other devices in the network.

Routers can have these types of ports:

- **Management port (console, Ethernet, auxiliary [AUX]):** The router uses a console port to attach to a terminal that is used for management, configuration, and control. High-end routers have a dedicated Ethernet port used only for management. An IP address is assigned to the Ethernet port and the router may be accessed from the management subnet. The AUX interface is used for remote management of the router. Typically, a modem is connected to the AUX interface for dial-in access. From a security standpoint, enabling the option to connect remotely to a network device carries with it the responsibility of vigilant device management.
- **Network port:** The router has a number of network ports, including various LAN or WAN media ports, which may be copper or fiber cable.

Do Not Duplicate.
Post beta, not for release.

Router Functions

This topic describes the two most important functions of routers, path determination and packet forwarding.

Router Functions

- Path determination
- Packet forwarding

```
RouterA#show ip route
Codes: L - local, C - connected, S - static, 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
       <output omitted>
Gateway of last resort is not set
 172.17.0.0/16 is variably subnetted, 8 subnets
O    172.17.14.0/24 [110/51] via 172.17.100.22, 1d05h
B    172.17.25.0/24 [200/0] via 172.17.100.22, 6d05h
D    172.17.43.0/24 [90/30720] via 172.17.50.4, 3d20h, GigabitEthernet0/0
C    172.17.50.0/24 is directly connected, GigabitEthernet0/0
L    172.17.50.2/32 is directly connected, GigabitEthernet0/0
S    172.17.92.0/24 [1/0] via 172.17.50.4
C    172.17.100.0/24 is directly connected, GigabitEthernet0/1
L    172.17.100.12/32 is directly connected, GigabitEthernet0/1
```

- Routing table on RouterA

© 2013 Cisco Systems, Inc.

Routers are devices that gather routing information from neighboring routers in the network. The routing information that is processed locally goes into the routing table. The routing table contains a list of all known destinations to the router and provides information about how to reach them. Routers have these two important functions:

- **Path determination:** Routers must maintain their own routing tables and ensure that other routers know about changes in the network. Routers use a routing protocol to communicate network information to other routers. A routing protocol distributes the information from a local routing table on the router. Different protocols use different methods to populate the routing table. In the **show ip route** output in the figure, the first letter in each line of the routing table indicates which protocol was the source for the information (for example, O = OSPF). It is possible to statically populate routing tables by manually configuring static routes. However, statically populating routing tables does not scale well and leads to problems when the network topology changes. Design changes and outages can also pose problems.
- **Packet forwarding:** Routers use the routing table to determine where to forward packets. Routers forward packets through a network interface toward the destination network. Each line of the routing table indicates which network interface is used to forward a packet. The destination IP address in the packet defines the packet destination. Routers use their local routing table and compare the entries to the destination IP address of the packet. The result is a decision about which outgoing interface to use to send the packet out of the router. If routers do not have a matching entry in their routing tables, the packets are dropped.

Routers support three packet-forwarding mechanisms:

- **Process switching:** Process switching is the oldest forwarding mechanism that is available in Cisco routers. Every packet requires full lookup in the routing table, which makes this mechanism very slow. It is typically not used in modern networks.

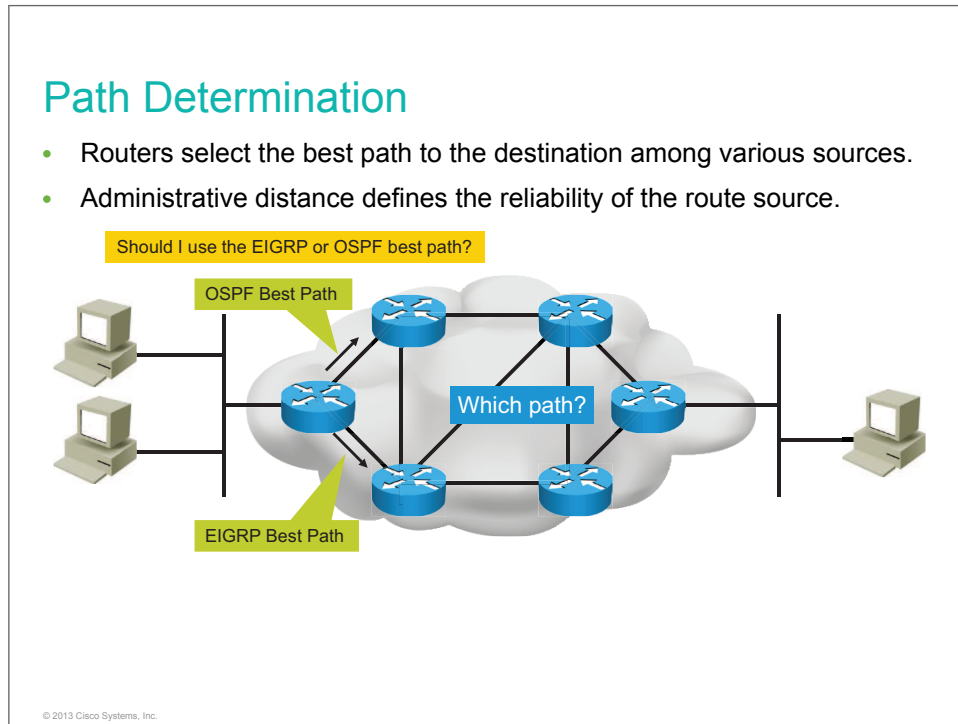
- **Fast switching:** To overcome the slow performance of process switching, Cisco IOS platforms support several switching mechanisms that use a cache to store the most recently used destinations. The first packet whose destination is not found in the fast-switching cache is process-switched, and an entry is created in the cache. Subsequent packets are switched in the interrupt code, using the cache to improve performance.
- **Cisco Express Forwarding:** Cisco Express Forwarding is the most recent and preferred Cisco IOS packet-forwarding mechanism, which incorporates the best of the previous switching mechanisms. Generation of cache table entries is not packet-triggered but change-triggered. When something changes in the network topology, the change is also reflected in the cache table. This makes Cisco Express Forwarding the fastest forwarding mechanism and the preferred choice.

In the figure, the **show ip route** command displays the routing table that the Cisco IOS Software of RouterA is currently using to choose the best path to its destination networks.

Do Not Duplicate.
Post beta, not for release.

Path Determination

During the path-determination portion of transmitting data over a network, routers evaluate the available paths to remote destinations. This topic describes how routers determine the most efficient path for forwarding packets.



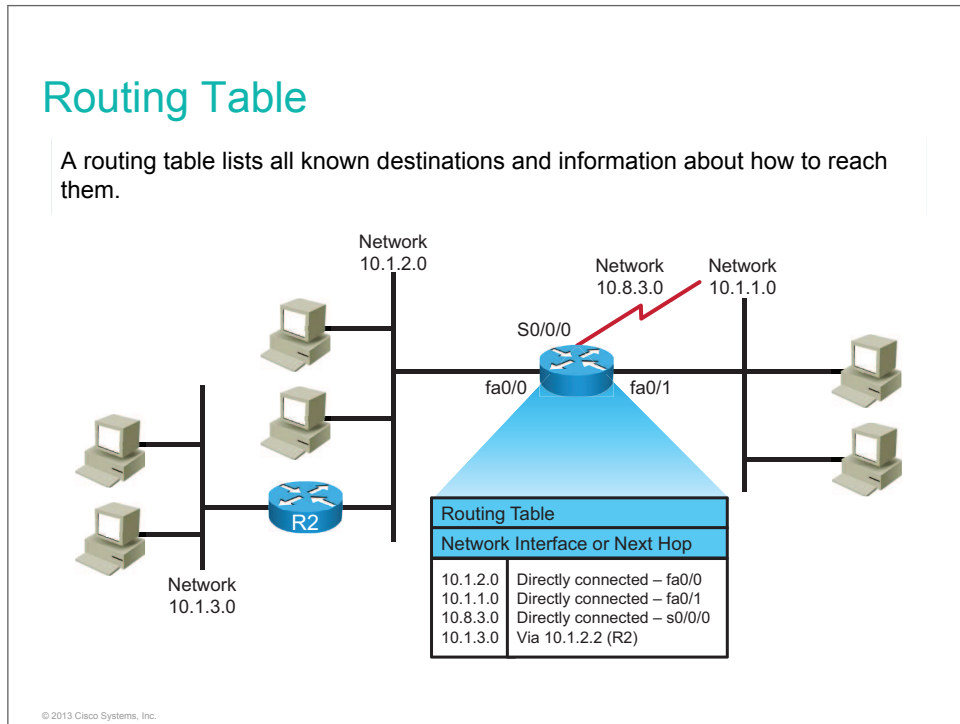
A routing table holds only one entry per network. More sources of information about a particular destination might exist. A router must be able to determine which source (routing protocol) it should use if it has two identical routes to a network from two different sources. Multiple sources result from having multiple dynamic routing protocols running and from static and default information being available. The routing process that runs on the router must be able to evaluate all the sources and select the best one to populate the routing table.

Routing protocols use different metrics to measure the distance and desirability of a path to a destination network. Administrative distance is the feature that routers use to select the best path when there are two or more routes to the same destination network from two routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized from most to least reliable (believable) with the help of an administrative distance value.

For example, in the figure, the router on the far left has two paths to the destination network on the far right. One of the paths is learned through a dynamic routing protocol, OSPF, and the other path is learned through EIGRP. Since EIGRP has a better (lower) administrative distance than OSPF, the router on the far left will use the EIGRP path and publish only the EIGRP path to the destination network in its routing table.

Routing Table

As part of the path-determination procedure, the routing process builds a routing table that identifies known networks and how to reach them. This topic describes the function of the routing table in the routing process.



Routers forward packets using the information in a routing table. Each router has its own local routing table, populated from different sources. Routing metrics vary, depending on the routing protocol that is running in the router. The figure shows how routers maintain a table of information.

Routing Table Information

The routing table consists of an ordered list of known network addresses. Network addresses can be learned dynamically by the routing process or by being statically configured. All directly connected networks are added to the routing table automatically. Routing tables also include information about destinations and next-hop associations. These associations tell a router that a particular destination is either directly connected to the router or that it can be reached via another router. This router is the next-hop router and is on the path to the final destination. When a router receives an incoming packet, it uses the destination address and searches the routing table to find the best path. If no entry can be found, the router discards the packet after sending an ICMP message to the source address of the packet.

In the figure, the routing table of the router in the middle shows the forwarding rules. When the router receives a packet with a destination address on the 10.1.3.0 network, it must forward the packet to router R2 (the R2 interface with the IP address 10.1.2.2).

Routing Update Messages

Routers communicate with each other and maintain their routing tables. A number of update messages are transmitted between routers in order to keep the routing tables updated. The information that is contained in the routing update messages includes the destination networks that the router can reach and the routing metric for each destination. By analyzing routing updates from neighboring routers, a router can dynamically build and maintain its routing table.

Types of Routes

Routers can learn about other networks via directly connected networks, static routes, dynamic routes, and default routes. This topic describes each of these types of routes.

```
Types of Routes

RouterA#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.1.1.1 to network 0.0.0.0
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.2/32 is directly connected, GigabitEthernet0/0
O 172.16.1.0/24 [110/2] via 192.168.10.2, 00:01:08, GigabitEthernet0/1
D 192.168.20.0/24 [90/156160] via 10.1.1.1, 00:01:23, GigabitEthernet0/0
S 192.168.30.0/24 [1/0] via 192.168.10.2
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 10.1.1.1

© 2013 Cisco Systems, Inc.
```

The routing table can be populated by these methods:

- **Directly connected networks:** This entry comes from having router interfaces that are directly attached to network segments. This method is the most certain method of populating a routing table. If the interface fails or is administratively shut down, the entry for that network is removed from the routing table. The administrative distance is 0 and therefore preempts all other entries for that destination network. Entries with the lowest administrative distance are the best, most-trusted sources.
- **Static routes:** A system administrator manually enters static routes directly into the configuration of a router. The default administrative distance for a static route is 1; therefore, static routes will be included in the routing table unless there is a direct connection to that network. Static routes can be an effective method for small, simple networks that do not change frequently. For bigger or unstable networks, static routes are not a scalable solution.
- **Dynamic routes:** The router learns dynamic routes automatically when a routing protocol is configured and a neighbor relationship to other routers is established. The information changes with changes in the network and updates constantly. Larger networks require the dynamic routing method because there are usually many addresses and constant changes. These changes require updates to routing tables across all routers in the network, or connectivity is lost.
- **Default routes:** A default route is an optional entry that is used when no explicit path to a destination is found in the routing table. The default route can be manually inserted or it can be populated from a dynamic routing protocol.

The figure displays the **show ip route** command, which is used to show the contents of the routing table in a router. The first part of the output explains the codes, presenting the letters and the associated source of the entries in the routing table.

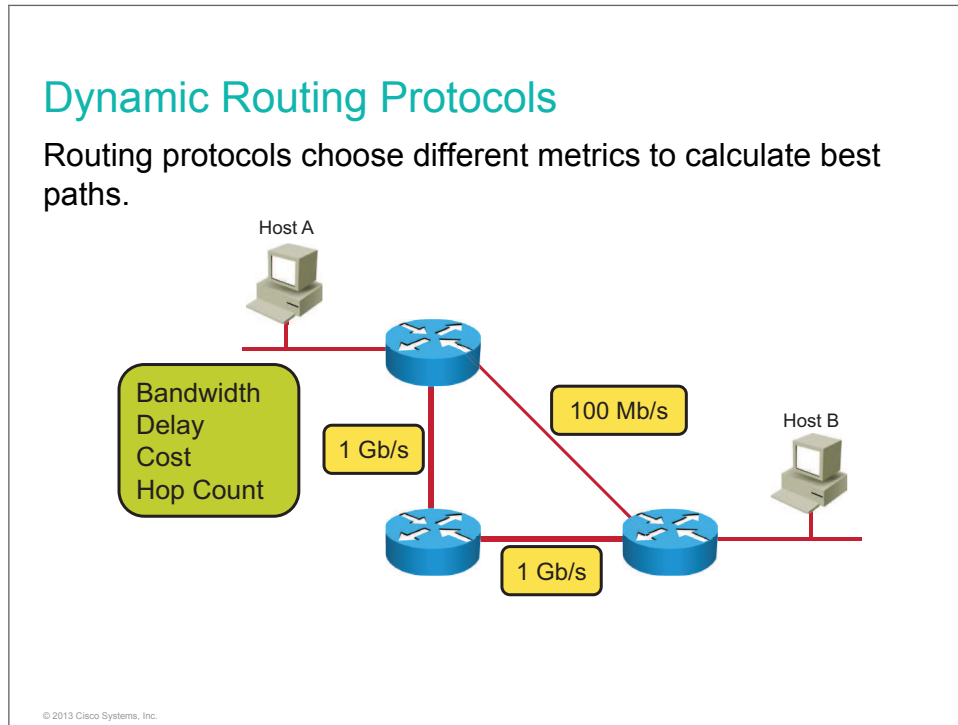
- The letter C, which is reserved for directly connected networks, labels the first and seventh entries.

- The letter L, which is reserved for local routes and indicating local interfaces within connected networks, labels the second and eighth entries.
- The letter S, which is reserved for static routes, labels the sixth entry. The letter S with an asterisk (*) indicates a static default route, as shown in the figure.
- The letter O, which is reserved for the OSPF routing protocol, labels the third entry.
- The letter D, which is reserved for EIGRP, labels the fourth entry. The letter D stands for DUAL, the update algorithm used by EIGRP.

Do Not Duplicate.
Post beta, not for release.

Dynamic Routing Protocols

Routing protocols use their own rules and metrics to build and update routing tables automatically. This topic describes the routing metrics and methods that routing protocols use.



When a routing protocol updates a routing table, the primary objective of the protocol is to determine the best information to include in the table. The routing algorithm generates a number, called the *metric*, for each path through the network. Sophisticated routing protocols can base route selection on multiple metrics, combining them into a single metric. Typically, the lower the metric value, the better the path.

Metrics can be based on either a single characteristic or on several characteristics of a path. These metrics are most commonly used by routing protocols:

- **Bandwidth:** The data capacity of a link (the connection between two network devices).
- **Delay:** The length of time that is required to move a packet along each link from the source to the destination. The delay depends on the bandwidth of intermediate links, port queues at each router, network congestion, and physical distance.
- **Cost:** An arbitrary value that is assigned by a network administrator, usually based on bandwidth, administrator preference, or other measurement, such as load or reliability.
- **Hop count:** The number of routers that a packet must travel through before reaching its destination. In the figure, the hop count from Host A to Host B would be two if the path over the 100-Mb/s link is used. The hop count would be three if the path over the 1-Gb/s link is used.

Distance Vector vs. Link State



You can divide routing protocols into two groups, based on how they operate and how they calculate the best path:

- **Distance vector routing protocols** have information available that is similar to the information from a road sign. If you are on the road and you do not have a map, you must rely on road signs that tell you the direction of the destination and the distance to it. Similarly, in distance vector routing, a router does not have to know the entire path to every network segment. The router only has to know the direction, or vector, in which to send the packet. The distance vector routing approach determines the direction (vector) and distance (hop count) to any destination network. An example of a distance vector protocol is RIP, which uses hop count as its routing metric.
- **Link state routing protocols** have a complete map of the area. Each router builds its own internal map of the entire network topology in its link state (topology) database. Each router on its own runs an SPF algorithm to calculate the shortest path to all known destinations. An example of a link state routing protocol is OSPF, which uses cost as its routing metric.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Routers enable internetwork communication.
- Routers include various ports and hardware similar to PCs.
- The primary functions of a router are path determination and packet forwarding.
- Routers select the best path from among different sources, based on administrative distance.
- Routing tables provide an ordered list of best paths to known networks.
- Routers use various types of routes: directly connected networks and static, dynamic, and default routes.
- Dynamic routing protocols use different metrics to calculate the best path.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Configuring a Cisco Router

Overview

After hardware installation, when a Cisco router is turned on, it goes through its startup procedure. After the operating system is loaded, you can start configuring the router. This lesson describes basic configuration, how to configure interfaces, and how to use Cisco Discovery Protocol to discover connected neighboring devices.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe router startup
- Perform initial router setup
- Configure router interfaces
- Configure a router interface IP address
- Verify the router interface configuration
- Describe the need for a network discovery protocol
- Describe Cisco Discovery Protocol
- Use the CLI to discover neighbors on a network using Cisco Discovery Protocol

Initial Router Startup

Starting a Cisco router requires verifying the physical installation, powering up the router, and viewing the Cisco IOS Software output on the console. This topic describes the initial startup of Cisco routers.

Initial Router Startup

Initial startup:

- Before you start the router, verify the power and cooling requirements, cabling, and console connection.
- Push the power switch to On.
- System startup routines initiate the router software.
- Cisco IOS Software output text appears on the console.



© 2013 Cisco Systems, Inc.


When a Cisco router powers up, it performs a power-on self-test (POST). During the POST, the router executes diagnostics to verify the basic operation of the CPU, memory, and interface circuitry.

After verifying the hardware functions, the router proceeds with software initialization. During software initialization, the router finds and loads the Cisco IOS image. When the Cisco IOS image is loaded, the router finds and loads the configuration file, if one exists.

Initial Router Setup

When the router starts, it looks for a device configuration file. If it does not find one, the router executes a question-driven initial configuration routine called *setup*. This topic describes the initial command-line output and explains how to skip the setup dialog.

Initial Router Setup



```
RouterX con0 is now available
Press RETURN to get started.
RouterX>
```

- A configured router with an existing configuration displays a user EXEC mode prompt.

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

- A router without an existing configuration enters the system configuration dialog.

© 2013 Cisco Systems, Inc.

After a router completes the POST and loads a Cisco IOS image, it looks for a device configuration file in its NVRAM. The NVRAM of the router is a type of memory that retains its contents, even when power is turned off. If the router has a configuration file in NVRAM, the user EXEC mode prompt appears. The figure shows the *RouterX>* prompt.

When you start a new Cisco router or a Cisco router without a configuration in NVRAM, there will be no configuration file. If no valid configuration file exists in NVRAM, the operating system executes a question-driven initial configuration routine that is referred to as the *system configuration dialog* or *setup mode*.

The system configuration dialog is an interactive CLI mode that prompts you for information that is needed to build an initial configuration for a Cisco networking device. It is not intended for more advanced configuration. Rather than using setup mode, you can use various other manual configuration modes to configure the router.

To skip the system configuration dialog and configure the router manually, answer the first question in the system configuration dialog with **No** or press **Ctrl-C**. If desired, you can enter the system configuration dialog anytime by issuing the **setup** command in privileged EXEC mode.

Configuring Router Interfaces

One of the main functions of a router is to forward packets from one network device to another. For the router to perform this task, you must define the characteristics of the interfaces through which the packets are received and sent. This topic describes the commands that are used to configure interfaces on Cisco routers.

Configuring Router Interfaces

```
RouterX(config)#interface GigabitEthernet 0/0
RouterX(config-if)#
```

- Enters GigabitEthernet 0/0 interface configuration mode

```
RouterX(config)#interface Serial 0/0/0
RouterX(config-if)#description Link to ISP
```

- Enters Serial 0/0/0 interface configuration mode and adds descriptive text

© 2013 Cisco Systems, Inc.

The router interface characteristics include, but are not limited to, interface description, the IP address of the interface, the data-link encapsulation method, the media type, the bandwidth, and the clock rate.

You can enable many features on a per-interface basis. Enter interface configuration mode using this command:

Command	Description
interface <i>type module/slot/port</i>	Specifies an interface and enters interface configuration mode. The <i>type</i> values include GigabitEthernet, Serial, Loopback, Dialer, Tunnel, and others. The <i>module</i> , <i>slot</i> , and <i>port</i> options identify specific interfaces.

A number that is used to identify each interface is assigned, based on the physical location of the interface hardware in the router. This identification is critical when there are multiple interfaces of the same type in a single router.

You can add a description to an interface to help you remember specific information about that interface. Common descriptions include the network that is serviced by that interface or the customer that is connected to that interface. The description is meant solely as a comment to help identify how the interface is being used.

Command	Description
<code>description string</code>	Adds a text comment to the interface configuration when in interface configuration mode. The <i>string</i> value is limited to 238 characters. To remove the description, use the no form of this command.

To quit interface configuration mode and to move into global configuration mode, enter the **exit** command.

The description will appear in the output when the configuration of the router is displayed. The same text will appear in the **show interfaces** command output:

```
RouterX#show interfaces
<output omitted>
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet,
  address is 5475.d08e.9ad8 (bia 5475.d08e.9ad8)
  Description: Link to ISP
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

Configuring Router Interfaces (Cont.)

```
RouterX#configure terminal
RouterX(config)#interface GigabitEthernet 0/0
RouterX(config-if)#no shutdown
%LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

- Enables an interface that is administratively shut down

```
RouterX#configure terminal
RouterX(config)#interface Serial 0/0/0
RouterX(config-if)#shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to down
```

- Administratively disables an interface

© 2013 Cisco Systems, Inc.

When an interface is first configured, except in setup mode, you must administratively enable the interface before it can be used to transmit and receive packets. Use the **no shutdown** command to allow Cisco IOS Software to use the interface.

You may want to disable an interface to perform hardware maintenance on a specific interface or a segment of a network. You may also want to disable an interface if a problem exists on a specific segment of the network and you must isolate that segment from the rest of the network.

The **shutdown** command administratively turns off an interface. To restart the interface, use the **no shutdown** command.

Configuring the Cisco Router IP Address

Each interface on a Cisco router must have its own IP address to uniquely identify it on the network. This topic describes how to configure the IP address for each interface on a Cisco router.

Configuring the Cisco Router IP Address

Each router interface needs a unique IP address.

```
RouterX#configure terminal
RouterX(config)#interface Serial 0/0/0
RouterX(config-if)#ip address 172.18.0.1 255.255.0.0
```

- Configures an IP address on the Serial 0/0/0 interface on router RouterX

© 2013 Cisco Systems, Inc.

Unique IP addressing is required for communication between hosts and other network devices. Each router link to a different network is associated to a dedicated and unique subnet. The router needs to have an IP address configured on each of its links to each network.

To configure an interface on a Cisco router, complete these steps.

Step	Action	Results and Notes
1	Enter global configuration mode using the configure terminal command: Router# configure terminal	Displays a new prompt: Router(config)#
2	Identify the specific interface that requires an IP address by using the interface type module/slot/port command: Router(config)# interface Serial 0/0/0	Displays a new prompt; for example: Router(config-if)#
3	Set the IP address and subnet mask for the interface by using the ip address ip-address mask command: Router(config-if)# ip address 172.18.0.1 255.255.0.0	Configures the IP address and subnet mask for the selected interface
4	Enable the interface to change state from administratively down to up by using the no shutdown command: Router(config-if)# no shutdown	Enables the current interface
5	Exit configuration mode for the interface by using the exit command. Router(config-if)# exit	Displays the global configuration mode prompt: Router(config)#

Verifying Interface Configuration and Status

When you have completed the router interface configuration, you can verify the configuration by using various **show** commands. This topic describes the **show** commands and the output that you see to verify the configuration.

Router show ip interface brief Command

```
RouterX#show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down
down
GigabitEthernet0/0      10.1.1.1        YES manual up
GigabitEthernet0/1      209.165.200.226 YES manual up
GigabitEthernet0/2      unassigned      YES NVRAM  administratively down
down
Serial0/0/0              172.18.0.1      YES manual up
Serial0/0/1              unassigned      YES manual administratively down
down
```

- Verifies the status of all interfaces

© 2013 Cisco Systems, Inc.

Router show ip interface brief Command (Cont.)

```
Branch#show ip route
<output omitted>
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/24 is directly connected, GigabitEthernet0/0
L    10.1.1.1/32 is directly connected, GigabitEthernet0/0
 172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.18.0.0/16 is directly connected, Serial0/0/0
L    172.18.0.1/32 is directly connected, Serial0/0/0
 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.226/31 is directly connected, GigabitEthernet0/1
L    209.165.200.226/32 is directly connected, GigabitEthernet0/1
```

- Enabled interfaces populate the routing table

© 2013 Cisco Systems, Inc.

To display a brief summary of the IP information and status of an interface, use the **show ip interface brief** command in privileged EXEC mode. The output fields and their meanings are shown in the table.

Output Field	Description
Interface	Type of interface
IP-Address	IP address assigned to the interface
OK?	"Yes" means that the IP address is valid, "No" means that the IP address is not valid
Method	Describes how the IP address was obtained or configured
Status	Shows the status of the interface
Protocol	Shows the operational status of the routing protocol on this interface

For more details about the **show ip interface brief** command, refer to the Cisco IOS Interface and Hardware Component Command Reference at <http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s5.html>

Router show interfaces Command

```
RouterX#show interfaces
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is f866.f231.7250 (bia
f866.f231.7250)
  Description: Link to LAN
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:53, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
<output omitted>
```

- Verifies the statistics for all interfaces that are configured on the router

© 2013 Cisco Systems, Inc.

The **show interfaces** command displays the status and statistics of all of the network interfaces on the router. The status for a specific interface can be displayed by using the **show interfaces type module/slot/port** command. Some of the output fields for a Gigabit Ethernet interface and their meanings are shown in the table.

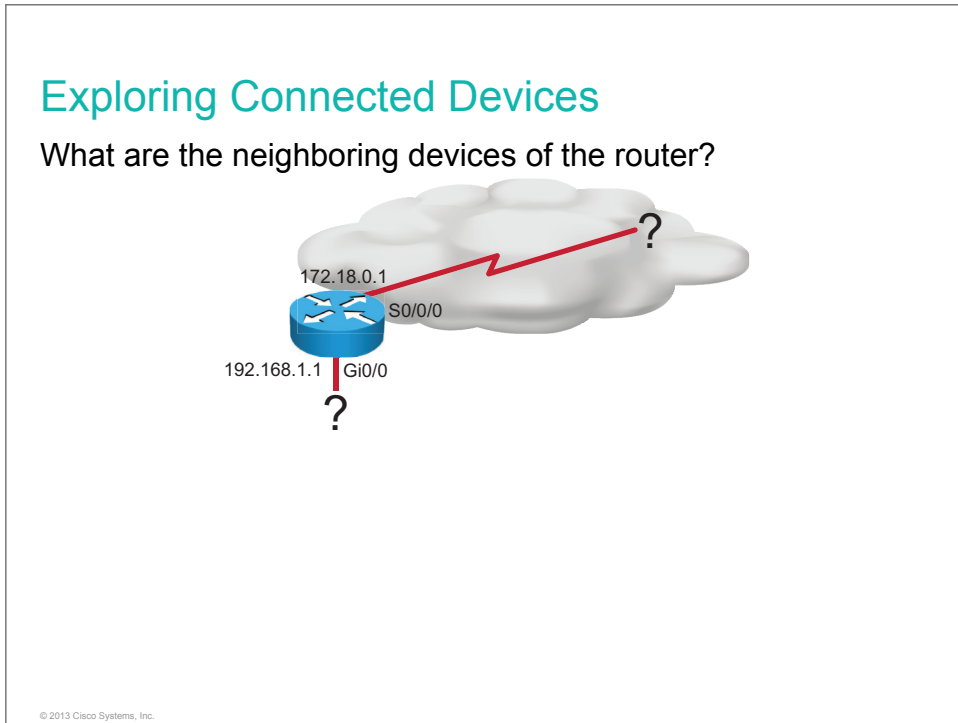
Output	Description
GigabitEthernet...is {up down administratively down}	Indicates whether the interface hardware is currently active, down, or has been taken down by an administrator.
line protocol is {up down}	Indicates whether the software processes that manage the line protocol consider the interface usable (that is, whether keepalives are successful). If the interface misses three consecutive keepalives, the line protocol is marked as down.
hardware	Hardware type and MAC address.

Output	Description
description	Displays the configured interface description.
Internet address	IP address followed by the prefix length (subnet mask).
MTU	MTU of the interface.
BW	Bandwidth of the interface, in kilobits per second. The bandwidth parameter is used to compute routing protocol metrics and other calculations.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
encapsulation	Encapsulation method that is assigned to an interface.
5 minute input rate, 5 minute output rate	Average number of bits and packets that were transmitted per second in the last 5 minutes.

For more details about the **show interfaces** command, refer to Cisco IOS Interface and Hardware Component Command Reference at <http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/irs4.html>

Exploring Connected Devices

Most network devices, by definition, do not work in isolation. A Cisco device frequently has other Cisco devices as neighbors on the network. Being able to obtain information about those other devices is important to assist with network design decisions, troubleshooting, and completing equipment changes. This topic describes why network discovery is needed and describes a tool that can be used for discovery.



If no documentation about the network topology is available or if the existing documentation is not up to date, you may need to discover the neighboring devices of a router. You can sometimes do this manually by inspecting the physical wiring, if the devices are installed next to each other. When neighboring devices are in other buildings or cities, you must use a different method.

One possibility is to use a dynamic discovery protocol that gathers information about directly connected devices.

Cisco devices support Cisco Discovery Protocol, which provides information about directly connected Cisco devices and their functions and capabilities.

Cisco Discovery Protocol

Cisco Discovery Protocol is a powerful network monitoring and troubleshooting tool. It is also an information-gathering tool that is used by network administrators to obtain information about directly connected Cisco devices. This topic describes the function of Cisco Discovery Protocol.

Cisco Discovery Protocol

- A proprietary utility that gathers information about directly connected Cisco switches, routers, and other Cisco devices
- Discovers neighboring devices, regardless of which protocol suite they are running
- LLDP—an alternative standards-based discovery protocol

Upper-layer entry addresses	IPv4, IPv6, and others
Cisco Discovery Protocol	Discovers and displays information about directly connected Cisco devices
Media	LAN, Frame Relay, ATM, others

© 2013 Cisco Systems, Inc.

Cisco Discovery Protocol is a proprietary tool that enables you to access a summary of protocol and address information about Cisco devices that are directly connected. By default, each Cisco device sends periodic messages, known as Cisco Discovery Protocol advertisements, to other directly connected Cisco devices. These advertisements contain information such as the types of devices that are connected, the router interfaces to which they are connected, the interfaces that are used to make the connections, and the model numbers of the devices.

Information that is gathered from other devices can assist you in making network design decisions, troubleshooting, and making changes to equipment. Cisco Discovery Protocol can be used as a network discovery tool, helping you to build a logical topology of a network when such documentation is missing or lacking in detail.

Cisco Discovery Protocol runs over the OSI data link layer, connecting the physical media to the upper-layer protocols. Because Cisco Discovery Protocol operates at the data link layer, two or more Cisco network devices can learn about each other even if they are using different network layer protocols, if they are not configured, or if IP addressing, for example, is misconfigured on neighboring routers.

LLDP is a standardized vendor-independent discovery protocol that discovers neighboring devices from different vendors. It is standardized by IEEE as the 802.1AB standard and it performs functions similar to Cisco Discovery Protocol.

More information about LLDP and a comparison with Cisco Discovery Protocol can be found at http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html.

Discovering Neighbors Using Cisco Discovery Protocol

The Cisco Discovery Protocol verification commands display information about neighboring devices. This topic describes the information that is provided by the **show cdp neighbors** command.

Discovering Neighbors Using Cisco Discovery Protocol

```
Branch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce   Holdtme    Capability   Platform         Port ID
HQ                Ser 0/0/0       123        R S I        CISCO2901        Ser 0/0/1
SW1               Gig 0/0         124        S I          WS-C2960-        Fas 0/13
```

- Displays information about neighboring devices discovered with Cisco Discovery Protocol

© 2013 Cisco Systems, Inc.

The figure shows the output from the **show cdp neighbors** command for router Branch. For each Cisco Discovery Protocol neighbor, this information is displayed:

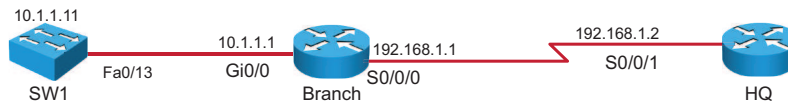
- Neighbor device ID
- Local interface
- Hold time value, in seconds
- Neighbor device capability code
- Neighbor hardware platform
- Neighbor remote port ID

Note The command output in the figure clearly shows OSI Layer 2 and OSI Layer 3 neighbors, a switch and router, respectively.

The format of the **show cdp neighbors** output varies among different types of devices, but the available information is generally consistent across devices.

The **show cdp neighbors** command can be also used on a Cisco Catalyst switch to display the Cisco Discovery Protocol updates that were received on the local interfaces. Note that on a switch, the local interface is referred to as the *local port*.

Using the show cdp neighbors detail Command



```
Branch#show cdp neighbors detail
-----
Device ID: HQ
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco CISCO2901/K9, Capabilities: Router Switch IGMP
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 132 sec
Version: Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M),
Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 20-Mar-12 18:57 by prod_rel_team
<output omitted>
```

- Displays detailed information about neighboring devices

© 2013 Cisco Systems, Inc.

The **show cdp neighbors detail** or **show cdp entry *** command displays detailed information about neighboring devices. To display information about a specific neighbor, the command string must include the IP address or device ID of the neighbor. The **show cdp entry** command shows the following information:

- Neighbor device ID (router HQ in the figure)
- OSI Layer 3 protocol information (for example, IP address 192.168.1.2 in the figure)
- Device platform (Cisco 2901 in the figure)
- Device capabilities (router, switch, IGMP in the figure)
- Local interface type and outgoing remote port ID (Serial 0/0/0 in the figure)
- Hold time value, in seconds (132 seconds in the figure)
- Cisco IOS Software type and release (C2900 Software [C2900-UNIVERSALK9-M], Version 15.2[4]M1, in the figure)

For more details about **show cdp** commands, refer to the Cisco IOS Network Management Command Reference at http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_12.html#wp1115418

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The router startup sequence begins with POST, then the Cisco IOS image is found and loaded. Finally, the configuration file is loaded, if it exists.
- If a router starts without a configuration, the Cisco IOS Software executes a question-driven configuration dialog, which can be skipped.
- The main function of a router is to relay packets from one network device to another.
- Interface characteristics, such as the IP address and description, are configured using interface configuration mode.
- When you have completed router interface configuration, you can verify it by using the **show ip interface brief** and **show interfaces** commands

© 2013 Cisco Systems, Inc.

Summary (Cont.)

- Cisco Discovery Protocol is an information-gathering tool used by network administrators to obtain information about directly connected devices.
- Cisco Discovery Protocol exchanges hardware and software device information with its directly connected Cisco Discovery Protocol neighbors.
- The **show cdp neighbors** command displays information about the Cisco Discovery Protocol neighbors of a router.
- The **show cdp neighbors detail** command displays detailed Cisco Discovery Protocol information on a Cisco device.

© 2013 Cisco Systems, Inc.

Exploring the Packet Delivery Process

Overview

Understanding the packet delivery process is a fundamental part of understanding networking devices. You must understand host-to-host communications to administer a network. This lesson describes host-to-host communications through a router by providing a graphic representation. The beginning of the lesson illustrates the role of Layer 2 and Layer 3 addresses in packet delivery. The role of ARP follows. The lesson ends with a step-by-step analysis of the packet delivery process that shows all the mechanisms in a network scenario.

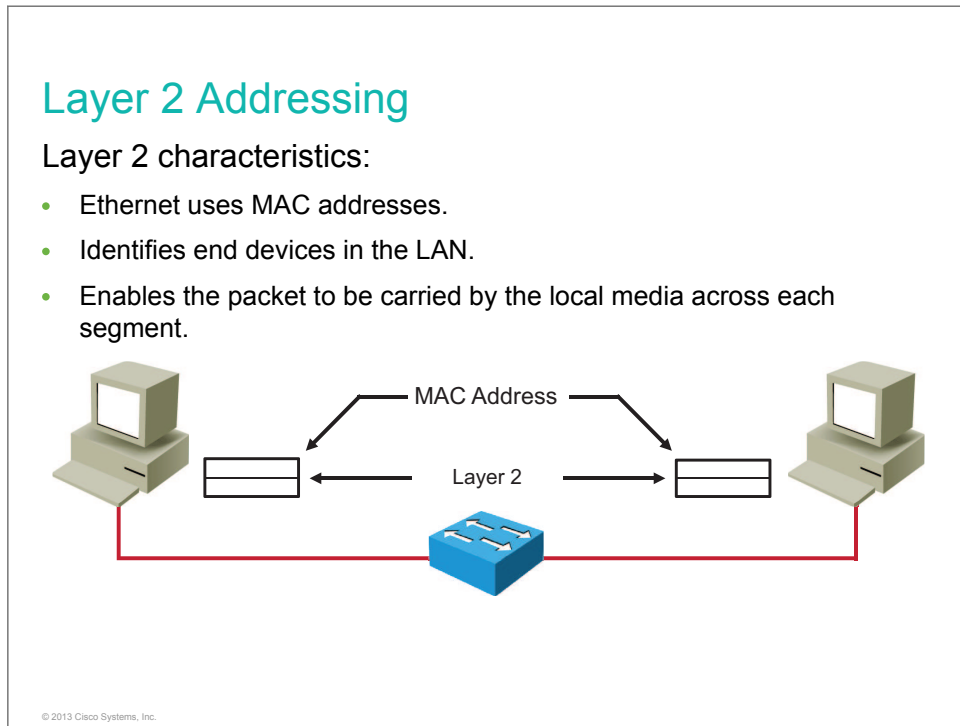
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe Layer 2 addressing
- Describe Layer 3 addressing
- Explain the role of ARP
- Describe the host-to-host packet delivery
- Describe the host-to-host packet delivery process through a switch

Layer 2 Addressing

This topic describes where the Layer 2 address fits into the host-to-host packet delivery process.



Layer 2 defines how data is formatted for transmission and how access to the physical media is controlled. Layer 2 devices provide an interface with the physical media. Some common examples are an NIC installed in a host or switch.

Host-to-host communications require Layer 2 addresses. MAC addresses are assigned to end devices such as hosts.

The OSI data link layer (Layer 2) physical addressing that is implemented as an Ethernet MAC address is used to transport the frame across the local media. Although unique host addresses are provided, physical addresses are not hierarchical. They are associated with a particular device, regardless of its location or to which network it is connected. These Layer 2 addresses have no meaning outside the local network media.

An Ethernet MAC address is a two-part, 48-bit binary value that is expressed as 12 hexadecimal digits. The address formats might appear like 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, or 0005.9A3C.7800.

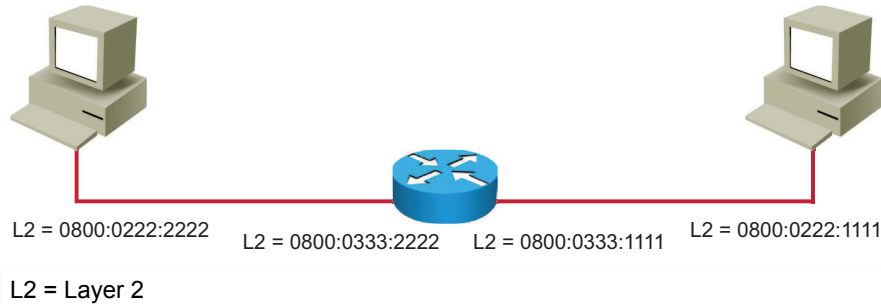
All devices that are connected to an Ethernet LAN have MAC-addressed interfaces. The NIC uses the MAC address to determine if a message should be passed to the upper layers for processing. The MAC address is permanently encoded into a ROM chip on an NIC. The MAC address is made up of the OUI and the vendor assignment number.

Switches do not need assigned MAC addresses for frame forwarding. However, they need a MAC address when remote access management is configured.

Layer 2 Addressing (Cont.)

Layer 2 addressing:

- The router has two interfaces directly connected to two PCs.
- Each PC and each router interface has its own unique MAC address.



The figure describes Layer 2 addressing in the host-to-host communications model. MAC addresses are assigned to end devices such as hosts. The physical interfaces on a router provide a Layer 2 function and are also assigned a MAC address.

As seen in the example, the router has two interfaces directly connected to two PCs. Each PC and each router interface has its own unique MAC address.

Layer 3 Addressing

This topic describes where Layer 3 devices and addressing fit into the host-to-host communications model.

Layer 3 Addressing

Layer 3 devices and functions:

- The network layer provides connectivity and path selection between two host systems.
- In the host, this is the path between the data link layer and the upper layers.
- In the router, it is the actual path across the network.

© 2013 Cisco Systems, Inc.

The network layer provides connectivity and path selection between two host systems that may be located on geographically separated networks. At the boundary of each local network, an intermediary network device, usually a router, de-encapsulates the frame to read the destination address that is contained in the header of the packet (the Layer 3 PDU). Routers use the network identifier portion of this address to determine which path to use to reach the destination host. Once the path is determined, the router encapsulates the packet in a new frame and sends it toward the destination end device.

Layer 3 Addressing (Cont.)

Layer 3 addressing:

- Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks.
- TCP/IP protocol stack uses IP.

© 2013 Cisco Systems, Inc.

Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks. In the TCP/IP protocol suite, every IP host address contains information about the network where the host is located.

Intermediary devices that connect networks are called *routers*. The role of the router is to select paths for and direct packets toward a destination. This process is known as *routing*. A router uses a list of paths that is called a *routing table* to determine where to send data.

Layer 3 Addressing (Cont.)

- Layer 3 addresses are assigned to hosts and network devices that provide Layer 3 functions.
- Network devices maintain a routing table.

Routing Table

192.168.3.0/24	Interface Gi0/0
192.168.4.0/24	Interface Gi0/1

L3 = 192.168.3.1 L3 = 192.168.3.2 L3 = 192.168.4.1 L3 = 192.168.4.2

L3 = Layer 3

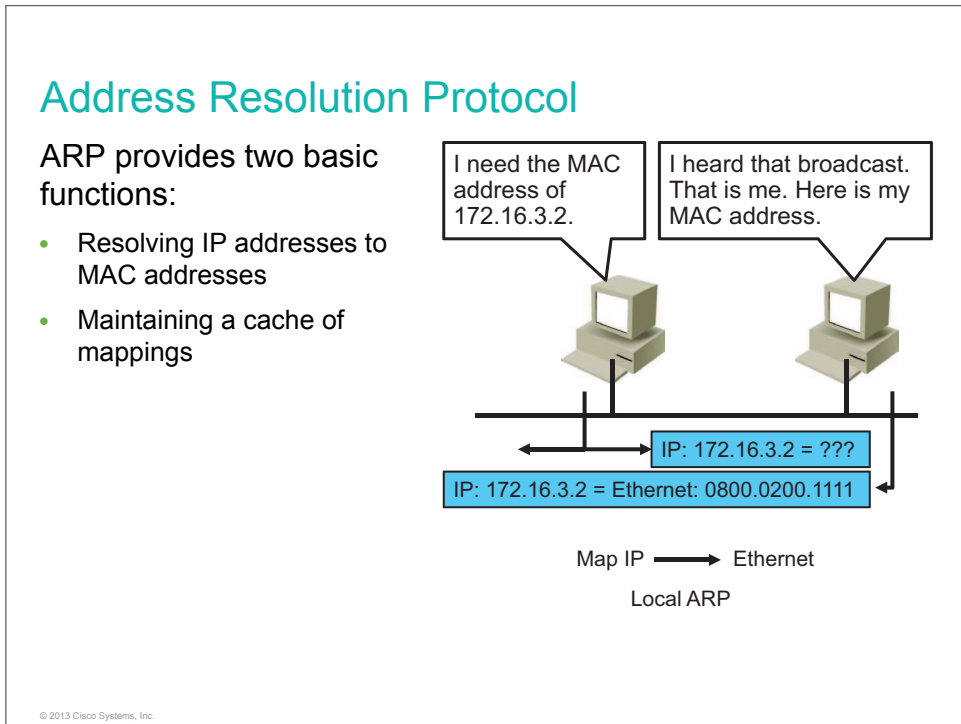
© 2013 Cisco Systems, Inc.

Layer 3 addresses are assigned to end devices such as hosts and to network devices that provide Layer 3 functions. The router has its own Layer 3 address on each interface. Each network device that provides a Layer 3 function maintains a routing table.

As seen in the example, the two router interfaces belong to different networks. The left interface and the directly connected PC belong to the 192.168.3.0/24 network, while the right interface and the directly connected PC belong to the 192.168.4.0/24 network. For devices in different IP networks, a Layer 3 device is needed to route traffic.

Address Resolution Protocol

For IP communication on Ethernet-connected networks, the logical (IP) address must be bound to the physical (MAC) address of its destination. This process is performed by ARP, which is described in this topic.



To send data to a destination, a host on an Ethernet network must know the physical (MAC) address of the destination. ARP provides the essential service of mapping IP addresses to physical addresses on a network.

The term *address resolution* refers to the process of binding the network layer IP address of a remote device to its locally reachable, data link layer MAC address. The address is considered to be resolved when ARP broadcasts the known information—the target destination IP address and its own IP address. All of the devices on the Ethernet segment receive the broadcast. When the target recognizes itself by reading the contents of the ARP request packet, it responds with the required MAC address in its ARP reply. The address resolution procedure is completed when the originator receives the reply packet, which contains the required MAC address, from the target and updates the table containing all of the current bindings. This table is usually called the *ARP table* or *ARP cache*. The ARP table is used to maintain a correlation between each IP address and its corresponding MAC address.

Address Resolution Protocol (Cont.)

The ARP table keeps a record of recent bindings of IP addresses to MAC addresses.

On the PC:

```
C:\Windows\system32>arp -a
Interface: 192.168.250.11 --- 0xb
Internet Address      Physical Address      Type
192.168.250.1        00-1b-0c-5d-91-0f    dynamic
192.168.250.12       00-0c-29-13-cc-bf    dynamic
```

On the router:

```
Branch#show ip arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 10.1.1.100   5          000c.2993.6a84 ARPA   GigabitEthernet0/0
Internet 10.1.1.101   4          000c.2913.ccc9 ARPA   GigabitEthernet0/0
```

© 2013 Cisco Systems, Inc.

Each IP device on a network segment maintains a table in memory: the ARP table. This table maps the IP addresses of other devices on the network with their physical (MAC) addresses. When a host wants to transmit data to another host on the same network, it searches the ARP table to see if there is an entry. If there is an entry, the host uses it. If there is not, ARP is used to get an entry.

Each entry, or row, of the ARP table has a pair of values: an IP address and a MAC address. The relationship between the two values is a map, which simply means that you can locate an IP address in the table and discover the corresponding MAC address. The ARP table caches the mapping for the devices on the local LAN.

The ARP table is created and maintained dynamically. It adds and changes address relationships as they are used on the local host. The entries in an ARP table on a PC usually expire after 300 seconds, which is the default value. It takes up to four hours by default on routers. Such timeout ensures that the table does not contain information for systems that may be switched off or that have been moved. When the local host wants to transmit data again, the entry in the ARP table is regenerated through the ARP process.

If no device responds to the ARP request, the packet is dropped because a frame cannot be created.

The **arp -a** command displays the current ARP table for all interfaces on a PC using the Microsoft Windows operating system.

To display the ARP table on the router, use the **show ip arp EXEC** command as follows:

```
show ip arp [ip-address] [host-name] [mac-address] [interface type number]
```

Syntax Description

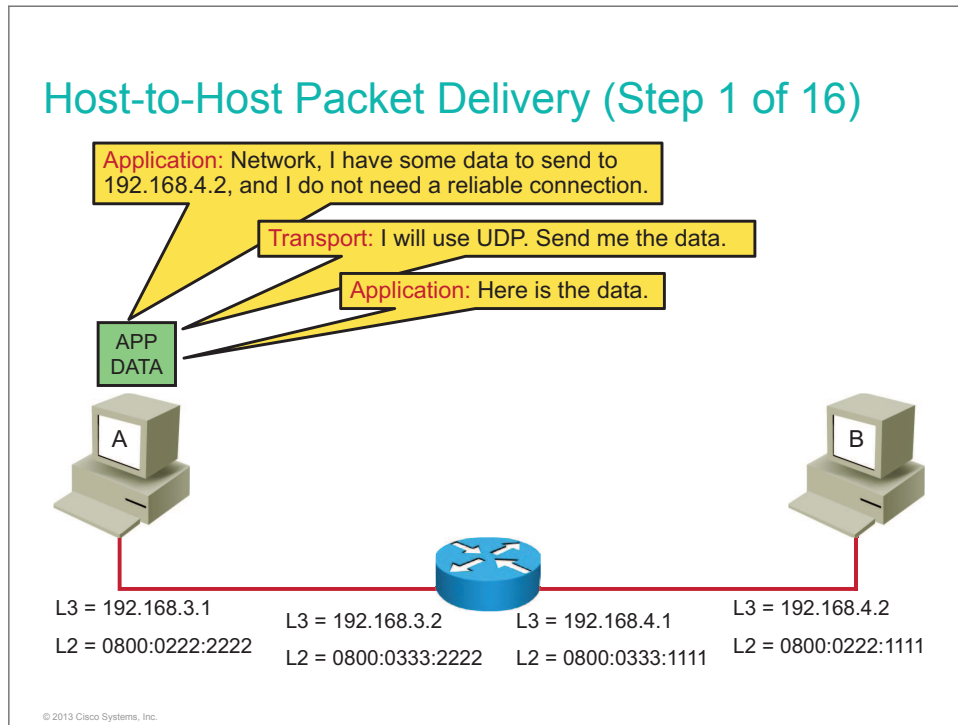
Parameter	Description
<i>ip-address</i>	(Optional) Displays ARP entries matching this IP address
<i>host-name</i>	(Optional) Hostname

Parameter	Description
<i>mac-address</i>	(Optional) 48-bit MAC address
<i>interface type number</i>	(Optional) Displays ARP entries that are learned via this interface type and number

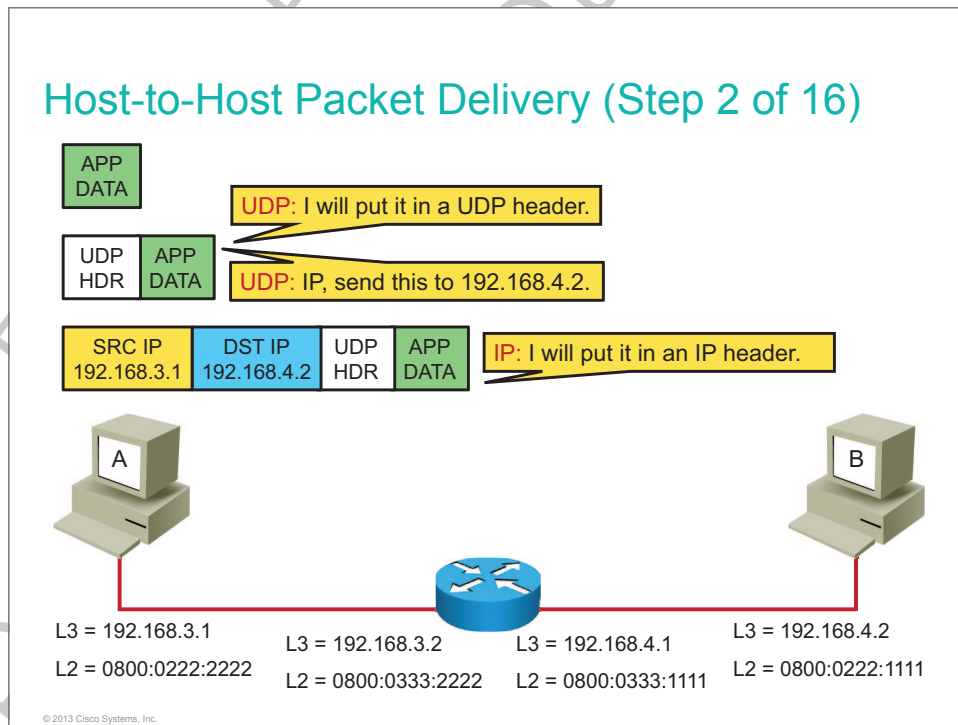
Do Not Duplicate.
Post beta, not for release.

Host-to-Host Packet Delivery

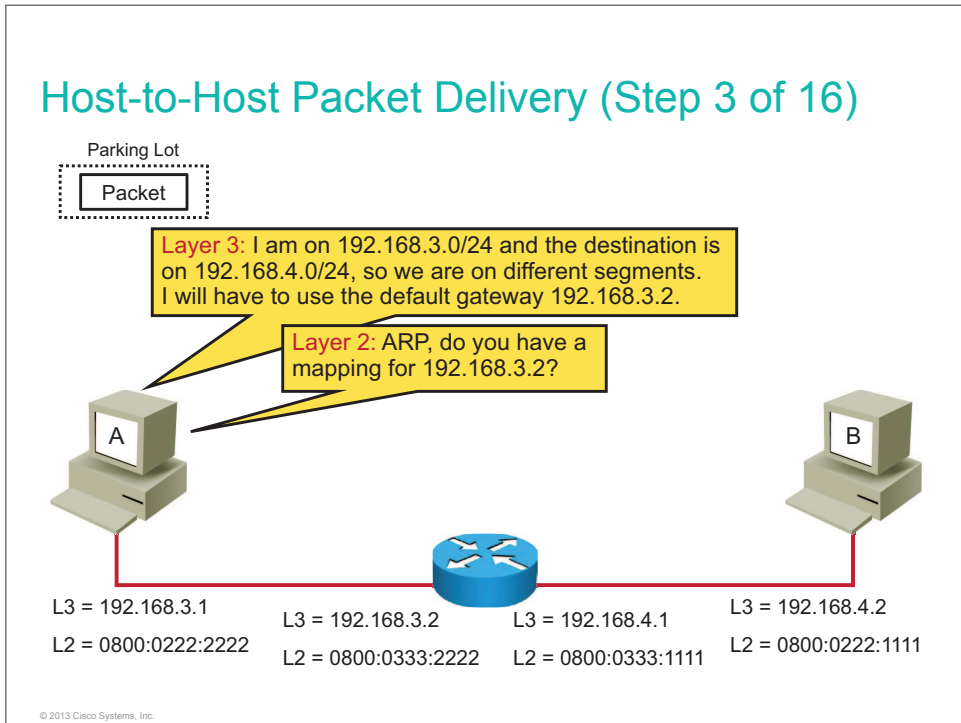
This topic describes the process of delivering an IP packet over a routed network.



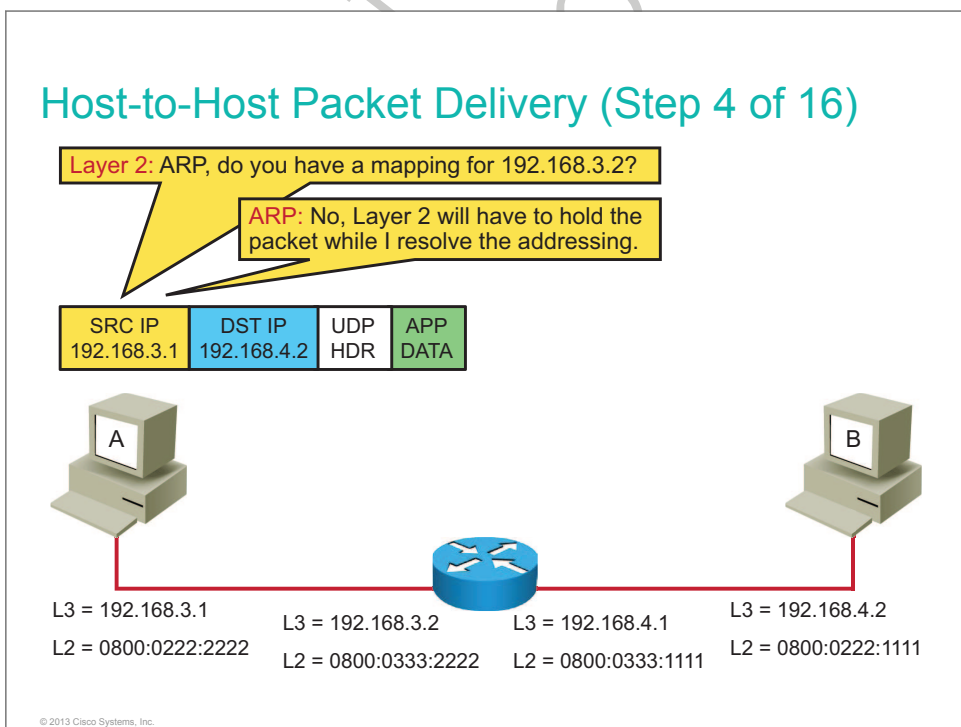
In this example, host 192.168.3.1 has data that it wants to send to host 192.168.4.2. The application does not need a reliable connection, therefore UDP is selected. Because it is not necessary to set up a session, the application can start sending data.



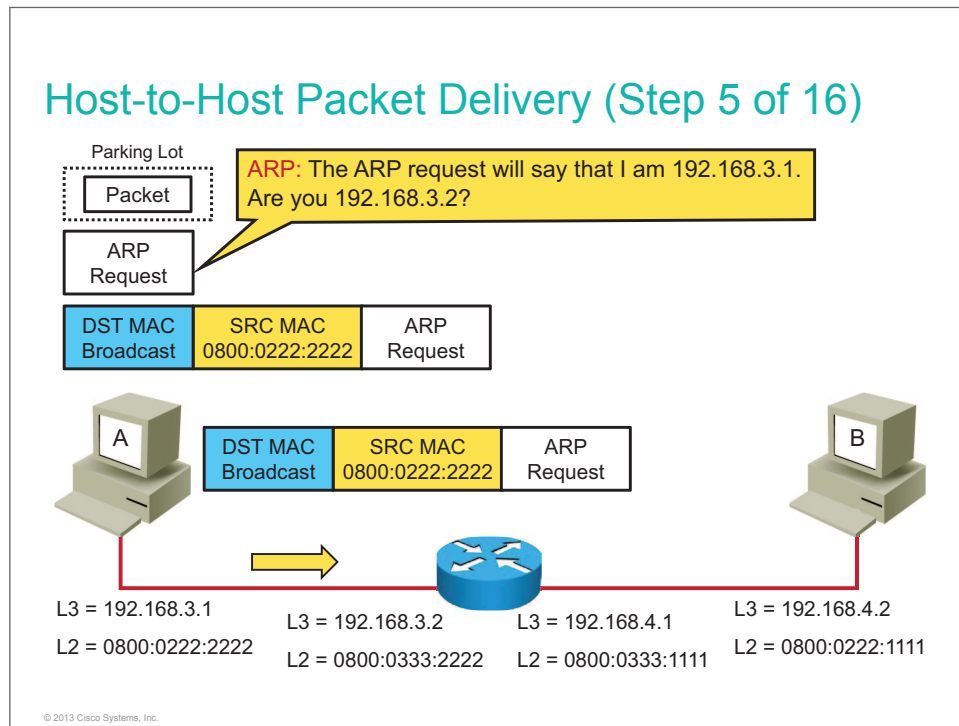
UDP prepends a UDP header (UDP HDR) and passes the PDU to IP (Layer 3) with an instruction to send the PDU to 192.168.4.2. IP encapsulates the PDU in a Layer 3 packet, setting the source IP address (SRC IP) of the packet to 192.168.3.1, while the destination IP address (DST IP) is set to 192.168.4.2.



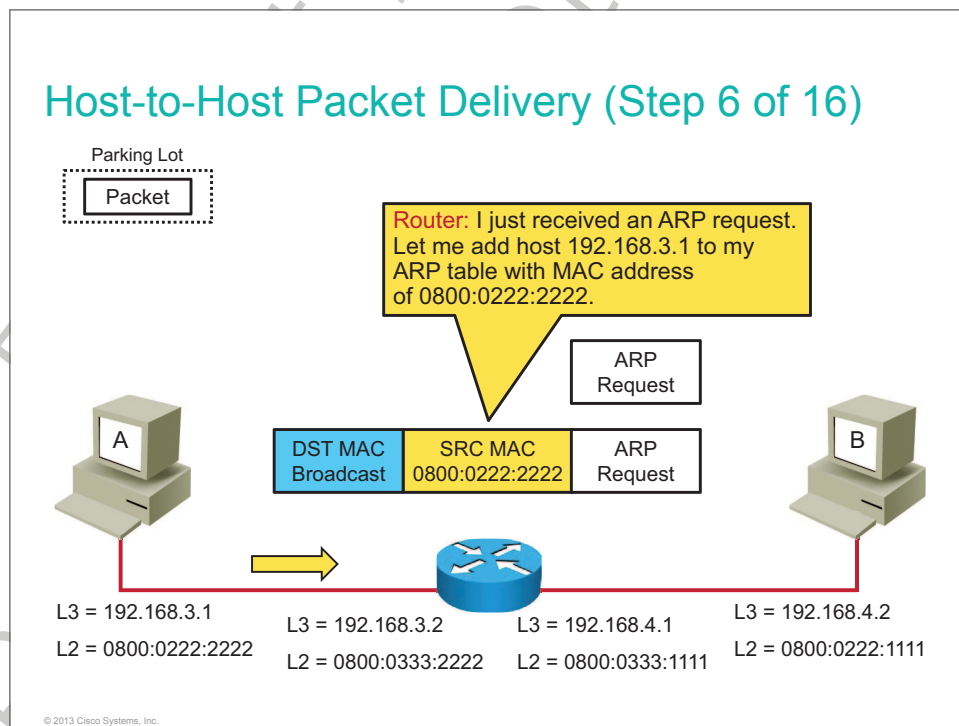
The host sends any packet that is not destined for the local IP network to the default gateway. The default gateway is the address of the local router, which must be configured on hosts (PCs, servers, and so on). IP encapsulates the PDU in a Layer 3 packet and passes it to Layer 2 with instructions to forward it to the default gateway.



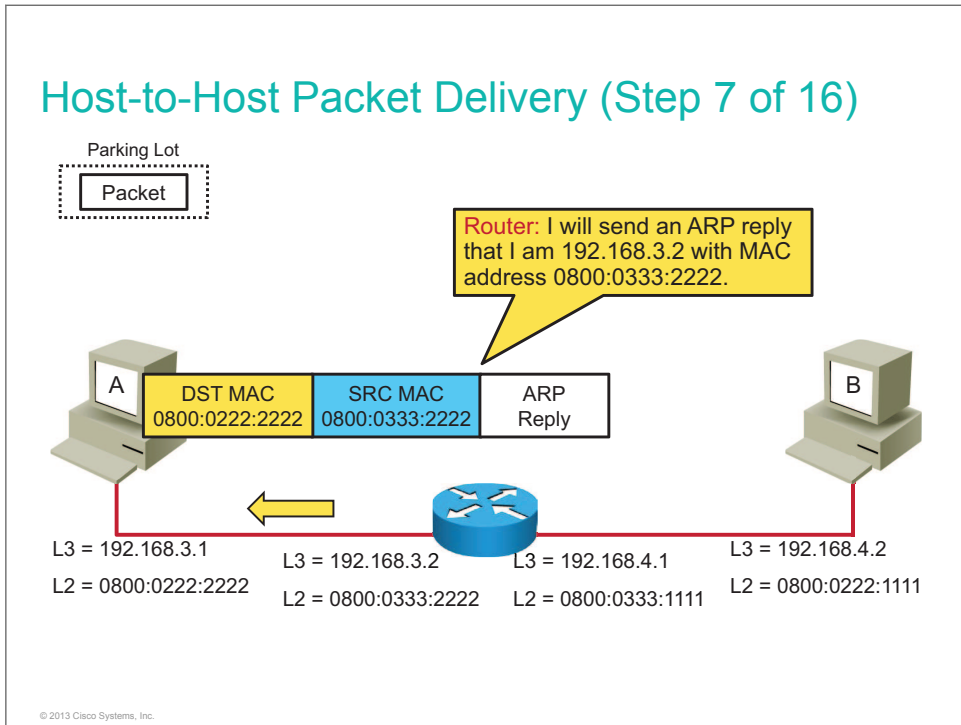
To deliver the packet, the host needs the Layer 2 information of the next-hop device. The ARP table in the host does not have an entry and must resolve the Layer 2 address (MAC address) of the default gateway. The default gateway is the next hop for the packet. The packet waits while the host resolves the Layer 2 information.



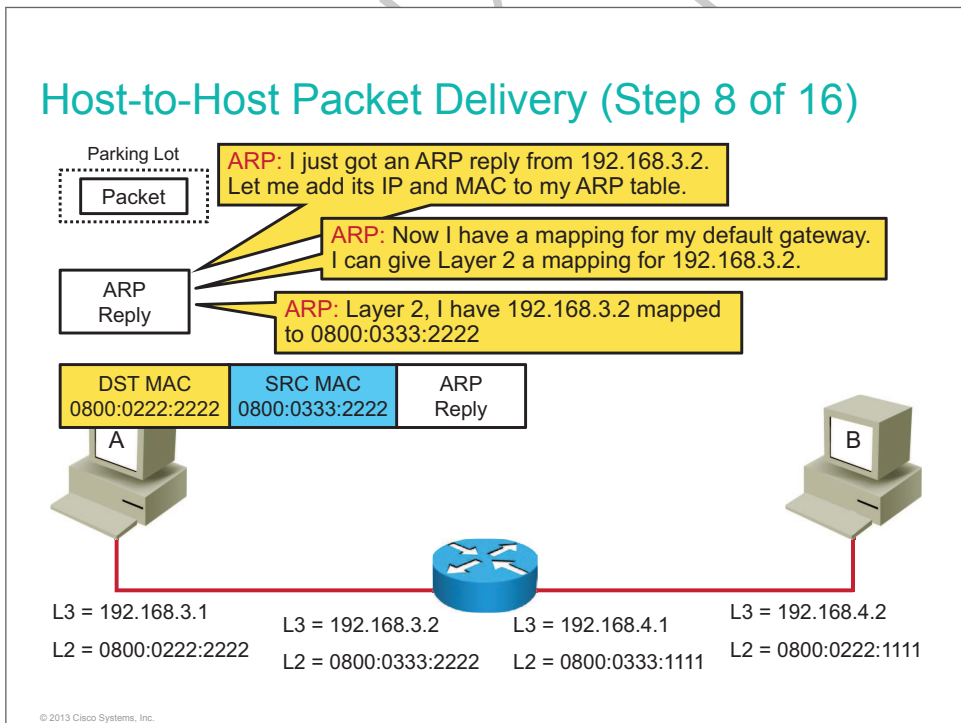
Since the host does not have a mapping of Layer 2 and Layer 3 addresses for the default gateway, the host uses the standard ARP process to obtain the mapping. The host sends an ARP request to the router.



The user has programmed the IP address of 192.168.3.2 as the default gateway. Host 192.168.3.1 sends out the ARP request, and the router receives it. The ARP request contains information about the host, and the router adds the information in its ARP table.

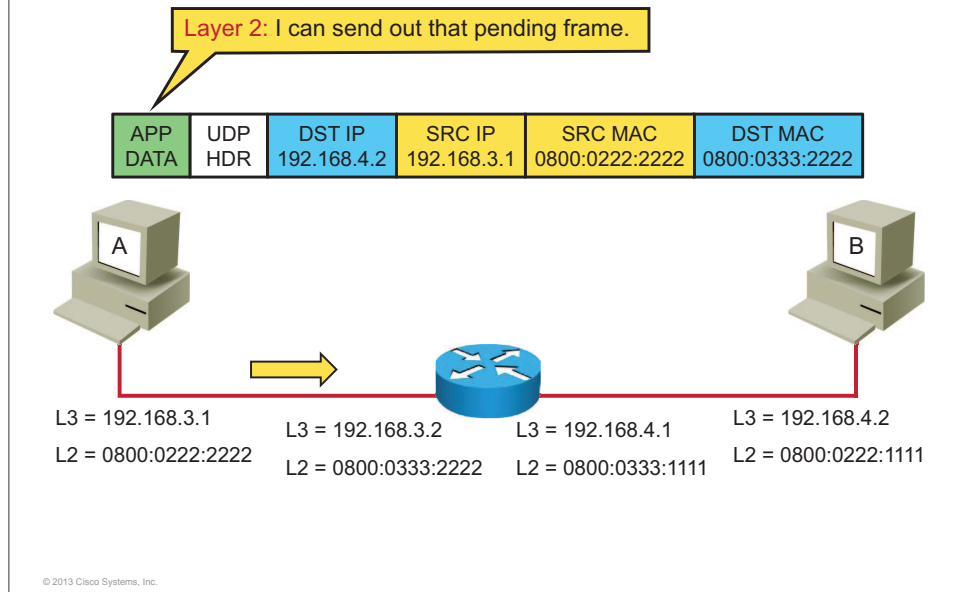


The router processes the ARP request like any other host and sends the ARP reply with its own information.



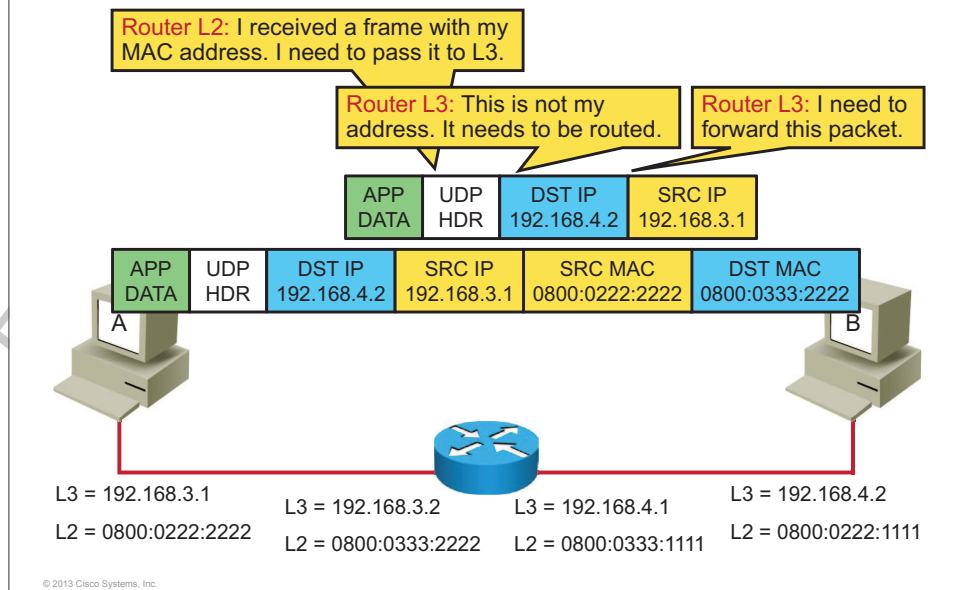
The host receives an ARP reply to the ARP request and enters the information in its local ARP table.

Host-to-Host Packet Delivery (Step 9 of 16)



Now the Layer 2 frame with the application data can be sent to the default gateway. The pending frame is sent with the local host IP address and MAC address as the source. However, the destination IP address is that of the remote host, but the destination MAC address is that of the default gateway.

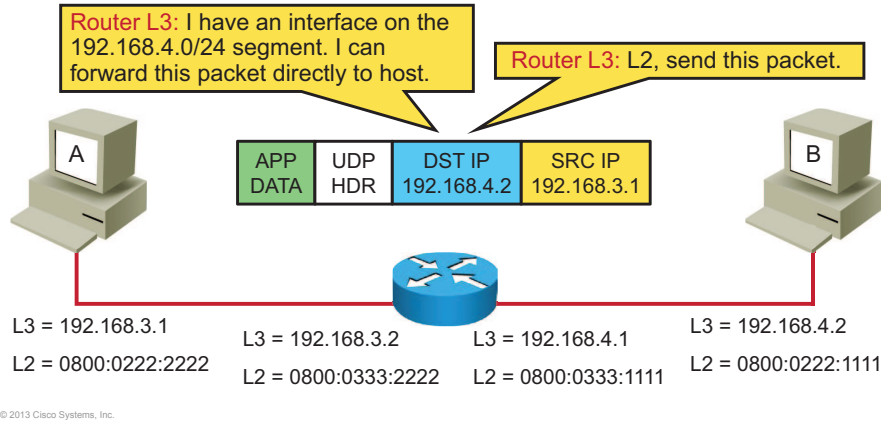
Host-to-Host Packet Delivery (Step 10 of 16)



When the frame is received by the router, the router recognizes its MAC address and processes the frame. At Layer 3, the router sees that the destination IP address is not its address. A host Layer 3 device would discard the frame. However, because this device is a router, it passes all packets that are for unknown destinations to the routing process. The routing process determines where to send the packet.

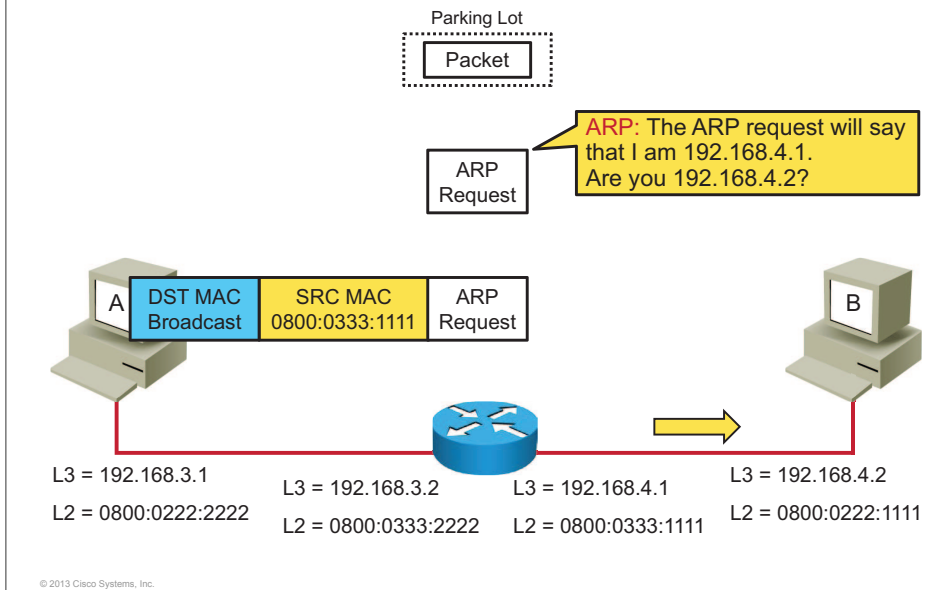
Host-to-Host Packet Delivery (Step 11 of 16)

Destination	Next Hop	Interface
192.168.3.0/24	Connected	Gi 0/0
192.168.4.0/24	Connected	Gi 0/1



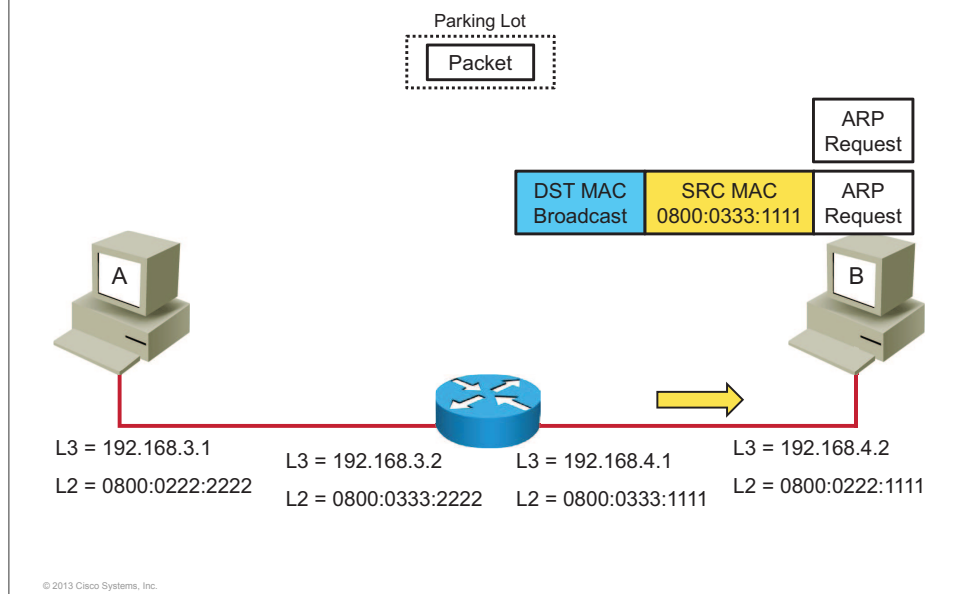
The routing process looks up the destination IP address in its routing table. In this example, the destination segment is directly connected. Therefore, the routing process can pass the packet directly to Layer 2 for the appropriate interface.

Host-to-Host Packet Delivery (Step 12 of 16)



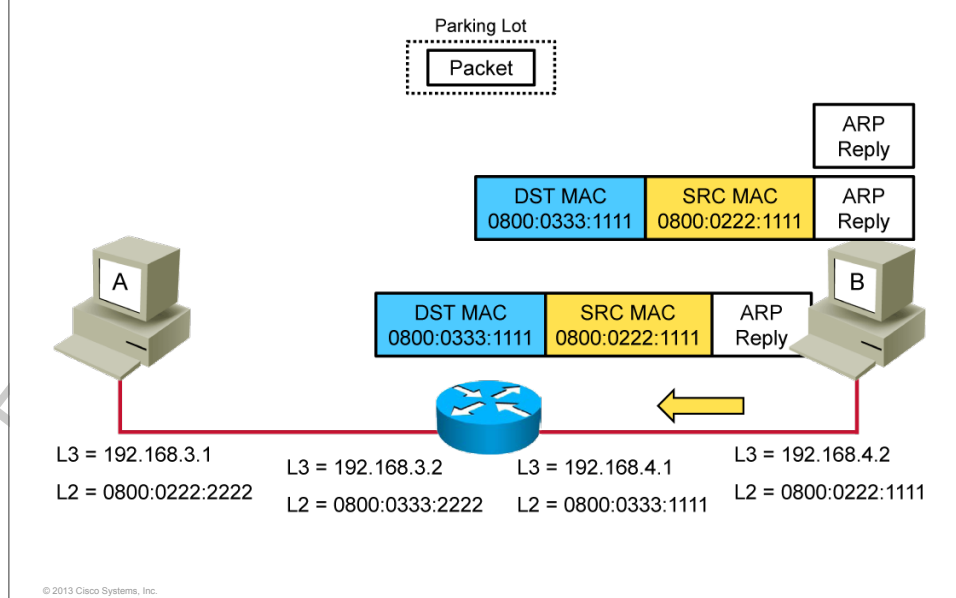
Layer 2 uses the ARP process to obtain the mapping for the IP address and the MAC address. The router asks for the Layer 2 information in the same way as the hosts. An ARP request for the destination Layer 3 address is sent to the link.

Host-to-Host Packet Delivery (Step 13 of 16)



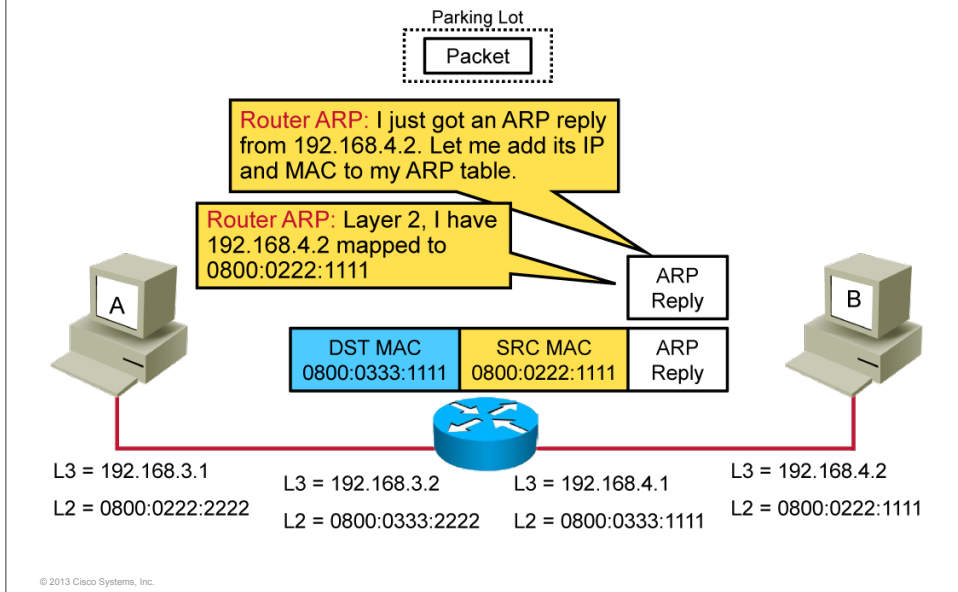
The destination receives and processes the ARP request.

Host-to-Host Packet Delivery (Step 14 of 16)



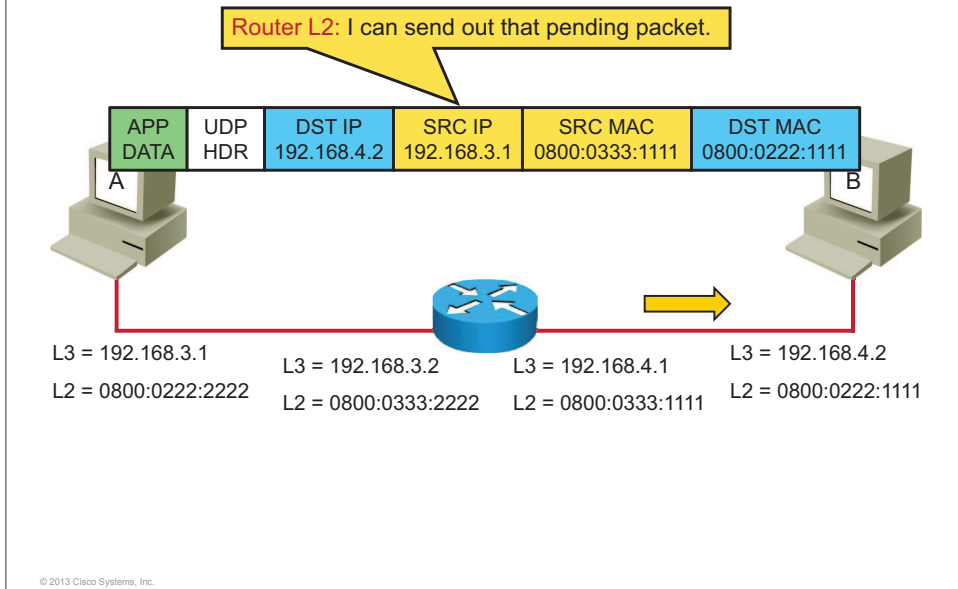
The host receives the frame that contains the ARP request and passes the request to the ARP process. The ARP process takes the information about the router from the ARP request and places the information in its local ARP table. The ARP process generates the ARP reply and sends it back to the router.

Host-to-Host Packet Delivery (Step 15 of 16)



The router receives the ARP reply and takes the information that is required for forwarding the packet to the next hop. The router populates its local ARP table and starts the packet-forwarding process.

Host-to-Host Packet Delivery (Step 16 of 16)



The frame is forwarded to the destination. Note that the router changed the Layer 2 address as needed, but it will not change the Layer 3 address.

Note The router changes source and destination MAC addresses, while source and destination IP addresses remain the same.

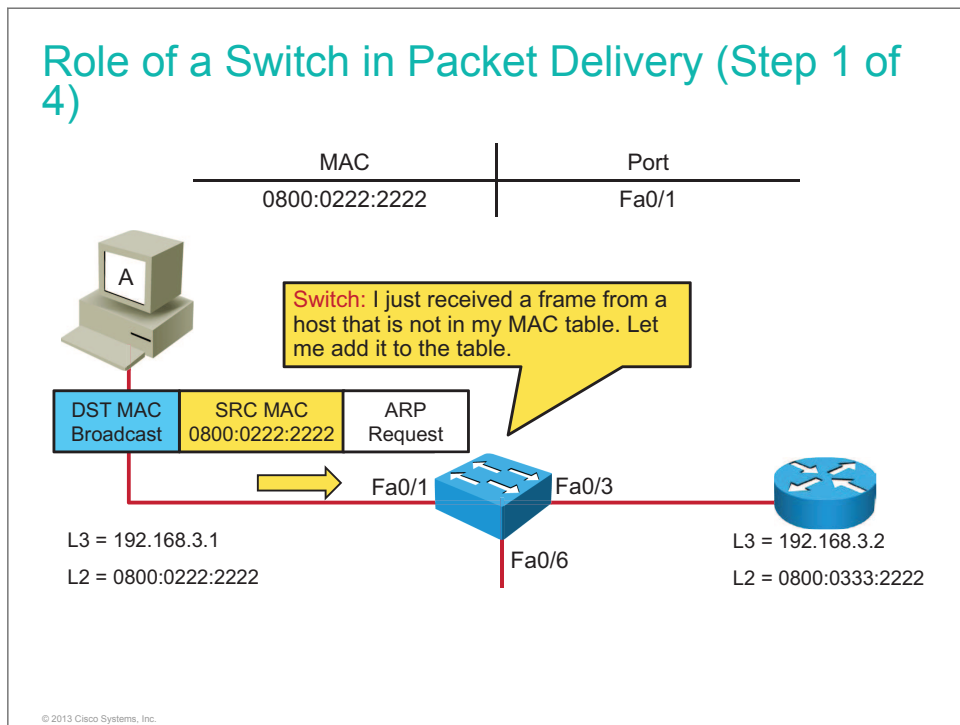
Note

Remember that a switch does not change the frame in any way. When the switch receives the frame, it needs to forward it out the proper port according to the MAC address table.

Do Not Duplicate.
Post beta, not for release.

Role of a Switch in Packet Delivery

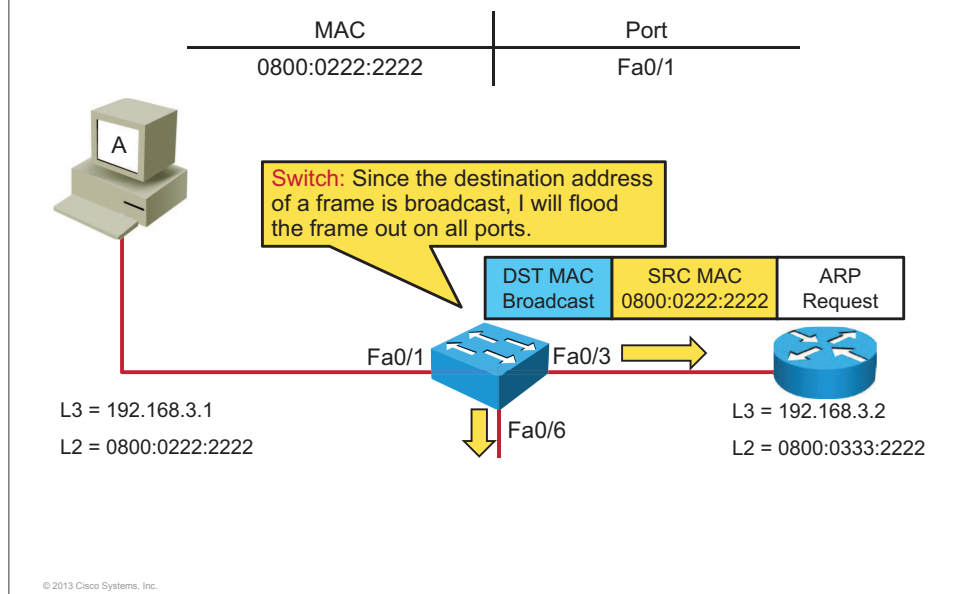
This topic describes host-to-host communication when data passes through a switch.



This example focuses on the role of a switch in the host-to-host packet delivery process. An application on host PC A wishes to send data to a distant network. Before an IP packet can be forwarded to the default gateway, its MAC address needs to be obtained. ARP protocol on PC A creates an ARP request and sends it out. Before the ARP request reaches other devices on a network, the switch receives it.

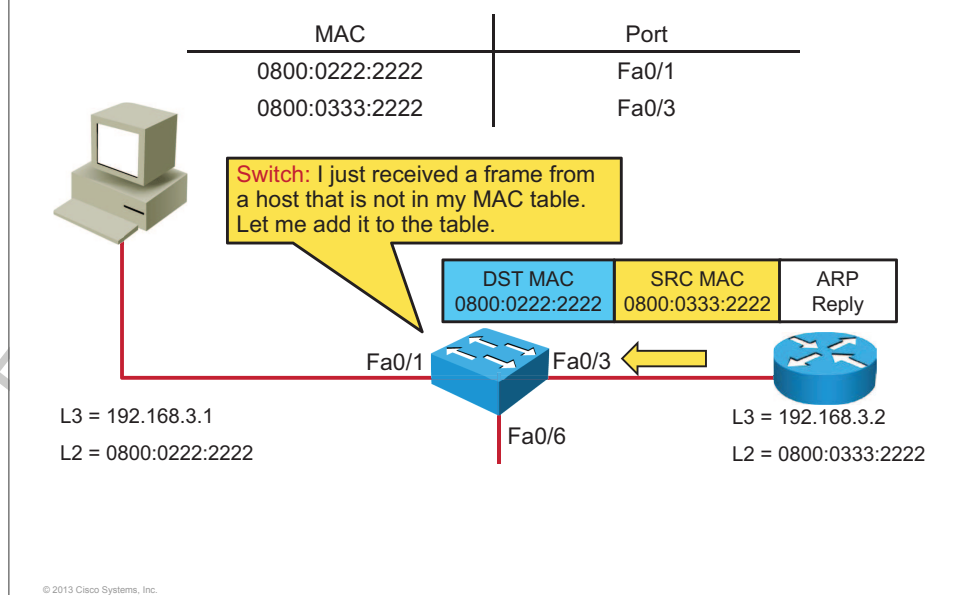
When the switch receives the frame, it needs to forward it out on the proper port. However, in this example, the source and the destination MAC addresses are not in the MAC address table of the switch. The switch can learn the port mapping for the source host from the source MAC address in the frame, so the switch will add it to the table (0800:0222:2222 = port Fa0/1).

Role of a Switch in Packet Delivery (Step 2 of 4)



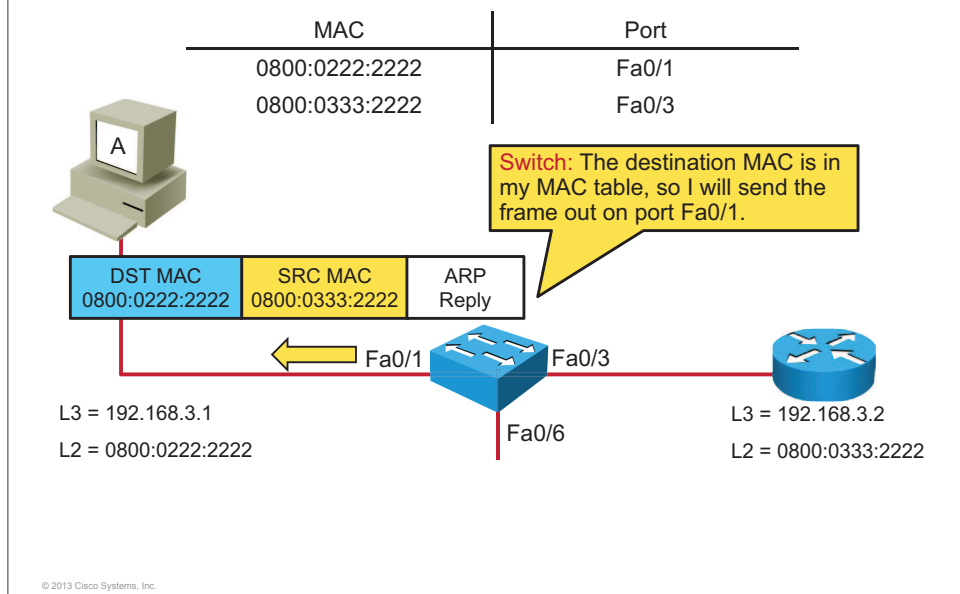
Because the destination address of the frame is a broadcast, the switch has to flood the packet out to all of the ports. The only exception is the port on which the switch received the broadcast frame.

Role of a Switch in Packet Delivery (Step 3 of 4)



The router replies to the ARP request and sends an ARP reply packet back to the sender as a unicast frame. The switch learns the port mapping for the new source host from the source MAC address in the frame. The switch adds it to the MAC address table (0800:0333:2222 = port Fa0/3).

Role of a Switch in Packet Delivery (Step 4 of 4)



The destination address of the frame is found in the MAC address table, therefore the switch can forward the frame out on port Fa0/1. In the case when the destination address is not found in the MAC address table, the switch would need to flood the frame out on all ports.

All frames pass through the switch unchanged. When the MAC address table is built, all unicast frames are sent directly to a destination host based on the destination MAC address and data stored in MAC address table.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- If hosts are not in the same network, the frame is sent to the default gateway.
- Frames sent to the default gateway have the local host source MAC address and the default gateway destination MAC address.
- A router changes the Layer 2 address as needed, but it does not change the Layer 3 address.
- The switch does not change the frame in any way, it just forwards the frame out on the proper port according to the MAC address table.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Enabling Static Routing

Overview

Routing is the process by which a packet moves from one location to another. In the terms of computer networks, it is the process of determining where to send data packets destined for addresses outside of the local network.

A router is a special-purpose computer that performs packet forwarding by learning about remote networks and maintaining routing information. The router is the junction or intersection that connects multiple IP networks. The primary forwarding decision of the router is based on OSI Layer 3 information, which is the destination IP address.

To effectively manage an IP network, you must understand how both static and dynamic routing operate and the impact that they have on IP networks. This lesson introduces static IP routing.

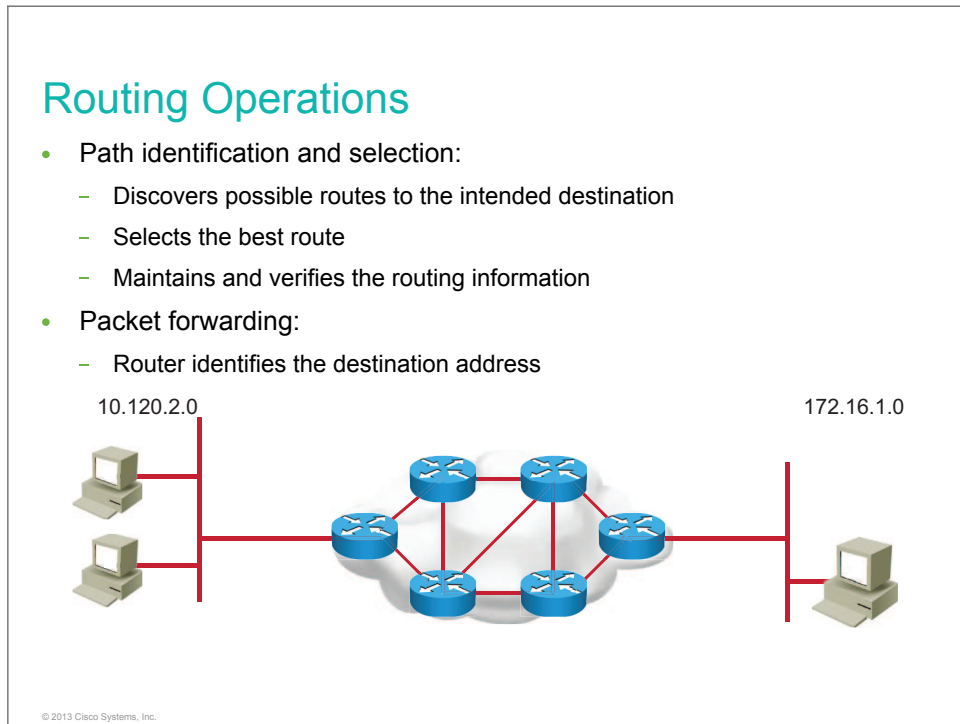
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the basic characteristics of routing operations
- Explain the differences between static and dynamic routing
- Explain when to use static routing
- Configure static routes
- Configure default routes
- Verify static route configuration

Routing Operations

This topic describes basic static and dynamic routing operations.



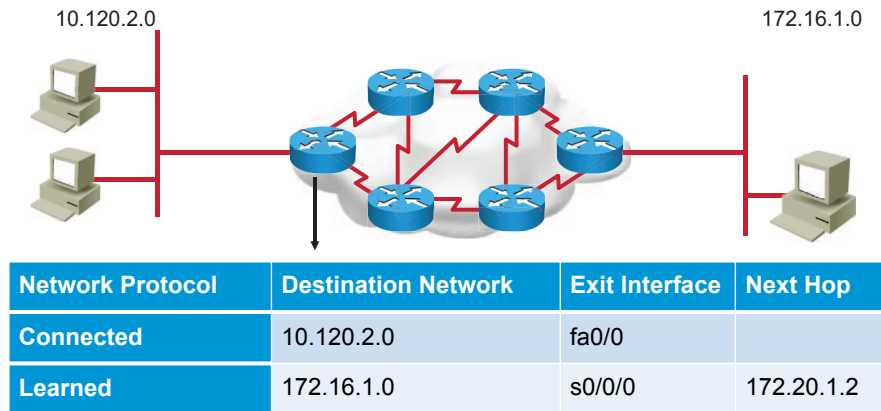
In networking, a router is the device that is used to route traffic. Routers forward packets by learning about remote networks and maintaining routing information. To forward packets correctly, a router needs some basic information about the network and the packet to be forwarded. The primary forwarding decision of the router is based on Layer 3 information, which is the destination IP address.

To be able to route something, a router or any entity that performs routing must perform these functions:

- Path identification and selection:
 - **Identify the sources of routing information:** Determine from which sources (other routers) that the router can learn the paths to the given destinations.
 - **Identify routes:** Determine the initial possible routes or paths to the intended destination.
 - **Select routes:** Select the best path to the intended destination.
 - **Maintain and verify routing information:** Determine whether the known paths to the destination are the most current.
- Packet forwarding:
 - **Identify the destination address:** Determine the destination (or address) of the packet that needs to be routed.

Routing Operations (Cont.)

- A router must learn about destinations that are not directly connected to it.
- The routing table is used to determine the best path to the destination.



© 2013 Cisco Systems, Inc.

A router receives routing information from other routers and places it in its routing table. The routing table is used to find the best match and path between the destination IP of a packet and a network address in the routing table. The routing table ultimately determines the outgoing interface for forwarding the packet, and the router encapsulates that packet in the appropriate data-link frame for that outgoing interface.

The routing table stores information about connected and remote networks. A connected network is directly attached to one of the router interfaces. These interfaces are the gateways for the hosts on various local networks. If the destination network is directly connected, the router already knows which interface to use when forwarding packets.

Static and Dynamic Routing Comparison

This topic describes the differences between static and dynamic routing.

Static and Dynamic Routing Comparison

Static routes:

- A network administrator manually enters static routes into the router.
- A network topology change requires a manual update to the route.
- Routing behavior can be precisely controlled.

Dynamic routes:

- A network routing protocol automatically adjusts dynamic routes when the topology or traffic changes.
- Routers learn and maintain routes to the remote destinations by exchanging routing updates.
- Routers discover new networks by sharing routing table information.

© 2013 Cisco Systems, Inc.

Based on the router configuration, routers can forward packets over static routes or dynamic routes. Remote networks are added to the routing table by an administrator either configuring static routes or enabling a dynamic routing protocol.

There are two ways to tell the router where to forward packets to the networks that are not directly connected:

- **Static routes:** Routes to remote networks with an associated next hop can be manually configured on the router. These routes are known as *static routes*. The administrator must manually update a static route entry whenever an internetwork topology change requires an update. Static routes are user-defined routes that specify the path that packets take between a source and a destination. These administrator-defined routes allow very precise control over the routing behavior of the IP internetwork.
- **Dynamic routes:** The router dynamically learns routes and adds them to the routing table after an administrator configures a routing protocol that helps determine routes. After the administrator enables dynamic routing, the routing process automatically updates route knowledge whenever new topology information is received. The router learns and maintains routes to remote destinations by exchanging routing updates with other routers in the internetwork.

When to Use Static Routing

This topic describes when to use static routing.

When to Use Static Routing

Use static routes:

- In a small network that requires only simple routing
- In a hub-and-spoke network topology
- When you want to create a quick ad hoc route

Do *not* use static routes:

- In a large network
- When the network is expected to scale

© 2013 Cisco Systems, Inc.

Depending on network size, complexity, desired security, and design, you can choose between a dynamic routing protocol and configuring static routes.

Static routing has some advantages over dynamic routing:

- **Conserves router resources:** Static routing does not consume network bandwidth and the CPU resources of the router. When you use a routing protocol, the traffic between routers adds some overhead as the routers exchange routing updates about remote networks. Depending on the size of the network, a router requires some CPU cycles to compute the best way to remote networks.
- **Simple to configure in a small network:** Static routes are commonly used in small networks that have few routers. Many small networks are designed as stub networks (networks that are accessed by a single route), and static routes are the most appropriate solution. Also, most of these networks are designed in a hub-and-spoke topology, where you can use default routes for branches pointing to the hub, which is the gateway to other networks.

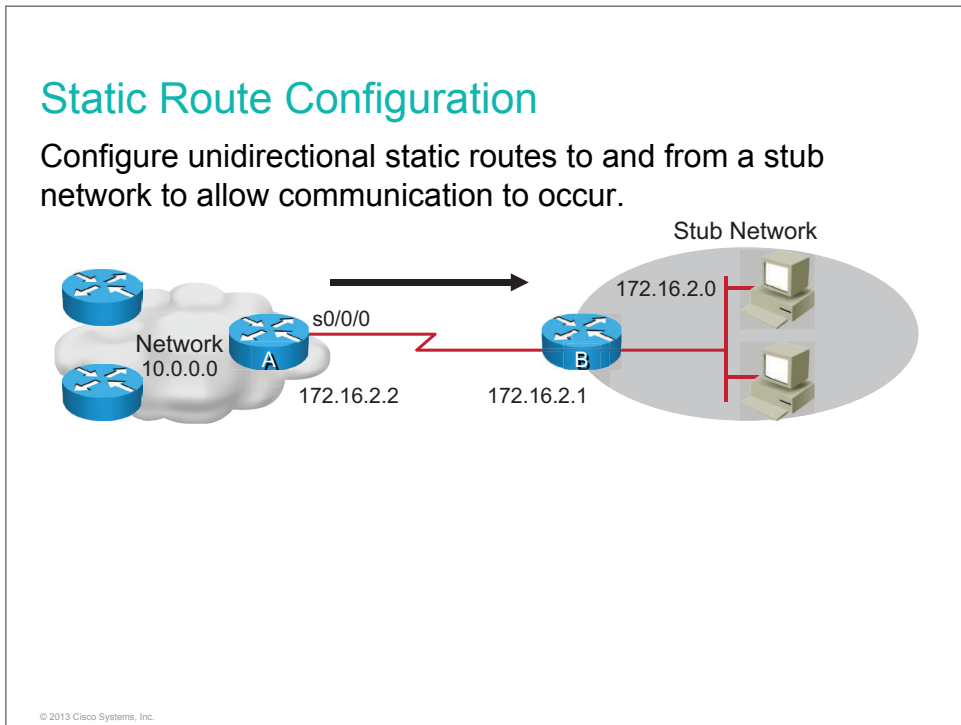
The disadvantages of static routing can be summarized as follows:

- **Scalability:** Static routing is appropriate for networks that have fewer than four or five routers. Dynamic routing is more appropriate for large networks to reduce the probability of errors in routing configuration.
- **More manual configuration in larger networks:** When the number of routers increases, the number of static routes also increases. In large networks that use static routing, adding even one router with only one new network means that you must configure the newly added router with static routes to other networks, and also that you must configure all existing routers in the network with static routes to the new network.

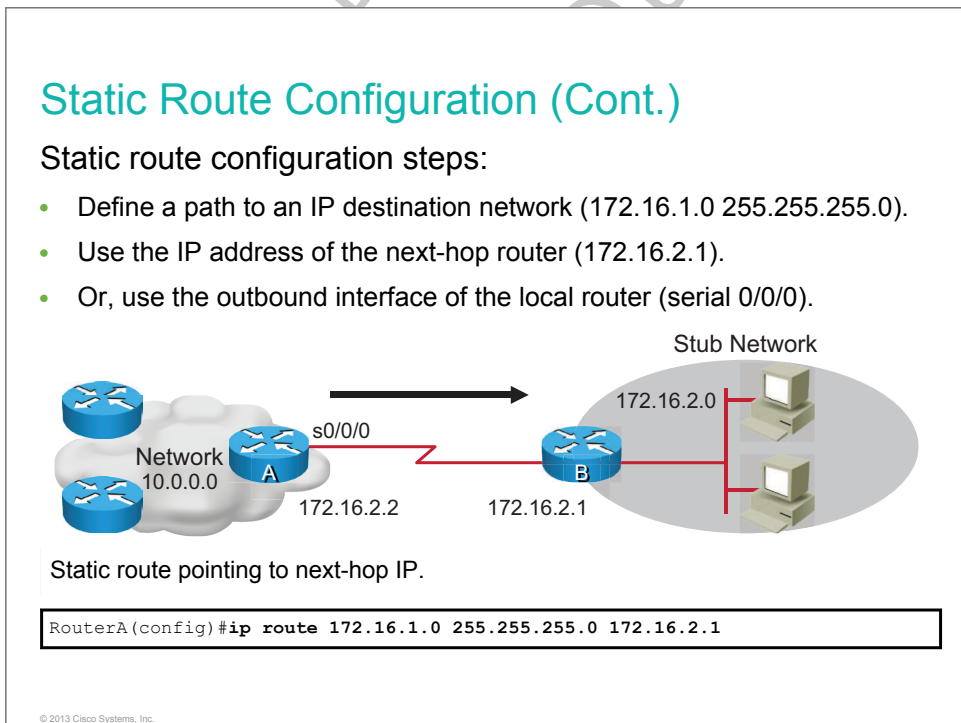
Organizations often use a combination of static and dynamic routes.

Static Route Configuration

This topic describes how to configure static routes on Cisco routers.



Static routes are commonly used when you are routing from a network to a stub network (a network that is accessed by a single link). Static routes can also be useful for specifying a “gateway of last resort” to which all packets with an unknown destination address are sent.



In the figure, router A is configured with a static route to reach the 172.16.1.0 subnet via the next hop IP 172.16.2.1 using the **ip route** command.

Alternatively, the static route can be configured by pointing to the exit interface instead of using the next-hop IP address.

```
RouterA(config)#ip route 172.16.1.0 255.255.255.0 serial10/0/0
```

The table lists the **ip route** command parameters for this example.

Command Parameters	Description
ip route	Identifies the static route
172.16.1.0	IP address of a static route to the destination subnetwork
255.255.255.0	Indicates the subnet mask—there are 8 bits of subnetting in effect
172.16.2.1	IP address of the next-hop router in the path to the destination
Serial 0/0/0	Identifies the interface that will be used to reach the next-hop router

Assigning a static route to reach the stub network 172.16.1.0 is proper for router A because there is only one way to reach that network.

In the figure, router B also needs to be configured with a static or default route to reach the networks behind router A via the serial interface of router B.

Note A static route is configured for connectivity to remote networks that are not directly connected to your router. For end-to-end connectivity, a static route must be configured in both directions.

Default Routes

This topic describes how to configure default route forwarding.

Default Routes

This route allows the stub network to reach all known networks beyond Router A.

Default route pointing to next-hop IP.

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

Default route pointing to exit interface.

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

© 2013 Cisco Systems, Inc.

Use a default route when the route from a source to a destination is not known or when it is not feasible for the router to maintain many routes in its routing table.

A default static route is a route that matches all packets. Default static routes are used in these instances:

- When no other routes in the routing table match the destination IP address of the packet or when a more specific match does not exist. A common use for a default static route is to connect the edge router of a company to an ISP network.
- When a router has only one other router to which it is connected. This condition is known as a stub router.

The syntax for a default static route is like that for any other static route, except that the network address is 0.0.0.0 and the subnet mask is 0.0.0.0.

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

or

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1
```

The 0.0.0.0 network address and 0.0.0.0 mask is called a *quad-zero* route.

In the figure, router B is configured to forward to router A all packets that do not have the destination network that is listed in the router B routing table.

This table lists the **ip route** command parameters for this example.

Command Parameters	Description
ip route	Identifies the static route
0.0.0.0	Routes to networks that are not in the routing table

Command Parameters	Description
0.0.0.0	Special mask that indicates the default route
172.16.2.2	IP address of the next-hop router to be used as the default for packet forwarding

Do Not Duplicate.
Post beta, not for release.

Static Route Configuration Verification

This topic describes how to verify static route configuration.

Static Route Configuration Verification

```
RouterA#show ip route
Codes: L - local, C - connected, S - static, 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
       <output omitted>

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, FastEthernet0/0
 172.16.0.0/24 is subnetted, 2 subnets
S    172.16.1.0/24 [1/0] via 172.16.2.1
C    172.16.2.0/24 is directly connected, Serial10/0/0
L    172.16.2.2/32 is directly connected, Serial10/0/0
```

© 2013 Cisco Systems, Inc.

Static Route Configuration Verification (Cont.)

To verify static routes in the routing table, examine the routing table with the **show ip route** command:

- Includes network address and subnet mask as well as IP address of next-hop router or exit interface
- Denoted with the code “S” in the routing table

Routing tables must contain directly connected networks that are used to connect remote networks before static or dynamic routing can be used.

© 2013 Cisco Systems, Inc.

Most routing tables contain a combination of static routes and dynamic routes. However, the routing table must first contain the directly connected networks that are used to access the remote networks before any static or dynamic routing can be used.

A static route includes the network address and subnet mask of the remote network, along with the IP address of the next-hop router or exit interface. Static routes are denoted with the code “S” in the routing table, as shown in the figure.

When you configure a static route to use an exit interface instead of a next-hop IP address, the routing table entry is changed as follows:

```
RouterA#show ip route
Codes: L - local, C - connected, S - static, 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
       <output omitted>

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, FastEthernet0/0
 172.16.0.0/24 is subnetted, 2 subnets
S    172.16.1.0/24 is directly connected, Serial0/0/0
C    172.16.2.0/24 is directly connected, Serial0/0/0
L    172.16.2.2/32 is directly connected, Serial0/0/0
```

Note that the entry in the routing table no longer refers to the next-hop IP address but refers directly to the exit interface. This exit interface is the same one to which the static route was resolved when it used the next-hop IP address. Now that the routing table process has a match for a packet and this static route, it is able to resolve the route to an exit interface in a single lookup.

Note The static route displays the route as directly connected. It is important to understand that this does not mean that this route is a directly connected network or a directly connected route. This route is still a static route.

Verifying the Default Route Configuration

To verify the default route configuration, examine the routing table on RouterB:

```
RouterB#show ip route
Codes: L - local, C - connected, S - static,
       R - RIP, M - mobile, B - BGP
       <output omitted>
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

 172.16.0.0/24 is subnetted, 2 subnets
C    172.16.1.0/24 is directly connected, FastEthernet0/0
C    172.16.2.0/24 is directly connected, Serial0/0/0
S*  0.0.0.0/0 [1/0] via 172.16.2.2
```

© 2013 Cisco Systems, Inc.

The example in the figure shows the RouterB routing table after configuration of the default route.

The asterisk (*) indicates the last path option that the router will use when forwarding a packet.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Routing is the process by which items get from one location to another. Routers can forward packets over static routes or dynamic routes.
- Static routes are entered manually by a network administrator. Dynamic routes are learned by a routing protocol, and dynamic routes change automatically when circumstances in the network change.
- Unidirectional static routes must be configured to and from a stub network to allow communication to occur.
- The **ip route** command can be used to configure default route forwarding.
- The **show ip route** command is used to verify that static routing is properly configured. Static routes are signified in the command output by “S” in the first position.

© 2013 Cisco Systems, Inc.

Managing Traffic Using ACLs

Overview

ACLs enable administrators to identify specific traffic that receives special treatment. The lesson introduces the concept of ACL operation, followed by an explanation of wildcard masking. While different types of ACLs are considered, configuration details are shown only for standard numbered ACLs.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe ACLs as a Cisco IOS tool for traffic identification
- Explain how ACLs operate
- Describe wildcard masking
- Describe wildcard bit mask abbreviations
- Compare standard and extended ACLs
- Explain what is tested when a packet is tested against a numbered standard access list
- Configure and verify standard IPv4 ACLs

Using ACLs

This topic describes how ACLs can be used as a tool to identify traffic.

Understanding ACLs

What is an ACL?

- An ACL is a Cisco IOS tool for traffic identification.
- An ACL is a list of permit and deny statements.
- An ACL identifies traffic based on the information within the IP packet.
- After traffic is identified, different actions can be taken.
- ACLs can be used on routers and switches.

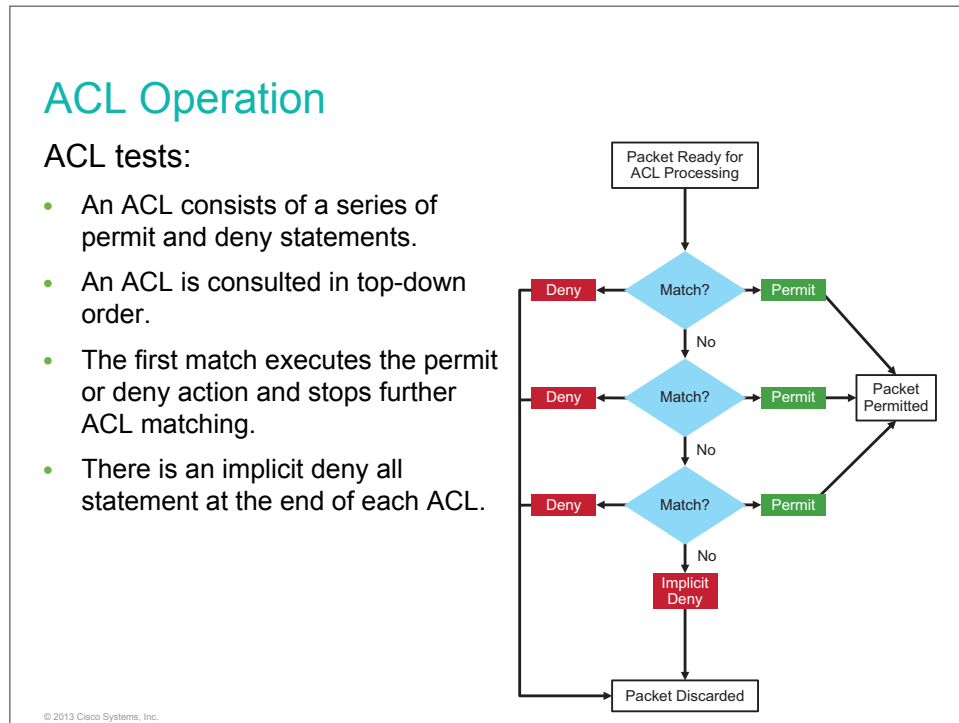
© 2013 Cisco Systems, Inc.

An ACL is a Cisco IOS feature that is used for traffic identification. The ACL enables an administrator to create a set of rules in the form of permit and deny statements that describe which traffic should be identified. Traffic identification is based on the header values in the IP packet. Identified traffic can receive different treatment, depending on which Cisco IOS function is using the ACLs.

ACLs are supported on a wide range of products, including routers and switches.

ACL Operation

This topic describes how ACLs operate.



ACL statements operate in sequential, logical order. They evaluate packets from the top down, one statement at a time. If a packet header and an ACL statement match, the rest of the statements in the list are skipped. The packet is then permitted or denied, as determined by the matched statement. If a packet header does not match an ACL statement, the packet is tested against the next statement in the list. This matching process continues until the end of the list is reached.

A final implied statement covers all packets for which conditions did not test true. This final test condition matches all other packets and results in a deny instruction. The router denies all of these remaining packets. This final statement is often referred to as the “implicit deny any” statement. Because of this statement, an ACL should have at least one permit statement in it; otherwise, the ACL denies all packets.

ACL Wildcard Masking

When processing ACLs, a router needs a mechanism to determine which bits of an IP address must match. A wildcard mask describes which bits of an IP address must match in an IP packet to result in a match for a permit or deny statement. This topic describes how to use wildcard masks with ACLs.

ACL Wildcard Masking

Wildcard bits—how to check the corresponding address bits:

- 0 means to match the value of the corresponding address bit.
- 1 means to ignore the value of the corresponding address bit.

128	64	32	16	8	4	2	1	Octet Bit Position and Address Value for Bit
0	0	0	0	0	0	0	0	0 = Match All Address Bits (Match All)
0	0	1	1	1	1	1	1	1 = Ignore Last 6 Address Bits
0	0	0	0	1	1	1	1	1 = Ignore Last 4 Address Bits
1	1	1	1	1	1	0	0	0 = Match Last 2 Address Bits
1	1	1	1	1	1	1	1	1 = Do Not Check Address (Ignore Bits in Octet)

Examples

© 2013 Cisco Systems, Inc.

ACL statements include masks, also called *wildcard masks*. A wildcard mask is a string of binary digits that tell the router which parts of the subnet number to look at. Although wildcard masks have no functional relationship with subnet masks, they do provide a similar function. The mask determines how much of an IP source or destination address to apply to the address match. The numbers 1 and 0 in the mask identify how to treat the corresponding IP address bits. However, they are used for different purposes and follow different rules.

Wildcard masks and subnet masks are both 32 bits long and use binary 1s and 0s. Subnet masks use binary 1s and 0s to identify the network, subnet, and host portion of an IP address. Wildcard masks use binary 1s and 0s to filter individual or groups of IP addresses to permit or deny access to resources based on an IP address. By carefully setting wildcard masks, you can permit or deny a single or several IP addresses.

Wildcard masks and subnet masks differ in the way in which they match binary 1s and 0s. Wildcard masks use the following rules to match binary 1s and 0s:

- **Wildcard mask bit 0:** Match the corresponding bit value in the address.
- **Wildcard mask bit 1:** Ignore the corresponding bit value in the address.

The figure shows how different wildcard masks filter IP addresses. As you look at the example, remember that binary 0 signifies a match and that binary 1 signifies ignore.

Note A wildcard mask is sometimes referred to as an *inverse mask*. In a subnet mask, binary 1 is equal to a match and binary 0 is not a match. The reverse is true for wildcard masks. A 0 in a bit position of the wildcard mask indicates that the corresponding bit in the address must be matched. A 1 in a bit position of the wildcard mask indicates that the corresponding bit in the address is not interesting and can be ignored.

By carefully setting wildcard masks, you can permit or deny with one ACL statement. You can select a single IP address or many IP addresses.

The figure shows how to check corresponding address bits.

ACL Wildcard Masking (Cont.)

Filter for IP subnets 170.30.16.0/24 to 172.30.31.0/24.

Address and wildcard mask:

172.30.16.0 0.0.15.255

© 2013 Cisco Systems, Inc.

ACL Wildcard Masking (Cont.)

This example shows the wildcard masking process for IP subnets.

		Network.Host								
		172.30.16.0								
Wildcard Mask:		0	0	0	1	0	0	0	0	
		0	0	0	0	1	1	1	1	
		<---- Match ---->				> <---- Don't Care ---->				
		0	0	0	1	0	0	0	0	= 16
		0	0	0	1	0	0	0	1	= 17
		0	0	0	1	0	0	1	0	= 18
					:					:
		0	0	0	1	1	1	1	1	= 31

© 2013 Cisco Systems, Inc.

In the figure, an administrator wants to test a range of IP subnets that is to be permitted or denied. Assume that the IP address is a Class B address (the first two octets are the network number), with 8 bits of subnetting (the third octet is for subnets). The administrator wants to use the IP wildcard masking bits to match subnets 172.30.16.0/24 to 172.30.31.0/24.

To use one ACL statement to match this range of subnets, use the IP address 172.30.16.0 in the ACL, which is the first subnet to be matched, followed by the required wildcard mask.

First, the wildcard mask matches the first two octets (172 and 30) of the IP address using corresponding 0 bits in the first two octets of the wildcard mask.

Because there is no interest in an individual host, the wildcard mask ignores the final octet by using the corresponding 1 bit in the wildcard mask. For example, the final octet of the wildcard mask is 255 in decimal.

In the third octet, where the subnet address occurs, the wildcard mask of decimal 15, or binary 00001111, matches the high-order 4 bits of the IP address. In this case, the wildcard mask matches subnets starting with the 172.30.16.0/24 subnet. For the final (low-end) 4 bits in this octet, the wildcard mask indicates that the bits can be ignored. In these positions, the address value can be binary 0 or binary 1. Thus, the wildcard mask matches subnet 16, 17, 18, and so on, up to subnet 31. The wildcard mask does not match any other subnets.

In the example, the address 172.30.16.0 with the wildcard mask 0.0.15.255 matches subnets 172.30.16.0/24 to 172.30.31.0/24.

In some cases, you must use more than one ACL statement to match a range of subnets. For example, to match 10.1.4.0/24 to 10.1.8.0/24, use 10.1.4.0 0.0.3.255 and 10.1.8.0 0.0.0.255.

Do Not Duplicate
Post beta, not for release

Wildcard Bit Mask Abbreviations

This topic describes wildcard mask abbreviations.

Wildcard Bit Mask Abbreviations

Using wildcard bit mask abbreviations:

- 172.30.16.29 0.0.0.0 matches all of the address bits.
- Abbreviate this wildcard mask using the IP address preceded by the keyword **host** (**host 172.30.16.29**).
- 0.0.0.0 255.255.255.255 ignores all address bits.
- Abbreviate *expression* with the keyword **any**.

© 2013 Cisco Systems, Inc.

The 0 and 1 bits in an ACL wildcard mask cause the ACL to either match or ignore the corresponding bit in the IP address. Working with decimal representations of binary wildcard mask bits can be tedious. For the most common uses of wildcard masking, you can use abbreviations so that you need not enter as many numbers when configuring address test conditions.

In the example, instead of entering 172.30.16.29 0.0.0.0, you can use the string **host 172.30.16.29**. Using the abbreviation **host** communicates the same test condition to Cisco IOS Software.

In the example, instead of entering 0.0.0.0 255.255.255.255, you can use the keyword **any** by itself. Using the abbreviation **any** communicates the same test condition to Cisco IOS Software.

Types of ACLs

This topic identifies the two main types of ACLs, standard and extended, and two methods of identifying ACLs, numbering and naming.

Types of ACLs

Two main types of ACLs:

- Standard ACL:
 - Checks source IP address
 - Permits or denies entire protocol suite
- Extended ACL:
 - Checks source and destination IP address
 - Generally permits or denies specific protocols and applications

Two methods that you can use to identify standard and extended ACLs:

- Numbered ACLs
- Named ACLs

© 2013 Cisco Systems, Inc.

ACLs can be categorized into the following types:

- **Standard ACLs:** Standard IP ACLs check the source addresses of packets that can be routed. The result either permits or denies the output for an entire protocol suite, which is based on the source network, subnet, or host IP address.
- **Extended ACLs:** Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allows administrators more flexibility and control.

There are two methods that you can use to identify standard and extended ACLs:

- Numbered ACLs use a number for identification.
- Named ACLs use a descriptive name or number for identification.

Types of ACLs (Cont.)

How to identify ACLs:

- Numbered standard IPv4 ACLs (1 to 99) test conditions of all IP packets for source addresses. The expanded range is 1300 to 1999.
- Numbered extended IPv4 ACLs (100 to 199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports. The expanded range is 2000 to 2699.
- Named ACLs identify IP standard and extended ACLs with an alphanumeric string (name).

IPv4 ACL Type	Number Range or Identifier
Numbered Standard	1–99, 1300–1999
Numbered Extended	100–199, 2000–2699
Named (Standard and Extended)	Name

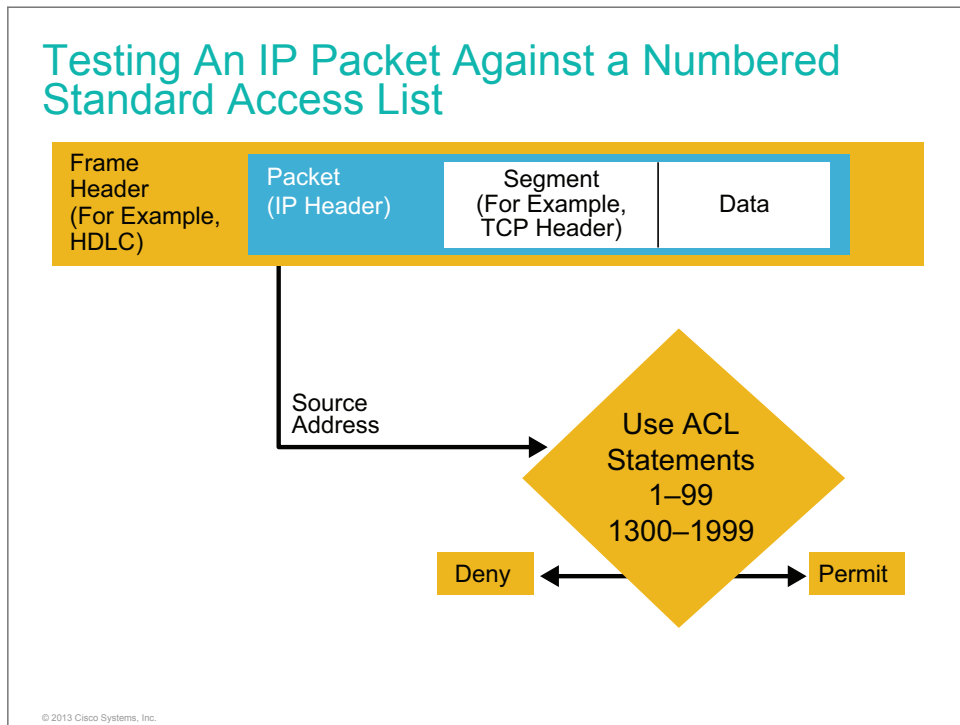
© 2013 Cisco Systems, Inc.

You can create many ACLs for a protocol. Select a different ACL number for each new ACL within a given protocol. However, on an interface, you can apply only one ACL per protocol, per direction.

Specifying an ACL number from 1 to 99 or 1300 to 1999 instructs the router to accept numbered standard IPv4 ACL statements. Specifying an ACL number from 100 to 199 or 2000 to 2699 instructs the router to accept numbered extended IPv4 ACL statements.

Testing an IP Packet Against a Numbered Standard Access List

This topic describes how standard numbered ACL operates.



Standard IPv4 ACLs, whether numbered (1 to 99 and 1300 to 1999) or named, filter packets based on a source address and mask, and they permit or deny the entire TCP/IP protocol suite.

Note The standard ACL may not provide the required level of control that you require. You may need a more precise tool to select network traffic.

Basic Configuration of Numbered Standard IPv4 ACLs

This topic describes how to configure a basic numbered standard IPv4 ACL.

Basic Configuration of Numbered Standard IPv4 ACLs

Configure a numbered standard IPv4 ACL:

```
RouterX(config)#access-list 1 permit 172.16.0.0 0.0.255.255
```

- The statement matches any source address that starts with 172.16.x.x.
- Standard ACL configuration uses 1 to 99, or 1300 to 1999, for the ACL number (1 in the example).
- The default wildcard mask is 0.0.0.0 (only standard ACL).

Display the current ACLs configured on RouterX:

```
RouterX#show access-lists
Standard IP access list 1
 10 permit 172.16.0.0, wildcard bits 0.0.255.255
```

© 2013 Cisco Systems, Inc.

You can configure numbered standard IPv4 ACLs on a Cisco router in global configuration mode. The **access-list** command creates an entry in a standard IPv4 filter list. The figure shows the syntax of this command.

In the figure, the output of the **show access-list** command displays the current ACLs that are configured on router RouterX.

Basic Configuration of Numbered Standard IPv4 ACLs (Cont.)

Delete a numbered standard IPv4 ACL:

```
RouterX(config)#no access-list 1
RouterX(config)#exit
RouterX#show access-lists
RouterX#
```

- Use the **no access-list 1** command to remove the entire ACL 1.

© 2013 Cisco Systems, Inc.

To remove the ACL, use the **no access-list number** command in global configuration mode. Issue the **show access-list** command to confirm that ACL 1 has been removed. With numbered ACLs, individual entries cannot be removed with the **no access-list** command, because this command removes the entire ACL. The traditional way of removing or modifying a single numbered ACL entry would be to copy the whole ACL to a text editor, make the changes that are needed, and remove the entire ACL from the router using the **no access-list** command. The modified ACL can then be copied and pasted from the text editor. Newer Cisco IOS Software versions allow easier editing by using sequence numbering.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- An ACL is a tool to identify traffic for special handling.
- ACLs perform top-down processing and can be configured for incoming or outgoing traffic.
- In a wildcard bit mask, a 0 bit means to match the corresponding address bit and a 1 bit means to ignore the corresponding address bit.
- You can create an ACL using a named or numbered ACL. Named or numbered ACLs can be configured as standard or extended ACLs, which determines what they can filter.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Enabling Internet Connectivity

Overview

It has become common for small sites to use the Internet to connect to other sites. Internet service is obtained through an ISP. In some cases, the ISP provides a static IP address for the interface that is connected to the Internet. In other cases, this IP address is provided using DHCP.

Two scalability challenges for the Internet are the depletion of the registered IPv4 address space and scaling in routing. Cisco IOS NAT and PAT are mechanisms for conserving registered IP addresses in large networks, and they also simplify IP addressing tasks. NAT and PAT translate IP addresses within private internal networks to valid IP addresses for transport over public external networks, such as the Internet, without requiring a registered subnet address. Incoming traffic is translated for delivery within the inside network. This translation of IP addresses eliminates the need for host renumbering and allows the same IP address range to be used in multiple intranets.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

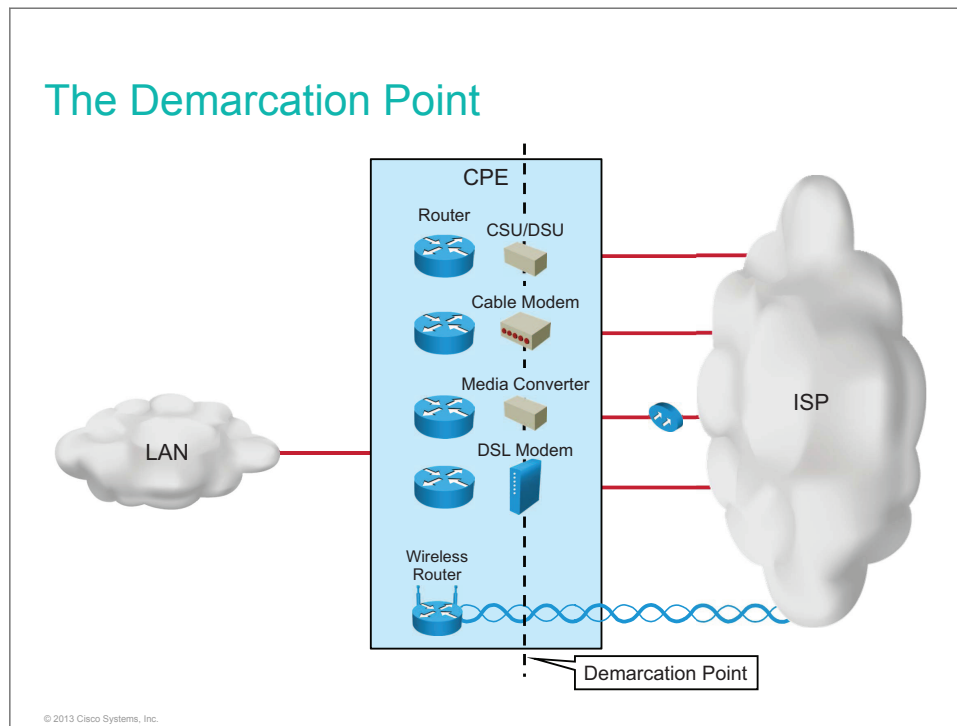
- Describe various connectivity options for Internet access
- Explain what is the demarcation point
- Define the function of DHCP
- Describe the process of obtaining a public IP address
- Configure a router with a static public IP address
- Configure a Cisco router as a DHCP client
- Compare public and private IPv4 addresses
- Describe the features and benefits of NAT

- Describe types of NAT addresses
- Describe types of NAT
- Understand how static NAT operates
- Configure static NAT
- Verify static NAT configuration
- Understand how dynamic NAT works
- Describe an example of configuring dynamic NAT
- Describe an example of verifying dynamic NAT
- Understand how NAT Overload operates
- Describe an example of configuring PAT
- Describe an example of verifying PAT
- Describe how to troubleshoot NAT
- Troubleshoot NAT

Do Not Duplicate.
Post beta, not for release.

The Demarcation Point

This topic describes the demarcation point and explains its importance.



Although functions within the service provider network are not usually of concern to customers, there are some terms and concepts that you should be familiar with.

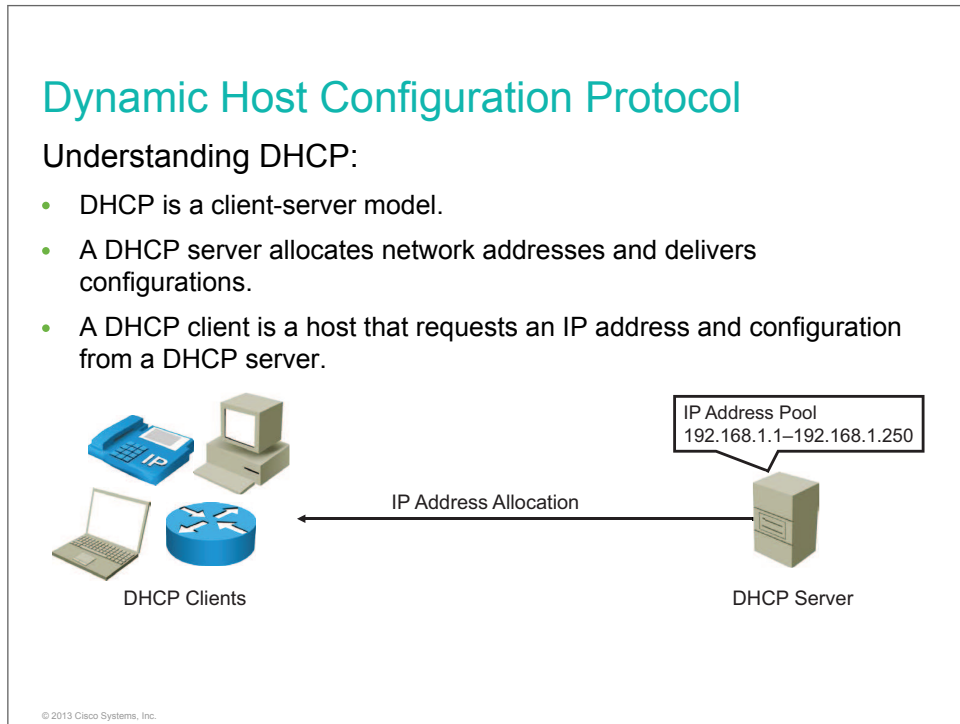
Service providers install a connection point (usually in the form of an RJ-45 jack) that physically connects a circuit to their nearest switching office. This link is known as the *demarcation point* and represents the point at which the service provider responsibility is said to end. In other words, the service provider ensures that the link functions correctly up to that point. The other end of this link connects to the service provider network. These links are part of what is known as the *local loop* or *last mile*. The local loop may consist of a variety of technologies, including DSL, cable, fiber optics, traditional twisted-pair wiring, and others.

The customer side of the demarcation point is the location of the CPE. The term CPE is often used quite loosely, but it traditionally refers to equipment that is owned and managed by the customer for the purpose of connecting to the service provider network. However, many companies lease CPE from their service providers, and this equipment is still considered to be CPE. Before physically connecting to a service provider network, a company needs to determine the type of WAN service or connectivity that it requires.

Note The exact demarcation point is different from country to country. The example described is for the United States.

Dynamic Host Configuration Protocol

Originally, network administrators had to manually configure IP addresses and other network parameters on equipment connecting to the Internet. DHCP was introduced to automate assignment of network parameters.



Managing a network can be time-consuming. Network clients break or are moved around, and new clients appear that need network connectivity—all part of the network administrator job. Manually configuring IP addresses for all devices in the network is impossible in some cases. DHCP can greatly lighten the workload of the network administrator. DHCP automatically assigns an IP address from an IP address pool that is defined by the administrator. However, DHCP is much more than just an IP address allocation mechanism. A DHCP server can push other initial configuration parameters to the client devices, such as the time or a log server address.

DHCP is built on a client-server model. The DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. The term “client” refers to a host that is requesting initialization parameters from a DHCP server.

Dynamic Host Configuration Protocol (Cont.)

DHCP IP address allocation mechanisms:

- **Automatic allocation:** A permanent IP address is assigned to a client.
- **Dynamic allocation:** A client is assigned an IP address for a limited time.
- **Manual allocation:** A client is assigned an IP address by the network administrator.

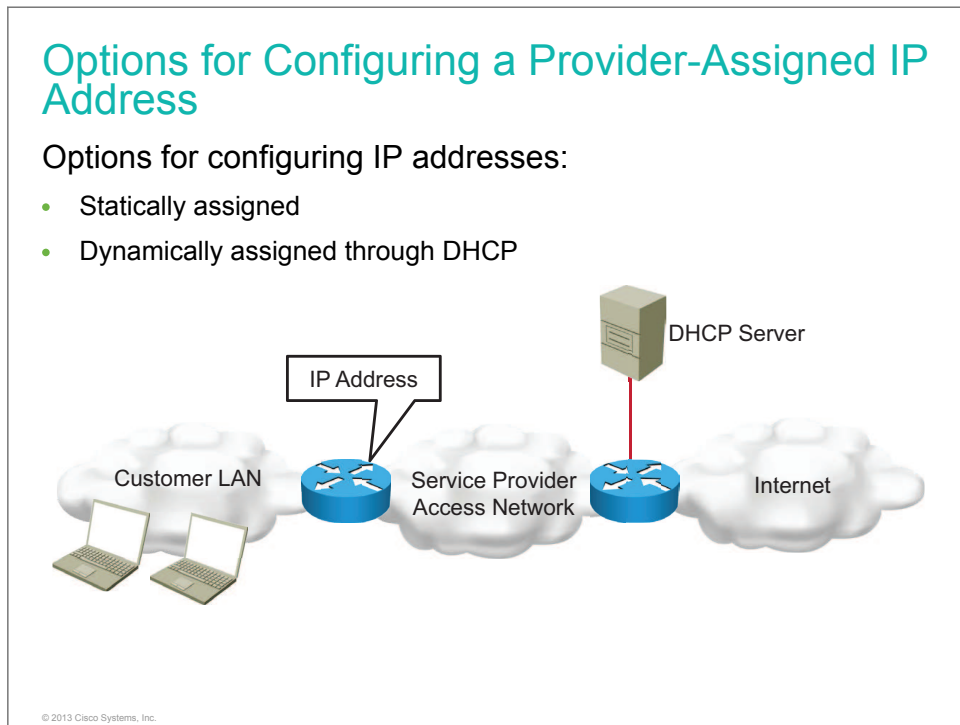
© 2013 Cisco Systems, Inc.

DHCP supports three mechanisms for IP address allocation. With automatic allocation, DHCP assigns a permanent IP address to a client. With dynamic allocation, DHCP assigns an IP address to a client for a limited time (or until the client explicitly relinquishes the address). With manual allocation, a client is assigned an IP address by the network administrator, and DHCP is used simply to convey the assigned address to the client.

Dynamic allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned. Dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Dynamic allocation may also be a good choice for assigning an IP address to a new client that is being permanently connected to a network in which IP addresses are so scarce that it is important to reclaim them when clients are retired.

Options for Configuring a Provider-Assigned IP Address

This topic describes options for configuring a provider-assigned IP address.



The DHCP service enables devices on a network to obtain IP addresses and other information from a DHCP server. This service automates assignment of IP addresses, subnet masks, gateways, and other IP networking parameters.

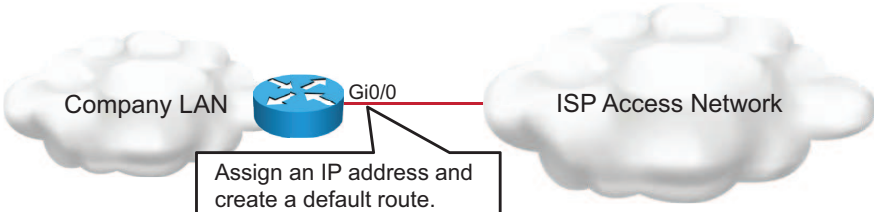
A service provider sometimes provides a static address for an interface that is connected to the Internet. In other cases, the address is provided using DHCP. On larger local networks or where the user population changes frequently, DHCP is preferred. New users may arrive with laptops and need a connection. Others have new workstations that need to be connected. Rather than have the network administrator assign an IP address for each workstation, it is more efficient to have IP addresses assigned automatically using DHCP.

If an ISP uses DHCP to provide interface addressing, no manual addresses can be configured. Instead, the interface is configured to operate as a DHCP client. This configuration means that when the router is connected to a cable modem, for example, it is a DHCP client and requests an IP address from the ISP.

Configuring a Static Provider-Assigned IP Address

This topic describes how to configure a static provider-assigned IP address on a Cisco router.

Configuring a Static Provider-Assigned IP Address



```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shutdown
```

- Configures a public IP address.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

- Creates a default route that points toward the next-hop IP address.

© 2013 Cisco Systems, Inc.

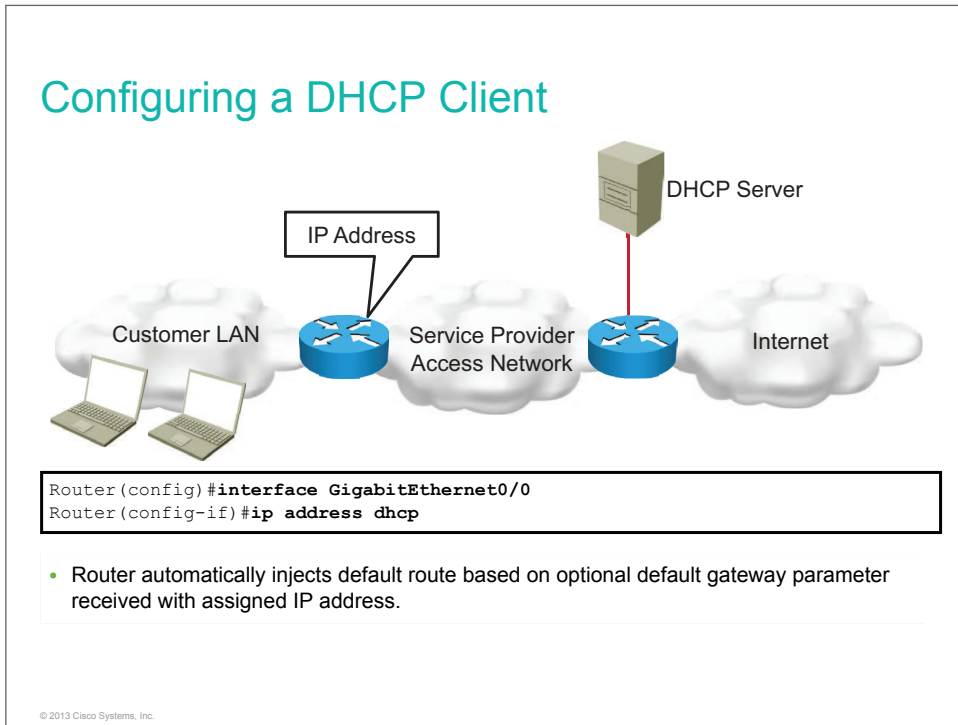
Static provider-assigned IP addresses can be more useful in several respects than dynamic addresses. Static IP addresses can be linked to a domain name (such as *www.cisco.com*), and public or private servers can be run for access by outside users.

For example, your ISP assigns you a static IP address of 209.165.200.225/27. You proceed with a two-step process. The first step is to configure the static IP address that you were assigned on the outside interface of the router. The second step is to configure a default route that forwards all traffic that is intended for the Internet to the outside interface.

Command	Description
interface <i>interface</i>	Specifies an interface and enters interface configuration mode
ip address <i>address subnet_mask</i>	Sets the IP address and mask of the device
no shutdown	Enables an interface
ip route <i>net-prefix prefix-mask next_hop_ip_address</i>	Establishes a static route to destination

Configuring a DHCP Client

This topic describes how to configure a router interface so that a device can acquire an IP address from a DHCP server.



An ISP sometimes provides a static address for an interface that is connected to the Internet. In other cases, an address is provided using DHCP. If the ISP uses DHCP to provide interface addressing, no manual address can be configured. Instead, the interface is configured to operate as a DHCP client.

If the router receives an optional DHCP parameter called default gateway with the assigned IP address, the default route will be injected into the routing table, pointing to the default gateway IP address.

Command	Description
<code>interface interface</code>	Specifies an interface and enters interface configuration mode.
<code>ip address dhcp</code>	Specifies that the interface acquires an IP address through DHCP.

Public vs. Private IPv4 Addresses

Some networks connect to each other through the Internet, while others are private. For instance, the example addresses used in this course are private, which means that they are not assigned to public use. Public and private IP addresses are required for both of these network types. This topic describes the purpose and sources for public and private IP addresses.

Public vs. Private IPv4 Addresses	
Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255
Class	Public Address Range
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

© 2013 Cisco Systems, Inc.

Private IP Addresses

Internet hosts require a globally unique IP address, but private hosts that are not connected to the Internet can use any valid address, as long as it is unique within the private network. However, because many private networks exist alongside public networks, grabbing "just any address" is strongly discouraged.

Three blocks of IP addresses (one Class A network, 16 Class B networks, and 256 Class C networks) are designated for private, internal use. The figure shows the address ranges for each class. Addresses in these ranges are not routed on the Internet backbone. Internet routers are configured to discard private addresses.

In a private intranet, these private addresses can be used instead of globally unique addresses.

When a network that is using private addresses must connect to the Internet, it is necessary to translate the private addresses to public addresses. This translation process is called NAT. A router is often the network device that performs NAT.

Public IP Addresses

Public IP addresses are used for the hosts that are publicly accessible from the Internet. Internet stability depends directly on the uniqueness of publicly used network addresses. Therefore, a mechanism is needed to ensure that addresses are, in fact, unique. This mechanism was originally managed by the InterNIC. IANA succeeded InterNIC. IANA carefully manages the remaining supply of IP addresses to ensure that duplication of publicly used addresses does not occur. Duplication would cause instability in the Internet and would compromise its ability to deliver datagrams to networks using the duplicated addresses.

To obtain a provider-dependent IP address or block of addresses, you must contact an ISP. To obtain provider-independent IP addresses, you must contact an LIR. LIRs obtain IP address pools from their RIRs:

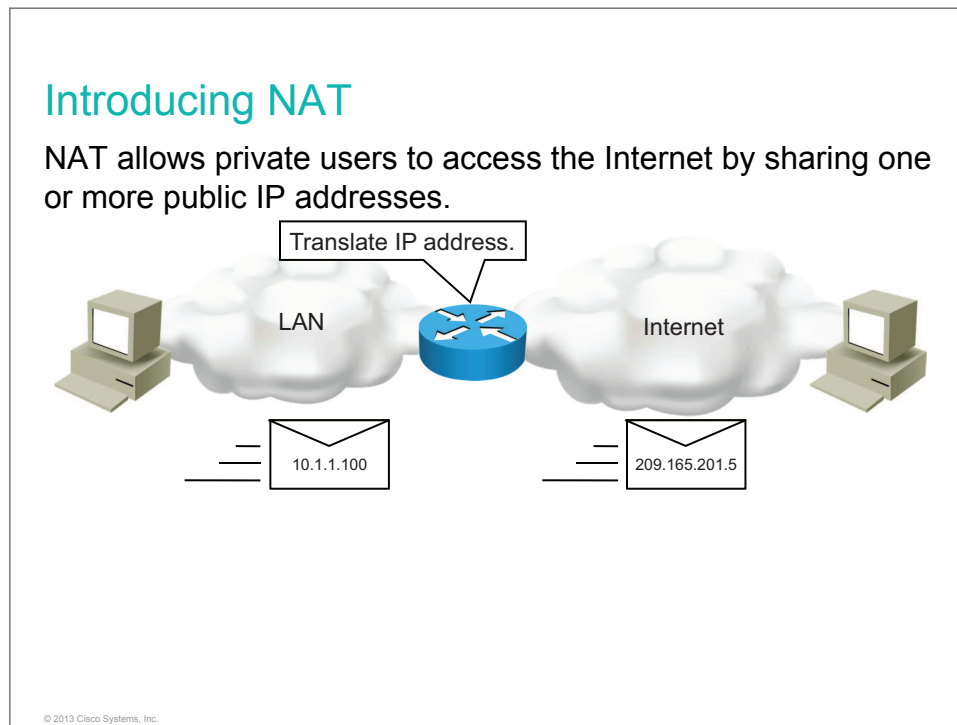
- AfriNIC
- APNIC
- ARIN
- LACNIC
- RIPE NCC

With the rapid growth of the Internet, public IP addresses began to run out. New mechanisms such as NAT, CIDR, VLSM, and IPv6 were developed to help solve the problem.

Do Not Duplicate.
Post beta, not for release.

Introducing NAT

This topic describes why NAT is used.



Small networks are commonly implemented using private IP addressing as defined in RFC 1918. Private addressing gives enterprises considerable flexibility in network design. This addressing enables operationally and administratively convenient addressing schemes as well as easier growth. However, you cannot route private addresses over the Internet, and there are not enough public addresses to allow all organizations to provide a private address to all of their hosts. Therefore, network administrators need a mechanism to translate private addresses to public addresses (and back) at the edge of their network.

NAT provides this mechanism. Before NAT, a host with a private address could not access the Internet. Using NAT, companies can provide some or all of their hosts with private addresses and use NAT to provide address translation to allow access to the Internet.

NAT is like the receptionist in a large office. Assume that you have left instructions with the receptionist not to forward any calls to you unless you request it. Later, you call a potential client and leave a message asking the client to call you back. You tell the receptionist that you are expecting a call from this client, and you ask the receptionist to put the call through to you. The client calls the main number to your office, which is the only number that the client knows. When the caller gives the receptionist your name, the receptionist checks a lookup table that matches your name to your extension. The receptionist knows that you requested this call and forwards the caller to your extension.

Usually, NAT connects two networks and translates the private (inside local) addresses in the internal network to public (inside global) addresses before packets are forwarded to another network. You can configure NAT to advertise only one address for the entire network to the outside world. Advertising only one address effectively hides the internal network, providing additional security as a side benefit.

The network address translation process of swapping one address for another is separate from the convention that is used to determine what is public and private, and devices must be configured to recognize which IP networks are to be translated. This requirement is one of the reasons why NAT can also be deployed internally when there is a clash of private IP addresses, such as, for example, when two companies merge.

Benefits of NAT

These are the benefits of NAT:

- Eliminates the need to readdress all hosts that require external access, saving time and money.
- Conserves addresses through application port-level multiplexing. With PAT, multiple internal hosts can share a single registered IPv4 address for all external communication. In this type of configuration, relatively few external addresses are required to support many internal hosts, which conserves IPv4 addresses.
- Protects network security. Because private networks do not advertise their addresses or internal topology, they remain reasonably secure when they gain controlled external access in conjunction with NAT.

Drawbacks of NAT

These are disadvantages of NAT:

- Many IP addresses and applications depend on end-to-end functionality, with unmodified packets forwarded from the source to the destination. By changing end-to-end addresses, NAT blocks some applications that use IP addressing. For example, some security applications, such as digital signatures, fail because the source IP address changes. Applications that use physical addresses instead of a qualified domain name do not reach destinations that are translated across the NAT router. Sometimes, this problem can be avoided by implementing static NAT mappings.
- End-to-end IP traceability is also lost. It becomes much more difficult to trace packets that undergo numerous packet address changes over multiple NAT hops, so troubleshooting is challenging. On the other hand, hackers who want to determine the source of a packet find it difficult to trace or obtain the original source or destination address.
- Using NAT also complicates tunneling protocols, such as IPsec, because NAT modifies the values in the headers, which interferes with the integrity checks done by IPsec and other tunneling protocols.
- Services that require the initiation of TCP connections from the outside network, or stateless protocols such as those using UDP, can be disrupted. Unless the NAT router makes a specific effort to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts (passive mode FTP, for example) but fail when both systems are separated from the Internet by NAT.
- The last disadvantage involves performance. NAT increases switching delays because translation of each IP address within the packet headers takes time. The first packet is process-switched, meaning that it always goes through the slower path. The router must look at each packet to decide whether it needs translation. The router needs to alter the IP header and possibly alter the TCP or UDP header. Remaining packets go through the fast-switched path if a cache entry exists; otherwise, they too are delayed.

Types of Addresses in NAT

This topic describes NAT address types.

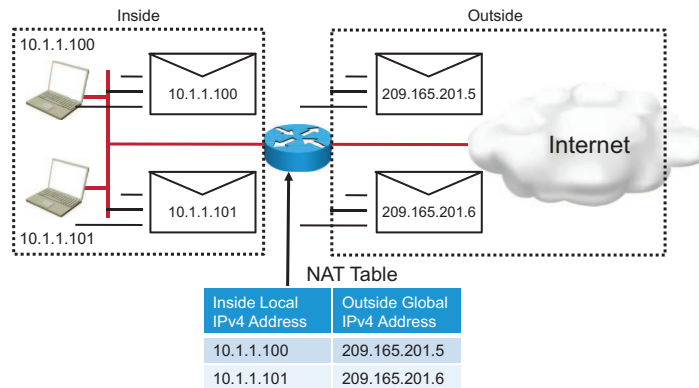
Types of Addresses in NAT

These are the most important types of addresses in NAT:

- **Inside local:** Host on the inside network
- **Inside global:** Usually assigned by an ISP and allows the customer outside access
- **Outside global:** Host on the outside network

© 2013 Cisco Systems, Inc.

Types of Addresses in NAT (Cont.)



© 2013 Cisco Systems, Inc.

In NAT terminology, the *inside network* is the set of networks that are subject to translation. The *outside network* refers to all other addresses. Usually, these are valid addresses that are located on the Internet.

Cisco defines these NAT terms:

- **Inside local address:** The IPv4 address that is assigned to a host on the inside network. The inside local address is likely not an IPv4 address that is assigned by the network information center or service provider.
- **Inside global address:** A legitimate IPv4 address that is assigned by the network information center or service provider that represents one or more inside local IPv4 addresses to the outside world.
- **Outside global address:** The IPv4 address that is assigned to a host on the outside network by the host owner. The outside global address is allocated from a globally routable address or network space.
- **Outside local address:** The IPv4 address of an outside host as it appears to the inside network. Not necessarily legitimate, the outside local address is allocated from a routable address space on the inside.

A good way to remember what is local and what is global is to add the word *visible*. An address that is locally visible normally implies a private IP address, and an address that is globally visible normally implies a public IP address. The rest is simple. *Inside* means internal to your network and *outside* means external to your network. So, for example, an inside global address means that the device is physically inside your network and has an address that is visible from the Internet. It could be a web server, for instance.

Do Not Duplicate
Post beta, not for release

Types of NAT

This topic describes the types of NAT.

Types of NAT

These are the types of NAT:

- **Static NAT:** One-to-one address mapping
- **Dynamic NAT:** Many-to-many address mapping
- **PAT:** Many-to-one address mapping

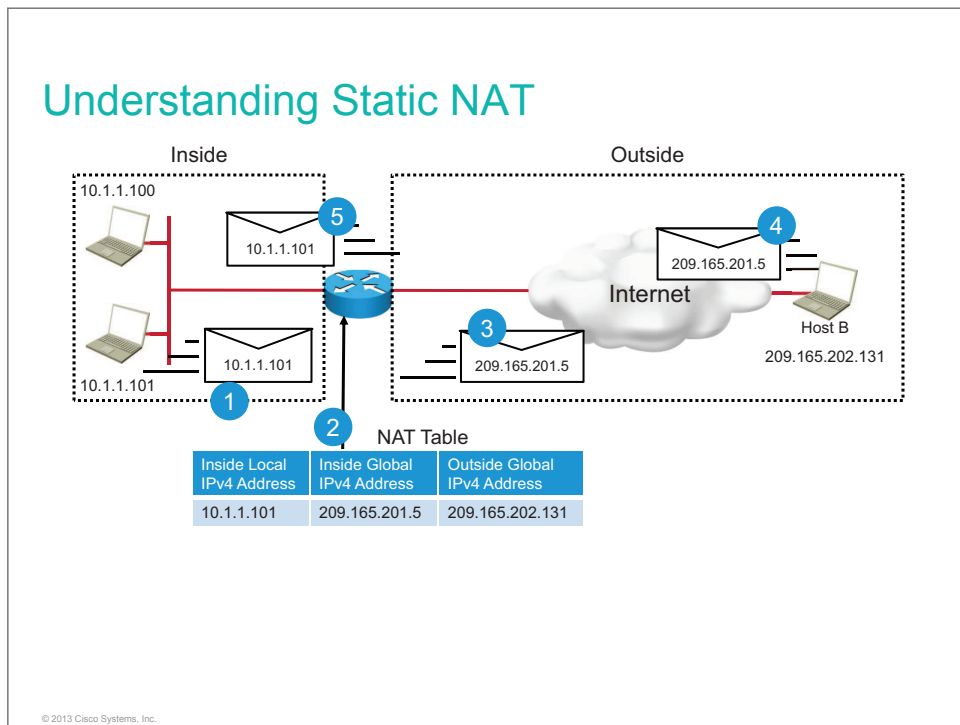
© 2013 Cisco Systems, Inc.

NAT can work in these ways:

- **Static NAT:** Maps an unregistered IPv4 address to a registered IPv4 address (one to one). Static NAT is particularly useful when a device must be accessible from outside the network. This type of NAT is used when a company has a server for which it needs a static IP address.
- **Dynamic NAT:** Maps an unregistered IPv4 address to a registered IPv4 address from a group of registered IPv4 addresses. This type of NAT is used, for example, when two companies merge that are using the same private address space. With the use of dynamic NAT readdressing, use of the entire address space is avoided or at least postponed.
- **PAT:** PAT maps multiple unregistered IPv4 addresses to a single registered IPv4 address (many to one) by using different ports. PAT is also known as NAT overloading. It is a form of dynamic NAT and is the most common use for NAT. It is used every day in your place of business or your home. Multiple users of PCs, tablets, and phones are able to access the Internet, even though only one public IP address is available for that LAN.

Understanding Static NAT

This topic describes how static NAT works.



You can translate your own IPv4 addresses into globally unique IPv4 addresses when you are communicating outside your network.

The figure illustrates a router that is translating a source address inside a network into a source address outside the network. These are the steps for translating an inside source address:

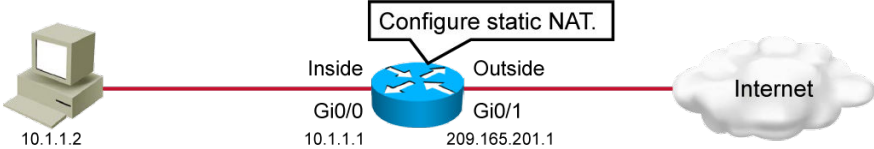
- 1 The user at host 10.1.1.101 wants to open a connection to host B (IP address 209.165.202.131).
- 2 The first packet that the router receives on its NAT inside-enabled interface from host 10.1.1.101 causes the router to check its NAT table.
- 3 The router replaces the inside local source address of host 10.1.1.101 with the translated inside global address (209.165.201.5) and forwards the packet.
- 4 Host B receives the packet and responds to host 10.1.1.101, using the inside global IPv4 destination address 209.165.201.5.
- 5 When the router receives the packet on its NAT outside-enabled interface with the inside global IPv4 address of 209.165.201.5, the router performs a NAT table lookup using the inside global address as a key. The router then translates the address back to the inside local address of host 10.1.1.101 and forwards the packet to host 10.1.1.101.
- 6 Host 10.1.1.101 receives the packet and continues the conversation. The router performs Steps 2 through 5 for each packet.

Configuring Static NAT

This topic describes how to configure static NAT.

Configuring Static NAT

Example: Configuring static NAT



```

Router (config) #interface GigabitEthernet 0/1
Router (config-if) #ip address 209.165.201.1 255.255.255.240
Router (config-if) #ip nat outside
Router (config-if) #exit
Router (config) #interface GigabitEthernet 0/0
Router (config-if) #ip address 10.1.1.1 255.255.255.0
Router (config-if) #ip nat inside
Router (config-if) #exit
Router (config) #ip nat inside source static 10.1.1.2 209.165.201.5
    
```

© 2013 Cisco Systems, Inc.

Remember that static NAT is a one-to-one mapping between an inside address and an outside address. Static NAT allows external devices to initiate connections to internal devices. For instance, you may want to map an inside global address to a specific inside local address that is assigned to your web server.

Configuring static NAT translations is a simple task. You need to define the addresses to translate and then configure NAT on the appropriate interfaces. Packets arriving on an inside interface from the identified IP address are subject to translation. Packets arriving on an outside interface that are addressed to the identified IP address are also subject to translation.

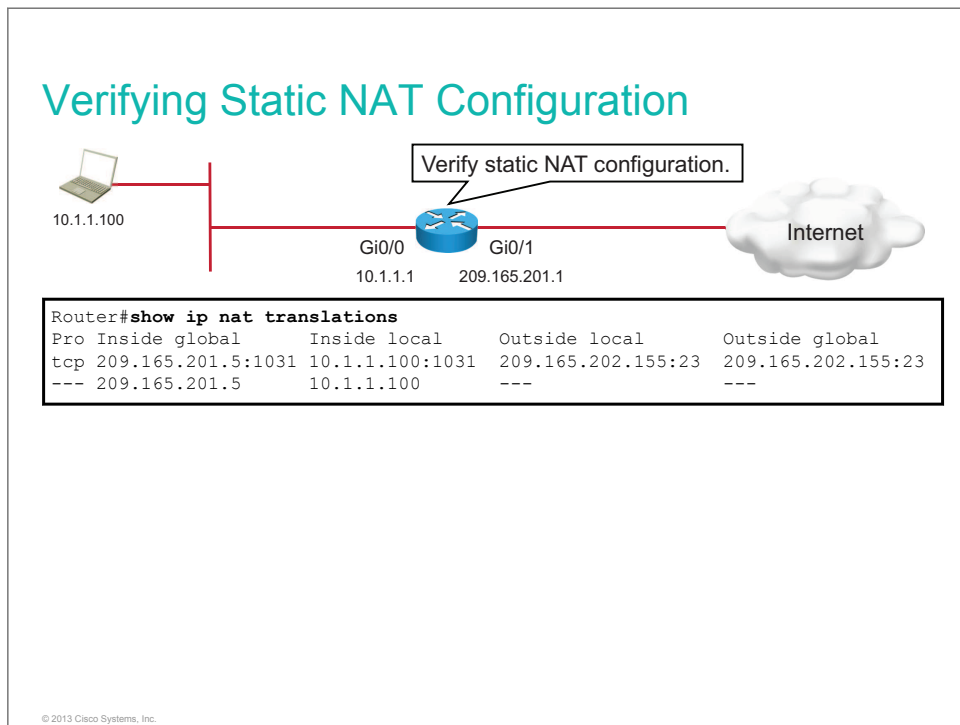
The figure shows the example of the commands for the steps. You enter static translations directly into the configuration. Unlike dynamic translations, these translations are always in the NAT table.

Command	Description
interface <i>interface</i>	Specifies an interface and enters interface configuration mode
ip address <i>address subnet_mask</i>	Sets the IP address and mask of the device
ip nat inside	Marks the interface as connected to the inside network
ip nat outside	Marks the interface as connected to the outside network
ip nat inside source static <i>inside_address outside_address</i>	Establishes a static translation between an inside local and inside global address

For more details about the **ip nat inside** and **ip nat outside** commands and related commands, check the *Cisco IOS IP Addressing Services Command Reference* at http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

Verifying Static NAT Configuration

This topic describes verifying static NAT.

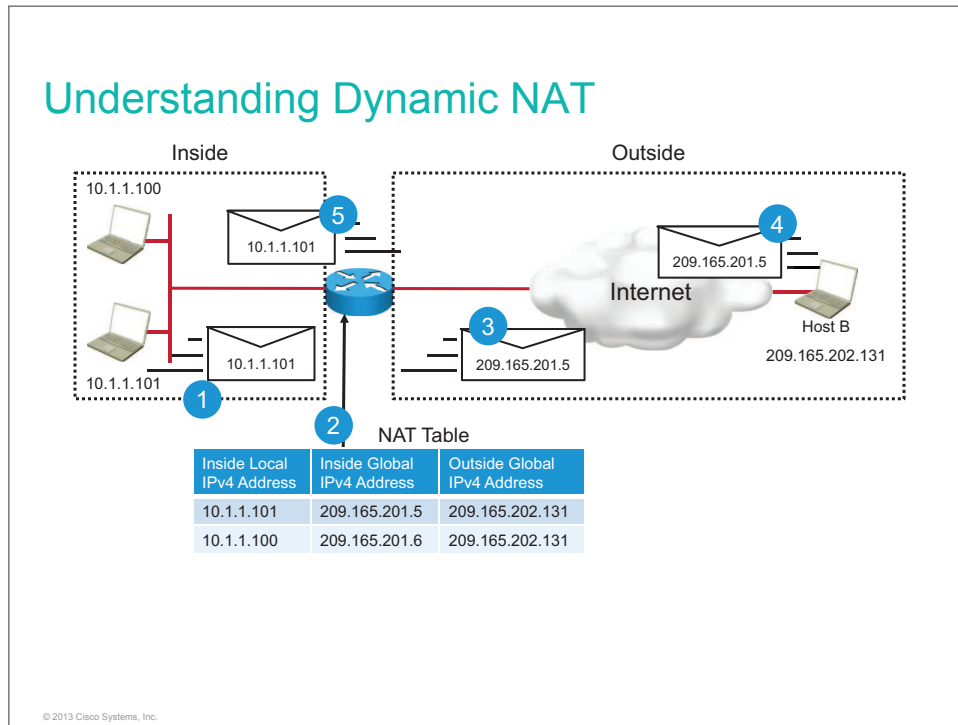


Command	Description
show ip nat translations	Displays active NAT translations.

For more details about the **ip nat inside**, **ip nat pool**, and **show ip nat translations** commands and related commands, check the *Cisco IOS IP Addressing Services Command Reference* at http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

Understanding Dynamic NAT

This topic describes how dynamic NAT functions.



While static NAT provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. These public IP addresses come from a NAT pool. Dynamic NAT configuration differs from static NAT, but it also has some similarities. Like static NAT, it requires the configuration to identify each interface as an inside or outside interface. However, rather than creating a static map to a single IP address, a pool of inside global addresses is used.

The figure illustrates a router that is translating a source address inside a network into a source address outside the network. These are the steps for translating an inside source address:

1. The users at hosts 10.1.1.100 and 10.1.1.101 want to open a connection to host B (IP address 209.165.202.131).
2. The first packet that the router receives from host 10.1.1.101 causes the router to check its NAT table. If no static translation entry exists, the router determines that the source address 10.1.1.101 must be translated dynamically. The router then selects a legal global address from the dynamic address pool and creates a translation entry (in this example, 209.165.201.5). This type of entry is called a *simple entry*. For the second host, 10.1.1.100, the router selects a legal global address from the dynamic address pool and creates a second translation entry (in this example, 209.165.201.6).
3. The router replaces the inside local source address of host 10.1.1.101 with the translated inside global address and forwards the packet.
4. Host B receives the packet and responds to host 209.165.201.5, using the inside global IPv4 destination address 209.165.201.5. When host B receives the second packet, it responds to host 209.165.201.6, using the inside global IPv4 destination address 209.165.201.6.

5. When the router receives the packet with the inside global IPv4 address of 209.165.201.5, the router performs a NAT table lookup using the inside global address as a key. The router then translates the address back to the inside local address of host 10.1.1.101 and forwards the packet to host 10.1.1.101. When the router receives the packet with the inside global IPv4 address of 209.165.201.6, the router performs a NAT table lookup using the inside global address as a key. The router then translates the address back to the inside local address of host 10.1.1.100 and forwards the packet to host 10.1.1.100.
6. Hosts 10.1.1.100 and 10.1.1.101 receive the packets and continue the conversation. The router performs Steps 2 through 5 for each packet.

Do Not Duplicate.
Post beta, not for release.

Configuring Dynamic NAT

This topic provides an example of configuring dynamic NAT.

Configuring Dynamic NAT

```

Router (config) #access-list 1 permit 10.1.1.0 0.0.0.255
Router (config) #ip nat pool NAT-POOL 209.165.201.5 209.165.201.10 netmask
255.255.255.240
Router (config) #interface GigabitEthernet 0/1
Router (config-if) #ip address 209.165.201.1 255.255.255.240
Router (config-if) #ip nat outside
Router (config-if) #exit
Router (config) #interface GigabitEthernet 0/0
Router (config-if) #ip address 10.1.1.1 255.255.255.0
Router (config-if) #ip nat inside
Router (config-if) #exit
Router (config) #ip nat inside source list 1 pool NAT-POOL
    
```

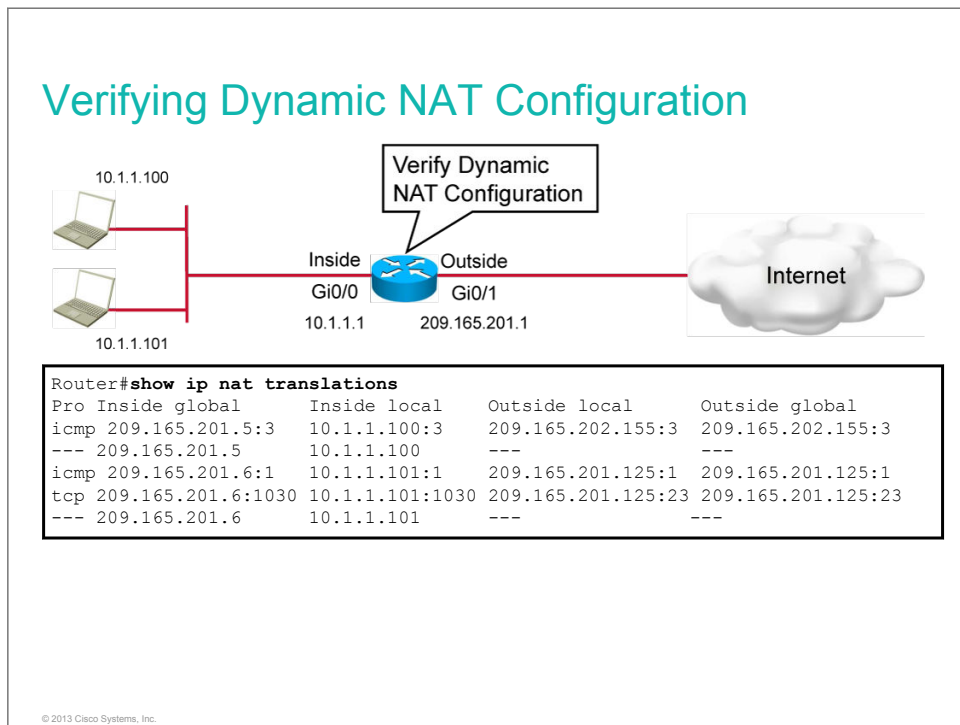
© 2013 Cisco Systems, Inc.

Command	Description
interface <i>interface</i>	Specifies an interface and enters interface configuration mode
ip nat pool <i>pool_name start_ip end_ip netmask netmask</i>	Defines an IP address pool
ip nat inside source list <i>acl_number pool pool_name</i>	Establishes a dynamic source translation by specifying the <u>ACL</u> and the address pool
ip address <i>address subnet_mask</i>	Sets the IP address and mask
ip nat inside	Marks the interface as connected to the inside network
ip nat outside	Marks the interface as connected to the outside network
access-list <i>acl_number permit ip_address netmask</i>	Creates an access list that defines the inside local addresses that are eligible to be translated

Note The ACL must permit only those addresses that need to be translated. Remember that there is an implicit **deny any** statement at the end of each ACL. An ACL that is too permissive can lead to unpredictable results. Using **permit any** can result in NAT consuming too many router resources, which can cause network problems.

Verifying Dynamic NAT Configuration

This topic describes an example of verifying NAT.

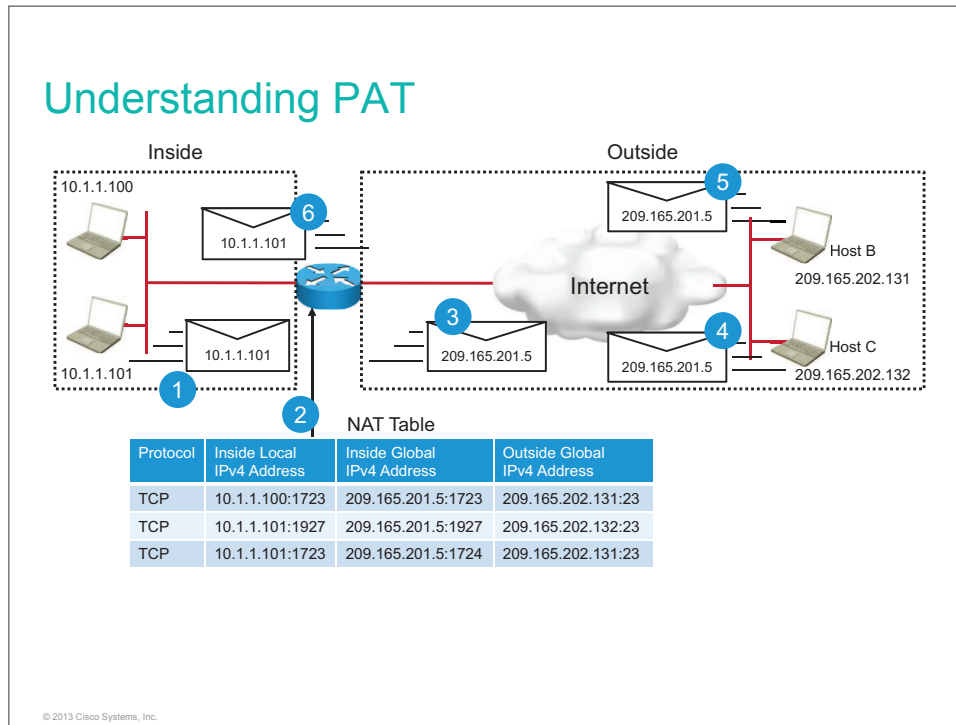


Command	Description
show ip nat translations	Displays active NAT translations.

For more details about the **ip nat inside**, **ip nat pool**, and **show ip nat translations** commands and related commands, check the *Cisco IOS IP Addressing Services Command Reference* at http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

Understanding PAT

This topic describes the operation of PAT.



One of the main forms of NAT is PAT, which is also referred to as *overload* in Cisco IOS configuration. Several inside local addresses can be translated using NAT into just one or a few inside global addresses by using PAT. Most home routers operate in this manner. Your ISP assigns one address to your router, yet several members of your family can simultaneously surf the Internet.

With NAT overload, multiple addresses can be mapped to one or a few addresses because a TCP or UDP port number tracks each private address. When a client opens a TCP/IP session, the NAT router assigns a port number to its source address. NAT overload ensures that clients use a different TCP or UDP port number for each client session with a server on the Internet. When a response comes back from the server, the source port number (which becomes the destination port number on the return trip) determines the client to which the router routes the packets. It also validates that the incoming packets were requested, thus adding a degree of security to the session.

- PAT uses unique source port numbers on the inside global IPv4 address to distinguish between translations. Because the port number is encoded in 16 bits, the total number of internal addresses that NAT can translate into one external address is, theoretically, as many as 65,536.
- PAT attempts to preserve the original source port. If the source port is already allocated, PAT attempts to find the first available port number. It starts from the beginning of the appropriate port group, 0 to 511, 512 to 1023, or 1024 to 65535 (in the figure, port 2031 is used). If PAT does not find an available port from the appropriate port group and if more than one external IPv4 address is configured, PAT moves to the next IPv4 address and tries to allocate the original source port again. PAT continues trying to allocate the original source port until it runs out of available ports and external IPv4 addresses.

NAT generally translates IP addresses only as a 1:1 correspondence between publicly exposed IP addresses and privately held IP addresses. NAT overload modifies the private IP address and potentially the port number of the sender. NAT overload chooses the port numbers that hosts see on the public network.

NAT routes incoming packets to their inside destination by referring to the incoming source IP address given by the host on the public network. With NAT overload, there is generally only one publicly exposed IP address (or a very few). Incoming packets from the public network are routed to their destinations on the private network by referring to a table in the NAT overload device that tracks public and private port pairs. This mechanism is called *connection tracking*.

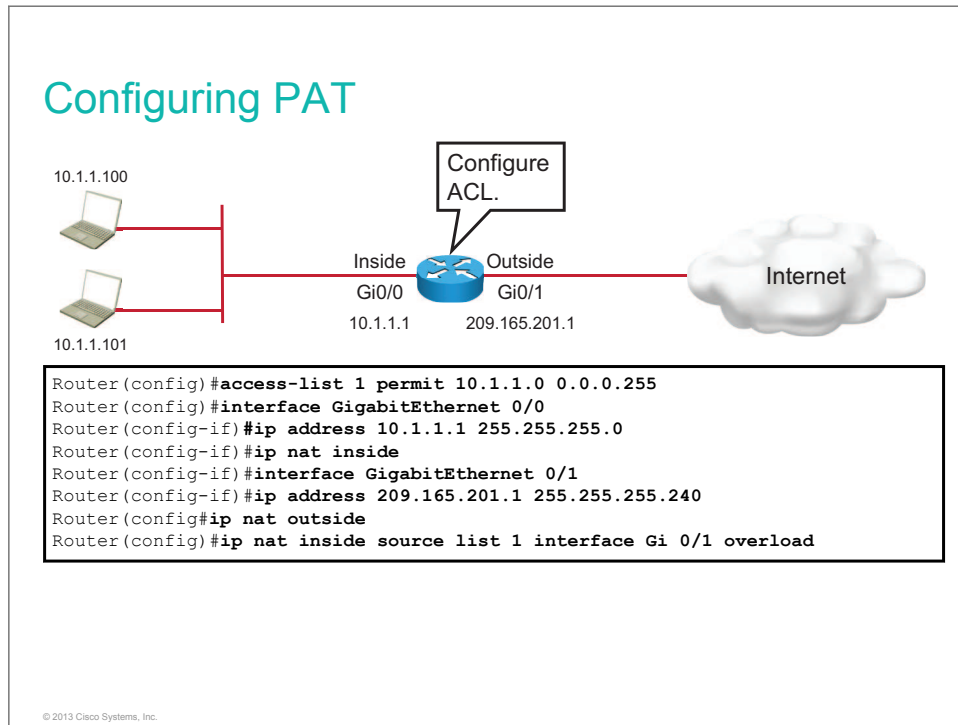
The figure illustrates PAT operation when one inside global address represents multiple inside local addresses. The TCP port numbers act as differentiators. Both hosts B and C think that they are talking to a single host at address 209.165.201.5. They are actually talking to different hosts, and the port number is the differentiator. In fact, many inside hosts could share the inside global IPv4 address by using many port numbers.

The router performs this process when it overloads inside global addresses:

1. The user at host 10.1.1.100 opens a connection to host B. A second user at host 10.1.1.101 opens a connection to host B and C.
2. The first packet that the router receives from host 10.1.1.100 causes the router to check its NAT table. If no translation entry exists, the router determines that address 10.1.1.100 must be translated and sets up a translation of inside local address 10.1.1.100 into a legal inside global address. If overloading is enabled and another translation is active, the router reuses the inside global address from that translation and saves enough information to be able to translate back. This type of entry is called an extended entry.
3. The router replaces the inside local source address 10.1.1.100 with the selected inside global address 209.165.201.5 and forwards the packet.
4. Host B receives the packet and responds to host 10.1.1.100, using the inside global IPv4 address 209.165.201.5. Host C receives a packet with the same inside global address, even though the packet originated from host 10.1.1.101.
5. When the router receives the packet with the inside global IPv4 address, the router performs a NAT table lookup. Using the inside global address and port and outside global address and port as a key, the router translates the address back into the correct inside local address, 10.1.1.100, and forwards the packet to host 10.1.1.100.
6. Host 10.1.1.100 receives the packet and continues the conversation. The router performs Steps 2 through 5 for each packet.

Configuring PAT

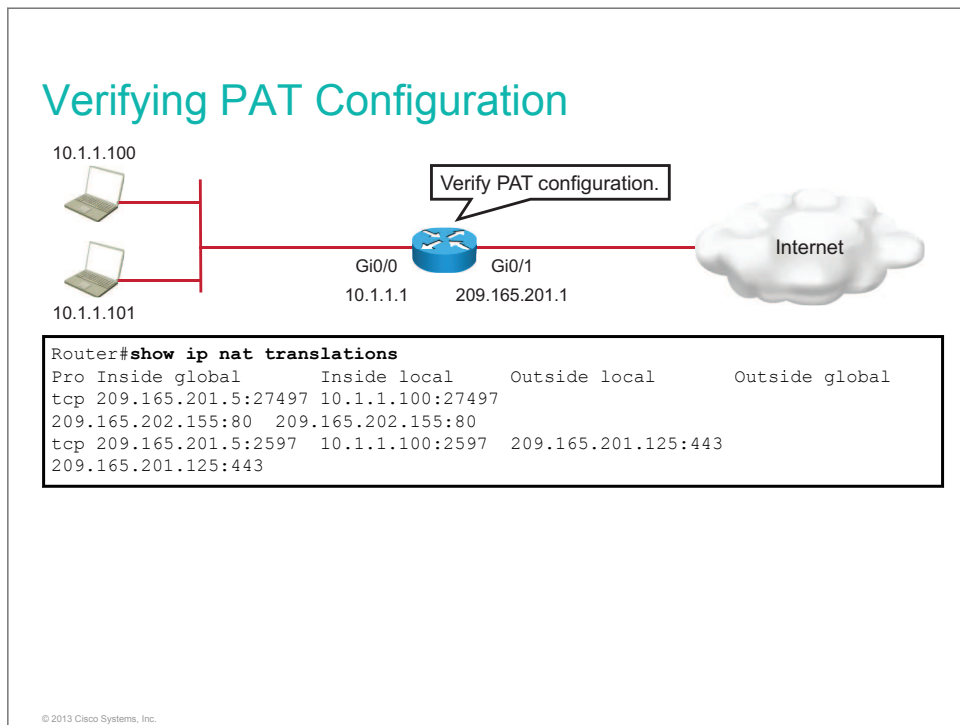
This topic describes an example of configuring PAT.



Command	Description
interface <i>interface</i>	Specifies an interface and enters interface configuration mode
ip address <i>address subnet_mask</i>	Sets the IP address and mask
ip nat inside	Marks the interface as connected to the inside network
ip nat outside	Marks the interface as connected to the outside network
ip nat inside source list <i>access-list-number</i> interface <i>interface</i> overload	Establishes dynamic source translation, specifying the ACL
access-list <i>acl_number</i> permit <i>ip_address netmask</i>	Creates an ACL that defines the inside local addresses that are eligible to be translated

Verifying PAT Configuration

This topic describes an example of verifying PAT.

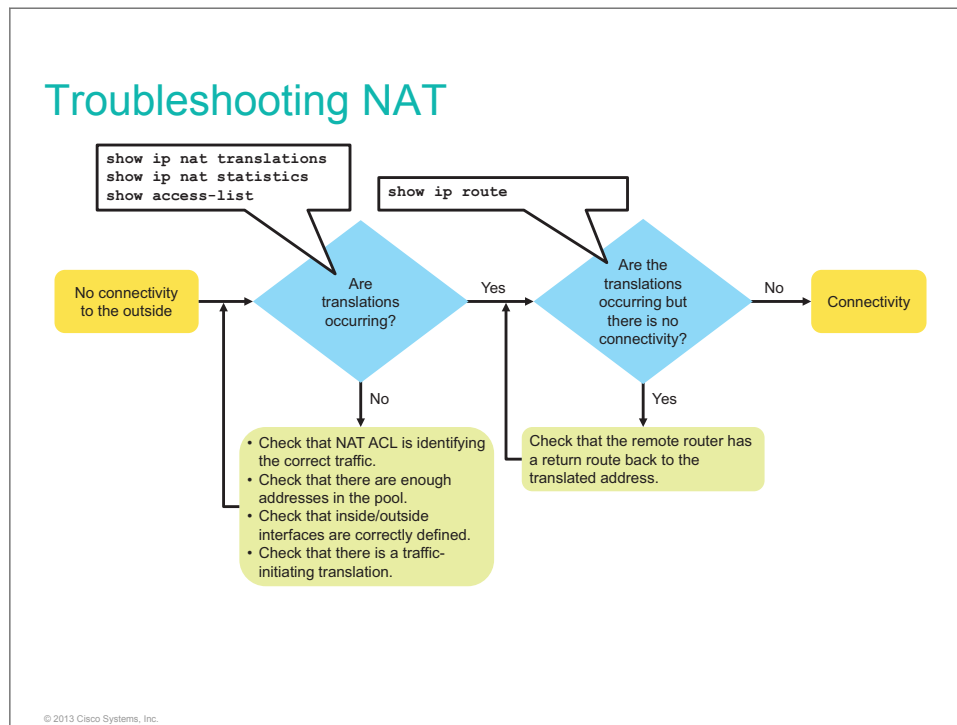


Command	Description
show ip nat translations	Displays active NAT translations.

For more details about the **ip nat inside**, **ip nat pool**, and **show ip nat translations** commands and related commands, check the *Cisco IOS IP Addressing Services Command Reference* at http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

Troubleshooting NAT

This topic describes how to troubleshoot NAT.



When you have IPv4 connectivity problems in a NAT environment, it is often difficult to determine the cause of the problem. NAT is often blamed, when in reality there is an underlying problem. When you are trying to determine the cause of an IPv4 connectivity problem, it helps to eliminate NAT as the problem. Follow these steps to verify that NAT is operating as expected:

1. Verify that translations are occurring:
 - Use the **show ip nat translations** command to determine if translations exist in the translation table.
 - Verify that the translation is actually occurring, by using the **show ip nat statistics** and **debug ip nat** commands.
 - Use the **show access-list** command to verify that the ACL associated with the NAT command is permitting all necessary networks.
 - Use the **show ip nat statistics** command to verify that the router interfaces are appropriately defined as NAT inside or NAT outside.
 - If some devices have connectivity but others do not, the NAT pool might be out of addresses.
2. If translations are occurring but there is no connectivity, use **show ip route** to verify that there is a return route to the translated address.

Troubleshooting NAT (Cont.)

Are Addresses Being Translated?

```
Router#show ip nat statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: Serial0
Inside Interfaces: Ethernet0 , Ethernet1
Hits: 42 Misses: 44
<output omitted>
```

- Monitors NAT statistics

```
Router#show access-list
access-list 1 permit 10.1.1.100 0.0.0.255
```

- Verifies that the NAT ACL is permitting all necessary networks

© 2013 Cisco Systems, Inc.

In a simple network environment, it is useful to monitor NAT statistics with the **show ip nat statistics** command. The **show ip nat statistics** command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number that have been allocated. However, in a more complex NAT environment, with several translations taking place, this **show** command may not clearly identify the issue. It may be necessary to run **debug** commands on the router.

Note You can use the **clear ip nat translation *** command to clear all dynamic address translation entries. By default, translation entries time out after 24 hours. When testing the NAT configuration, it can be useful to clear translations.

Troubleshooting NAT (Cont.)

- To display detailed dynamic data and events, you can use **debug** commands.
 - A **debug** command can intensively use device resources. Use carefully on production equipment.
 - Always turn off **debug** after troubleshooting with the **no debug all** command.

```
Router#debug ip nat
NAT*: s=10.1.1.100->209.165.201.1, d=172.16.1.100 [103]
NAT*: s=172.16.1.100, d=209.165.201.1->10.1.1.100 [103]
NAT*: s=10.1.1.100->209.165.201.1, d=172.16.1.100 [104]
NAT*: s=172.16.1.100, d=209.165.201.1->10.1.1.100 [104]
<output omitted>
```

- Displays information about every packet that is translated by the router.

© 2013 Cisco Systems, Inc.

Note

The **debug** command, especially the **debug all** command, should be used sparingly. These commands can disrupt router operations. The **debug** commands are useful when configuring or troubleshooting a network. However, they can make intensive use of CPU and memory resources. It is recommended that you run as few debug processes as necessary and disable them immediately when they are no longer needed. The **debug** commands should be used with caution on production networks because they can affect the performance of the device.

The **debug ip nat** command displays information about every packet that the router translates, which helps you to verify NAT operation. The **debug ip nat detailed** command generates a description of each packet that is considered for translation. This command also provides information about certain errors or exception conditions, such as the failure to allocate a global address. The **debug ip nat detailed** command generates more overhead than the **debug ip nat** command, but it can provide the detail that you need to troubleshoot the NAT problem. Always remember to turn off debugging when finished.

The figure shows a sample **debug ip nat** output. In the output, you can see that inside host 10.1.1.100 initiated traffic to outside host 209.165.202.131 and has been translated to address 209.165.201.5.

For decoding the **debug** output, note what the following symbols and values indicate:

- *: The asterisk next to "NAT" indicates that the translation is occurring in the fast-switched path. The first packet in a conversation is always process-switched, which is slower. The remaining packets go through the fast-switched path if a cache entry exists.
- s=: Refers to the source IP address.
- a.b.c.d->w.x.y.z: Indicates that source address a.b.c.d is translated to w.x.y.z.
- d=: Refers to the destination IP address.
- [xxx]: The value in brackets is the IP identification number. This information may be useful for debugging because it enables correlation with other packet traces from protocol analyzers.

Finally, you should make sure that the ACL that the NAT command references is permitting all of the necessary networks. Notice that ACLs use wildcard masks and not subnet masks.

Troubleshooting NAT (Cont.)

If translations are occurring, but there is no connectivity, verify that the remote router has a route to the translated address.



```
Branch#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 209.165.201.1 to network 0.0.0.0
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.2/32 is directly connected, GigabitEthernet0/0
C 209.165.201.0/27 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.201.1
```

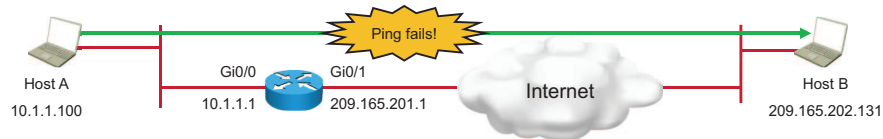
© 2013 Cisco Systems, Inc.

If the translations are occurring but a ping to the remote network still fails, the issue might be a missing route back to the translated address. This problem can arise in NAT between a headquarters and branch office. It is usually not an issue when connecting to an ISP, because the service provider takes care of routing all of the necessary traffic back to the customer.

Troubleshooting NAT Case Study

Troubleshooting NAT Case Study

Host A and host B are unable to ping after a new NAT configuration is put in place.



© 2013 Cisco Systems, Inc.

The figure shows that host A (10.1.1.100) cannot ping host B (209.165.202.131). Relevant part of configuration is shown in the **show running-config** output.

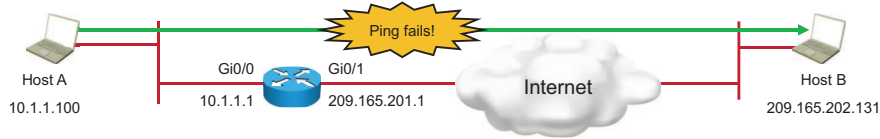
Troubleshooting NAT Case Study (Cont.)

```
Router#show running-config
<output omitted>
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
access-list 20 permit 0.0.0.0 255.255.255.0
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
!
interface GigabitEthernet0/1
 ip address 209.165.200.1 255.255.255.254
 ip nat inside
!
ip nat inside source list 20 interface GigabitEthernet0/1 overload
```

© 2013 Cisco Systems, Inc.

Troubleshooting NAT Case Study (Cont.)

Translations are not occurring.



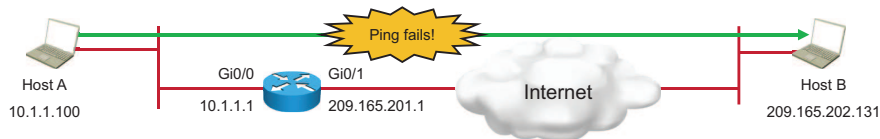
```
Router#show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
```

© 2013 Cisco Systems, Inc.

To troubleshoot the problem, you use the **show ip nat translation** command to see if any translations are currently in the table. You find that no translations are in the table.

Troubleshooting NAT Case Study (Cont.)

The router interfaces are incorrectly defined as NAT inside and NAT outside.



```
Router#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
GigabitEthernet0/0
Inside interfaces:
GigabitEthernet0/1
<output omitted>
```

© 2013 Cisco Systems, Inc.

Troubleshooting NAT Case Study (Cont.)

How to fix configuration:

```
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface GigabitEthernet 0/1
Router(config-if)#ip nat outside
```

© 2013 Cisco Systems, Inc.

Next, you must determine whether any translations have ever taken place and identify the interfaces between which translation should be occurring. You use the **show ip nat statistics** command.

As shown in the example, you determine that the NAT counters are at 0, verifying that no translation has occurred. You also find that the router interfaces are incorrectly defined as NAT inside or NAT outside. The output also shows how to fix configuration.

Troubleshooting NAT Case Study (Cont.)

Verify that the access list is correct.



```
RouterA#show access-list
Standard IP access list 20
 10 permit 0.0.0.0, wildcard bits 255.255.255.0
```

How to fix access list:

```
Router#config terminal
Router(config)#no access-list 20
Router(config)#access-list 20 permit 10.1.1.0 0.0.0.255
```

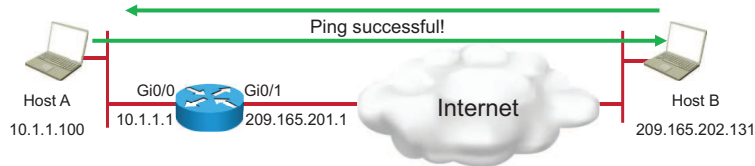
© 2013 Cisco Systems, Inc.

After you correctly define the NAT inside and outside interfaces, you generate another ping from host A to host B. The ping still fails. To troubleshoot the problem, you use the **show ip nat translations** and **show ip nat statistics** commands again. You find that translations are still not occurring.

Next, you use the **show access-list** command to determine whether the ACL that the NAT command references is permitting all of the necessary networks. You determine that an incorrect wildcard bit mask has been used in the ACL that defines the addresses that need to be translated.

Troubleshooting NAT Case Study (Cont.)

Verify that translations are occurring and you have connectivity to the remote network.



```
Router#ping 209.165.202.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.131, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.201.1:1  10.1.1.100:1     209.165.202.131:1 209.165.202.131:1
```

© 2013 Cisco Systems, Inc.

After you correct the wildcard mask, you generate another ping from host A to host B. The connectivity test is now a success. You issue the **show ip nat translations** command to verify the translation.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Provider-assigned IP addresses can be configured on a router statically or can be dynamically assigned through DHCP.
- A DHCP client is a host that requests an IP address and configuration from a DHCP server.
- A DHCP server allocates network addresses and delivers configurations.

© 2013 Cisco Systems, Inc.

Summary (Cont.)

- NAT enables private IP internetworks that use private IP addresses to connect to the Internet. PAT, or NAT overload, a feature of NAT, enables several internal addresses to be translated to only one or a few external addresses.
- Static NAT is one-to-one address mapping. Dynamic NAT addresses are picked from a pool.
- PAT allows you to map many inside addresses to one outside address.
- Use the **show ip nat translations** command to display the translation table and verify that translation has occurred.
- To determine whether a current translation entry is being used, use the **show ip nat statistics** command to check the hits counter.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- IP is a Layer 3 media-independent connectionless protocol that uses hierarchical logical addressing and provides best-effort service.
- Internet hosts require a unique public IP address. Hosts in private networks can have any valid private IP address that is unique locally in each network.
- Networks, particularly large networks, are often divided into smaller subnetworks, or subnets. Subnets can improve network performance and control.
- TCP is a connection-oriented protocol that provides reliable transport. UDP is a connectionless transport protocol that provides best-effort transport.

Module Summary (Cont.)

- The main function of a router is to relay packets from one network device to another. To do this, you must define the characteristics of the interfaces through which packets are received and sent. Interface characteristics, such as the IP address, are configured in interface configuration mode.
- Cisco Discovery Protocol is an information-gathering tool that is used by network administrators to obtain information about directly connected devices.
- Static routers use a route that a network administrator manually enters into the router. Dynamic routers use a route that a network routing protocol adjusts automatically for topology or traffic changes.

© 2013 Cisco Systems, Inc.

Module Summary (Cont.)

- ACLs can be used as a Cisco IOS tool to identify traffic that receives special handling.
- NAT enables private IP internetworks that use private IP addresses to connect to the Internet. PAT, a feature of NAT, enables several internal addresses to be translated to one external address or a few external addresses.

© 2013 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. How many bits are in an IPv4 address? (Source: Understanding the TCP/IP Internet Layer)
 - A. 4
 - B. 8
 - C. 16
 - D. 32
 - E. 64
 - F. 128
2. Which characteristic is similar in TCP and UDP? (Source: Understanding the TCP/IP Transport Layer)
 - A. operates at the transport layer of the OSI model and the TCP/IP stack
 - B. capable of performing error checking
 - C. provides service on a best-effort basis and does not guarantee packet delivery
 - D. provides no special features that recover lost or corrupted packets
3. What is the purpose of a router? (Source: Exploring the Functions of Routing)
 - A. to interconnect networks and choose the best paths between them
 - B. to provide the connection points for the media
 - C. to serve as the endpoint in the network, sending and receiving data
 - D. to provide the means by which signals are transmitted from one networked device to another

4. TCP is best for which two applications? (Choose two.) (Source: Understanding the TCP/IP Transport Layer)
- A. email
 - B. voice streaming
 - C. downloading
 - D. video streaming
5. Match each IPv4 address type with its description. (Source: Understanding the TCP/IP Internet Layer)
- A. local broadcast address only used as source address until valid IP is obtained
 - B. directed broadcast address used to address all devices in local network
 - C. loopback address special address for each network that allows communication to all of the hosts in that network
 - D. all zeros address used to let the system send a message to itself for testing
6. Which network does a host with an IP address of 10.44.45.46/23 belong to? (Source: IP Addressing and Subnets)
- A. 10.44.45.45
 - B. 10.44.45.0
 - C. 10.44.44.0
 - D. 10.44.0.0
7. Match the numerical addresses with their descriptions for network 192.168.4.0/24. (Source: Understanding IP Addressing and Subnets)
- A. last host address 192.168.4.255
 - B. broadcast address 192.168.4.254
 - C. next network address 192.168.4.1
 - D. first host address 192.168.4.0
 - E. network address 192.168.5.0
8. Match the types of routes with their descriptions. (Source: Exploring the Functions of Routing)
- A. default routes The router learns about them automatically through a routing protocol.
 - B. directly connected networks The system administrator manually enters them into the configuration of a router.
 - C. static routes This entry comes from having router interfaces that are directly attached to network segments.
 - D. dynamic routes They are used when no explicit path to a destination is found in the routing table.

9. Which two statements about Cisco Discovery Protocol are correct? (Choose two.) (Source: Configuring a Cisco Router)
- A. It was developed by the IETF.
 - B. It gathers information about directly connected Cisco switches, routers, and other Cisco devices.
 - C. If two neighbor devices have misconfigured IP addresses, they will still learn about each other through this protocol.
 - D. The original name of the protocol was Connected Discovery Protocol.
10. Which two statements correctly describe MAC addresses? (Choose two.) (Source: Exploring the Packet-Delivery Process)
- A. Ethernet uses MAC addresses.
 - B. They are used for addressing at the TCP/IP internet layer.
 - C. A MAC address is a 32-bit binary value.
 - D. The MAC address identifies end devices in a LAN.
11. Which two statements correctly describe ARP? (Choose two.) (Source: Exploring the Packet-Delivery Process)
- A. resolves IP addresses to MAC addresses
 - B. resolves MAC addresses to IP addresses
 - C. has an expiration period for entries in the ARP table, usually 300 seconds for PCs
 - D. is turned off by default on Cisco switches
12. In which three situations would you use static routing? (Choose three.) (Source: Enabling Static Routing)
- A. when the network is large
 - B. when the network is expected to scale
 - C. in a small network that requires simple routing
 - D. in a hub-and-spoke network topology
 - E. when you want to quickly create an ad hoc route
13. Which command syntax correctly configures a default route? (Source: Enabling Static Routing)
- A. **ip default-route 172.16.0.1**
 - B. **ip default-route 0.0.0.0 0.0.0.0 172.16.0.1**
 - C. **ip route 0.0.0.0 0.0.0.0 172.16.0.1**
 - D. **ip route 172.16.0.1**
14. Which two statements correctly identify ACLs? (Choose two.) (Source: Managing Traffic Using ACLs)
- A. have an implicit deny all at the bottom of each ACL
 - B. are consulted in a bottom-to-top order
 - C. use wildcard masks
 - D. can be used only for filtering

15. Which command syntax correctly describes an ACL that permits all hosts from subnet 10.1.0.0/16? (Source: Managing Traffic Using ACLs)
- A. **access-list 10.1.1.0 0.0.255.255**
 - B. **access-list 1 permit 10.1.0.0 255.255.0.0**
 - C. **access-list 1 deny 10.1.0.0 0.0.255.255**
 - D. **access-list 1 permit 10.1.0.0 0.0.255.255**
16. Which two statements correctly describe NAT? (Choose two.) (Source: Enabling Internet Connectivity)
- A. The total number of internal addresses that NAT can translate into one external address is 128.
 - B. PAT uses unique source port numbers on the inside global IPv4 address to distinguish between translations.
 - C. Static, dynamic, and automatic are three NAT types.
 - D. Private users can access the Internet by sharing one or more public IP addresses.

Do Not Duplicate.
Post beta, not for release.

Answer Key

1. D
2. A
3. A
4. A, C
5.

A. local broadcast address	used to address all devices in local network
B. directed broadcast address	special address for each network that allows communication to all of the hosts in that network
C. loopback address	used to let the system send a message to itself for testing
D. all zeros address	only used as source address until valid IP is obtained
6. C
7.

A. network address	192.168.4.0
B. broadcast address	192.168.4.255
C. first host address	192.168.4.1
D. last host address	192.168.4.254
E. next network address	192.168.5.0
8.

A. directly connected networks	This entry comes from having router interfaces that are directly attached to network segments.
B. static routes	The system administrator manually enters them into the configuration of a router.
C. dynamic routes	The router learns about them automatically through a routing protocol.
D. default routes	They are used when no explicit path to a destination is found in the routing table.
9. B, C
10. A, D
11. A, C
12. C, D, E
13. C
14. A, C

15. D

16. B, D

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate:
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Managing Network Device Security

This module describes the steps that are required to secure local and remote access to network devices. It provides general recommendations for improving device hardening. It describes how network devices can control traffic on the network. It explains ACLs and their use for traffic filtering and shows configuration examples.

Objectives

Upon completing this module, you will be able to meet these objectives:

- Implement a basic security configuration
- Implement basic steps to harden network devices
- Implement standard, extended, numbered, and named ACLs to filter traffic

Do Not Duplicate.
Post beta, not for release.

Securing Administrative Access

Overview

After physical access has been enabled, you must ensure that access to the switch via the console port and the vty ports is secure. You must also filter access to network devices from remote or internal locations.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- List the actions that are required to secure a network device
- Secure access to privileged EXEC mode
- Secure console access to a network device
- Secure remote access to a network device
- Enable remote access connectivity on a switch
- Limit remote access with an ACL
- Explain why external authentication should be used
- Configure a login banner

Network Device Security Overview

This topic describes common threats to network device security.

Network Device Security Overview

Network devices are vulnerable to these common threats:

- Remote access threats
 - Unauthorized remote access
- Local access and physical threats
 - Damage to equipment
 - Password recovery
 - Device theft
- Environmental threats
 - Extreme temperature
 - High humidity
- Electrical threats
 - Insufficient power supply voltage
 - Voltage spikes
- Maintenance threats
 - Improper handling
 - Poor cabling
 - Inadequate labeling

© 2013 Cisco Systems, Inc.

Common threats to network device security and mitigation strategies can be summarized as follows:

- **Remote access threats:** Unauthorized remote access is a threat when security is weak in remote access configuration. Mitigation techniques for this type of threat include configuring strong authentication and encryption for remote access policy and rules, configuration of login banners, use of ACLs, and VPN access.
- **Local access and physical threats:** Threats include physical damage to network device hardware, password recovery that is allowed by weak physical security policies, and device theft. Mitigation techniques for this type of threat include locking the wiring closet and allowing access only by authorized personnel and blocking physical access through a dropped ceiling, raised floor, window, duct work, or other possible point of entry. Use electronic access control, and log all entry attempts. Monitor facilities with security cameras.
- **Environmental threats:** Temperature extremes (heat or cold) or humidity extremes (too wet or too dry) can present a threat. Mitigation techniques for this type of threat include creating the proper operating environment through temperature control, humidity control, positive air flow, remote environmental alarms, and recording and monitoring.
- **Electrical threats:** Voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss are potential electrical threats. Mitigation techniques for this type of threat include limiting potential electrical supply problems by installing UPS systems and generator sets, following a preventative maintenance plan, installing redundant power supplies, and using remote alarms and monitoring.
- **Maintenance threats:** These threats include improper handling of important electronic components, lack of critical spare parts, poor cabling, and inadequate labeling. Mitigation techniques for this type of threat include using neat cable runs, labeling critical cables and components, stocking critical spares, and controlling access to console ports.

Securing Access to Privileged EXEC Mode

This topic describes how to configure access to privileged EXEC mode.

Securing Access to Privileged EXEC Mode

Configuring enable password:

```
Switch(config)# enable password C1sco123
```

Configuring enable secret password:

```
Switch(config)# enable secret sanfran
```

Verification of configured passwords:

```
Switch# show running-config | include enable
enable secret 5 $1$WPHF$uWo4ucV0/vA1/abu6LlWQ1
enable password C1sco123
```

© 2013 Cisco Systems, Inc.

Securing Access to Privileged EXEC Mode (Cont.)

Encrypting plaintext passwords:

```
Switch(config)# service password-encryption
Switch(config)# exit
Switch# show running-config | include enable
enable secret 5 $1$vWZa$2sYQLDv4R4xMtU5NFDrbX.
enable password 7 04785A150C2E1D1C5A
```

© 2013 Cisco Systems, Inc.

You can secure a switch by using passwords to restrict access. Using passwords and assigning privilege levels is a way to provide terminal access control in a network and is a form of management-plane hardening. Passwords can be established on individual lines, such as the console, and to privileged EXEC mode. Passwords are case-sensitive.

Note The passwords that are shown in the figure are for instructional purposes only. Passwords that are used in an actual implementation should meet the requirements for strong passwords.

The **enable password** global command restricts access to privileged EXEC mode. You can assign an encrypted form of the enable password, called the enable secret password, by entering the **enable secret password** command with the desired password at the global configuration mode prompt. When the enable secret password is configured, it is used instead of the enable password rather than in addition to it.

You can also add a further layer of security, which is particularly useful for passwords that cross the network or are stored on a TFTP server. Cisco provides a feature that allows the use of encrypted passwords. To set password encryption, enter the **service password-encryption** command in global configuration mode.

Passwords that are displayed or set after you configure the **service password-encryption** command will be encrypted. Service password encryption uses type-7 encryption, which is not very secure. There are several tools and web pages available that convert an encrypted password into a plaintext string.

On the other hand, the **enable secret** command uses MD5-type encryption that, to this point, has not been broken. It is recommended that you use always use the **enable secret** secret password instead of the **enable password** command.

Note Although the **enable password** command can be encrypted with the **service password-encryption** command, the encryption is weak and has been broken with cracker programs available online. However, the enable secret password uses MD5-type encryption that, to this point, has not been broken. It is recommended that you use the **enable secret** secret password, not the **enable password** command.

Securing Console Access

This topic describes how to secure console access.

Securing Console Access

Console password:

```
Switch(config)# line console 0
Switch(config-line)# login
Switch(config-line)# password C1sco123
```

EXEC timeout:

```
Switch(config-line)# exec-timeout 5
```

© 2013 Cisco Systems, Inc.

Use the **line console 0** command followed by the **password** and **login** subcommands to require login and establish a login password on a console terminal or vty port. By default, logging in is not enabled on console or vty ports.

Note Enter the **service password-encryption** command in global configuration mode to encrypt the console password. Although this encryption is weak and can be easily decrypted, it is still better than a cleartext password. At least you are protected against exposing the password to casual observers.

The **exec-timeout** command prevents users from remaining connected to a console port when they leave a station. In the example, when no user input is detected on the console for 5 minutes, the user that is connected to the console port is automatically disconnected.

Note The EXEC timeout will be left at 60 in the lab for lab purposes.

Securing Remote Access

This topic describes how to secure remote access.

Securing Remote Access

Virtual terminal password:

```
Switch(config)# line vty 0 15
Switch(config-line)# login
Switch(config-line)# password CiScO
```

EXEC timeout:

```
Switch(config-line)# exec-timeout 5
```

© 2013 Cisco Systems, Inc.

Securing Remote Access (Cont.)

Configuring SSH:

```
Switch(config)# hostname SwitchX
SwitchX(config)# ip domain-name cisco.com
SwitchX(config)# username user1 secret CIsco123
SwitchX(config)# crypto key generate rsa modulus 1024
The name for the keys will be: SwitchX.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
SwitchX(config)# line vty 0 15
SwitchX(config-line)# login local
SwitchX(config-line)# transport input ssh
SwitchX(config-line)# exit
SwitchX(config)# ip ssh version 2
```

© 2013 Cisco Systems, Inc.

The **line vty 0 15** command, followed by the **login** and **password** subcommands, requires login and establishes a login password on incoming Telnet sessions.

The **login local** command can be used to enable password checking on a per-user basis using the username and secret password that are specified with the **username** global configuration command. The **username** command establishes username authentication with encrypted passwords.

The **exec-timeout** command prevents users from remaining connected to a vty port when they leave a station. In the example, when no user input is detected on a vty line for 5 minutes, the vty session is automatically disconnected.

To configure SSH on a Cisco switch or router, you need to complete the following steps:

- Use the **hostname** command to configure the host name of the device so that it is not *Switch* (on a Cisco switch) or *Router* (on a Cisco router).
- Configure the DNS domain with the **ip domain name** command. The domain name is required to be able to generate certificate keys.
- Generate RSA keys to be used in authentication with the **crypto key generate rsa** command.
- Configure the user credentials to be used for authentication. By specifying the **login local** command for vty lines, you are essentially telling the network device to use locally defined credentials for authentication. Configure locally defined credentials using the **username username secret password** command.
- (Optional) You can also limit access to a device to users that use SSH and block Telnet with the **transport input ssh** vty mode command. If you want to support login banners and enhanced security encryption algorithms, force SSH version 2 on your device with the **ssh version 2** command in global configuration mode.

Securing Remote Access (Cont.)

Verify that SSH is enabled:

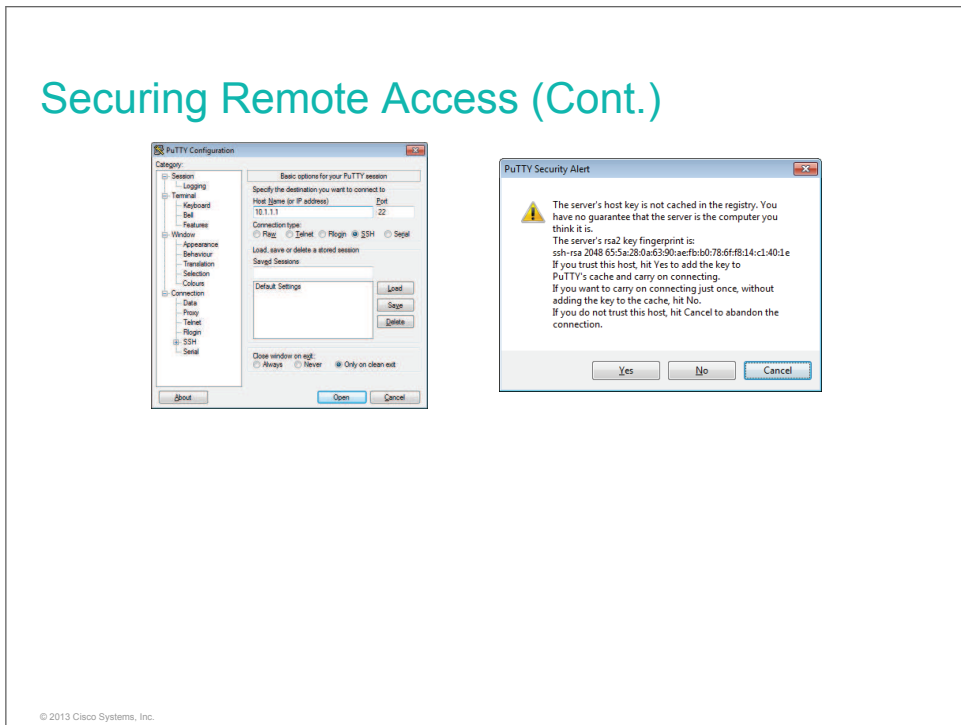
```
Switch# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

Check the SSH connection to the device:

```
Switch# show ssh
Connection  Version  Encryption  State          Username
0           1.5     3DES        Session started  cisco
```

© 2013 Cisco Systems, Inc.

Securing Remote Access (Cont.)



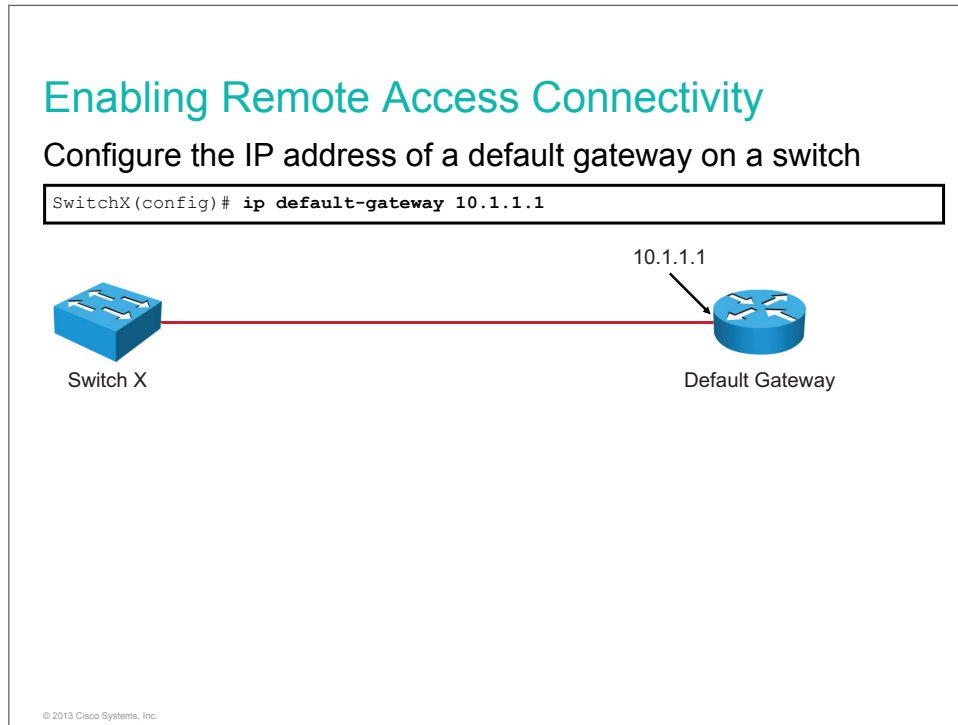
You can establish an SSH connection to the SSH-enabled device (a switch, in this example) using an SSH client on your PC, such as PuTTY. When you establish a connection for the first time from a specific computer, you are presented with a security alert window that indicates that the server host key is not cached in the PuTTY cache. By adding a key to the cache, you will avoid seeing this security alert window every time that you establish an SSH connection from this computer.

To display the version and configuration data for SSH on the device that you configured as an SSH server, use the **show ip ssh** command. In the example, SSH version 2 is enabled.

To check the SSH connection to the device, use the **show ssh** command.

Enabling Remote Access Connectivity

This topic describes how to enable remote access connectivity by configuring the IP address of a default gateway for a switch.



To configure the switch so that it can be accessed remotely, a default gateway is needed. To configure a default gateway for the switch, use the **ip default-gateway** command. Enter the IP address of the next-hop router interface (10.1.1.1) that is directly connected to the switch where a default gateway is being configured.

Once the default gateway is configured, the switch sends packets for all unknown IP destinations to the configured gateway, which enables switch connectivity with distant networks.

Limiting Remote Access with ACLs

This topic describes how to limit remote access to vty lines.

Limiting Remote Access with ACLs

Use an ACL to permit Telnet access from 10.1.1.0 /24 but deny everybody else:

```
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# access-list 1 deny any log
```

Apply the ACL on vty lines:

```
Router(config)# line vty 0 15
Router(config-line)# access-class 1 in
```

© 2013 Cisco Systems, Inc.

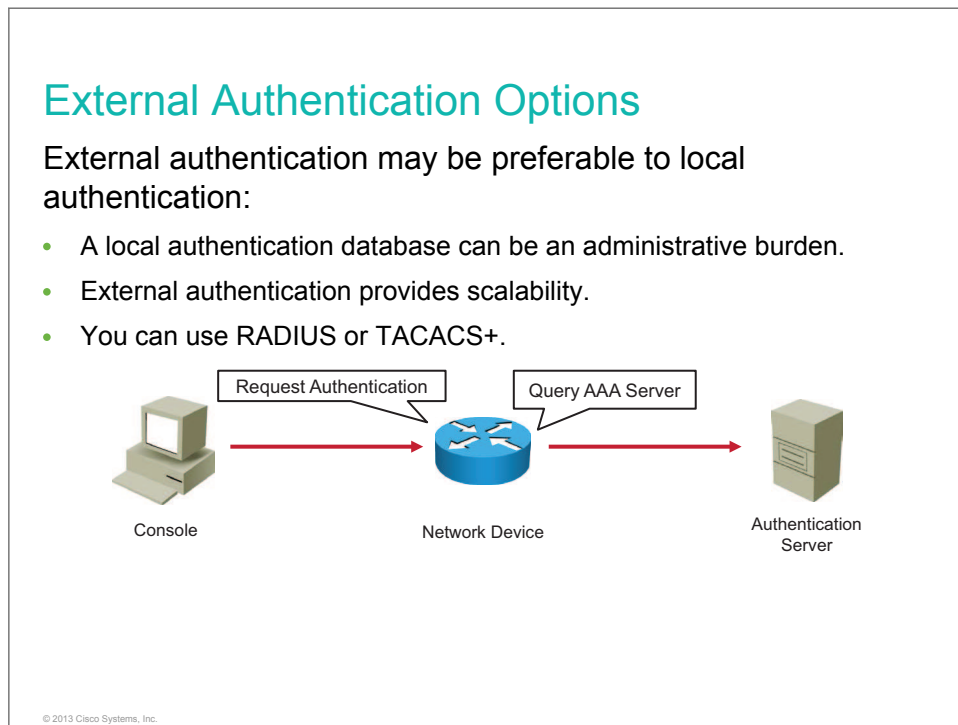
You can limit access to vty lines to specific IP addresses or subnets in order to control remote administration of network devices. Remote administration is commonly run over a Telnet or SSH connection, where the SSH connection is an encrypted communication channel between the administrator workstation and the device.

There are commonly two steps that you must complete to limit remote access with ACLs:

- **Configure an ACL:** The example shows an ACL that is being configured with two lines. The first line permits Telnet access from network addresses in the 10.1.1.0 /24 subnet. The second line is not mandatory because there is an implicit deny statement at the end of every ACL, but creating an explicit deny statement and appending the **log** keyword allows you to monitor attempts to access the device by unauthorized sources.
- **Apply the ACL to the lines:** The **access-class** command applies the ACL on vty lines. Using the **in** keyword after the name of the ACL tells the router to limit vty connections coming into the network device.

External Authentication Options

This topic describes external authentication options for remote administration of network devices.



In a small network, local authentication is often used. When you have more than a few user accounts in a local device database, managing those user accounts becomes more complex. For example, if you have 100 network devices, adding one user account means that you have to add this user account on all 100 devices in the network. Also, when you add one network device to the network, you have to add all user accounts to the local device database to enable all users to access this device.

AAA is a security architecture for distributed systems that enables control over which users are allowed access to certain services and how much of the resources they have used.

The two most popular options for external authentication of users are RADIUS and TACACS+:

- RADIUS is an open standard with low use of CPU resources and memory. It is used by a range of network devices, such as switches, routers, and wireless devices.
- TACACS+ is a security mechanism that enables modular AAA services. It uses a TACACS+ daemon running on a security server.

Note The details about AAA, RADIUS, and TACACS+ are out of the scope of this course.

Configuring the Login Banner

This topic describes how to configure a banner message that appears when a user tries to log into a Cisco IOS network device.

Configuring the Login Banner

Configure a login banner:

```
Switch(config)# banner login "Access for authorized users only. Please enter your username and password."
```

A user connecting to the device sees this message:

```
Access for authorized users only. Please enter your username and password.
User Access Verification
Username:
```

© 2013 Cisco Systems, Inc.

You can define a customized login banner to be displayed before the username and password login prompts. To configure a login banner, use the **banner login** command in global configuration mode. Enclose the banner text in quotation marks or use a delimiter that is different from any character appearing in the banner string.

Note Use caution when you create the text that is used in the login banner. Words like “welcome” may imply that access is not restricted and may allow hackers some legal defense of their actions.

To define and enable an MOTD banner, use the **banner motd** command in global configuration mode. To delete the MOTD banner, use the **no** form of this command.

This MOTD banner is displayed to all terminals that are connected and is useful for sending messages that affect all users (such as impending system shutdowns).

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Security threats to network devices include remote access threats, physical and local access threats, environmental threats, electrical threats, and maintenance threats.
- You can secure a network device by using passwords to restrict access.
- You can secure console access to a network device by using console passwords and by using an EXEC timeout setting to prevent access from connected terminals.
- You can secure a network device for Telnet and SSH access by using vty passwords to restrict access and an EXEC timeout setting to prevent access from connected terminals.
- You can secure a network device for Telnet and SSH access by using an ACL to limit the users who can access the device.
- If you want a scalable option instead of a local authentication database, use the RADIUS or TACACS+ external authentication service.
- Use the **banner** command to configure a login or MOTD banner.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Implementing Device Hardening

Overview

This lesson first describes the need for securing unused ports. It presents port security as a solution to the problem of maintaining control of utilized ports. The need to disable unused services is illustrated, and configuration examples show how to disable them. The last part of this lesson explains why correct system time is important and what can happen if the system time is not correct. NTP is introduced with a configuration example.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Secure unused ports
- Describe port security
- Configure port security
- Verify port security
- Disable unused services
- Describe NTP
- Configure basic NTP
- Verify NTP

Securing Unused Ports

This topic describes the need to secure unused ports.

Securing Unused Ports

- Unsecured ports can create a security vulnerability.
- A device that is plugged into an unused port is added to the network.
- Unused ports can be secured by disabling interfaces (ports).

© 2013 Cisco Systems, Inc.

Unused ports on a switch can be a security risk. A hacker can plug a switch into an unused port and become part of the network. Therefore, unsecured ports can create a security hole.

A simple method that many administrators use to help secure their network from unauthorized access is to disable all unused ports on a network switch.

Disabling an Interface (Port)

To shut down multiple ports, use the **interface range** command and use the **shutdown** command.

```
SwitchX(config)# interface range FastEthernet0/1 - 3
SwitchX(config-if-range)# shutdown
```

```
SwitchX# show running-config
<output omitted>
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
<output omitted>
```

The Fa0/1, Fa0/2, and Fa0/3 interfaces are disabled in the example.

© 2013 Cisco Systems, Inc.

For example, imagine that the Cisco switch has 24 ports. If there are three Fast Ethernet connections in use, practicing good security demands that you disable the 21 unused ports.

It is simple to disable multiple ports on a switch. Navigate to each unused port and issue the Cisco IOS **shutdown** command. An alternate way to shut down multiple ports is to use the **interface range** command. If a port needs to be activated, you can manually enter the **no shutdown** command on this interface.

The process of enabling and disabling ports can become a tedious task, but the enhanced security on your network is well worth the effort.

Do Not Duplicate:
Post beta, not for release.

Port Security

This topic describes port security, which is a mechanism to protect ports in use on switches.

Port Security

- How do you secure used ports?
- How do you prevent users from connecting unauthorized host devices to the network?

Example scenario:

- A classroom with PCs is connected to the network.
- How would you prevent students from unplugging classroom PCs and connecting their own notebooks to the network?

© 2013 Cisco Systems, Inc.

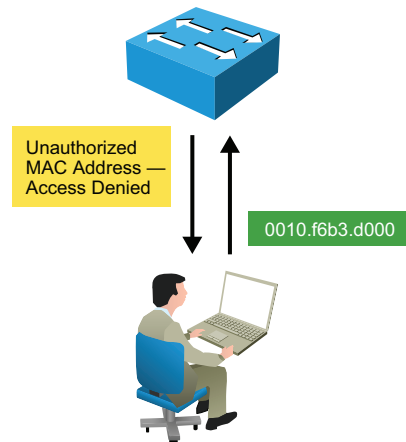
Having control over used ports on the switch is as important as securing unused ports. While unused ports on a switch can easily be secured by putting them into the shutdown state, securing ports in use presents a different challenge. When securing used ports on the switch, you need a control over which kind of devices are connected to the switch and have access to the network.

In the example scenario of a classroom environment, you will normally find PCs that are connected to the network to enable students access to online exercises. To prevent students from disconnecting classroom PCs and connecting their own notebooks, you will need to implement additional security mechanisms. Port security is one possible solution of how to implement control over connected devices on Cisco switches.

Port Security (Cont.)

Port security restricts port access by the MAC address.

- Dynamic (limited number of addresses)
- Static (static configuration of addresses)
- Combination (static plus dynamic)
- Sticky learning



© 2013 Cisco Systems, Inc.

Port security, a feature that is supported on Cisco Catalyst switches, restricts access to a switch port to a specific set or number of MAC addresses. The switch can learn these addresses dynamically, or you can configure them statically. A port that is configured with port security accepts frames only from the addresses that it has learned or that you have configured.

There are several implementations of port security:

- **Dynamic:** You specify how many MAC addresses are permitted to use a port at one time. Use the dynamic approach when you care only about how many rather than which specific MAC addresses are permitted. Depending on how you configure the switch, these dynamically learned addresses age out after a certain period, and new addresses are learned, up to the maximum that you have defined.
- **Static:** You statically configure the specific MAC addresses that are permitted to use a port. Source MAC addresses that you do not specifically permit are not allowed to source frames to the port.
- **A combination of static and dynamic learning:** You can choose to specify some of the permitted MAC addresses and let the switch learn the rest of the permitted MAC addresses. For example, if the number of MAC addresses is limited to four, you can statically configure two MAC addresses. The switch dynamically learns the next two MAC addresses that it receives on this port. Port access is limited to these four addresses, two static and two dynamically learned. The two statically configured addresses do not age out, but the two dynamically learned addresses can age out, depending on the switch configuration.
- **“Sticky learning”:** When this feature is configured on an interface, the interface converts dynamically learned addresses to “sticky secure” addresses. This feature adds the dynamically learned addresses to the running configuration as if they were statically configured using the **switchport port-security mac-address** command. Sticky-learned addresses do not age out.

Imagine five individuals whose laptops are allowed to connect to a specific switch port when they visit an area of the building. You want to restrict switch port access to the MAC addresses of those five laptops and allow no addresses to be learned dynamically on this port.

The table describes the process that can achieve the desired results.

Step	Action	Notes
1	Port security is configured to allow only five connections on this port, and one entry is configured for each of the five allowed MAC addresses.	This step populates the MAC address table with five entries for this port and allows no additional entries to be learned dynamically.
2	Allowed frames are processed.	When frames arrive on the switch port, their source MAC address is checked against the MAC address table. If the source MAC address matches an entry in the table for this port, the frames are forwarded to the switch to be processed.
3	New addresses are not allowed to create new MAC address table entries.	When frames with an unauthorized MAC address arrive on the port, the switch determines that the address is not in the current MAC address table and does not create a dynamic entry for this new MAC address.
4	The switch takes action in response to unauthorized frames.	The switch disallows access to the port and takes one of these configuration-dependent actions: (a) the entire switch port can be shut down; (b) access can be denied for only this MAC address, and a log error message is generated; and (c) access can be denied for this MAC address, but no log message is generated.

Do Not Duplicate
Post beta, not for

Port Security Configuration

This topic describes how to configure port security.

Configuring Port Security

To configure port security on the Fa0/5 port to limit and identify the MAC addresses of stations that are allowed to access the port, do as follows:

- 1 Enable port security
- 2 Set the MAC address limit
- 3 Specify the allowable MAC addresses (optional)
- 4 Define the violation action

```
SwitchX(config)# interface FastEthernet0/5
SwitchX(config-if)# switchport mode access
SwitchX(config-if)# switchport port-security
SwitchX(config-if)# switchport port-security maximum 1
SwitchX(config-if)# switchport port-security mac-address sticky
SwitchX(config-if)# switchport port-security violation shutdown
```

© 2013 Cisco Systems, Inc.

Port security limits the number of valid MAC addresses that are allowed on a port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

If you limit the number of secure MAC addresses to one and assign a single MAC address to this port, only the workstation with this particular secure MAC address can successfully connect to this switch port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, a security violation occurs when the MAC address of a workstation that is attempting to access the port is different from any of the identified secure MAC addresses.

The figure shows how to enable sticky port security on Fast Ethernet port 0/5 of switch SwitchX.

Note Before port security can be activated, the port mode must be set to “access” or “trunk” using the **switchport mode access|trunk** command.

Use the **switchport port-security** interface command *without* keywords to enable port security on an interface. Use the **switchport port-security** interface command *with* keywords to configure a secure MAC address, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default state.

You can configure the maximum number of secure MAC addresses. In this figure, you can see the Cisco IOS command syntax that is used to set the maximum number of MAC addresses to one (**switchport port-security maximum 1**).

You can add secure addresses to the address table after setting the maximum number of secure MAC addresses that are allowed on a port in these ways:

- Manually configure all of the addresses (**switchport port-security mac-address 0008.eeee.eeee**).

- Allow the port to dynamically configure all of the addresses (**switchport port-security mac-address sticky**).
- Configure a number of MAC addresses and allow the rest of the addresses to be dynamically configured.

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and add them to the running configuration by enabling sticky learning. To enable sticky learning, enter the **switchport port-security mac-address sticky** interface configuration command. When you enter this command, the interface converts all of the dynamic secure MAC addresses, including the MAC addresses that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

The violation mode is set to **shutdown** (**switchport port-security violation shutdown**). This violation mode is also a default setting. If any frames are detected from an address that is not allowed, the interface is error-disabled, a log entry is made, an SNMP trap is sent, and manual intervention or error-disable recovery must be used to make the interface usable.

Note Two other violation modes are **protect** and **restrict**. For both violation modes, frames from the address that is not allowed are dropped, but the interface is not put into the error-disable state.

Security violation situations are as follows:

- The maximum number of secure MAC addresses has been added to the address table. A station whose MAC address is not in the address attempts to access the interface.
- An address that is learned or configured on one secure interface is seen on another secure interface in the same VLAN.

Note Port security is disabled by default.

Port Security Verification

This topic describes how to verify port security operation.

Port Security Verification

```
SwitchX# show port-security interface FastEthernet 0/5
```

- Displays the port security settings that are defined for an interface

```
SwitchX# show port-security interface FastEthernet 0/5
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : fc99.47e5.2598:1
Security Violation Count : 0
```

- Displays the port security settings that are defined for the FastEthernet 0/5 interface

© 2013 Cisco Systems, Inc.

After you have configured port security for your switch, verify that it has been configured correctly. You must check each interface to verify that you have set the port security correctly. You must also verify that you have configured static MAC addresses correctly. Use the **show port-security interface** privileged EXEC command to display the port security settings that are defined for an interface.

The output displays this information (from the top down):

- Whether the port security feature is enabled
- The violation mode
- The maximum allowed number of secure MAC addresses for each interface
- The number of secure MAC addresses on the interface
- The number of security violations that have occurred

Port Security Verification (Cont.)

```
SwitchX# show port-security interface FastEthernet 0/5
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 001a.2fe7.3089:1
Security Violation Count : 1
```

- Displays the port security violation for the FastEthernet 0/5 interface

© 2013 Cisco Systems, Inc.

Port Security Verification (Cont.)

```
SwitchX# show interface status
Port      Name      Status      Vlan    Duplex  Speed Type
Fa0/1     Name1     connected   1       a-full  a-100 10/100BaseTX
Fa0/2     Name2     notconnect  1       auto    auto  10/100BaseTX
Fa0/3     Name3     notconnect  1       auto    auto  10/100BaseTX
Fa0/4     Name4     notconnect  1       auto    auto  10/100BaseTX
Fa0/5     Name5     err-disabled 1       auto    auto  10/100BaseTX
<output omitted>
```

- Verifies the status of the interface

© 2013 Cisco Systems, Inc.

When MAC addresses are assigned to a secure port, the port does not forward frames with source MAC addresses outside the group of defined addresses. When a port that is configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device that is attached to the port differs from the list of secure addresses, the port either shuts down until it is administratively re-enabled (default mode) or drops incoming frames from the insecure host (the **restrict** option). The behavior of the port depends on how it is configured to respond to a security violation.

The output in the figure shows that a security violation has occurred, and the port is in the secure-shutdown state.

Because the port security violation mode is set to **shutdown**, the port with the security violation (source MAC addresses outside the group of defined addresses) goes to the error-disabled state. You receive this notification on the switch:

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5,
putting Fa0/5 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC
address 000c.292b.4c75 on port FastEthernet0/5.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/5,
changed state
to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
```

To verify the status of the interface, use the **show interface status** command.

To make the interface operational again, you need to disable the interface administratively and then enable it again:

```
SwitchX(config)# interface FastEthernet 0/5
SwitchX(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down
SwitchX(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5,
changed state
to up
```

Port Security Verification (Cont.)

```
SwitchX# show port-security address
Secure Mac Address Table
-----
Vlan Mac Address      Type                Ports    Remaining Age (mins)
-----
1    0008.dddd.eeee    SecureConfigured   Fa0/5    -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Displays the secure MAC addresses for all ports

```
SwitchX# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/5      1              1              0              Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Displays the port security settings for the switch

© 2013 Cisco Systems, Inc.

Use the **show port-security address** command to display the secure MAC addresses for all ports. Use the **show port-security** command without keywords to display the port security settings for the switch.

Disabling Unused Services

This topic describes disabling unused services to increase network security.

Disabling Unused Services

Some services on Cisco devices may not be needed and therefore can be disabled, providing these benefits:

- Helps preserve system resources
- Eliminates the potential for security exploits on the disabled services

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot  Local Address  Foreign Address  Service  State
tcp   *:22            *:0              SSH-Server  LISTEN
tcp   *:23            *:0              Telnet     LISTEN
udp   *:49            172.26.150.206:0 TACACS service LISTEN
udp   *:67            *:0              DHCPD Receive LISTEN
```

- Displays the UDP or TCP ports that the router is listening to

To facilitate deployment, Cisco routers and switches start with a list of services that are turned on and considered to be appropriate for most network environments. However, because not all networks have the same requirements, some of these services may not be needed. Disabling these unnecessary services has two benefits: it helps preserve system resources, and it eliminates the potential for security exploits on the unneeded services.

The general best practice is to identify open ports. Use the **show control-plane host open-ports** command to see which UDP or TCP ports the router is listening to and to determine which services need to be disabled.

Note As an alternative, Cisco IOS Software provides the AutoSecure function that helps disable these unnecessary services while enabling other security services.

In the example, services that are enabled on the router are SSH, Telnet, TACACS, and DHCP.

Disabling Unused Services (Cont.)

The following are some general best practices:

- The finger, identification, TCP, and UDP small servers should remain disabled on all routers and switches.
- You should disable Cisco Discovery Protocol on interfaces where the service may represent a risk.
- It is strongly recommend that you turn off the HTTP service running on the router (HTTPS can stay on).

© 2013 Cisco Systems, Inc.

Unless they are explicitly needed, ensure that finger, identification (identd), and TCP and UDP small servers remain disabled on all routers and switches. In Cisco IOS Software Release 15.0 and later, all of these services are disabled by default.

Disable Cisco Discovery Protocol on interfaces where the service may represent a risk. Examples are external interfaces, such as those at the Internet edge, and data-only ports at the campus and branch access. Cisco Discovery Protocol is enabled by default in Cisco IOS Software Release 15.0 and later.

Cisco routers can be accessed via a web page, but it is strongly recommend that you turn off the HTTP service that is running on the router. HTTP service is disabled by default in Cisco IOS Software Release 15.0 and later.

Disabling Unused Services (Cont.)

There are two options to disable Cisco Discovery Protocol:

Disable it globally (on all interfaces)

```
Router(config)# no cdp run
```

Disable it on a specific interface

```
Router(config)# interface FastEthernet0/24
Router(config-if)# no cdp enable
```

It is recommended that you disable the HTTP service

```
Router(config)# no ip http server
```

© 2013 Cisco Systems, Inc.

If you prefer not to use the Cisco Discovery Protocol device discovery capability, you can disable it with the **no cdp run** global configuration command. To re-enable Cisco Discovery Protocol after disabling it, use the **cdp run** command in global configuration mode.

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and receive Cisco Discovery Protocol information. Cisco Discovery Protocol is not on by default on Frame Relay interfaces. You can disable Cisco Discovery Protocol on an interface that supports it with the **no cdp enable** interface configuration command. To re-enable Cisco Discovery Protocol on an interface after disabling it, use the **cdp enable** command in interface configuration mode.

It is strongly recommended that you turn off the HTTP service that is running on the router. You can use the **no ip http server** global configuration command to disable it. To re-enable the HTTP service after disabling it, use the **ip http server** command in global configuration mode.

Network Time Protocol

This topic describes NTP.

Network Time Protocol

Correct time within networks is important:

- Correct time allows the tracking of events in the network in the correct order.
- Clock synchronization is critical for the correct interpretation of events within syslog data.
- Clock synchronization is critical for digital certificates.

© 2013 Cisco Systems, Inc.

Networks use NTP to synchronize the clocks of various devices across a network. Clock synchronization within a network is critical for digital certificates and for correct interpretation of events within syslog data. A secure method of providing clocking for the network is for network administrators to implement their own private network master clocks, synchronized to UTC, using satellite or radio. However, if network administrators do not wish to implement their own master clocks because of cost or other reasons, other clock sources are available on the Internet.

Network Time Protocol (Cont.)

NTP provides time synchronization between network devices.

- NTP can get the correct time from an internal or external time source:
 - Local master clock
 - Master clock on the Internet
 - GPS or atomic clock
- A router can act as an NTP server and client. Other devices (NTP clients) synchronize time with the router (NTP server).

© 2013 Cisco Systems, Inc.

NTP is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source will have more consistent time settings.

You can configure a router as an NTP server, to which other devices (NTP clients) synchronize their time settings.

Do Not Duplicate.
Post beta, not for release.

Configuring NTP

This topic describes how to configure NTP on Cisco devices.

Configuring NTP

Configure the Branch router as the NTP client, which will synchronize its time with the NTP server.

```
Branch (config) # ntp server 209.165.201.15
```

Configure the SW1 switch as the NTP client, which will synchronize its time with the Branch router.

```
SW1 (config) # ntp server 10.1.1.1
```

The diagram illustrates a network topology for NTP configuration. On the left is a switch labeled 'SW1', which is identified as an 'NTP Client'. It is connected to a blue router labeled 'Branch', also identified as an 'NTP Client'. The connection between SW1 and Branch is labeled with the network '10.1.1.0/24'. The Branch router is further connected to an 'NTP Server' represented by a server rack icon, with the IP address '209.165.201.15' shown below it. A copyright notice '© 2013 Cisco Systems, Inc.' is visible at the bottom left of the diagram area.

The figure shows an example configuration scenario. Both router Branch and switch SW1 are configured as NTP clients using the **ntp server ip-address** global configuration command. As argument IP address of the NTP server is configured.

A Cisco IOS device acting as an NTP client will also respond to received time requests. This enables switch SW1 to sync directly with router Branch and optimize traffic flows. Alternatively, you could configure switch SW1 to sync with an external NTP server as well.

Cisco IOS devices can also act as NTP servers. To configure Cisco IOS Software as an NTP master clock to which peers synchronize themselves, use the **ntp master** command in global configuration mode:

ntp master [*stratum*]

Note Use this command with caution. Valid time sources can be easily overridden using this command, especially if a low stratum number is configured. Configuring multiple devices in the same network with the **ntp master** command can cause instability in keeping time if the devices do not agree on the time.

The *stratum* value is a number from 1 to 15. The lowest stratum value indicates a higher NTP priority. It also indicates the NTP stratum number that the system will claim.

Verifying NTP

This topic describes how to verify NTP on Cisco devices.

Verifying NTP

```
Branch# show ntp associations
address      ref clock    st when poll reach delay offset disp
*~209.165.201.15 127.127.1.1 1 17 64 1 0.856 0.050 187.57
! sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

- Displays the status of NTP associations

```
Branch# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.201.15
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D40ADC27.E644C776 (13:18:31.899 UTC Mon Sep 24 2012)
clock offset is 6.0716 msec, root delay is 1.47 msec
root dispersion is 15.41 msec, peer dispersion is 3.62 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000091 s/s
system poll interval is 64, last update was 344 sec ago.
```

- Displays the status of NTP

To display the status of NTP associations, use the **show ntp associations** command in privileged EXEC mode.

Significant fields that are shown in the display follow:

- *****: Peer that is synchronized to this peer
- **~**: Peer that is statically configured
- **address**: Address of the peer
- **st**: Stratum setting for the peer

Note It may take several minutes for an NTP client to be synchronized with the NTP server.

To display the status of NTP, use the **show ntp status** command in user EXEC mode.

Significant fields that are shown in the display follow:

- **synchronized**: System synchronized to an NTP peer
- **stratum**: NTP stratum of this system
- **reference**: Address of the peer to which a clock is synchronized

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Secure unused ports by disabling interfaces.
- The port security feature restricts a switch port to a specific set or number of MAC addresses.
- Before port security can be activated, the port mode must be set to static switchport mode.
- Use the **show port-security interface** command to display the port security settings that are defined for an interface.
- Some services on Cisco devices may not be needed and therefore can be disabled.
- NTP provides time synchronization between network devices.
- A Cisco router can act as an authoritative NTP server.
- Use the **show ntp associations** command to display the status of NTP associations.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Implementing Traffic Filtering with ACLs

Overview

Once you understand how ACLs operate, you can implement them for an important network security mechanism: traffic filtering. Standard ACLs provide only limited traffic filtering. Extended ACLs can provide more precise traffic-filtering capabilities.

This lesson also describes access-list configuration mode. This mode enables you to define named ACLs that are identified with descriptive names instead of numbers. Further, the lesson shows how to verify that ACLs are functioning properly and discusses some common configuration errors.

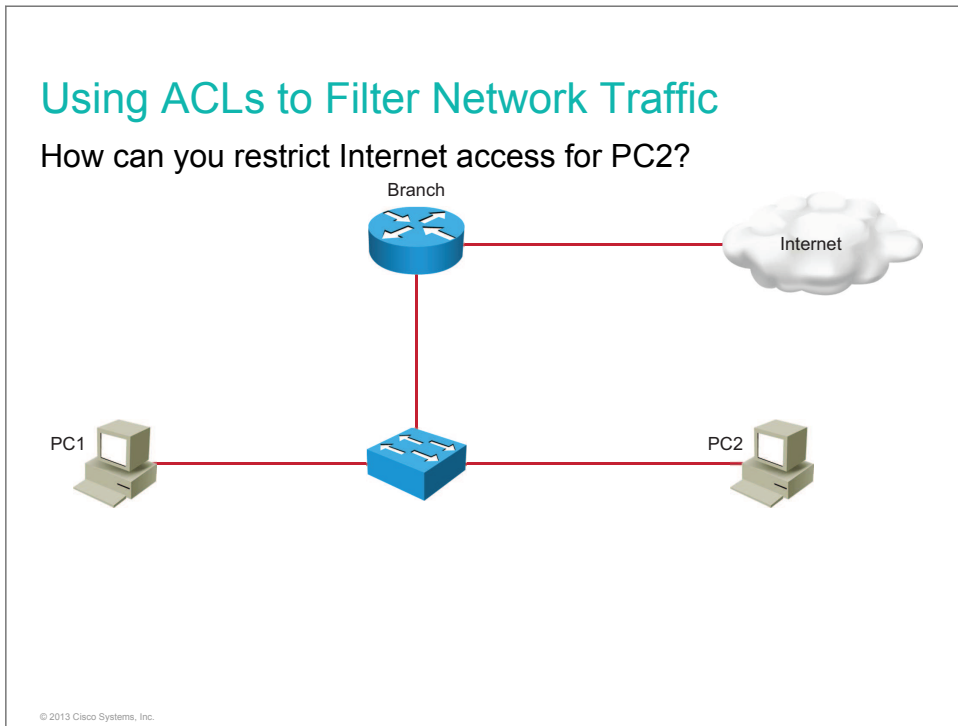
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe traffic filtering with ACLs
- Explain how inbound and outbound ACLs operate
- Apply an ACL to an interface
- Describe the need for extended ACLs
- Configure and verify numbered, extended IPv4 ACLs
- Configure and edit named IPv4 ACLs
- Describe ACL configuration guidelines
- Monitor and verify ACLs
- Identify and resolve common ACL configuration errors

Using ACLs to Filter Network Traffic

This topic describes how to use ACLs to filter network traffic.

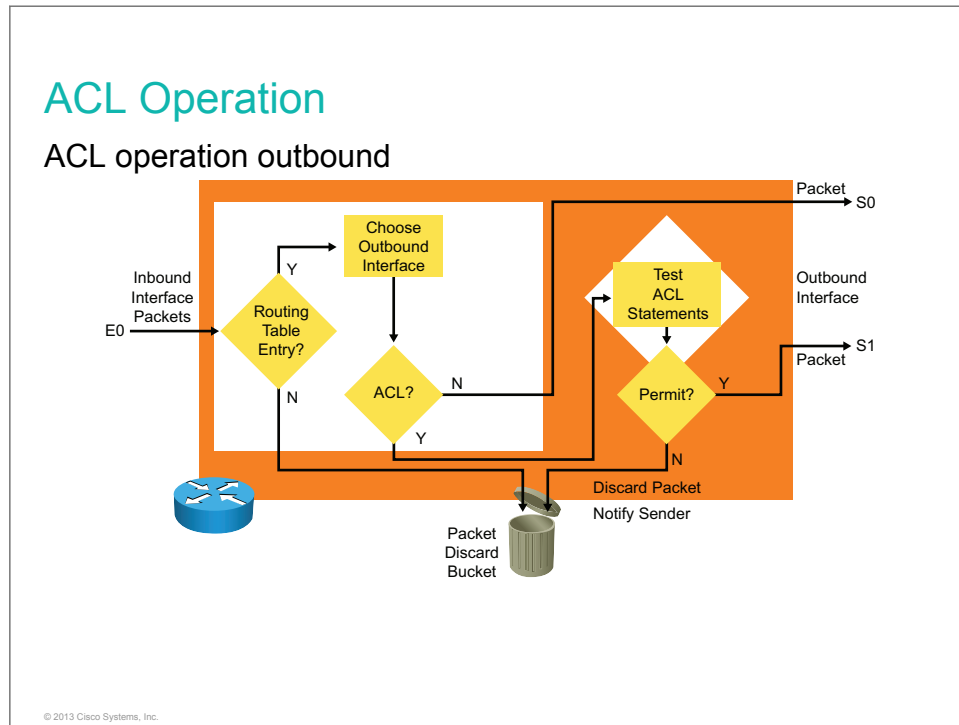


The figure introduces a common task for network administrators: a need to implement network traffic filtering to allow, limit, or restrict access to a network resource. A common mechanism that is used for traffic filtering is ACLs, which enable you to control access based on Layer 3 packet-header information.

In the scenario in the figure, traffic filtering can be implemented on the router either inbound on an interface that is connected to the LAN or outbound on an interface that is connected to the Internet. By using a simple standard ACL, you can prevent packets from PC2 entering or leaving the interface. You should not forget to explicitly allow traffic for other devices in the LAN, such as PC1.

ACL Operation

This topic describes how ACLs filter traffic.



When ACLs are used for traffic filtering, they can operate inbound or outbound. The direction determines at which point packets are tested against the ACL as they pass through the router.

- **Outbound ACLs:** Incoming packets are routed to the outbound interface and then are processed through the outbound ACL. If packets match a permit statement, they are forwarded through the interface. If packets match a deny statement or if there is no match, they are discarded.
- **Inbound ACLs:** Incoming packets are processed by the ACL before they are routed to an outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the filtering tests deny the packet and it is discarded. If the tests permit the packet, it is processed for routing.

Applying ACLs to Interfaces

This topic describes how to apply ACLs to interfaces.

Applying ACLs to Interfaces

Applies ACL 1 on the interface as an outbound filter:

```
Branch(config-if)# ip access-group 1 out
```

Applies ACL 2 on the interface as an inbound filter:

```
Branch(config-if)# ip access-group 2 in
```

Important: Only one ACL per protocol, per direction, and per interface is allowed.

© 2013 Cisco Systems, Inc.

After an ACL is configured, it is linked to an interface using the **ip access-group** command. Only one ACL per protocol, per direction, and per interface is allowed. The figure shows examples of this command, showing how to apply the ACL as an inbound and outbound filter.

Note To remove an ACL from an interface, enter the **no ip access-group** command on the interface, then enter the global **no access-list** command to remove the entire ACL if needed.

The table provides an example of the steps that are required to configure and apply a numbered standard ACL on a router.

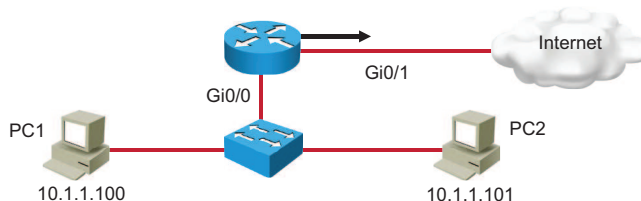
Numbered Standard ACL Configuration Procedure

Step	Action	Notes
1	Use the access-list global configuration command to create an entry in a standard IPv4 ACL. Branch(config)# access-list 1 permit 10.1.1.0 0.0.0.255	The example ACL statement matches any address that starts with 10.1.1.x.
2	Use the interface configuration command to select an interface in which to apply the ACL. Branch(config)# interface GigabitEthernet 0/0	After you enter the interface command, the CLI prompt changes from (config)# to (config-if)#.
3	Use the ip access-group interface configuration command to activate the existing ACL on the interface. Branch(config-if)# ip access-group 1 in	This example activates the standard IPv4 ACL 1 on the interface as an inbound filter.

Applying ACLs to Interfaces (Cont.)

Example:

- Deny Internet access for a specific host (10.1.1.101).
- Allow all other LAN hosts to access the Internet.



```
Branch(config)# access-list 1 deny 10.1.1.101  
Branch(config)# access-list 1 permit 10.1.1.0 0.0.0.255  
Branch(config)# interface GigabitEthernet 0/1  
Branch(config-if)# ip access-group 1 out
```

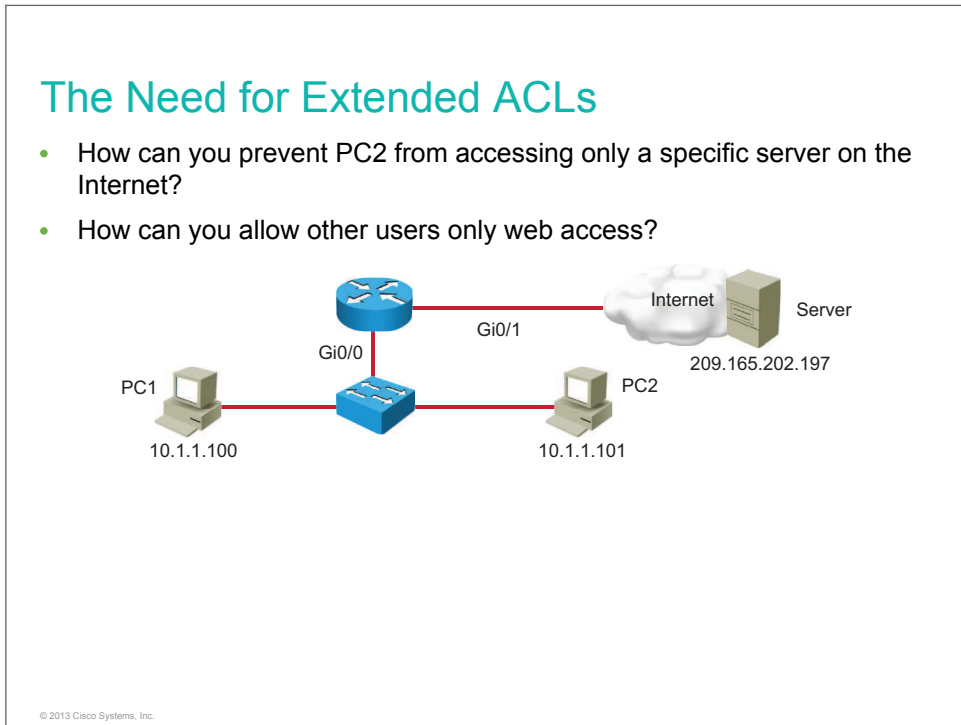
© 2013 Cisco Systems, Inc.

The figure shows a scenario in which ACL 1 is applied in the outbound direction on router Branch to provide traffic filtering. ACL 1 includes a deny statement that matches traffic from a specific host with IP address 10.1.1.101. The second line in the ACL permits traffic from hosts within network 10.1.1.0 /24. It is important to specify a permit statement because ACLs end with an implicit deny all statement.

Note Alternatively, the ACL could be applied in the inbound direction on interface GigabitEthernet 0/0. This solution would not only prevent host PC2 from accessing the Internet but also would deny all communication between PC2 and the router.

The Need for Extended ACLs

Standard ACLs cannot fulfill all traffic-filtering requirements. This topic describes extended ACLs and illustrates why you need them.



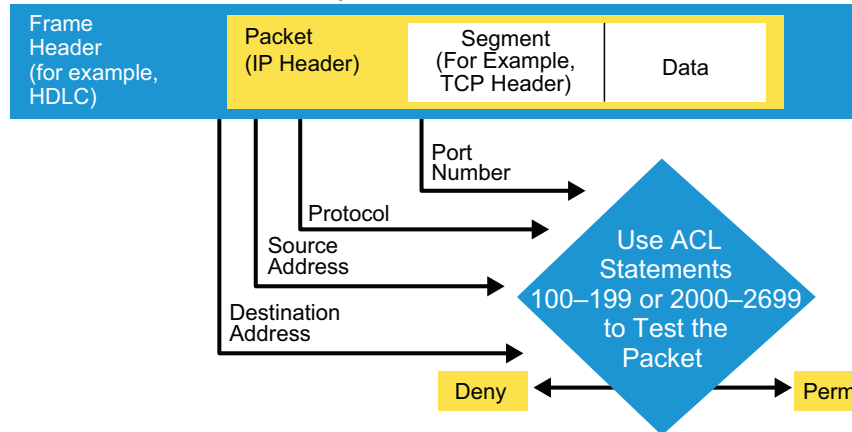
Standard ACLs provide only limited options for network traffic filtering. It is impossible to meet the requirement that is shown in the figure using just standard ACLs. For more precise traffic filtering, use extended ACLs.

To prevent PC2 from communicating with a specific server, use an extended ACL matching the PC2 IP address as the source address and the server IP address as the destination address.

The Need for Extended ACLs (Cont.)

Testing packets with extended IPv4 ACLs

An Example from a TCP/IP Packet



Extended ACLs provide a greater range of control. In addition to verifying packet source addresses, extended ACLs also check destination addresses, protocols, and port numbers, as shown in the figure. They provide more criteria on which to base the ACL. For example, an extended ACL can simultaneously allow email traffic from a network to a specific destination and deny file transfers and web browsing for a specific host.

The ability to filter on protocol and port number allows you to build very specific extended ACLs. Using the appropriate port number, you can specify an application by configuring either the port number or the name of a well-known port.

Extended ACLs are numbered from 100 to 199 and from 2000 to 2699, providing a total of 800 possible extended ACLs. Named, extended ACLs are also supported.

Configuring Numbered, Extended IPv4 ACLs

This topic describes how to configure numbered, extended IPv4 ACLs.

Configuring Numbered Extended IPv4 ACLs

```
Branch(config)# access-list 110 deny ip host 10.1.1.101 host 209.165.202.197
Branch(config)# access-list 110 permit tcp 10.1.1.0 0.0.0.255 any eq 80
```

- The number 110 is chosen to define an ACL as an extended ACL.
- The first statement matches IP traffic between two specific hosts and denies it.
- The second statement matches HTTP TCP traffic from network 10.1.1.0 /24.
 - The operator eq (equal) is used to match TCP port 80.
- The implicit deny statement is present at the end of the ACL

```
Branch(config-if)# ip access-group 110 in
```

An extended ACL is activated on the interface in the same way as a standard ACL.

© 2013 Cisco Systems, Inc.

The figure shows an example of configuring an extended ACL that specifies source and destination IP addresses and TCP port numbers to match specific traffic.

The table explains the command syntax that is presented in the figure.

access-list Command Parameters

Command Parameters	Description
<i>access-list-number</i>	Number of an ACL. Use a decimal number from 100 to 199 or from 2000 to 2699 for an extended ACL.
permit deny	Either permits or denies traffic if conditions are matched.
<i>protocol</i>	Name of an Internet protocol. You can specify either the name or number of the protocol. The most commonly used keywords are ip , tcp , udp , and icmp .
<i>source source-wildcard</i>	Number of the network and corresponding wildcard that define the source network from which the packet is being sent.
<i>destination destination-wildcard</i>	Number of the network and corresponding wildcard that define the destination network to which the packet is being sent.
<i>operator</i>	Optional parameter that compares source and destination ports when TCP or UDP is specified as a protocol. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).
<i>port</i>	Optional decimal number or name of a TCP or UDP port.

To configure and apply an extended ACL on a router, follow the configuration procedure that is described in the table.

Numbered, Extended ACL Configuration Procedure

Step	Action	Notes
1	<p>Define an extended IPv4 ACL. Use the access-list global configuration command.</p> <pre>Branch(config)#access-list 110 deny ip host 10.1.1.101 host 209.165.202.197</pre> <pre>Branch(config)#access-list 110 permit tcp 10.1.1.0 0.0.0.255 any eq 80</pre>	<p>Use the show access-lists command to display the contents of the ACL.</p> <p>In the example, ACL 110 denies IP traffic between specific hosts 10.1.1.101 and 209.165.202.197. The second statement allows TCP traffic destined to port 80 between hosts on network 10.1.1.0 /24 and any destination.</p> <p>All other traffic is denied by the implicit deny all at the end of the ACL.</p>
2	<p>Select the interface to be configured. Use the interface global configuration command.</p> <pre>Branch(config)# interface GigabitEthernet 0/0</pre>	<p>After you enter the interface command, the CLI prompt changes from (config)# to (config-if)#.</p>
3	<p>Link the extended IPv4 ACL to an interface. Use the ip access-group interface configuration command.</p> <pre>RouterX(config-if)# ip access-group 110 in</pre>	<p>Use the show ip interfaces command to verify that an IP ACL is applied to the interface.</p>

Configuring Named ACLs

Designating ACLs by a descriptive name instead of a number provides a better way to describe the intention of the ACL. This topic describes named ACLs and shows how to configure them.

Configuring Named ACLs

The ACL configuration mode is used to configure a named ACL.

```
Branch(config)# ip access-list extended WEB_ONLY  
Branch(config-ext-nacl)# permit tcp 10.1.1.0 0.0.0.255 any eq www  
Branch(config-ext-nacl)# 20 permit tcp 10.1.1.0 0.0.0.255 any eq 443
```

- The alphanumeric name string (WEB_ONLY in the example) must be unique.
- If sequence numbers are not configured, they are generated automatically, starting at 10 and incrementing by 10.
- The **no 10** command removes the specific test that is numbered with 10 from the named ACL.

```
Branch(config-if)# ip access-group WEB_ONLY in
```

Named ACLs are activated on an interface with the same command as numbered ACLs.

© 2013 Cisco Systems, Inc.

Naming an ACL makes it easier to understand its function. For example, an ACL to deny FTP could be called NO_FTP. When you identify your ACL with a name instead of a number, the configuration mode and command syntax are slightly different.

Access-list configuration mode is used to define named ACLs. To enter this mode, use the command **ip access-list**.

Note Numbered ACLs can also be defined using access-list configuration mode. You just specify an ACL number instead of a unique name.

In the figure, the command output shows the commands that are used to configure an extended ACL that is named WEB_ONLY on the Branch router. The ACL permits traffic from hosts on the 10.1.1.0/24 network that are destined to HTTP and HTTPS ports.

Capitalizing ACL names is not required, but it makes them stand out when you view the running configuration output.

Configuring Named ACLs (Cont.)

Edit an ACL in the access-list configuration mode to deny web access for host 10.1.1.25:

```
Branch# show access-lists
Extended IP access list WEB_ONLY
 10 permit tcp 10.1.1.0 0.0.0.255 any eq www
 20 permit tcp 10.1.1.0 0.0.0.255 any eq 443
Branch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)# ip access-list extended WEB_ONLY
Branch(config-ext-nacl)# 5 deny ip host 10.1.1.25 any
Branch(config-ext-nacl)# end
Branch# show access-lists
Extended IP access list WEB_ONLY
 5 deny ip host 10.1.1.25 any
 10 permit tcp 10.1.1.0 0.0.0.255 any eq www
 20 permit tcp 10.1.1.0 0.0.0.255 any eq 443
```

© 2013 Cisco Systems, Inc.

Named IP ACLs allow you to add, modify, or delete individual entries in a specific ACL. You can use sequence numbers to insert statements anywhere in the named ACL.

When statements are added to the ACL, the default increment is 10. The figure shows an additional entry that is numbered 5 in the WEB_ONLY ACL, which is inserted in front of line 10.

Note that reload will change the sequence numbers in the ACL. The sequence numbers will be 10, 20, and 30 instead of 5, 10, and 20 after reload. Use the **access-list resequence** command to renumber the ACL entries in an ACL without having to reload.

For more details about the **ip access-list** command and related commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_i1.html#wp1079735.

ACL Configuration Guidelines

This topic describes recommended configuration guidelines for ACLs.

ACL Configuration Guidelines

These guidelines are recommended:

- The type of ACL, standard or extended, determines what is filtered.
- Only one ACL per interface, per protocol, and per direction is allowed.
- The most specific statement should be at the top of an ACL. The most general statement should be at the bottom of an ACL.
- The last ACL test is always an implicit “deny everything else” statement, so every list needs at least one permit statement.
- When placing an ACL in a network, do as follows:
 - Place extended ACLs close to the source.
 - Place standard ACLs close to the destination.
- An ACL can filter traffic going through the router or traffic to and from the router, depending on how it is applied.

© 2013 Cisco Systems, Inc.

Well-designed and well-implemented ACLs add an important security component to your network. Follow these general principles to ensure that the ACLs that you create have the intended results:

- Based on the test conditions, choose a standard or an extended ACL.
- Only one ACL per protocol, per direction, and per interface is allowed. Multiple ACLs are permitted per interface, but each must be for a different protocol or different direction.
- Your ACL should be organized to allow processing from the top down. The more specific references to a network or subnet should appear before more general conditions. Place conditions that occur more frequently before conditions that occur less frequently.
- Your ACL always contains an implicit deny any statement at the end.
 - Unless you add an explicit permit any statement, the ACL by default denies all traffic that fails to match any of the ACL lines.
 - Every ACL should have at least one permit statement. Otherwise, all traffic is denied.
- You should typically place extended ACLs as close as possible to the source of the traffic that you want to deny. Because standard ACLs do not specify destination addresses, you must put the standard ACL as close as possible to the destination of the traffic that you want to deny so the source can reach intermediary networks.
- Depending on how you apply the ACL, the ACL filters traffic either going through the router or going to and from the router, such as traffic to or from vty lines.

Monitoring ACLs

This topic describes how to monitor and verify ACLs.

Monitoring ACLs

```
Branch# show access-lists
```

- Displays the content of ACLs

```
Branch# show access-lists
Standard IP access list SALES
 10 deny 10.1.1.0, wildcard bits 0.0.0.255
 20 permit 10.3.3.1
 30 permit 10.4.4.1
 40 permit 10.5.5.1
Extended IP access list ENG
 10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
 20 permit tcp host 10.33.33.1 any eq ftp
 30 permit tcp host 10.44.44.1 any eq ftp-data
```

© 2013 Cisco Systems, Inc.

When you finish the ACL configuration, use the **show access-lists** command to display the contents of all ACLs. By entering the ACL name or number as an option for this command, you can display a specific ACL.

The output in the figure shows counters that describe how many packets were matched by a specific ACL statement. This information is useful for analyzing an ACL operation.

Monitoring ACLs (Cont.)

```
Branch# show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
Internet address is 10.1.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is WEB ONLY
Proxy ARP is enabled
Local Proxy ARP is disabled
<text omitted>
```

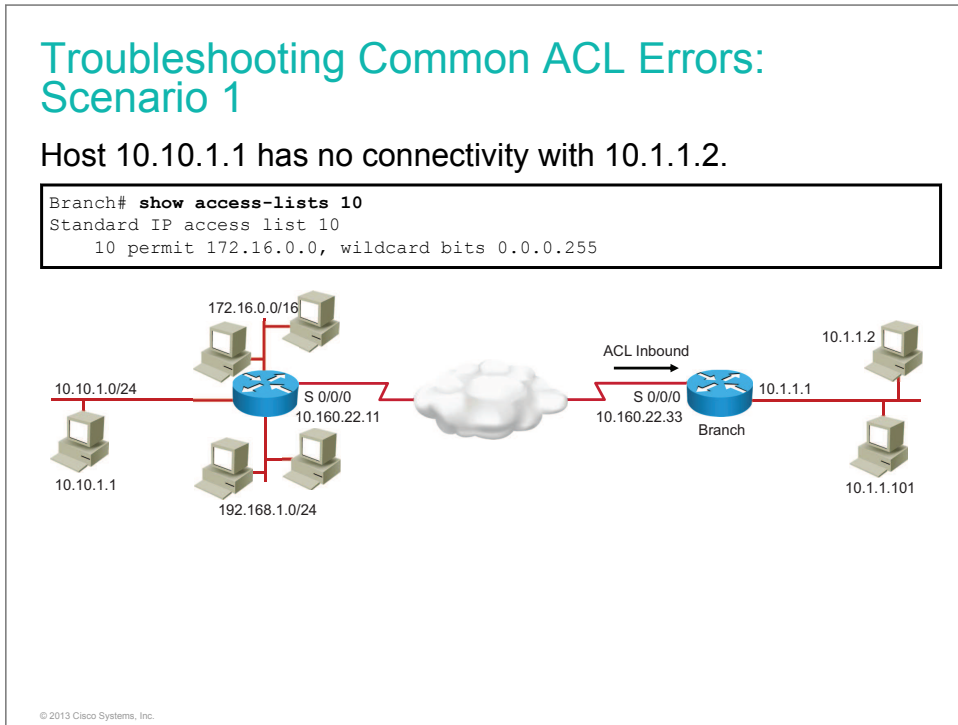
- Shows whether an ACL is applied to an interface

© 2013 Cisco Systems, Inc.

Troubleshooting Common ACL Errors

This topic illustrates common ACL mistakes.

Scenario 1



Analyze the output of the **show access-lists** command to troubleshoot this problem:

- **Problem:** Host 10.10.1.1 has no connectivity with 10.1.1.2.

One of the most common errors involves the "deny all traffic" statement that is implied at the end of every ACL, also referred to as the "implicit deny any" statement. If a packet does not match any of the ACL entries, it is automatically blocked. The implied denial of all traffic that does not match an ACL entry is the default behavior of ACLs and cannot be changed. Therefore, in the figure, host 10.10.1.1 is not able to communicate with host 10.1.1.2.

- **Solution:** The ACL requires a new statement to allow traffic from the 10.10.1.0 network.

Scenario 2

Troubleshooting Common ACL Errors: Scenario 2

Host 10.10.1.1 has no connectivity with 10.1.1.2.

```
Branch# show access-lists 10
Standard IP access list 10
 10 deny  10.10.1.0, wildcard bits 0.0.0.255
 20 permit 10.10.1.1
 30 permit any
```



© 2013 Cisco Systems, Inc.

Analyze the output from the **show access-lists** command to troubleshoot this problem:

- **Problem:** Host 10.10.1.1 has no connectivity with 10.1.1.2.
- **Solution:** Host 10.10.1.1 has no connectivity with 10.1.1.2 because of the order of the rules in ACL 10. Because the router processes ACLs from the top down, statement 10 would deny host 10.10.1.1, and statement 20 would not be processed. Statements 10 and 20 should be reversed.

Note Later Cisco IOS Software versions display an alert if you use the wrong order for ACL statements.

Scenario 3

Troubleshooting Common ACL Errors: Scenario 3

Users from the 192.168.1.0 network cannot open a TFTP session to 10.1.1.2.

```
Branch# show access-lists 120
Extended IP access list 120
 10 deny tcp 172.16.0.0 0.0.255.255 any eq telnet
 20 deny tcp 192.168.1.0 0.0.0.255 any eq smtp
 30 permit tcp any any
```



Analyze the output from the **show access-lists** command to troubleshoot this problem:

- **Problem:** Users from the 192.168.1.0 network cannot use TFTP to connect to 10.1.1.2.
- **Solution:** The 192.168.1.0 network cannot use TFTP to connect to 10.1.1.2 because TFTP uses the UDP transport protocol. Statement 30 in ACL 120 allows all other TCP traffic. Because TFTP uses UDP, it is implicitly denied. Statement 30 should be **permit ip any any**.

Scenario 4

Troubleshooting Common ACL Errors: Scenario 4

Users from the 172.16.0.0 network can use Telnet to connect to 10.1.1.2, but this connection should not be allowed.

```
Branch# show access-lists 130
Extended IP access list 130
 10 deny tcp any eq telnet any
 20 deny tcp 192.168.1.0 0.0.0.255 any eq smtp
 30 permit ip any any
```



© 2013 Cisco Systems, Inc.

Analyze the output from the **show access-lists** command to troubleshoot this problem:

- **Problem:** The 172.16.0.0 network can use Telnet to connect to 10.1.1.2, but this connection should not be allowed.
- **Solution:** The 172.16.0.0 network can use Telnet to connect to 10.1.1.2 because the Telnet port number in statement 10 of ACL 130 is listed in the wrong position. Statement 10 currently denies any source with a Telnet port number that is trying to establish a connection to any IP address. If you want to deny Telnet inbound on S0/0/0, you should deny the destination port number that is equal to the Telnet port. For example, configure **deny tcp any any eq telnet** or **deny tcp any any eq 23**.

Scenario 5

Troubleshooting Common ACL Errors: Scenario 5

Host 10.10.1.1 can use Telnet to connect to 10.1.1.2, but this connection should not be allowed.

```
Branch# show access-lists 140
Extended IP access list 140
 10 deny tcp host 10.160.22.11 any eq telnet
 20 deny tcp 192.168.1.0 0.0.0.255 any eq smtp
 30 permit ip any any
```



Analyze the output from the **show access-lists** command to troubleshoot this problem:

- **Problem:** Host 10.10.1.1 can use Telnet to connect to 10.1.1.2, but this connection should not be allowed.
- **Solution:** Host 10.10.1.1 can use Telnet to connect to 10.1.1.2 because there are no rules that deny host 10.10.1.1 or its network as the source. Statement 10 of ACL 140 denies the router interface from which traffic would depart. But as these packets depart from the router, they have a source address of 10.10.1.1 and not the address of the router interface.

Scenario 6

Troubleshooting Common ACL Errors: Scenario 6

Host 10.1.1.2 can use Telnet to connect to 10.10.1.1, but this connection should not be allowed.



```
Branch# show access-lists 150
Extended IP access list 150
 10 deny tcp host 10.1.1.2 any eq telnet
 20 permit ip any any
Branch# show running-config interface Serial 0/0/0
interface Serial0/0/0
 ip address 10.160.22.33 255.255.255.0
 ip access-group 150 in
<output omitted>
```

© 2013 Cisco Systems, Inc.

Analyze the output from the **show access-lists** command and information about the ACL to troubleshoot this problem:

- **Problem:** Host 10.1.1.2 can use Telnet to connect to 10.10.1.1, but this connection should not be allowed.
- **Solution:** Host 10.1.1.2 can use Telnet to connect to 10.10.1.1 because of the direction in which ACL 150 is applied to the S0/0/0 interface. Statement 10 denies the source address of 10.1.1.2, but this address would be the source only if the traffic were outbound on S0, not inbound.

Scenario 7

Troubleshooting Common ACL Errors: Scenario 7

Host 10.10.1.1 can use Telnet to connect into the Branch router IP address, but this connection should not be allowed.

```
Branch# show access-lists 160
Extended IP access list 160
 10 deny tcp any host 10.160.22.33 eq telnet
 20 permit ip any any
```



© 2013 Cisco Systems, Inc.

Analyze the output from the **show access-lists** command to troubleshoot this problem:

- **Problem:** Host 10.10.1.1 can connect into router B using Telnet, but this connection should not be allowed.
- **Solution:** Host 10.10.1.1 can connect into the Branch router using Telnet because using Telnet to connect *into* the router is different from using Telnet to connect *through* the router to another device. Statement 10 of ACL 160 denies Telnet access to the address that is assigned to the S0/0/0 interface of router B. Host 10.10.1.1 can still use Telnet to connect into the Branch router simply by using a different interface address (for example 10.1.1.1). When you want to block Telnet traffic into and out of the router itself, use the **access-class** command to apply ACLs to the vty lines.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- ACLs that are used for traffic filtering can operate in the inbound or outbound direction.
- One ACL per protocol, per direction, per interface is supported.
- Extended ACLs are used to filter traffic based on source and destination IP addresses, protocol, and port numbers.
- Numbered, extended ACLs use numbers from 100 to 199 and from 2000 to 2699.

© 2013 Cisco Systems, Inc.

Summary (Cont.)

- Access-list configuration mode allows adding, modifying, and deleting individual statements from an ACL.
- Place more specific statements at the top of an ACL and more general ones at the bottom.
- Use the **show access-lists** verification command to troubleshoot common ACL configuration errors.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- You should secure network devices by using passwords to restrict console, SSH, and Telnet access.
- Device hardening includes disabling unused ports, disabling unneeded services, configuring the port security feature, and configuring NTP.
- ACLs can be used for traffic filtering.

Do Not Duplicate.
Post beta, not for release.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which three types of access can be protected with a password? (Choose three.) (Source: Securing Administrative Access)
 - A. console access
 - B. vty access
 - C. user-level access
 - D. privileged EXEC-level access
 - E. configuration mode access
2. Which message is customized text that is displayed before the username and password login prompts? (Source: Securing Administrative Access)
 - A. message of the day
 - B. login banner
 - C. access warning
 - D. user banner
 - E. warning message
3. Which Cisco IOS feature can be used to control access to the vty ports? (Source: Securing Administrative Access)
 - A. shutdown
 - B. port security
 - C. ACL
 - D. firewall

4. Which Cisco IOS command can be used to increase the security of unused switch ports? (Source: Implementing Device Hardening)
- A. **shutdown**
 - B. **port security**
 - C. **mac-secure**
 - D. **firewall**
5. Which command disables Cisco Discovery Protocol on a device as a whole? (Source: Implementing Device Hardening)
- A. **no run cdp**
 - B. **no cdp run**
 - C. **no cdp enable**
 - D. **no cdp execute**
6. What does the command **no cdp enable** do? (Source: Implementing Device Hardening)
- A. disables Cisco Discovery Protocol on a specific interface
 - B. enables Cisco Discovery Protocol on the device as a whole
 - C. enables Cisco Discovery Protocol on an individual interface
 - D. enables Cisco Discovery Protocol on a specific type of interface
7. Which protocol is used on a device to synchronize its time with a time server? (Source: Implementing Device Hardening)
- A. Cisco Discovery Protocol
 - B. NTP
 - C. STP
 - D. FTP
8. What does a Cisco router do with a packet when the packet matches an outbound ACL permit statement on the interface? (Source: Implementing Traffic Filtering with ACLs)
- A. discards the packet
 - B. returns the packet to its originator
 - C. sends the packet to the output buffer
 - D. holds the packet for further processing
9. Which phrase is the term for the final default statement at the end of every ACL? (Source: Implementing Traffic Filtering with ACLs)
- A. implicit deny any
 - B. implicit deny host
 - C. implicit permit any
 - D. implicit permit host

10. A system administrator wants to configure an IPv4 standard ACL that is attached to the interface on a Cisco router to allow only packets from hosts on subnet 10.1.1.0/24 to enter an interface on a router. Which ACL configuration accomplishes this goal? (Source: Implementing Traffic Filtering with ACLs)
- A. **access-list 1 permit 10.1.1.0**
 - B. **access-list 1 permit 10.1.1.0 host**
 - C. **access-list 99 permit 10.1.1.0 0.0.0.255**
 - D. **access-list 100 permit 10.1.1.0 0.0.0.255**

Do Not Duplicate.
Post beta, not for release.

Answer Key

1. A, B, D
2. B
3. C
4. A
5. B
6. A
7. B
8. C
9. A
10. C

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Building a Medium-Sized Network

When you understand how a switch and router operate, how they communicate, and how to configure basic security, you can move on to understanding an expanded network. This module shows how to "virtualize" your LAN using VLANs and how to configure Layer 3 connectivity between these VLANs. Then it describes how to decrease the administrative burden of assigning IP addresses by using DHCP. The introduction to WANs continues with an explanation of OSPF and of how to configure this routing protocol so that a branch office router can exchange routing information with a headquarters router.

Objectives

Upon completing this module, you will be able to meet these objectives:

- Implement and verify VLANs and trunking
- Describe the application and configuration of inter-VLAN routing
- Configure a Cisco IOS DHCPv4 server on a Cisco router and switch
- Describe WANs and list major technologies
- Describe the need for and purpose of dynamic routing protocols
- Describe the operation and configuration of single-area OSPF

Do Not Duplicate.
Post beta, not for release.

Implementing VLANs and Trunks

VLANs contribute to network performance by separating large broadcast domains into smaller segments. A VLAN allows a network administrator to create logical groups of network devices. These devices act as if they were in their own independent network, although they share a common infrastructure with other VLANs. A VLAN is a logical broadcast domain that can span multiple physical LAN segments. Within the switched internetwork, VLANs provide segmentation and organizational flexibility. You can design a VLAN structure that lets you group stations that are segmented logically by functions, project teams, and applications, without regard to the physical location of the users. VLANs allow you to implement access and security policies to particular groups of users.

A VLAN can exist on a single switch or span multiple switches. VLANs can include stations in a single building or multiple-building infrastructures. VLANs can also connect across WANs. A process of forwarding network traffic from one VLAN to another VLAN using a router is called *inter-VLAN routing*. VLANs are associated with unique IP subnets on the network. This subnet configuration facilitates the routing process in a multi-VLAN environment. When you use a router to facilitate inter-VLAN routing, the router interfaces can be connected to separate VLANs. Devices on those VLANs send traffic through the router to reach other VLANs.

When multiple switches are implemented on the same network, there is a potential for intentional or unintentional physical loops. When loops occur, broadcast storms may result, propagating frames throughout the network. STP solves the problem of broadcast storms by disabling redundant links and keeping them on standby if the primary link fails.

Objectives

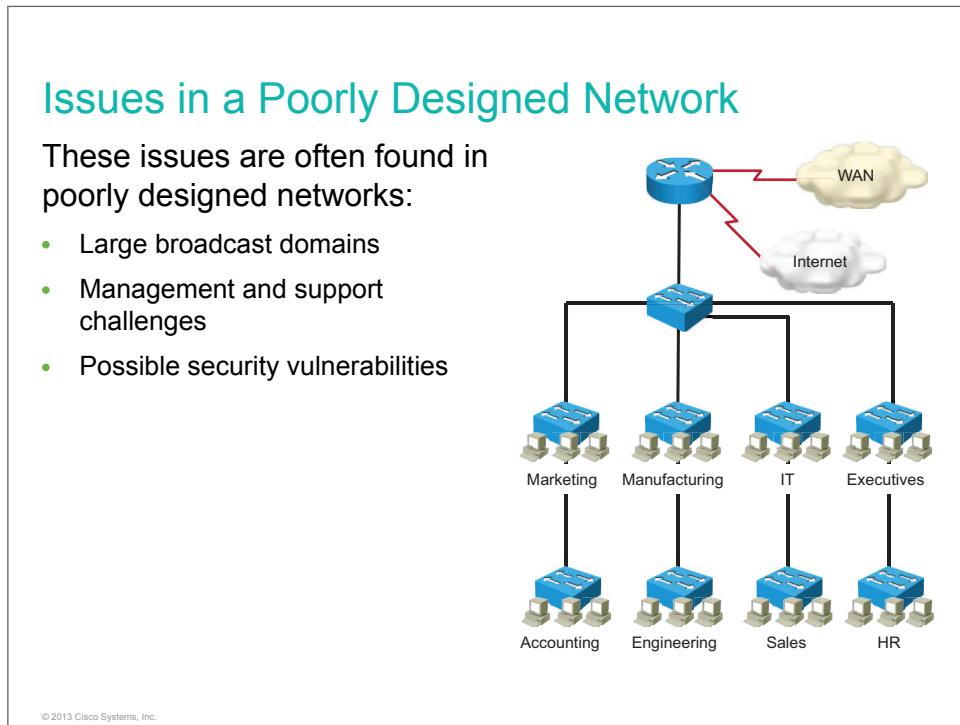
Upon completing this lesson, you will be able to meet these objectives:

- Describe the issues in poorly designed LANs
- Describe the purpose and functions of VLANs
- Define the purpose and function of trunking

- Implement and verify VLANs
- Assign ports to a VLAN
- Configure and verify IEEE 802.1Q trunking
- Describe VLAN design and creation guidelines
- Describe how redundancy in a network can cause broadcast loops and describe a solution to this problem

Issues in a Poorly Designed Network

This topic describes the common issues that are found in poorly designed local networks.



A poorly designed network has increased support costs, reduced service availability, and limited support for new applications and solutions. Less-than-optimal performance directly affects end users and their access to central resources. Some of the issues that stem from a poorly designed network include the following:

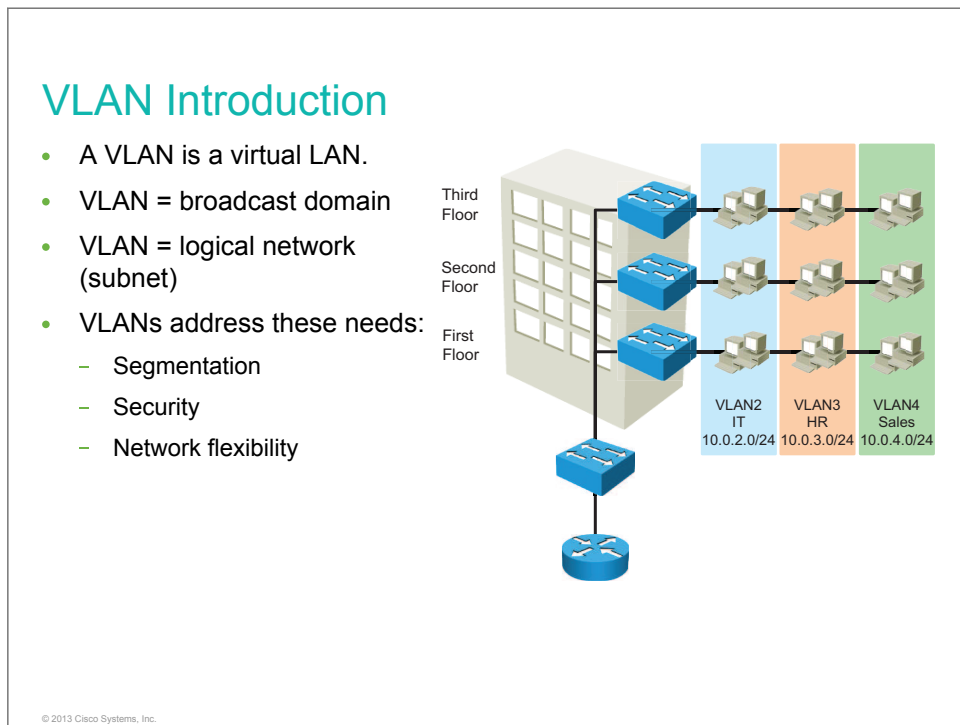
- **Large broadcast domains:** Broadcasts exist in every network. Many applications and network operations use broadcasts to function properly. Therefore, it is not possible to eliminate them completely. In the same way that avoiding failure domains involves clearly defining boundaries, broadcast domains should also have clear boundaries. They should also include an optimal number of devices to minimize the negative effect of broadcasts.
- **Management and support difficulties:** A poorly designed network may be disorganized, poorly documented, and lack easily identified traffic flows, all of which can make support, maintenance, and problem resolution time-consuming and difficult.
- **Possible security vulnerabilities:** A switched network that has been designed with little attention to security requirements at the access layer can compromise the integrity of the entire network.
- **Failure domains:** One of the reasons to implement an effective network design is to minimize the extent of problems when they occur. When Layer 2 and Layer 3 boundaries are not clearly defined, failure in one network area can have a far-reaching effect.

A poorly designed network always has a negative effect, and it becomes a support burden and a cost burden for any organization.

Do Not Duplicate.
Post beta, not for release.

VLAN Introduction

This topic describes the basic idea behind VLANs.



VLANs improve network performance by separating large broadcast domains into smaller segments. A VLAN allows a network administrator to create logical groups of network devices. These devices act as if they were in their own independent network, even if they share a common infrastructure with other VLANs. A VLAN is a logical broadcast domain that can span multiple physical LAN segments. Within the switched internetwork, VLANs provide segmentation and organizational flexibility. You can design a VLAN structure that lets you group stations that are segmented logically by functions, project teams, and applications without regard to the physical location of the users. VLANs allow you to implement access and security policies to particular groups of users. You can assign each switch port to only one VLAN, which adds a layer of security (if the port is operating as an access port). Ports in the same VLAN share broadcasts. Ports in different VLANs do not share broadcasts. Containing broadcasts within a VLAN improves the overall performance of the network.

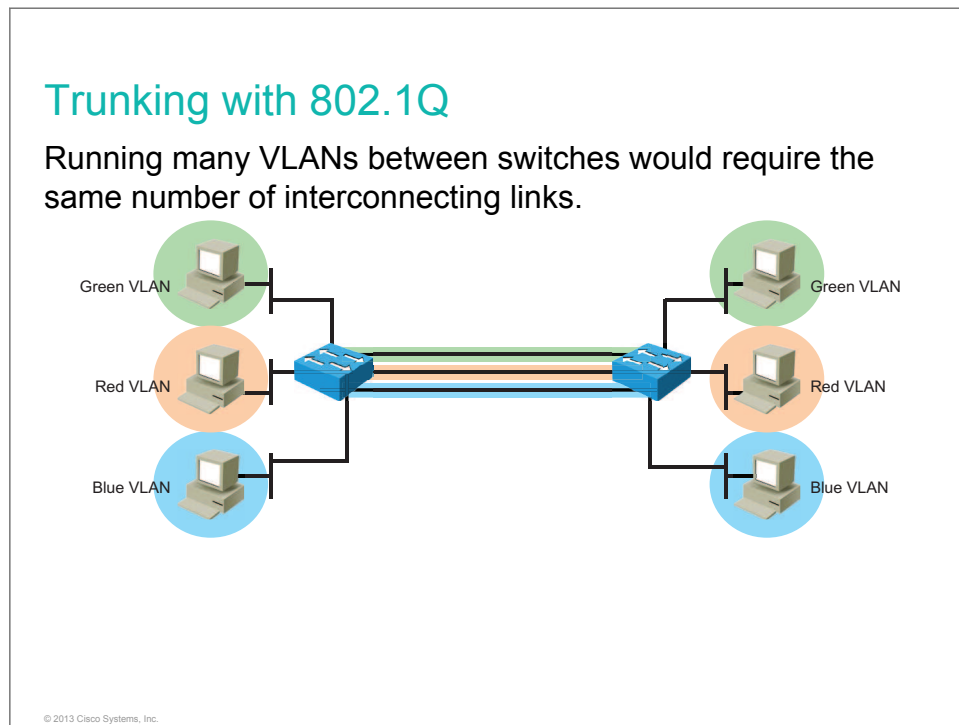
A VLAN can exist on a single switch or span multiple switches. VLANs can include stations in a single building or multiple buildings. VLANs can also connect across WANs. The process of forwarding network traffic from one VLAN to another VLAN using a router is called "inter-VLAN routing." VLANs are associated with unique IP subnets on the network. This subnet configuration facilitates the routing process in a multi-VLAN environment. When you are using a router to facilitate inter-VLAN routing, the router interfaces can be connected to separate VLANs. Devices on those VLANs send traffic through the router to reach other VLANs.

Usually the subnets are chosen according to which VLANs they are associated with. The figure shows that VLAN2 uses subnet 10.0.2.0/24, VLAN3 uses 10.0.3.0/24, and VLAN4 uses 10.0.4.0/24. In this example, the third octet clearly identifies the VLAN that the device belongs to.

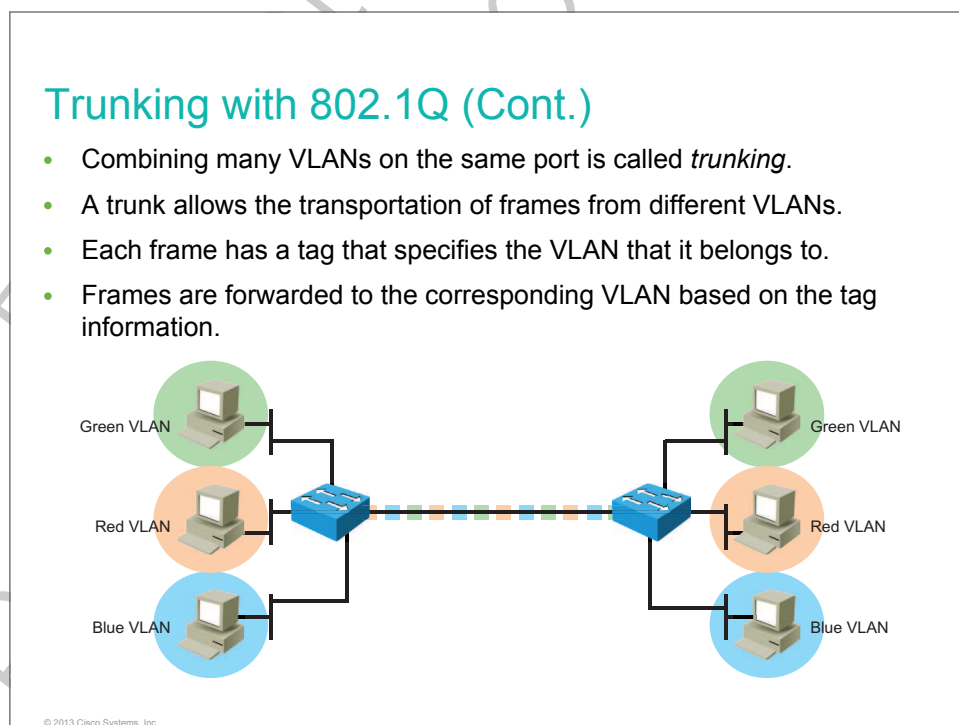
Each VLAN in a switched network corresponds to an IP network. Therefore, VLAN design must take into consideration the implementation of a hierarchical, network-addressing scheme.

Trunking with 802.1Q

This topic describes the basic functionality that is provided by IEEE 802.1Q trunking.

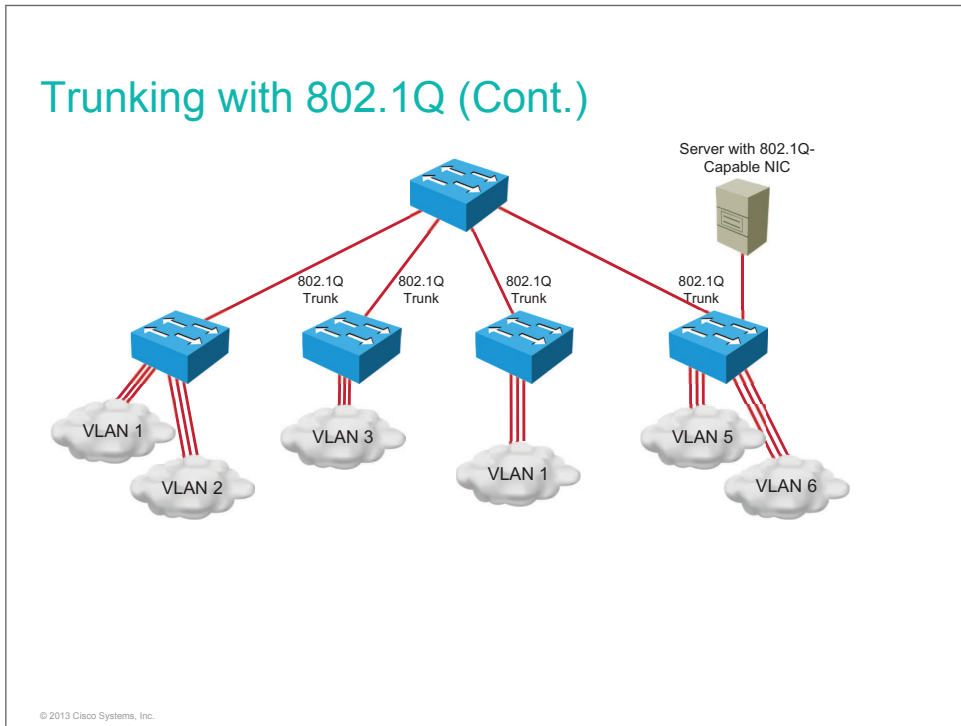


If every port belongs to one VLAN and you have several VLANs that are configured on switches, interconnecting these VLANs would require one physical cable per VLAN. When the number of VLANs increases, so does the number of required interconnecting links. Ports are then used for interswitch connectivity instead of attaching end devices.



To fix this problem, you can use trunks that allow transportation of frames from different VLANs on the same physical link.

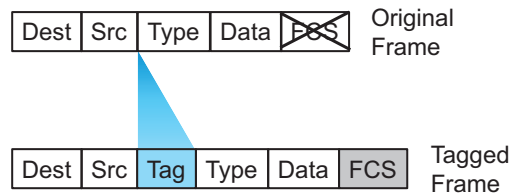
A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device, such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link and allow you to extend the VLANs across an entire network. A trunk does not belong to a specific VLAN. It is a vehicle for VLANs between switches and routers. A special protocol is used to carry multiple VLANs over a single link between two devices. Cisco supports the 802.1Q trunking protocol for Ethernet interfaces. A trunk could also be used between a network device and a server or other device that is equipped with an appropriate 802.1Q-capable NIC.



You can configure an interface as trunking or nontrunking, or you can have it negotiate trunking with the neighboring interface.

By default, all configured VLANs are carried over a trunk interface.

Trunking with 802.1Q (Cont.)



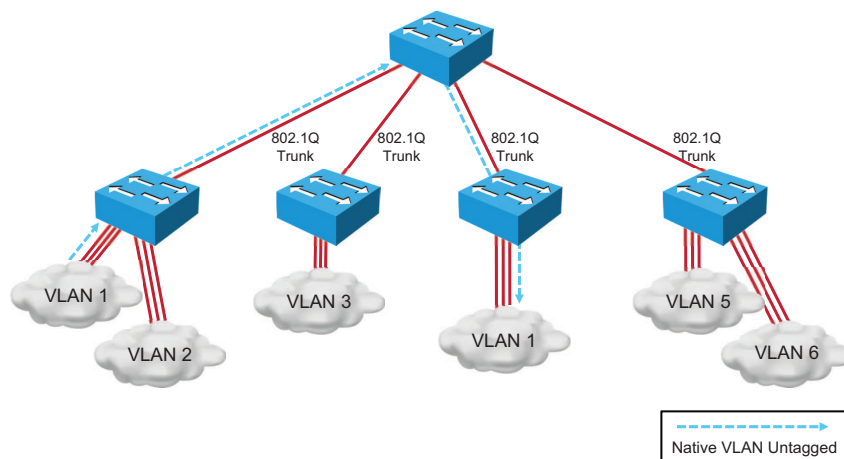
© 2013 Cisco Systems, Inc.

When Ethernet frames are placed on a trunk, they need additional information about the VLANs that they belong to. This task is accomplished by using the 802.1Q encapsulation header. The 802.1Q standard uses an internal tagging mechanism that inserts a 4-byte tag into the original Ethernet frame between the Source Address and Type or Length fields. Because 802.1Q alters the frame, the trunking device recomputes the FCS on the modified frame.

A 12-bit VLAN ID field within the tag is used to specify the VLAN to which the frame belongs.

A tiny part of the 4-byte tag field—3 bits, to be exact—is used to specify the priority of the frame. The details are specified in the IEEE 802.1p standard.

Trunking with 802.1Q (Cont.)



© 2013 Cisco Systems, Inc.

An 802.1Q trunk and its associated trunk ports have a native VLAN value. When configuring an 802.1Q trunk, a matching native VLAN must be defined on each end of the trunk link. 802.1Q does not tag frames for the native VLAN. Therefore, ordinary stations can read the native untagged frames but cannot read any other frame because the frames are tagged.

Note The default native VLAN is VLAN 1.

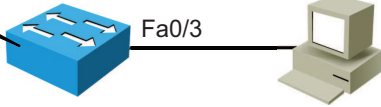
Do Not Duplicate:
Post beta, not for release.

Creating a VLAN

This topic describes how to create a VLAN.

Creating a VLAN

Create VLAN 2



```
SwitchX# configure terminal
SwitchX(config)# vlan 2
SwitchX(config-vlan)# name Sales
```

- Adds VLAN 2 and names it "Sales"

© 2013 Cisco Systems, Inc.

The table lists the commands to use when adding a VLAN.

Command and Variable	Description
vlan <i>vlan-id</i>	ID of the VLAN to be added and configured. Do not enter leading zeros. You can enter a single VLAN ID, a series of VLAN IDs that are separated by commas, or a range of VLAN IDs that are separated by hyphens.
name <i>vlan-name</i>	(Optional) Specify the VLAN name, which is an ASCII string from 1 to 32 characters that must be unique within the administrative domain.

For many Cisco Catalyst switches, you use the **vlan** global configuration command to create a VLAN and enter VLAN configuration mode. Use the **no** form of this command to delete the VLAN. The example shows how to add VLAN 2 to the VLAN database and how to name it “Sales.”

To add a VLAN to the VLAN database, assign a number and name to the VLAN. VLAN 1 is the factory default VLAN. Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.

Configurations for VLAN IDs 1 to 1005 are written to the `vlan.dat` file (VLAN database). You can display the VLANs by entering the **show vlan** privileged EXEC command. The `vlan.dat` file is stored in flash memory.

To add an Ethernet VLAN, you must specify at least a VLAN number. If no name is entered for the VLAN, the default is to append the VLAN number to the **vlan** command. For example, `VLAN0004` would be the default name for VLAN 4 if no name is specified.

For more details about the **vlan** (VLAN configuration mode) command, see the Cisco IOS LAN Switching Command Reference at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_16.html.

Creating a VLAN (Cont.)

```
SwitchX# show vlan id 2
```

VLAN Name	Status	Ports
2 Sales	active	Fa0/2, Fa0/12

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
2	enet	100002	1500	-	-	-	-	-	0	0

<output omitted>

- Verifies VLAN2

After you configure the VLAN, validate the parameters for this VLAN.

Use the **show vlan id** *vlan_number* or the **show vlan name** *vlan-name* command to display information about a particular VLAN. The figure shows an example of using the **show vlan** command to display the contents of the `vlan.dat` file. The “Sales” VLAN, which is VLAN 2, is highlighted in the example.

Use the **show vlan** command to display information on all configured VLANs. The **show vlan** command displays the switch ports that are assigned to each VLAN.

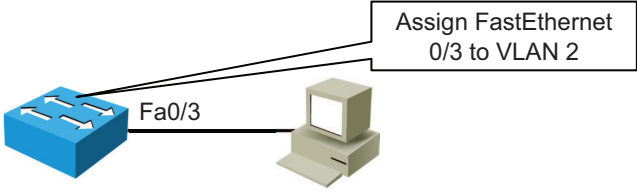
For more details about the **show vlan** command, see the Cisco IOS LAN Switching Command Reference at the following URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_14.html

Assigning a Port to a VLAN

This topic shows how to assign a port to a VLAN.

Assigning a Port to a VLAN



```
SwitchX# configure terminal
SwitchX(config)# interface FastEthernet 0/3
SwitchX(config-if)# switchport access vlan 2
```

- Assigns port FastEthernet0/3 to VLAN 2

© 2013 Cisco Systems, Inc.

The table lists the commands to use when assigning a port to a VLAN.

Command and Variable	Description
interface <i>interface</i>	Enters interface configuration mode
switchport access vlan <i>vlan_number</i>	Sets a nontrunking, untagged single VLAN Layer 2 interface

When an end system is connected to a switch port, it should be associated with a VLAN, in accordance with the network design. To associate a device with a VLAN, the switch port to which the device connects is assigned to a single-data VLAN and therefore becomes an access port.

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

Note By default, all ports are members of VLAN 1.

Assigning a Port to a VLAN (Cont.)

```
SwitchX# show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1
2    Sales                   active    Fa0/3
3    vlan3                   active
4    vlan4                   active
<output omitted>
```

- Verifies that port FastEthernet0/3 was assigned to VLAN 2

© 2013 Cisco Systems, Inc.

Assigning a Port to a VLAN (Cont.)

```
SwitchX# show interface FastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (Sales)
<output omitted>
```

- Verifies VLAN membership on the Fa0/3 interface

© 2013 Cisco Systems, Inc.

Use the **show vlan** privileged EXEC command to display the VLAN assignment and membership type for all switch ports. The **show vlan** command displays one line for each VLAN. The output for each VLAN includes the VLAN name, status, and switch ports.

For more details about the **show vlan** command, see the Cisco IOS LAN Switching Command Reference at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_14.html.

Alternatively, use the **show interfaces switchport** privileged EXEC command to display the VLAN information for a particular interface. The output in the example shows information about interface Fa0/3, where VLAN 2, named “Sales,” is assigned.

For more details about the **show interfaces switchport** command, see the Cisco IOS LAN Switching Command Reference at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_13.html.

Do Not Duplicate:
Post beta, not for release.

Configuring an 802.1Q Trunk

This topic shows how to configure an IEEE 802.1Q trunk.

Configuring an 802.1Q Trunk

- Enter the interface configuration mode.
- Configure the Fa0/11 interface as a VLAN trunk.
- Change the native VLAN from 1 to 99.

```
SwitchX# configure terminal
SwitchX(config)# interface FastEthernet 0/11
SwitchX(config-if)# switchport mode trunk
SwitchX(config-if)# switchport trunk native vlan 99
```

© 2013 Cisco Systems, Inc.

Command and Variable	Description
<code>interface interface</code>	Enters interface configuration mode.
<code>switchport mode trunk</code>	Sets the interface type. The keyword trunk specifies a trunking VLAN Layer 2 interface.
<code>switchport trunk native vlan vlan_number</code>	Sets the native VLAN for the trunk in 802.1Q trunking mode.

The example configures the FastEthernet0/11 port on SwitchX as a trunk port. Use the **switchport mode** interface configuration command to set a Fast Ethernet port to trunk mode. Many Cisco Catalyst switches support DTP, which manages automatic trunk negotiation. DTP is a Cisco proprietary protocol. Switches from other vendors do not support DTP. DTP is automatically enabled on a switch port when certain trunking modes are configured on the switch port. DTP manages trunk negotiation only if the port on the other switch is configured in a trunk mode that supports DTP.

The example shows the configuration of FastEthernet interface 0/11. The **switchport trunk mode** command sets FastEthernet port 0/11 to trunk mode. The example shows the reconfiguration of the native VLAN. VLAN 99 is configured as native VLAN. Therefore, traffic from VLAN 99 will be sent untagged, so management traffic such as Cisco Discovery Protocol and STP will now be sent from this switch in this VLAN instead of VLAN 1.

Ensure that the other end of the trunk link (SwitchY) is configured for trunking and with the native VLAN that is changed to 99.

Note For details on all of the parameters that are associated with the **switchport mode** interface command, visit http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_15.html.

Configuring an 802.1Q Trunk (Cont.)

```
SwitchX# show interfaces FastEthernet0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 99
Trunking Native Mode VLAN: 99
<output omitted>
```

```
SwitchX# show interfaces FastEthernet0/11 trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/11    on        802.1q         trunking    99
Port      Vlans allowed on trunk
Fa0/11    1-4094
Port      Vlans allowed and active in management domain
Fa0/11    1-13
<output omitted>
```

- Verifies a trunk on the Fa0/11 interface

© 2013 Cisco Systems, Inc.

To verify a trunk configuration on a switch, use the **show interfaces switchport** and **show interfaces trunk** commands. These two commands display the trunk parameters and VLAN information of the port.

For more details about the **show interfaces switchport** and **show interfaces trunk** commands, see the Cisco IOS Interface and Hardware Component Command Reference at <http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s5.html>.

VLAN Design Considerations

This topic explains what you should be aware of when you segment your network with VLANs.

VLAN Design Considerations

- The maximum number of VLANs is switch-dependent.
- VLAN 1 is the factory-default Ethernet VLAN.
- A use-dedicated VLAN is for the Cisco switch management IP address.
- Keep management traffic in a separate VLAN.
- Change the native VLAN to something other than VLAN 1.

© 2013 Cisco Systems, Inc.

Typically, access-layer Cisco switches support up to 64, 256, or 1024 VLANs. The maximum number of VLANs is switch dependent.

Cisco switches have a factory-default configuration in which various default VLANs are preconfigured to support various media and protocol types. The default Ethernet VLAN is VLAN 1. Cisco Discovery Protocol advertisements are sent on VLAN 1. A good security practice is to separate management and user data traffic because you do not want users to be able to establish Telnet sessions to the switch.

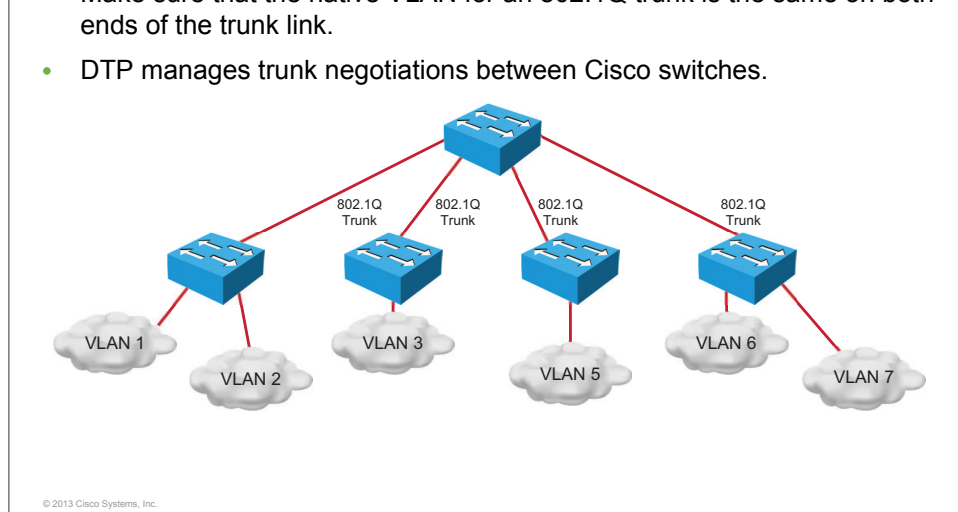
If you want to communicate with the Cisco switch remotely for management purposes, the switch must have an IP address. This IP address must be in the management VLAN, which by default is VLAN 1.

A good security practice is to change the native VLAN to something other than VLAN 1 (for example, VLAN 98) and tag native VLAN traffic.

VLAN Design Considerations (Cont.)

When configuring a trunk link, consider the following:

- Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link.
- DTP manages trunk negotiations between Cisco switches.

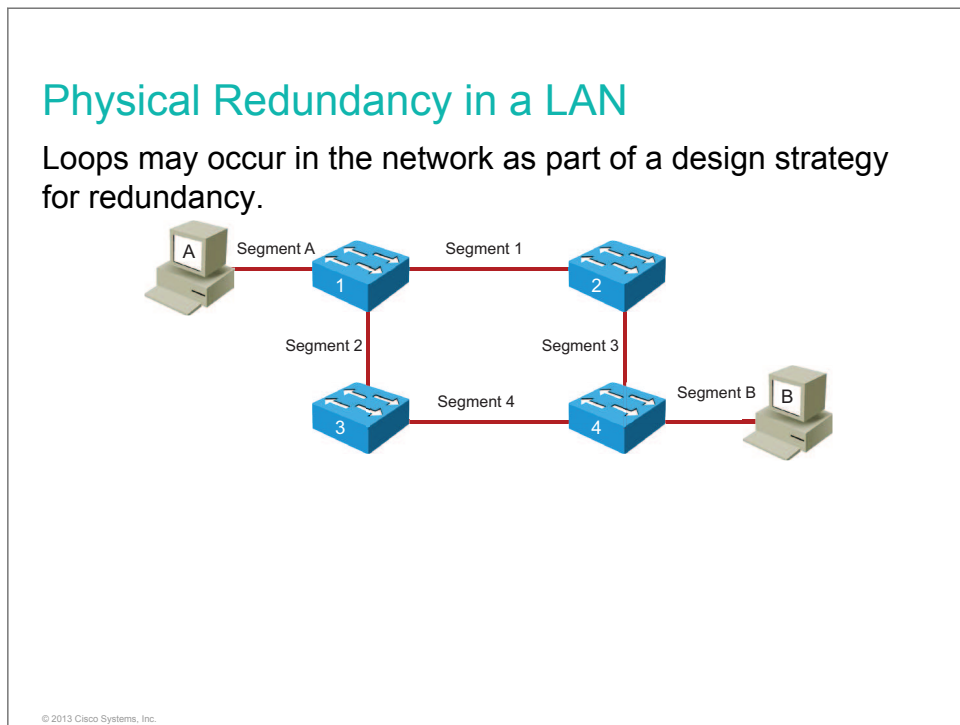


Ensure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the ends are different, spanning-tree loops might result. If IEEE 802.1Q trunk configuration is not the same on both ends, Cisco IOS Software will report error messages. Also ensure that native VLAN frames are untagged.

DTP offers four switchport modes: switch, trunk, dynamic auto, and dynamic desirable. A general guideline is to disable autonegotiation. That is, do not use the dynamic auto and dynamic desirable switchport modes. For details on all of the parameters that are associated with the **switchport mode** interface command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_15.html.

Physical Redundancy in a LAN

This topic describes how loops can affect performance in a switched LAN and introduces STP as a solution.



Adding switches to LANs can add the benefit of redundancy. Connecting two switches to the same network segments ensures continuous operation if there are problems with one of the segments. Redundancy can ensure the availability of the network at all times.

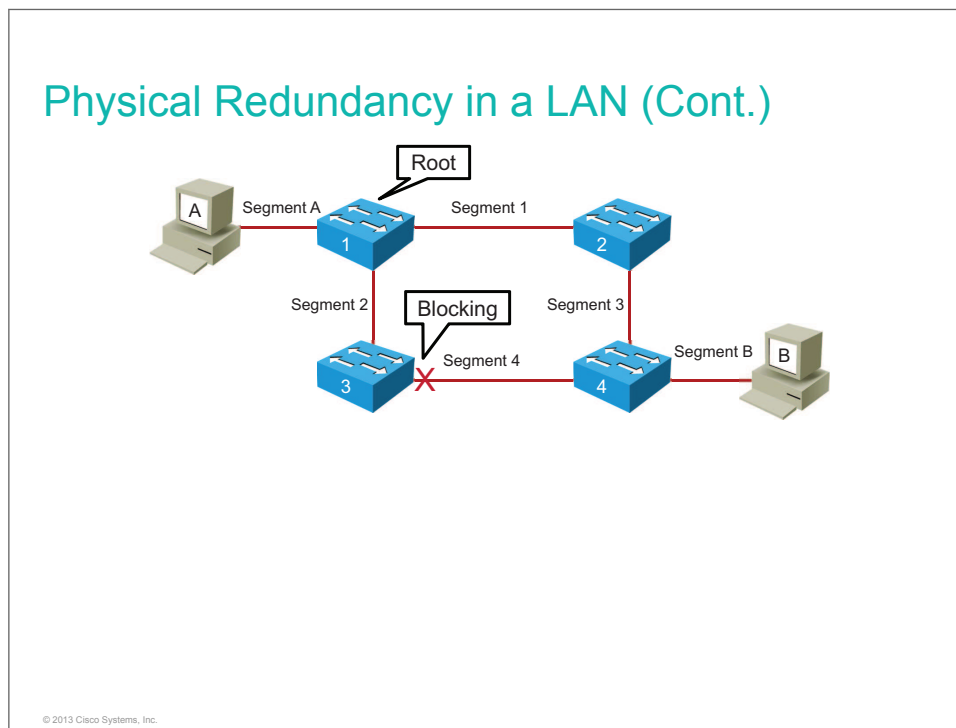
However, when switches are used for redundancy in a network, loops are a potential problem. When a host on one network segment transmits data to a host on another network segment, and the two are connected by two or more switches, each switch receives the data frames, looks up the location of the receiving device, and forwards the frame. Because each switch forwards the frame, each frame is duplicated. A loop results, and the frame circulates between the two paths without being removed from the network. The MAC tables may also be updated with incorrect address information, resulting in inaccurate forwarding.

Suppose that a host named A sends a frame to a host named B. Host A resides on network segment A, and host B resides on network segment B. Redundant connections between hosts are provided to ensure continuous operation if a segment fails. For this example, it is assumed that none of the switches have learned the address of host B.

Switch 1 receives the frame that is destined for host B and floods it out to switches 2 and 3. Switches 2 and 3 both receive the frame from host A (via switch 1) and correctly learn that host A is on segments 1 and 2, respectively. Each switch forwards the frame to switch 4.

Switch 4 receives two copies of the frame from host A: one copy through switch 2 and one copy through switch 3. Assume that the frame from switch 2 arrives first. Switch 4 learns that host A resides on segment 3. Because switch 4 does not know where host B is connected, it forwards the frame to all of its ports (except the incoming port) and therefore to host B and switch 3. When the frame from switch 3 arrives at switch 4, switch 4 updates its table to indicate that host A resides on segment 4. It then forwards the frame to host B and switch 2.

Switches 2 and 3 now change their internal tables to indicate that host A is on segments 3 and 4. If the initial frame from host A is a broadcast frame, both switches forward the frames endlessly. They would use all of the available network bandwidth and block transmission of other packets on both segments. This situation is called a *broadcast storm*.



The solution to loops is STP, which manages the physical paths to given network segments. STP provides physical path redundancy while preventing the undesirable effects of active loops in the network. STP is on by default in Cisco Catalyst switches.

STP behaves as follows:

- STP forces certain ports into a standby state so that they do not listen to, forward, or flood data frames. The overall effect is that there is only one path to each network segment that is active at any time.
- If there is a problem with connectivity to any of the segments within the network, STP re-establishes connectivity by automatically activating a previously inactive path, if one exists.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- VLANs are independent LAN networks and address segmentation, security, and organizational flexibility.
- Ethernet trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across many switches.
- To implement VLANs and trunking, you need to create VLANs, configure trunk links, and assign switch ports to selected VLANs.
- Physical redundancy is required for network reliability.
- STP ensures a loop-free topology.

© 2013 Cisco Systems, Inc.

Routing Between VLANs

Routing is the process of determining where to send data packets that are destined for addresses outside of the local network. Routers gather and maintain routing information to enable the transmission and receipt of data packets. For traffic to cross from one VLAN to another, a Layer 3 process is necessary.

This lesson describes the basics of inter-VLAN routing operations, including subinterfaces and routers with a trunk link.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

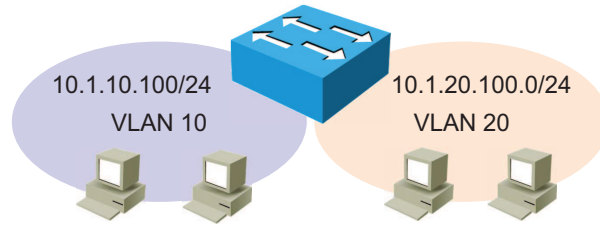
- Describe the need for inter-VLAN routing
- Describe options for inter-VLAN routing
- Configure router with a trunk link

Purpose of Inter-VLAN Routing

This topic describes the concept and purpose of inter-VLAN routing.

Purpose of Inter-VLAN Routing

- A VLAN creates a separate switching segment.
- Traffic cannot be switched between VLANs.
- VLANs have different IP subnets.
- Routing is necessary to forward traffic between VLANs.



Each VLAN is a unique broadcast domain. Computers on separate VLANs are, by default, not able to communicate. The way to permit these end stations to communicate is to use a solution called *inter-VLAN routing*. Inter-VLAN communication occurs between broadcast domains via a Layer 3 device.

VLANs perform network partitioning and traffic separation at Layer 2 and are usually associated with unique IP subnets on the network. This subnet configuration facilitates the routing process in a multi-VLAN environment. Inter-VLAN communication cannot occur without a Layer 3 device. When you use a router to facilitate inter-VLAN routing, the router interfaces can be connected to separate VLANs.

Options for Inter-VLAN Routing

Options for Inter-VLAN Routing

These solutions can provide inter-VLAN routing:

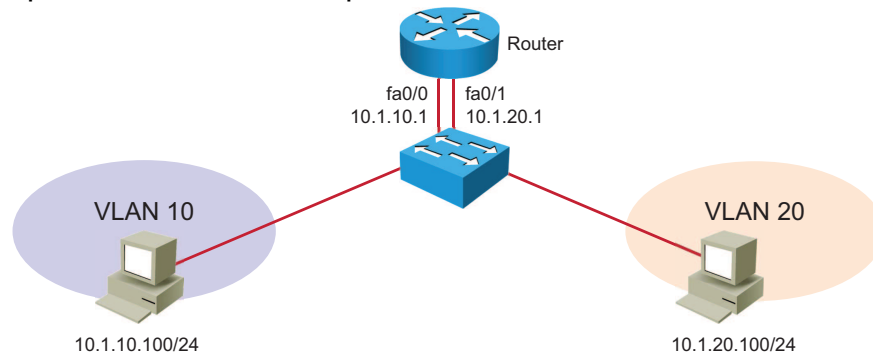
- Router with a separate interface in each VLAN
- Router with a trunk link
- Layer 3 switch

© 2013 Cisco Systems, Inc.

Inter-VLAN routing is a process of forwarding network traffic from one VLAN to another VLAN using a Layer 3 device.

Options for Inter-VLAN Routing (Cont.)

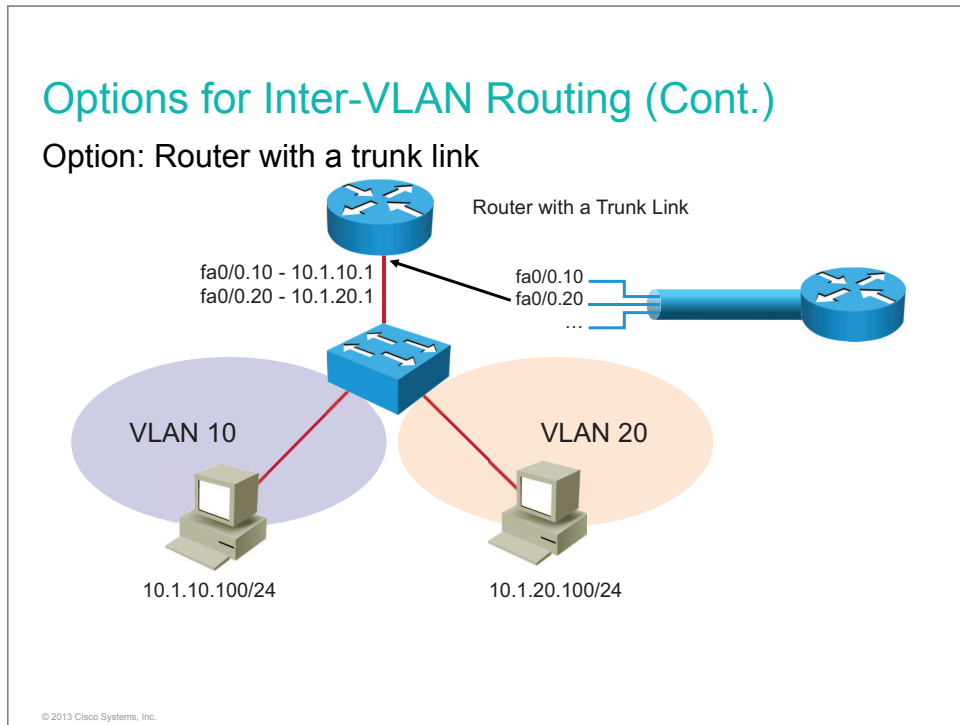
Option: Router with a separate interface in each VLAN



© 2013 Cisco Systems, Inc.

Traditional inter-VLAN routing requires multiple physical interfaces on both the router and the switch. VLANs are associated with unique IP subnets on the network. This subnet configuration facilitates the routing process in a multi-VLAN environment. When using a router to facilitate inter-VLAN routing, the router interfaces can be connected to separate VLANs. Devices on those VLANs send traffic through the router to reach other VLANs.

When you use a separate interface for each VLAN on a router, you can quickly run out of interfaces. This solution is not very scalable.



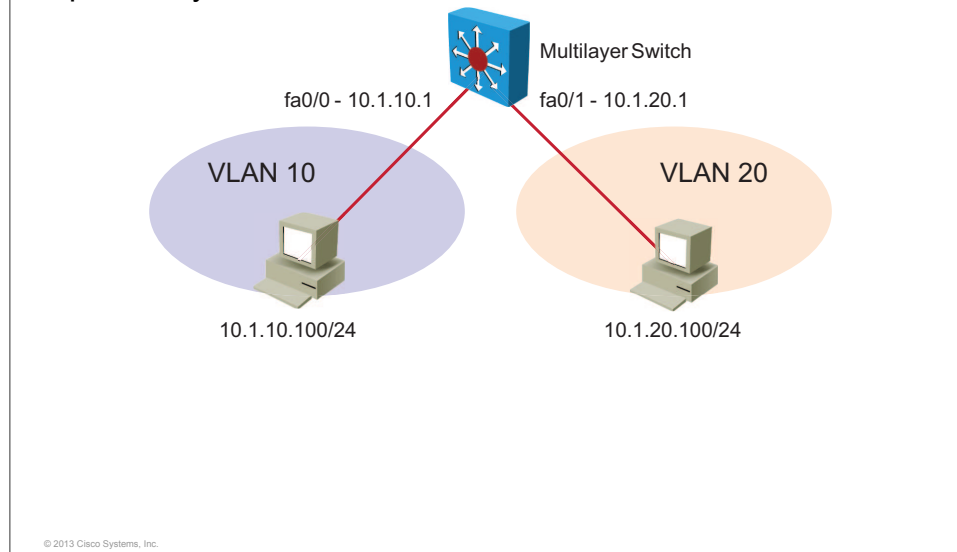
Not all inter-VLAN routing configurations require multiple physical interfaces. Some router software permits configuring router interfaces as trunk links. Trunk links open up new possibilities for inter-VLAN routing. A router with a trunk link is a type of router configuration in which a single physical interface routes traffic between multiple VLANs on a network.

The figure shows a router that is attached to a core switch. The configuration between a router and a core switch is sometimes referred to as a *router on a stick*. The router interface is configured to operate as a trunk link and is connected to a switch port that is configured in trunk mode. The router performs inter-VLAN routing by accepting VLAN-tagged traffic on the trunk interface coming from the adjacent switch and internally routing between the VLANs using subinterfaces. (Subinterfaces are multiple virtual interfaces that are associated with one physical interface.) To perform inter-VLAN routing functions, the router must know how to reach all VLANs that are being interconnected. There must be a separate logical connection on the router for each VLAN, and VLAN trunking (such as IEEE 802.1Q) must be enabled on those connections. The router already knows about directly connected networks. The router then forwards the routed VLAN traffic that is tagged for the destination VLAN out the same physical interface.

These subinterfaces are configured in software. Each is independently configured with its own IP addresses and a VLAN assignment to operate on a specific VLAN. Subinterfaces are configured for different subnets corresponding to their VLAN assignment to facilitate logical routing before the data frames are VLAN-tagged and sent back out the physical interface.

Options for Inter-VLAN Routing (Cont.)

Option: Layer 3 switch



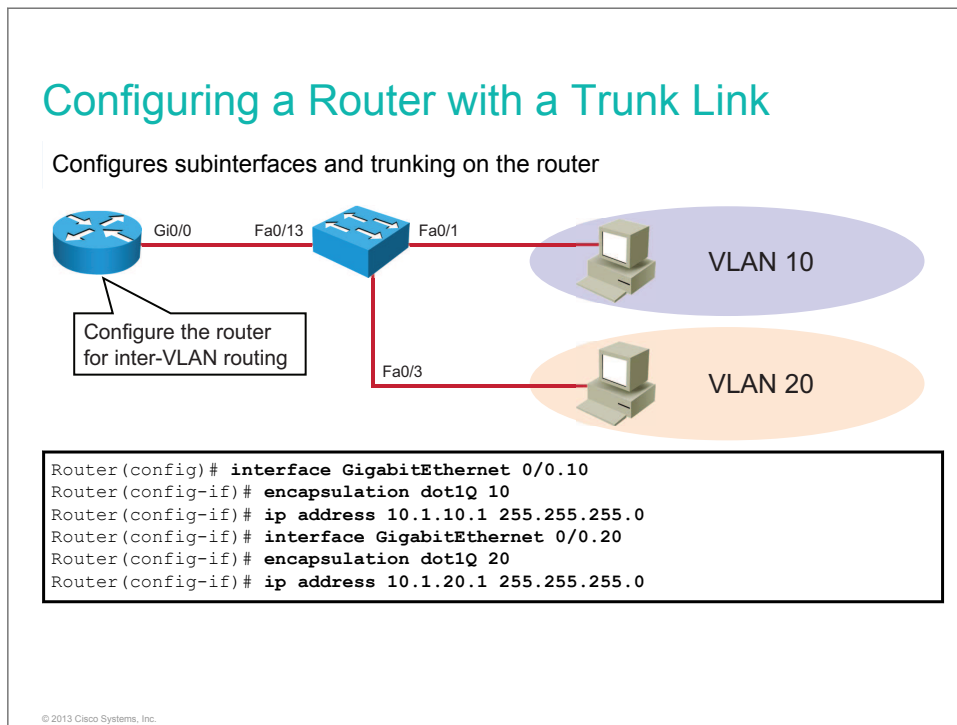
Some switches can perform Layer 3 functions, replacing the need for dedicated routers to perform basic routing on a network. Layer 3 switches are capable of performing inter-VLAN routing. Traditionally, a switch makes forwarding decisions by looking at the Layer 2 header, while a router makes forwarding decisions by looking at the Layer 3 header. A layer 3 switch combines the functionality of a switch and a router into one device. It switches traffic when the source and destination are in the same VLAN and routes traffic when the source and destination are in different VLANs (that is, on different IP subnets). To enable a Layer 3 switch to perform routing functions, VLAN interfaces on the switch need to be properly configured. You must use the IP addresses that match the subnet that the VLAN is associated with on the network. The Layer 3 switch must also have IP routing enabled.

Layer 3 switching is more scalable than routers with a trunk link because the latter can only have so much traffic through the trunk link. In general, a Layer 3 switch is primarily a Layer 2 device that has been upgraded to have some routing capabilities. A router is a Layer 3 device that can perform some switching functions.

However, the line between switches and routers becomes hazier every day. Some Layer 2 switches, such as the switches in the Cisco Catalyst 2960 Series, support limited Layer 3 functionality. The Catalyst 2960 switch supports static routing on SVIs. Static routes can be configured, but routing protocols are not supported. For more information, go to http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swipstatrout.html.

Configuring a Router with a Trunk Link

This topic demonstrates how to configure a router on a stick.



Command and Variable	Description
interface <i>interface</i>	Enters interface configuration mode
encapsulation dot1Q <i>vlan_number</i>	Defines the encapsulation format as IEEE 802.1Q and specifies the VLAN identifier
ip address <i>ip_address network_mask</i>	Assigns an IP address and network mask to an interface

In the figure, the GigabitEthernet0/0 interface is divided into subinterfaces: GigabitEthernet0/0.10 and GigabitEthernet0/0.20. Each subinterface represents the router in each of the VLANs for which it routes.

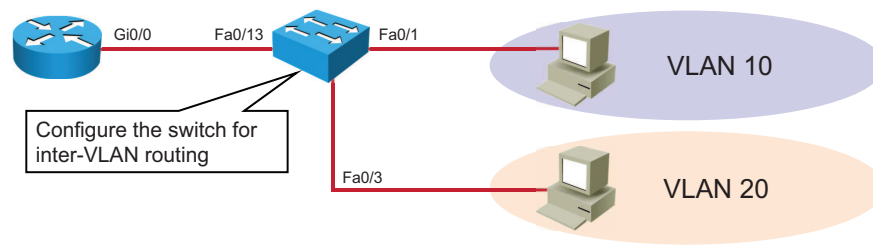
In the example, the **encapsulation dot1q 20** command enables 802.1Q encapsulation trunking on the GigabitEthernet0/0.20 subinterface. The value 20 represents the VLAN number (or VLAN identifier), therefore associating 802.1Q-tagged traffic from this VLAN with the subinterface.

Each 802.1Q-tagged VLAN on the trunk link requires a subinterface with 802.1Q encapsulation trunking that is enabled in this manner. The subinterface number does not have to be the same as the dot1q VLAN number. However, management and troubleshooting are easier when the two numbers are the same.

In this example, devices in different VLANs use the subinterfaces of the router as gateways to access the devices that are connected to the other VLANs.

Configuring Router with a Trunk Link (Cont.)

Assigns ports to specific VLANs and configures the port toward the router as a trunk



```
Switch(config)# interface FastEthernet 0/13
Switch(config-if)# switchport mode trunk
Switch(config-if)# interface FastEthernet 0/1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# interface FastEthernet 0/3
Switch(config-if)# switchport access vlan 20
```

© 2013 Cisco Systems, Inc.

Command and Variable	Description
interface <i>interface</i>	Enters interface configuration mode.
switchport mode trunk	Sets the interface type. The trunk keyword specifies a trunking VLAN Layer 2 interface.
switchport access <i>vlan_number</i>	Sets the access VLAN when the interface is in access mode. To reset the access-mode VLAN to the appropriate default VLAN for the switch, use the no form of this command.

On the switch, assign interfaces to the appropriate VLANs and configure the interface toward the router as a trunk. The trunk link will carry traffic from different VLANs, and the router will route between those VLANs.

Configuring Router with a Trunk Link (Cont.)

Verifies the VLAN subinterfaces

```
Router# show vlans
<output omitted>
Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)
VLAN Trunk Interface: GigabitEthernet0/0.10
  Protocols Configured:  Address:      Received:  Transmitted:
                        IP            10.1.10.1    11         18
<output omitted>
Virtual LAN ID: 20 (IEEE 802.1Q Encapsulation)
VLAN Trunk Interface: GigabitEthernet0/0.20
  Protocols Configured:  Address:      Received:  Transmitted:
                        IP            10.1.20.1    11         8
<output omitted>
```

© 2013 Cisco Systems, Inc.

To verify the router configuration, use **show** commands to display the current (running) configuration, IP routing information, and IP protocol information per VLAN to verify that the routing table represents the subnets of all VLANs.

The **show vlans** command displays the information about the Cisco IOS VLAN subinterfaces. The sample output shows two VLAN subinterfaces, FastEthernet0/0.10 and FastEthernet0/0.20.

Configuring Router with a Trunk Link (Cont.)

Verifies the IP routing table for VLAN subinterfaces

```
Router# show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L    10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C    10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
L    10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
```

© 2013 Cisco Systems, Inc.

The **show ip route** command displays the current state of the routing table. The sample output shows two subinterfaces. The GigabitEthernet0/0.10 and GigabitEthernet0/0.20 VLAN subinterfaces are directly connected to the router.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Inter-VLAN communication cannot occur without a Layer 3 device (Layer 3 switch or router).
- Routing is necessary to forward traffic between VLANs.
- A router with a trunk link is configured with a subinterface for each VLAN.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Using a Cisco Network Device as a DHCP Server

Originally, network administrators had to manually configure the host address, default gateway, and other network parameters on each host. However, DHCP provides these parameters dynamically. This lesson describes the use of a Cisco router as a DHCP server.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the need for dynamic host IP address assignment
- Describe DHCP operation
- Configure a DHCP server
- Describe how to monitor DHCP server functions
- Describe the DHCP relay agent mechanism

Need for a DHCP Server

This topic describes the need for a DHCP server in medium-sized LANs.

Need for a DHCP Server

A manual IP address assignment in a medium-sized LAN is as follows:

- Time consuming
- Prone to errors
- Unfavorable to employee mobility

A DHCP IP address assignment in a segmented LAN is as follows:

- An IP address that is automatically assigned in accordance with user VLAN settings
- A centralized IP address allocation that enables consistency across the whole organization

© 2013 Cisco Systems, Inc.

While manual assignment of IP addresses to network hosts is acceptable in small networks, it can present an administrative burden in medium-sized LANs.

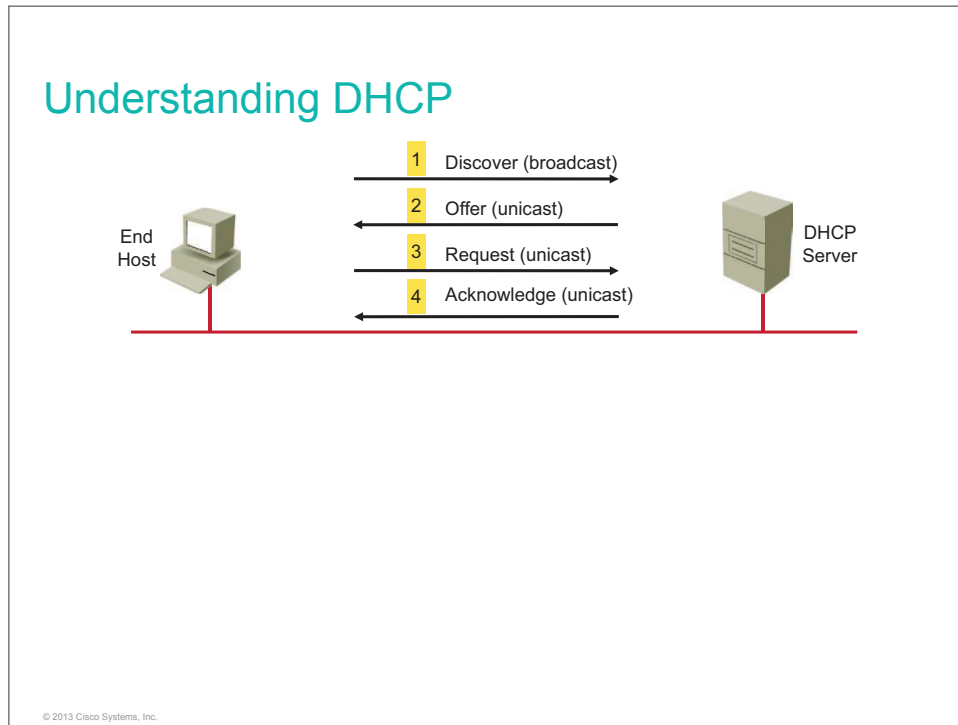
Manually setting all network connectivity parameters on the end host whenever it is moved or replaced can be a time-consuming task for administrators. For mobile employees, who usually work from home and occasionally come into the office, manually setting the correct network parameters can be challenging. In addition, manual settings may be incorrect, or equipment brought to the office may already have settings in place. The result could be poor network connectivity on the host or even a problem for other users if a host with a duplicate IP address is connected to the local network.

Introducing a DHCP server to the local network simplifies IP address assignment. A DHCP server is commonly used in small networks to support frequent changes and to assign correct IP addresses to guest hosts that are connecting to a LAN. An even greater contribution to simplified administration is seen when LANs are segmented using VLANs. A DHCP server automatically assigns IP addresses to end hosts according to the VLAN assignment of the host.

Using a centralized DHCP server enables organizations to administer all dynamic IP address assignments in one place. This practice ensures consistency across the organization, and branch offices, for example, can be easily managed.

Understanding DHCP

This topic describes how DHCP operates.



DHCP dynamic allocation of IP addresses is based on a client-server model. The figure displays an example of how an end host obtains an IP address from a DHCP server.

When DHCP dynamically allocates an IP address, the operation can be divided into the following phases:

- 1 **DHCP discover:** A client broadcasts a DHCP discover message with its own hardware MAC address to discover available DHCP servers.
- 2 **DHCP offer:** When a DHCP server receives a DHCP discover from a client, it reserves an IP address for the client and sends a DHCP offer to the client. This message contains the client MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server that is making the offer.
- 3 **DHCP request:** When a client receives a DHCP offer message, it responds with a DHCP request message, indicating its intent to accept the parameters in the DHCP offer. A DHCP request message is broadcast because the DHCP client has still not received an acknowledged IP address.
- 4 **DHCP acknowledgment:** After the DHCP server receives the DHCP request message, it acknowledges the request with a unicast DHCP acknowledgment message. The packet includes confirmation for all requested parameters. At this point, the IP configuration process is completed.

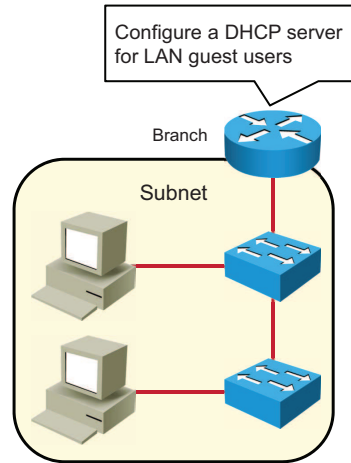
Configuring a DHCP Server

This topic describes how to configure a DHCP server on a Cisco IOS device.

Configuring a DHCP Server

Configuration scenario:

- Configure a DHCP server on a Cisco router
- Assign IP addresses from address pool 10.1.50.0/24 with a lease time of 12 hours
- Do not assign IP addresses from 10.1.50.1 to 10.1.50.50
- Additional parameters: default gateway, domain name, and DNS server



© 2013 Cisco Systems, Inc.

In this example configuration scenario, a DHCP server will be configured on a Cisco IOS router. Guest LAN users need to receive an IP address from the specified address pool along with a default gateway, domain name, and IP address of a DNS server. The IP address assignment should be valid for 12 hours.

Note A DHCP server can also be implemented on Cisco Catalyst switches.

Configuring a DHCP Server (Cont.)

Cisco IOS DHCP server configuration:

- Enter the DHCP pool configuration mode
- Assign DHCP parameters to the DHCP pool
- Exclude IP addresses from the DHCP assignment

```
Branch(config)# ip dhcp pool Guests
Branch(dhcp-config) #network 10.1.50.0 /24
Branch(dhcp-config) # default-router 10.1.50.1
Branch(dhcp-config) # dns-server 10.1.50.1
Branch(dhcp-config) # domain-name example.com
Branch(dhcp-config) # lease 0 12
Branch(dhcp-config) # exit
Branch(config)# ip dhcp excluded-address 10.1.50.1 10.1.50.50
```

© 2013 Cisco Systems, Inc.

To enable the Cisco IOS DHCP server, enter DHCP configuration mode by defining a DHCP pool. Use the commands that are shown in the table to define the pool parameters.

Command	Description
ip dhcp pool <i>name</i>	Defines the pool name and enters DHCP configuration mode.
network <i>network-number</i> [<i>mask</i> <i>prefix-length</i>]	Defines addresses in the DHCP pool. Optionally, define a subnet mask or prefix length to define the network part.
default-router <i>address</i>	Specifies the IP address of the default router for a DHCP client.
domain-name <i>domain</i>	Specifies the domain name for the DHCP client.
lease { <i>days</i> [<i>hours</i>] [<i>minutes</i>] <i>infinite</i> }	Specifies the duration of the lease. The default is a one-day lease.
ip dhcp excluded-address <i>ip-address</i> [<i>last-ip-address</i>]	In global configuration mode, specifies a single excluded IP address or range of addresses that a DHCP server should not assign to DHCP clients.

Monitoring DHCP Server Functions

This topic describes verification commands that can be used to monitor and verify a DHCP server implementation on Cisco IOS Software.

Monitoring DHCP Server Functions

```
Branch# show ip dhcp pool
Pool Guests :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 2
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
10.1.50.55 10.1.50.1 - 10.1.50.254 2
```

- Verifies information about configured DHCP address pools

You can verify configured DHCP parameters using the **show ip dhcp pool** command in privileged EXEC mode. The total number of available addresses, configured address range, and number of leased addresses is displayed. Keep in mind that the total addresses number does not take excluded IP addresses into account.

For more details about the **show ip dhcp pool** command, refer to Cisco IOS IP Addressing Services Command Reference at <http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-23A47402-6EB5-4945-8DEB-ABCB7BCF3D68>

Monitoring DHCP Server Functions (Cont.)

```
Branch# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration      Type
Hardware address/
User name
10.1.50.54      0100.0c29.8807.34  Oct 18 2012 06:56 PM  Automatic
10.1.50.56      0100.0c29.4532.be  Oct 18 2012 07:08 PM  Automatic
```

- Displays address bindings information

© 2013 Cisco Systems, Inc.

To verify the operation of a DHCP server, use the **show ip dhcp binding** command, which displays a list of all IP address-to-MAC address bindings that have been provided by the DHCP service. Additionally, the lease expiration time and type of DHCP allocation are listed.

Monitoring DHCP Server Functions (Cont.)

```
Branch# show ip dhcp conflict
IP address      Detection method  Detection time      VRF
10.1.50.52      Gratuitous ARP    Oct 18 2012 06:56 AM
10.1.50.53      Ping              Oct 18 2012 07:08 AM
```

- Displays the address conflicts that are found by a DHCP server
 - **IP Address:** The IP address of the host as recorded on the DHCP server
 - **Detection Method:** The manner in which the IP address of the hosts were found on the DHCP server; can be a ping or a gratuitous ARP
 - **Detection time:** The time when the conflict was found

© 2013 Cisco Systems, Inc.

To display address conflicts that are found by a DHCP server when addresses are offered to the client, use the **show ip dhcp conflict** command in user EXEC or privileged EXEC mode.

The server uses ping to detect conflicts. The client uses GARP to detect conflicts. If an address conflict is detected, the address is removed from the pool and the address is not assigned until an administrator resolves the conflict.

The output in the figure shows, for each conflicting IP address, how the conflict was detected and the time when it was detected.

You can clear conflicting IP addresses by using the **clear ip dhcp conflict** privileged EXEC command.

For more details about the **show ip dhcp conflict** command, refer to Cisco IOS IP Addressing Services Command Reference at <http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-5A27A4B1-4B2A-417D-8530-9F792D072454>.

Do Not Duplicate:
Post beta, not for release.

DHCP Relay Agent

This topic reviews the need for a centralized DHCP solution and describes how to support its implementation in a branch office.

DHCP Relay Agent

The need for a centralized DHCP solution:

- Managing individual DHCP servers across many locations is time-consuming.
- Ensuring consistency in several different places can easily lead to errors.

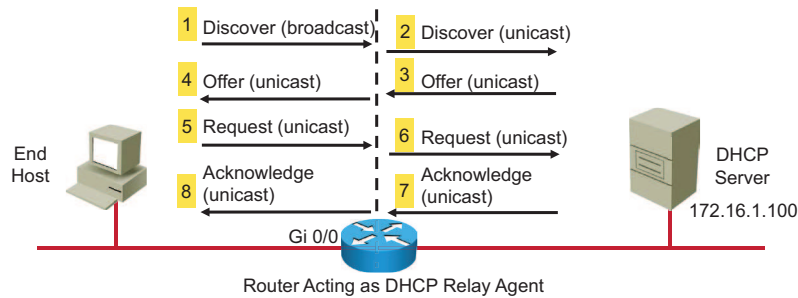
To support a centralized DHCP solution in branch offices, only the DHCP relay agent needs to be configured.

© 2013 Cisco Systems, Inc.

When DHCP clients try to obtain an IP address, they search for a DHCP server within their segment. Managing one DHCP server in each network segment can represent considerable administrative work. If DHCP servers are spread across different physical locations and are managed by different administrators, there is also a greater chance of human error.

A centralized DHCP solution enables an administrator to manage IP address assignment in one place for a whole organization. While DHCP servers are usually positioned in the center of the network infrastructure, other network devices can be configured with the DHCP relay agent functionality to enable clients to obtain an IP address from a central DHCP server.

DHCP Relay Agent (Cont.)



```
Branch(config-if)# ip helper-address 172.16.1.100
```

- Enables DHCP relay agent on a local interface

DHCP clients use UDP broadcasts to send their initial DHCP discover message because they do not have information about the network to which they are attached. If the client is on a network that does not include a DHCP server, broadcasts are normally not forwarded by the attached router.

To allow DHCP clients on subnets that are not directly served by DHCP servers to communicate with DHCP servers, DHCP relay agents can be installed on these subnets. You can configure the relay agent for a specific segment with the **ip helper-address** *address* interface configuration command, where you specify the IP address of a DHCP server.

When the DHCP relay agent receives the broadcast DHCP discover message, the relay agent transmits the message to one or more DHCP servers as a unicast packet after the relay agent stores its own IP address in the `giaddr` field of the DHCP packet. The DHCP server uses the `giaddr` to determine the subnet on which the relay agent received the broadcast and allocates an IP address belonging to the same subnet. When the DHCP server replies to the client, it sends the reply to the `giaddr` address, again using unicast. The relay agent receives the response and retransmits it on the local network.

Note The **ip helper-address** command enables forwarding of all of the well-known UDP ports that may be included in a UDP broadcast message.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- A DHCP server provides dynamic IP address assignment to end hosts, reducing errors and the time that is needed to administer address assignment.
- Before a client obtains an IP address from a DHCP server, it exchanges DHCP discover, offer, request, and acknowledge messages with the DHCP server.
- Both Cisco routers and Cisco Catalyst switches can be configured as DHCP servers.
- Use the verification commands **show ip dhcp pool**, **show ip dhcp binding**, and **show ip dhcp conflict** to monitor a DHCP server.
- When a centralized DHCP server is in use, configure DHCP relay agent functionality using the **ip helper-address** interface configuration command.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Introducing WAN Technologies

As an enterprise grows beyond a single location, it becomes necessary to interconnect LANs in various locations to form a WAN. Several technologies are involved in the functioning of WANs. This lesson describes the functions and characteristics of WANs.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

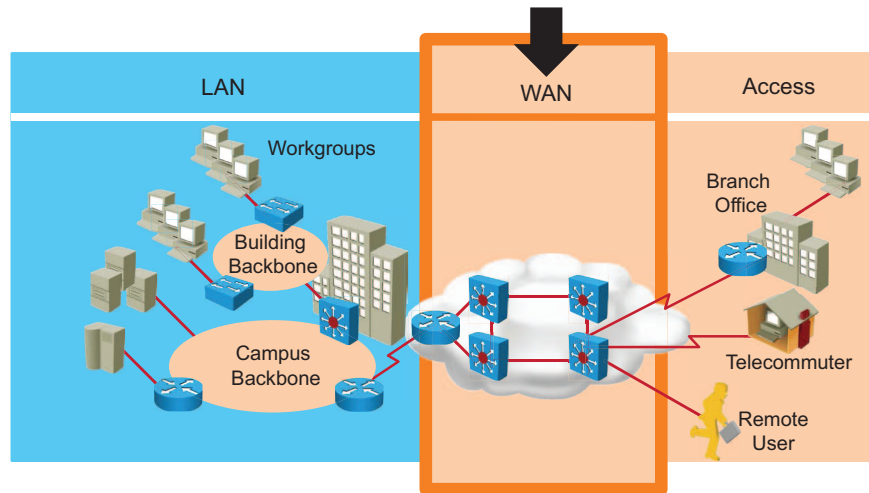
- Describe a WAN and explain the need for WANs
- Compare LANs and WANs
- Describe the role of routers for WAN access
- List the major options for WAN access communication links
- Describe Ethernet emulation for point-to-point connectivity
- Configure Ethernet interface for point-to-point connectivity

Introducing WANs

A WAN is a data communications network that operates beyond the geographic scope of a LAN. This topic describes the basic idea behind WANs.

Introducing WANs

What is a WAN?



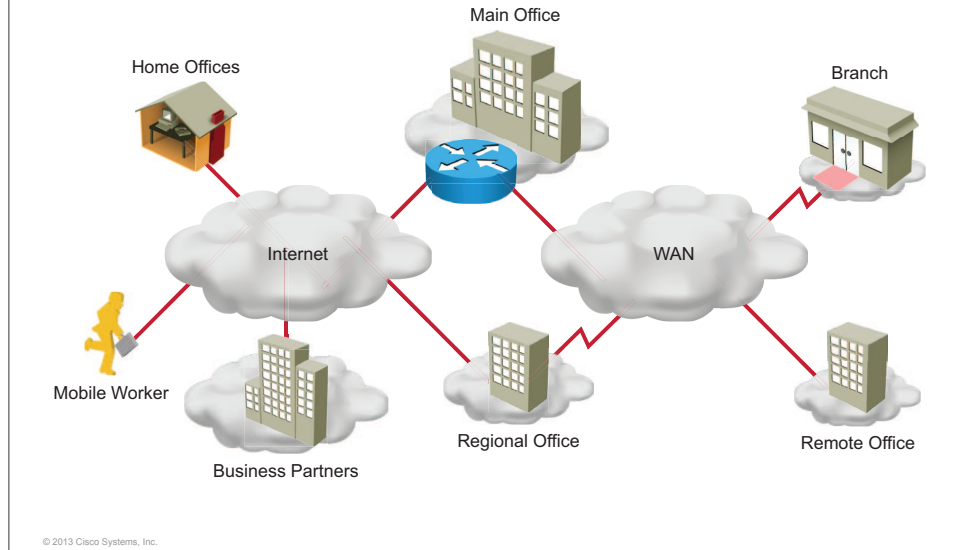
WANs use facilities that are provided by a service provider or carrier, such as a telephone or cable company. They connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs generally carry various traffic types such as voice, data, and video.

Here are the three major characteristics of WANs:

- WANs connect devices that are located over wide geographical areas.
- WANs use the services of carriers such as telephone companies, cable companies, satellite systems, and network providers.
- WANs use various connection types to provide access to bandwidth over large geographical areas.

Introducing WANs (Cont.)

Why are WANs needed?



There are several reasons why WANs are necessary in a communications environment. LAN technologies provide both speed and cost effectiveness for the transmission of data in organizations in relatively small geographic areas. However, there are other business needs that require communication among remote users:

- People in regional or branch offices of an organization need to be able to communicate and share data.
- Organizations often want to share information with other organizations across large distances. For example, software manufacturers routinely communicate product and promotion information to distributors that sell their products to end users.
- Employees who travel on company business or work from home frequently need to access information that resides on their corporate networks.

Because it is obviously not feasible to connect computers across a country or around the world with LAN cables, various technologies have evolved to meet this need. WANs allow organizations and individuals to meet their wide-area communications needs.

In recent years, several new technologies, which use Internet infrastructure to connect distant locations, matured to offer good alternatives to traditional WAN connectivity options.

WANs vs. LANs

This topic compares WANs and LANs.

WANs vs. LANs

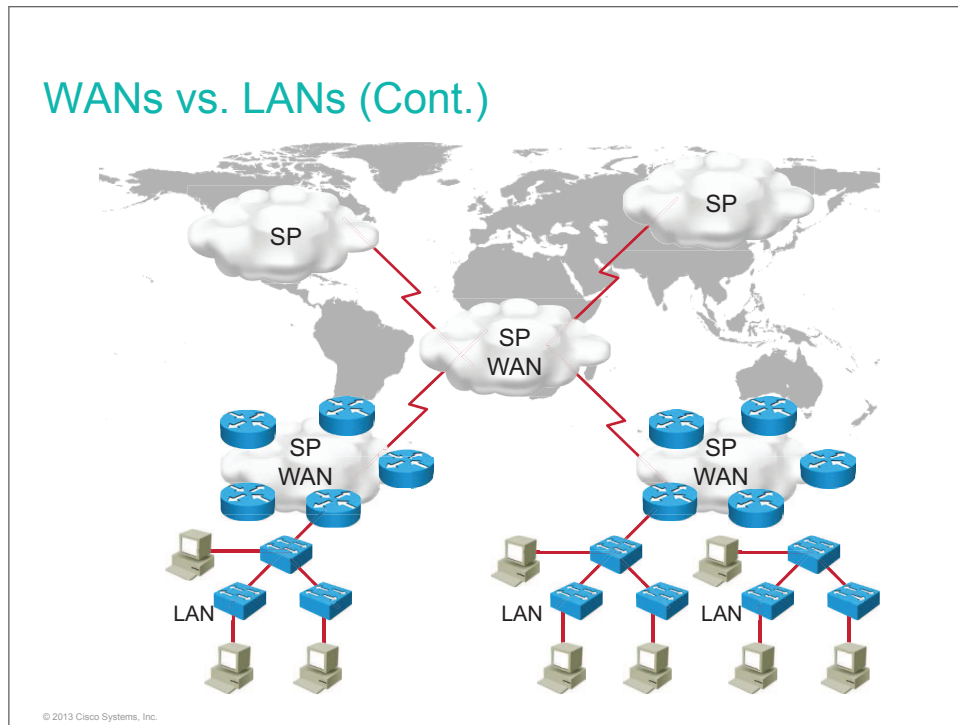
WAN = A collection of LANs

	WANs	LANs
Area	Wide geographic area	Single building or small geographic area
Ownership	Subscription to outside service provider	Owned by organization
Cost	Recurring	Fixed

© 2013 Cisco Systems, Inc.

WANs are different from LANs in several ways. The most significant differences are geographical area and ownership. A LAN connects computers, peripherals, and other devices in a single building or other small geographic area. A WAN allows the transmission of data across broad distances. In addition, a company or organization must subscribe to an outside WAN service provider to use WAN carrier network services. LANs are typically owned by the company or organization that uses them. This is reflected also in costs. While LANs usually require a one-time investment, WAN services normally involve a recurring monthly fee, which is paid to a service provider.

WANs vs. LANs (Cont.)

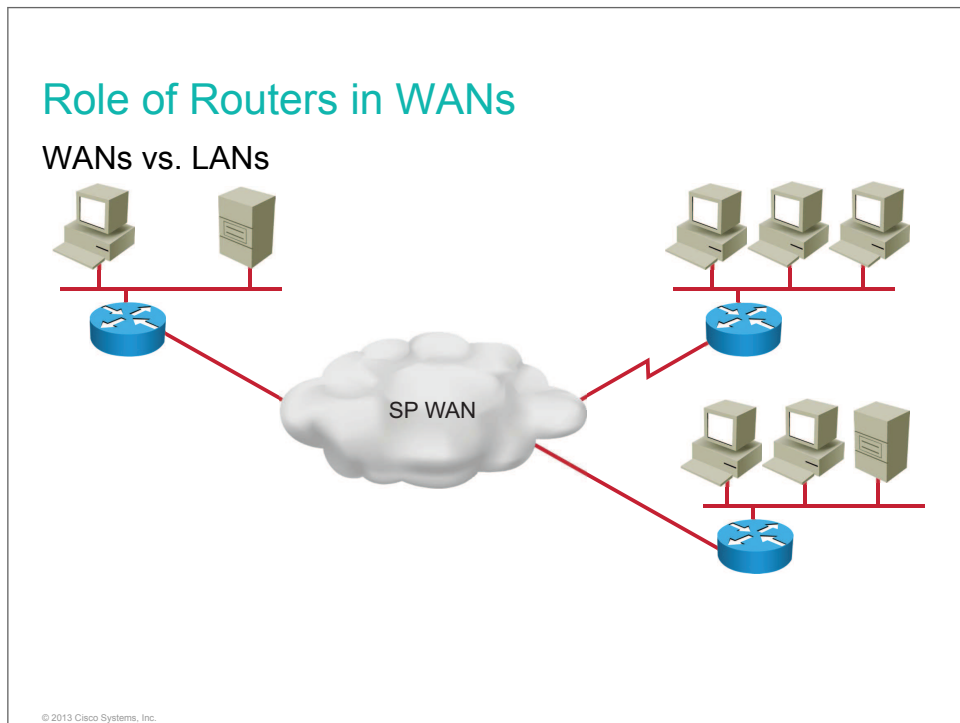


Some WANs are privately owned. However, because the development and maintenance of a private WAN is expensive, only very large organizations can afford to maintain a private WAN. Most companies purchase WAN connections from a service provider or ISP. The service provider is then responsible for maintaining the back-end network connections and network services between the LANs.

When an organization has many global sites, establishing WAN connections and service can be complex. For example, the major service provider for the organization may not offer service in every location or country in which the organization has an office. As a result, the organization must purchase services from multiple service providers. Using multiple service providers often leads to differences in the quality of the services that are provided. In many emerging countries, for example, network designers find differences in equipment availability, WAN services that are offered, and encryption technology for security. To support an enterprise network, it is important to have uniform standards for equipment, configuration, and services.

Role of Routers in WANs

An enterprise WAN is a collection of separate but connected LANs. Routers play a central role in transmitting data through this interconnected network. This topic describes the functions and role of the router in a WAN environment.

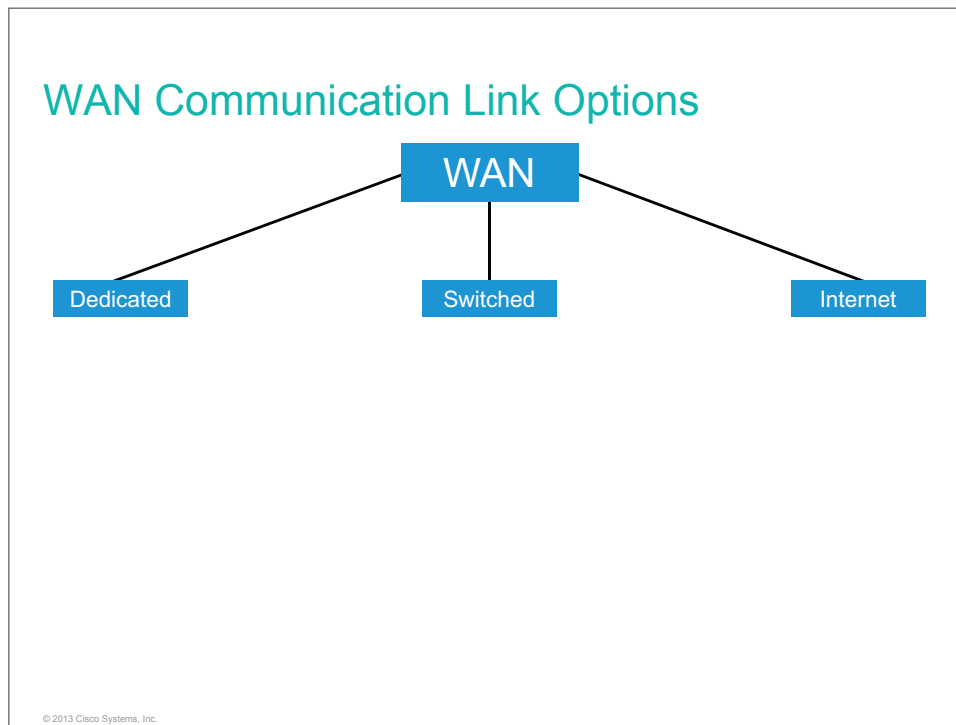


Routers have both LAN and WAN interfaces. While a router is used to segment LANs, it is also used as the WAN access connection device. The functions and role of a router in accessing the WAN can be best understood by looking at the types of connections that are available on the router. There are three basic types: LAN interfaces, WAN interfaces, and management ports. LAN interfaces allow the router to connect to the LAN media through Ethernet or some other LAN technology.

WAN connections are made through a WAN interface on a router to a service provider to a distant site or to the Internet. These may be serial connections or any number of other WAN interfaces. With some types of WAN interfaces, an external device such as a DSU, CSU, or modem (such as an analog modem, cable modem, or DSL modem) is required to connect the router to the local POP of the service provider. The physical demarcation point is the place where the responsibility for the connection changes from the user to the service provider. It is very important because, when problems arise, both sides of the link need to know which side the problem resides on.

WAN Communication Link Options

This topic presents various WAN communication link options.



Options for implementing WAN solutions differ in technology, speed, and cost. WAN connections can be carried over a private infrastructure or over a public infrastructure, such as the Internet.

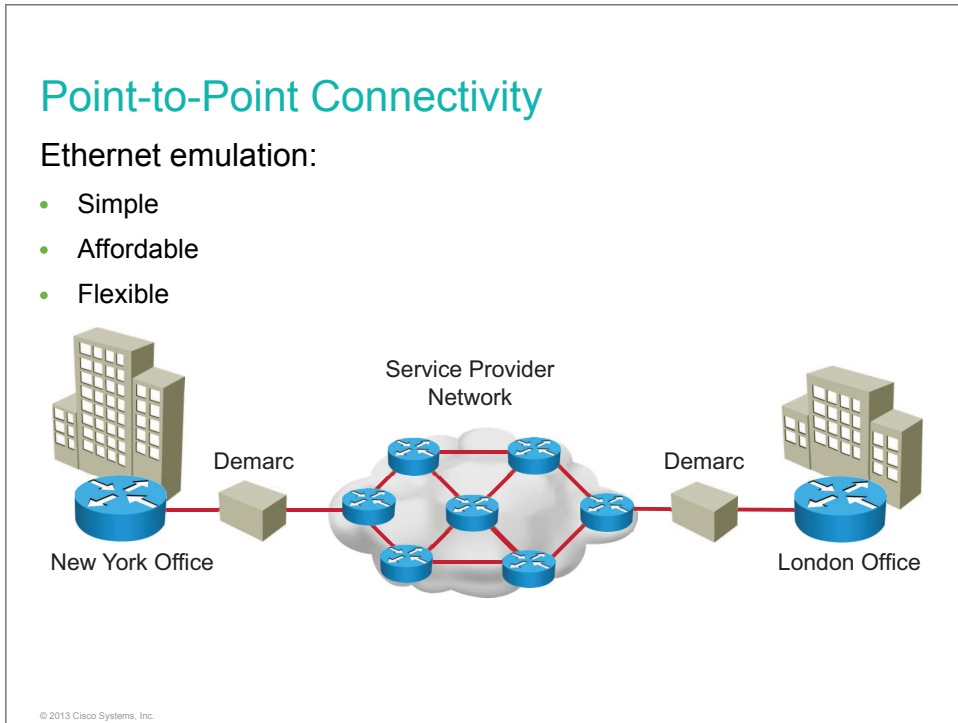
Private connections include dedicated and switched communication link options.

- **Dedicated communication links:** When permanent, dedicated connections are required, point-to-point lines are used with various capacities that are limited only by underlying physical capabilities and the willingness of users to pay for these dedicated lines. A point-to-point link provides an established WAN communications path from the customer premises through the provider network to a remote destination. Point-to-point lines are usually leased from a carrier and are also called *leased lines*.
- **Switched communication links:** Many WAN users do not make efficient use of the fixed bandwidth that is available with dedicated communication links because the data flow fluctuates. Service providers have data networks that are available to more appropriately service these users. In packet-switched networks, the data is transmitted in labeled cells, frames, or packets over a common infrastructure, which is utilized by several customers at once. Different technologies can be used to ensure privacy and isolation of different customers and to provide desired bandwidth requirements and SLAs.

Public connections use the global Internet infrastructure. Until recently, the Internet was not a viable networking option for many businesses because of the significant security risks and lack of adequate performance guarantees in an end-to-end Internet connection. With the development of VPN technology, however, the Internet is now an inexpensive and secure option for connecting to teleworkers and remote offices when performance guarantees are not critical. Internet WAN connection links are through broadband services such as DSL, cable modem, and broadband wireless, and they are combined with VPN technology to provide privacy across the Internet. Broadband connection options are typically used to connect telecommuting employees to a corporate site over the Internet.

Point-to-Point Connectivity

A point-to-point communication link provides a single, established WAN communication path from the customer premises through a service provider infrastructure to a remote network. Different technologies can be used to provide point-to-point connectivity. This topic introduces the concept of point-to-point links based on Ethernet emulation, which is commonly offered by service providers.



When permanent connections are required, a point-to-point link is used to provide an established WAN communication path from the customer premises through the provider network to a remote destination. A point-to-point link can connect two geographically distant sites, such as a corporate office in New York and a regional office in London. Point-to-point links are usually leased from a service provider.

Service providers can use different technologies to provide point-to-point connectivity. In recent years, different solutions that are based on Ethernet emulation became popular.

The advantages of Ethernet emulation services include the following:


- **Simplicity:** Although different technologies are used in service provider networks, customers always obtain an Ethernet link that is simply plugged into their equipment. Which technology is used beyond the demarcation point is transparent for end customers.
- **Cost:** Ethernet ports on customer equipment are the cheapest connectivity option compared to other solutions such as optical or serial interfaces.
- **Flexibility:** Service providers are able to offer different link capabilities depending on the technology that is used. Different bandwidth arrangements, bandwidth guarantees, and SLAs can be offered to define the appropriate service that fits customer needs.

Configuring a Point-to-Point Link

This topic shows how to configure a point-to-point link.

Configuring a Point-to-Point Link

Configuring the Branch router with an IP address and interface description



```
Branch (config)# interface GigabitEthernet0/1
Branch (config-if)# ip address 192.168.1.1 255.255.255.252
Branch (config-if)# description WAN Link to HQ
Branch (config-if)# no shutdown
```

- Use ping to verify end-to-end connectivity

© 2013 Cisco Systems, Inc.

The figure displays configuration commands that are needed on the Branch router in an example topology to establish connectivity over the WAN with Ethernet emulation.

Command and Variable	Description
interface <i>interface</i>	Enters interface configuration mode
ip address <i>ip_address</i> <i>subnet_mask</i>	Sets an IP address and subnet mask on the interface
[no] shutdown	Disables or enables the interface
description	Sets the description on the interface

To perform verification, you can use the **show interfaces** command. Because the local interface is connected to service provider equipment, the status of the interface and line protocol does not always reflect the status of the WAN connection. You can use ping to verify end-to-end connectivity over the WAN link.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- A WAN allows the transmission of data across broad geographic distances.
- A WAN is a collection of LANs, and routers play a central role in transmitting data through WANs.
- There are three WAN communication link options: dedicated communication links, switched communication links, and public connections.
- A common type of WAN connectivity is the point-to-point connection that emulates Ethernet.
- Configuring an interface for emulated Ethernet WAN connectivity consists of setting the IP address and enabling the interface.

© 2013 Cisco Systems, Inc.

Introducing Dynamic Routing Protocols

Routing is the process of determining where to send data packets that are destined for addresses outside the local network. Routers gather and maintain routing information to enable the transmission and receipt of these data packets. Routing information takes the form of entries in a routing table, with one entry for each identified route. The router can use a routing protocol to create and maintain the routing table dynamically so that network changes can be accommodated whenever they occur.

To effectively manage an IP network, you must understand the operation of dynamic routing protocols and the effect that they have on an IP network. This lesson discusses the need for routing protocols and describes the differences between interior and exterior routing protocols and also between link-state and distance vector routing protocols. The operation of link-state protocols is explained.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the purpose of dynamic routing protocols
- Compare interior and exterior routing protocols
- Compare link-state and distance vector routing protocols
- Describe the operation and characteristics of link-state routing protocols

Purpose of Dynamic Routing Protocols

This topic describes the purpose of dynamic routing protocols.

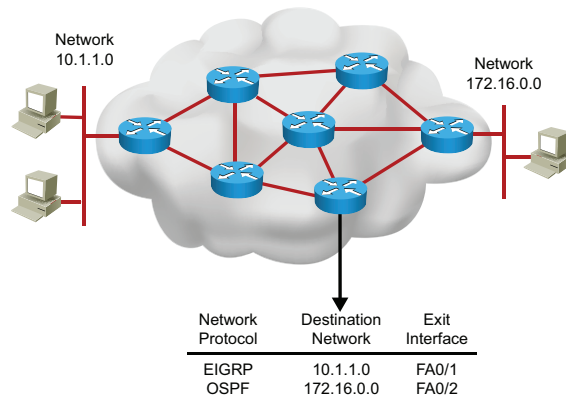
Purpose of Dynamic Routing Protocols

Dynamic routing protocol characteristics follow:

- Routing protocols are sets of processes, algorithms, and messages that are used to exchange routing information.
- After directly connected routes have been installed, a router populates its routing table with the best paths to remote destinations, as chosen by the routing protocol.
- After the path is determined, a router can route to the learned networks.

© 2013 Cisco Systems, Inc.

Purpose of Dynamic Routing Protocols (Cont.)



© 2013 Cisco Systems, Inc.

Dynamic routing relies on a routing protocol to disseminate knowledge. A routing protocol defines the rules that a router uses when it communicates with neighboring routers to determine paths to remote networks and maintain those networks in the routing tables.

A routing protocol facilitates the exchange of routing information between networks, allowing routers to build routing tables dynamically. As routers become aware of changes to the networks for which they act as the gateway or of changes to links between routers, this information is passed to other routers. When a router receives information about new or changed routes, it updates its own routing table and, in turn, passes the information to other routers. In this way, all routers have accurate routing tables that are updated dynamically and can learn about routes to remote networks that are many hops away.

Routing protocols describe this information:

- How updates are conveyed
- What knowledge is conveyed
- When to convey the knowledge
- How to locate recipients of the updates

Purpose of Dynamic Routing Protocols (Cont.)

Dynamic routing protocols do as follows:

- Discover remote networks
- Maintain up-to-date routing information
- Choose the best path to destination networks
- Find a new best path if the current path is no longer available

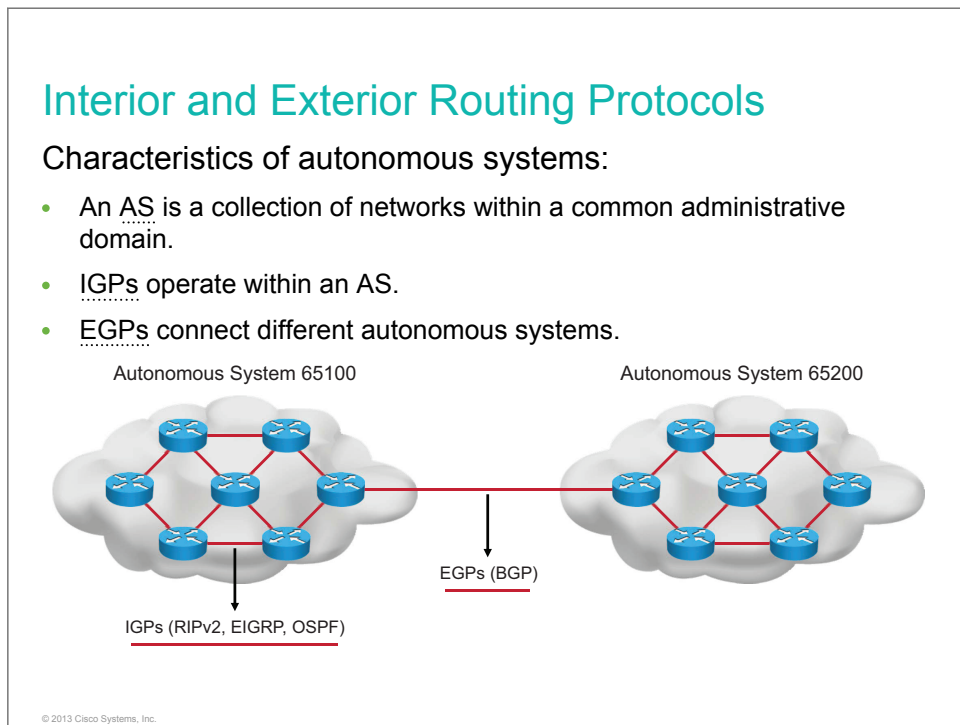
© 2013 Cisco Systems, Inc.

The purpose of a routing protocol includes the following:

- **Discovering remote networks:** There is no need to manually define the available destination (routes). The routing protocol discovers remote networks and updates the internal routing table of the router.
- **Maintaining up-to-date routing information:** The routing table contains entries about remote networks. When changes occur in the network, routing tables are automatically updated.
- **Choosing the best path to destination networks:** Routing protocols discover remote networks. More paths to the destinations are possible, and the best paths enter the routing table.
- **Finding a new best path if the current path is no longer available:** The routing table is constantly updated, and new paths may also be added. When the current best path is not available or better paths are found, the routing protocol selects a new best path.

Interior and Exterior Routing Protocols

This topic compares interior and exterior routing protocols.



IGPs are used for routing within a routing domain. Those networks are under the control of a single organization. An AS commonly comprises many individual networks belonging to companies, schools, and other institutions.

An IGP is used to route within the AS and also within the individual networks themselves. For example, the Corporation for Education Network Initiatives in California operates an AS that includes California schools, colleges, and universities. The corporation uses an IGP to route within its AS to interconnect all of these institutions. Each educational institution also uses an IGP of its own choosing to route within its own individual network. The IGP that is used by each entity provides the best-path determination within its own routing domains, just as the IGP that is used by the corporation provides the best-path routes within the AS itself.

IGPs for IP include RIP, EIGRP, OSPF, and others. Some IGPs may be adequate in large corporate networks but are not designed to handle tens of thousands or hundreds of thousands of routes, such as the many thousands of routes that are present on the Internet.

EGPs, however, are designed for use between Autonomous systems that are under the control of different administrations. BGP is an example of an EGP and is the routing protocol that is used in the Internet. BGP is a path vector protocol that can use many different attributes to measure routes. BGP is typically used between ISPs and sometimes between a company and an ISP.

Distance Vector and Link-State Routing Protocols

This topic compares link-state and distance vector routing protocols.

Distance Vector and Link-State Routing Protocols

The types of dynamic routing protocols follow:

- **Distance vector:** RIP
- **Advanced distance vector:** EIGRP
- **Link-state:** OSPF and IS-IS

© 2013 Cisco Systems, Inc.

Within an AS, most IGP routing can be classified as conforming to one of these algorithms:

- **Distance vector:** The distance vector routing approach determines the direction (vector) and distance (a metric, such as hop count in the case of RIP) to any link in the internetwork. Pure distance vector protocols periodically send complete routing tables to all connected neighbors. This mode of operation is key in defining what a distance vector routing protocol is. In large networks, these routing updates can become enormous, causing significant traffic on the links. The only information that a router knows about a remote network is the distance or metric to reach this network and which path or interface to use to get there. Different distance vector routing protocols may use different kinds of metrics. Distance vector routing protocols do not have an actual map of the network topology. For a router, the view of the network is based on the information that is provided by its neighbors.
- **Advanced distance vector:** The advanced distance vector approach combines aspects of the link-state and distance vector algorithms. EIGRP is a Cisco proprietary routing protocol that combines the advantages of link-state and distance vector routing protocols. EIGRP may act like a link-state routing protocol because it uses a Hello protocol to discover neighbors and form neighbor relationships and because only partial updates are sent when a change occurs. However, EIGRP is still based on the key distance vector routing protocol principle that information about the rest of the network is learned from directly connected neighbors.

- **Link-state:** The link-state approach, which uses the SPF algorithm, creates an abstraction of the exact topology of the entire internetwork, or at least of the partition in which the router is situated. A link-state router uses the link-state information to create a topology map and to select the best path to all destination networks in the topology. All link-state routers use an identical "map" of the network and calculate the shortest paths to reach the destination networks in relation to where they are on this map. Unlike their distance vector counterparts, complete routing tables are *not* exchanged periodically. Instead, event-based, "triggered" updates containing only specific link-state information are sent. Periodic keepalives that are small and efficient, in the form of hello messages, are exchanged between directly connected neighbors to establish and maintain reachability to this neighbor.

Do Not Duplicate.
Post beta, not for release.

Understanding Link-State Routing Protocols

This topic describes the operation and characteristics of link-state routing protocols and of OSPF in particular.

Understanding Link-State Routing Protocols

Characteristics of link-state routing protocols follow:

- A complete view of the network topology is created.
- Updates are sent when there is a link change.
- They are associated with SPF calculations.
- They use the link-state information to do as follows:
 - Create a topology map.
 - Select the best path to all destination networks in the topology.

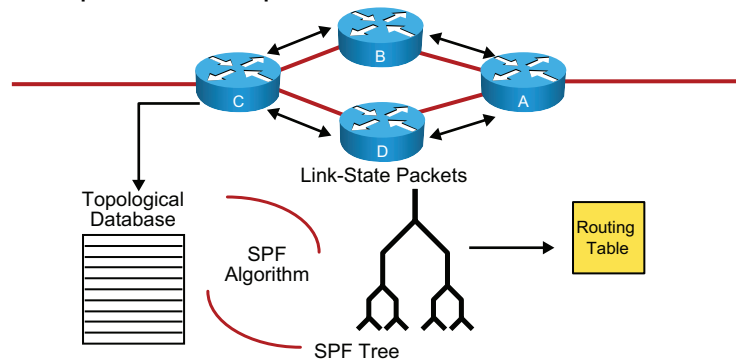
© 2013 Cisco Systems, Inc.

Link-state routing protocols collect routing information from all other routers in the network or within a defined area of the network. After all of the information is collected, each router, independent of the other routers, calculates the best paths to all destinations in the network. Because each router maintains its own view of the network, the router is less likely to propagate incorrect information that is provided by a router.

A link is like an interface on a router. The state of the link is a description of this interface and of its relationship to its neighboring routers. An example description of the interface would include the IP address of the interface, the mask, the type of network to which it is connected, the routers that are connected to this network, and so on. The collection of link states forms a link-state (or topological) database. The link-state database is used to calculate the best paths through the network. Link-state routers find the best paths to destinations by applying Dijkstra's algorithm against the link-state database to build the SPF tree. The best paths are then selected from the SPF tree and placed in the routing table.

Understanding Link-State Routing Protocols (Cont.)

Link-state protocol components:



© 2013 Cisco Systems, Inc.

Link-state routing protocols are much more complex than their distance vector counterparts. However, the basic functionality and configuration of link-state routing protocols are not complex at all.

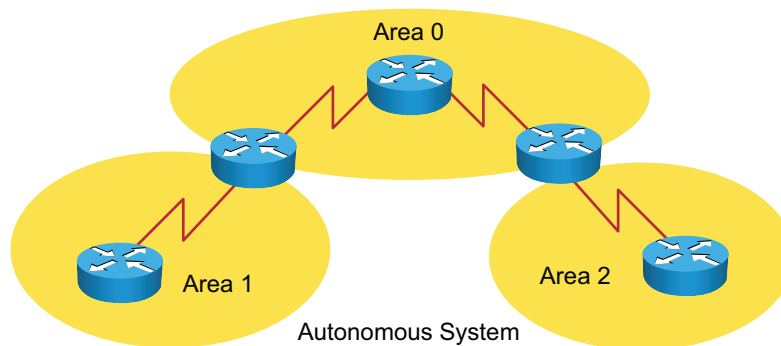
To maintain routing information, link-state routing uses LSAs, a topological database, the SPF algorithm, the resulting SPF tree, and a routing table of paths and ports to each network.

LSAs are used in OSPF for the routers to exchange knowledge about the network topology. The topological, or link-state, database holds all of the information about the topology of the network. This database is used by the SPF algorithm, which builds the SPF tree. The best paths are then inserted into the routing table, and routing decisions are made based on the entries in the routing table.

Understanding Link-State Routing Protocols (Cont.)

Hierarchical routing:

- Consists of areas and autonomous systems



© 2013 Cisco Systems, Inc.

The ability of link-state routing protocols, such as OSPF, to divide one large AS into smaller groupings of routers (called *areas*) is referred to as *hierarchical routing*. Link-state routing protocols use the concept of areas for scalability. Topological databases contain information about every router and the associated interfaces, which in large networks can use resources intensively. Arranging routers into areas effectively partitions this potentially large database into smaller and more manageable databases.

With hierarchical routing, routing still occurs between the areas (interarea routing). At the same time, many of the minute internal routing operations, such as recalculating the database, are kept within an area.

When a failure occurs in the network, such as a neighbor becoming unreachable, link-state protocols flood LSAs using a special multicast address throughout an area. Each link-state router takes a copy of the LSA, updates its link-state (topological) database, and forwards the LSA to all neighboring devices. LSAs cause every router within the area to recalculate routes. Because LSAs must be flooded throughout an area and all routers within this area must recalculate their routing tables, the number of link-state routers that can be in an area should be limited.

The figure shows three areas. If Area 1 is having problems with an intermittent link, routers in the other areas do not need to continually run their SPF calculation because they are isolated from the Area 1 problem.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Routing protocols are a set of processes, algorithms, and messages that are used to exchange routing information.
- IGPs operate within an AS, while EGPs connect different autonomous systems.
- The distance vector routing approach determines the direction (vector) and distance to any link in the internetwork.
- Routers running link-state routing protocols maintain their own view of the network, so the router is less likely to propagate incorrect information that is provided by another router.

© 2013 Cisco Systems, Inc.

Implementing OSPF

OSPF is an IGP that was designed by the IETF. Because OSPF is a widely deployed standard protocol, knowledge of its configuration and maintenance is essential. This lesson describes the function of OSPF and explains how to configure a single-area OSPF network on a Cisco router.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the features of OSPF
- Explain how OSPF routers become neighbors
- Explain how OSPF decides what is the best path through the network
- Explain the OSPF router ID
- Configure a single-area OSPF network
- Verify a single-area OSPF configuration

Introducing OSPF

This topic describes the features of OSPF.

Introducing OSPF

- Developed by the IETF
- Creates a neighbor relationship by exchanging hello packets
- Propagates LSAs rather than routing table updates:
 - Link: Router interface
 - State: Description of an interface and its relationship to neighboring routers
- Floods LSAs to all OSPF routers in the area, not just directly connected routers
- Pieces together all of the LSAs that are generated by the OSPF routers to create the OSPF link-state database
- Uses the SPF algorithm to calculate the shortest path to each destination and places it in the routing table

© 2013 Cisco Systems, Inc.

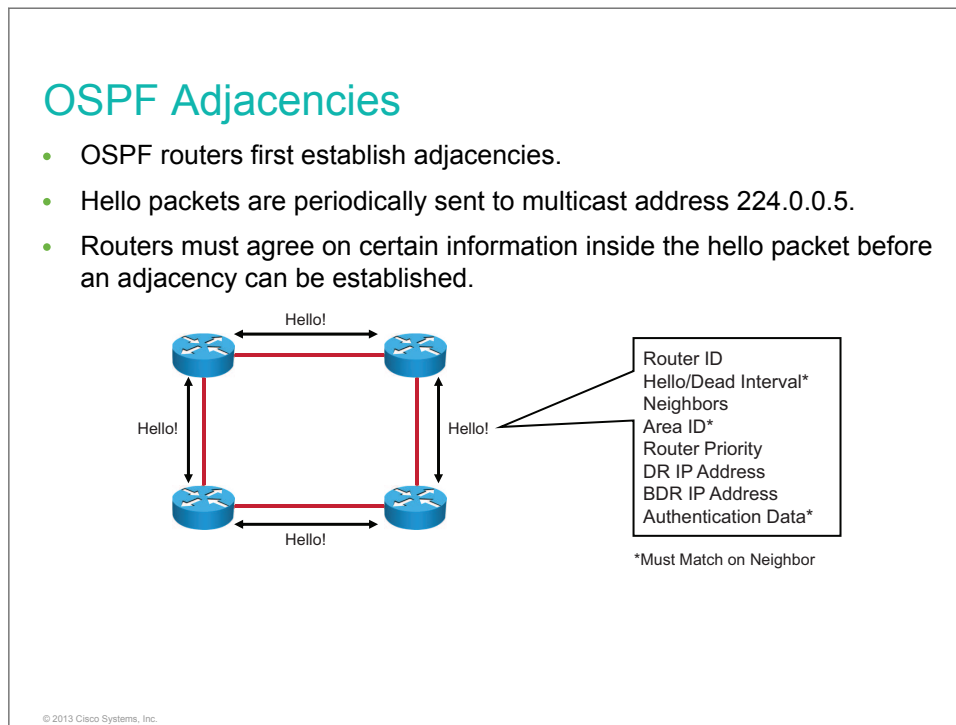
OSPF was developed as a replacement for the distance vector routing protocol RIP. The major advantages of OSPF over RIP are its fast convergence and its ability to scale to much larger networks.

A router sends LSA packets immediately to advertise its state when there are state changes and sends them periodically as well (every 30 minutes by default). Information about attached interfaces, metrics that are used, and other variables are included in OSPF LSAs. As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node.

A topological (link-state) database is, essentially, an overall picture of networks in relation to routers. The topological database contains the collection of LSAs that were received from all routers in the same area. Because routers within the same area share the same information, they have identical topological databases.

OSPF Adjacencies

This topic describes how OSPF adjacencies are built.



Neighbor OSPF routers must recognize each other on the network before they can share information because OSPF routing depends on the status of the link between two routers. The routers recognize each other by using the Hello protocol. OSPF routers send hello packets on all OSPF-enabled interfaces to determine if there are any neighbors on those links.

Receiving OSPF hello packets on an interface confirms to the OSPF router the presence of another OSPF router on a link. The hello packet contains information that allows the OSPF routers to establish and maintain neighbor relationships by ensuring bidirectional (two-way) communication between neighbors.

An OSPF neighbor relationship, or adjacency, is formed between two routers if they both agree on the area ID, hello and dead intervals, and authentication. Of course, the routers must be on the same IP subnet. Bidirectional communication occurs when a router recognizes itself in the neighbors list that is contained in the hello packet that it receives from a neighbor.

Each interface that is participating in OSPF uses IP multicast address 224.0.0.5 to periodically send hello packets. A hello packet contains this information:

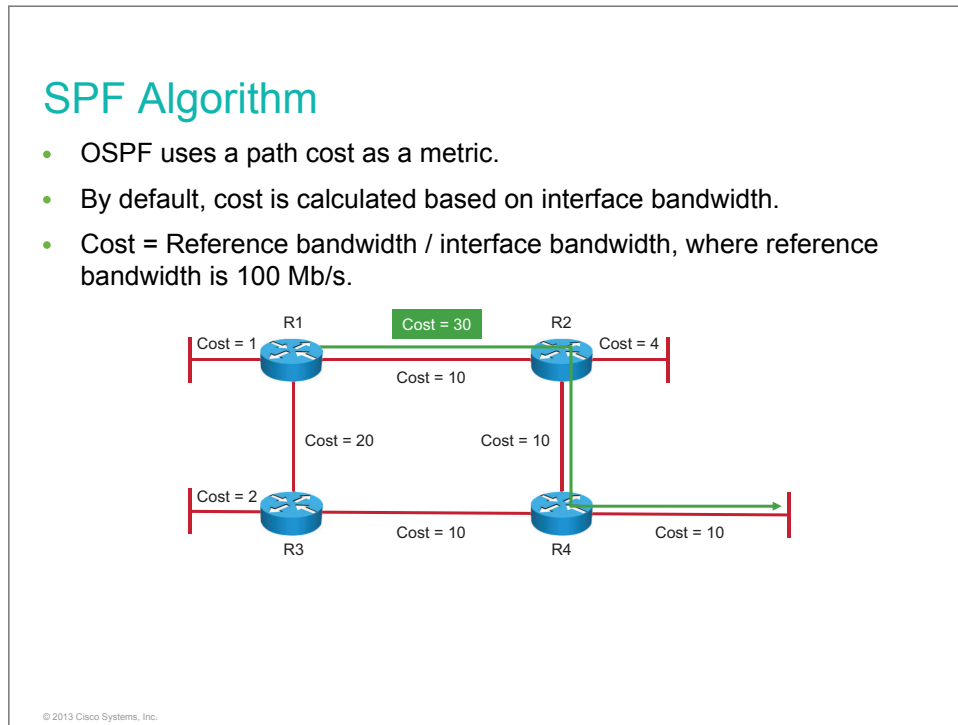
- **Router ID:** The router ID is a 32-bit number that uniquely identifies the router.
- **Hello and dead intervals:** The hello interval specifies the frequency in seconds at which a router sends hello packets. The dead interval is the time in seconds that a router waits to hear from a neighbor before declaring the neighboring router out of service.
- **Neighbors:** The Neighbors field lists the adjacent routers with established bidirectional communication.
- **Area ID:** To communicate, two routers must share a common segment, and their interfaces must belong to the same OSPF area on this segment.
- **Router priority:** The router priority is an 8-bit number that indicates the priority of a router.

- **DR and BDR IP addresses:** These addresses are the IP addresses of the DR and BDR for the specific network, if they are known.
- **Authentication password:** If router authentication is enabled, two routers must exchange the same password.

Do Not Duplicate.
Post beta, not for release.

SPF Algorithm

This topic describes how OSPF builds the routing table and what it bases routing decisions on.



The SPF algorithm places each router at the root of a tree and calculates the shortest path to each node, using Dijkstra's algorithm. Dijkstra's algorithm is based on the cumulative cost to reach this destination.

A metric is an indication of the overhead that is required to send packets across a certain interface. OSPF uses cost as a metric. A lower cost indicates a better path than a higher cost. The cost of an interface is inversely proportional to the bandwidth of the interface, so a higher bandwidth indicates a lower cost. More overhead, higher cost, and more time delays are involved in crossing a 10-Mb/s Ethernet line than in crossing a 100-Mb/s Ethernet line.

The formula that is used to calculate OSPF cost follows:

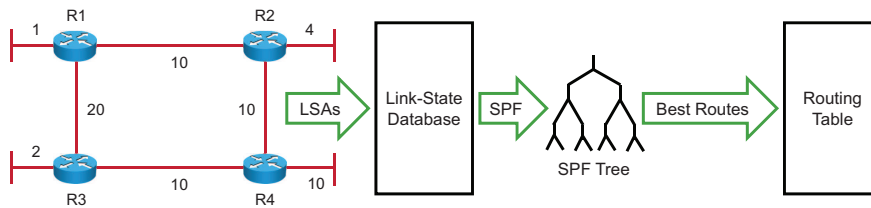
Cost = reference bandwidth / interface bandwidth (in bits per second)

The default reference bandwidth is 10^8 , which is 100,000,000, or the equivalent of the bandwidth of Fast Ethernet. Therefore, the default cost of a 10-Mb/s Ethernet link is $10^8 / 10^7 = 10$, and the cost of a 100-Mb/s link is $10^8 / 10^8 = 1$. A problem arises with links that are faster than 100 Mb/s. Because OSPF cost has to be an integer, all links that are faster than Fast Ethernet have an OSPF cost of 1. In this case, you must change the OSPF cost on an interface manually or adjust the reference bandwidth to a higher value.

To adjust the reference bandwidth for links with bandwidths greater than Fast Ethernet, use the **auto-cost reference-bandwidth** command in router configuration mode.

The cost to reach a distant network from a router is the cumulative cost of all links on the path from the router to the network. In the example, the cost from router R1 to the destination network via R3 is 40 (20 + 10 + 10), and the cost via router R2 is 30 (10 + 10 + 10). The path via R2 is better because it has a lower cost.

SPF Algorithm (Cont.)



R1 SPF Tree

Destination	Shortest Path	Cost
R2 LAN	R1 to R2	14
R3 LAN	R1 to R3	22
R4 LAN	R1 to R4	30

© 2013 Cisco Systems, Inc.

LSAs are flooded throughout the area using a reliable algorithm, which ensures that all routers in an area have the same topological database. As a result of the flooding process, router R1 in the example has learned the link-state information for each router in its routing area. Each router uses the information in its topological database to calculate a shortest-path tree, with itself as the root. The SPF tree is then used to populate the IP routing table with the best paths to each network.

For R1, the shortest path to each LAN and the cost are shown in the table. The shortest path is not necessarily the path. Each router has its own view of the topology, although all of the routers build a shortest-path tree using the same link-state database.

Router ID

This topic explains the router ID.

Router ID

- The number by which the router is known to OSPF can be set manually using the **router-id** command.
- If **router-id** is not configured, the highest IP address on the active loopback interface at the moment of OSPF process startup is selected as the router ID.
- If there is no active loopback interface, then the router selects the highest IP address on the active interface at the moment of OSPF process startup.

© 2013 Cisco Systems, Inc.

The OSPF router ID is used to uniquely identify each router in the OSPF routing domain. A router ID is simply a label and is expressed as an IP address. Cisco routers derive the router ID based on three criteria and with this precedence:

1. The router uses the IP address (or dotted decimal number) that is configured with the OSPF **router-id** command.
2. If the router ID is not configured, the router chooses the highest IP address of its loopback interfaces.
3. If no loopback interfaces are configured, the router chooses the highest active IP address of its physical interfaces.

Note The router ID looks like an IP address, but it is not routable and therefore is not included in the routing table, unless the OSPF routing process chooses an interface (physical or loopback) that is appropriately defined by a **network** command.

Router ID (Cont.)

```
RouterX# show ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
<output omitted>
```

- Verifies the device OSPF router ID

If an OSPF router is not configured with an OSPF **router-id** command and no loopback interfaces are configured, the OSPF router ID will be the highest active IP address on any of its interfaces. The interface does not need to be enabled for OSPF, meaning that it does not need to be included in one of the OSPF **network** commands. However, the interface must be active—it must be in the up state. The example shows the router ID of RouterX with no OSPF **router-id** command and no loopback interfaces that are configured.

For more details about the **show ip protocols** command, check the Cisco IOS IP Routing: Protocol-Independent Command Reference at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_13.html.

Configuring Single-Area OSPF

This topic describes how to configure single-area OSPF.

Configuring Single-Area OSPF

```
Branch (config)# router ospf 1
Branch (config-router)# network 10.0.0.0 0.255.255.255 area 0
```

```
Branch (config)# interface GigabitEthernet 0/1
Branch (config-if)# ip ospf 1 area 0
```

- Configures OSPF on the Branch router

© 2013 Cisco Systems, Inc.

Basic OSPF is configured in two steps:

1. Enable the OSPF routing process.
2. Identify the networks that you want to advertise.

Command and Variable	Description
router ospf <i>process_id</i>	Enters into OSPF routing configuration mode. The process ID is a number between 1 and 65,535 and is chosen by the network administrator. The process ID is locally significant, which means that it does not have to match other OSPF routers to establish adjacencies with those neighbors.
network <i>ip-address wildcard_mask area area_id</i>	The network command uses a combination of network address and wildcard mask and serves as a criteria match to identify the interfaces that are enabled to send and receive OSPF packets. The network address, along with the wildcard mask, identifies which IP networks are part of the OSPF network and are included in OSPF routing updates. The area ID identifies the OSPF area to which the network belongs. When all of the routers are within the same OSPF area, the network commands must be configured with the same area ID on all routers. Even if no areas are specified, there must be an Area 0. In a single-area OSPF environment, the area is always 0.
ip ospf <i>process_id area area_id</i>	Alternatively to a network command, you can use this interface configuration mode command that enables OSPF explicitly on the selected interface.

The network that is identified in the **network** command does not tell the router which network to advertise; rather, it indicates interfaces on which OSPF will be enabled. The subnet on this interface is what will be advertised. For example, entering **network 10.1.1.1 0.0.0.0 area 0** on the Branch router tells the router to enable interface GigabitEthernet 0/0.1 for the routing process. The OSPF process advertises the network that is on this interface (10.1.1.0/24).

For more details on the **router ospf** command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_11.html.

For more details on the **network** command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_10.html.

Configuring Single-Area OSPF (Cont.)

```
Branch(config)# router ospf 1
Branch(config-router)# passive-interface GigabitEthernet 0/0.1
```

- Configures the passive interface on GigabitEthernet 0/0.1 on the Branch router.

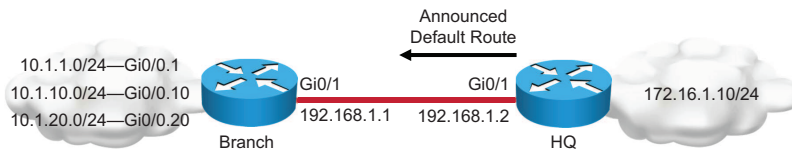
© 2013 Cisco Systems, Inc.

The router automatically sends OSPF hello packets out of every interface that is included into the OSPF process. To limit the amount of unnecessary traffic in the LAN or to prevent other routers on a local network to learn about routes dynamically, you can stop sending routing updates out of a specific interface. This is achieved by configuring a passive interface option for a selected interface on which OSPF adjacency is not desired.

In the figure, interface GigabitEthernet 0/0.1 on router Branch is configured as passive in OSPF configuration mode with the **passive-interface** *GigabitEthernet 0/0.1* configuration command.

For more details about the **passive-interface** command, go to [Cisco IOS IP Routing: Protocol-Independent Command Reference](#).

Configuring Single-Area OSPF (Cont.)



- The HQ router announces the default route through OSPF.

© 2013 Cisco Systems, Inc.

To be able to perform routing toward external networks or toward the Internet, a router must either know all of the destination networks or have a default route. You can statically configure the default route, but it can also be learned dynamically via the OSPF routing protocol. The router that announces the default route needs to be configured with the **default-information originate** command in the routing protocols configuration mode.

For more details about the **default-information originate** command, go to [Cisco IOS IP Routing: OSPF Command Reference](#).

Verifying OSPF Configuration

This topic describes how to verify the configuration of single-area OSPF.

Verifying OSPF Configuration

```
Branch# show ip protocols
Routing Protocol is "ospf"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.255.255.255 area 0
  Routing on Interfaces Configured Explicitly (Area 0):
    GigabitEthernet0/1
  Passive Interface(s):
    GigabitEthernet0/0.1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:50:43
  Distance: (default is 110)
```

- Verifies that OSPF on the Branch router is routing for all networks that it needs to

The **show ip protocols** command shows a summary of configured routing protocol information. It can be very useful for a quick verification of how routing protocols are configured. You can see which protocols are enabled and which networks these protocols are routing for. You can also see on which interfaces the routing protocols were enabled explicitly. If passive interfaces are configured, they will be seen in the output as well.

For more information about the **show ip protocols** command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_13.html.

Verifying OSPF Configuration (Cont.)

```
Branch# show ip ospf interface brief
Interface  PID  Area      IP Address/Mask  Cost  State Nbrs F/C
Gi0/0.1    1    0         10.1.1.1/24     1     DR   0/0
Gi0/1      1    0         192.168.1.1/24  1     BDR  1/1
Gi0/0.20   1    0         10.1.20.1/24    1     DR   0/0
Gi0/0.10   1    0         10.1.10.1/24    1     DR   0/0
```

- Shows which interfaces are enabled for the OSPF routing process

© 2013 Cisco Systems, Inc.

The **show ip ospf interface** command shows you which interfaces are enabled for OSPF. It is useful to determine if your network statements were correctly composed.

For more information about the **show ip ospf interface** command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_13.html.

Verifying OSPF Configuration (Cont.)

```
Branch# show ip ospf neighbor
Neighbor ID  Pri  State      Dead Time  Address      Interface
1.1.1.1     1    FULL/DR    00:00:36  192.168.1.2  GigabitEthernet0/1
```

- Shows OSPF neighbors

© 2013 Cisco Systems, Inc.

The **show ip ospf neighbor** command displays OSPF neighbor information on a per-interface basis.

The example shows output from the **show ip ospf neighbor** command, with a single line of summary information for each neighbor. The Branch router formed a full adjacency (as shown under State) with its neighbor (Neighbor ID). The full state means that the router and its neighbor have identical OSPF link-state databases.

The figure also shows the expected time before Cisco IOS Software will declare the neighbor of the router dead (Dead Time), the neighbor IP addresses (Address), and the interfaces that the neighbors are connected to (Interface).

For more information about the **show ip ospf neighbor** command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_13.html.

Verifying OSPF Configuration (Cont.)

```
Branch# show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

- The routing table displays OSPF routes.

© 2013 Cisco Systems, Inc.

Verifying OSPF Configuration (Cont.)

```
O*E2 0.0.0.0/0 [110/1] via 192.168.1.2, 00:02:45, GigabitEthernet0/1
  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C    10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
L    10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
C    10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L    10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C    10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
L    10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
L    172.16.0.0/32 is subnetted, 1 subnets
O    172.16.1.100 [110/2] via 192.168.1.2, 00:56:58, GigabitEthernet0/1
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

- The routing table displays OSPF routes.

© 2013 Cisco Systems, Inc.

The **show ip route** command displays the routes that are known to the router and how they were learned. This command is one of the best ways to determine connectivity between the local router and the rest of the internetwork. In the figure, two routes from OSPF are in the routing table. One describes the 172.16.1.100 network, while the second one represents the default route that was learned dynamically over OSPF.

For more information about the **show ip route** command, go to http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_13.html.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- OSPF is a link-state routing protocol that uses an area hierarchy.
- OSPF exchanges hello packets to establish neighbor adjacencies between routers.
- The SPF algorithm uses a cost metric to determine the best path. Lower cost indicates a better path.
- Configuration of basic OSPF requires two steps:
 - Enable the OSPF routing process.
 - Identify the networks to advertise.
- The **show ip ospf neighbor** command displays OSPF neighbor information on a per-interface basis.

© 2013 Cisco Systems, Inc.

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- VLANs are independent LAN networks that address segmentation, security, and organizational flexibility.
- Inter-VLAN communication cannot occur without a Layer 3 device (a Layer 3 switch or router).
- The DHCP server provides dynamic IP address assignments to end hosts, reducing errors and the time that is needed to administer address assignment.
- A WAN is a collection of LANs, and routers play a central role in transmitting data through these networks.
- Routing protocols are a set of processes, algorithms, and messages that are used to exchange routing information.
- Configuration of basic OSPF requires two steps:
 - Enable the OSPF routing process.
 - Identify the networks to advertise.

Do Not Duplicate.
Post beta, not for release.

Module Self-Check

Questions

Use the questions here to review what you learned. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Which feature is required for multiple VLANs to span multiple switches? (Source: Implementing VLANs and Trunks)
 - multilayer switch
 - router
 - bridge
 - trunk
- Which information does the **show vlan** command display? (Source: Implementing VLANs and Trunks)
 - redundancy information
 - which ports are trunks
 - names of the VLANs and ports that are assigned to the VLANs
 - STP information
- Match the terms and statements. (Source: Implementing VLANs and Trunks)

A. native VLAN	<input type="checkbox"/>	sends frames untagged
B. STP	<input type="checkbox"/>	ensures a loop-free topology
C. VLAN 1	<input type="checkbox"/>	factory default Ethernet VLAN

4. Which command correctly assigns a subinterface to VLAN 50 using 802.1Q trunking? (Source: Routing Between VLANs)
- A. Router(config)# **encapsulation 50 dot1Q**
 - B. Router(config)# **encapsulation trunk dot1Q 50**
 - C. Router(config-if)# **encapsulation dot1Q 50**
 - D. Router(config-if)# **encapsulation 802.1Q vlan 50**
5. Arrange the steps of DHCP operation in the correct order. (Source: Using a Cisco Network Device as a DHCP Server)
- | | | |
|------------|--------------------------|---------------------|
| A. phase 1 | <input type="checkbox"/> | DHCP acknowledgment |
| B. phase 4 | <input type="checkbox"/> | DHCP offer |
| C. phase 3 | <input type="checkbox"/> | DHCP discover |
| D. phase 2 | <input type="checkbox"/> | DHCP request |
6. Which command would you use to verify the number of available addresses in a DHCP pool? (Source: Using a Cisco Network Device as a DHCP Server)
- A. **show ip dhcp available addresses**
 - B. **show ip dhcp conflict**
 - C. **show ip dhcp binding**
 - D. **show ip dhcp pool**
7. Which two protocols are link-state routing protocols? (Choose two.) (Source: Introducing Dynamic Routing Protocols)
- A. OSPF
 - B. EIGRP
 - C. BGP
 - D. IS-IS
 - E. RIP
8. Which two statements correctly describe link-state routing protocols? (Choose two.) (Source: Introducing Dynamic Routing Protocols)
- A. They send complete routing tables to all connected neighbors.
 - B. They use the SPF algorithm.
 - C. The only information that a router knows about a remote network is the distance or metric to reach this network.
 - D. They use triggered updates.
 - E. Two examples are OSPF and EIGRP.

9. Which two statements correctly describe OSPF? (Choose two.) (Source: Implementing OSPF)
- A. OSPF is a Cisco proprietary protocol.
 - B. Routers create a neighbor relationship by exchanging hello packets.
 - C. By default, cost is configured by the network administrator.
 - D. The OSPF topological database contains the collection of LSAs that were received from all routers in the same area.
 - E. The OSPF neighbor table contains all of the routers within an OSPF area.
10. Which command would you use to enter the OSPF routing configuration mode? (Source: Implementing OSPF)
- A. Router(config)# **router ospf**
 - B. Router(config)# **router ospf 1**
 - C. Router(config)# **network 10.0.0.0 0.0.0.255 area 0**
 - D. Router(config-router)# **network 10.0.0.0 0.0.0.255 area 0**

Answer Key

1. D
2. C
3. A. VLAN 1
B. native VLAN
C. STP
factory default Ethernet VLAN
sends frames untagged
ensures a loop-free topology
4. C
5. A. phase 1
B. phase 2
C. phase 3
D. phase 4
DHCP discover
DHCP offer
DHCP request
DHCP acknowledgment
6. D
7. A, D
8. B, D
9. B, D
10. B

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate:
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Introducing IPv6

Activity Objective

The growth of the Internet and the adoption of networking over the past 20 years are pushing IPv4 to the limits of its addressing capacity and its ability for continued growth. To sustain the evolution of the Internet, the IETF developed a next-generation protocol, IPv6. This module describes the factors leading toward IPv6 development and compares IPv4 with IPv6.

Objectives

Upon completing this module, you will be able to meet these objectives:

- Describe IPv6 main features, addresses, and basic configuration
- Describe IPv6 operations
- Identify routing protocols for IPv6

Do Not Duplicate.
Post beta, not for release.

Introducing Basic IPv6

Overview

The ability to scale networks for future demands requires a limitless supply of IP addresses and improved mobility. To cope with the depletion of IP addresses, several short-term solutions were developed.

IPv6 satisfies the increasingly complex requirements of hierarchical addressing that IPv4 does not satisfy.

With a 128-bit address length, the IPv6 address space is significantly larger and more diverse, and therefore is more complicated to manage.

This lesson describes IPv6 main features, addresses, and basic configuration.

Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Identify issues in IPv4
- Identify main IPv6 features
- Describe IPv6 addresses and address types
- Describe IPv6 unicast addresses
- Describe manual address assignment, stateless autoconfiguration, and DHCPv6
- Configure and verify basic IPv6 connectivity on Cisco IOS routers

IPv4 Addressing Exhaustion Workarounds

This topic describes the issues in IPv4.

IPv4 Addressing Exhaustion Workarounds

- To extend the lifetime and usefulness of IPv4 and circumvent address shortage, several mechanisms were created:
 - CIDR
 - VLSM
 - NAT
 - DHCP
- Over the years, hardware support has been added to devices to support IPv4 enhancements.

© 2013 Cisco Systems, Inc.

In an effort to allocate IPv4 addresses efficiently, CIDR was developed. CIDR allowed the address space to be divided into smaller blocks.

VLSMs allow more efficient use of IP addresses, specifically on small segments such as point-to-point serial links. VLSM usage was recommended in RFC 1817. CIDR and VLSM support is a prerequisite for ISPs to receive additional allocations.

NAT introduced a model in which a device facing outward to the Internet would have a globally routable IPv4 address, while the internal network would be configured with private addresses. These private addresses could never leave the site, so they could be identical in many different enterprise networks. In this way, even large enterprises with thousands of systems could hide behind a small number of routable public networks.

The DHCP is used by a client to acquire configuration information, such as an IP address, a default route, and DNS setup from a server.

Problems with IPv4 Addressing Workarounds

- NAT breaks the end-to-end model of IP.
- NAT inhibits end-to-end network security.
- Some applications are not NAT friendly.
- The merging of private networks is difficult if overlapping IP address ranges are used.

© 2013 Cisco Systems, Inc.

One of the arguments against deploying IPv6 is that NAT will solve the problems of limited address space in IPv4. The use of NAT merely delays the exhaustion of the IPv4 address space by using global addresses for large internal networks.

There are several negative implications of using NAT, some of which are identified in RFC 2775 and RFC 2993, as follows:

- NAT breaks the end-to-end model of IP. IP was defined so that underlying layers do not process the connection; only the endpoints process the connection.
- NAT inhibits end-to-end network security. To protect the integrity of the IP header by some cryptographic functions, the IP header cannot be changed between the origin of the packet (to protect the integrity of the header) and the final destination (to check the integrity of the received packet). Any translation of parts of a header on the path will break the integrity check.
- When applications are not “NAT-friendly”—which means that, for a specific application, more than just port and address mapping are necessary to forward the packet through the NAT device—NAT has to embed complete knowledge of all the applications to perform correctly. This is especially true for dynamically allocated ports with rendezvous ports, embedded IP addresses in application protocols, security associations, and so on. Therefore, the NAT device needs to be upgraded each time a new non-NAT-friendly application is deployed (for example, peer-to-peer).
- When different networks use the same private address space and they have to merge or connect, there is an address-space collision. Hosts that are different but that have the same address cannot communicate with each other. This problem can be resolved by techniques such as renumbering or Twice NAT. (Twice NAT is the practice of changing both the source and destination address of a packet.) However, these techniques are costly and, later on, increase NAT complications.

IPv6 Features

This topic describes the main features of IPv6.

IPv6 Features

- **Larger address space:** Global reach capability, flexibility, aggregation, multihoming, autoconfiguration, “plug-and-play,” renumbering
- **Simpler header:** Routing code streamlined, simpler processing in hardware
- **Security and mobility:** Built into the standard, not as extensions
- **Transition richness:** Several mechanisms available, including “dual-stacking”

© 2013 Cisco Systems, Inc.

IPv6 includes a number of features that make it attractive for building global-scale, highly effective networks. The larger address space, strict aggregation, and autoconfiguration provide important capabilities.

Streamlined header structures make processing IPv6 packets faster and more efficient for intermediate routers within the network. This is especially true when large numbers of packets are routed in the core of the IPv6 Internet.

Features that were not part of the original IPv4 specification, such as security and mobility, are now built into IPv6.

IPv6 also includes a rich set of transition tools to allow an easy, nondisruptive transition over time to IPv6-dominant networks.

IPv6 Addresses

This topic describes IPv6 addresses and different address types.

IPv6 Addresses

Address representation follows:

- Format is x:x:x:x:x:x:x, where x is a 16-bit hexadecimal field:
 - Example: 2001:0DB8:010F:0001:0000:0000:0000:0ACD
- Leading zeros in a field are optional:
 - Example: 2001:DB8:10F:1:0:0:0:ACD
- Successive fields of 0 are represented as "::" but only once in an address:
 - Example: 2001:DB8:10F:1::ACD

© 2013 Cisco Systems, Inc.

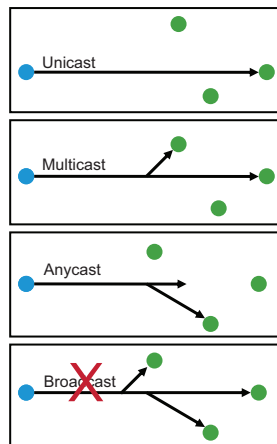
IPv6 addresses are represented as a series of eight 16-bit hexadecimal fields that are separated by colons. The A, B, C, D, E, and F in hexadecimal fields are case-insensitive.

These are some ways to shorten the writing of IPv6 addresses:

- The leading zeros in a field are optional, so 010F can be written as 10F and 0000 can be written as 0.
- Successive fields of zeros can be represented as a double colon (::) but only once in an address. An address parser can identify the number of missing zeros by separating the two parts and filling in zeros until the 128 bits are completed. However, if two double colons are placed in the address, there is no way to identify the size of each block of zeros. Therefore, only one double colon is possible in a valid IPv6 address.

The use of the double-colon technique makes many addresses very small; for example, FF01:0:0:0:0:0:0:1 becomes FF01::1. The unspecified address is written as a double colon because it contains only zeros.

IPv6 Address Types



© 2013 Cisco Systems, Inc.

IPv6 supports three types of addresses:

- **Unicast:** Unicast addresses are used in a one-to-one context.
- **Multicast:** A multicast address identifies a group of interfaces. Traffic that is sent to a multicast address is sent to multiple destinations at the same time. An interface may belong to any number of multicast groups.
- **Anycast:** An IPv6 anycast address is assigned to an interface on more than one node. When a packet is sent to an anycast address, it is routed to the nearest interface that has this address. The nearest interface is found according to the measure of distance of the particular routing protocol. All nodes that share the same address should behave the same way so that the service is offered similarly regardless of the node that services the request.

Each address type has specific rules regarding its construction and use.

IPv6 has no support for broadcast addresses in the way that they are used in IPv4. Instead, specific multicast addresses (such as the all-nodes multicast address) are used.

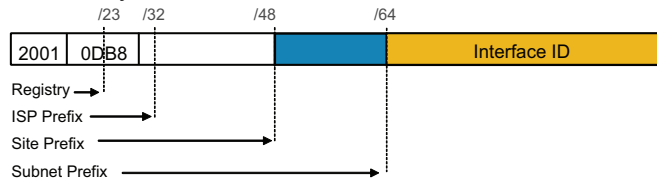
IPv6 Unicast Addresses

This topic describes the IPv6 unicast addresses.

IPv6 Unicast Addresses

Types of IPv6 unicast addresses:

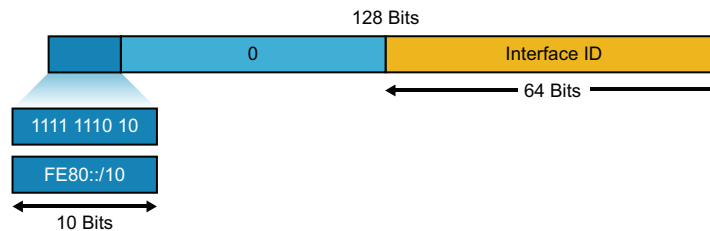
- **Global:** Starts with 2000::/3 and assigned by the Internet Assigned Numbers Authority



© 2013 Cisco Systems, Inc.

IPv6 Unicast Addresses (Cont.)

- **Private:** Link local (starts with FE80::/10)



- **Loopback** (::1)
- **Unspecified** (::)
- **Reserved:** Used by the IETF

© 2013 Cisco Systems, Inc.

There are several basic types of IPv6 unicast addresses: global, reserved, private (link-local), loopback, and unspecified.

RFC 4291 specifies 2000::/3 to be global unicast address space that the IANA may allocate to the RIRs. A global unicast address is an IPv6 address from the global unicast prefix. The structure of global unicast addresses enables the aggregation of routing prefixes, which limits the number of routing table entries in the global routing table. Global unicast addresses that are used on links are aggregated upward through organizations and eventually to the ISPs.

Link-local addresses are new to the concept of addressing with IP in the network layer. These addresses refer only to a particular physical link. Link-local addresses typically begin with "FE80." The next digits can be defined manually. If you do not define them manually, the interface MAC address is used based on the EUI-64 format.

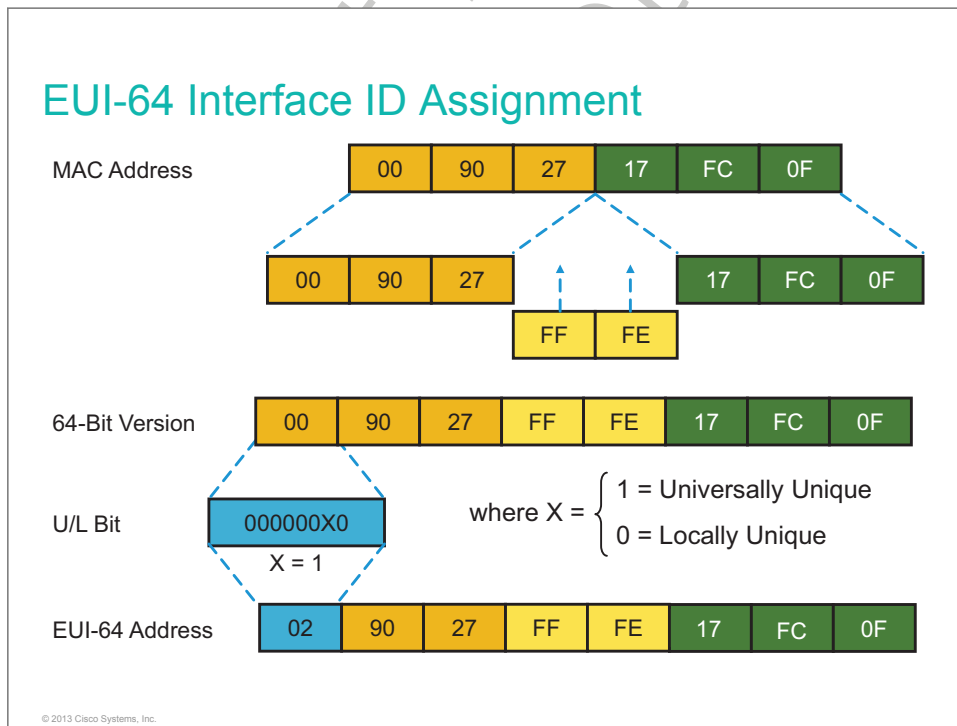
Just as in IPv4, a provision has been made for a special loopback IPv6 address for testing; datagrams that are sent to this address "loop back" to the sending device. However, in IPv6 there is just one address, not a whole block, for this function. The loopback address is 0:0:0:0:0:0:0:1, which is normally expressed as "::1".

In IPv4, an IP address of all zeroes has a special meaning in that it refers to the host itself and is used when a device does not know its own address. In IPv6, this concept has been formalized, and the all-zeroes address is named the "unspecified" address. This address is typically used in the source field of a datagram that is sent by a device that seeks to have its IP address configured. You can apply address compression to this address. Because the address is all zeroes, the address becomes just "::".

The IETF reserved a portion of the IPv6 address space for various uses, both present and future. Reserved addresses represent 1/256th of the total IPv6 address space.

- The lowest address within each subnet prefix (the interface identifier set to all zeroes) is reserved as the "subnet-router" anycast address.
- The 128 highest addresses within each /64 subnet prefix are reserved to be used as anycast addresses.

EUI-64 Interface ID Assignment

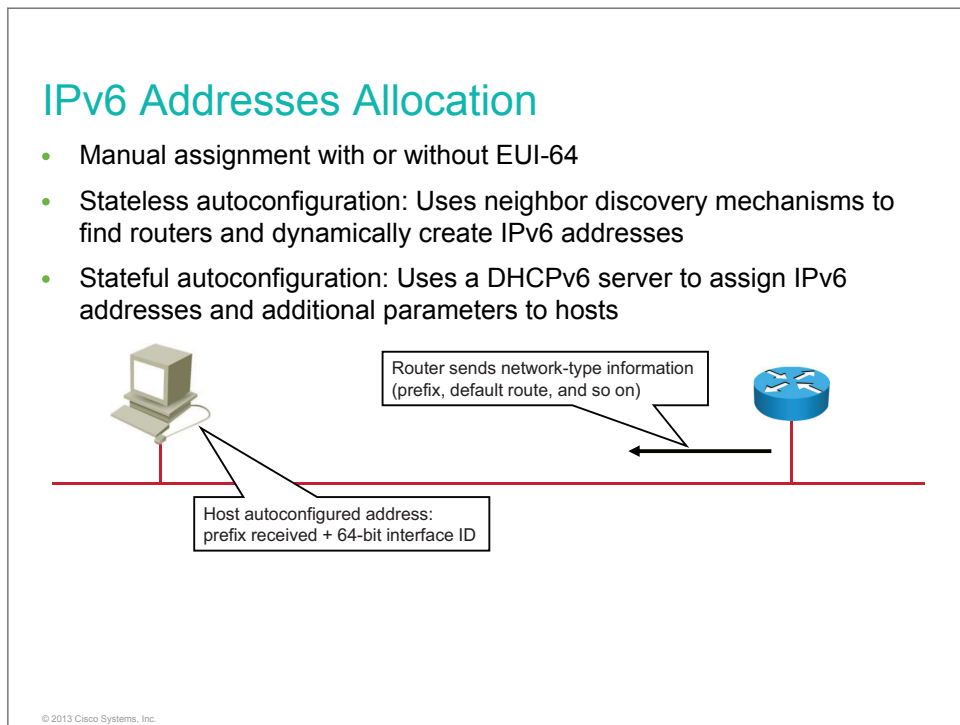


The EUI-64 standard explains how to stretch IEEE 802 MAC addresses from 48 to 64 bits by inserting the 16-bit 0xFFFE in the middle (at the 24th bit) of the MAC address to create a 64-bit, unique interface identifier. In the first byte of the vendor OUI, bit 7 indicates the scope: 0 for global and 1 for local. As most burned-in addresses are globally scoped, bit 7 will usually be 0. The EUI-64 standard also specifies that the value of the 7th bit be inverted. So for example, MAC address 00-90-27-17-FC-0F becomes 02-90-27-17-FC-0F. The resulting EUI-64 address on network 2001:0DB8:0:1::/64 would be 2001:0DB8:0:1:0290:27FF:FE17:FC0F.

Do Not Duplicate.
Post beta, not for release.

IPv6 Addresses Allocation

This topic describes different address assignment options.



The IPv6 address can be completely specified, or the host identifier (the right-most 64 bits) can be computed from the EUI-64 of the interface.

Having a much larger address space that is available, IPv6 engineers designed a way to enable autoconfiguration of the addresses while still keeping the global uniqueness. A router on the local link will send network-type information, such as the prefix of the local link and the default route, to all of the nodes on the local link. A host can autoconfigure itself by appending its data link layer address (in a special 64-bit EUI [EUI-64] format) to the local link prefix (64 bits). This autoconfiguration results in a complete 128-bit IPv6 address that is usable on the local link and is, most likely, globally unique. To avoid the rare event of address collision, a process is enabled to detect duplicate addresses.

Autoconfiguration enables “plug and play,” which connects devices to the network without any configuration and without any stateful servers (such as DHCP servers). Autoconfiguration is an important feature for enabling deployment of new devices on the Internet, such as cell phones, wireless devices, home appliances and networks, and so on.

Autoconfiguration can be accomplished in two ways: stateless—via neighbor discovery and router advertisements—as previously described, and stateful, using a DHCPv6 server. The difference between the two is that, with the stateful method, a record is kept of which hosts are assigned which addresses. The stateless method does not maintain these records.

A router announcement can indicate to hosts whether or not additional configuration parameters are available via stateful configuration (DHCPv6), such as DNS, IP options, and so on.

DNS is a distributed Internet directory service that is used to translate between domain names and IP addresses as well as between IP addresses and domain names. The DNS protocol had to be updated to support IPv6 in addition to IPv4. Using DDNS, DHCPv6 clients can dynamically update their records in DNS.

Basic IPv6 Connectivity

This topic describes needed configuration and verification tasks to enable IPv6 connectivity.

Basic IPv6 Connectivity

```
Router(config)# ipv6 unicast-routing
```

- Enables IPv6 routing on Cisco routers.

```
Router(config-if)# ipv6 address 2001:db8:D1A5:C900::1/64
```

- Configures the interface with a specific IPv6 address.

© 2013 Cisco Systems, Inc.

These are some configuration commands for enabling IPv6.

Configuring IPv6 Commands

Command	Description
<code>ipv6 unicast-routing</code>	Enables IPv6 routing on Cisco routers.
<code>ipv6 address ipv6-address/ipv6-length [eui-64]</code>	Configures the interface IPv6 address. With the eui-64 option, the last 64 bits in the address are calculated by the EUI-64 format from the MAC address. When configuring an IPv6 address and IPv6 length, there is a slash between them. Be careful, there is no space between the IPv6 address, slash, and IPv6 length.

Cisco IOS IPv6 Configuration Example



IPv6 configuration on the Branch router:

```
Branch(config)# ipv6 unicast-routing
Branch(config)# interface GigabitEthernet 0/1
Branch(config-if)# ipv6 address 2001:db8:D1A5:C900::1/64
```

IPv6 configuration on the headquarters router:

```
HQ(config)# ipv6 unicast-routing
HQ(config)# interface GigabitEthernet 0/1
HQ(config-if)# ipv6 address 2001:db8:D1A5:C900::2/64
```

© 2013 Cisco Systems, Inc.

The example shows an IPv6 configuration on two routers. The routers are connected with the Gigabit Ethernet interface.

Cisco IOS IPv6 Configuration Example (Cont.)

Cisco IOS IPv6 verification:

- Display IPv6 interface status

```
Branch# show ipv6 interface GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::FE99:47FF:FEE5:2599
  No Virtual link-local address(es):
  Description: Link to HQ
  Global unicast address(es):
    2001:DB8:D1A5:C900::1, subnet is 2001:DB8:D1A5:C900::/64
  < output omitted >
```

- Verify IPv6 connectivity

```
Branch# ping 2001:db8:D1A5:C900::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:D1A5:C900::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

© 2013 Cisco Systems, Inc.

Basic IPv6 Connectivity (Cont.)

Cisco IOS IPv6 verification (Cont.):

- Trace the IPv6 address

```
Branch# traceroute 2001:db8:D1A5:C900::2
Type escape sequence to abort.
Tracing the route to 2001:DB8:D1A5:C900::2
 1 2001:DB8:D1A5:C900::2 0 msec 0 msec 0 msec
```

- Telnet to the IPv6 address

```
Branch# telnet 2001:db8:D1A5:C900::2
Trying 2001:DB8:D1A5:C900::2 ... Open
HQ#
```

- SSH to the IPv6 address

```
Branch# ssh -l ccna 2001:DB8:D1A5:C900::2
Password:
HQ#
```

© 2013 Cisco Systems, Inc.

These are some commands for IPv6 verification.

Configuring IPv6 Commands

Command	Description
<code>show ipv6 interface interface</code>	Verifies IPv6 interface status and setup
<code>ping ipv6-address</code>	Verifies IPv6 connectivity
<code>traceroute ipv6-address</code>	Traces the IPv6 address
<code>telnet ipv6-address</code>	Uses Telnet to connect to the IPv6 address
<code>ssh -l username ipv6-address</code>	Establishes SSH remote session to the IPv6 address

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- To extend the lifetime and usefulness of IPv4 and circumvent address shortage, several mechanisms were created: CIDR, VLSM, NAT, and DHCP.
- Main IPv6 features are larger address space, simpler header, security, mobility, and transition richness.
- IPv6 addresses are represented as a series of eight 16-bit hexadecimal fields that are separated by colons.
- There are several basic types of IPv6 unicast addresses: global, reserved, private (link-local), loopback, and unspecified.
- IPv6 addresses can be allocated by manual assignment with or without EUI-64. Addresses can also be obtained automatically through stateless or stateful autoconfiguration.
- To enable IPv6 on the router, use the **ipv6 unicast-routing** command.

© 2013 Cisco Systems, Inc.

Understanding IPv6

Overview

The header format for each IP packet carries crucial information for the routing and processing of each packet payload. Header construction plays an important role in the efficiency and extensibility of the network. ICMP plays an important role in troubleshooting networks, facilitating simple tools such as ping, or determining that a packet could not reach its destination. This lesson describes both IPv6 and ICMPv6.

Any device that attaches to a network goes through numerous processes to identify itself and to obtain services from the network. This premise is true in either an IPv4 or IPv6 network. However, people who design and manage IPv6 networks will discover that although the processes that are used in IPv6, have some similarities to those that are used in IPv4, they are different. Understanding these processes is fundamental to properly supporting an IPv6-enabled environment.

This lesson describes IPv6 neighbor discovery, which is the process in which neighbors discover each other and autoconfigure addresses.

The lesson also explains how stateless autoconfiguration helps to automatically assign IPv6 addresses to devices in the network.

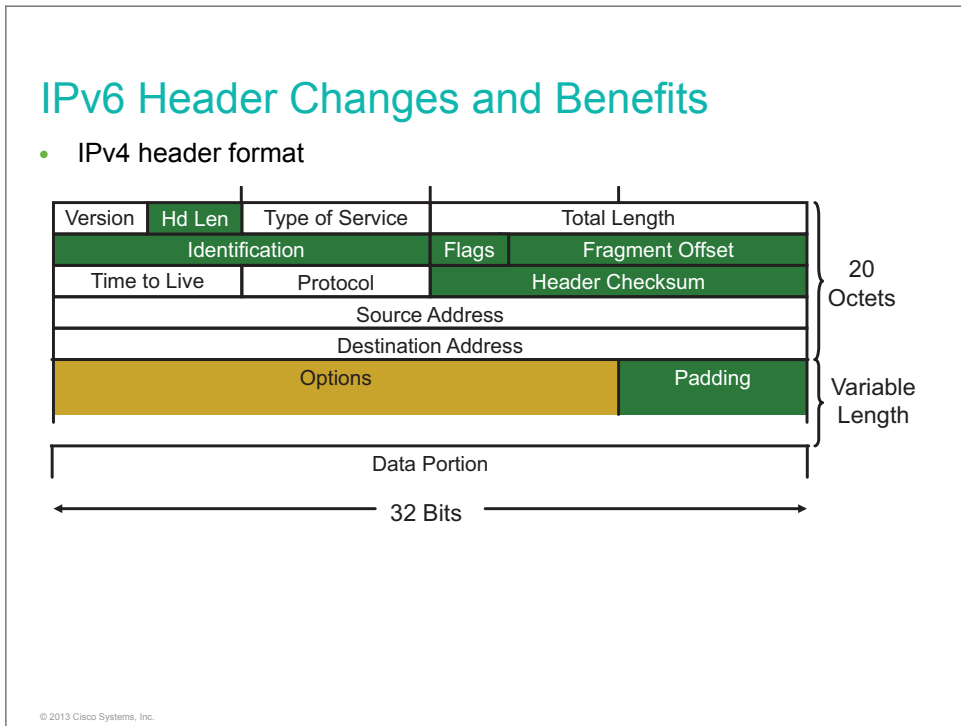
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe the IPv6 header format
- Describe ICMPv6
- Describe the neighbor discovery process and mapping from IPv6 addresses to Layer 2 addresses
- Describe and configure stateless autoconfiguration

IPv6 Header Changes and Benefits

This topic describes the IPv6 header format.



The IPv4 header contains 12 fields. Following these fields is an Options field of variable length that the figure shows in yellow and a data portion that is usually the transport layer segment. The basic IPv4 header has a size of 20 octets. The Options field increases the size of the IP header.

Of these 12 header fields, 6 are removed in IPv6; these fields are in green in the figure. The main reasons for removing these fields in IPv6 are as follows:

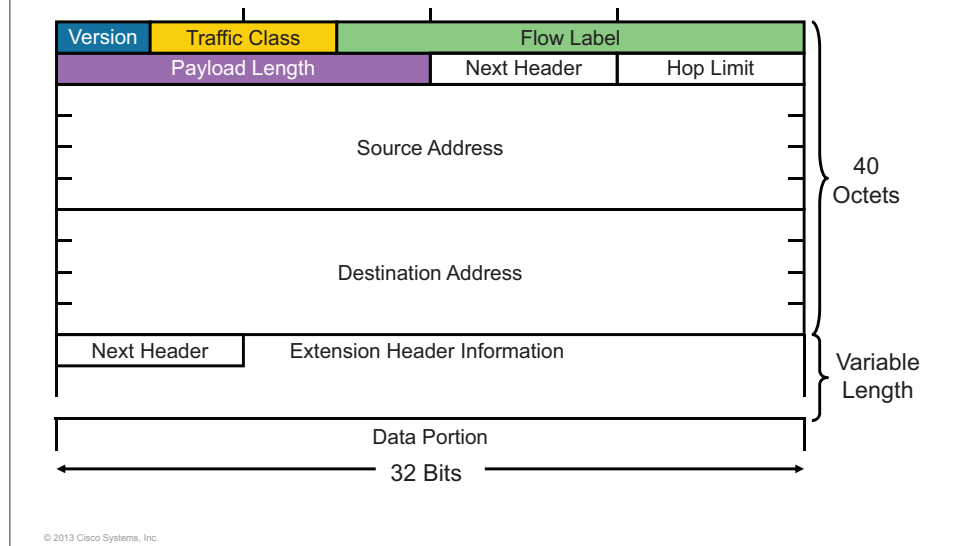
- The Internet Header Length (Hd Len) field was removed because all IPv6 headers are a fixed, 40-byte length, unlike IPv4, in which the header length is variable.
- Fragmentation is now processed differently and does not need the fields in the basic IP header. In IPv6, routers no longer process fragmentation, which is a change that removes the processing issues that result when routers process IPv4 fragmentation. The related, removed fields appear in the Fragmentation Extension Header in IPv6, which is attached only to a packet that is actually fragmented.
- The Header Checksum field at the IP layer was removed because most data link layer technologies already perform checksum and error control and because the relative reliability of the data link layer is very good. However, this removal forces the upper-layer optional checksums, such as UDP, to become mandatory.

The Options field is changed in IPv6 and is now processed by an extension header chain.

Most other fields were either unchanged or changed only slightly.

IPv6 Header Changes and Benefits (Cont.)

- IPv6 header format



The IPv6 header has 40 octets, instead of 20 octets as in IPv4. The IPv6 header has fewer fields, and the header is aligned on 64-bit boundaries to enable fast processing by current and next-generation processors. Address fields are four times larger than in IPv4.

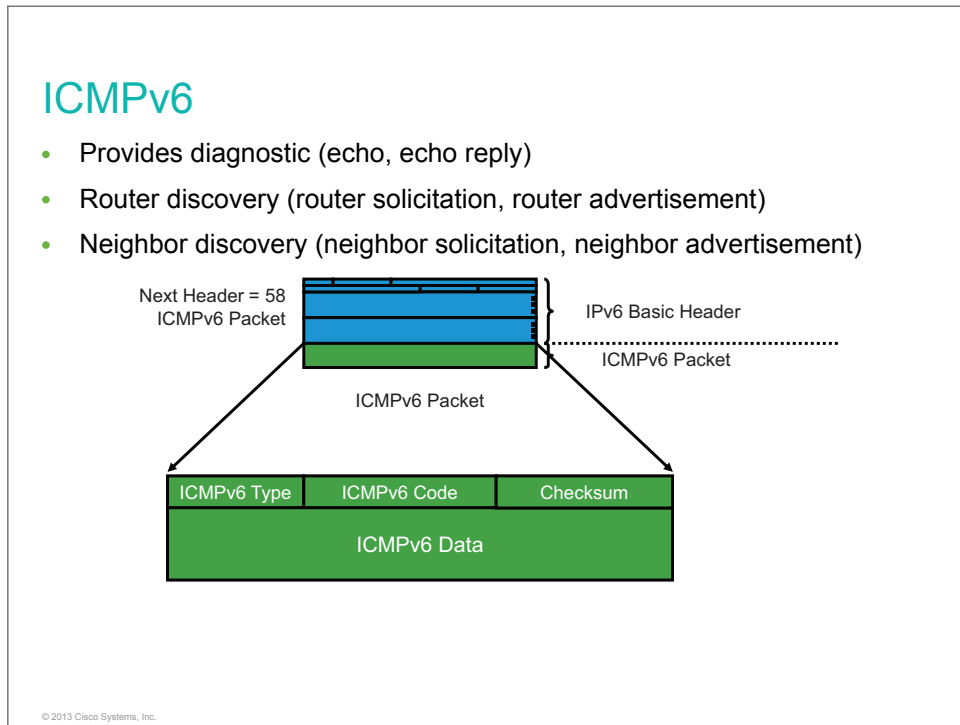
The IPv6 header contains eight fields:

1. **Version:** This 4-bit field contains the number 6, instead of the number 4 as in IPv4.
2. **Traffic Class:** This 8-bit field is like the ToS field in IPv4.
3. **Flow Label:** This new field has a length of 20 bits and is used to mark individual traffic flows with unique values, of which routers can use to provide per-flow nondefault treatment.
4. **Payload Length:** This field is like the Total Length field of IPv4, but because the IPv6 base header is a fixed size, this field describes the length of the payload only, not of the entire packet.
5. **Next Header:** The value of this field determines the type of information that follows the basic IPv6 header.
6. **Hop Limit:** This field specifies the maximum number of hops that an IP packet can traverse.
7. **Source Address:** This field of 16 octets or 128 bits identifies the source of the packet.
8. **Destination Address:** This field of 16 octets or 128 bits identifies the destination of the packet.

Following these eight fields are the extension headers, if any, that carry optional Internet layer information. The number of extension headers is not fixed, so the total length of the extension header chain is variable.

ICMPv6

This topic describes different ICMPv6 message types and how they are used.



ICMPv6 is like ICMPv4. ICMPv6 enables nodes to make diagnostic tests and report problems. Like ICMPv4, ICMPv6 implements two kinds of messages: error messages, such as Destination Unreachable, Packet Too Big, or Time Exceeded, and informational messages, such as Echo Request and Echo Reply.

The ICMPv6 packet is identified as 58 in the Next Header field. Inside the ICMPv6 packet, the Type field identifies the type of ICMP message. The Code field further details the specifics of this type of message. The Data field contains information that is sent to the receiver for diagnostics or information purposes.

ICMPv6 is used on-link for router solicitation and advertisement, for neighbor solicitation and advertisement (acquisition of data link layer addresses for IPv6 neighbors), and for the redirection of nodes to the best gateway.

Neighbor Discovery

This topic describes the neighbor discovery process and mapping between IPv6 addresses and Layer 2 addresses.

Neighbor Discovery

Neighbor discovery performs the same functions in IPv6 as ARP does in IPv4

- Neighbor discovery:
 - Determines the link layer address of a neighbor
 - Finds neighbor routers on the link
 - Queries for duplicate addresses
 - Is achieved by using ICMPv6 with IPv6 multicast

© 2013 Cisco Systems, Inc.

Neighbor discovery is used on-link for router solicitation and advertisement, for neighbor solicitation and advertisement, and for the redirection of nodes to the best gateway.

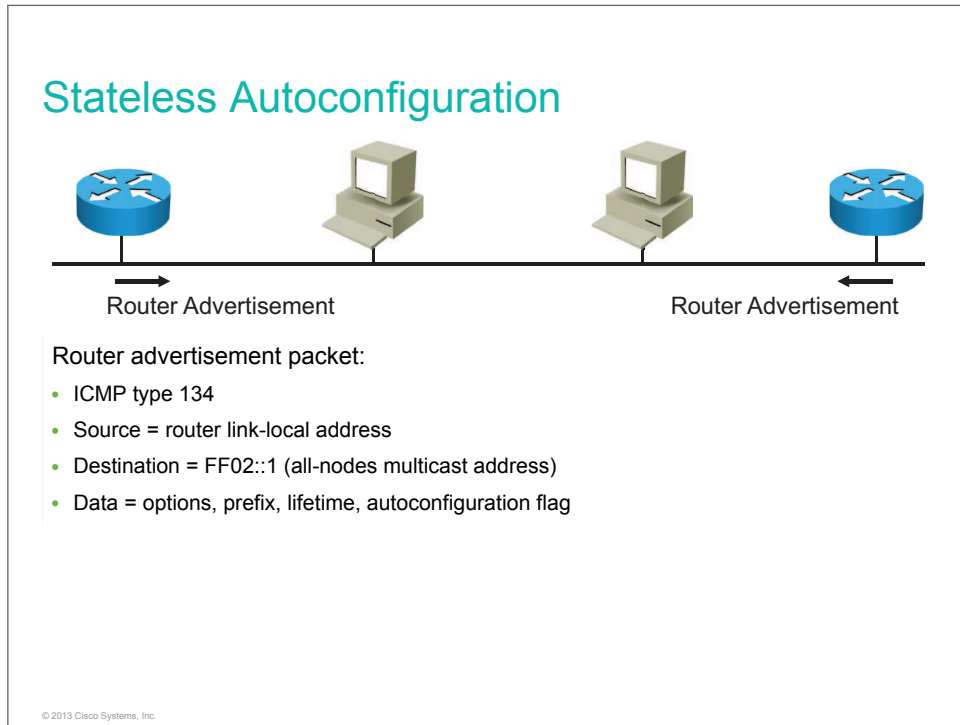
Neighbor discovery is a process that enables these functions:

- Determines the data link layer address of a neighbor on the same link, such as ARP does in IPv4
- Finds neighbor routers
- Keeps track of neighbors

Neighbor discovery achieves these results by using ICMP with multicast addresses.

Stateless Autoconfiguration

Stateless autoconfiguration uses neighbor discovery mechanisms to find routers and dynamically create IPv6 addresses. This topic describes operation and configuration of IPv6 stateless autoconfiguration.



Router advertisements are sent periodically and on request by routers on all of their configured interfaces. A router advertisement is sent to the all-nodes multicast address. This information might be contained in the message:

- One or more prefixes that can be used on the link. This information enables stateless autoconfiguration of the hosts. These prefixes must be /64 for stateless autoconfiguration.
- Lifetime of the prefixes. By default, in Cisco IOS Software, the lifetime is very long: The default valid lifetime is 30 days, and the default preferred lifetime is 7 days.
- Flags that indicate the kind of autoconfiguration that the hosts can perform.
- Default router information, such as existence and lifetime.
- Other types of information for hosts, including default MTU and hop count.

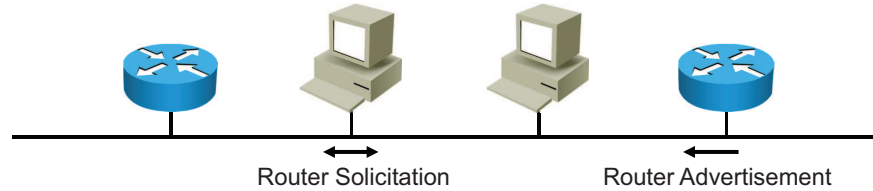
By sending prefixes, a router advertisement enables the autoconfiguration of hosts. By assigning lifetimes to prefixes, a router advertisement enables the renumbering of hosts. An old, deprecated prefix has a lifetime that is decreased to zero, and a new prefix will have a normal lifetime.

Router advertisement timing and other parameters can be configured on the routers.

Stateless Autoconfiguration (Cont.)

Router solicitations

At boot time, nodes send router solicitations to promptly receive router advertisements.



Router solicitation packet:

- ICMP type 133
- Source = :: (unspecified address)
- Destination = FF02::2 (all-routers multicast address)

© 2013 Cisco Systems, Inc.

A router advertisement is typically sent immediately following a router solicitation. Router solicitations are sent by hosts at boot time to ask routers to send an immediate router advertisement on the local link so that the host can receive the autoconfiguration information without waiting for the next scheduled router advertisement.

The router solicitation message is defined as follows:

- The ICMP type is 133.
- The source address is the unspecified address (or the IP address that is assigned to the sending interface when the IP address is known, which is not usually the case).
- The destination address is the all-routers multicast address with the link-local scope.

When an answer to a router solicitation is sent, the destination address of the router advertisement is the unicast address of the requestor.

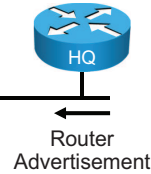
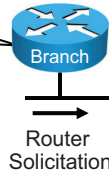
To avoid flooding, a router solicitation should be sent only at boot time and only three times. This practice avoids flooding of router solicitation packets in the absence of a router on the network.

Stateless Autoconfiguration (Cont.)

- The Branch router configures stateless autoconfiguration on the interface.
- The default route is added, based on route advertisement information, if the default keyword is added.

```
Branch(config-if)# ipv6 address autoconfig [default]
```

Configure stateless autoconfiguration on the interface



© 2013 Cisco Systems, Inc.

This is a configuration command that enables stateless autoconfiguration on the router interface.

Configuring Stateless Autoconfiguration Command

Command	Description
<code>ipv6 address autoconfig [default]</code>	Configures stateless autoconfiguration on the interface.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The IPv6 header has removed unnecessary fields, resulting in a more streamlined, simpler protocol.
- ICMPv6 provides diagnostic, router, and neighbor discovery.
- Neighbor discovery is a critical process that allows neighbors to determine the link-layer address that is associated with a given IPv6 address.
- Autoconfiguration provides a type of network “plug-and-play” feature, in which devices can assign their own address, based on router-provided information.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Configuring IPv6 Routing

Overview

Routing protocols must support IPv6 to facilitate the successful transport and operations of IPv6-generated traffic. OSPF is a widely used IGP. Understanding the differences between OSPFv2 and OSPFv3 are required for the successful deployment and operation of an IPv6 network using OSPF for routing. This lesson describes how to configure and verify static IPv6 routes and OSPFv3.

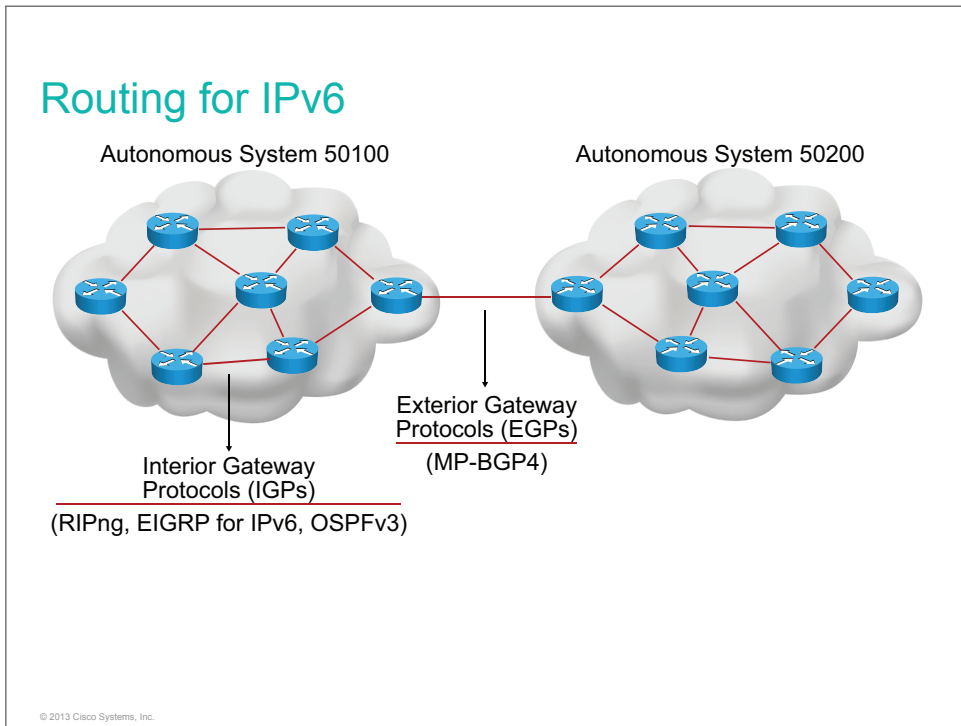
Objectives

Upon completing this lesson, you will be able to meet these objectives:

- Describe routing types for IPv6
- Configure and verify static routing for IPv6
- Configure and verify OSPFv3

Routing for IPv6

This topic describes different routing protocols and methods that support IPv6 routing.



Routing for IPv6 (Cont.)

IPv6 routing types:

- static
- RIPng (RFC 2080)
- EIGRP for IPv6
- OSPFv3 (RFC 2740)
- MP-BGP4 (RFC 2545/2858)

© 2013 Cisco Systems, Inc.

Many of the common routing protocols have been modified to handle longer IPv6 addresses and different header structures.

You can use and configure IPv6 static routing in the same way that you would with IPv4. There is an IPv6-specific requirement per RFC 2461 that a router must be able to determine the link-local address of each of its neighboring routers to ensure that the target address of a redirect message identifies the neighbor router by its link-local address. This requirement means that using a global unicast address as a next-hop address with IPv6 routing is not recommended.

Do Not Duplicate:
Post beta, not for release.

Static Routing

This topic describes how to configure and verify static IPv6 routing.

Static Routing

The diagram illustrates IPv6 static routing between two routers: Branch and HQ. The Branch router is connected to the HQ router via their Gi0/1 interfaces. The Branch router has a default route pointing to the HQ router. The HQ router has a static route pointing to the Branch router. The Branch router is connected to a network with the address 2001:DB8:A01::/48. The HQ router is connected to a network with the address 2001:DB8:AC10:100::/64. A server is connected to the HQ router, and the Internet is also connected to the HQ router. The diagram shows the flow of traffic from the Branch router to the HQ router and back.

The static IPv6 route is configured on the HQ router:

```
HQ(config)# ipv6 route 2001:DB8:A01::/48 Gi0/1 2001:DB8:D1A5:C900::1
```

The default IPv6 route is configured on the Branch router:

```
Branch(config)# ipv6 route ::/0 Gi0/1 2001:DB8:D1A5:C900::2
```

© 2013 Cisco Systems, Inc.

These are IPv6 static and default route commands:

Configuring an IPv6 Static Route Command

Command	Description
<code>ipv6 route ipv6_network/ipv6_mask outgoing_interface ipv6_next_hop</code>	Configures a static IPv6 route
<code>ipv6 route ::/0 outgoing_interface ipv6_next_hop</code>	Configures a default IPv6 route

Static Routing (Cont.)

Verify the static IPv6 route on the HQ router:

```
HQ# show ipv6 route static
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery, 1 - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    2001:DB8:A01::/48 [1/0]
    via 2001:DB8:D1A5:C900::1, GigabitEthernet0/1
```

© 2013 Cisco Systems, Inc.

Static Routing (Cont.)

Verify the default IPv6 route on the Branch router:

```
Branch# show ipv6 route static
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery, 1 - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    ::/0 [1/0]
    via 2001:DB8:D1A5:C900::2, GigabitEthernet0/1
```

© 2013 Cisco Systems, Inc.

Static Routing (Cont.)

Verify IPv6 connectivity from the Branch router to IPv6 address
2001:db8:AC10:100::64:

```
Branch# ping 2001:db8:AC10:100::64
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:AC10:100::64, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

© 2013 Cisco Systems, Inc.

These are IPv6 static routing verification commands:

IPv6 Static Routing Verification Commands

Command	Description
<code>show ipv6 route</code>	Displays IPv6 routing information
<code>ping ipv6_address</code>	Verifies connectivity to the IPv6 address

OSPFv3

This topic describes how to configure and verify OSPFv3.

OSPFv3

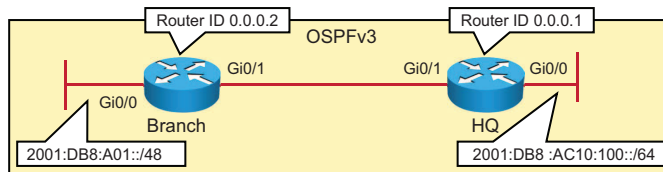
- Router ID looks like an IPv4 address.
- Adjacencies and next-hop attributes use link-local addresses.
- IPv6 is used for transport of the LSA.
- OSPFv3 is enabled per link, not per network.

© 2013 Cisco Systems, Inc.

These OSPF features have been updated for IPv6:

- The OSPFv3 process no longer requires an IPv4 address for the router ID, but it does require a 32-bit number to be set.
- OSPFv3 adjacencies use link-local addresses to communicate. Router next-hop attributes are neighboring router link-local addresses. Because link-local addresses have the same prefix, OSPF needs to store the information about the outgoing interface.
- OSPFv3 uses IPv6 for transport of LSAs. IPv6 protocol number 89 is used.
- OSPFv3 is enabled per-link and identifies which networks (prefixes) are attached to this link for determining prefix reachability propagation and OSPF area.

OSPFv3 (Cont.)



OSPFv3 is configured on the HQ router:

```
HQ(config)# interface GigabitEthernet0/0
HQ(config-if)# ipv6 ospf 1 area 0
HQ(config-if)# exit
HQ(config)# interface GigabitEthernet0/1
HQ(config-if)# ipv6 ospf 1 area 0
HQ(config-if)# exit
HQ(config)# ipv6 router ospf 1
HQ(config-rtr)# router-id 0.0.0.1
```

© 2013 Cisco Systems, Inc.

OSPFv3 (Cont.)

OSPFv3 is configured on the Branch router:

```
Branch(config)# interface GigabitEthernet0/0
Branch(config-if)# ipv6 ospf 1 area 0
Branch(config-if)# exit
Branch(config)# interface GigabitEthernet0/1
Branch(config-if)# ipv6 ospf 1 area 0
Branch(config-if)# exit
Branch(config)# ipv6 router ospf 1
Branch(config-rtr)# router-id 0.0.0.2
```

© 2013 Cisco Systems, Inc.

These are OSPFv3 commands:

Configuring OSPFv3 Commands

Command	Description
<code>ipv6 ospf process_id area area_id</code>	Enables OSPFv3 routing on the interface
<code>ipv6 router ospf process_id</code>	Enables the OSPFv3 routing process and enters routing process configuration mode
<code>router-id router_id</code>	Sets the OSPFv3 router ID with a 32-bit number

OSPFv3 (Cont.)

Verify the OSPFv3 route on the Branch router:

```
Branch# show ipv6 route ospf
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery, 1 - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O      2001:DB8:AC10:100::64/128 [110/1]
      via FE80::FE99:47FF:FEE5:2551, GigabitEthernet0/1
```

Verify the OSPFv3 neighbor on the Branch router:

```
Branch# show ipv6 ospf neighbor
Neighbor ID    Pri  State           Dead Time   Interface ID  Interface
0.0.0.1       1    FULL/BDR       00:00:38   4             GigabitEthernet0/1
```

© 2013 Cisco Systems, Inc.

OSPFv3 (Cont.)

Verify OSPFv3 settings on the Branch router:

```
Branch# show ipv6 ospf
Routing Process "ospfv3 1" with ID 0.0.0.2
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
< output omitted >
```

© 2013 Cisco Systems, Inc.

These are OSPFv3 verification commands:

OSPFv3 Verification Commands

Command	Description
show ipv6 route	Displays IPv6 routing information
show ipv6 ospf neighbor	Displays OSPFv3 neighbors
show ipv6 ospf	Displays OSPFv3 settings (process ID, timers, and number of areas)

Do Not Duplicate.
Post beta, not for release.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Cisco supports all of the major IPv6 routing protocols: RIPng, OSPFv3, and EIGRP.
- Configure the IPv6 static and default route by using the **ipv6 route** command.
- OSPFv3 is enabled per link and not per network. OSPFv3 adjacencies use link-local addresses to communicate.

© 2013 Cisco Systems, Inc.

Do Not Duplicate.
Post beta, not for release.

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- IPv6 includes a number of features that make it attractive for building global-scale, highly effective networks. The larger address space and autoconfiguration provide important capabilities.
- Neighbor discovery is used on-link for router solicitation and advertisement, for neighbor solicitation and advertisement, and for the redirection of nodes to the best gateway.
- You can use and configure IPv6 static routing in the same way that you would with IPv4. OSPFv3 is one of the dynamic routing protocols that supports IPv6.

Do Not Duplicate.
Post beta, not for release.

Module Self-Check

Do Not Duplicate.
Post beta, not for release.

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. What was the primary issue that was solved by creating IPv6? (Source: Introducing Basic IPv6)
 - A. running out of address space
 - B. complicated IPv4 header
 - C. security and mobility
 - D. richness in the transition tools

2. What is the shortest way to represent IPv6 address 2001:0DB8:0000:300F:0000:0000:A87C:040B? (Source: Introducing Basic IPv6)
 - A. 2001:DB8:0:300F:0:A87C:40B
 - B. 2001:DB8:0:300F::A87C:40B
 - C. 2001:DB8::300F::A87C:40B
 - D. 2001:0DB8:0:300F::A87C:040B

3. Which three IPv4 header fields were present in the IPv4 header but not in the IPv6 header? (Choose three.) (Source: Understanding IPv6)
 - A. IHL
 - B. type of service
 - C. header checksum
 - D. flags
 - E. flow label

4. The extension headers serve which important function in IPv6 networks? (Source: Understanding IPv6)
 - A. carry optional Internet layer information
 - B. allow IPv6 nodes to manipulate routers
 - C. identify processes that manipulate the routers in the path of a packet
 - D. replace the traditional role of TCP and UDP in a network

5. Neighbor discovery is used for which two of these functions? (Choose two.) (Source: Understanding IPv6)
 - A. discover Layer 2 addresses of on-link IPv6 peers
 - B. discover the global unicast address of the other host on the subnet
 - C. discover the Layer 2 address of the other host on the subnet
 - D. discover the link-local IPv6 addresses of on-link neighbors

6. Which interface command causes the IPv6 interface address to be obtained using stateless autoconfiguration? (Source: Understanding IPv6)
- A. **autoconfig ipv6 address**
 - B. **ipv6 address autoconfig**
 - C. **autoconfig ip address**
 - D. **ipv6 address stateless autoconfig**
7. Which command is used to configure the static IPv6 default route? (Source: Configuring IPv6 Routing)
- A. **ipv6 route ::/0 interface next_hop**
 - B. **ipv6 route default interface next_hop**
 - C. **ipv6 route 0.0.0.0/0 interface next_hop**
 - D. **ip route 0.0.0.0/0 interface next_hop**
8. Which item represents similarities between OSPFv3 and OSPFv2? (Source: Configuring IPv6 Routing)
- A. support for IPv4 and IPv6
 - B. support for IPv4
 - C. enabled per-link, rather than per-network, using network statements
 - D. link-state routing protocols

Answer Key

1. A
2. B
3. A, C, D
4. A
5. A, C
6. B
7. A
8. D

Do Not Duplicate.
Post beta, not for release.

Do Not Duplicate:
Post beta, not for release.

Do Not Duplicate.
Post beta, not for release.

Glossary

Term	Definition
AAA	authentication, authorization, and accounting. Pronounced "triple a."
ACL	access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
AfriNIC	African Network Information Center.
API	application program interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. A set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.
APNIC	Asia Pacific Network Information Center. Nonprofit Internet registry organization for the Asia Pacific region. The other Internet registries are currently IANA, RIPE NCC, and InterNIC.
ARIN	American Registry for Internet Numbers. A nonprofit organization established for the purpose of administrating and registering IP numbers to the geographical areas currently managed by Network Solutions (InterNIC). Those areas include, but are not limited to, North America, South America, South Africa, and the Caribbean.
ARP	Address Resolution Protocol. Internet protocol that is used to map an IP address to a MAC address. Defined in RFC 826.
AS	autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA.
BDR	backup designated router.
BGP	Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.
BIA	burned-in MAC address.
CAM	content-addressable memory.

Term	Definition
CIDR	classless interdomain routing. Technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes together to reduce the quantity of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity. With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, followed by a forward slash and a two-digit number that represents the subnet mask.
CoS	class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition comprises a virtual route number and a transmission priority field. Also called <i>ToS</i> .
CPE	customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. Can also refer to any telephone equipment residing on the customer site.
CRC	cyclic redundancy check. Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection. Media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. Ethernet and IEEE 802.3 use CSMA/CD access.
CSU	channel service unit. Digital interface device that connects end-user equipment to the local digital telephone loop. Often referred to together with DSU, as <i>CSU/DSU</i> .
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.
DR	designated router.

Term	Definition
DSL	digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.
DSU	data service unit. Device used in digital transmission that adapts the physical interface on a DTE device to a transmission facility, such as T1 or E1. The DSU also is responsible for such functions as signal timing. Often referred to together with CSU, as <i>CSU/DSU</i> .
DTP	Dynamic Trunking Protocol.
DUAL	Diffusing Update Algorithm. Convergence algorithm used in EIGRP that provides loop-free operation at every instant throughout a route computation. Allows routers involved in a topology change to synchronize at the same time, while not involving routers that are unaffected by the change.
EBCDIC	extended binary coded decimal interchange code. Any of a number of coded character sets developed by IBM consisting of 8-bit coded characters. Older IBM systems and telex machines use this character code.
EGP	Exterior Gateway Protocol. Internet protocol for exchanging routing information between autonomous systems. Documented in RFC 904. Not to be confused with the general term <i>exterior gateway protocol</i> . EGP is an obsolete protocol that was replaced by BGP.
EIGRP	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link-state protocols with those of distance vector protocols.
EMI	electromagnetic interference. Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
EUI	extended universal identifier
FC	fiber-optic connector.
FCS	frame check sequence. Extra characters added to a frame for error control purposes. Used in HDLC, Frame Relay, and other data link layer protocols.
FTP	File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.
GARP	Gratuitous Address Resolution Protocol.
giaddr	gateway IP address

Term	Definition
Gigabit Ethernet	Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.
header	Control information placed before data when encapsulating that data for network transmission.
IANA	Internet Assigned Numbers Authority. Organization operated under the auspices of the ISOC as a part of the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the InterNIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP stack, including autonomous system numbers.
ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.
IEEE 802.11	A set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4-, 3.6-, and 5-GHz frequency bands.
IEEE 802.1Q	The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information and defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure.
IETF	Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.
IGMP	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.
IGP	interior gateway protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.
IHL	Internet Header Length. Name of an IP header field.
InterNIC	Organization that serves the Internet community by supplying user assistance, documentation, training, registration service for Internet domain names, and other services. Formerly called NIC.
IOS	Internetwork Operating System
IP	Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

Term	Definition
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.
IPsec	IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
IPv4	IP version 4
IPv6	IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).
IS-IS	Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, whereby ISs (routers) exchange routing information based on a single metric to determine network topology.
ISP	Internet service provider. Company that provides Internet access to other companies and individuals.
LACNIC	Latin American and Caribbean Network Information Center.
LC	local connector.
LIR	local Internet registry
LLC	Logical Link Control. The higher of the two data link layer sublayers defined by the IEEE. The LLC sublayer handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants.
LLDP	Link Layer Discovery Protocol
LSA	link-state advertisement. Broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables. Sometimes called an LSP.

Term	Definition
MD5	Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPsec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.
MMF	multimode fiber. Optical fiber supporting the propagation of multiple frequencies of light.
MOTD banner	message-of-the-day banner
MP-BGP	Multiprotocol Border Gateway Protocol
MSB	most significant bit. Bit $n-1$ in an n bit binary number, the bit with the greatest weight ($2^{(n-1)}$). The first or leftmost bit when the number is written in the usual way.
MTBF	mean time between failures.
MTU	maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.
multicast address	Single address that refers to multiple network devices. Synonymous with group address.
NAT	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.
NCC	Network Coordination Centre.
NFS	Network File System. As commonly used, a distributed file system protocol suite developed by Sun Microsystems that allows remote file access across a network. In actuality, NFS is simply one protocol in the suite. NFS protocols include NFS, RPC, XDR, and others. These protocols are part of a larger architecture that Sun refers to as ONC.
NIC	network interface card. Board that provides network communication capabilities to and from a computer system. Also called an adapter.
NTP	Network Time Protocol. Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
NVRAM	nonvolatile RAM. RAM that retains its contents when a unit is powered off.
OSI	Open Systems Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.

Term	Definition
OSPF	Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol.
OUI	Organizational Unique Identifier. Three octets that are assigned by the IEEE in a block of 48-bit LAN addresses.
PAT	port address translation. Translation method that allows the user to conserve addresses in the global address pool by allowing source ports in TCP connections or UDP conversations to be translated. Different local addresses then map to the same global address, with port translation providing the necessary uniqueness. When translation is required, the new port number is picked out of the same range as the original following the convention of Berkeley Standard Distribution (SD).
PDU	protocol data unit. OSI term for packet.
POP	Post Office Protocol. Protocol that client email applications use to retrieve mail from a mail server.
POST	power-on self test. Set of hardware diagnostics that runs on a hardware device when this device is powered on.
QoS	quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
RFC	Request For Comments. Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.
RFI	radio frequency interference. Radio frequencies that create noise that interferes with information being transmitted across unshielded copper cable.
RIP	Routing Information Protocol. IGP supplied with UNIX BSD systems. The most common IGP in the Internet. RIP uses hop count as a routing metric.
RIPE	Reseaux IP Europeennes. Group formed to coordinate and promote TCP/IP-based networks in Europe.
RIPng	Routing Information Protocol next generation
RIR	regional Internet registry
RSA	Acronym stands for Rivest, Shamir, and Adleman, the inventors of the technique. Public-key cryptographic system that can be used for encryption and authentication.

Term	Definition
RTT	round-trip time. Time required for a network communication to travel from the source to the destination and back. RTT includes the time required for the destination to process the message from the source and to generate a reply. RTT is used by some routing algorithms to aid in calculating optimal routes.
SC	subscriber connector.
SCP	Service Control Point. An element of an SS7-based Intelligent Network that performs various service functions, such as number translation, call setup and teardown, and so on.
SLA	service level agreement.
SMF	single-mode fiber. Fiber-optic cabling with a narrow core that allows light to enter only at a single angle. Such cabling has higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width (for example, a laser). Also called monomode fiber.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SPF	shortest path first. Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.
SSH	Secure Shell Protocol. Protocol that provides a secure remote connection to a router through a TCP application.
SSL	Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
ST	straight tip.
STP	Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning Tree Protocol standard and the earlier Digital Equipment Corporation Spanning Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.
SVI	switch virtual interface
TCP/IP	Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.

Term	Definition
TLS	Transport Layer Security. A future IETF protocol to replace SSL.
ToS	type of service
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
ULP	upper-layer protocol. Protocol that operates at a higher layer in the OSI reference model, relative to other layers. ULP is sometimes used to refer to the next-highest protocol (relative to a particular protocol) in a protocol stack.
UPS	uninterruptible power supply.
UTC	Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.
UTP	unshielded twisted-pair. Four-pair wire medium used in a variety of networks. UTP does not require the fixed spacing between connections that is necessary with coaxial-type connections. Five types of UTP cabling are commonly used: Category 1, Category 2, Category 3, Category 4, and Category 5.
VLSM	variable-length subnet mask. Capability to specify a different subnet mask for the same network number on different subnets. VLSM can help optimize available address space.
3G mobile network	third generation mobile network. Refers generically to a category of next-generation mobile networks, such as UMTS and IMT-2000.
4G	the fourth generation of mobile phone mobile communications standards.

Do Not Duplicate.
Post beta, not for release.