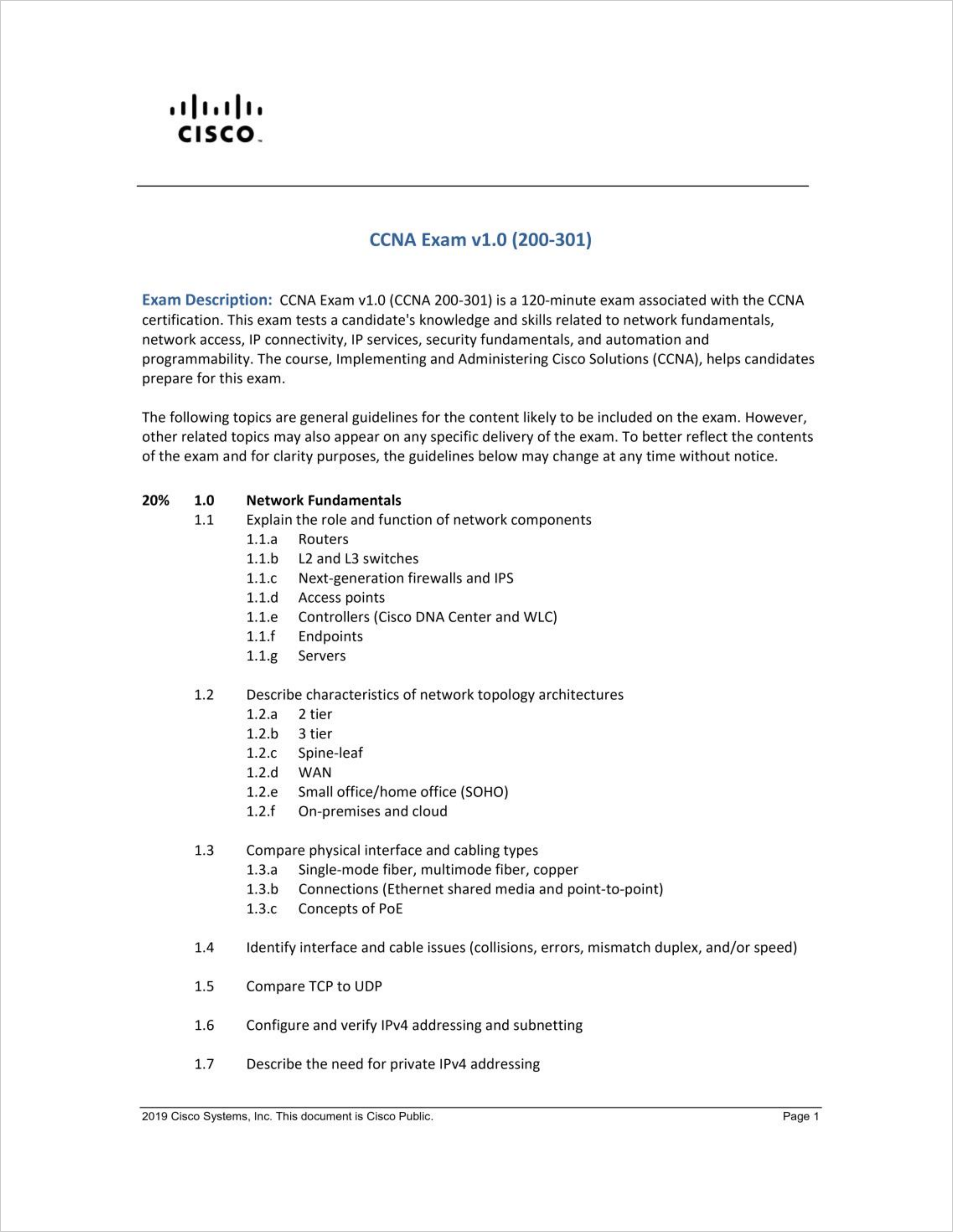
Exam Objectives

Monday, June 14, 2021 2:27 PM



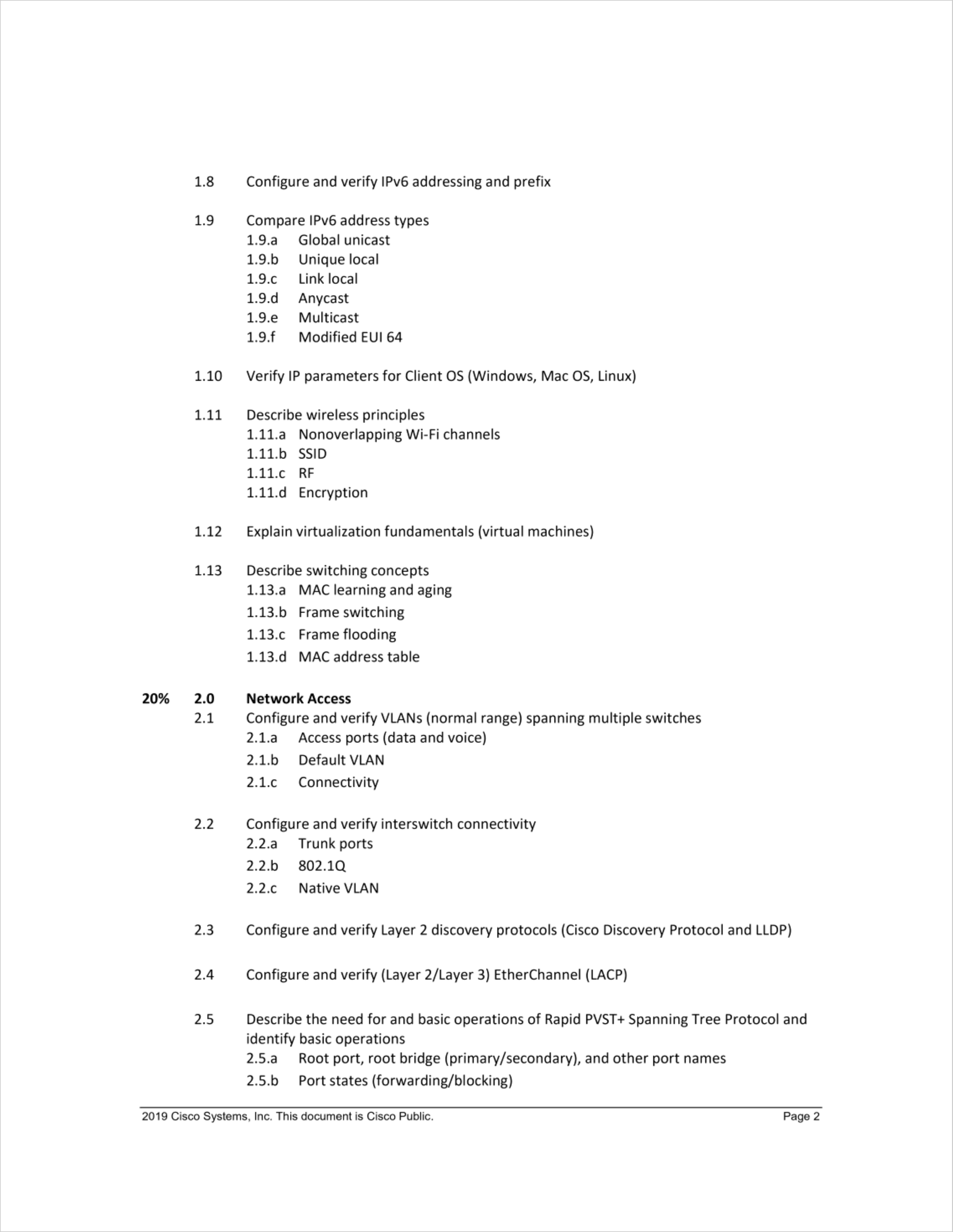
CCNA Exam v1.0 (200-301)

Exam Description: CCNA Exam v1.0 (CCNA 200-301) is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. The course, Implementing and Administering Cisco Solutions (CCNA), helps candidates prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

20% 1.0 Network Fundamentals

- 1.1 Explain the role and function of network components
  - 1.1.a Routers
  - 1.1.b L2 and L3 switches
  - 1.1.c Next-generation firewalls and IPS
  - 1.1.d Access points
  - 1.1.e Controllers (Cisco DNA Center and WLC)
  - 1.1.f Endpoints
  - 1.1.g Servers
- 1.2 Describe characteristics of network topology architectures
  - 1.2.a 2 tier
  - 1.2.b 3 tier
  - 1.2.c Spine-leaf
  - 1.2.d WAN
  - 1.2.e Small office/home office (SOHO)
  - 1.2.f On-premises and cloud
- 1.3 Compare physical interface and cabling types
  - 1.3.a Single-mode fiber, multimode fiber, copper
  - 1.3.b Connections (Ethernet shared media and point-to-point)
  - 1.3.c Concepts of PoE
- 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
- 1.5 Compare TCP to UDP
- 1.6 Configure and verify IPv4 addressing and subnetting
- 1.7 Describe the need for private IPv4 addressing



1.8 Configure and verify IPv6 addressing and prefix

1.9 Compare IPv6 address types

1.9.a Global unicast

1.9.b Unique local

1.9.c Link local

1.9.d Anycast

1.9.e Multicast

1.9.f Modified EUI 64

1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)

1.11 Describe wireless principles

1.11.a Nonoverlapping Wi-Fi channels

1.11.b SSID

1.11.c RF

1.11.d Encryption

1.12 Explain virtualization fundamentals (virtual machines)

1.13 Describe switching concepts

1.13.a MAC learning and aging

1.13.b Frame switching

1.13.c Frame flooding

1.13.d MAC address table

20% 2.0 Network Access

2.1 Configure and verify VLANs (normal range) spanning multiple switches

2.1.a Access ports (data and voice)

2.1.b Default VLAN

2.1.c Connectivity

2.2 Configure and verify interswitch connectivity

2.2.a Trunk ports

2.2.b 802.1Q

2.2.c Native VLAN

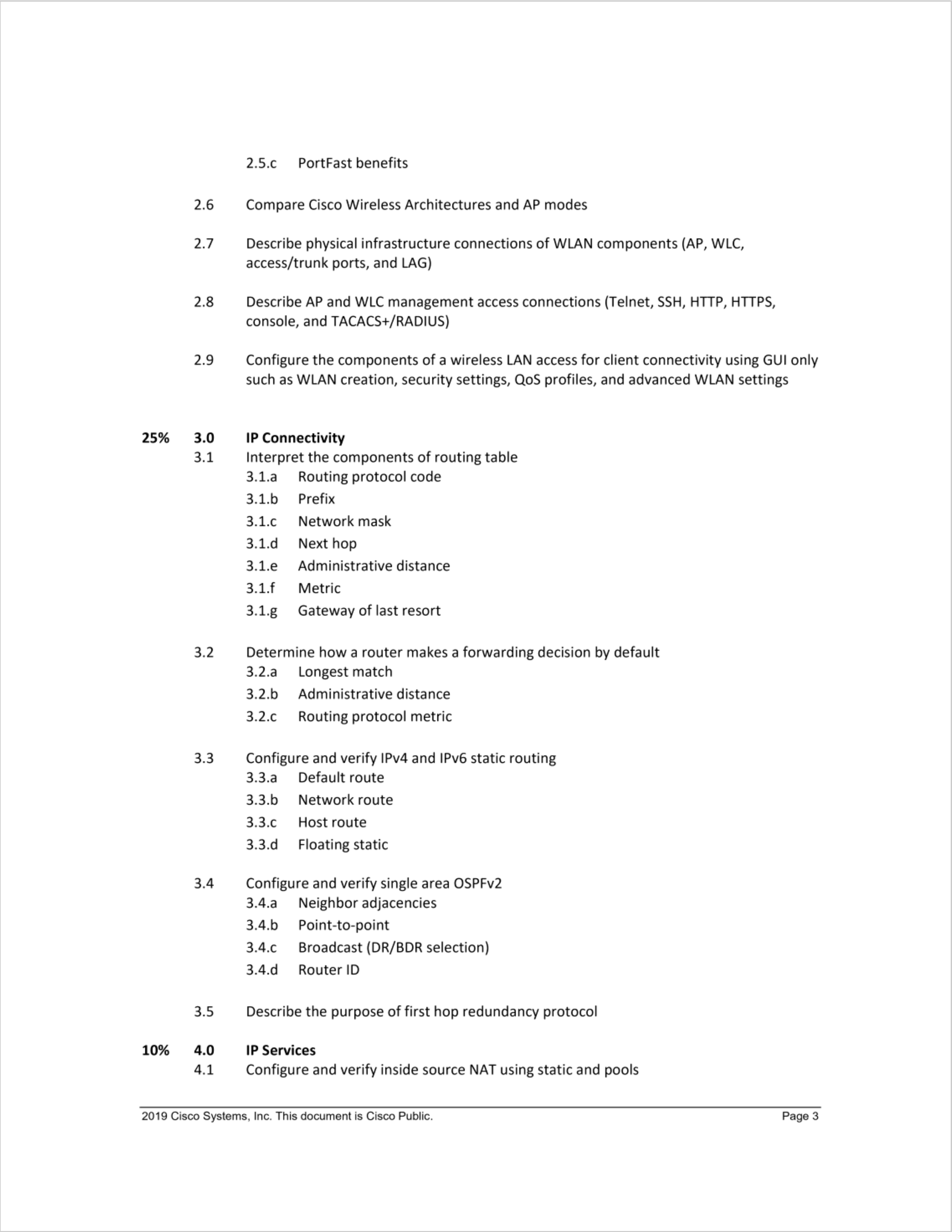
2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations

2.5.a Root port, root bridge (primary/secondary), and other port names

2.5.b Port states (forwarding/blocking)



2.5.c PortFast benefits

2.6 Compare Cisco Wireless Architectures and AP modes

2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)

2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)

2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

25% 3.0 IP Connectivity

3.1 Interpret the components of routing table

3.1.a Routing protocol code

3.1.b Prefix

3.1.c Network mask

3.1.d Next hop

3.1.e Administrative distance

3.1.f Metric

3.1.g Gateway of last resort

3.2 Determine how a router makes a forwarding decision by default

3.2.a Longest match

3.2.b Administrative distance

3.2.c Routing protocol metric

3.3 Configure and verify IPv4 and IPv6 static routing

3.3.a Default route

3.3.b Network route

3.3.c Host route

3.3.d Floating static

3.4 Configure and verify single area OSPFv2

3.4.a Neighbor adjacencies

3.4.b Point-to-point

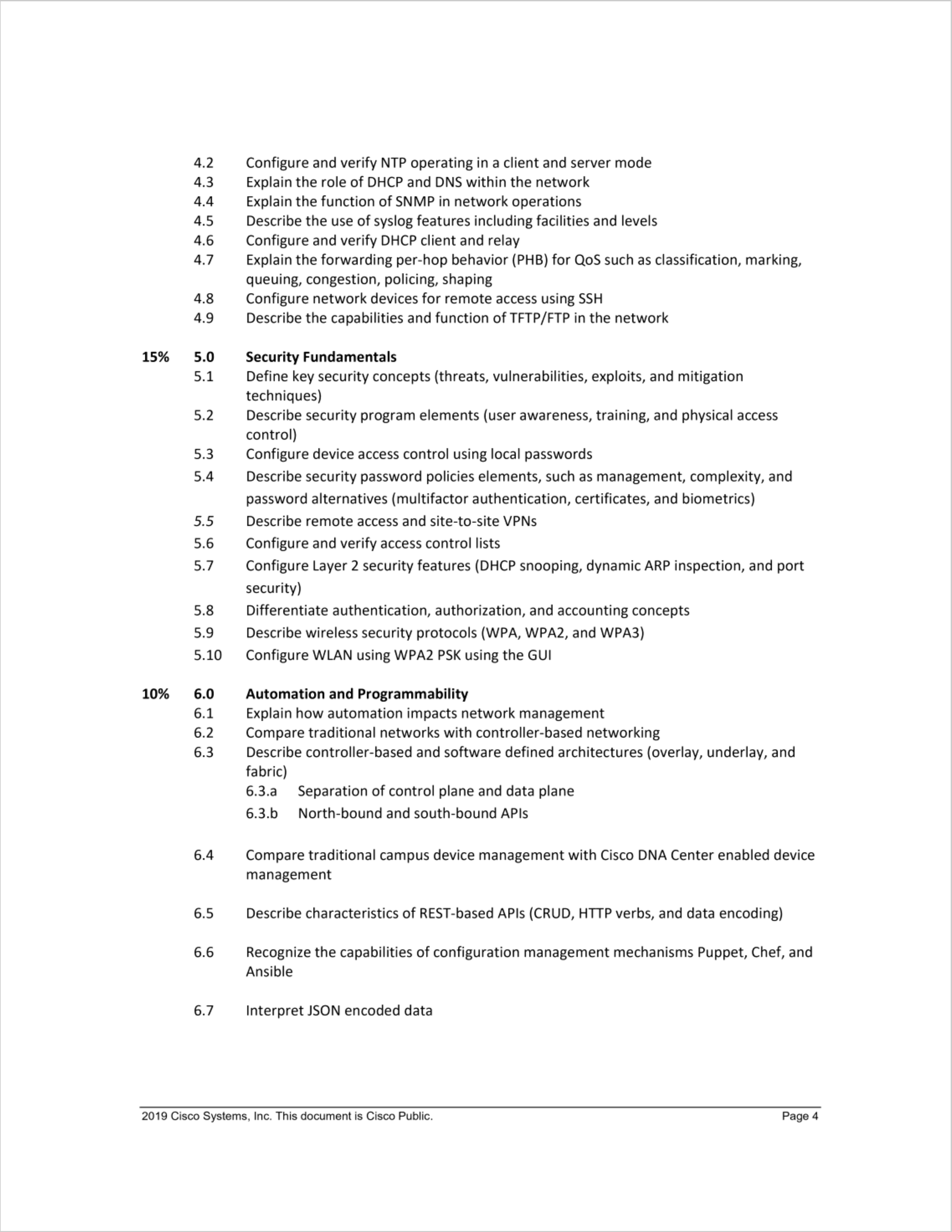
3.4.c Broadcast (DR/BDR selection)

3.4.d Router ID

3.5 Describe the purpose of first hop redundancy protocol

10% 4.0 IP Services

4.1 Configure and verify inside source NAT using static and pools



4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

15% 5.0 Security Fundamentals
5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
5.2 Describe security program elements (user awareness, training, and physical access control)
5.3 Configure device access control using local passwords
5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
5.5 Describe remote access and site-to-site VPNs
5.6 Configure and verify access control lists
5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
5.8 Differentiate authentication, authorization, and accounting concepts
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
5.10 Configure WLAN using WPA2 PSK using the GUI

10% 6.0 Automation and Programmability
6.1 Explain how automation impacts network management
6.2 Compare traditional networks with controller-based networking
6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)
6.3.a Separation of control plane and data plane
6.3.b North-bound and south-bound APIs

6.4 Compare traditional campus device management with Cisco DNA Center enabled device management

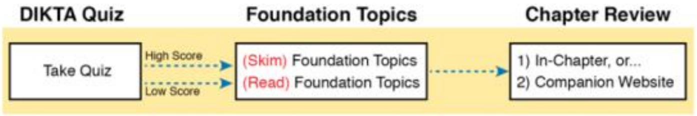
6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible

6.7 Interpret JSON encoded data

Study Plan

Monday, May 17, 2021 7:56 AM



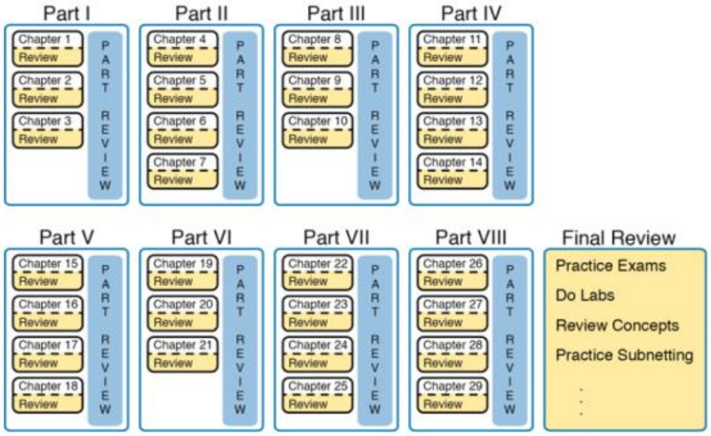
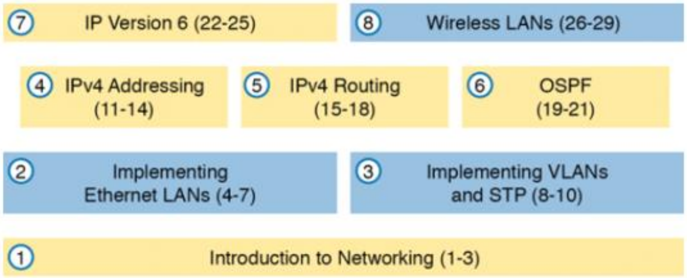


Figure 2 *Eight Parts, with an Average of Four Chapters Each, with Part Reviews*


7 IP Version 6 (22-25)
8 Wireless LANs (26-29)
4 IPv4 Addressing (11-14)
5 IPv4 Routing (15-18)
6 OSPF (19-21)
2 Implementing Ethernet LANs (4-7)
3 Implementing VLANs and STP (8-10)
1 Introduction to Networking (1-3)

1. TCP/IP basic

Tuesday, April 27, 2021 10:21 AM

Exam Topics:

1.0 Network Fundamentals

1.3 Compare physical interface and cabling types

1.3a Single-mode fiber, multimode fiber, copper

1.3b Connections (Ethernet shared media and point-to-point)

TCP/IP Model

-Application
-Transport
-Network
-Data Link
-Physical

Application Layer

- services for applications
- http provides interface between software and the network
- HTTP overview
  - HTTP Header GET home.html
  - HTTP Header OK/ Data

Same layer interaction on different computers

- Communicate with the same layer on another computer.

Adjacent layer interaction on the same computer

- One lower layer provides a service to the layer just above.
- The higher layer makes the next lower layer perform a function

*Wireless protocols are Layer 2

Encapsulation

- TCP/ Data (segment)
- IP/ Data (Packet)
- LH/ Data/ LT (Frame) (Link header & Link Trailer)

Protocol Data Units

- L7H/ Data (L7PDU)
- L6H/ Data (L6PDU)
- L5H/ Data (L5PDU)

- L4H/ Data (L4PDU)
- L3H/ Data (L3PDU)
- L2H/ Data/ L2T (L2PDU)

2. Ethernet LANs

Thursday, June 10, 2021 8:00 AM

1.0 Network Fundamentals
1.1 Explain the role and function of network components
1.1.b L2 and L3 Switches
1.2 Describe characteristics of network topology architectures
1.2.e Small office/home office (SOHO)
1.3 Compare physical interface and cabling types
1.3.a Single-mode fiber, multimode fiber, copper
1.3.b Connections (Ethernet shared media and point-to-point)

802.3 (Ethernet Standards

10BASE-T

- 10 Mbps
- Ethernet
- 802.3
- Copper/ 100 m

100BASE-T

- 100 Mbps
- Fast Ethernet
- 802.3u
- Copper/ 100m

1000BASE-LX

- 1000 Mbps
- Gigabit Ethernet
- 802.3z
- Fiber, 5000 m

1000BASE-T

- 1000 Mbps
- Gigabit Ethernet
- 802.3ab
- Copper, 100m

10GBASE-T

- 10 Gbps
- 10 Gig Ethernet
- 802.3an
- Copper 100m

Three most common

- 10BASE-T, 100BASE-T, and 1000BASE-T

Twisting of the wires helps reduce EMI.

Crosstalk
-EMI between wire pairs

Gigabit Ethernet interface Converter (GBIC)

- The original form factor for a removeable transceiver for Gigabit interfaces; larger than SFPs

Small Form Pluggable (SFP)

- The replacement for GBICs, used on gigabit interfaces, with a smaller size, taking less space on the side of the networking card or switch.

Small Form Pluggable Plus (SFP+)

- Same size as the SFP, but used on 10-Gbps interfaces

UTP Cabling Pinouts for 10BASE-T and 100BASE-T

10BASE-T and 100BASE-T
- 2 wire pairs,
- one pair for each direction

Crossover

PC/ Router/ AP
- transmits on pins 1/2
- RECEIVES ON PINS 3/6

Switch/ Hub
- Transmits on pins 3/6
- receives on pins 1/2

Ethernet NIC transmitters send on pins 1 and 2
NIC receivers receive on pins 3 and 6

Straight through cable

- Pins 1/2 > 1/2
- Pins 3/6 > 3/6

auto-mdix (cisco)

- Notices when a wrong cable is used
- automatically changes it's logic to make the link work.

1000BASE-T

- 4 wire pairs
- Both ends transmit and receive simultaneously on each wire pair.

- pairs 1/2, 3/6, 4/5, 7/8
- Crossover cable crosses the pairs at pins 1/2 and 3/6, it also crosses pairs 4/5 with 7/8

Fiber Cabling Transmission Concepts

Physical cable

- Core >
- Cladding >
- Buffer >
- Strengthener >
- Outer Jacket

Optical Transmitter

- Shines light into the core

Multimode fiber

- multiple angles (modes) of light waves
- Less expensive
- 10 gigabit over ethernet allows for distance up to 400m

Single mode fiber

- Smaller diameter (around 1/5 of multimode) core
- laser-based transmitter
- single angle
  More expensive SFP/ SFP+ hardware
  Distances up to tens of kilometers

Transmit port on one end of the fiber connects to the receive port on the other end (Tx and Rx)

10Gbps Fiber Standards

- 10GBASE-S/ MM/ 400m
- 10GBASE-LX4/ MM/ 300m
- 10GBASE-LR/ SM/ 10km
- 10GBASE-E/ SM/ 30km

UTP, MM, and SM comparisons

UTP
- low cable cost
- low switch port cost
- 100m Max Distance
- Some susceptibility to interference
- Some risk of copying from cable emissions

Multimode
- Medium cable cost
- Medium switch port cost
- 500m Max Distance

- No susceptibility to interference
- No risk of copying from cable emissions

Single-Mode

- Medium cable cost
- High switch port cost
- 40Km Max Distance
- No susceptibility to interference
- No risk of copying from cable emissions

Sending Data In Ethernet Networks

Ethernet Header (preamble/sfd/Destination/Source/Type/Dataandpad/FCS)

Header

- Preamble
  - □ 7 bites
  - □ Synchronization
- Start Frame Delimiter (SFD)
  - □ 1 Byte
  - □ Signifies next byte begins the Destination MAC Address Field
- Destination MAC Address
  - □ 6 Bytes
- Source MAC Address
  - □ 6 Bytes
- Type
  - □ 2 bytes
  - □ Type of protocol listed in the frame (IPv4 or IPv6)

- Data and Pad
  - 46-1500Bytes
  - padding can be added to meet the minimum length requirement

Trailer

- Frame Check Sequence (FCS)
- Used to determine if the frame experienced transmission errors

Maximum Transmission Unit (MTU)

- Maximum layer 3 packet that can be sent

Ethernet Addressing

- 6 bytes long (48 bits)
- 12 digit hexadecimal
- Cisco switch may list a mac address with periods: 0000.0C12.3456
- Unicast address
  - an address for a single NIC or port

OUI (Organizationally unique indentifier)

- Universally unique manufacturer code
- 24 Bits
- 6 Hex Digits

Vendor Assigned

- 24 Bits
- 6 Hex Digits

Group addresses

Broadcast Address

- Delivered to all devices on the Ethernet LAN.
- FFFF.FFFF.FFFF

Multicast Address

- Copied and forwarded to a subset of devices on the LAN

Identifying Network Layer Protocols with the Ethernet Type Field

The type field identifies which type of layer 3 packet exists within the ethernet frame (IPv6 or IPv4)
Ethertype is the term used for the type field in an ethernet frame

Error Detection with FCS

- Error detection does not mean error recovery
- Ethernet decide whether the frame should be discarded and does not attempt to recover the lost frame.

Sending Ethernet frames with switches and hubs

- Switches allow the use of Full Duplex Logic
- Hubs use half-duplex logic

Sending in Modern Ethernet LANs Using Full Duplex

Half duplex

- must wait to send if it is currently receiving a frame
- cannot send and receive at the same time

Full Duplex

- Does not have to wait before sending,
- send and receive at the same time.

Hubs

- Uses physical link standards instead of data link standards and are considered layer 1 devices

Carrier Sense multiple access with Collision Detection (CSMA/CD)

1. Listen until line is not busy
2. Send frame
3. Listen for a collision while sending if a collision occurs:
    i. Send jamming signal telling all nodes a collision has occurred
    ii. each node waits a random time then tries to send again
    iii. Back to step one

- All links between PCs and switches use full duplex
- A link connected to a hub should be half duplex
- Ethernet Shared media
    - refers to hubs that use CSMA/CD and share bandwidth
- Ethernet point-to-point
    - network built with switches where links work independently of others
    - A frame can be sent on every Point-to-point link in an ethernet at the same time.

3. WANs and IP Routing

Friday, June 11, 2021 10:24 AM

1.0 Network Fundamentals
1.1 Explain the role and function of network components
1.1.a Routers
1.2 Describe characteristics of network topology architectures
1.2.d WAN

Leased-Line WANs

Physical Details of Leased Lines

- predetermined speed
- Full Duplex
- Uses two pairs of wires one for each direction
- Conceptually crossover

Leased Circuit

- Electrical circuit (line) between 2 endpoints

Serial Link (line)

- Bits flow serially
- Routers use serial interfaces

Point to point link (line)

- two points only

T1

- 1.544 Mbps

WAN link

- General term

Private Line

- Data is private

HDLC Data-Link Details of Leased Lines

- Leased line specifies layer 1
- HDLC and PPP are the most popular Layer 2 protocols used on leased lines

HDLC

- less work than ethernet because of point to point leased line
- has an address field, but the destination is implied
- Cant use between cisco and non cisco
- Cisco HDLC type field is proprietary

Comparing HDLC Header Fields to Ethernet

HDLC Header

Flag

- Like preamble, SFD
- 1 byte

Destination address

- 1 byte

Control

- No longer used
- 1 byte

Type

- Type of layer 3 packet inside the frame
- 2 bytes

Data

FCS

- Error detection
- 2 bytes

How Router Use a WAN Data Link

How routers use HDLC when sending data

- LAN1 802.3header/IP Packet/ 802.3trailer >
- HDLC HDLCheader/IP Packet/ HDLC Trailer >
- LAN2 802.3header/Ippacket/802.3trailer >

Leased line negatives

- Higher cost and
- long install times
- Slow speeds

Ethernet as a WAN technology

Customer Router

  - CPE

Service provider

  - point of Presence (PoP)
    - Where the fiber connects at the provider

Common ethernet WAN names

  - Ethernet WAN
  - Ethernet Line Service (E-Line)
  - Ethernet emulation
  - Ethernet over MPLS (EoMPLS) (Multi protocol label switching) A technology used to create ethernet service for a customer.
    - Acts like simple ethernet link between two routers

How Routers Route IP Packets Using Ethernet Emulation

EoMPLS WAN (Provider network simulating an ethernet link)

  - 802.3 header and trailer

IP Routing

1. Use FCS field to ensure that the frame had no errors; if errors occurred, discard the frame.

2. Discard the old data-link header and trailer, leaving the IP packet.

3. Compare the IP packet's destination IP address to the routing table, and find the route that best matches the destination address. This route identifies the outgoing interface of the router and possibly the next-hop router IP address.

4. Encapsulate the IP packet inside a new data-link header and trailer, appropriate for the outgoing interface, and forward the frame

The IP Header (20 bytes)

- Version, Length, DS Field, Packet Length (4 bytes)
- Identification, Flags, Fragment Offset (4 bytes)
- Time to Live, Protocol, Header Checksum (4 bytes)
- Source IP (4 bytes)
- Destination IP (4 bytes)

IP Routing Protocols

1. add route for each directly connected subnet
2. tell neighbors about routes in routing table
3. add new routes learned to routing table, with next hop as the router the address was learned from

ARP

- Ethernet broadcast arp request >

    - Sender IP, sender MAC, Target IP, target MAC ??
- < Ethernet unicast ARP reply
    - Target IP, Target MAC, Sender IP, sender MAC

arp -a

- to see arp cache on most operating systems

4. CLI

Thursday, June 17, 2021 12:53 PM

Reload

- Tells the system to reboot IOS

Keyboard Shortcuts

up arrow or **Ctrl+P**
- Recently used (Previous)

Down arrow or **Ctrl+N**
- Go back up from the above command (next)

Left arrow or **Ctrl+B**
- Move cursor (back)

Right Arrow or Ctrl+F
- Move cursor (forward)

Back Space
- Delete

Debug

- Tells user details about the operation of the switch

Navigation

End or Ctrl+Z
- Global Config > Enable Mode

Exit
- Line or VLAN modes > Global config

Memory

RAM
- Stores Running config

Flash Memory
- Chip or removable memory
- Stores Cisco IOS images
- Default IOS location for booting
- Store backup config files

ROM
- Stores Bootstrap

NVRAM
- stores initial or startup config

5. Switching

Friday, June 18, 2021 7:07 AM

1.0 Network Fundamentals
1.1 Explain the role and function of network components
1.1.b L2 and L3 Switches
1.13 Describe switching concepts
1.13.a MAC learning and aging
1.13.b Frame switching
1.13.c Frame flooding
1.13.d MAC address table
2.0 Network Access
2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations

Overview of Switching Logic

- Forward or filter frame based on destination MAC Address
- Examine source MAC address of each frame received

Learning MAC Addresses

- If a frame enters the switch and the source MAC address is not in the MAC address table, the switch creates an entry in the table
- when there is no matching entry in the table, switches forward the frame out all interfaces (except the incoming interface) (Flooding)

STP

- either a blocking state or a forwarding state.
- Blocking
  - interface cannot forward or receive data frames
- forwarding
  - interface can send and receive data frames.

LAN Switching Summary

Forward Frames based on destination MAC address

- If the destination MAC address is a broadcast, multicast, or unknown destination unicast (a unicast not listed in the MAC table), the switch floods the frame.
- If the destination MAC address is a known unicast address (a unicast address found in the MAC table):
  - the switch forwards the frame out the outgoing interface.
  - If the outgoing interface is the same as the interface in which the frame was received, the switch filters the frame

learning MAC address table entries:

- examine the source MAC address on each frame received and note the interface from which the frame was received.
- If it is not already in the table, add the MAC address and interface it was learned on.

Verifying and Analyzing Ethernet Switching

- interfaces are enabled by default
- 10/100 and 10/100/1000 interfaces use autonegotiation by default.

Demonstrating MAC Learning

#show mac address-table
- View mac address table

#show mac address-table dynamic
- Show only dynamically learned MAC addresses

#show interfaces status
- status of all interfaces (connected or disconnected)

#show interfaces f0/1 status
- interface status of f0/1

#show interfaces f0/1
- Displays detailed set of messages about the interface

#show interfaces f0/1 counters
- Lists the number of unicast, multicast, and broadcast frames (inbound and outbound), and total byte count for those frames

#show mac address-table dynamic address 0200.1111.1111
- Shows MAC entry for a single MAC address

#show mac address-table dynamic interface fastEthernet 0/1
- Shows MAC entries for a single interface

Quick Commands

MAC Addresses

```
#show mac address-table
#show mac address-table dynamic
#show interfaces status
#show interfaces f0/1 status
#show interfaces f0/1
show interfaces f0/1 counters
#show mac address-table dynamic address 0200.1111.1111
#show mac address-table dynamic interface fastEthernet 0/1
#show mac address-table dynamic vlan 1
```

Managing MAC tables

```
#show mac address-table aging-time
#show mac address-table count
#(en)clear mac address-table dynamic
#(en)clear mac address-table dynamic vlan 1
#(en)clear mac address-table dynamic interface fa0/1
#(en)clear mac address-table dynamic address 3d44.2aab.12c3
```

#show mac address-table dynamic vlan 1

- Shows mac entries for vlan 1

Managing the MAC Address Table (Aging, Clearing)

The switch will remove (time out) the entries due to:

- age
- table filling
- using a command

aging out MAC table entries,

- default of 300 seconds

if an entry already exists

- inactivity timer goes back to 0 for that entry

aging time

- can be configured to a different time
  - globally
  - per-VLAN using the **mac address-table aging-time** *time-in-seconds* **[vlan** *vlan-number***]** global configuration command.

#show mac address-table aging-time

- Shows age time settings for mac entries

#show mac address-table count

- Shows how many mac addresses in the table and how much address space is available

if the table fills,

- Oldest entries are removed

content-addressable memory (CAM),

- a physical memory that has great table lookup capabilities.
- Used for MAC Address tables

#(en)clear mac address-table dynamic

- remove dynamic entries from the mac address table

#(en)clear mac address-table dynamic vlan 1

#(en)clear mac address-table dynamic interface fa0/1

#(en)clear mac address-table dynamic address 3d44.2aab.12c3

6. Management

Thursday, June 24, 2021 9:28 AM

1.0 Network Fundamentals
1.6 Configure and verify IPv4 addressing and subnetting
4.0 IP Services
4.6 Configure and verify DHCP client and relay
4.8 Configure network devices for remote access using SSH
5.0 Security Fundamentals
5.3 Configure device access control using local passwords

data plane

- work a switch does to forward frames generated by the devices connected to the switch

control plane

- configuration and processes that control and change the choices made by the switch's data plane

management plane

- deals with managing the device itself, rather than controlling what the device is doing

SSH

crypto key generate rsa modulus *modulus-value*

- (Use at least a 768-bit key to support SSH version 2.)

show ip ssh

- lists status information about the SSH server

show ssh

- lists information about each SSH client currently connected into the switch

Switch DHCP

ip address dhcp

Show dhcp lease

show interfaces vlan 1

show ip default-gateway

show history

- lists the commands currently held in the history buffer.

terminal history size *x*

- allows a single user to set the size of their history buffer
- just for this one login session

history size x

- console or vty line configuration mode
- sets the default number of commands saved in the history buffer for the users of the console or vty lines

Logging and domain lookup

no logging console

logging console

exec-timeout minutes seconds

- line subcommand
- enables you to set the length of that inactivity timer.
- In the lab (but not in production), you might want to use the special value of 0 minutes and 0 seconds meaning "never time out."

Quick Commands

SSH

```
#crypto key generate rsa modulus (modulus value)
#show ip ssh
#show ssh
```

Switch DHCP

```
#ip address dhcp
#show dhcp lease
#show interfaces vlan 1
#show ip default-gateway
```

History

```
#show history
#terminal history size x
#history size x
```

Logging and Domain Lookup

```
#no logging console
#no ip domain-lookup
#exec timeout (minutes)
```

7. Switch Interfaces

Wednesday, June 30, 2021 8:01 AM

1.0 Network Fundamentals
1.1 Explain the role and function of network components
1.1.b L2 and L3 switches
1.4 Describe switching concepts

Configuring Speed, Duplex, and Description

- autonegotiate
    - What speed to use
    - enabled by default

duplex {auto | full | half} and speed {auto | 10 | 100 | 1000}

- configure the speed and duplex settings

(config-int) # description *text*

- add a text description to the interface

show interfaces status

- lists port #, Name, status, vlan, duplex, speed, and type

a-full and a-100

a- means that the listed speed and duplex values were autonegotiated.

Autonegotiation

IEEE autonegotiation (IEEE standard 802.3u)

- each node states what it can do, and
- then each node picks the best options that both nodes support:
    - the fastest speed and the best duplex setting, with full duplex being better than half duplex.
- disable autonegotiation
    - Configure both the speed and duplex on a switch interface
- when a node tries to use autonegotiation but hears nothing from the device.

Speed: Use your slowest supported speed (often 10 Mbps).
Duplex: If your speed = 10 or 100, use half duplex; otherwise, use full duplex.

Cisco switches can actually sense the speed used by other nodes, even without IEEE autonegotiation.

- Cisco switches use this slightly different logic to choose the speed when autonegotiation fails:
    - Speed: Sense the speed (without using autonegotiation), but if that fails, use the IEEE default (slowest supported speed, often 10 Mbps).
    - Duplex: Use the IEEE defaults: If speed = 10 or 100, use half duplex; otherwise, use full duplex.
- Ethernet interfaces using speeds faster than 1 Gbps always use full duplex.
- hubs do not react to autonegotiation messages

show interfaces and **show interfaces description**

Shutdown command is configured

- Line status = administratively down
- Protocol status = down
- Interface status = disabled

Cable, speed mismatch, neighbor device is off**, shutdown,** or err-disabled

- Line status = down
- Protocol status = down
- Interface status = notconnect

Not expected on LAN switch physical interfaces

- Line status = up
- Protocol status = down
- Interface status = notconnect

Port security has disabled the interface

- Line status = down
- Protocol status = down (err-disabled)
- Interface status = err-disabled

the interface is working

- Line status = up
- Protocol status = up
- Interface status = connected

show interfaces fa0/13 (without the status option)

- lists the speed and duplex for interface Fast Ethernet 0/13
- with nothing implying that the values were learned through autonegotiation.

Quick Commands

Speed/ duplex

#duplex auto/full/half
#speed auto/10/100/1000

Description

#description (text)

Interface

#show interfaces status
#show interfaces fa0/3

speed manually set 10 Mbps on one switch and 100 Mbps on the other

- both switches would list the port in a down/down or notconnect state

if the duplex settings do not match

- the switch interface will still be in a connected (up/up) or connected state.

How to identify duplex mismatch problems,

- check the duplex setting on each end of the link to see if the values mismatch.
- watch for incrementing collision and late collision counters

Common Layer 1 problems

- receiving device might receive a frame whose bits have changed values.
- These frames do not pass the error detection logic as implemented in the FCS field in the Ethernet trailer,
- The receiving device discards the frame and counts it as some kind of input error.
- Cisco switches list this error as a CRC error

Runts:

- Frames that did not meet the minimum frame size requirement
  - (64 bytes, including the 18-byte destination MAC, source MAC, type, and FCS).
- Can be caused by collisions.

Giants:

- Frames that exceed the maximum frame size requirement
  - (1518 bytes, including the 18-byte destination MAC, source MAC, type, and FCS)

Input Errors:

- A total of many counters, including runts, giants, no buffer, CRC, frame, overrun, and ignored counts.

CRC:

- Received frames that did not pass the FCS math
- can be caused by collisions

Frame:

- Received frames that have an illegal format
  - (like ending with a partial byte)
- can be caused by collisions.

Packets Output:

- Total number of packets (frames) forwarded out the interface.

Output Errors:

- Total number of packets (frames) that the switch port tried to transmit, but for which some problem occurred.

Collisions:

- Counter of all collisions that occur when the interface is transmitting a frame

Late Collisions:

- The subset of all collisions that happen after the 64th byte
  - (In a properly working Ethernet LAN, collisions should occur within the first 64 bytes
- Often point to a duplex mismatch

Collisions occur as a normal part of the half-duplex logic imposed by CSMA/CD

a switch interface with an increasing collisions counter might not even have a problem.

- if the CRC errors grow, but the collisions counters do not, the problem might simply be interference on the cable.

8. VLANS

Friday, July 2, 2021 2:50 PM

1.0 Network Fundamentals
1.13 Describe switching concepts
1.13.a MAC learning and aging
1.13.b Frame switching
1.13.c Frame flooding
1.13.d MAC address table
2.0 Network Access
2.1 Configure and verify VLANs (normal range) spanning multiple switches
2.1.a Access ports (data and voice)2.1.b Default VLAN
2.1.c Connectivity
2.2 Configure and verify interswitch connectivity
2.2.a Trunk ports
2.2.b 802.1Q
2.2.c Native VLAN

Virtual LAN Concepts

reasons for choosing to create smaller broadcast domains (VLANs):

- reduce CPU overhead on each device
- reduce security risks
- different security policies per VLAN
- more flexible designs that
    - group users by department, or by groups that work together, instead of by physical location
- solve problems more quickly
    - failure domain for many problems is the same set of devices as those in the same broadcast domain
- reduce the workload for the Spanning Tree Protocol (STP)
    - by limiting a VLAN to a single access switch

802.1q and ISL

802.1Q

- inserts a 4-byte 802.1Q VLAN header into the Ethernet header

12-bit VLAN ID field inside the 802.1Q header

- supports a theoretical maximum of 212 (4096) VLANs, but in practice it supports a maximum of 4094.
- Both 802.1Q and ISL use 12 bits to tag the VLAN ID, with two reserved values [0 and 4095].

- 802.1q header includes Type, priority, Flag, Vlan ID

- Cisco switches break the range of VLAN IDs (1–4094) into the normal range and the extended range.

normal-range

- 1 to 1005.
- all switches can use

Extended range

Only some switches can use
1006 to 4094
depends on the configuration of the VLAN Trunking Protocol (VTP)

231852+

- 802.1Q simply does not add an 802.1Q header to frames in the native VLAN

#show vlan brief

VLAN Trunking Protocol (VTP)

vtp mode transparent
vtp mode off

show vtp status

If your switch uses VTP server or client mode

- The server switches can configure VLANs in the standard range only (1–1005).
- The client switches cannot configure VLANs.
- Both servers and clients may be learning new VLANs from other switches and seeing their VLANs deleted by other switches because of VTP.

show running-config

- does not list any vlan commands

- If possible in the lab, switch to disable VTP and ignore VTP for your switch configuration practice until you decide to learn more about VTP for other purposes.

VLAN Trunking Configuration

Dynamic Trunking Protocol (DTP).

- negotiate ISL or 802.1q
- If both switches support both protocols, they use ISL;
    - otherwise, they use the protocol that both support.

switchport trunk encapsulation {dot1q | isl | negotiate}

- configure the type or allow DTP to negotiate the type.

Access

- always access

trunk

- always trunk

dynamic desirable

- initiates negotiation messages and responds to negotiation messages
- Access if other side is access, otherwise trunk

dynamic auto

Quick Commands

VTP

#show vtp status

Trunking

#switchport trunk encapsulation dot1q/isl/negotiate
#switchport mode access/trunk/dynamic desirable/dynamic auto
#switchport trunk allowed vlan
#show interfaces trunk output
#show interfaces trunk
#show interfaces switchport
#switchport trunk native vlan 2

Voice

#show int f0/4 trunk
#switchport voice vlan 13

VLAN

#show vlan brief
#show vlan
#show spanning-tree vlan 2

        - passively waits to receive trunk negotiation messages
        - default setting
        - access if both ends use this
        - trunk if other end is trunk or Dynamic desirable

- On a switch that supports both ISL and 802.1Q, this value would by default list "negotiate," to mean that the type of encapsulation is negotiated.

- Cisco recommends disabling trunk negotiation on most ports for better security

    (config-if) switchport nonegotiate
        Disable DTP

Data and Voice VLAN Concepts

switchport voice *vlan 11*
  - can configure on the same access port that has a normal vlan assigned
  - CDP must be enabled*

- Voice Data is tagged with 802.1Q header

show interfaces *FastEthernet 0/4* **switchport**
  - see the voice vlan
  - administrative and operational mode
  - access mode vlan

show interfaces trunk
show interfaces *f0/4* **trunk**

- vlans allowed on trunk
  - 1-4094
  - minus vlans removed by the **switchport trunk allowed** command

- vlans allowed and active in management domain
  - the first list minus vlans that are not configured
  - minus vlans that are **shutdown**

- vlans in spanning tree forwarding state and not (VTP) pruned
  - minus vlans that are in a STP blocking state
  - minus vlans that are VTP pruned

- **Show interfaces trunk** will not show the voice VLAN as a trunk, it will only show it if you specify the interface.

Troubleshooting VLANS and VLAN trunks

Confirm that all VLANs are both defined and active.
show vlan
Show vlan brief

Check the allowed VLAN lists on both ends of each trunk

show interfaces *interface-id* **trunk**
  - lists information about currently operational trunks

#switchport trunk allowed vlan

Show vlan
  - (does the vlan exist and is it active?

- Has the vlan been vtp pruned?

- Is the vlan in an STP forwarding state?
  #show spanning-tree *vlan 2*

Check for incorrect trunk configuration settings that result in one switch operating as a trunk, with the neighboring switch not operating as a trunk.

#show interfaces trunk
#show interfaces switchport.
  - check administrative and operational modes

- The trunk is in an STP forwarding state in that VLAN (as also seen in the **show spanning-tree vlan** *vlan-id* command).
  #switchport trunk allowed vlan
- DTP on one switch but not the other

Check the native VLAN settings on both ends

- Native vlan must match on both switches.
  #switchport trunk native vlan *2*
- vlan hopping
  a frame being sent in one vlan but then being believed to be in a different vlan

9. Spanning Tree Protocol Concepts

Monday, July 26, 2021 11:27 AM

2.0 Network Access
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
2.5.a Root port, root bridge (primary/secondary), and other port names
2.5.b Port states (forwarding/blocking)
2.5.c PortFast benefits

- RSTP is most common now
- Cisco defaults to RSTP

MAC table instability

- The switches MAC address tables keep changing because frames with the same source MAC arrive on different ports.

Broadcast storms

- forwarding of a frame repeatedly on the same links

Multiple frame transmission

- side effect of looping frames
- Multiple copies are delivered to a host, confusing the host.

What Spanning Tree Does

- blocking state
    - interfaces does not process any frames
    - except STP/RSTP messages and some other overhead messages

  STP Convergence

    - switches collectively realize that something has changed in the LAN topology
    - determine whether they need to change which ports block and which port forward

How Spanning Tree works

three criteria to choose whether to put and interface in forwarding state:

elect a root switch.

- STP puts all working interfaces on the root switch in forwarding state

nonroot switches

- select the port with the least administrative cost (root port)
    - cost between itself and the root switch (root cost) (root cost path)
    - root port (RP) gets put in a forwarding state
- The switch with the lowest root cost, as compared with the other switches attached to the same link, is placed in forwarding state.

        - That switch is the designated switch, and that switch's interface, attached to that segment, is called the designated port (DP)

STP States

All the root switches ports

- forwarding
- root switch is always the designated switch

All nonroot switch's root ports

- forwarding
- port with the least cost to the root switch (lowest root cost)

Each LAN's designated port

- forwarding
- switch forwarding the Hello on to the segment with the lowest root cost is the designated switch for the segment

All other working ports

- blocking
- Not used for forwarding frames
- frames received on these interfaces to not forward

The STP Bridge ID and Hello BPDU

- bridge ID (BID)
    - 8-byte value unique to each switch.
    - 2-byte priority field
    - 6-byte system ID
        - based on a universal (burned-in) MAC address

- bridge protocol data units (BPDU)
    - configuration BPDUs, which switches
    - used to exchange information with each other (switches) The most common BPDU, called a
    - hello BPDU,
        - sending switch's BID
            - switches can tell which switch sent which Hello BPDU
        - Root Bridge ID
            - BID the sender currently believes to be the root switch
        - Sender's root cost
            - STP cost between this switch and current root
        - Timer values on the root switch
            - Hello timer, MaxAge timer, and forward delay timer

Electing the Root Switch

- based on the BIDs in the BPDUs.
- root switch is the switch with the lowest numeric value for the BID.
- Because the two-part BID starts with the priority value,
    - essentially the switch with the lowest priority becomes the root.
- If a tie occurs based on the priority portion of the BID,
    - the switch with the lowest MAC address portion of the BID is the root.

    - Mac addresses are the second part of the BID

- all switches claim to be the root by sending Hello BPDUs listing their own BID as the root BID.
- If a switch hears a Hello that lists a better (lower) BID
    - that switch stops advertising itself as root and starts forwarding the superior Hello.
        - The Hello sent by the better switch lists the better switch's BID as the root.

    - superior hello (better hello)
        - the listed root's BID is better (numerically lower),
    - Inferior hello (worse Hello), meaning that
        - the listed root's BID is not as good (numerically higher)

- each nonroot switch chooses its one and only root port. A switch's RP is its interface through which it has the least STP/RSTP cost to reach the root switch (least root cost).

Choosing Each Switch's Root Port

- each nonroot switch chooses its one and only root port.
    - its interface through which it has the least STP/RSTP cost to reach the root switch (least root cost).

- The STP/RSTP port cost is simply an integer value assigned to each interface, per VLAN

- The switches also look at their neighbor's root cost, as announced in Hello BPDUs received from each neighbor.

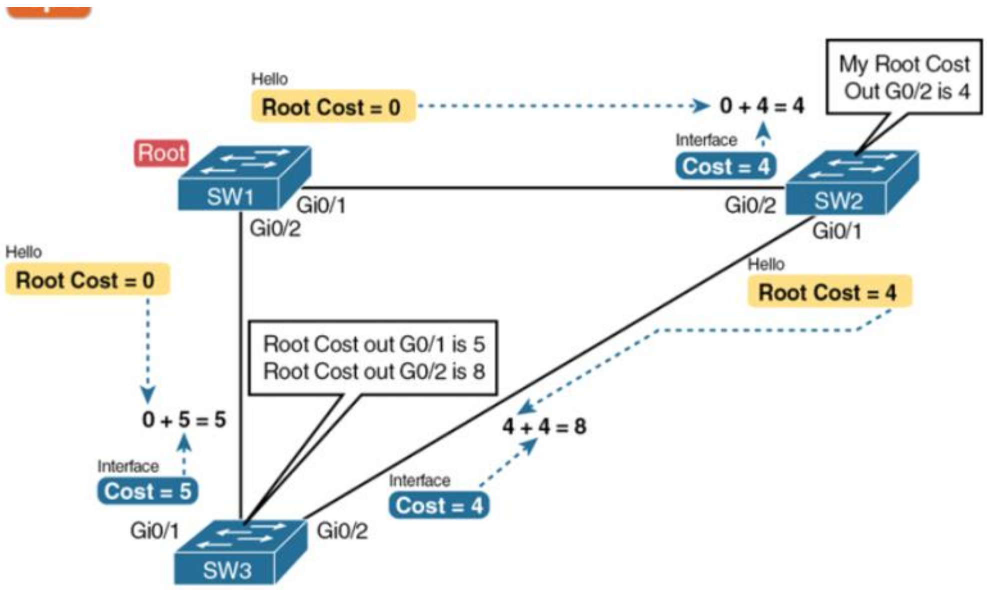


Figure 9-6 *How STP/RSTP Actually Calculates the Cost from SW3 to the Root*

    - SW3 calculates its cost to reach the root over the two possible paths by adding the advertised cost (in Hello messages) to the interface costs listed in the figure.

    - The root switch sends Hellos, with a listed root cost of 0. The idea is that the root's cost to reach itself is 0.

    - Each switch places its root port into a forwarding state.

- tiebreaker to use in case the best root cost ties for two or more paths.
    - Choose based on the lowest neighbor bridge ID.
    - Choose based on the lowest neighbor port priority.
    - Choose based on the lowest neighbor internal port number.

Choosing the Designated Port on each LAN Segment

- final step to choose the STP/RSTP topology is to choose the designated port on each LAN segment.
- The designated port (DP) on each LAN segment is the switch port that advertises the lowest-cost Hello onto a LAN segment.
- When a nonroot switch forwards a Hello, the nonroot switch sets the root cost field in the Hello to that switch's cost to reach the root. In effect, the switch with the lower cost to reach the root, among all switches connected to a segment, becomes the DP on that segment.

- All DPs are placed into a forwarding state

  Two additional tiebreakers are needed in some cases
    - these would be unlikely today.
    - A single switch can connect two or more interfaces to the same collision domain by connecting to a hub.
        - In that case, the one switch hears its own BPDUs.
        - So, if a switch ties with itself, two additional tiebreakers are used:
            - the lowest interface STP/RSTP priority and,
            - if that ties, the lowest internal interface number.

- switch ports connected to endpoint devices should become DPs and settle into a forwarding state.

Configuring to influence the STP Topology

- configure the bridge ID and change STP/RSTP port costs.

    - change the BID, the engineer can
        - set the priority used by the switch, while
        - continues to use the universal MAC address as the final 48 bits of the BID.
            - giving a switch the lowest priority value among all switches will cause that switch to win the root election.

    - to favor one link, give the ports on that link a lower cost, or to avoid a link, give the ports a higher cost.

Link Costs

10 Mbps
- 2,000,000
- 100 (old)

100Mbps
- 200,000
- 19 (old)

1gbps

- 20,000
- 4 (old)

10Gbps

- 2000
- 2 (old)

100Gbps

- 200
- N/A (old)

1Tbps

- 20
- N/A (old)

- the cost defaults based on the operating speed of the link, not the maximum speed

- **(config) # spanning-tree pathcost method long**
    - Cisco Catalyst switches can be configured to use the long values as defaults

Details specific to STP

STP Activity When the Network Remains Stable

- An STP root switch sends a new Hello BPDU every 2 seconds by default.
- Each nonroot switch forwards the Hello on all DPs, but only after changing items listed in the Hello.
- (As a result, the Hello flows once over every working link in the LAN.)

- When forwarding the Hello BPDU, each switch sets the root cost to that local switch's calculated root cost. The switch also sets the "sender's bridge ID" field to its own bridge ID. (The root's bridge ID field is not changed.)

Step 1. The root creates and sends a Hello BPDU, with a root cost of 0, out all its working interfaces (those in a forwarding state).

Step 2. The nonroot switches receive the Hello on their root ports. After changing the Hello to list their own BID as the sender's BID and listing that switch's root cost, the switch forwards the Hello out all designated ports.

Step 3. Steps 1 and 2 repeat until something changes.

- When a switch ceases to receive the Hellos, or receives a Hello that lists different details, something has failed, so the switch reacts and starts the process of changing the spanning-tree topology.

STP Timers That Manage STP Convergence

- STP convergence process requires the use of three timers

- All switches use the timers as dictated by the root switch, which the root lists in its periodic Hello BPDU messages.

hello
- 2 seconds by default
- Period between hellos created by the root

MaxAge
- 10 times the hello (20 seconds by default hello)
- How long the switch will go without receiving any hellos before it attempts to change the stp topology

Forward Delay
- 15 seconds
- how long the port stays in listening and learning state

- After MaxAge expires, the switch essentially makes all its STP choices again, based on any Hellos it receives from other switches.

Changing Interface States with STP

Roles, like root port and designated port, relate to how STP analyzes the LAN topology. States, like forwarding and blocking, tell a switch whether to send or receive frames.

When STP converges, a switch chooses new port roles, and the port roles determine the state (forwarding or blocking).

Switches using STP can simply move immediately from forwarding to blocking state, but they must take extra time to transition from blocking state to forwarding state.

when a port that formerly blocked needs to transition to forwarding, the switch first puts the port through two intermediate interface states.

Listening:
- interface does not forward frames.
- switch removes old stale (unused) MAC table entries for which no frames are received from each MAC address during this period.
- These stale MAC table entries could be the cause of the temporary loops.
- Transitory

Learning:
- do not forward frames
- switch begins to learn the MAC addresses of frames received on the interface.
- Transitory

Blocking
- does not forward frames
- does not learn mac addresses
- stable

Forwarding
- learns mac addresses
- forwards frames
- stable

Disabled
- does not forward or learn mac addresses
- stable

blocking > listening, > learning > forwarding.

STP leaves the interface in each interim state for a time equal to the forward delay timer, which defaults to 15 seconds.

a convergence event that causes an interface to change from blocking to forwarding requires 30 seconds to transition from blocking to forwarding.

a switch might have to wait MaxAge seconds (default 20 seconds) before even choosing to move an interface from blocking to forwarding state.

Rapid STP Concepts

- 802.1w
- Sits in 802.1q standards document

Comparing STP and RSTP

- similarities
  - elect the root switch using the same rules and tiebreakers.
  - switches select their root ports with the same rules.
  - elect designated ports on each LAN segment with the same rules and tiebreakers.
  - place each port in either forwarding or blocking state
    - (RSTP calls the blocking state the discarding state.)

- they can both be used in the same network.

- RSTP improves network convergence when topology changes occur, usually converging within a few seconds (or in slow conditions, in about 10 seconds).

RSTP defines more cases in which the switch can avoid waiting for a timer to expire, such as the following:

- a switch can replace its root port, without any waiting to reach a forwarding state (in some conditions).
- replace a designated port, without any waiting to reach a forwarding state (in some conditions).
- lowers waiting times for cases in which RSTP must wait for a timer.
- MaxAge is only 3 times the hello
- uses the term alternate port to refer to a switch's other ports that could be used as the root port if the root port ever fails.
- The backup port concept provides a backup port on the local switch for a designated port.
  - backup ports apply only to designs that use hubs, so they are unlikely to be useful today.)

RSTP Port roles

Root Port

    - Nonroot switch's port that has the best path to the root

Alternate port
    - Replaces the root port when the root port fails

Designated port
    - port designated to forward onto a collision domain

Backup Port
    - Replaces designated port when designated port fails

Disabled ports
    - administratively disabled

- each switch independently generates its own Hellos.
- allows for queries between neighbors
    - (rather than waiting on timers to expire to learn new information)

RSTP and the Alternate (Root) Port Role

alternate port
- both the RP and the alternate port must receive Hellos that identify the same root switch.

the switch changes the former root port's role and state:
- the role from root port to a disabled port, and
- the state from forwarding to discarding
- without waiting on any timers, the switch changes roles and state for the alternate port:
    - its role changes to be the root port, with a forwarding state.

- the new root port also does not need to spend time in other states, such as learning state, instead moving immediately to forwarding state.

Step 1. The link between SW1 and SW3 fails, so SW3's current root port (Gi0/1) fails.
Step 2. SW3 and SW2 exchange RSTP messages to confirm that SW3 will now transition its former alternate port (Gi0/2) to be the root port. This action causes SW2 to flush the required MAC table entries.
Step 3. SW3 transitions Gi0/1 to the disabled role and Gi0/2 to the root port role.
Step 4. SW3 transitions Gi0/2 to a forwarding state immediately, without using learning state, because this is one case in which RSTP knows the transition will not create a loop.

RSTP States and Processes

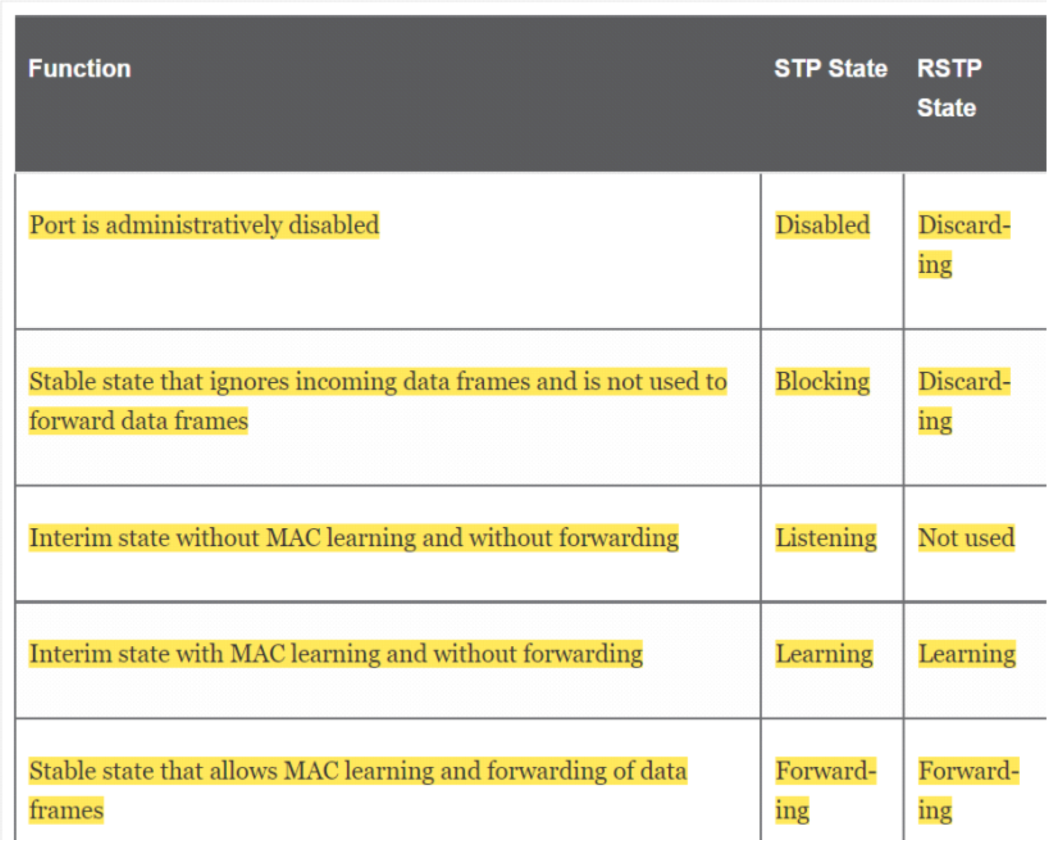
- RSTP keeps both the learning and forwarding states as compared with STP, for the same purposes

- RSTP does not even define a listening state,

- RSTP renames the blocking state to the discarding state and redefines its use slightly.

- RSTP uses the discarding state for what STP defines as two states: disabled state and blocking state.

Table 9-10 Port States Compared: STP and RSTP



Function	STP State	RSTP State
Port is administratively disabled	Disabled	Discarding
Stable state that ignores incoming data frames and is not used to forward data frames	Blocking	Discarding
Interim state without MAC learning and without forwarding	Listening	Not used
Interim state with MAC learning and without forwarding	Learning	Learning
Stable state that allows MAC learning and forwarding of data frames	Forwarding	Forwarding

- RSTP switches tell each other (using messages) that the topology has changed.
- Those messages also direct neighboring switches to flush the contents of their MAC tables in a way that removes all the potentially loop-causing entries, without a wait.
- As a result, RSTP creates more scenarios in which a formerly discarding port can immediately transition to a forwarding state, without waiting, and without using the learning state, as shown in the example in Figure 9-9.

- RSTP backup port role creates a way for RSTP to quickly replace a switch's designated port on some LAN.

RSTP Port Types

- several links between two switches. RSTP considers these links to be point-to-point links and the ports connected to them to be point-to-point ports

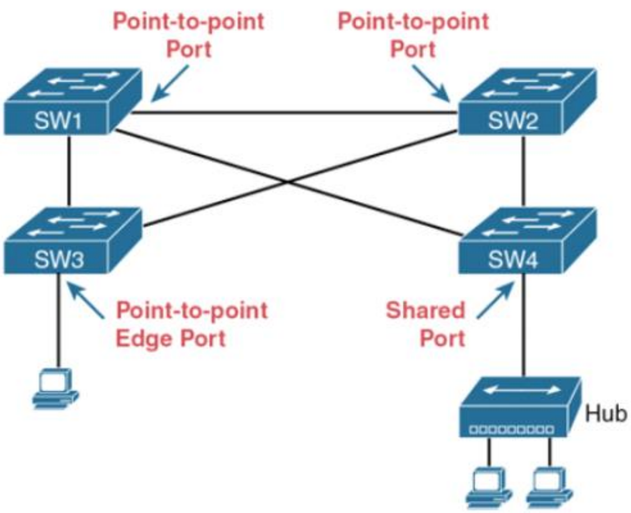


Figure 9-11 *RSTP Link Types*

- Ports that instead connect to a single endpoint device at the edge of the network, like a PC or server, are called point-to-point edge ports, or simply edge ports.

- "shared" to describe ports connected to a hub.

  - hubs also force the attached switch port to use half-duplex logic. RSTP assumes that all half-duplex ports may be connected to hubs, treating ports that use half duplex as shared ports.
  - RSTP converges more slowly on shared ports as compared to all point-to-point ports.

Optional STP Features

Etherchannel

- The switches treat the EtherChannel as a single interface with regard to STP.

  Layer 2 EtherChannels combine links that switches use as switch ports, with the switches using Layer 2 switching logic to forward and receive Ethernet frames over the EtherChannels. Layer 3 EtherChannels also combine links, but the switches use Layer 3 routing logic to forward packets over the EtherChannels.

PortFast

PortFast

- allows a switch to immediately transition from blocking to forwarding, bypassing listening and learning states.

- only ports on which you can safely enable PortFast are ports on which you know that no bridges, switches, or other STP-speaking devices are connected.

- Cisco switches enable RSTP point-to-point edge ports by enabling PortFast on the port.

BPDU Guard

- An attacker could connect a switch to one of these ports, one with a low STP/RSTP priority value, and become the root switch. The new STP/RSTP topology could have worse performance than the desired topology.

- The attacker could plug into multiple ports, into multiple switches, become root, and actually forward much of the traffic in the LAN. Without the networking staff realizing it, the attacker could use a LAN analyzer to copy large numbers of data frames sent through the LAN.

- Users could innocently harm the LAN when they buy and connect an inexpensive consumer LAN switch (one that does not use STP/RSTP). Such a switch, without any STP/RSTP function, would not choose to block any ports and could cause a loop.

- Cisco BPDU Guard feature helps defeat these kinds of problems by disabling a port if any BPDUs are received on the port. So, this feature is particularly useful on ports that should be used only as an access port and never connected to another switch.

- In addition, the BPDU Guard feature helps prevent problems with PortFast. PortFast should be enabled only on access ports that connect to user devices, not to other LAN switches. Using BPDU Guard on these same ports makes sense because if another switch connects to such a port, the local switch can disable the port before a loop is created.

10. RSTP and EtherChannel

Tuesday, July 27, 2021 12:04 PM

2.0 Network Access
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
2.5.a Root port, root bridge (primary/secondary), and other port names
2.5.b Port states (forwarding/blocking)
2.5.c PortFast benefits

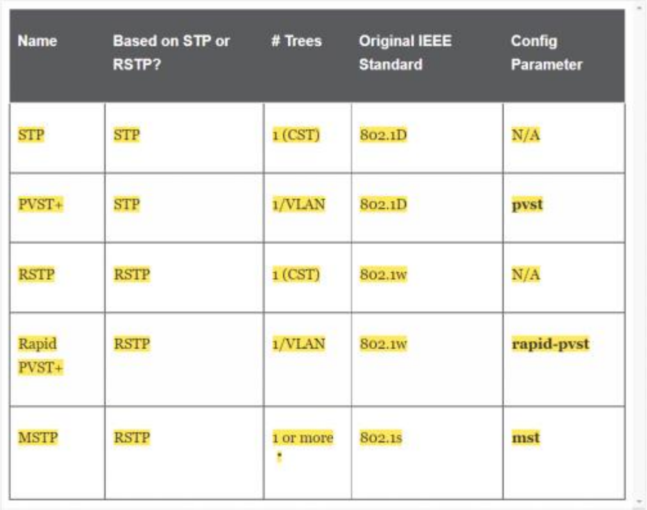
Most network engineers make the distribution layer switches be the root.

STP Modes and Standards

Three options to configure on the spanning-tree mode command, which tells the switch which type of STP to use

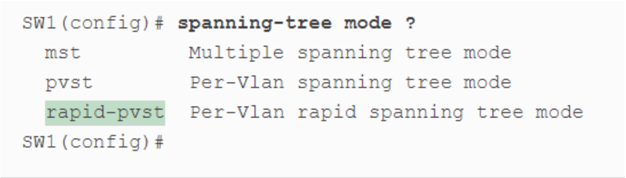
the switches do not support STP or RSTP with the single tree (CST). They can use either the Cisco-proprietary and STP-based PVST+, Cisco-proprietary and RSTP-based RPVST+, or the IEEE standard MSTP.

Table 10-2 STP Standards and Configuration Options



Name	Based on STP or RSTP?	# Trees	Original IEEE Standard	Config Parameter
STP	STP	1 (CST)	802.1D	N/A
PVST+	STP	1/VLAN	802.1D	**pvst**
RSTP	RSTP	1 (CST)	802.1w	N/A
Rapid PVST+	RSTP	1/VLAN	802.1w	**rapid-pvst**
MSTP	RSTP	1 or more *	802.1s	**mst**

MSTP allows the definition of as many instances (multiple spanning tree instances, or MSTIs) as chosen by the network designer but does not require one per VLAN.



```
SW1(config)# spanning-tree mode ?
  mst          Multiple spanning tree mode
  pvst         Per-Vlan spanning tree mode
  rapid-pvst   Per-Vlan rapid spanning tree mode
SW1(config)#
```

STP and MSTP now exist as part of the 802.1Q standard, which defines VLANs and VLAN trunking.

The revised rules divide the original priority field into two separate fields, as shown in Figure 10-4: a 4-bit priority field and a 12-bit subfield called the system ID extension (which represents the VLAN ID

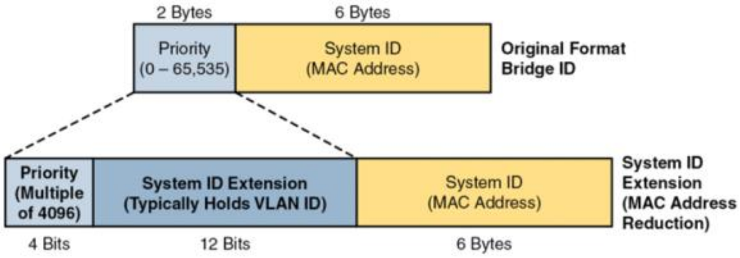

2 Bytes
6 Bytes
Priority (0 – 65,535)
System ID (MAC Address)
Original Format Bridge ID
Priority (Multiple of 4096)
System ID Extension (Typically Holds VLAN ID)
System ID (MAC Address)
System ID Extension (MAC Address Reduction)
4 Bits
12 Bits
6 Bytes

Figure 10-4 *STP System ID Extension*

Cisco switches let you configure the BID, but only the priority part.

The switch fills in its universal (burned-in) MAC address as the system ID. It also plugs in the VLAN ID of a VLAN in the 12-bit system ID extension field; you cannot change that behavior either. The only part configurable by the network engineer is the 4-bit priority field.

the configuration command (spanning-tree vlan vlan-id priority x) requires a decimal number between 0 and 65,535. But not just any number in that range will suffice; it must be a multiple of 4096, as emphasized in the

Command Guide

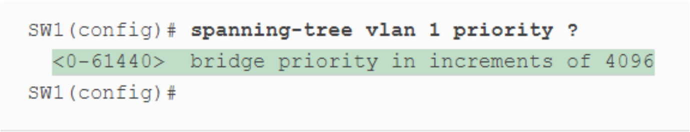
RSTP

#spanning-tree vlan vlan-id priority x
#spanning-tree vlan x root primary
#spanning-tree vlan x root secondary
#show spanning-tree vlan 9

EtherChannel

(int)#channel-group 1 mode on
#show etherchannel 1 summary
#show etherchannel summary
#show etherchannel 1 port-channel
#show etherchannel load-balance
#channel-group 1 mode desirable/auto (PAgP)
#channel-group 1 mode active/passive (LACP)
#port-channel load-balance src-dst-mac

help text shown in Example 10-2.



```
SW1(config)# spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096
SW1(config)#
```

#spanning-tree vlan x root primary (on the switch that should be primary)

#spanning-tree vlan x root secondary (on the switch that should be secondary)

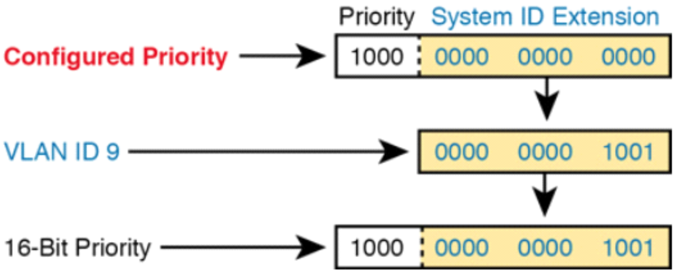
These two commands cause the switch to make a choice of priority value but then store the chosen priority value in the spanning-tree vlan x priority value command. The command with root primary or root secondary does not appear in the configuration. When configuring root primary, the switch looks at the priority of the current root switch and chooses either (a) 24,576 or (b) 4096 less than the current root's priority (if the current root's priority is 24,576 or less) to the configuration instead. When configuring, root secondary always results in that switch using a priority of 28,672, with the assumption that the value will be less than other switches that use the default of 32,768, and higher than any switch configured as root primary.

How Switches Use the Priority and System ID Extension

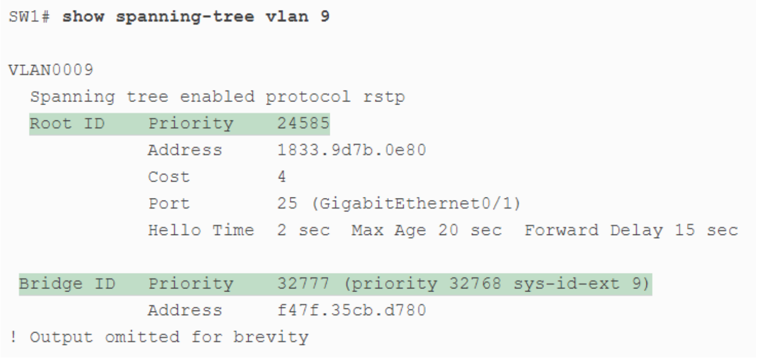
Cisco Catalyst switches configure the priority value using a number that represents a 16-bit value; however, the system ID extension exists as the low-order 12 bits of that same number.

When the switch builds its BID to use for RSTP in a VLAN, it must combine the configured priority with the VLAN ID of that VLAN.

the configured priority results in a 16-bit priority that always ends with 12 binary 0s.



Root Switch: 24,576 (priority) + 9 (VLAN ID) = 24585
Local Switch: 32,768 (priority) + 9 (VLAN ID) = 32777



```
SW1# show spanning-tree vlan 9

VLAN0009
  Spanning tree enabled protocol rstp
  Root ID    Priority    24585
             Address     1833.9d7b.0e80
             Cost        4
             Port        25 (GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID   Priority    32777  (priority 32768 sys-id-ext 9)
             Address     f47f.35cb.d780
! Output omitted for brevity
```

RSTP Methods to Support Multiple Spanning Trees

RSTP creates one tree—the Common Spanning Tree (CST)—while RPVST+ creates one tree for each and every VLAN.

RSTP sends one set of RSTP messages (BPDUs) in the network, no matter the number of VLANs, while RPVST+ sends one set of messages per VLAN.

RSTP and RPVST+ use different destination MAC addresses: RSTP with multicast address 0180.C200.0000 (an address defined in the IEEE standard), and RPVST+ with multicast address 0100.0CCC.CCCD (an address chosen by Cisco).

When transmitting messages on VLAN trunks, RSTP sends the messages in the native VLAN with no VLAN header/tag. RPVST+ sends each VLAN's messages inside that VLAN—for instance, BPDUs about VLAN 9 have an 802.1Q header that lists VLAN 9.

RPVST+ adds an extra type-length value (TLV) to the BPDU that identifies the VLAN ID, while RSTP does not (because it does not need to, as RSTP ignores VLANs.)

Both view the 16-bit priority as having a 12-bit System ID Extension, with RSTP setting the value to 0000.0000.0000, meaning "no VLAN," while RPVST+ uses the VLAN ID.

Other RSTP Configuration Options

Switch Priority: The global command spanning-tree vlan x priority y lets an engineer set the switch's priority in that VLAN.

Primary and Secondary Root Switches: The global command spanning-tree vlan x root primary | secondary also lets you set the priority, but the switch decides on a value to make that switch likely to be the primary root switch (the root) or the secondary root switch (the switch that becomes root if the primary fails).

Port Costs: The interface subcommand spanning-tree [vlan x] cost y lets an engineer set the switch's STP/RSTP cost on that port, either for all VLANs or for a specific VLAN on that port. Changing those costs then changes the root cost for some switches, which impacts the choice of root ports and designated ports.

Configuring Layer 2 Etherchannel

Configuring a Manual Layer 2 EtherChannel

simply add the correct channel-group configuration command to each physical interface, on each switch, all with the on keyword, and all with the same number. The on keyword tells the switches to place a physical interface into an EtherChannel, and the number identifies the PortChannel interface number that the interface should be a part of.

three terms as synonyms: EtherChannel, PortChannel, and Channel-group. Oddly, IOS uses the channel-group configuration command, but then to display its status, IOS uses the show etherchannel command. Then the output of this show command refers to neither an "EtherChannel" nor a "Channel-group," instead using the term "PortChannel." So, pay close attention to these three terms in the example.

Step 1. Add the channel-group number mode on command in interface configuration mode under each physical interface that should be in the channel to add it to the channel.

Step 2. Use the same number for all commands on the same switch, but the channel-group number on the neighboring switch can differ.

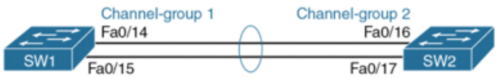
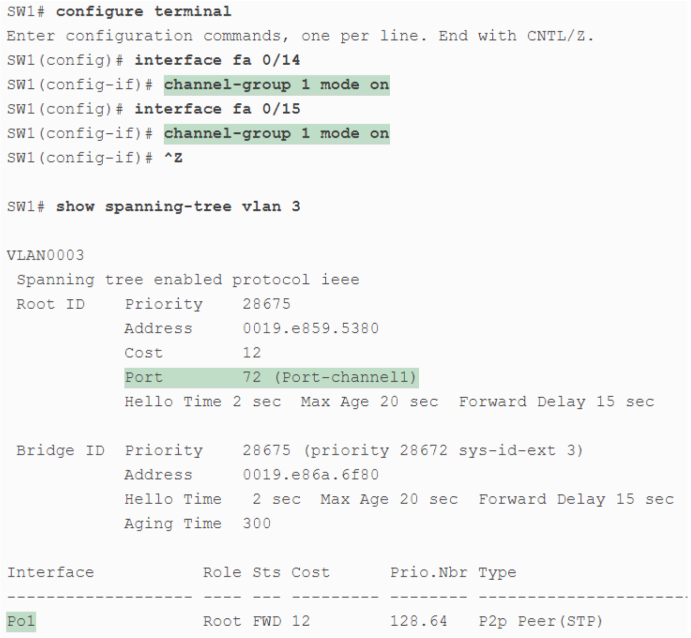
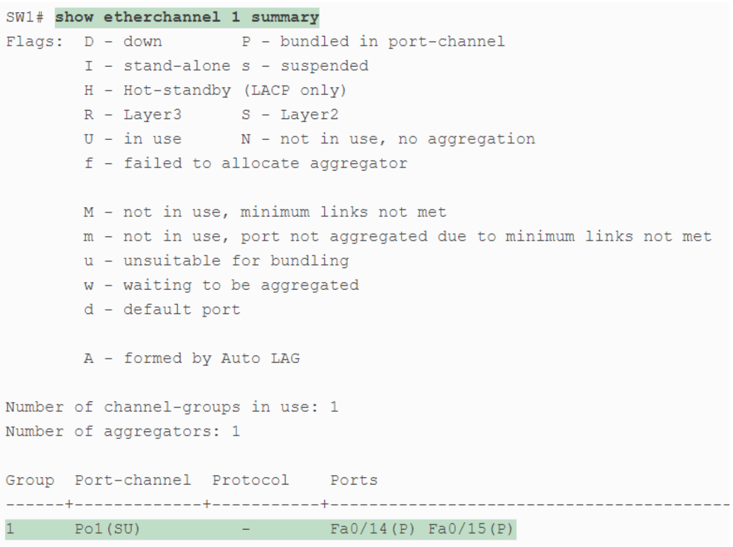


Figure 10-6 *Sample LAN Used in EtherChannel Example*



```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface fa 0/14
SW1(config-if)# channel-group 1 mode on
SW1(config)# interface fa 0/15
SW1(config-if)# channel-group 1 mode on
SW1(config-if)# ^Z

SW1# show spanning-tree vlan 3

VLAN0003
 Spanning tree enabled protocol ieee
 Root ID    Priority    28675
            Address     0019.e859.5380
            Cost        12
            Port        72 (Port-channel1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

 Bridge ID  Priority    28675 (priority 28672 sys-id-ext 3)
            Address     0019.e86a.6f80
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Po1                 Root FWD 12        128.64   P2p Peer(STP)
```



```
SW1# show etherchannel 1 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------
1      Po1(SU)          -        Fa0/14(P)  Fa0/15(P)
```

Po1, short for PortChannel1

Configuring Dynamic EtherChannels

Cisco switches also support two different configuration options that then use a dynamic protocol to negotiate whether a particular link becomes part of an EtherChannel or not. Basically, the configuration enables a protocol for a particular channel-group number. At that point, the switch can use the protocol to send messages to/from the neighboring switch and discover whether their configuration settings pass all checks. If a given physical link passes, the link is added to the EtherChannel and used; if not, it is placed in a down state, and not used, until the configuration inconsistency can be resolved.

Most Cisco Catalyst switches support the Cisco-proprietary Port Aggregation Protocol (PAgP) and the IEEE standard Link Aggregation Control Protocol (LACP),

negotiate so that only links that pass the configuration checks are actually used in an EtherChannel.

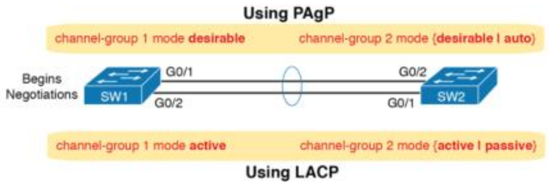
LACP does support more links in a channel—16—as compared to PAgP's maximum of 8. With LACP, only 8 can be active at one time, with the others waiting to be used should any of the other links fail.

To configure either protocol, a switch uses the channel-group configuration commands on each switch, but with a keyword that either means "use this protocol and begin negotiations" or "use this protocol and wait for the other switch to begin negotiations."

desirable and auto keywords enable PAgP

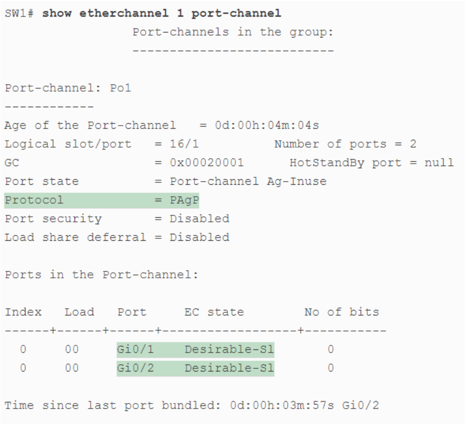
active and passive keywords enable LACP.

with PAgP, at least one of the two sides must use desirable, and with LACP, at least one of the two sides must use active.


Using PAgP
channel-group 1 mode desirable
channel-group 2 mode (desirable | auto)
Begins Negotiations
SW1
G0/1
G0/2
G0/2
G0/1
SW2
channel-group 1 mode active
channel-group 2 mode (active | passive)
Using LACP

Do not use the on parameter on one end, and either auto or desirable (or for LACP, active or passive) on the neighboring switch. The on option uses neither PAgP nor LACP, so a configuration that uses on, with PAgP or LACP options on the other end, would prevent the EtherChannel from working.

#show etherchannel 1 port-channel.



```
SW1# show etherchannel 1 port-channel
                 Port-channels in the group:
                 ---------------------------

Port-channel: Po1
------------
Age of the Port-channel   = 0d:00h:04m:04s
Logical slot/port   = 16/1          Number of ports = 2
GC                  = 0x00020001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            = PAgP
Port security       = Disabled
Load share deferral = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Desirable-Sl       0
  0     00     Gi0/2    Desirable-Sl       0

Time since last port bundled: 0d:00h:03m:57s Gi0/2
```

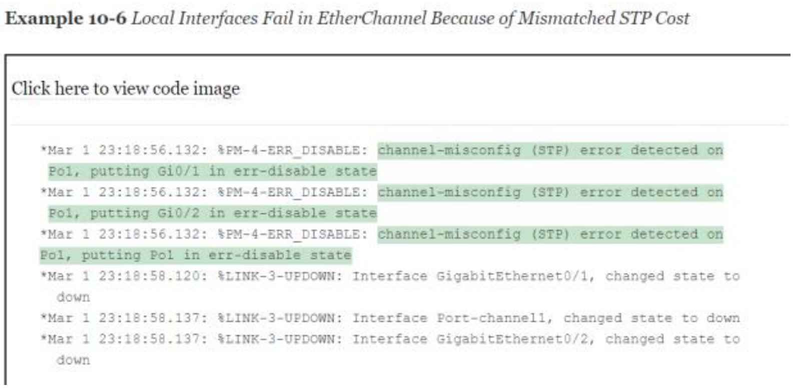
Physical Interface Configuration and EtherChannels

the switch compares the new physical port's configuration to the existing ports in the channel. That new physical interface's settings must be the same as the existing ports' settings; otherwise, the switch does not add the new link to the list of approved and working interfaces in the channel. That is, the physical interface remains configured as part of the PortChannel, but it is not used as part of the channel,

The list of items the switch checks includes the following:

- Speed
- Duplex
- Operational access or trunking state (all must be access, or all must be trunks)
- If an access port, the access VLAN
- If a trunk port, the allowed VLAN list (per the switchport trunk allowed command)
- If a trunk port, the native VLAN
- STP interface settings

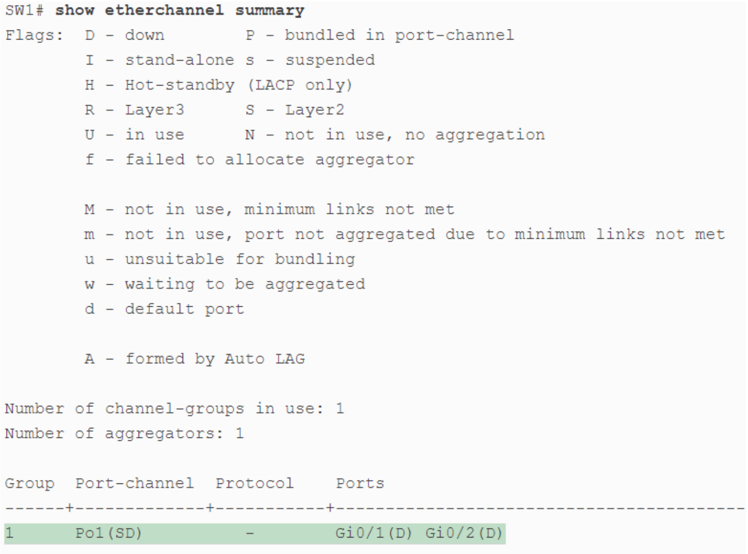
switches check the settings on the neighboring switch. To do so, the switches either use PAgP or LACP (if already in use) or use Cisco Discovery Protocol (CDP) if using manual configuration. When checking neighbors, all settings except the STP settings must match.



Example 10-6 *Local Interfaces Fail in EtherChannel Because of Mismatched STP Cost*

Click here to view code image

```
*Mar 1 23:18:56.132: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on
 Po1, putting Gi0/1 in err-disable state
*Mar 1 23:18:56.132: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on
 Po1, putting Gi0/2 in err-disable state
*Mar 1 23:18:56.132: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on
Po1, putting Po1 in err-disable state
*Mar 1 23:18:58.120: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
  down
*Mar 1 23:18:58.137: %LINK-3-UPDOWN: Interface Port-channel1, changed state to down
*Mar 1 23:18:58.137: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to
  down
```



```
SW1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SD)          -        Gi0/1(D)  Gi0/2(D)
```

the PortChannel and physical interfaces must be shutdown, and then no shutdown, to recover from the err-disabled state.

when a switch applies the shutdown and no shutdown commands to a PortChannel, it applies those same commands to the physical interfaces, as well; so, just do the shutdown/no shutdown on the PortChannel interface.

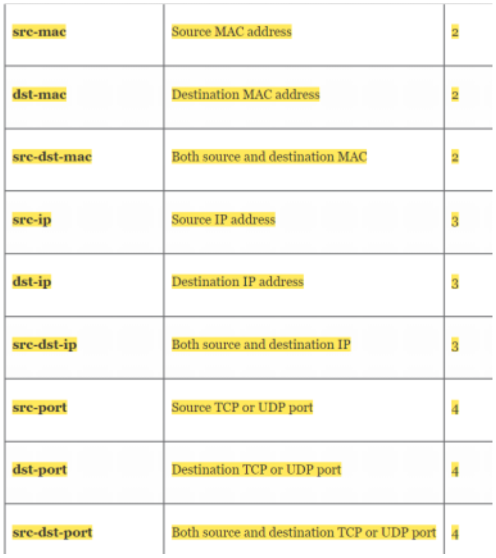
EtherChannel Load Distribution

When using Layer 2 EtherChannels, a switch's MAC learning process associates MAC addresses with the PortChannel interfaces and not the underlying physical ports. Later, when a switch makes a forwarding decision to send a frame out a PortChannel interface, the switch must do more work: to decide out which specific physical port to use to forward the frame. IOS documentation refers to those rules as EtherChannel load distribution or load balancing.

Configuration options for EtherChannel Load Distribution

EtherChannel load distribution makes the choice for each frame based on various numeric values found in the Layer 2, 3, and 4 headers. The process uses one configurable setting as input: the load distribution method as defined with the port-channel load-balance method global command. The process then performs some match against the fields identified by the configured method.

some switches may support only MAC-based methods, or only MAC- and IP-based methods, depending on the model and software version.



src-mac	Source MAC address	2
dst-mac	Destination MAC address	2
src-dst-mac	Both source and destination MAC	2
src-ip	Source IP address	3
dst-ip	Destination IP address	3
src-dst-ip	Both source and destination IP	3
src-port	Source TCP or UDP port	4
dst-port	Destination TCP or UDP port	4
src-dst-port	Both source and destination TCP or UDP port	4

various load distribution algorithms do share some common goals:

To cause all messages in a single application flow to use the same link in the channel, rather than being sent over different links. Doing so means that the switch will not inadvertently reorder the messages sent in that application flow by sending one message over a busy link that has a queue of waiting messages, while immediately sending the next message out an unused link.

To integrate the load distribution algorithm work into the hardware forwarding ASIC so that load distribution works just as quickly as the work to forward any other frame.

To use all the active links in the EtherChannel, adjusting to the addition and removal of active links over time.
Within the constraints of the other goals, balance the traffic across those active links.

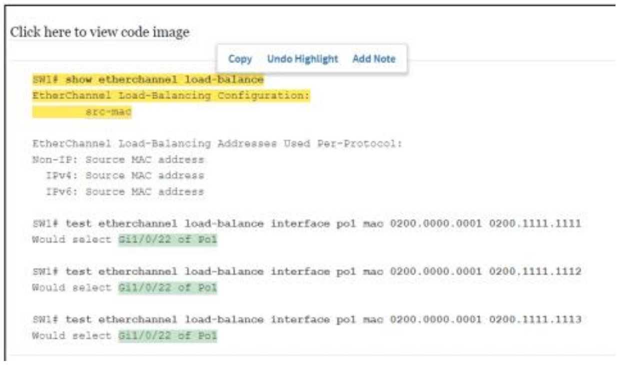
the algorithms first intend to avoid message reordering, make use of the switch forwarding ASICs, and use all the active links. However, the algorithm does not attempt to send the exact same number of bits over each link over time. The algorithm does try to balance the traffic, but always within the constraints of the other goals.

The algorithm focuses on the low-order bits in the fields in the headers because the low-order bits typically differ the most in real networks, while the high-order bits do not differ much. By focusing on the lower-order bits, the algorithm achieves better balancing of traffic over the links.

The Effects of the EtherChannel Load Distribution Algorithm

showing the use of the test etherchannel load-balance EXEC command. That command asks the switch to consider some addresses or ports and answer the question: which link would you use when forwarding a message with those address/port values?

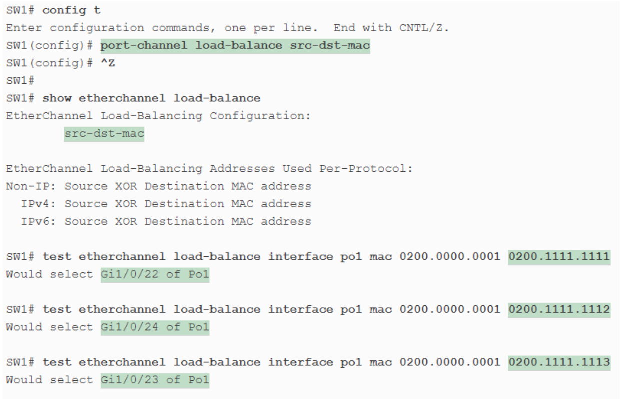
Example 10-7 *Testing with Identical Source MACs When Using* **src-mac** *Balancing*


Click here to view code image

```
SW1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source MAC address
  IPv4: Source MAC address
  IPv6: Source MAC address

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1111
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1112
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1113
Would select Gi1/0/22 of Po1
```

All three tests list the same outgoing physical interface because (1) the method uses only the source MAC address, and

all three tests use the same MAC addresses. All three tests use a different destination MAC address, with different low-order bits, but that had no impact on the choice because the method—src-mac—does not consider the destination MAC address.



```
SW1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)# port-channel load-balance src-dst-mac
SW1(config)# ^Z
SW1#
SW1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination MAC address
  IPv6: Source XOR Destination MAC address

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1111
Would select Gi1/0/22 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1112
Would select Gi1/0/24 of Po1

SW1# test etherchannel load-balance interface po1 mac 0200.0000.0001 0200.1111.1113
Would select Gi1/0/23 of Po1
```

chennel-group command cannot override the channel-protocol command

12. Classful IPv4

Friday, July 30, 2021 1:58 PM

Table 12-2 IPv4 Address Classes Based on First Octet Values

Class	First Octet Values	Purpose
A	1–126	Unicast (large networks)
B	128–191	Unicast (medium-sized networks)
C	192–223	Unicast (small networks)
D	224–239	Multicast
E	240–255	Reserved (formerly experimental)

address ranges of all addresses that begin with 0 and all addresses that begin with 127 are reserved

15 Router Operation

Friday, November 12, 2021 9:28 PM

The configuration of IP addresses differs in some ways, with switches using a VLAN interface and routers using an IP address configured on each working interface.

switches do not have auxiliary ports.

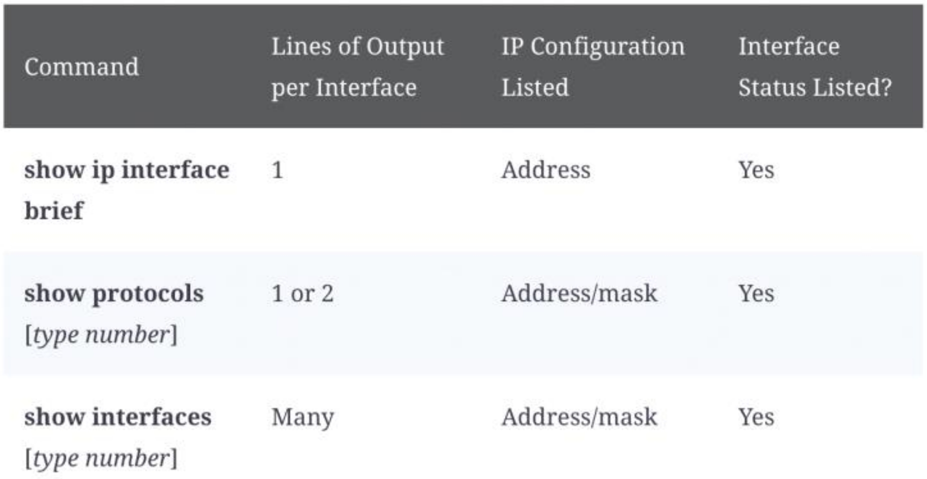
Layer 2 switches support the **show mac address-table** command, while Cisco routers do not.

routers support the **show ip route** command, while Cisco Layer 2 switches do not.

Layer 2 switches use the **show interfaces status** command to list one line of output per interface (and routers do not)

show protocols command. This command confirms the state of each of the three R1 interfaces in Figure 15-6 and the IP address and mask configured on those same interfaces.

Table 15-4 Key Commands to List Router Interface Status



Command	Lines of Output per Interface	IP Configuration Listed	Interface Status Listed?
show ip interface brief	1	Address	Yes
show protocols [*type number*]	1 or 2	Address/mask	Yes
show interfaces [*type number*]	Many	Address/mask	Yes

16 Static Routes

Friday, November 12, 2021 9:33 PM

1.0 Network Fundamentals

1.6 Configure and verify IPv4 addressing and subnetting

3.0 IP Connectivity

3.1 Interpret the components of routing table

3.1.a Routing protocol code

3.1.b Prefix

3.1.c Network mask

3.1.d Next hop

3.1.e Administrative distance

3.1.f Metric

3.1.g Gateway of last resort

3.2 Determine how a router makes a forwarding decision by default

3.2.a Longest match

3.2.b Administrative distance

3.3 Configure and verify IPv4 and IPv6 static routing

3.3.a Default route

3.3.b Network route

3.3.c Host route

3.3.d Floating static

Routers first learn connected routes, which are routes for subnets attached to a router interface. Routers can also use static routes, which are routes created through a configuration command (ip route) that tells the router what route to put in the IPv4 routing table. And routers can use a routing protocol, in which routers tell each other about all their known routes, so that all routers can learn and build routes to all networks and subnets.

Step 1. If the destination is local, send directly:

A. ''Find the destination host’s MAC address. Use the already-known Address Resolution Protocol (ARP) table entry, or use ARP messages to learn the information.

B. Encapsulate the IP packet in a data-link frame, with the destination data-link address of the destination host.

For each received data-link frame, choose whether or not to process the frame. Process it if

The frame has no errors (per the data-link trailer Frame Check Sequence [FCS] field).

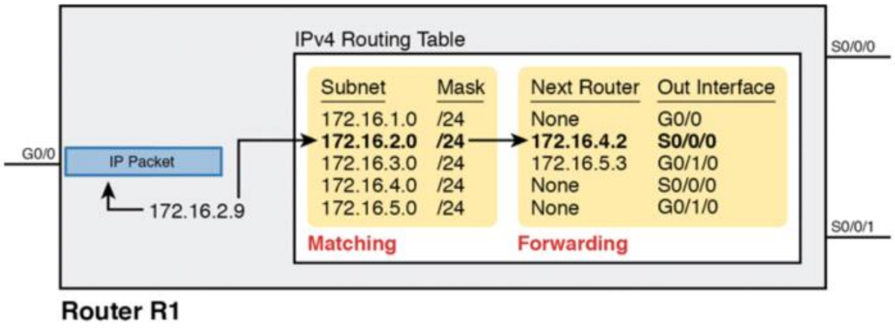
The frame’s destination data-link address is the router’s address (or an appropriate multicast or broadcast address).

If choosing to process the frame at Step 1, de-encapsulate the packet from inside the data-link frame.

Make a routing decision. To do so, compare the packet’s destination IP address to the routing table and find the route that matches the destination address. This route identifies the outgoing interface of the router and possibly the next-hop router.

Encapsulate the packet into a data-link frame appropriate for the outgoing interface. When forwarding out LAN interfaces, use ARP as needed to find the next device’s MAC address.

Transmit the frame out the outgoing interface, as listed in the matched IP route.



Subnet	Mask	Next Router	Out Interface
172.16.1.0	/24	None	G0/0
172.16.2.0	**/24**	**172.16.4.2**	**S0/0/0**
172.16.3.0	/24	172.16.5.3	G0/1/0
172.16.4.0	/24	None	S0/0/0
172.16.5.0	/24	None	G0/1/0

Figure 16-7 *Routing Step 3 on Router R1: Matching the Routing Table*

- The interface is in a working state. In other words, the interface status in the **show interfaces** command lists a line status of up and a protocol status of up.
- The interface has an IP address assigned through the **ip address** interface subcommand.

Routing Protocol Code: The legend at the top of the show ip route output (about nine lines) lists all the routing protocol codes (exam topic 3.1.a). This book references the codes for connected routes (C), local (L), static (S), and OSPF (O).

Prefix: The word prefix (exam topic 3.1.b) is just another name for subnet ID.

Mask: Each route lists a prefix (subnet ID) and network mask (exam topic 3.1.c) in prefix format, for example, /24.

The ARP Table on a Cisco Router

Dynamically learned ARP table entries have an upward counter, like the 35-minute value for the ARP table entry for IP address 172.16.1.9. By default, IOS will time out (remove) an ARP table entry after 240 minutes in which the entry is not used.

clear ip arp [ip-address] EXEC command.

Configuring Static Routes

The static route is considered a network route when the destination listed in the ip route command defines a subnet, or an entire Class A, B, or C network. In contrast, a default route matches all destination IP addresses, while a host route matches a single IP address (that is, an address of one host.)

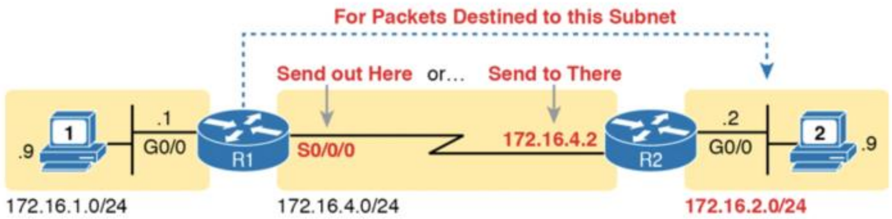


Figure 16-11 *Static Route Configuration Concept*

However, the route that used the outgoing interface configuration is also noted as a connected route; this is just a quirk of the output of the **show ip route** command.

also lists a few statistics about all IPv4 routes. For example, the example shows two lines, for the two static routes configured in Example 16-4, but statistics state that this router has routes for eight subnets.

IOS adds and removes these static routes dynamically over time, based on whether the outgoing interface is working or not. For example, in this case, if R1's S0/0/0 interface fails, R1 removes the static route to 172.16.2.0/24 from the IPv4 routing table. Later, when the interface comes up again, IOS adds the route back to the routing table.

Static Host Routes

To configure such a static route, the **ip route** command uses an IP address plus a mask of 255.255.255.255 so that the matching logic matches just that one address.

An engineer might use host routes to direct packets sent to one host over one path, with all other traffic to that host's subnet over some other path. For instance, you could define these two static routes for subnet 10.1.1.0/24 and host 10.1.1.9, with two different next-hop addresses, as follows:

routers use the most specific route (that is, the route with the longest prefix length)

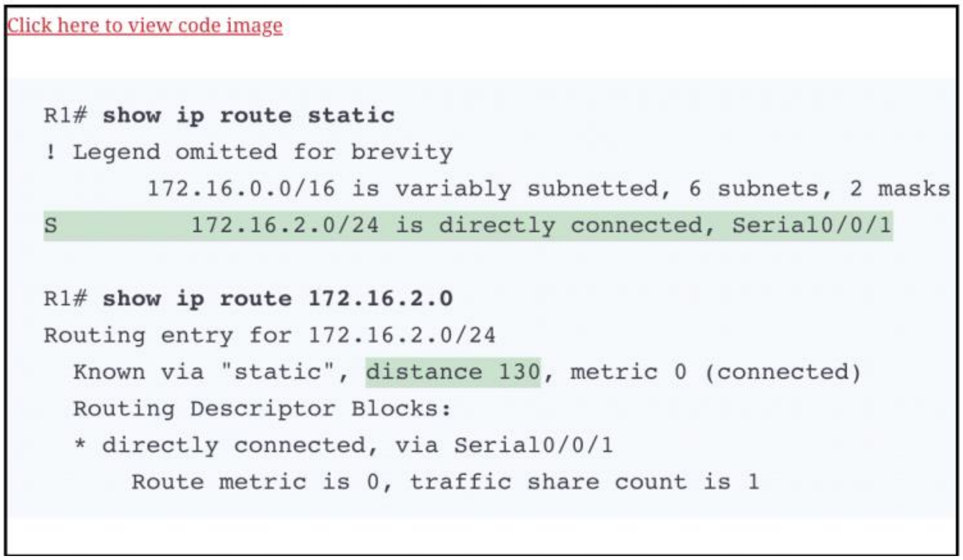
Floating Static Routes

the router must first decide which routing source has the better *administrative distance*, with lower being better, and then use the route learned from the better source

By default, IOS considers static routes better than OSPF-learned routes. By default, IOS gives static routes an administrative distance of 1 and OSPF routes an administrative distance of 110

To implement a floating static route, you need to use a parameter on the **ip route** command that sets the administrative distance for just that route, making the value larger than the default administrative distance of the routing protocol. For example, the **ip route 172.16.2.0 255.255.255.0 172.16.5.3 130**

while the **show ip route** command lists the administrative distance of most routes, as the first of two numbers inside two brackets, the **show ip route** *subnet* command plainly lists the administrative distance.



Click here to view code image

```
R1# show ip route static
! Legend omitted for brevity
       172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
S         172.16.2.0/24 is directly connected, Serial0/0/1

R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "static", distance 130, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/1
      Route metric is 0, traffic share count is 1
```

Static Default Routes

ip route 0.0.0.0 0.0.0.0 S0/0/1 creates a static default route on Router B1—a route that matches all IP packets—and sends those packets out interface S0/0/1.

show ip route

a *, meaning it is a *candidate default route*. A router can learn about more than one default route, and the router then has to choose which one to use; the * means that it is at least a candidate to become the default route.

Troubleshooting Static Routes

- The route is in the routing table but is incorrect.
  - Is there a subnetting math error in the subnet ID and mask?
  - Is the next-hop IP address correct and referencing an IP address on a neighboring router?
  - Does the next-hop IP address identify the correct router?
  - Is the outgoing interface correct, and referencing an interface on the local router (that is, the same router where the static route is configured)?

- The route is not in the routing table.

    table. IOS also considers the following before adding the route to its routing table:

    Key Topic

    - For **ip route** commands that list an outgoing interface, that interface must be in an up/up state.
    - For **ip route** commands that list a next-hop IP address, the local router must have a route to reach that next-hop address.
    - You can configure a static route so that IOS ignores these basic checks, always putting the IP route in the routing table. To do so, just use the **permanent** keyword on the **ip route** command. For example, by adding the **permanent** keyword to the end of the two commands as demonstrated in Example 16-7, R1 would now add these routes, regardless of whether the two WAN links were up.

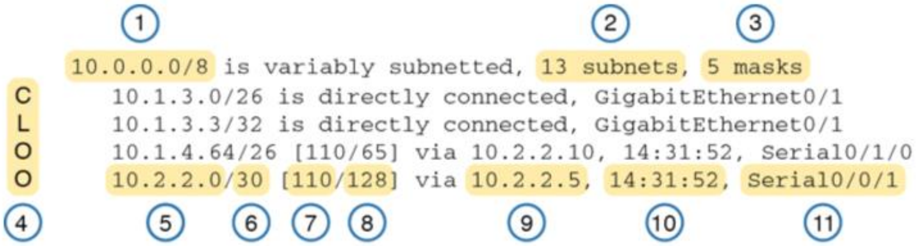
- The route is in the routing table and is correct, but the packets do not arrive at the destination host.

Many legitimate router features can cause these multiple routes to appear in a router's routing table, including

- Static routes
- Route autosummarization
- Manual route summarization

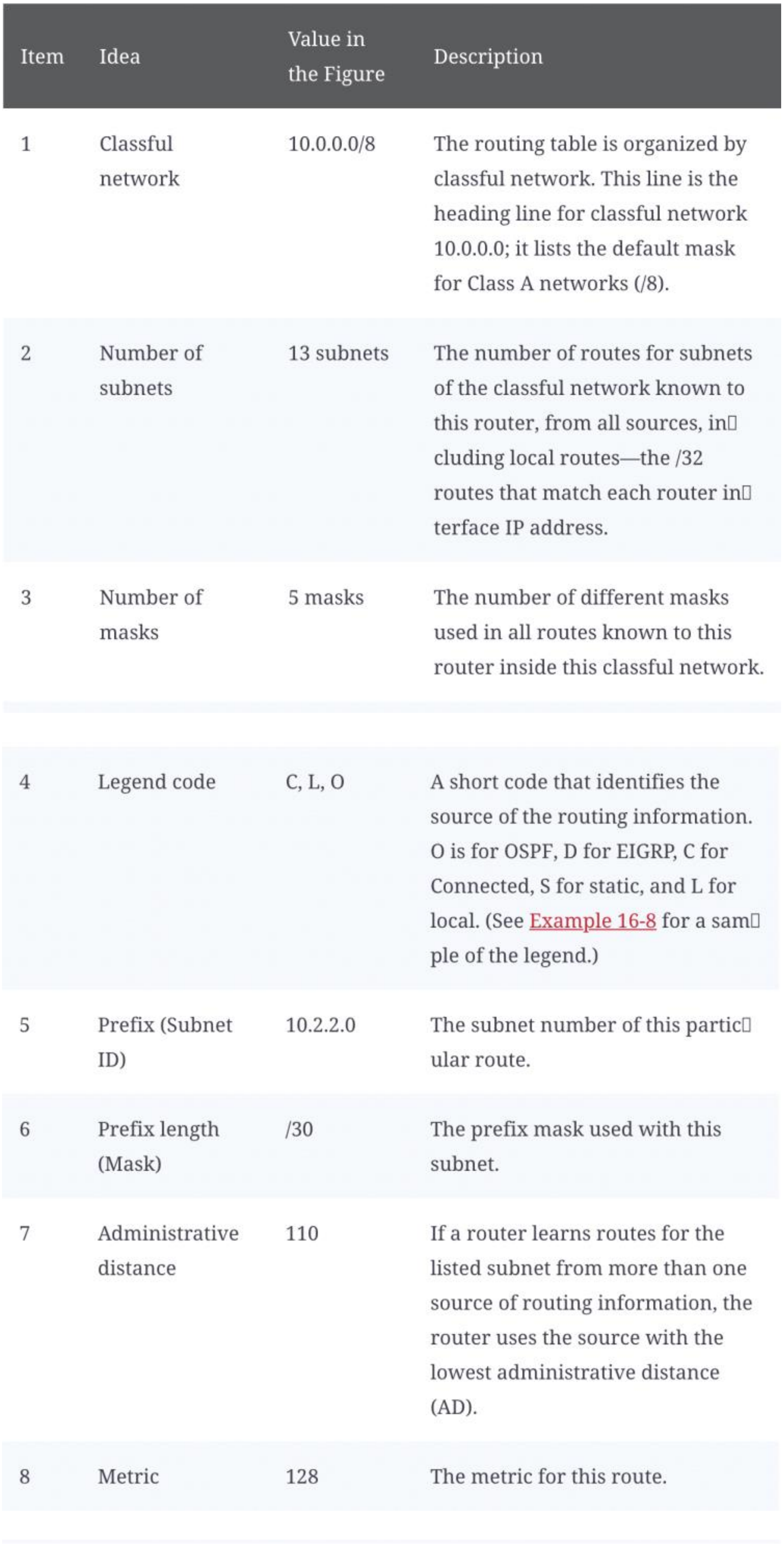
When a particular destination IP address matches more than one route in a router's IPv4 routing table, the router uses the most specific route—in other words, the route with the longest prefix length mask.

A second way to identify the route a router will use, one that does not require any subnetting math, is the **show ip route** *address* command. The last parameter on this command is the IP address of an assumed IP packet. The router replies by listing the route it would use to route a packet sent to that address.

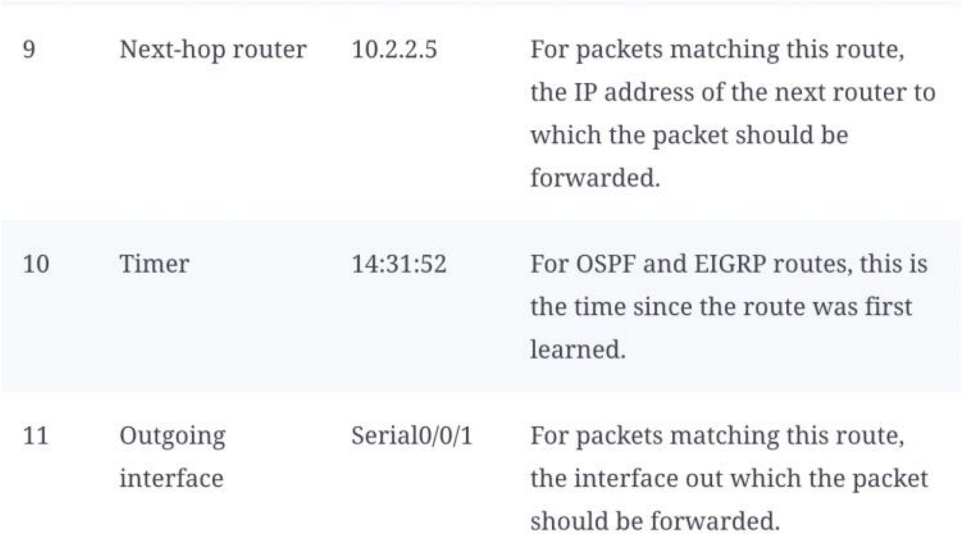


```
     10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
C       10.1.3.0/26 is directly connected, GigabitEthernet0/1
L       10.1.3.3/32 is directly connected, GigabitEthernet0/1
O       10.1.4.64/26 [110/65] via 10.2.2.10, 14:31:52, Serial0/1/0
O       10.2.2.0/30 [110/128] via 10.2.2.5, 14:31:52, Serial0/0/1
```

Figure 16-15 show ip route *Command Output Reference*



Item	Idea	Value in the Figure	Description
1	Classful network	10.0.0.0/8	The routing table is organized by classful network. This line is the heading line for classful network 10.0.0.0; it lists the default mask for Class A networks (/8).
2	Number of subnets	13 subnets	The number of routes for subnets of the classful network known to this router, from all sources, including local routes—the /32 routes that match each router interface IP address.
3	Number of masks	5 masks	The number of different masks used in all routes known to this router inside this classful network.
4	Legend code	C, L, O	A short code that identifies the source of the routing information. O is for OSPF, D for EIGRP, C for Connected, S for static, and L for local. (See Example 16-8 for a sample of the legend.)
5	Prefix (Subnet ID)	10.2.2.0	The subnet number of this particular route.
6	Prefix length (Mask)	/30	The prefix mask used with this subnet.
7	Administrative distance	110	If a router learns routes for the listed subnet from more than one source of routing information, the router uses the source with the lowest administrative distance (AD).
8	Metric	128	The metric for this route.



9	Next-hop router	10.2.2.5	For packets matching this route, the IP address of the next router to which the packet should be forwarded.
10	Timer	14:31:52	For OSPF and EIGRP routes, this is the time since the route was first learned.
11	Outgoing interface	Serial0/0/1	For packets matching this route, the interface out which the packet should be forwarded.

17 Routing in the LAN

Monday, November 22, 2021 9:39 AM

A. Use the **sdm prefer lanbase-routing** command (or similar) in global configuration mode to change the switch forwarding ASIC settings to make space for IPv4 routes at the next reload of the switch.

B. Use the **reload EXEC** command in enable mode to reload (reboot) the switch to pick up the new sdm prefer command setting.

C. Once reloaded, use the **ip routing** command in global configuration mode to enable the IPv4 routing function in IOS software and to enable key commands like **show ip route**.

if you then enabled OSPF on the Layer 3 switch, the configuration and verification would work the same as it does on a router, as discussed in Chapter 20, "Implementing OSPF." The routes that IOS adds to the Layer 3 switch's IP routing table would list the VLAN interfaces as outgoing interfaces.

Troubleshooting Routing with SVIs

look to those first few configuration commands listed in the configuration checklist found in the earlier section "Configuring Routing Using Switch SVIs." Those commands are sdm prefer (followed by a reload) and then ip routing (after the reload).

The sdm prefer command changes how the switch forwarding chips allocate memory for different forwarding tables, and changes to those tables require a reload of the switch. By default, many access switches that support Layer 3 switching still have an SDM default that does not allocate space for an IP routing table. Once changed and reloaded, the **ip routing** command then enables IPv4 routing in IOS software. Both are necessary before some Cisco switches will act as a Layer 3 switch.

Scenario 1: The last access interface in VLAN 10 is shut down (F0/1), so IOS shuts down the VLAN 10 interface.

Scenario 2: VLAN 20 (not VLAN interface 20, but VLAN 20) is deleted, which results in IOS then bringing down (not shutting down) the VLAN 20 interface.

Scenario 3: VLAN 30 (not VLAN interface 30, but VLAN 30) is shut down, which results in IOS then bringing down (not shutting down) the VLAN 30 interface.

VLAN Routing with Layer 3 Switch Routed Ports

On a routed port, the switch does not perform Layer 2 switching logic on that frame. Instead, frames arriving in a routed port trigger the Layer 3 routing logic, including

Stripping off the incoming frame's Ethernet data-link header/trailer

Making a Layer 3 forwarding decision by comparing the destination IP address to the IP routing table

Adding a new Ethernet data-link header/trailer to the packet

Forwarding the packet, encapsulated in a new frame

The exam topics do not mention routed interfaces specifically, but the exam topics do mention L3 EtherChannels, meaning Layer 3 EtherChannels.

Implementing Routed Interfaces on Switches

Enabling a switch interface to be a routed interface instead of a switched interface is simple: just use the no switchport subcommand on the physical interface.

To make the port stop acting like a switch port and instead act like a router port, use the no switchport command on the interface.

Once the port is acting as a routed port, think of it like a router interface

the routed interface will show up differently in command output in the switch. In particular, for an interface configured as a routed port with an IP address, like interface GigabitEthernet0/1 in the previous example:

Key Topic.
show interfaces: Similar to the same command on a router, the output will display the IP address of the interface. (Conversely, for switch ports, this command does not list an IP address.)

show interfaces status: Under the "VLAN" heading, instead of listing the access VLAN or the word trunk, the output lists the word routed, meaning that it is a routed port.

show ip route: Lists the routed port as an outgoing interface in routes.

show interfaces type number switchport: If a routed port, the output is short and confirms that the port is not a switch port. (If the port is a Layer 2 port, this command lists many configuration and status details.)

All the ports that are links directly between the Layer 3 switches can be routed interfaces.

Implementing Layer 3 EtherChannels

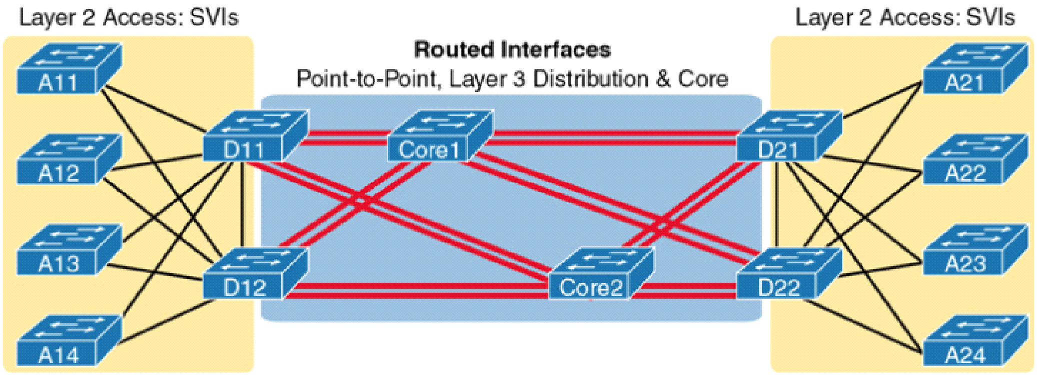


Figure 17-6 *Two Links Between Each Distribution and Core Switch*

each pair of switches has one routing protocol neighbor relationship with the neighbor, and not two. Each switch learns one route per destination per pair of links, and not two. IOS then balances the traffic, often with better balancing than the balancing that occurs with the use of multiple IP routes to the same subnet.

Step 1. Configure the physical interfaces as follows, in interface configuration mode:

A. Add the channel-group number mode on command to add it to the channel. Use the same number for all physical interfaces on the same switch, but the number used (the channel-group number) can differ on the two neighboring switches.

B. Add the **no switchport** command to make each physical port a routed port.

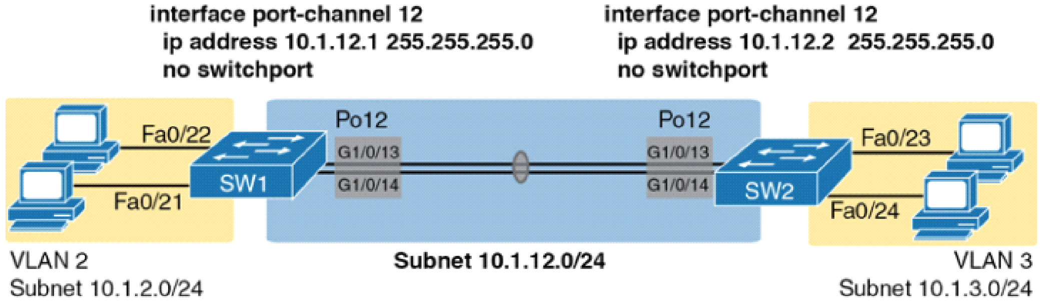
Step 2. Configure the PortChannel interface:

A. Use the **interface port-channel number** command to move to port-channel configuration mode for the same channel number configured on the physical interfaces.

B. Add the **no switchport** command to make sure that the port-channel interface acts as a routed port. (IOS may have already added this command.)

C. Use the **ip address address mask** command to configure the address and mask.

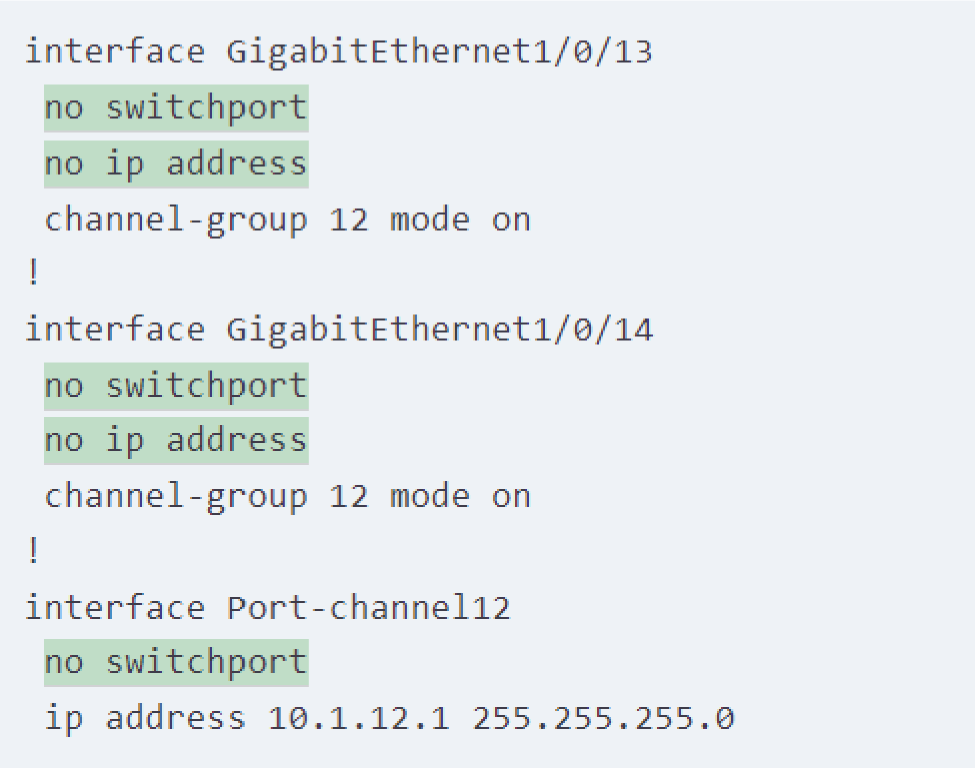
Cisco uses the term EtherChannel in concepts discussed in this section and then uses the term PortChannel, with command keyword port-channel, when verifying and configuring EtherChannels.



```
interface port-channel 12
 ip address 10.1.12.1 255.255.255.0
 no switchport
```

```
interface port-channel 12
 ip address 10.1.12.2  255.255.255.0
 no switchport
```

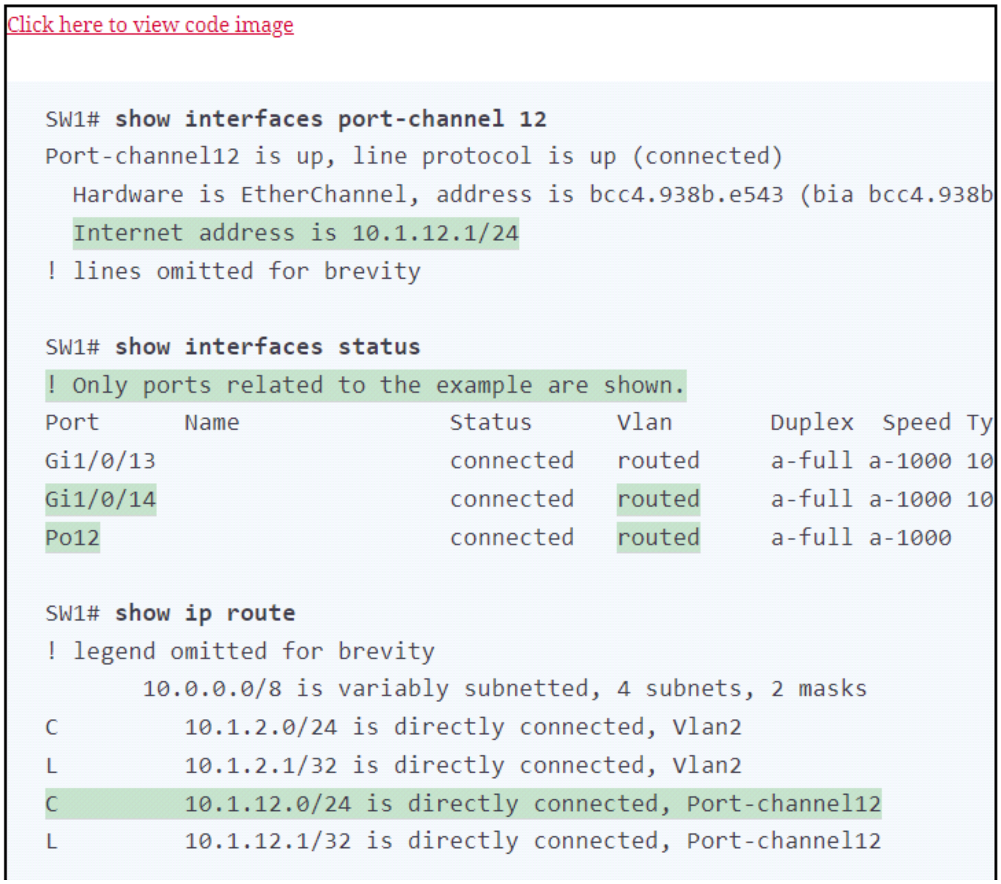
Figure 17-7 *Design Used in EtherChannel Configuration Examples*



```
interface GigabitEthernet1/0/13
 no switchport
 no ip address
 channel-group 12 mode on
!
interface GigabitEthernet1/0/14
 no switchport
 no ip address
 channel-group 12 mode on
!
interface Port-channel12
 no switchport
 ip address 10.1.12.1 255.255.255.0
```

although the physical interfaces and PortChannel interface are all routed ports, the IP address should be placed on the PortChannel interface only. In fact, when the no switchport command is configured on an interface, IOS adds the no ip address command to the interface.

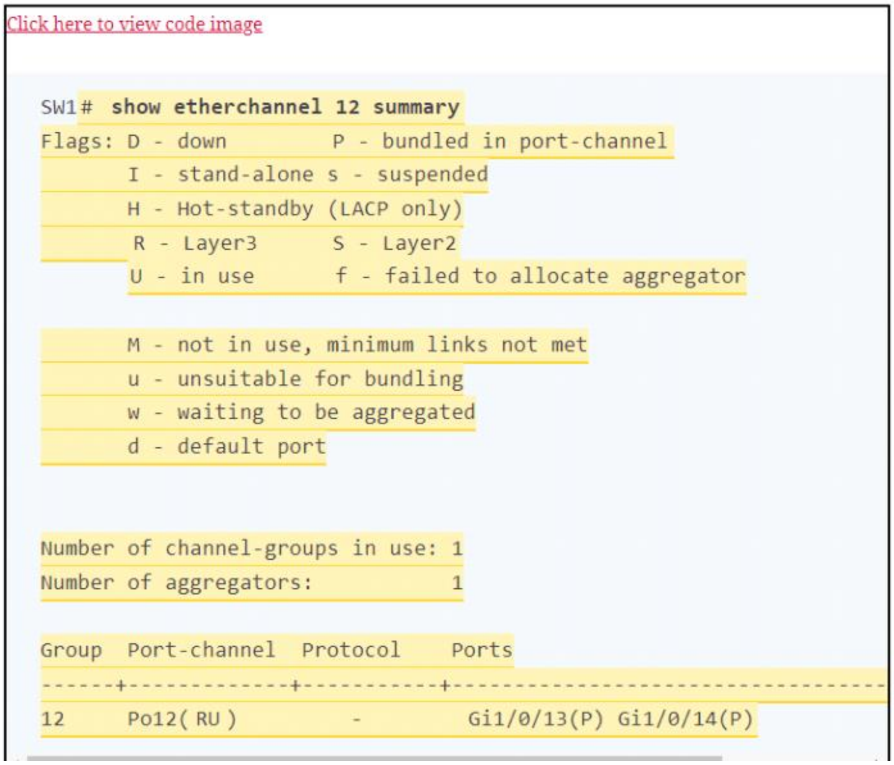
Example 17-13 *Verification Commands Listing Interface Port-Channel 12 from Switch SW1*



Click here to view code image

```
SW1# show interfaces port-channel 12
Port-channel12 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is bcc4.938b.e543 (bia bcc4.938b
  Internet address is 10.1.12.1/24
! lines omitted for brevity

SW1# show interfaces status
! Only ports related to the example are shown.
Port       Name               Status       Vlan        Duplex  Speed Ty
Gi1/0/13                      connected    routed      a-full a-1000 10
Gi1/0/14                      connected    routed      a-full a-1000 10
Po12                          connected    routed      a-full a-1000

SW1# show ip route
! legend omitted for brevity
       10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C         10.1.2.0/24 is directly connected, Vlan2
L         10.1.2.1/32 is directly connected, Vlan2
C         10.1.12.0/24 is directly connected, Port-channel12
L         10.1.12.1/32 is directly connected, Port-channel12
```

Example 17-14 *Verifying the EtherChannel*



Click here to view code image

```
SW1# show etherchannel 12 summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
       U - in use         f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
12     Po12( RU )        -        Gi1/0/13(P) Gi1/0/14(P)
```

look at the configuration of the **channel-group** command, which enables an interface for an EtherChannel. Second, you should check a list of settings that must match on the interfaces for a Layer 3 EtherChannel to work correctly.

As for the **channel-group interface** subcommand, this command can enable EtherChannel statically or dynamically. If dynamic, this command's keywords imply either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) as the protocol to negotiate between the neighboring switches whether they put the link into the EtherChannel.

no switchport: The PortChannel interface must be configured with the no switchport command, and so must the physical interfaces.

Speed: The physical ports in the channel must use the same speed.

duplex: The physical ports in the channel must use the same duplex.

18 T-Shoot Routing

Tuesday, November 23, 2021 5:09 AM

Problem Isolation Using the ping Command

functions as part of Layer 3, as a control protocol to assist IP by helping manage the IP network functions.

Ping options

The name or IP address of the destination,
how many times the command should send an echo request,
how long the command should wait (timeout) for an echo reply,
how big to make the packets, and many other options.

Extended ping allows R1's ping command to use R1's LAN IP address from within subnet 172.16.1.0/24.

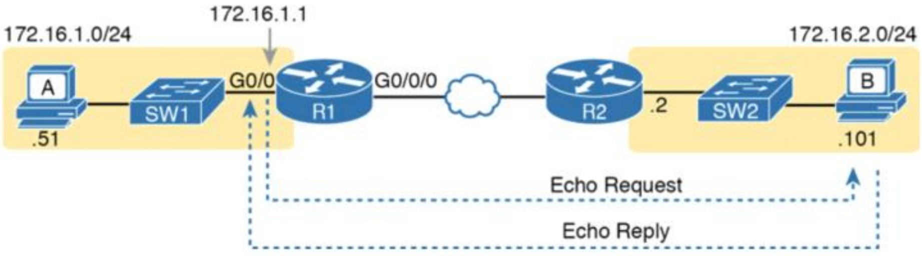


Figure 18-6 *Extended Ping Command Tests the Route to 172.16.1.51 (Host A)*

This same command could have been issued from the command line as ping 172.16.2.101 source 172.16.1.1.

```
R1# ping
Protocol [ip]:
Target IP address: 172.16.2.101
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.101, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Problems to test. (ping from router or from host?)

- IP ACLs that discard packets based on host A's IP address but allow packets that match the router's IP address
- LAN switch port security that filters A's frames (based on A's MAC address)
- IP routes on routers that happen to match host A's 172.16.1.51 address, with different routes that match R1's 172.16.1.1 address
- Problems with host A's default router setting

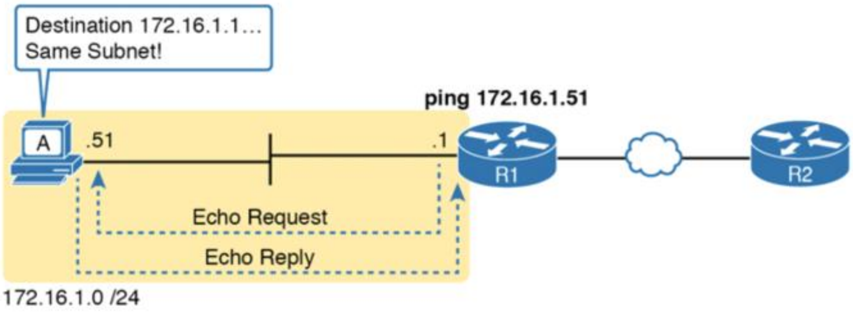


Figure 18-7 *Standard* **ping** *Command Confirms That the LAN Works*

If the ping works, it confirms the following, which rules out some potential issues:

The host with address 172.16.1.51 replied.

The LAN can pass unicast frames from R1 to host 172.16.1.51 and vice versa.

You can reasonably assume that the switches learned the MAC addresses of the router and the host, adding those to the MAC address tables.

Host A and Router R1 completed the ARP process and list each other in their respective Address Resolution Protocol (ARP) tables.

- **IP addressing problem:** Host A could be statically configured with the wrong IP address.
- **DHCP problems:** If you are using Dynamic Host Configuration Protocol (DHCP), many problems could exist.
- **VLAN trunking problems:** The router could be configured for 802.1Q trunking, when the switch is not (or vice versa).
- **LAN problems:** A wide variety of issues could exist with the Layer 2 switches, preventing any frames from flowing between host A and the router.

Testing LAN Neighbors with Extended Ping

an extended ping can test the host's default router setting. Both tests can be useful, especially for problem isolation, because

- If a standard ping of a local LAN host works…
- But an extended ping of the same LAN host fails…
- The problem likely relates somehow to the host's default router setting.

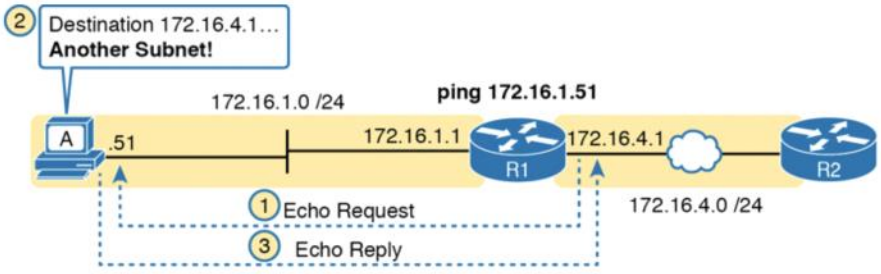


Figure 18-8 *Extended* **ping** *Command Does Test Host A's Default Router Setting*

Testing WAN Neighbors with Standard Ping

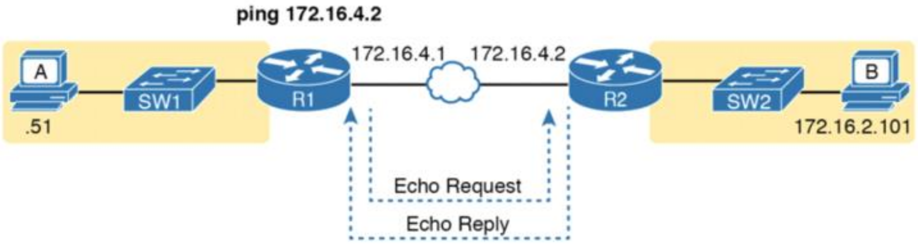


Figure 18-9 *Pinging Across a WAN Link*

A successful ping of the IP address on the other end of an Ethernet WAN link that sits between two routers confirms several specific facts, such as the following:

Both routers' WAN interfaces are in an up/up state.

The Layer 1 and 2 features of the link work.

The routers believe that the neighboring router's IP address is in the same subnet.

Inbound ACLs on both routers do not filter the incoming packets, respectively.

The remote router is configured with the expected IP address (172.16.4.2 in this case).

Using Ping with Names and with IP Addresses

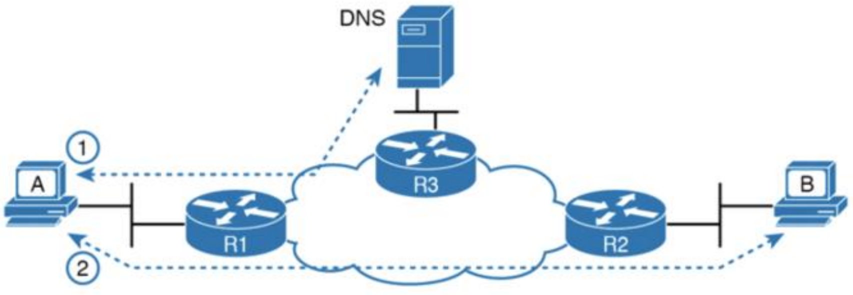


Figure 18-10 *DNS Name Resolution by Host A*

Problem Isolation Using the traceroute Command

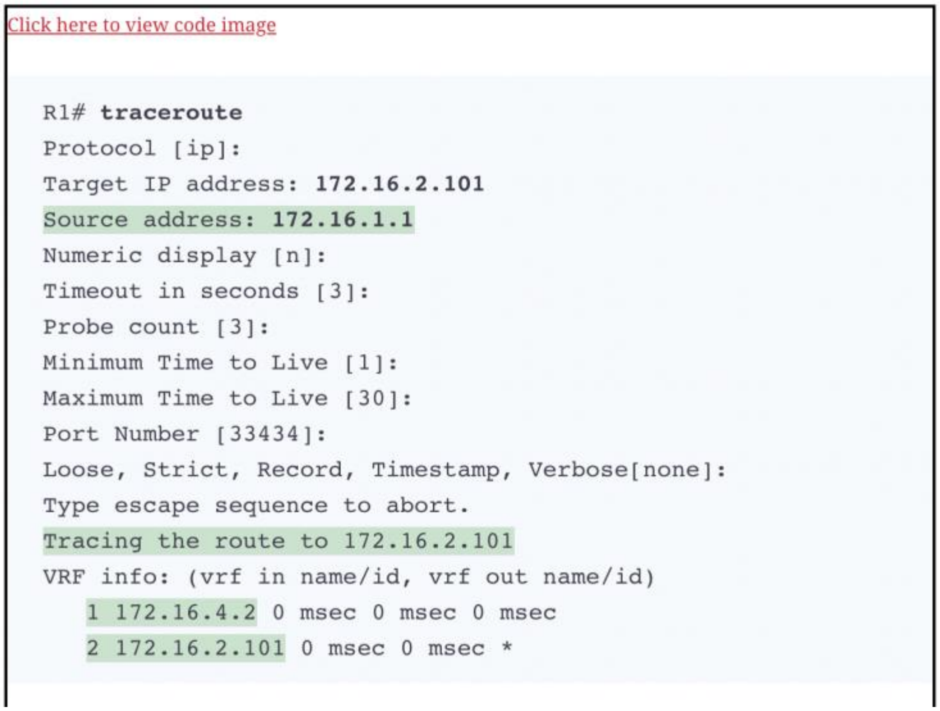
ping vs Tracert

- Both send messages in the network to test connectivity.
- Both rely on other devices to send back a reply.
- Both have wide support on many different operating systems.
- Both can use a hostname or an IP address to identify the destination.
- On routers, both have a standard and extended version, allowing better testing of the reverse route.

Standard and Extended traceroute

a standard **traceroute** command chooses an IP address based on the outgoing interface for the packet sent by the command. So, in this example, the packets sent by R1 come from source IP address 172.16.4.1, R1's G0/0/0 IP address.

Example 18-6 *Extended* **traceroute** *Command on R1*



Click here to view code image

```
R1# traceroute
Protocol [ip]:
Target IP address: 172.16.2.101
Source address: 172.16.1.1
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 172.16.2.101
VRF info: (vrf in name/id, vrf out name/id)
   1 172.16.4.2 0 msec 0 msec 0 msec
   2 172.16.2.101 0 msec 0 msec *
```

Host OS traceroute commands usually create ICMP echo requests. The Cisco IOS traceroute command instead creates IP packets with a UDP header. This bit of information may seem trivial at this point. However, note that an ACL may actually filter the traffic from a host's traceroute messages but not the router traceroute command, or vice versa.

Telnet and SSH

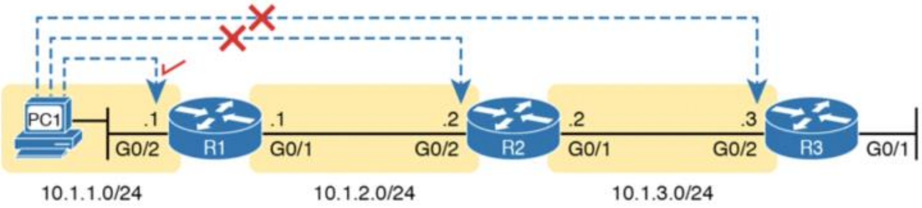


Figure 18-14 *Telnet Works from PC1 to R1 but Not to R2 or R3*

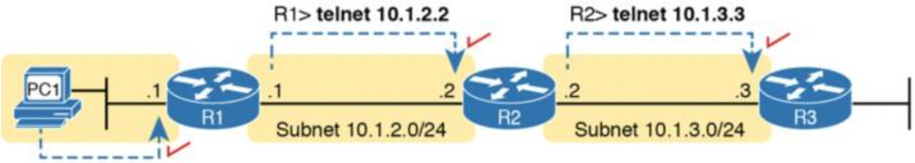
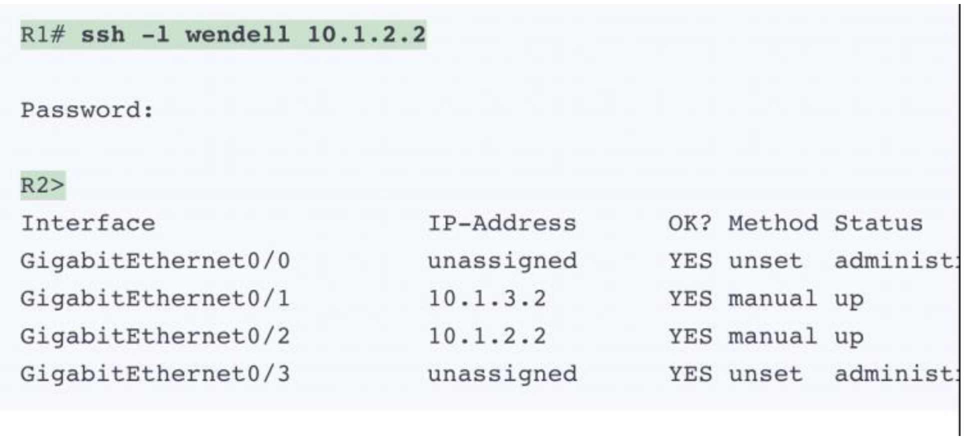


Figure 18-15 *Successive Telnet Connections: PC1 to R1, R1 to R2, and R2 to R3*



```
R1# ssh -l wendell 10.1.2.2

Password:

R2>
Interface                  IP-Address      OK? Method Status
GigabitEthernet0/0         unassigned      YES unset  administ
GigabitEthernet0/1         10.1.3.2        YES manual up
GigabitEthernet0/2         10.1.2.2        YES manual up
GigabitEthernet0/3         unassigned      YES unset  administ
```