CCNA 200-301 Study Notes

Disclaimer

This book was written as a study guide to Cisco CCNA certification. While every effort has been made to make this book as accurate as possible no warranty is implied. The author shall not be liable or responsible for any loss or damage arising from the information contained in this book.

About The Author

Shaun Hummel is author of certification books and recipient of Cisco spotlight awards for technical contributions. 15+ years of experience with Fortune 100 companies, large data centers, and certification training. There is a multifaceted training approach with study guide, video prep course, lab training, whiteboard review and practice tests. It is all designed to prepare you for CCNA certification.

Contents

Introduction 9

Section 1 Network Fundamentals 11

Binary Conversion 12
IPv4 Address Classes 12
IPv4 Address Types 12
RFC 1918 Private Addressing 13
Subnetting Examples 13
IPv6 Addressing Concepts 18
IPv6 Address Options 18
IPv6 Addressing Rules 18
IPv6 Address Types 19
IPv6 Packet 19
Interfaces and Cabling Media 20
Network Components 23
Wireless Characteristics 24
TCP vs UDP Comparison 24
Application Ports 25

Section 2 Network Access 27

Switching Concepts 27
MAC Address Table 27
MAC Learning and Aging 29
Frame Switching 31
Access Ports (Data and Voice) 34
Trunk Interface 35
802.1q VLAN Tag 35
Native VLAN 35
VLAN Pruning 36
Dynamic Trunking Protocol 36
Normal/Extended VLANs 37
LACP EtherChannel 39
Spanning Tree Protocol 40
Cisco Discovery Protocol 41
Link Layer Discovery Protocol 42

Section 3	**IP Connectivity**	**45**
	Routing Concepts	45
	Routing Table Components	45
	Routing Source Codes	46
	Per-Hop Addressing	48
	Route Selection	49
	IPv4 Static Routing	55
	IPv6 Static Routing	56
	IPv6 Route Types	56
	IPv4 Packet Structure	57
	OSPF Routing Protocol	58
	Neighbor Adjacency	59
	Metric Calculation	60
	Router ID	61
	Designated Router	62
	Network Type	66
	OSPF Operation	68
	OSPFv2 Configuration	69
	First Hop Redundancy Protocol	71
Section 4	**IP Services**	**75**
	DHCP Services	75
	DNS Commands	75
	Network Time Protocol	76
	Network Address Translation	77
	SNMP Monitoring	78
	Syslog Messaging	78
	QoS Per-Hop Behavior	81
	TFTP vs FTP	82
Section 5	**Security Fundamentals**	**85**
	Device Hardening	85
	Port Security	86
	Access Control Lists	88
	Cyber Security Concepts	91
	AAA Concepts	92
	Multi-Factor Authentication	92
	DHCP Snooping	93
	SSL vs VPN	94

Section 6	**Automation and Programmability**	**97**
	Traditional vs Controller-Based	97
	Network Underlays and Overlays	99
	SDN Architecture	101
	Automation Components	104
	Puppet, Chef and Ansible Tools	106
	Cisco DNA Center	107
	REST API Architecture	109
	Media Types	111
Section 7	**CCNA Exam Prep Tools**	**115**
	IOS Command Reference	115
	IOS Configuration Tool	123
	CCNA Score Your Best	129
	Exam Day Whiteboard	131

Introduction

CCNA certification has become increasingly difficult and requires proper preparation to pass the exam. This exam review is a study tool designed to prepare you 100% for exam day. Cisco is aligning the new CCNA 200-301 certification exam with a shift to internet-based connectivity model and IP-only routing. The new exam removes all dynamic routing protocols except OSPFv2. There are a significant number of new topics as well including cyber security, wireless, and automation. That is attributed to the popularity of mobility services, cloud computing and SDN.

The management of network infrastructure has radically changed with open source architecture. Cisco has programmable network devices and virtualization of physical equipment. CCNA engineers now support private and cloud data connections. The pre-exam review has some 300+ concepts with protocol operation, network addressing, cyber security, SDN, and study tools.

CCNA Training Strategy

Preparing for CCNA certification requires students to invest some time to pass the exam. It is important to learn and review what was learned as exam day approaches. CCNA candidates should learn test-taking skills as well to avoid common mistakes during the exam.

CCNA Training Solutions

- CCNA 200-301 Exam Day Whiteboard
- CCNA 200-301 Certification Lab Guide
- CCNA 200-301 Pre-Exam Practice Tests
- CCNA 200-301 Configuration Mega Labs

Network Fundamentals

Binary Conversion

It is important to understand how to convert from IPv4 decimal notation to binary for subnetting and wildcard masks. The following describes how to convert from IPv4 decimal notation to binary notation.

- The binary system is based on ones (1) and zeros (0).
- There are 8 bits per octet, 4 octets per IPv4 address.
- The bit value is based on position.
- The bit set to 1 sets the value. The bit set to zero = 0
- There are 8 bits per octet = 2^8 = 256 decimal values
- Set all bits to 1 = 255, set all bits to 0 = 0

Table 1-1 Binary Conversion

0	0	0	0	0	0	0	0	= 0
1	1	1	1	1	1	1	1	= 255
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**bit value**
8	7	6	5	4	3	2	1	bit position

Binary to Decimal Conversion

Converting binary number to an equivalent decimal number requires adding the values of each bit position set to (1) for each octet. The sum of each octet creates a dotted decimal address.

0 0 0 0 **1** 0 **1** 0 = 10

4th bit (8) + 2nd bit (2) = 10

Example 1

Converting the binary number to an equivalent decimal number requires adding the values of each bit position set to (1) for each octet. The sum of each octet creates a dotted decimal value (IP address).

0000**1**0**1**0 **.** 0**11**00000 **.** 00**1**0**1**000 **.** **1**0000000

8+2 **.** 64+32 **.** (32+8) **.** 128 = 10.96.40.128

Example 2

Converting IPv4 address 192.168.64.10 to an equivalent binary number requires setting specific bits for each octet to (1) value. The sum of each octet adds up to decimal value for each octet.

192 . 168 . 64 . 10

11000000 . **1**0**1**0**1**000 . 0**1**000000 . 0000**1**0**1**0

128+64 . 128+32+8 . 64 . 8+2

Table 1-2 IPv4 Address Classes

Class	IP Address Range	Default Subnet Mask
A	1.0.0.0 - 127.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	Multicast
E	240.0.0.0 - 255.255.255.255	Reserved

Table 1-3 IPv4 Address Types

Type	Description
static	manually assigned to a network interface
dynamic	DHCP assigned from an address pool
secondary	manually assigned from different subnet than primary address
loopback	logical interface manually assigned to a network device
gateway	Layer 3 address used for access to routing services

Table 1-4 RFC 1918 Private Addressing

IP Address Range	Mask	Network	Host
10.0.0.0 - 10.255.255.255	255.0.0.0	8 bits (/8)	24 bits
172.16.0.0 - 172.31.255.255	255.240.0.0	12 bits (/12)	20 bits
192.168.0.0 - 192.168.255.255	255.255.0.0	16 bits (/16)	16 bits

Table 1-5 Class C Subnetting Table

Subnet Mask	CIDR	Subnet Bits	Subnets	Host Bits	Hosts
255.255.255.0	/24	none	1	8	254
255.255.255.128	/25	1	2	7	126
255.255.255.192	/26	2	4	6	62
255.255.255.224	/27	3	8	5	30
255.255.255.240	/28	4	16	4	14
255.255.255.248	/29	5	32	3	6
255.255.255.252	/30	6	64	2	2

* The host number does not include network and broadcast address. They are reserved for each individual subnet and are not assignable to any hosts.

Example 1: Subnetting

What network address and subnet mask would allow at least 10 web servers (hosts) to be assigned to the same subnet?

A. 192.168.100.0 255.255.255.252

B. 192.168.100.0 255.255.255.248

C. 192.168.100.0 255.255.255.240

D. 192.168.240.0 255.255.255.252

Answer (C)

The subnet mask defines the network portion and host portion of an IP address. Increasing the subnet mask length will increase the number of subnets available.

There are ten network interfaces that each require a host IP address. That would require at least four host bits to enable 14 host assignments considering network address and broadcast address are not assignable.

2^3 = 3 host bits = 8 - 2 = 6 host assignments (no)

2^4 = 4 host bits = 16 - 2 = 14 host assignments (yes)

network portion = 32 bits - 4 bits = 28 bits (/28)

= 255.255.255.240

network (28 bits) | host (4 bits)

11111111.11111111.11111111.1111 0000

255. 255. 255. 240

The 255.255.255.240 (/28) subnet mask starts at the bit 5 of the 4th octet and has a value of 16. The subnets are multiples of 16 (0, 16, 32, 48 etc).

Answer: **192.168.100.0/28**

Example 2: Subnetting

As a network administrator, you are asked to create a network address plan for multiple point-to-point WAN links. What is the optimized subnet mask that enables the minimum number of host IP address assignments?

Answer

The question asks for the most effective addressing of point-to-point WAN links. There are only two network interfaces (host assignments) required per WAN link. They are assigned to the local and connected neighbor router physical interfaces in the same subnet.

- The number of host bits required = 2^2 = 4 - 2 = 2
- The number of network bits (subnet mask) = 30

network bits (/30) | host (1-2)

11111111.11111111.11111111.111111 00

The rightmost bit of the subnet mask (network bits) determines the subnet multiple. That is bit 3 of the 4th octet with a decimal value of 4. As a result the subnets are multiples of 2 (0, 4, 8, 12 etc). The zero subnet is included as a result of the default **ip subnet zero** feature. The following are the first assignable host IP addresses for the zero subnet.

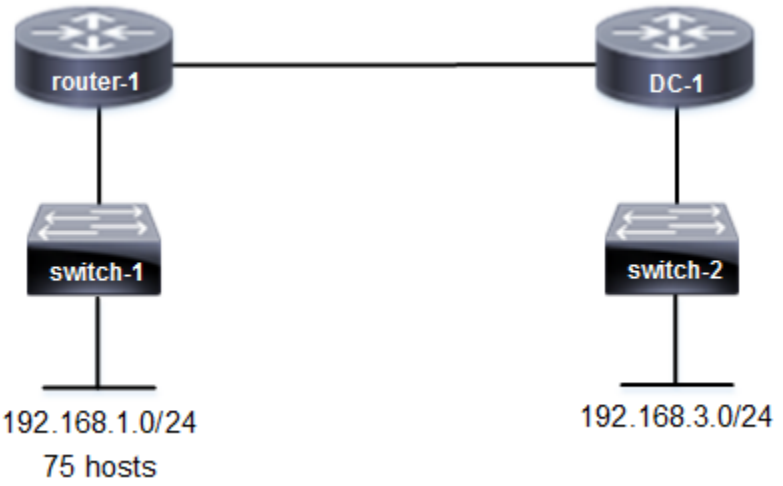
- network address = 192.168.1.0
- router interface addresses = 192.168.1.1/30, 192.168.1.2/30
- broadcast address = 192.168.1.3

Answer: **192.168.1.0/30**

Example 3: Subnetting

Refer to the network topology drawing. A new switch with 75 hosts has been added to switch-1. What is the minimum subnet mask that will provide enough IP addresses from network address 192.168.1.0/24?

Figure 1-1 Subnetting 75 Hosts



Answer

Class C addressing assigns all hosts from the 4th octet only. The subnet mask must support 75 new hosts that will connect to a new switch. That requires at least 7 bits for hosts (2^7 = 128) from the 4th octet. The rightmost 6 bits of 4th octet provide a maximum of only (2^6 = 64) host IP addresses assignable.

The network portion (subnet mask length) is 25 bits or (/25 for CIDR notation) based on the fact that 7 bits are assigned to the host portion. It is a Class C address so the 4th octet is being subnetted only. There is a single bit (leftmost bit of 4th octet) that provides subnets 192.168.1.0 and 192.168.1.128 so the correct answer is 192.168.1.128/25

network portion (/25) | host (7 bits)

11111111.11111111.11111111.1 0000000

Example 4: Subnetting

What IP address is assignable to host based on subnet mask 255.255.255.224?

A. 192.168.10.31

B. 192.168.10.29

C. 192.168.10.0

D. 192.168.10.32

Answer (B)

The network and broadcast addresses are not assignable to network interfaces. The subnet multiple is calculated based on bit value of bit position 6. The subnet multiple start at 0 with multiples of 32 (0, 32, 64, 96, 128, 160, 192, 224).

```
                network                 | host
11111111.11111111.11111111.111 00000
   255.      255.      255.    224
```

1. 4th octet is subnetted
2. subnet multiple = bit position 6 = decimal 32
3. network address of zero subnet = 192.168.10.0
4. host range = first 5 bits = 2^5 = 32 - 2 = 30 host assignments

- network address = 192.168.10.0
- host range = 192.168.10.1 - 192.168.10.30
- broadcast address = 192.168.10.31

Example 5: Subnetting

What is the network address of a host assigned 192.168.1.42/29?

Answer

The network address is the first address assigned to a subnet range. The IP address 192.168.1.42 is a Class C address. The nondefault subnet mask 255.255.255.248.0 (/29) provides the subnetting.

```
                                network                 | host
192.168.1.42      = 11000000.10101000.00000001.00101 010
255.255.255.248 = 11111111.11111111.11111111.11111 000
```

The host portion is the rightmost 3 bits of the 4th octet. The subnetted portion is the 5 bits of the 4th octet (bold). It is a Class C address so subnetting is only done on the 4th octet. The IP address class is key with subnetting questions.

The rightmost bit of the subnet mask (network bits) determines the subnet multiple and where it starts. In this example, it is bit 4 with decimal value of 8. The 5 subnetted bits (bold) enable 32 subnets with the first network address starting at subnet zero (0) and multiples of 8. (0, 8, 16, 24, 32, **40**, 48, 56, etc). The nearest subnet is 192.168.1.40 as the network address for 192.168.1.42

- network address = 192.168.1.40
- host addresses = 192.168.1.41 - 192.168.1.46
- broadcast address = 192.168.1.47

The next subnet of 192.168.1.48 is out of range.

IPv6 Addressing

IPv6 Address Characteristics

- 128 bits length address
- 8 groups with 4 bits per group
- prefix (64 bit) and interface identifier (64 bit)
- multicast, anycast and unicast messages only
- Regional Internet Registry (RIR) allocated
- loopback (**::1**) and link-local address mandatory per interface
- multiple address per interface supported

Table 1-6 IPv6 Addressing Options

Method	Description
Manual	traditional manual configuration of an IPv6 address.
Stateful DHCPv6	most similar to DHCPv4 server.
Stateless DHCPv6	SLAAC is used with this method to assign only an IPv6 address and default gateway to a network interface. DHCPv6 server is required for additional settings such as DNS server address for example.
SLAAC	Stateless Autoconfiguration (SLAAC) generates a unique link-local address based on EUI-64 format. The IPv6 address is assigned based on the network prefix (local subnet) for each client.

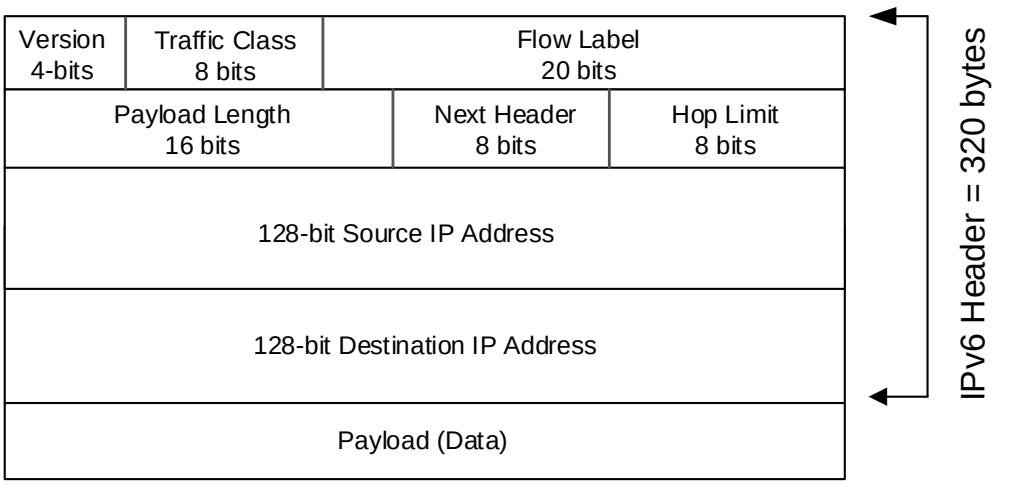
IPv6 Addressing Rules

- The double colon **::** is only permitted once per IPv6 address.
- Minimize multiple **consecutive** zero groups to a double colon **::**
- Delete leading zeros from a single group (**00**9F = **:**9F**:**)
- Minimize a **single** group with all zeros to single zero **:0:**
- Any IPv6 address with less than 8 groups must have a double colon that represents a single or multiple zero groups

Table 1-7 IPv6 Address Types

global unicast	internet routable with global routing prefix 2000::/3
multicast address	prefix FF00::/8 (send to group members)
unique local address	private global address, not internet routable, starts with FD00::/8
link-local address	mandatory, auto-configured, local subnet only, used for routing adjacency, prefix FE80::/10
loopback address	universal address, assigned to every interface, prefix ::1/128
modified eui-64	IPv6 host portion identifier, derived from MAC address
unspecified address	source address for initializing host, :1/128

IPv6 Packet



Network Interfaces and Cabling Media

Table 1-8 Network Cabling Types

straight-through	dissimilar device type	switch to router switch to host
rollover	console port	laptop to console
crossover	same device type	switch to switch router to router
serial	router to CSU/DSU	WAN

Table 1-9 Common Ethernet Standards

1000Base-LX/LH	Single-mode Fiber, 1 Gbps, 10 km
1000Base-SX	Multi-mode Fiber, 1 Gbps, 220 - 550 m
100Base-TX	Cat 5, Copper, Fast Ethernet, 100 m
1000Base-T	Cat 5, Copper, 1 Gbps, 100 m
10GBase-T	Cat 6, Copper, 10 Gbps, 55 m
1000Base-LX	Multi-mode Fiber, 1 Gbps, 550 m, SMF (5 km)
1000Base-ZX	Single-mode Fiber, 1 Gbps, 70 km

Operational vs Administrative

Operational status is the running state of a network device. Administrative status is how the device is configured. The operational status confirms for example that an interface is up, switch port mode or routing table entries. They are listed with various IOS show commands from CLI.

Network Interface States

There is no routing available unless Layer 1 and Layer 2 is working correctly on any network device. The possible interface states for network interfaces are *up/up***,** *up/down* and *administratively down / administratively down***.** The normal status of an Ethernet interface is up/up.

Interface = Layer 1, Line protocol = Layer 2

device# **show interfaces gigabitethernet 1/1**

GigabitEthernet1/1 up, Line Protocol up (normal state)

The **shutdown** command would change interface status to *administratively down*. It is not possible to have line protocol in *up* state when the interface (Ethernet) is *down* (down/up).

Typical Interface Errors

Layer 1 = cabling, switch configuration mismatches (speed/duplex) errors.

Layer 2 = encapsulation mismatch, spanning tree, clocking errors.

Err-Disabled State

Cisco switch interfaces that are in ***err-disabled*** state cannot send or receive frames and are essentially shutdown. The cause is either operational or a configuration mismatch. The following are typical causes of err-disabled state:

- duplex mismatch
- port security violation
- EtherChannel mismatch
- UDLD errors
- BPDU guard
- interface flapping

Duplex Setting

Gigabit Ethernet interface supports full-duplex. Traffic can be sent simultaneously in both directions to double the bandwidth available. That eliminates collisions and creates a collision domain per interface. The fact that there are no collisions increase throughput and decreases network latency.

Gigabit Ethernet eliminates collisions unless there is a configuration error or hardware issue. Collisions are caused most often when there is a duplex mismatch on connected switch interfaces. Collisions also occur when network interface hardware or cabling is defective. The following are recommended duplex settings to minimize interface errors on network interfaces.

- configure full-duplex setting on both switch link interfaces
- configure auto-negotiation on both switch link interfaces

Duplex mismatch with a neighbor interface cause the following interface errors:

- collisions
- input errors
- CRC errors
- slow performance

The cause of collisions on a broadcast domain (VLAN) instead of interfaces are typically the result of duplex mismatches and faulty network interface card (NIC). The most common cause of CRC and runts is collisions. Giant frames result from either a faulty network interface or an MTU configuration error

Network Components

Table 1-10 Network Services

Device Type	Network Services
router	route selection, logical IP addressing, frame rewrite, default gateway, proxy ARP, WAN
Layer 2 switch	endpoint access, frame switching, MAC addressing
Layer 3 switch	traffic aggregation, frame switching, route selection, default gateway, VLAN routing
access point	network access, bridging frames to wired network
wireless controller	manage user policies, optimize RF, configuration
firewall	network security, stateful packet inspection, IPS, malware detection, VPN

Table 1-11 Device Classes

Device Class	OSI Layer
wireless access point	Layer 2
wireless LAN controller	Layer 2
switch	Layer 2
router	Layer 3
firewall	Layer 7

Table 1-12 Traffic Domains

Device Type	Description	Traffic Flow
access point	collision domain	half-duplex
*switch port	collision domain	full-duplex
VLAN	broadcast domain	not physical interface
router interface	broadcast domain	full-duplex

* half-duplex switch ports are not configured on Gigabit interfaces unless required for compatibility with third party equipment or older devices.

Table 1-13 Wireless Network Standards

Access Point	Band	Data Rate	*Channels	Channel Width
802.11b	2.4 GHz	11 Mbps	1,6,11	20 MHz
802.11g	2.4 GHz	54 Mbps	1,6,11	20 MHz
802.11a	5 GHz	54 Mbps	23	20 MHz
802.11n	2.4 GHz	300 Mbps	1,6,11	20 MHz, 40 MHz
	5 GHz	450 Mbps	23	
802.11ac	5 GHz	900+ Mbps	23	20 MHz, 40 MHz 80 MHz, 160 MHz

*Non-overlapping channels

Table 1-14 TCP vs UDP Comparison

TCP	UDP
transport layer	transport layer
connection	connectionless
flow control	no flow control
error recovery	error check / discard
slower	faster
TCP window size	no windowing
guaranteed delivery	best effort
ordered data	unordered data
retransmission	no retransmission
HTTP, Telnet, SSH, FTP	DHCP, SNMP, VoIP, Video

TCP Handshake

TCP-based applications require a three-way handshake for host-to-server connectivity. The following describes the exchange of messages.

1. host sends TCP SYN message to server with bit set.
2. server sends TCP SYN/ACK message to host with bit set for both.
3. host sends message to server with TCP ACK bit set .

Table 1-15 Application Ports

Application	Port
Telnet	TCP 23
SMTP	TCP 25
FTP	TCP 21
HTTP	TCP 80
SNMP	UDP 161
DNS	TCP 53 | UDP 53
HTTPS	TCP 443
SSH	TCP 22
TFTP	UDP 69

Switching Concepts

The primary purpose of a switch is to make forwarding decisions based on a destination MAC address. The MAC address table is created with a list of MAC addresses for each connected device, switch port and VLAN membership. The newer Gigabit Ethernet ports are full-duplex and define a single collision domain per switch port.

The following is a list of network services provided by switches:

- Switches only read Ethernet frame header and forward traffic.
- Switches create and maintain the MAC address table.
- Switches create separate collision domains per Gigabit port.
- Switches create separate broadcast domains per VLAN.

The Gigabit Ethernet (or faster) switch port supports full-duplex traffic between the host and network switch. That eliminates collisions and creates a collision domain per port. The fact that there are no collisions increases data rate and decreases network latency for host connections.

Microsegmentation

Gigabit Ethernet switch port interfaces enable both full-duplex operation and microsegmentation. That eliminates collisions on the switch port and dedicates all port bandwidth to the connected host. CSMA/CD is a method for detecting Ethernet collisions on older hubs and bridges. It is no longer required with full-duplex switch ports.

VLAN creates a broadcast domain that is defined by assigning switch port/s to the same VLAN. All hosts connected to assigned switch ports are part of the same broadcast domain. Creating multiple VLANs will then define multiple broadcast domains. Switches do not forward broadcast or multicast traffic between VLANs minimizing bandwidth utilization.

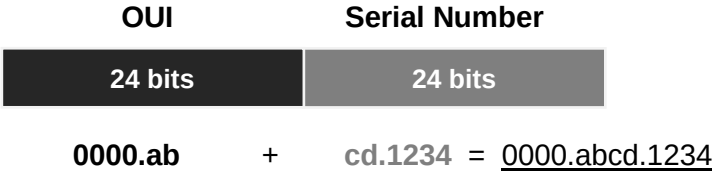
MAC Address Table

Every Ethernet network interface is assigned a unique manufacturer assigned physical hardware address called a MAC address. In addition, there is a MAC address assigned to all network devices. The MAC address provides a unique Layer 2 identifier. That enables communication between devices of the same or different VLAN. The switch forwards frames based on the MAC address and assigned port.

- Enable data forwarding between hosts in the same VLAN.
- Unique identifier associated with a network device or interface.

MAC (physical) address is 48 bits of hexadecimal numbers. The first 24 bits is a manufacturer OUI and the last 24 bits is a unique serial number (SN). There is a base MAC address assigned to each network device and unique MAC address per Ethernet interface.

Figure 2-1 MAC Physical Address



The switch builds a MAC address table comprised of MAC address, switch port and VLAN membership for each connected host. The switch creates a separate MAC address table for each configured VLAN. Any unicast flooding of a frame to learn a MAC address is for the assigned VLAN only. The following IOS show command will list the contents of the MAC address table for a switch. Where there are multiple VLANs configured, the switch will list all MAC address tables for all VLANs in a single table listing.

switch# **show mac address-table**

MAC Address Lookup

All hosts and network devices have MAC addressing that is used for Layer 2 connectivity. Each data message contains a frame with both source and destination MAC address. The host sending data is the source MAC address. The destination MAC address is the Layer 3 next hop. The switch builds a MAC address table with MAC addresses, assigned switch port and VLAN membership.

Layer 2 network switches does not rewrite the frame header MAC addressing. It examines the source MAC address and destination MAC address. The source MAC address and associated port is added to the MAC address table if it isn't listed. The switch then does a lookup of the destination MAC address.in the MAC address table to makes a forwarding decision. The frame is forwarded out the switch port associated with the destination MAC address.

Broadcast Frame

The host first sends an ARP request packet to learn the MAC address of a server. That occurs whether they are assigned to the same VLAN or different VLANs (subnets). Layer 2 broadcast frames are created by switches for the purpose of sending an ARP request and are not learned from inbound switch port. The switch creates a broadcast frame using **FFFF.FFFF.FFFF** as the destination MAC address. The broadcast frame is forwarded out of all switch ports and ends up at the default gateway. ARP request is then sent from the default gateway (router or L3 switch) to learn MAC address of server.

MAC Learning and Aging

MAC address learning occurs when the destination MAC address is not in the MAC address table. MAC learning is triggered as well when the aging time expires for an address. The switch removes MAC address table entries every 300 seconds as a default. Configuring the MAC aging timer to zero disables aging of MAC addresses. The switch will unicast flood a frame to update the MAC address table.

MAC Flooding

The host sends packets with an IP header encapsulated in a frame. The source and destination IP address are required for end-to-end connectivity. Layer 2 switch does not examine or understand IP addressing. They can only examine Layer 2 frame within a data message for source and destination MAC address.

The following summarizes what happens when a host sends data to a server.

1. The switch adds the source MAC address of the incoming frame if it is not listed in the MAC address table. That is a destination MAC address for any frames destined for that host.

2. The switch does a MAC address table lookup for the server destination MAC address.

3. The switch floods the frame out of all switch ports except the port where the source MAC address was learned. This only occurs when the destination MAC address is not in the MAC address table.

4. The server with the matching destination MAC address responds to the switch with a frame.

5. The switch then updates MAC address table with MAC address of server. .

Broadcast Domain

The VLAN creates a broadcast domain that is defined by assigning switch port/s to the same VLAN. All hosts connected to switch ports of the same VLAN are part of the same broadcast domain. Creating multiple VLANs defines multiple broadcast domains. Switches do not forward broadcast or multicast traffic between VLANs minimizing bandwidth utilization compared with hubs and bridges. The switch only forwards unicasts, broadcasts and multicasts on the same segment (VLAN).

Figure 2-2 Layer 2 and Layer 3 Broadcast Domains

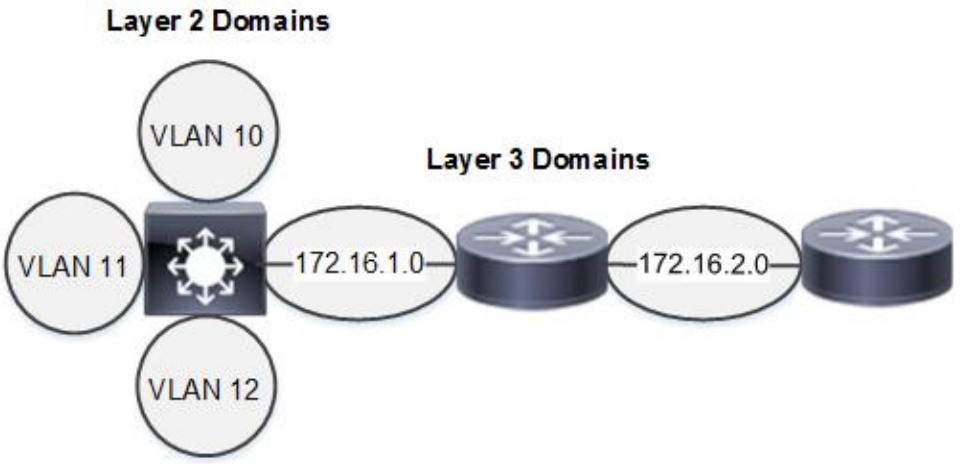


Table 2-1 Network Broadcasts

Broadcast Type	Destination Address	Examples
Layer 2	FFFF.FFFF.FFFF	ARP requests
Layer 3	255.255.255.255	DHCP, subnet only
Multicast	Reserved IP address	CDP, routing protocols

Cut-Through Switching

This switching technique optimizes performance by examining only the first six bytes (destination MAC address) of an Ethernet frame before making a forwarding decision. The switch does a MAC address table lookup for the destination MAC address and forwards the frame. The advantage is forwarding decision is made before all of the frame arrives and thereby minimizes latency.

Store-and-Forward Switching

The store-and-forward method is traditional switching where the frame is not forwarded until all of the frame has arrived. The switch copies the frame to memory before examining the destination MAC address.

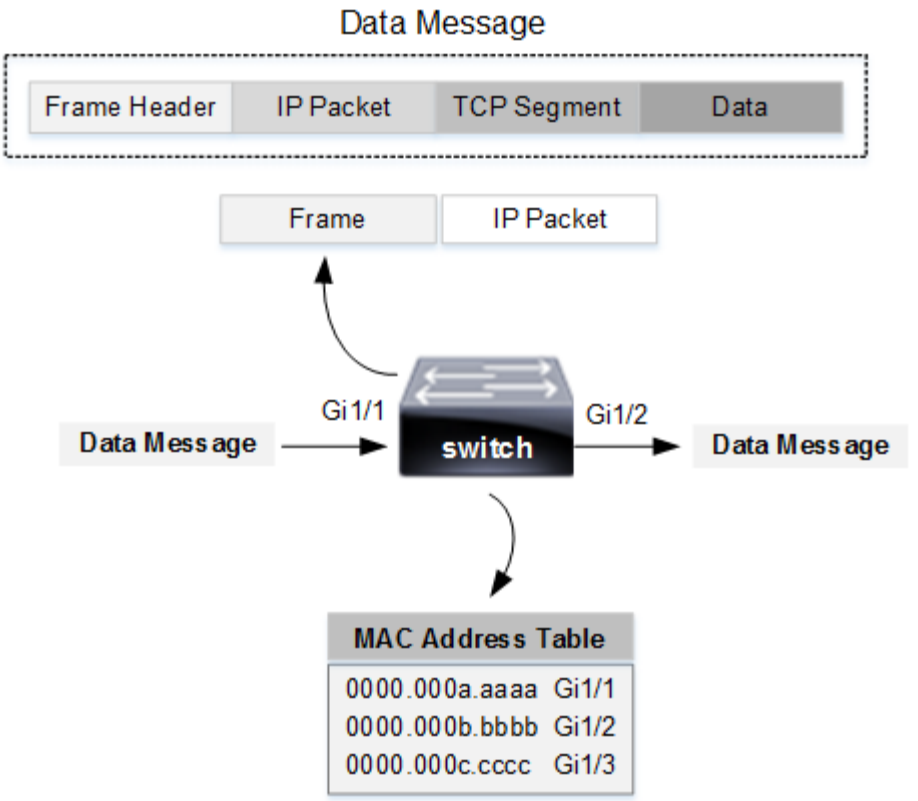
Cisco Express Forwarding (CEF)

CEF is a layer 3 switching technique that creates FIB and adjacency tables for optimized forwarding. It is only available on routers and switch platforms with routing enabled and the required hardware.

Frame Switching

Layer 2 switches only read the frame header within a data message to make a forwarding decision.

Figure 2-3 Frame Switching Operation



The switch examines the frame header for the destination MAC address and does a MAC address table lookup to make a forwarding decision. The frame is then forwarded out the switch port associated with the destination MAC address where the host is connected.

- Switches use MAC address in a frame to make forwarding decisions.
- Switches forward frames and do not frame rewrite MAC addressing.

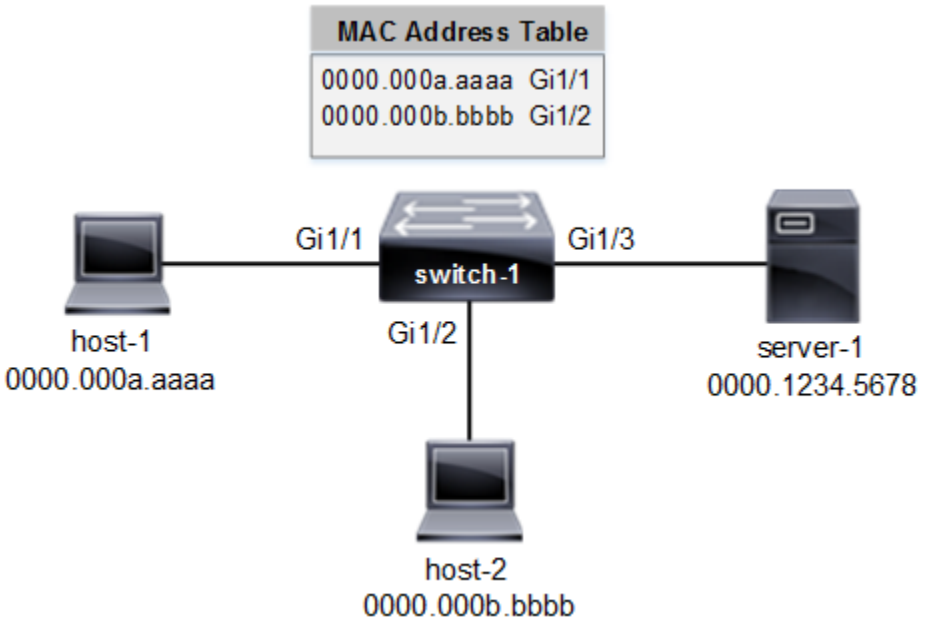
Switches and access points make forwarding decisions based on the destination MAC address in a frame. They do not rewrite MAC addressing in the frame header. **It is only routers, Layer 3 switches and WLC that do frame rewrite.** Wireless access points are essentially bridges that examine source and destination MAC address. The source MAC address of incoming frame is added to the MAC address table if it is not listed.

Frame Switching Examples

Example 1

Refer to the network drawing where host-1 is sending data to server-1. The destination MAC address is not in the MAC address table (unknown). The switch will unicast flood (learning) the frame out all ports except the port where the frame was learned from (Gi1/1).

Figure 2-4 Frame Switching Example



Server-1 with the matching destination MAC address receives the frame and sends a frame to switch-1. The switch then updates MAC address table with the MAC address of server-1 and associated port (Gi1/3).

Example 2

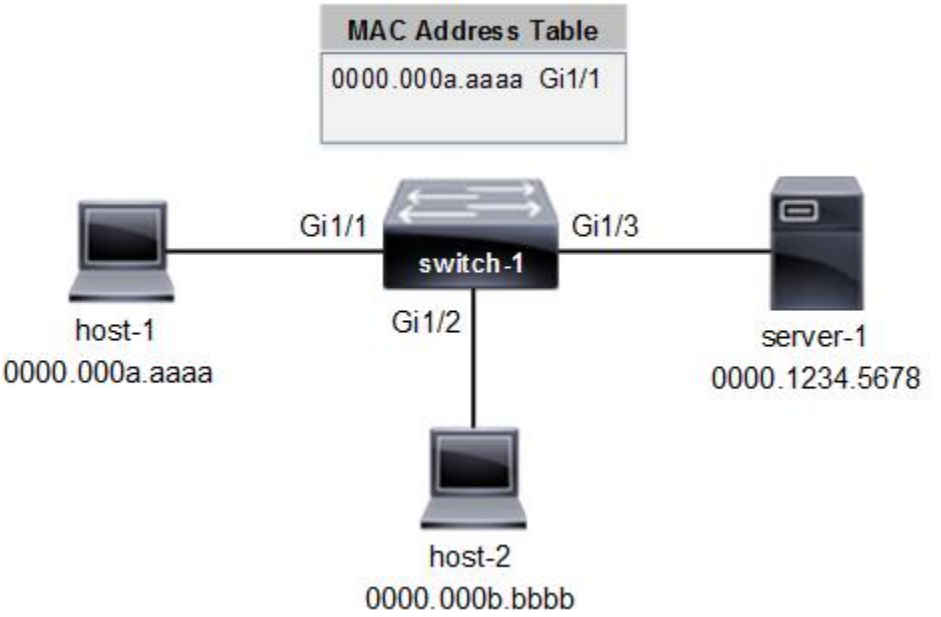
Refer to the network drawing where host-2 is sending data to server-1. The switch will examine the source and destination MAC address of the frame arriving on port Gi1/2 from host-2. The MAC address table has no entry for either source or destination MAC address.

The switch will then add the source MAC address (host-2) to the MAC table. In addition the switch will unicast flood (MAC learning) a frame out all ports except the port where the frame was learned (Gi1/2). That broadcast frame contains only a destination MAC address.

Server-1 with the matching destination MAC address receives the frame and sends a reply frame to the switch. The switch updates the MAC address table with the MAC address of server-1.

- 0000.000b.bbbb will be added to the MAC address table.
- Frame is forwarded out all active switch ports except port Gi1/2.

Figure 2-5 Frame Switching Example



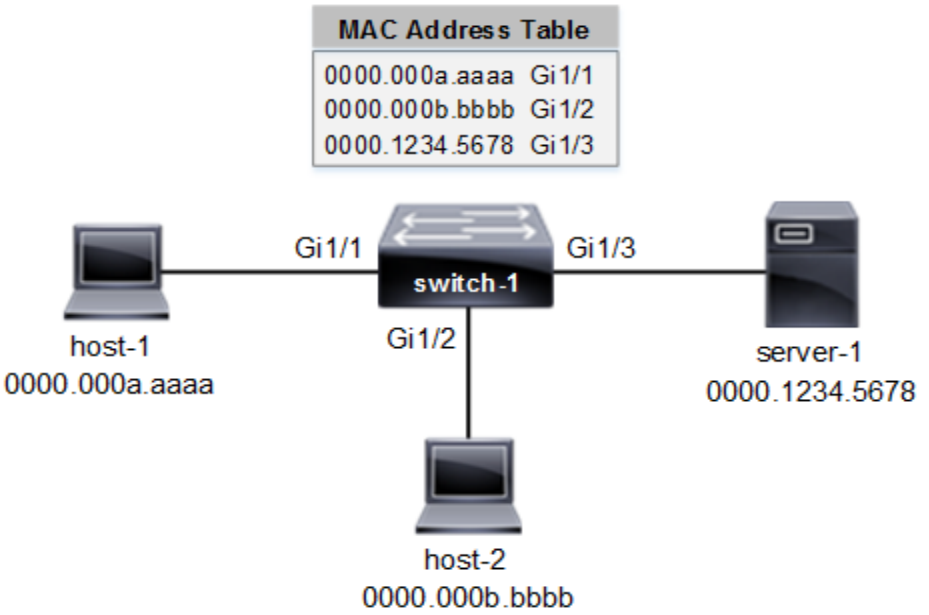
Example 3

Refer to the network drawing where host-2 is sending to data to server-1. In this example, switch-1 will examine the incoming frame from host-2 arriving on port Gi1/2. The switch will do a MAC table lookup based on the destination MAC address (0000.1234.5678).

The destination MAC address is assigned to server-1 and frame is forwarded out switch port Gi1/3 associated with server-1.

- Switch will examine the frame and do a MAC address table lookup.
- Frame is forwarded out switch port Gi1/3.

Figure 2-6 Frame Switching Example



Access Ports (data and voice)

Cisco switch ports supports access mode or trunk mode. The port mode is configured when enabling an interface. Layer 2 switch port is referred to as an access port unless trunk is enabled. Switch access ports that receives a packet with an 802.1q tag in the header will discard the packet without learning the source MAC address. The access port connects access devices such as a hosts, servers and wireless access points. The switch port can only be assigned one VLAN unless you are connecting an IP phone. The data VLAN and voice VLAN is permitted on an access port with the following configuration commands.

switch(config)# **interface fastethernet0/1**
switch(config-if)# **switchport mode access** *(configure access port mode)*
switch(config-if)# **switchport access vlan 9** *(assign vlan 9 to data traffic)*
switch(config-if)# **switchport voice vlan 10** *(assign vlan 10 to voice traffic)*

The following commands list all VLANs configured on a switch.

switch# **show vlan**
switch# **show vlan brief**

The following command is used to verify switch port/s assigned to a single VLAN.

switch# **show vlan id** [vlan]

Trunk Interface

The purpose of a switch trunk is to forward multiple VLANs between switches. The switch port must be configured for trunk mode to enable forwarding multiple VLANs. That allows communication between hosts assigned to the same VLAN spanning switches. Forwarding multiple VLANs across a switch link requires trunk mode to enable VLAN tagging feature. The following configures a switch trunk interface with native VLAN 999 and allow VLANs 10-12

```
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 999
switch(config-if)# switchport trunk allowed vlan 10-12
```

802.1q VLAN Tag

802.1q protocol has a 12 bit VLAN ID field used to identify VLAN membership of a frame. The switch adds a 4-byte tag to each Ethernet frame for VLAN membership. The Ethernet frame header is modified as a result of adding the VLAN tag. That requires recalculation of the FCS value used for CRC. Switch access ports that receives a packet with an 802.1q tag in the header will discard the packet without learning source MAC address.

- open standard for multi-vendor switch connectivity
- default setting for Cisco switches
- provide VLAN tagging across a switch trunk

Native VLAN

The native VLAN is used to forward control traffic across a switch trunk. Changing the native VLAN from VLAN 1 to any available nondefault VLAN is a Cisco security best practice. There are security vulnerabilities associated with the default VLAN 1. In addition STP issues are minimized by selecting a nondefault VLAN instead of VLAN 1. Control traffic (CDP, PAgP, VTP, STP and DTP) always uses VLAN 1 and travel on the native VLAN (untagged traffic) by default. The trunk tags all data VLANs for identification purposes. The untagged traffic is separated from data traffic as a result.

None of the control traffic except STP and DTP are forwarded across the native VLAN when the native VLAN is changed to a nondefault value. STP and DTP are management protocols that must be untagged across trunk links. The native VLAN configured on a trunk link must match between switches to forward untagged packets across the trunk correctly. STP and DTP can detect native VLAN mismatches.

VLAN Pruning

The purpose of VLAN pruning is to permit or deny VLANs across a switch trunk. The Cisco default is to allow all VLANs across the trunk. The local switch alerts the neighbor switch of all local VLANs that are not active (not configured). Any VLANs that are not configured are pruned by the neighbor switch to minimize unicast, broadcast and multicast traffic across the trunk. The Cisco default configuration is to allow all VLANs from the range 1 - 4094 across the trunk.

The network administrator can add or remove VLANs after that command is issued based on requirements. Specify multiple non-consecutive VLANs with commas or a hyphen to specify a range of consecutive VLANs. The following interface command **only allow** VLAN 10, VLAN 11 and VLAN 12 across trunk.

switch(config-if)# **switchport trunk allowed vlan 10-12**

The **add** | **remove** keyword only applies after pruning has already occurred on trunk interface to limit the initial default VLANs allowed from the range 1-4094.

switch(config-if)# **switchport trunk allowed vlan add** [vlan id, vlan id, ...]

The following interface command will remove VLAN 10 from the trunk. That will filter all traffic from that VLAN so it cannot traverse the trunk between switches.

switch(config-if)# **switchport trunk allowed vlan remove 10**

The following interface command will add VLAN 12 to the trunk interface. That permits all traffic from that VLAN so it can traverse the trunk between switches.

switch(config-if)# **switchport trunk allowed vlan add 12**

Dynamic Trunking Protocol

- DTP enables dynamic negotiation of a trunk between two switches
- DTP is Cisco proprietary protocol only
- DTP modes are **nonegotiate**, **desirable** and **auto**.
- DTP **auto** mode is enabled by default on switch ports
- There is no trunk negotiated with the default DTP mode setting

DTP request frames are sent to the neighbor switch to negotiate the trunk setup. The switch port configured with **desirable** or **auto** mode listen for DTP requests. The switch port configured with **desirable** mode actively sends DTP frames to establish a trunk with neighbor switch.

DTP provides dynamic negotiation based on the mode setting where at least one of the interfaces is configured with **desirable** mode. The switch interface configured with **switchport mode trunk** is a static trunk with **on** mode.

The following describe the operation of each switch port configuration:

- switchport mode access = access port only (no trunk), disable DTP
- switchport mode trunk = trunk statically formed and no DTP frames sent
- switchport mode dynamic auto = listens for DTP requests
- switchport mode dynamic desirable = listens and sends DTP requests
- switchport nonegotiate = disable DTP

Table 2-2 Cisco DTP Trunk Modes

Switch-1	Switch-2	Result
auto mode (default)	auto mode (default)	access port
auto mode	desirable mode	trunk
auto mode	static (on)	trunk
desirable mode	static (on)	trunk
nonegotiate	nonegotiate	access port

Table 2-2 describes how switch modes affects trunk setup between switches. DTP **auto** mode supports access mode and trunk mode. The neighbor incoming negotiation would determine whether the switch port operation is access or trunk. The **nonegotiate** mode is configured on both switch interfaces that do not support DTP mode or should not establish trunking. DTP frames are sent at one second intervals during negotiation and every 30 seconds after that. The following are methods for disabling DTP on a switch interface:

- **switchport nonegotiate** command
- **switchport mode access** command

Normal/Extended VLANs

Cisco switch ports are assigned to VLAN 1 as a default configuration. VLAN 1 is used for management traffic and cannot be deleted. The normal range that include VLAN range 2 - 1001 can be added, modified or deleted from the switch. Cisco recommends assigning all data and voice traffic to a non-default VLAN.

Table 2-3 Normal/Extended VLANs

VLAN Range	Description
VLAN 1 – 1005	normal VLAN range
VLAN 1006 – 4094	extended VLAN range
VLAN 1, 1002 – 1005	auto-created and cannot be deleted
VLAN 1 - 4094	default VLAN range allowed on trunk

LACP EtherChannel

EtherChannel bundles multiple physical switch links between switches into a single logical **port channel** interface. The advantages of EtherChannel include redundancy and higher bandwidth between switches. For example, bundling 8 Gigabit ports creates a logical 8 Gbps port channel interface.

Table 2-4 EtherChannel Protocols (LAG)

LACP	**PAgP**
open standard (multivendor)	Cisco proprietary
bundle = 8 ports + 8 standby	bundle = 8 ports
passive mode (default)	auto mode (default)
active mode	desirable mode
any port active mode = etherchannel	any port desirable mode = etherchannel

LACP is an open standard that enables dynamic negotiation of an EtherChannel between Cisco switches and/or multivendor equipment. LACP modes include **active mode and passive mode.** LACP enables the configuration of up to 16 switch ports however only 8 ports can be active. Standby ports are operational only when primary port fails. The default port priority is 32768 and lowest port numbers are selected as active by default. The **lacp port-priority** interface command manually assigns port priority, so lowest priority ports become active. The interface is assigned to a channel group with **channel-group** command and a protocol mode. The port channel logical interface is assigned a number that matches channel group number. The speed, duplex and VLAN setting must match for all ports members assigned to an EtherChannel.

Configure LACP active mode on a switch port and assign to channel group 1.

```
switch(config)# interface gigabitethernet1/1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 10
switch(config-if)# duplex auto
switch(config-if)# speed auto
switch(config-if)# lacp port-priority 2000
switch(config-if)# channel-group 1 mode active
```

Designate a switch to select the local active ports for an EtherChannel.

```
switch(config)# lacp system-priority 2000
```

Spanning Tree Protocol

Spanning Tree is deployed to prevent Layer 2 loops and broadcast storms where frames are forwarded in a loop between switches. The most current STP protocol supports per VLAN instances (PVST+). Redundant topologies are characterized by multiple paths that could cause Layer 2 loops. STP forwards and block specific ports to eliminate forwarding loops between switches. Some possible problems that can occur when configuring redundant links between switches:

- multiple copies of unicast frames
- broadcast storm flooding
- MAC address table instability

STP creates a loop free Layer 2 topology by enabling some switch ports to forward traffic and some to block. That is based on electing a root bridge. The switch with the lowest bridge ID is elected root bridge. The bridge ID is comprised of priority setting and MAC address. STP calculates lowest path cost for each neighbor interface to the root bridge. The neighbor switch port that receives the best BPDU (least cost to the root bridge) is assigned root port for that switch.

BPDU is an STP message that is sent between switches. The hello timer setting is the interval between BPDU advertisements. The BPDU message contains STP information from the sending switch. That includes STP timers, root bridge ID, sender bridge ID and port (path) cost. The following are four STP port states defined with 802.1d original standard.

- blocking
- listening
- learning = populating MAC address table
- forwarding

The newer 802.1w (RSTP) standard is comprised of three port states. They include discarding, learning and forwarding. The discarding state is new and equivalent to the blocking and listening states of older 802.1d protocol. The single RSTP discarding state enables faster convergence. RPVST+ is based on RSTP and includes separate STP instances for each VLAN enabled on a switch.

Root Bridge Selection

The default priority of a Cisco switch is 32768. STP selects the root bridge (switch) with the lowest priority. The switch with the lowest bridge ID is elected when all switches have the same priority. The bridge ID is calculated from the priority setting and MAC address. The switch with the lowest MAC address becomes the root bridge as a result. Spanning Tree election assigns root bridge along with designated ports, root ports and alternate ports to neighbor switches.

The root port is a switch port on a neighbor switch that has the least cost path to the root bridge. It is a primary forwarding link to the root bridge. STP operational status is available with **show spanning-tree summary** command.

PortFast

Spanning Tree Protocol (STP) enhancements are designed to optimize network convergence. The access layer connects hosts on single point-to-point connection where Layer 2 loops do not occur. PortFast is enabled on switch ports where hosts and wireless access points are connected. That allows the switch ports to transition from disabled or blocking state to forwarding state immediately on startup.

BPDU Guard

The purpose of BPDU guard is to err-disable (shutdown) an access switch port when BPDUs are received from a network device. BPDU guard is enabled on an access switch port where hosts or wireless devices connect. BPDU guard is configured on switch port to prevent devices from affecting the STP topology. Connecting a new switch to your cubicle jack would trigger an STP recalculation. The new switch is now connected to an access switch port causing a Layer 2 topology change notification. The result could include a new root bridge election.

Cisco Discovery Protocol (CDP)

CDP is a Layer 2 Cisco proprietary neighbor discovery protocol. Cisco IP phone appears to CDP as a unique neighbor device with an IP address. During bootup, the IP phone receives voice VLAN configuration from the access switch port.

- CDP is enabled by default both globally and on all network interfaces
- CDP update timer = 60 seconds (default)
- CDP is enabled globally by default on Cisco devices and interfaces
- CDP can be re-enabled CDP globally with **cdp run** global command
- CDP can be re-enabled per interface with **cdp enable** interface command

Link Layer Discovery Protocol (LLDP)

LLDP is an open standard network discovery protocol specified with IEEE 802.1ab standard for multi-vendor environments. The network devices share identity and functionality via LLDP and with neighbors.

- The default packet update interval for LLDP is 30 seconds.
- Network interfaces with LLDP enabled advertise default TLV attributes of chassis ID, port ID and TTL.
- Cisco IP phones are enabled for LLDP when LLDP packets are first sent from the phone to the switch.
- Global configuration command **lldp run** enables LLDP globally
- Interface level configuration command **lldp receive** enables an interface to receive LLDP packets.

IP Connectivity

Router Concepts

Routers are primarily responsible for logical addressing and best path selection between different subnets. Routers make forwarding decisions based on the destination subnet (prefix). The router will do a routing table lookup then rewrite the source and destination MAC address in the frame header.

They build a routing table with route entries comprised of route, metric and next hop address. The router selects the route based on longest match rule and forwards packets to the next hop router (neighbor). There is support for load balancing, flow control and error recovery as well. Each packet has a source IP address and destination IP address. The router does a routing table lookup for a route to the destination subnet. The packet is then forwarded to the next hop address associated with the selected route.

Routing Table Components

It is important to know how to read a routing table to verify that routing is working correctly. The routing table is generated by a router based on dynamically advertised routes (subnets) sent from neighbors. All locally connected routes and static routes are included as well. The directly connected route is a subnet based on the IP address assigned to a local interface. It is automatically added to the routing table when the interface is enabled. The local interface associated with the subnet (route) is the exit interface for packets destined to that subnet. Static routes including default and floating static routes are manually configured. All routing tables are comprised of the following components.

1. Routing protocol code is the route source.
2. Network address is the destination subnet.
3. Administrative distance is trustworthiness of the route source.
4. Metric is the calculated path cost to the destination subnet.
5. Next hop is the IP address of a neighbor in the forwarding path.
6. Local interface is the exit interface to the next hop address.
7. Age is the amount of time the route has been installed.

router# **show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

172.16.0.0/24 is subnetted, 3 subnets, 2 masks
C 172.16.1.0/24 is directly connected, Serial0/0
C 172.16.3.128/27 is directly connected, GigabitEthernet0/0
192.168.25.0/30 is subnetted, 2 subnets
O 192.168.2.1/24 [110/11] via 192.168.2.2, 00:01:12, Serial0/2
O 192.168.3.64/30 [110/15] via 192.168.1.65, 00:00:9,Serial0/3
S* 0.0.0.0/0 [1/0] via 172.16.0.1

Routing Protocol Code

The protocol code assigned to a route signifies the source where the route was learned. It is either a dynamic route, static route or connected route. The output of **show ip route** command displays the routing table.

Table 3-1 Routing Protocol Codes

Route Source	Protocol Code
OSPF	O
OSPF Inter-Area	IA
EGP	E
EIGRP	D
Static Route	S
Default Route	S*
Connected Route	C
Host (/32)	L

Network Address

This is the network address of a destination subnet for a routing entry. It is referred to as a prefix in the routing table. Each IP packet has an address field for source IP address and destination IP address. They do not change between endpoints. They are host addresses assigned to network interfaces. You cannot assign a network address or broadcast address to a network interface. The router examines destination IP address field of an inbound packet to learn the destination subnet. It then selects a route in the routing table to forward packets.

Administrative Distance

This is the reliability of a route when compared with other route sources. Each route type is assigned an administrative distance (AD). It is a value used by the router for route selection. The route with lowest AD number is installed when routes are advertised from multiple routing protocols .

Metric

This is a value that is assigned to each route that is calculated based on the route type. Metric is only considered for best path selection only when multiple routes exist from the same routing protocol. Each routing protocol calculated metric differently. OSPF is based on path cost or link bandwidth. RIPv2 use hop count (number of hops) between endpoints.

Next Hop Address

There is a next hop address associated with each route for packet forwarding purposes. It is IP address of a connected neighbor interface. All routing decisions are made per hop on a forwarding path. The router logic reads as - *to reach this destination subnet, forward packet out local interface that is connected to next hop neighbor with this IP address.*

Local Interface

Each route entry is associated with a local interface and next hop address used for packet forwarding. The local exit interface associated with that route is connected to next hop neighbor for packets that are destined to a subnet. The router is only concerned with identifying local exit interface to use for packet forwarding.

Age

The route entry has an associated age (min) that is based on the amount of time in the routing table. The route entry starts at zero when first learned and is reset if the table is flushed.

Example

This is an OSPF route entry from a routing table with each component defined. For example, 192.168.12.9 is the destination IP address in the IP header. It is a host address and not a network (subnet) address.

O 192.168.12.8/30 [110/128] via 192.168.12.5, 00:35:36, Serial0/0

- Routing protocol code = O (OSPF)
- Destination subnet = 192.168.12.8/30
- Administrative distance = 110
- Metric = 128
- Next hop address = 192.168.12.5
- Local exit interface = Serial0/0
- Age = 00:35:36

ARP Operation

ARP is a network protocol that resolves a known IP address to an unknown MAC address. The local host must know the MAC address of the remote host before packets can be sent. The host sends an ARP request to the default gateway if there is no local ARP entry. The default gateway (router) sends a proxy ARP broadcast and returns the MAC address for a server to the host. The switches note the server MAC address as well and update their MAC address table.

Frame Rewrite

The source and destination MAC address are updated by routers as frames are forwarded between routers. The source MAC address is the router egress interface and destination MAC address is the neighbor ingress interface. The forwarding decisions for routers are based on destination IP address and not destination MAC address. The source and destination IP address do not change between source and destination hosts. Any Layer 3 device such as a host or a router will write an IP header to create a packet with the source IP address and destination IP address.

Time-to-Live (TTL)

The IP header has a field called Time-to-Live (TTL) that has a default value of 255. The purpose of TTL is to prevent packets from infinitely looping as a result of a routing loop. The TTL field is decremented by one with each router hop. That guarantees the packet will be discarded after 255 hops.

Route Selection

The router selects routes to install in the routing table. Sometimes there are multiple routes advertised from multiple routing protocols to the same destination. The administrative distance of a route determines the route installed in the routing table.

The metric is used to select best path to a destination when multiple paths exist. Metric only applies when there are multiple routes from the same routing protocol to the same destination. The longest match rule selects the route with the longest subnet mask (prefix) from routes already in the routing table.

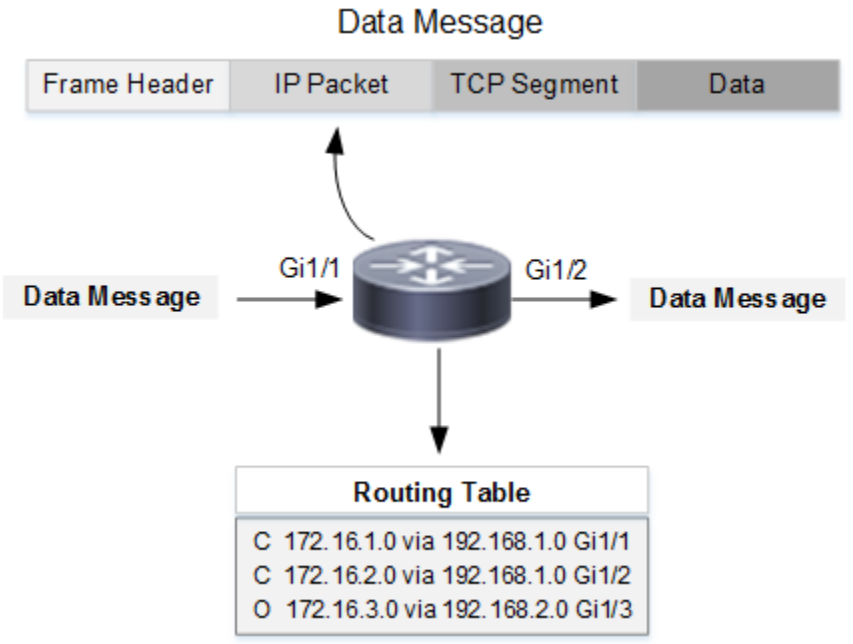
Step 1: Install route = lowest administrative distance

Step 2: Install route = lowest metric (same routing protocol)

Step 3: Select route = longest match rule (subnet mask)

Step 4: Packet discarded when no default route exists

Figure 3-1 Routing Table Lookup



Administrative Distance

The router builds a routing table with multiple routes (prefixes). Each route type is assigned an administrative distance and calculates a metric. The administrative distance (AD) is a value based on the routing protocol or route source. It is used by routers to select what route is installed in the routing table. The administrative distance and metric assigned to a route will determine what route is installed in the routing table.

The router installs the route with the lowest administrative distance. It is considered when multiple routes exist from multiple routing protocols to the same destination. Administrative distance is configurable to influence route selection.

The route with the lowest AD is considered the most reliable (trustworthy). Directly connected routes have the lowest administrative distance (0) and are the most reliable. The directly connected route is a subnet based on the IP address assigned to a local interface. It is automatically added to the routing table when the interface is enabled.

The following are the default administrative distances for each routing protocol and/or route type. Each routing entry in the routing table includes the administrative distance and metric in brackets [AD / Metric].

Table 3-2 Administrative Distance (AD)

Route Type	Administrative Distance
Directly Connected	0
Static Route	1
Default Route	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIPv2	120
iBGP	200
Unknown	255

Example

What is the administrative distance of the route to destination network 192.168.3.0/24?

router# **show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.33.0.1 to network 0.0.0.0

10.1.0.0/24 is subnetted, 5 subnets
C 10.1.0.0 is directly connected, Serial0/0
C 10.1.5.0 is directly connected, GigabitEthernet0/1
C 10.1.6.0 is directly connected, GigabitEthernet0/0
C 10.1.7.0 is directly connected, Serial0/1
C 10.1.254.0 is directly connected, Loopback0
O 192.168.3.0/24 [110/64] via 192.168.1.1, Serial0/0

The command lists all network prefixes to subnet destinations. The router would select the following route to destination subnet 192.168.3.0/24.

O 192.168.3.0/24 [**110**/64] via 192.168.1.1, Serial0/0

OSPF route with next hop 192.168.1.1 has an administrative distance of 110 and metric calculation of 64. Any route assigned an administrative distance of 255 is not installed into the routing table. The router doesn't trust the source of the route and considers it untrustworthy. The local exit interface is Serial0/0 where packets are forwarded to next hop neighbor.

Example: Dynamic Routing Protocols

EIGRP, OSPF and RIPv2 are advertising routes to the same destination. What route is selected based on the following information?

EIGRP = [90/1252335]

OSPF = [110/10]

RIPv2 = [120/3]

The route with lowest administrative distance is installed in the routing table. EIGRP (90) has a lower administrative distance than OSPF (110) or RIPv2 (120). The result is that EIGRP route is installed in the local routing table.

The metric is only considered for best path calculation when multiple routes exist for the same routing protocol to same destination.

Example: Static Route

The following route types are advertising routes to the same destination. What route is selected based on the following information?

OSPF = [110/27]

Static = [1/0]

Default = [1/0]

All routing sources are advertising a route to the same destination subnet. The route with the lowest administrative distance (AD) is installed in the routing table. In this example, static route and default route have same lowest AD = 1. The router would select the static route since it is always more specific than a default route.

Example: Connected Route

The following route types are advertising routes to the same destination. What route is selected based on the following information?

Static Route = 172.16.1.0/27

Default Route = 172.16.1.0/27

Connected Route = 172.16.1.0/27

The directly connected route, with AD of zero (0) is considered most reliable route to a destination. The subnet length is only considered when selecting from multiple routes to the same destination already installed in the routing table. It is referred to as longest match rule.

Example: Multiple Route Sources

What route is installed in the routing table from the following routes?

OSPF Route = 172.16.1.0/27

Static Route = 172.16.1.0/27

Default Route = 172.16.1.0/28

Connected Route = 172.16.1.0/29

This example includes a dynamic route (OSPF), static routes and a connected route. The route with lowest administrative distance is the connected route. Each route however has a different subnet mask length, and the router considers them routes to different destinations. All routes are installed in the routing table and administrative distance value is not relevant here.

Packet Forwarding

The longest match rule is used to **select a route already installed in the routing table** as a forwarding decision. Each route has a specific prefix (subnet mask) length. The route with the longest prefix is selected from multiple routes within the same subnet range (destination). For example, 172.16.0.0/22 has a longer prefix than 172.16.0.0/18 and would be selected to forward packets to 172.16.0.0 subnet destination.

Example 1: Longest Match Rule

Refer to the routing table. Where will router-1 send packets that have destination IP address of 172.16.1.1?

router-1# **show ip route**

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

172.16.0.0/24 is subnetted, 3 subnets, 3 masks
C 172.16.1.0/25 is directly connected, Serial0/1
C 172.16.1.0/26 is directly connected, Serial0/1
C 172.16.1.0/27 is directly connected, GigabitEthernet0/0
172.16.254.0/24 is subnetted, 1 subnet

The longest match rule is used to select a route already installed in the routing table as a forwarding decision. Each route to a destination has a specific network prefix (subnet mask) length. The route with the longest subnet prefix is selected from multiple routes to the same destination. For example, 172.16.1.0/27 has a longer prefix than 172.16.1.0/26 and 172.16.1.0/25. As a result, that route prefix is selected for packets with 172.16.1.1 destination IP address.

Example 2: Longest Match Rule

What route is selected for destination IP address 192.168.1.10?

A. 192.168.1.0/28

B. 192.168.1.0/26

C. 192.168.1.0/25

D. 192.168.1.0/27

Answer (A)

The longest match rule would select 192.168.1.0/28 route to destination IP address 192.168.1.10. The packet is forwarded to the next hop and local exit interface associated with the routing entry for that route.

Packet Discard

The router does a lookup for any route to the destination subnet that exists in the routing table. That includes any dynamic, static, default or directly connected route. The packet is discarded when no route exists and a destination unreachable ICMP message is sent to the host.

IPv4 and IPv6 Static Routing

Dynamic Route

There are various routing protocols designed to exchange route information with neighbors. The network administrator does not configure dynamic routes. They are learned so that each router installs and selects routes for best path selection.

Connected Route

Connected routes (subnet prefixes) are added based on local network interface addressing. The router installs a corresponding local host route (/32) as well for each connected interface.

IPv4 Static Route

The static route is more specific than a default route. The static route says – *to reach destination subnet 172.16.1.0/24 forward packets to next hop address 172.16.12.1 or exit interface Serial0/1*. Static routes are required at both routers as well to route (forward) in both directions when no routing protocols are enabled. The advantages are added security with manual routes and less advertisements when compared with dynamic routing protocols.

router(config)# **ip route 172.16.1.0 255.255.255.0 172.16.12.1**
router(config)# **ip route 172.16.1.0 255.255.255.0 Serial0/1**

IPv4 Floating Static Route

The static route configured with a higher administrative distance than a dynamic route or static route is a floating static route. It is installed in the routing table only when the currently selected route is not available. That could result from a link failure for example. The floating static route is typically configured to forward traffic across a backup link. The static route has a lower administrative distance compared with the floating static route and selected as the primary route.
The floating static route with the higher administrative distance **200** becomes active only when the primary static route is not available.

router(config)# **ip route 192.168.3.0 255.255.255.0 192.168.2**.1 **200**

IPv4 Default Route

The default route is referred to as gateway of last resort packet forwarding. Any route, where no match exists, is forwarded to the next hop IP address specified with the default route. The default route says – *forward all traffic to next hop address of 172.16.1.1 when no route to the destination exists in the routing table*. The default route is often configured to forward packets to the internet.

In addition they minimize route advertisements when compared with dynamic routes. The administrative distance of default and static routes is one.

router(config)# **ip route 0.0.0.0 0.0.0.0 172.16.1.1**

Default-Information Originate

The purpose of default-information originate is to advertise a default route to connected neighbors. There is a single route configured under a dynamic routing protocol. It is advertised to all neighbors that have the same routing protocol enabled. The traditional default route is configured locally on a router and used as a gateway of last resort. It is often deployed as a backup to a primary link.

IPv6 Static Routing

IPv6 static route to destination subnet 2001:DB8:3C4D:1::/64

router(config)# **ipv6 unicast-routing**
router(config)# **ipv6 route 2001:DB8:3C4D:1::/64 2001:DB8:3C4D:2::1**

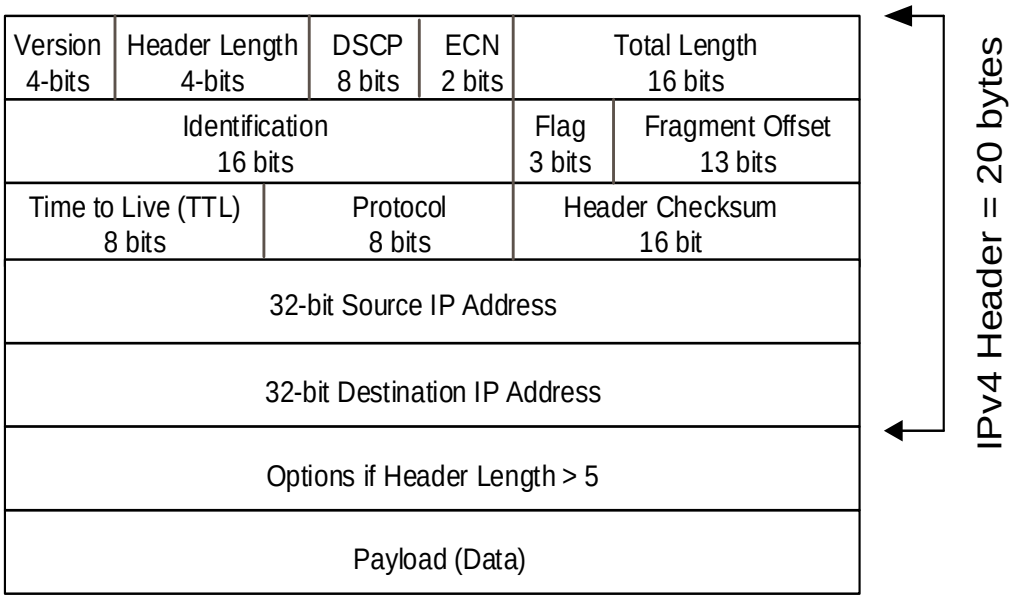
IPv6 default route with next hop of 2001:DB8:3C4D:2::1

router(config)# **ipv6 unicast-routing**
router(config)# **ipv6 route ::/0 2001:DB8:3C4D:2::1**

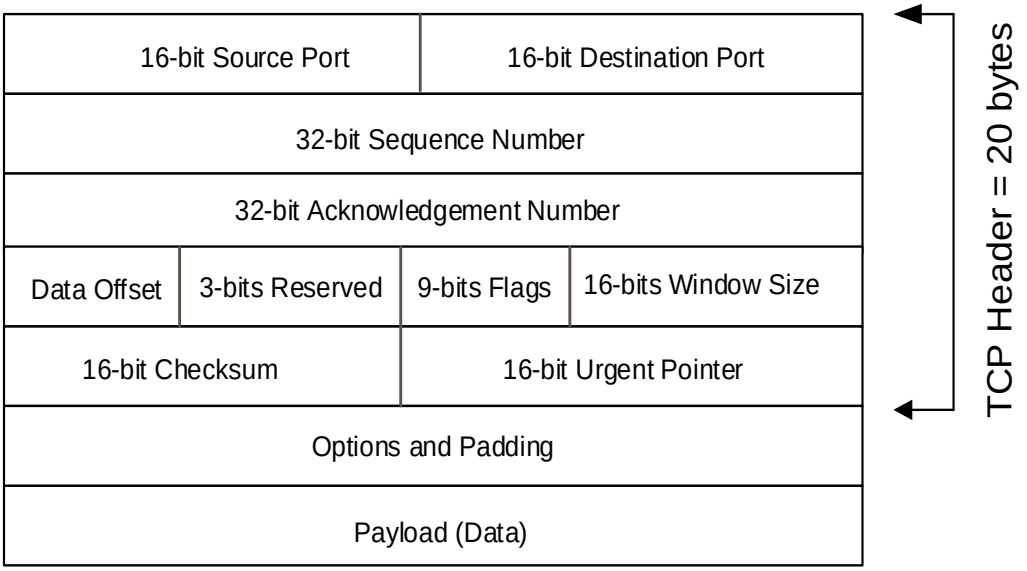
Table 3-3 IPv6 Route Type Examples

Route Type	Example
network prefix	/64
default route	ipv6 route ::/0 2001:DB8:3C4D:2::1
point-to-point address	/126
host route	/128
floating static	ipv6 route 2001:DB8::/32 Fa1/0 200
static route	ipv6 route 2001:DB8:3C4D::/64 Gi1/1
fully specified static	ipv6 route 2001:DB8:3C4D::/64 Gi1/1 FE80::2
host route	/128
directly connected static	ipv6 route 2001:DB8::/32 serial 1/0

IPv4 Packet



TCP Segment



OSPF Routing Protocol

There are various dynamic routing protocols that exchange route information with neighbors. The most popular include OSPF, EIGRP and BGP. Dynamic routes are learned and not configured, so each router installs and selects routes for best path selection. The distinction between each routing protocol is how they learn, update and advertise routes between neighbors.

OSPF is a link-state routing protocol that builds and maintains a global topology database. That is accomplished with the exchange of link-state advertisements (LSA) between OSPF routers. Topology and routing information is communicated to OSPF neighbors in LSAs. There are event-triggered updates that are sent only when a link failure occurs to conserve bandwidth.

OSPF Characteristics

- Link-state routing protocol
- Metric = link cost (bandwidth)
- Global view database topology table
- Shortest path to destination calculated
- Event-triggered routing updates
- Auto-summary disabled (default)
- Scalable to large enterprise domains
- Fast convergence when there is link failure
- Load balancing across four equal paths

OSPF is characterized by well-defined hierarchical layers that enable route summarization and smaller routing tables per router. The routing updates are minimized when there are link failures enabling faster convergence. In addition routing issues such as flapping and routing loops are limited to an OSPF area.

There is a mandatory common backbone area 0 for multi-area OSPF only. All other areas must connect to the OSPF backbone area. That is required to advertise routes between areas. OSPFv2 refers to the version of OSPF that only supports IPv4 addressing on network interfaces. It is the most widely deployed version of OSPF for dynamic routing. The area number for single-area OSPF does **not** have to be numbered area 0.

OSPF is an **IP-only** routing protocol that is well suited to current intranet and internet connectivity. Consider as well that internet and cloud-based services are IP-only connections. The single-area OSPF design reduces the routing tables and number of LSAs (routes) advertised between routers.

OSPF Neighbor Adjacency

The purpose of OSPF hello packets are to discover neighbors and establish neighbor adjacency. Hello packets are sent to maintain neighbor relationships as well, and confirm that a neighbor is still active. OSPF routers establish adjacency with all connected neighbors for bidirectional communication. That enables all routers to synchronize database and routing tables.

Adjacency States

The following describe the sequence of OSPF states required to establish neighbor adjacency and exchange routing tables.

1. **Down** - No hello packets have been received from neighbor/s.

2. **Attempt** - NBMA routers only. Hello packet has not been received from NBMA neighbor. Hello packet is sent to neighbor.

3. **Init** - Hello packet is received from neighbor without the router ID listed. There are settings such as timers verified to match.

4. **Two-Way** - Hello packets are sent between neighbor with router ID of local router. Neighbor adjacency is established and DR/BDR election occurs based on highest router ID.

5. **Exstart** - OSPF elected DR router starts exchanging LSAs with neighbors. The router with highest router ID remains DR unless priority was modified to influence selected router.

6. **Exchange** - Routers exchange database descriptor packets (DBD) and manage database synchronization to neighbor/s.

7. **Loading** - Routers complete exchange of all routes between neighbors.

8. **Full** - This is normal state where adjacency is established between OSPF neighbors and tables are updated for convergence.

There is a hello timer configured to send hello packets between routers at fixed intervals. All timers must match between directly connected neighbor interfaces. OSPF neighbor adjacency is not formed when there is a timer mismatch . The following are additional reasons why OSPF neighbor adjacency would not occur.

- Subnet mismatch
- Network type mismatch
- Timers mismatch
- MTU mismatch
- Area ID mismatch

Metric Calculation

Each routing protocol has a unique method for calculating route metric (cost). OSPF calculates cost based on interface bandwidth. The default cost of an OSPF enabled interface = 1 (100 Mbps / 100 Mbps).

interface cost = 100 Mbps / interface bandwidth

Each link is comprised of the local interface and a neighbor interface. The lowest cost assignable to a link is 1 even though calculation could arrive at a lower number. The reference bandwidth of OSPF is configurable to account for faster Ethernet interfaces that start at Gigabit (1000 Mbps) speed today. The reference bandwidth is a global configuration command that must match for all routers in the same OSPF routing domain.

router ospf 1
auto-cost reference-bandwidth 1000

The alternative to reference bandwidth method is **ip ospf cost** command. It allows you to configure the cost directly on a network interface. The third option is to manually configure interface speed with the IOS interface **bandwidth** command. That would affect how OSPF calculates metric for that specific link. You would have to configure the bandwidth command on both local and neighbor interfaces.

OSPF Hello Packets

OSPF hello packets establish neighbor adjacencies and maintain neighbor relationships. It also detects the operational status of neighbors and notifies router when there is a link failure. The following configuration settings are advertised in each OSPF hello packet to all connected neighbors.

- Hello and dead timer
- Router priority
- DR/BDR assigned
- Area assigned to neighbor interface
- Subnet mask of neighbor interface
- OSPF Authentication method
- OSPF network type

OSPF Router ID

OSPF routers must be assigned a router ID that is a unique identifier to all connected OSPF neighbors. The router ID is advertised in routing updates to identify where updates originated. Cisco default OSPF configuration has no router ID assigned. The following commands configure a router ID from router configuration mode.

```
router ospf 1
router-id 192.168.255.1
```

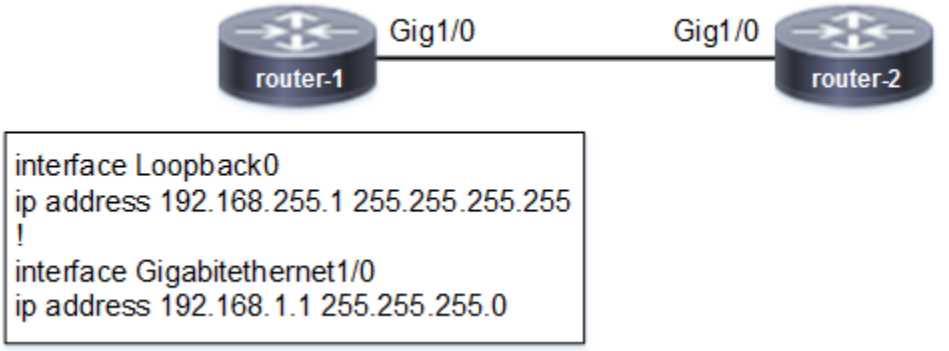
OSPF Router ID Selection

1. Unique 32-bit IPv4 dotted-decimal address.
2. Purpose is to identify each router for routing updates and adjacency.
3. Manually configured router ID is preferred first.
4. The highest IP address on a loopback interface is assigned when no router ID is configured.
5. The highest IP address of any active physical interface is assigned if no loopback interface exists.

Example: Router ID

Refer to the network topology drawing and determine what router ID is assigned for router-1?

Figure 3-2 Router ID Configuration



There is no manually configured router ID on router-1. Based on OSPF rules, the highest loopback interface address configured is assigned as router ID. OSPF borrows the IP address only and has no effect on loopback interface operation.

Table 3-4 OSPF Packet Types

Packet Type	Description
Hello	neighbor discovery, adjacency, and status
Database Descriptor	send database table update to neighbor
Link-State Request	LSA request for updates sent to neighbors
Link-State Update	flooding LSA (route) updates to neighbors
Link-State ACK	acknowledge LSA update from neighbor

OSPF Designated Router

OSPF designated router (DR) advertises routing updates to all connected spokes on a shared (broadcast) network. The most common example of a broadcast network type is Ethernet. OSPF DR minimizes routing updates between OSPF neighbors on a broadcast network. It is a hub router that advertises routing updates via 224.0.0.5 multicast address. Consider that a network broadcast segment refers to a common subnet or VLAN.

Designated Router (DR) Election

1. Router default OSPF priority = 1
2. Router with highest configured OSPF priority is elected DR
3. Router with highest router ID address is elected DR when priorities are equal. First preference is an explicitly configured router ID.
4. When no router ID is explicitly configured, the highest loopback address is assigned as router ID for a router. DR election then compares that router ID with neighbors for DR election.
5. Router assigns the highest physical interface address as router ID for OSPF when no loopback interface exists. DR election then compares that router ID with neighbors for DR election.
6. Router with second highest priority is elected BDR.
7. Router with second highest router ID is elected BDR.

All OSPF routers send routing updates via 224.0.0.6 multicast address to DR and BDR routers. The Cisco OSPF priority setting on a default router configuration has a value of 1. That is assigned to an OSPF enabled interface. The router priority is configurable to influence DR election.

Backup Designated Router

OSPF elects Backup Designated Router (BDR) on each broadcast domain. The purpose of BDR is to provide failover or redundancy to the elected DR. All routing updates from connected non-DR and non-BDR routers called spokes, are sent to the DR. The same routing updates are also sent to the elected BDR. The difference is that BDR never sends updates to spoke routers. That is only done from the elected DR as shown with Figure 3-19. Anytime there is a DR failure, then BDR is automatically assigned as DR for that subnet or VLAN.

Figure 3-3 OSPF DR/BDR Operation

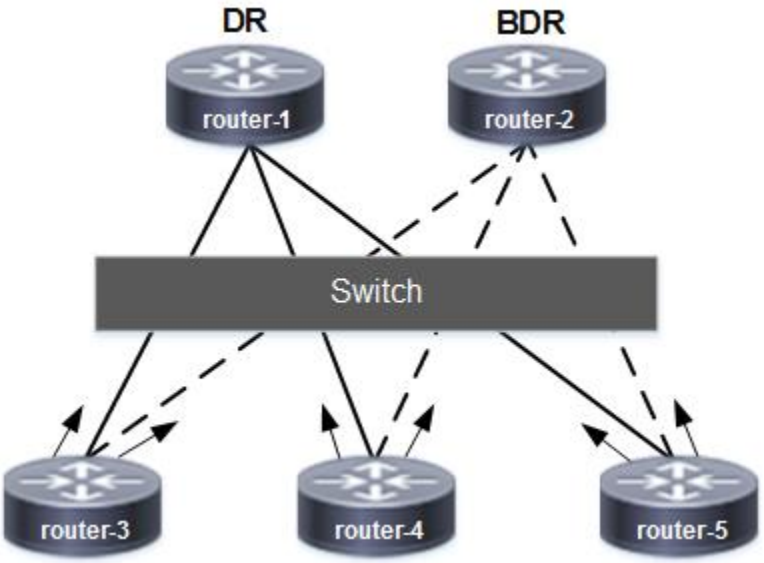


Table 3-5 OSPF Neighbor States

Neighbor State	Adjacency	DR Relationship	Description
Full/DR	FULL	Neighbor is DR	Neighbor_ID
Full/BDR	FULL	Neighbor is BDR	Neighbor_ID
Full/DROTHER	FULL	none	broadcast spoke
2-WAY/DROTHER	2-WAY	none	broadcast spoke

router-1# **show ip ospf neighbor**

Neighbor_ID	Pri	State	Dead Time	Address	Interface
172.16.4.1	1	**Full/DR**	00:00:12	172.16.1.2	Gig0/0

The results of **show ip ospf neighbor** command displays operational status information. The State column displays DR relationship with neighbor. For example, **Full/DR** indicates that the local router has full adjacency with 172.16.4.1 neighbor. That neighbor is elected DR for the broadcast domain. DROTHER indicates there is no exchange of routing updates between spoke neighbors. That is characteristic of a broadcast network where updates are only sent between DR and spoke routers.

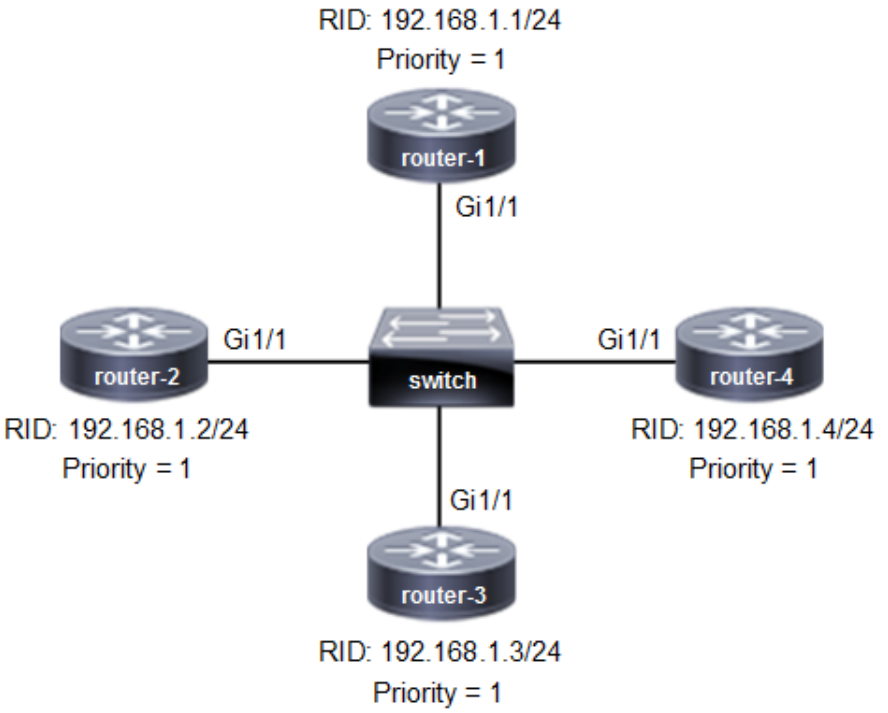
Neighbor Field Descriptions

- Neighbor_ID = Neighbor router ID
- Pri = Neighbor priority
- State = Neighbor adjacency + DR relationship
- Dead Time = Dead timer age
- Address = IP address of neighbor interface
- Interface = Ethernet interface of neighbor

Example: Designated Router

Refer to the network drawing. All routers are configured with the default OSPF priority (1). What router will be elected as designated router (DR)?

Figure 3-4 OSPF Designated Router Election



Answer

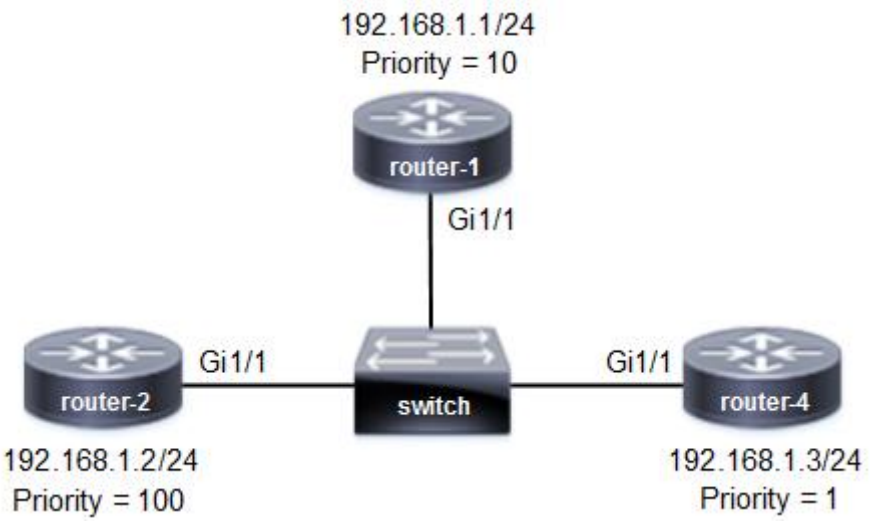
Ethernet interfaces within an OSPF broadcast domain are assigned to the same VLAN. There is a default configuration with the same priority on each router. The router with highest configured router ID (RID) is elected as DR for all routers connected to switch-1. The elected DR is Router-4 with **192.168.1.4** configured as router ID. Router-3 has second highest configured router ID **192.168.1.3** and elected Backup DR (BDR). The highest IP address is calculated from left to right. The numbers for each IP address match until octet 3 where subnet 4 is higher. That is the IP address assigned to Router-4.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3
- 192.168.1.**4** = Router-4

Example: DR Priority

Refer to the network topology drawing. What router is elected DR based on the configuration?

Figure 3-5 Designated Router Priority



The router with highest configured priority is elected as Designated Router from a broadcast domain. In this example, router-2 is elected DR with priority 100. Configuring priority setting influences the election of a specific router as DR/BDR. The router with second highest priority is elected as Backup Designated Router for the broadcast domain. In this example, router-1 is elected BDR with priority 10. OSPF enabled router with a priority of zero (0) cannot be elected as DR or BDR. The following command assigns a priority of zero (0) to an OSPF interface.

```
router(config-if)# ip ospf priority 0
```

OSPF Network Type

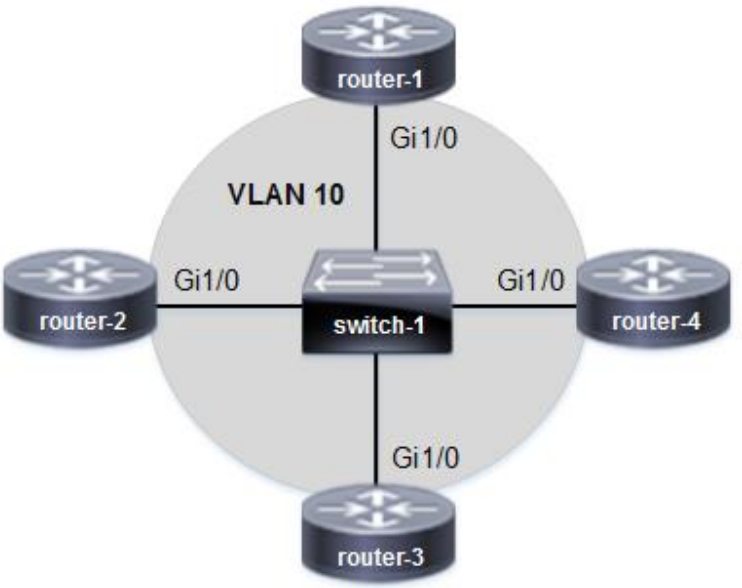
You can enable OSPF globally or per interface, however both methods will enable OSPF routing on an interface. All dynamic routing protocols are based on interfaces as opposed to the physical device. OSPF router interfaces all connect to an area. They also exchange routing updates with all directly connected OSPF neighbors. There are some exceptions where a configuration is per routing domain such as reference bandwidth.

OSPF network types are configured automatically based on the network interface media. For example, OSPF automatically assigns Broadcast network type to an Ethernet interface. There are serial interfaces as well that are assigned Point-to-Point network type. It is not a shared broadcast link as with an Ethernet segment. The OSPF serial interfaces connect only to a single neighbor.

Example: Network Type

Refer to the network topology drawing. What OSPF network type is assigned to the OSPF interfaces?

Figure 3-6 OSPF Network Type

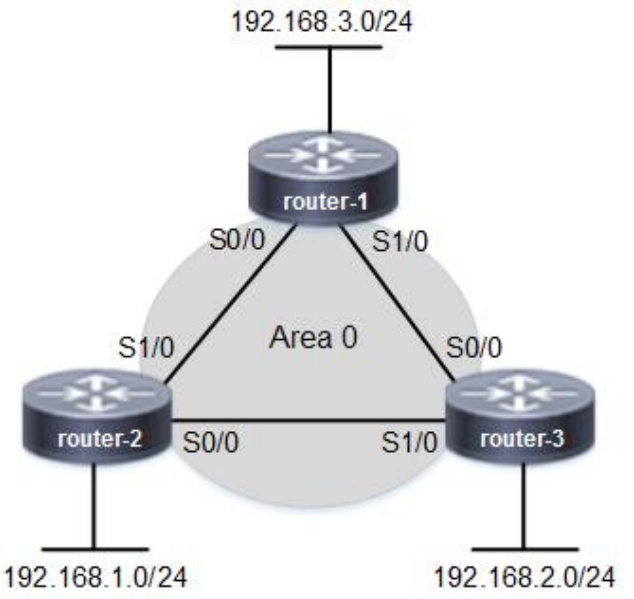


OSPF automatically assigns network type based on the interface media. In this example, OSPF interfaces are connected to an Ethernet switch. The network type assigned is Broadcast. Ethernet is a multi-access broadcast network where multiple routers are assigned to a broadcast domain. The purpose of a VLAN is to create a Layer 2 broadcast domain on a network switch. OSPF automatically elects DR/BDR routers on a broadcast network to send routing updates.

Example: Network Type

Refer to the network topology drawing. What OSPF network type is assigned to the OSPF interfaces?

Figure 3-7 OSPF Network Type



OSPF automatically assigns serial interfaces as point-to-point network type. There is no DR/BDR elected on a point-to-point network type. Each router advertises routing updates to the neighbor directly. In fact, there is a separate broadcast domain for each link on the same subnet. OSPF only advertises routing updates to neighbors within a common subnet. OSPF neighbors directly connected with Ethernet interfaces are manually configured as Point-to-Point network type. That is a common practice since OSPF will automatically configure Broadcast network type.

OSPF Operation

- OSPF multi-area is based on a hierarchical network topology where there is a backbone area. Any new area must be connected to the backbone area or have a virtual transit link through a connected area.

- Single-Area OSPF has only a single area where all routers are connected with at least one network interface.

- The OSPF process ID is a unique number assigned to an OSPF routing instance. It is only locally significant to the router. OSPF enabled interface can be assigned to multiple process ID.

- The valid range for a process ID is 1-65535. There is a separate OSPF database topology table per process ID.
- Cisco supports multiple OSPF instances per router defined with a process ID. There is a maximum of 32 processes permitted per router.
- All OSPF routers send hello packets to neighbors on the same segment (subnet) using multicast 224.0.0.5 destination IP address.
- Hello timer interval for broadcast and point-to-point network type is 10 seconds. The default dead timer is 4 hello intervals (40 seconds).
- There is no maximum hop count for OSPF so it is unlimited.
- Router ID is manually configured or default to highest loopback IP address.
- Passive interfaces prevent local router from sending hello message routing update on an interface to a non-OSPF neighbor.
- There is no maximum hop count for OSPF so it is unlimited.

OSPFv2 Configuration

OSPF is a classless routing protocol and wildcard masks are required to define subnets for route advertisements. OSPF **network area** command enables OSPF routing on all local interfaces that are assigned an address within the subnet range specified. The routes are advertised to the area assigned and all neighbor/s assigned to that area.

For example, an interface assigned 192.168.1.1 is enabled for OSPF when **network area** command is configured with 192.168.0.0/16 or 192.168.1.0/24 network address. The subnet (route) is then advertised to the area assigned. OSPF supports either 32-bit dotted-decimal number or the equivalent decimal number to an area. The assignable range is from 0.0.0.0 - 255.255.255.255 or decimal equivalent of 0 to 255,255,255,255.

OSPF can be enabled directly on an interface as well. For example, assigning interface Fa0/1 to OSPF process 1 and area 0 would require interface command **ip ospf 1 area 0**. The result is OSPF will advertise the subnet assigned to that local interface to OSPF neighbors. It takes precedence as well when a subnet from the **network area** command is within the same range of an interface subnet address.

Example: OSPF Configuration

The following command advertises 192.168.100.0/24 subnet from any local interface assigned within that same subnet to area 0.

```
network 192.168.100.0 0.0.0.255 area 0
```

The following commands are OSPFv2 single-area global configuration that is advertising subnet 192.168.0.0/16 to area 0 and 172.16.1.0/24 to area 0.

```
router ospf 1
router-id 172.16.255.1
network 192.168.0.0 0.0.255.255 area 0
network 172.16.1.0 0.0.0.255 area 0
```

Default-Information Originate

The purpose of **default-information originate** command is to advertise a default route to connected neighbors. It is a default route configured under a dynamic routing protocol and advertised to all neighbors. The traditional default route is configured locally on a router and used as a gateway of last resort.

Table 3-6 OSPF Characteristics

Routing Protocol	Characteristics
OSPF	• link-state • metric = link cost (bandwidth) • global view database topology table • shortest path to destination calculated • event-triggered routing updates • auto-summary disabled (default) • scalable to large enterprise domains • faster convergence than RIPv2 • load balancing 4 equal paths

OSPF is a classless routing protocol and wildcard masks are required to define subnets for advertising. OSPF **network area** command enable OSPF routing on local interfaces that are assigned an address within the subnet range specified. The routes are advertised to the area assigned. The following command will advertise 192.168.100.0 subnet (route) from any local interface assigned within that same subnet to all connected OSPF neighbors in area 0.

```
router(config-router)# network 192.168.100.0 0.0.0.255 area 0
```

This is an OSPFv2 multi-area global configuration that is advertising subnet 192.168.0.0/24 to area 0 and 172.16.1.0/24 to area 1.

```
router(config)# router ospf 1
router(config-router)# router-id 172.16.1.255
router(config-router)# network 192.168.0.0 0.0.255.255 area 0
router(config-router)# network 172.16.1.0 0.0.0.255 area 1
```

Table 3-7 OSPF Operational Commands

IOS Command	Description
show ip ospf database	display all link states for each area where router has an interface and advertising routers
show ip ospf neighbors	display all neighbors that have adjacency with local router and DR
show ip ospf interface	display operational state of OSPF enabled interface, timers. process ID and router ID

First Hop Redundancy Protocol (FHRP)

The purpose of a default gateway is to provide routing services to endpoints. It is a network interface with an IP address on a Layer 3 network device. The default gateway is an upstream router or Layer 3 switch for client and server endpoints. Any packets destined for a remote subnet are forwarded to the default gateway. DHCP service is often enabled to automatically configure a default gateway address on each endpoint. There is only a single default gateway address on any host client or network server.

- creates a single virtual router from at least two routers
- provides a default gateway service to multiple hosts
- share virtual IP address and MAC address
- router with highest priority setting is elected active virtual router
- default priority for a Cisco router is 100
- router with highest IP address is elected when priorities are equal
- preempt command is configured to assign a standby router
- not a routing protocol and virtual IP is not installed in the routing table

HSRP Configuration

This example configures router-1 interface Gi0/1 as active for group 1 and virtual IP address of 172.16.1.3 assigned. At least two routers are assigned per group.

router-1(config)# **interface gigabitethernet0/1**
router-1(config-if)# **ip address 172.16.1.1 255.255.255.0**
router-1(config-if)# **standby version 2** (*enables HSRPv2*)
router-1(config-if)# **standby 1 preempt** (*compare priorities for group 1*)
router-1(config-if)# **standby 1 priority 110** (*active router*)
router-1(config-if)# **standby 1 ip 172.16.1.3** (*virtual IP address*)

IP Services

DHCP Features

- assign and renew IP addresses from a designated pool
- configure TCP/IP address settings on hosts
- IP address is assigned to each host for a fixed lease time
- host sends request that DHCP server renew same IP address
- Ping or Gratuitous ARP is used to detect IP address conflicts
- IP address is removed from pool until conflict is resolved

DHCP request for an IP address:

Step 1: Server Discovery = DHCPDISCOVERY

Step 2: IP Lease Offer = DHCPOFFER

Step 3: IP Lease Request = DHCPREQUEST

Step 4: IP Lease Acknowledgement = DHCPACK

The following command displays IP address and MAC address of DHCP client, lease expiration and assignment type on the IOS DCHP server.

show ip dhcp binding

Table 4-1 DNS Commands

IOS Command	Description	Example
ip name-server	IP address of DNS server	172.16.1.254
ip domain-name	create FQDN hostname	cisco.server.com
no ip domain-lookup	disable DNS services	default is enabled
ip host	configure static mapping	ip host sw1 10.10.1.1

Table 4-2 Cisco Time Sources

Time Source	Description
private	internal network device
system calendar	initializes software clock after restart
software clock	initially set by hardware clock
public	external time server

Table 4-3 Network Time Protocol

Method	Description
ntp peer	backup time server configuration
system calendar	initializes software clock after restart
software clock	initially set by hardware clock
ntp server	configure time source for client
ntp master	configure internal time server as source

NTP Features

- Provides time source for logging and time stamp transactions
- N+1 server redundancy supported (NTP master + failover)
- Reference is UTC coordinated universal time
- DNS is required for resolving time server IP address
- server mode routers provide time source to client mode devices
- stratum level is the distance from NTP authoritative time source
- server mode routers poll external time server unless **ntp master** enabled
- **show ntp status** displays operational status of NTP server

Network Address Translation

- conceals private IP address assignments from the internet
- eases management of internet connectivity
- public IP address is assigned by Internet Service Provider
- network address translation is between private and public addressing

Static NAT

The static NAT translation is a 1:1 configured mapping between local and global addresses. The static translation manually assigns a private IP address to a public IP address. For instance, three public routable IP addresses will allow three static NAT translations. As a result they are a permanent entry in the NAT translation table. They enable a remote host connection from an outside (external) network.

Dynamic Pool

Dynamic NAT pool mapping translates each private IP address to an available public IP address (1:1) in the NAT pool. The dynamic NAT pool of public IP addresses is shared by all internal IP addresses on a first come first served basis. The maximum number of simultaneous internet connections available is limited to the number of public IP addresses in the NAT pool.

Port Address Translation

Port Address Translation (PAT) is an IP address translation technique that translates the most internal (private) IP addresses to a single or multiple public IP addresses. It is an enhancement to NAT that assigns a unique source port number to each translated IP address. The host IP address for instance could be identified with 200.200.1.1:10 as the translated source IP address. The 10 is the unique source port making the translated IP address unique. The 16 bit source port field allows for translating 65,535 private (internal) IP addresses.

Configure inside NAT interface

```
R1(config)# interface fastethernet2/0
R1(config)# ip address 192.168.1.3 255.255.255.0
R1(config-if)# ip nat inside
```

Configure outside NAT interface

```
R1(config)# interface fastethernet1/0
R1(config-if)# ip address 172.33.1.1 255.255.255.0
R1(config-if)# ip nat outside
```

Create a NAT pool name **cisco** and assign public internet IP address range 172.33.1.1 - 172.33.1.10

R1(config)# **ip nat pool cisco 172.33.1.1 172.33.1.10 netmask 255.255.255.0**

Configure extended ACL 100 to permit private host IP address range from 192.168.0.0 - 192.168.255.255

R1(config)# **access-list 100 permit ip 192.168.0.0 0.0.255.255 any**

Assign ACL 100 to pool name **cisco** and enable port address translation

R1(config)# **ip nat inside source list 100 pool cisco overload**

SNMP Monitoring

The alert messages generated by SNMP agents include both *Trap* and *Inform*. The purpose of *Trap* messages is to send alerts to the network management station (NMS). For instance, the network device sends a *Trap* to the NMS alerting that a network interface status is down. The *Inform* message is an acknowledgement of a *Trap* to confirm it arrived.

The following are SNMPv3 security enhancements

- message integrity
- authentication
- encryption

SNMPv2 authentication type used is community strings. The following configures SNMP community string to read-only access with password **cisco**. In addition there is a string with read/write access and password **simlabs** for additional rights access.

switch(config)# **snmp-server community cisco ro**
switch(config)# **snmp-server community simlabs rw**

Syslog Messaging

The following are correct statements concerning Syslog messaging.

- Syslog provides an external store for system messages
- Syslog messaging is disabled by default
- **service timestamps log datetime localtime** (add timestamp)

The **logging** command enables a Cisco device to log SNMP traps from 0 up to and including level 7. The traps are logged to the Syslog server. The Syslog servers receive informational (6) and lower severity messages as a default.

router(config)# **logging trap** [level]

Configure a router that will send system messages to a Syslog server that is assigned IP address 192.168.3.1

router(config)# **logging on**
router(config)# **logging host 192.168.3.1**
router(config)# **end**

The **logging facility** command enables you to create separate log files based on message type such as hardware, protocol or module for example. Syslog enables seven logging facilities from local0 to local7. The Cisco default setting for switches and routers is ***local7***

Table 4-4 Message Logging Levels

***Level**	**Message**
0	emergencies
1	alerts
2	critical
3	errors
4	warnings
5	notifications
6	informational
7	debugging

* Message severity level sends all lower messages as well

Selecting IOS Image on Bootup

1. The device starts and does Power on Self Test (POST) to verify all hardware is operational.

2. The bootstrap loader then determines where to load the IOS image based on the configuration register settings. The default setting loads the first IOS listed with any **boot system** command in the router startup configuration file. The **boot system** command points to a location of an IOS image stored in Flash memory. The file location configured with the first **boot system** command is used when multiple commands exist.

3. The first IOS image listed in Flash memory (where multiple IOS images exist) is loaded when there are no **boot system** commands.

4. IOS is loaded from TFTP server when there is no IOS image on Flash.

5. ROMmon mode starts when there is no IOS image on TFTP server.

Startup Configuration

The following describes what the Cisco network device does when no startup configuration file is found during bootup. Deleting the startup configuration and restarting the network devices will put the network interfaces in shutdown state.

1. The Cisco network device first attempts to load the startup configuration from NVRAM (default location). There is a copy made of the startup configuration loaded to DRAM for active use. That is referred to as the running configuration.

2. The network device attempts to load the startup configuration file from TFTP server if there is no startup configuration in NVRAM.

3. The network device starts the initial configuration dialog mode if there is no configuration to a TFTP server or it is unavailable. That enables a start from scratch configuration. The preferred method is to restore the most recent startup configuration where available.

    --- System Configuration Dialog ---

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

Table 4-5 Command Modes

CLI Mode	Command Prompt
user EXEC mode	device >
privileged EXEC mode	device#
global configuration mode	device(config)#
ROMmon mode	rommon >
routing configuration mode	device(config-router)#

Table 4-6 Quality of Service (QoS)

Technique	Description
congestion avoidance	WRED, tail drop, thresholds
bandwidth management	shaping, policing, CAR
congestion management	FIFO, WFQ, PQ, CBWFQ (queuing)
traffic marking	Class of Service, DHCP, NBAR
service-policy	attach policy to interface

* DHCP is Layer 3 marking of IP header DSCP field byte (ToS)
* Class of Service is Layer 2 marking of Ethernet frame 802.1q priority field
* default trust state for network interfaces is untrusted

Traffic Shaping vs Policing

The following is a list of features and operation of traffic shaping

- minimize the effect of bandwidth hogging on available network bandwidth.
- shaping does support packet queueing
- queuing prevents packet forwarding from exceeding maximum data rate
- shaping limits the maximum data rate on egress interface only
- shape traffic rate lower than maximum speed of physical interface.
- The queuing of packets can affect delay sensitive traffic with higher latency.

The following is a list of features and operation of policing

- policing does not queue packets and that minimizes latency
- policing drops or remarks traffic that exceed thresholds such as CIR
- policing can be applied to ingress and egress interfaces
- no minimum bandwidth guarantee with traffic shaping or policing.

Table 4-7 TFTP vs FTP

TFTP	FTP
UDP best effort delivery	TCP reliable connection-oriented
no user authentication	username/password authentication
IP phone configuration	not supported
single connection	control and data connection
faster	slower

Security Fundamentals

Device Hardening

username [*username*] **privilege** [*level*] **password** [*level*]

privilege 1 = user EXEC mode (lowest)

privilege 15 = privileged EXEC mode (highest)

password 5 = hidden secret password

password 7 = hidden password

service password-encryption = encrypt all passwords in configuration script

enable password [*password*] [*level*] = password protect privilege mode (default privilege level is 15 when not configured with enable command or based on username command)

Configure Telnet login, set the password to *cisco* and a timeout value of 5 minutes for all five default VTY lines

```
router(config)# line vty 0 4
router(config-line)# password cisco
router(config-line)# login
router(config-line)# exec-timeout 5
```

Configure console port with password *cisco* for local access security.

```
router(config)# line console 0
router(config-line)# password cisco
router(config-line)# login
```

Generate RSA keys for enabling SSH version 2 on a router. SSH version (1 | 2) of host client software is supported by the router when no version is configured.

```
router(config)# crypto key generate rsa
router(config)# ip ssh version 2
router(config)# ip ssh timeout 90 authentication-retries 2
```

The following are options for permit / deny of management protocols. Cisco default is to allow all protocols inbound and outbound access on VTY lines.

```
router(config-line)# transport input ssh (allow SSH only)
router(config-line)# transport input all (allow all protocols)
router(config-line)#transport input telnet ssh (allow Telnet / SSH only)
```

Port Security

The purpose of port security is to prevent any unauthorized network device from accessing the corporate network. For instance plugging a laptop from home into the Ethernet jack at work could affect network operations. The switch port enabled with port security would deny access based on the unknown MAC address. Cisco switches support sticky, static or dynamic port security modes.

Sticky

The **sticky** keyword saves the dynamically learned MAC address to the running configuration script. In addition sticky MAC addresses do not age out of the MAC address table. The switch does have to relearn the MAC addresses after every reboot unless the running configuration is saved to startup configuration file. Removing the **sticky** keyword causes dynamically learned the MAC addresses to persist in the MAC address table only for the connected session. The following commands enable port security on a switch port interface with sticky method.

```
interface fastethernet 0/1
switchport port-security
switchport port-security mac-address sticky
```

Static

The static option enables a switch interface to only accept frames from a host or network device with a specific MAC address. The static MAC is manually assigned to the switch port and must match to allow frames. The switch port would deny access based on an unknown MAC address. The default setting is to allow only one MAC address per switch port.

```
interface fastethernet 0/1
switchport port-security
switchport port-security mac-address 0000.1234.5678
```

Dynamic

This is the default setting for port security on a switch interface when enabled. The MAC address of the connected host or device is learned dynamically and added to the MAC address table. The MAC address persists in the switch table until switch is powered off or deleted when host is disconnected from the switch.

Maximum MAC Addresses

The following port security interface command prevent connecting any second host or network device to a switch port. There is support however for allowing multiple MAC addresses to a single switch port. The switch interface can add up to the maximum number of five allowed MAC addresses to the address table.

```
switch(config-if)# switchport port-security maximum 1
```

Violation Actions

There are protect, restrict, shutdown VLAN and shutdown violation modes. The default setting is shutdown where the port shuts down only when the maximum number of secure MAC addresses is exceeded. The switch then sends an SNMP trap notification. Protect mode only sends a security violation notification. There are additional options available with restrict and shutdown VLAN modes.

The security violation could trigger when there is an attempt from a host with a MAC address not in the MAC address table. Duplicate MAC address error cause a violation as well. The restrict mode causes the switch to drop all packets from an unknown source. SNMP trap alerts are sent, syslog messages are logged and the violation counter is incremented.

Access Control Lists

Standard ACL

The number range is from 1-99 and 1300-1999. It is comprised of permit or deny statement/s from a source address with a wildcard mask only. The single deny statement requires that you add **permit any** as a last statement for any standard ACL or all packet are denied from all sources.

access-list 99 deny host 172.33.1.1
access-list 99 permit any

Standard Named ACL

They are defined with a name instead of number and have the same rules as a standard ACL. The following ACL is named ***internet*** and will deny all traffic from all hosts connected to 192.168.1.0/24 subnet. It will log any packets that are denied.

ip access-list internet log
deny 192.168.1.0 0.0.0.255
permit any

Extended Named ACL

They are defined with a name and supports all syntax commands available with extended ACLs. You can dynamically add or delete statements to any named ACL without having to delete and rewrite all lines. They are easier to manage and troubleshoot based on naming conventions. The following named ACL permits http traffic from hosts assigned to 192.168.0.0/16 subnets access to server 192.168.3.1

ip access-list extended http-filter
remark permit http to web server
permit tcp 192.168.0.0 0.0.255.255 host 192.168.3.1 eq 80
permit ip any any

Extended ACL

The number range is from 100-199 and 2000-2699. It supports multiple permit/deny statements with source / destination IP address or subnet. In addition you can filter on IP, TCP or UDP protocols and destination port. Extended ACL must have a permit all source and all destination traffic with **permit ip any any** as a last statement.

Cisco best practices for creating and applying ACLs

- apply extended ACL near source
- apply standard ACL near destination
- order ACL with multiple statements from most specific to least specific
- one ACL can be applied inbound or outbound per interface per Layer 3 protocol
- ACL is applied to an interface with **ip access-group in | out** command

The following are primary differences between IPv4 and IPv6 for ACLs

- IPv6 supports only named ACLs
- IPv6 permits ICMP neighbor discovery (ARP) as implicit default
- IPv6 denies all traffic as an implicit default for the last line of the ACL

ACL Example 1

The following command permits http traffic from host 10.1.1.1 to host 10.1.2.1

access-list 100 permit tcp host 10.1.1.1 host 10.1.2.1 eq 80

The access control list (ACL) statement reads from left to right as - *permit all tcp traffic from source host only to destination host that is http (80)*. The TCP refers to applications that are TCP-based. The UDP keyword is used for applications that are UDP-based such as SNMP for instance.

ACL Example 2

What is the purpose or effect of applying the following ACL?

access-list 100 deny ip host 192.168.1.1 host 192.168.3.1
access-list 100 permit ip any any

The first statement denies **all** application traffic from host-1 (192.168.1.1) to web server (host 192.168.3.1). The ***ip*** keyword refers to Layer 3 and affects all protocols and applications at layer 3 and higher. The last statement is required to permit all other traffic.

ACL Example 3

What is the purpose or effect of applying the following ACL?

access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq telnet
access-list 100 permit ip any any

The first statement permits Telnet traffic from all hosts assigned to subnet 192.168.1.0/24 subnet. That include host-1 (192.168.1.1) and host-2 (192.168.1.2). The ***tcp*** keyword is Layer 4 and affects all protocols and applications at Layer 4 and higher. The ***permit tcp*** configuration allows the specified TCP application (Telnet). The ***any*** keyword allows Telnet sessions to any destination host. The last statement is mandatory and required to permit all other traffic.

ACL Example 4

What is the purpose or effect of applying the following ACL?

access-list 100 permit ip 172.16.1.0 0.0.0.255 host 192.168.3.1
access-list 100 deny ip 172.16.2.0 0.0.0.255 any
access-list 100 permit ip any any

- The first ACL permits only hosts assigned to subnet 172.16.1.0/24 access to all applications on server-1 (192.168.3.1)

- The second statement denies hosts assigned to subnet 172.16.2.0/24 access to either server. That would include any additional hosts added to that subnet and any new servers added.

- The last ACL statement is required to permit all other traffic not matching previous filtering statements.

- ACL is applied to an interface with **ip access-group** command**.** Most **r**outers often have multiple interfaces (subnets) with hosts assigned. ACL applied outbound to an interface shared by multiple subnets will filter traffic from all hosts for each subnet.

Cyber Security

Exploit - Attack strategy that leverages an existing security vulnerability. The exploit is software designed to attack a specific vulnerability. (malware, root kit etc.) email phishing, MITM, spoofing, DDoS.

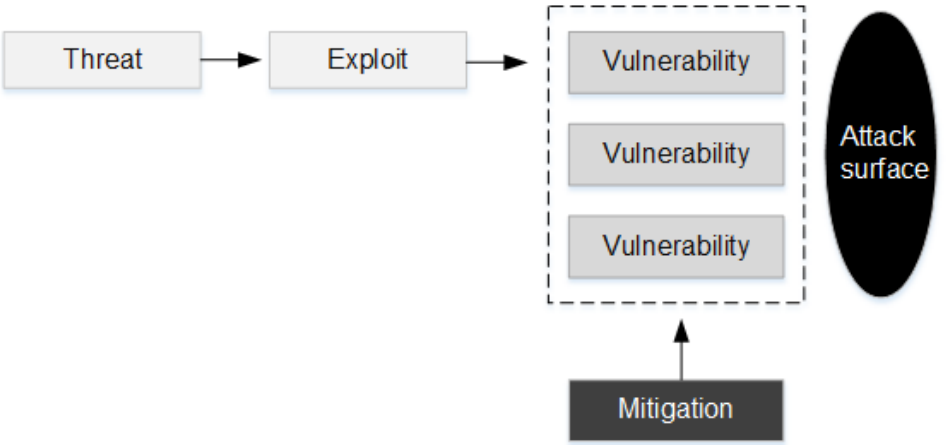
Vulnerability - Existing security flaws such as software bugs, default passwords and misconfigured firewall rules that could be exploited.

Mitigation - Specific techniques employed to decrease or eliminate the security threat level of a vulnerability. Some examples include awareness training, software updates, IPS, firewall inspection, Incident response and vulnerability assessment testing.

Threat – This is a potential danger, or event that results from exploiting a vulnerability. Hackers will often use multiple exploits in a threat. Some examples are spyware, malware, power outage, virus, and software error.

Attack Surface - The number of attack vectors that exist for a hacker to exploit vulnerabilities that enables unauthorized access.

Figure 5-1 Cyber Attack Chain Flow



AAA Security Model

AAA is a well-established security framework for controlling and monitoring network access. It is based on authentication, authorization and accounting of requests for network services and data. There are solutions to manage physical access, surveillance systems, network devices and web servers are all different. The common elements of the AAA model should be included when deploying your security solution. The following describes and compared each element of the AAA security model.

Authentication

This security control verifies the identity of a device and/or user before there is authorization permitted to data. Network level access is initially based on some authentication protocol or technique. The traditional username/password text string has been a standard for years. It is being replaced with Multi-Factor Authentication (MFA) for more robust layered authentication.

Authorization

This security control is in effect only after user authentication has been verified. The purpose of user authorization is to permit or deny access to data, services and commands. It is much more complex and involves permission levels for device modes, files and data that exist.

Accounting

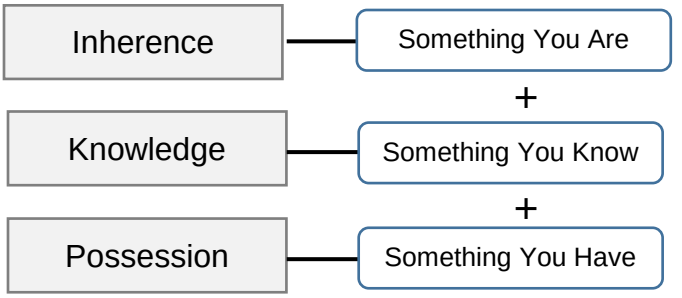
This security service includes monitoring, logging and auditing of all security events. Any request for network access generates an event record that is stored for all users and transactions. The transaction would consist of username, time stamp, event type, and resources accessed. In addition, any user access denied is logged and alerts sent based on severity level. It is used for tracking, sending alerts, notifications, attack forensics and auditing.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is part of a multilayered security architecture. Network access is often available globally from a variety of public and private locations. MFA is a preferred solution to the increasing fraud and problem of stolen credentials. User identity is based on at least two or more independent security credentials.

Consider that multiple security layers exist from when you swipe an ID card, enter a building and then access your data. Having multiple authentication also eliminates any single point of failure when security credentials are stolen or compromised. It blends static and dynamic credentials to optimize security posture.

Figure 5-2 Multi-Factor Authentication Elements



DHCP Snooping

DHCP snooping is a Layer 2 security feature that acts like a firewall between DHCP clients and DHCP servers. The primary purpose of DHCP snooping is to prevent rogue DHCP servers from offering an IP address to clients. The rogue or unauthorized DHCP server attempts to respond to DHCP requests from clients. It is commonly referred to as a man-in-the-middle attack (MITM).

DHCP snooping enables trusted switch ports that are connected directly to an authorized DHCP server. Any frames that do not originate from an authorized DHCP server are dropped. In addition, there is a system error message logged. The following services are provided by DHCP snooping.

- Permit DHCP packets on DHCP trusted port only.
- Prevent rogue DHCP servers from offering IP address to hosts.

DHCP snooping is enabled both globally per access switch and per VLAN. The network administrator would enable snooping on VLAN/s assigned to switch access ports. It is enabled on any uplink to the router as well. Typically you would enable all host VLANs for DHCP snooping. For DHCP snooping to work properly, all authorized DHCP servers must be connected to the switch through trusted interfaces. All untrusted DHCP messages are forwarded only to trusted interfaces as well.

Table 5-1 SSL vs IPsec

SSL VPN	IPsec VPN
dynamic VPN	static VPN
application layer	network layer
browser-based	host-based
virtual connections	tunnel
easy to deploy	complex to deploy
digital certificate encryption	IPsec encryption
host to application	router to router
device/user authentication is digital certificate	device authentication is pre-shared keys or certificate
granular security authorization	user authentication (VPN gateway)

Automation and Programmability

Traditional Network Architecture

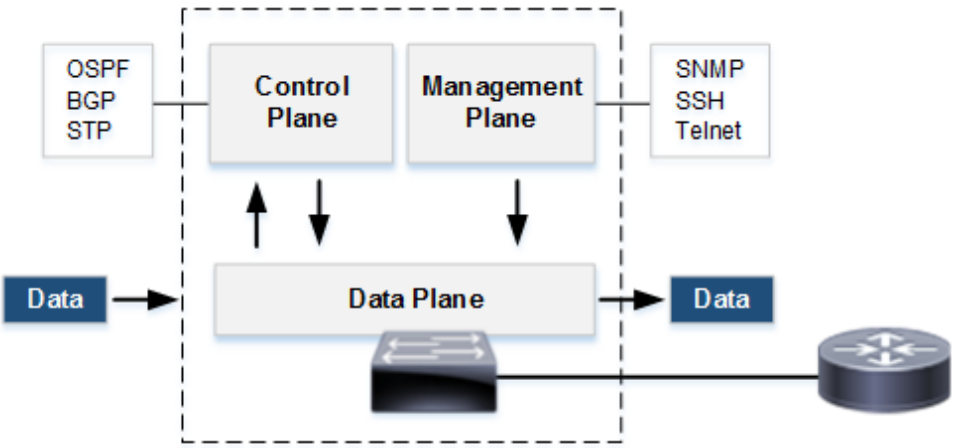
The purpose of any network is to enable data communication between host endpoints. That is accomplished with infrastructure devices that communicate via network protocols. The network operational model can be described using the concept of planes. Each network device within a traditional network has a data plane, control plane and management plane. It is a functional model that describes the dynamics of data communications and networking services. There are also differences between traditional and newer controller-based architecture, that is evident with the location of operational planes.

Data Plane

The data plane is only responsible for forwarding of endpoint data traffic between network interfaces. All data plane traffic is **in-transit** between neighbors, and not associated with communication protocols. It is not handled by the processor as a result. For example, routing tables created by the control plane are used by the data plane to select a route. The packet is then forwarded to a next hop neighbor address.

- MAC learning and aging
- MAC address table lookup
- Routing table lookup
- ARP table lookup
- MAC frame rewrite

Figure 1 Traditional Network Architecture



Similarly, MAC address and ARP tables created by the control plane, are used by the data plane to forward traffic. While all three planes exist on all network devices, the services provided are based on the device class. For example, only routers and L3 switches support routing tables, ARP tables and frame rewrite. Conversely, all switches create MAC address tables while routers do not.

Control Plane

The control plane is responsible for building network tables used by the data plane to make forwarding decisions. Control plane protocols only communicate with directly connected neighbors. It is only the processor that handles inbound and outbound control plane traffic. There are routing protocols that build routing tables from neighbor advertised routes for Layer 3 connectivity. Some examples of Layer 3 control plane protocols include OSPF, EIGRP, BGP, and ICMP.

- Network tables
- Path selection
- Frame switching
- Link negotiation
- Error messages

Control plane protocols also enable interconnection of switches within Layer 2 domains. For example, STP enables a loop free topology between multiple switches. There is dynamic trunk negotiation between neighbor switches and EtherChannels. Examples of Layer 2 control plane protocols include STP, DTP, LACP, and CDP. Network switches create MAC address tables for frame switching within Layer 2 domains.

Management Plane

The management plane is responsible for configuration and monitoring of network devices. There are various application protocols that are used to manage the network. SSH is initiated to the management plane of a router to configure network interfaces. SNMP sends traps to a network management station to alert on operational status of interfaces.

- Configuration
- Monitoring
- Automation
- Programmability

There are newer protocols such as NETCONF that enable automation of management functions. Similar to the control plane, is the fact that all management plane protocols must be handled by the processor. Some other examples of management plane protocols include TFTP, Telnet, RESTCONF, Syslog, NTP, DNS, and DHCP.

1. The management plane initiates a session with the local router to configure OSPF and enable network interfaces.

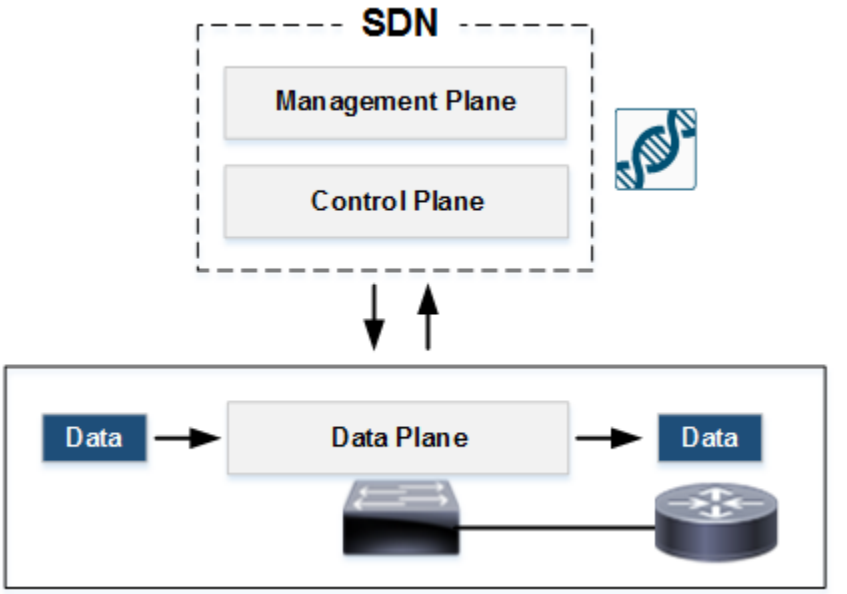
2. The control plane has a routing table with a route that includes a next hop address and local exit interface.

3. The data plane does a routing table lookup for the next hop address associated with a destination subnet. The data plane then forwards all packets to neighbor with next hop address.

Software-Defined Networking (SDN)

Software Defined Networking (SDN) is an architecture that separates the control plane from the data plane. Cisco IOS software is moved to an SDN controller. That decouples the control plane from hardware and enables direct programmability of all network devices. The controller communicates via agents installed on devices. The same functions are provided as with traditional networking architecture for each operational plane. Figure 6-2 illustrates how the management plane is also moved to the controller as well.

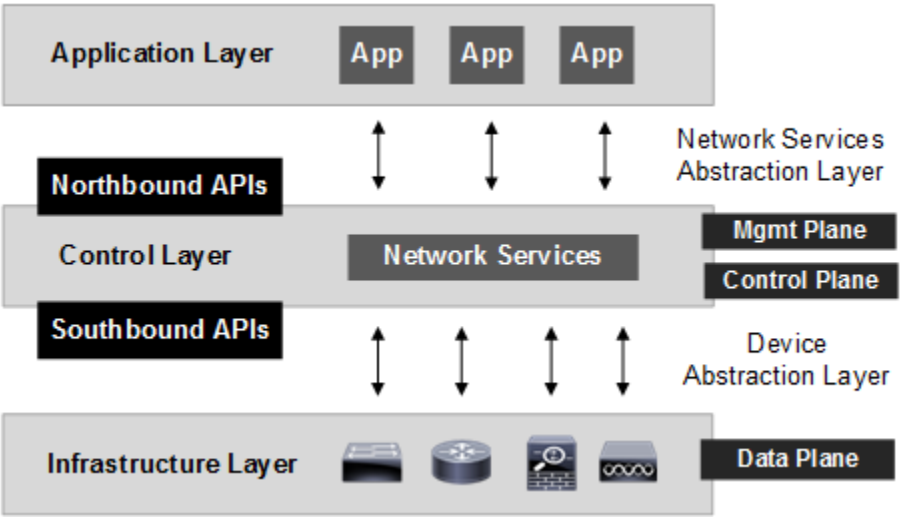
Figure 2 SDN Operational Planes



It is similar to a hypervisor layer that abstracts (separates) server hardware from application software. There is a centralized control plane that is software-based with an underlying physical data plane transport. SDN enables overlays and programmable devices for management with centralized policy engine and global view.

- SDN decouples the control and data plane.
- Control plane is software-based and not a hardware module.
- SDN controller is a centralized control plane with a policy engine.
- Network infrastructure is an underlay for programmable fabric.

Figure 3 SDN Architecture Layers



SDN Components

The SDN controller provides centralized management where the network appears as a single logical switch. Network services are dynamically configurable when the control plane is moved from physical infrastructure to a software-based SDN controller with API modules. The northbound and southbound APIs enables communication between applications and network devices.

Table 1 SDN Components

Attribute	Description
SDN Application	software that send requests to SDN controller via northbound APIs.
Northbound API	software on controller that expose SDN applications to controller services.
Controller	centralized control software that translates requests from SDN applications to network devices.
Southbound API	software that sends messages to communicate with agents on network devices for programmability.
Infrastructure	physical and virtual programmable network devices that provide data plane (forwarding) services.

SDN controllers communicate with physical and virtual network devices via southbound APIs. Conversely, communication from controller to SDN applications is via northbound APIs. There is a policy engine configured on a controller for orchestration and automation of network services.

- **Programmability** - network is directly programmable because it is decoupled from infrastructure and data plane forwarding.
- **Agility** - abstracting control plane from data plane enables dynamic configuration to modify traffic flows as network conditions change.
- **Centralized Management** - network intelligence is centralized in software-based SDN controllers. The global network appears to applications and policy engines as a single logical switch.
- **Automation** - dynamic configuration (provisioning) of network devices and software upgrades is based on APIs.

Network Functions Virtualization (NFV) increase agility by decoupling network services from proprietary hardware and moving it to software modules on SDN controllers. That makes it easier to provision, automate, and orchestrate network services such as DNS, firewall inspection and network address translation.

Advantages of Programmability

- Workload mobility
- Elastic auto scaling
- Dynamic policy provisioning
- Security-based diversion
- Dynamic path selection
- Services insertion
- Automated push configuration
- Dynamic bandwidth allocation
- Wireless RF optimization
- Network security updates

The advantage of programmability include automation and rapid deployment of new services and applications. Turn up of a new branch office or an application is now accomplished in minutes. Newer Cisco devices support programmable ASICs. Open APIs translate between application and hardware to initialize, manage and change network behavior dynamically.

New requirements now include on-demand bandwidth, dynamic security and elastic capacity. In addition rapid cost effective deployment of applications and services. The provisioning of wired and wireless services requires automated turn-up of network services, push configuration, automatic monitoring and real-time analysis.

Network Overlays

Cisco has recently developed SD-Access fabric architecture for data center and enterprise connectivity. The purpose is to enable automation, programmability and mobility for physical and virtual platforms. It is comprised of an underlay, fabric overlays and Cisco DNA Center.

Fabric Underlay

The fabric is comprised of a physical underlay designed for high-speed transport of traffic. It is characterized by network devices, topology and protocols for communication. There is a common underlay that provides transport for overlay traffic. That would include control plane protocols such as STP, DTP, OSPF, EIGRP and ARP.

- Network infrastructure used for transport of all data traffic
- Comprised of network devices, protocols and configuration
- Network devices must support programmability with agents
- Physical underlay operation is independent of overlays

Fabric Overlay

There is also path virtualization enabled with fabric overlays that are built on top of (or over) the underlay. Overlays create a virtual topology across a physical underlay infrastructure with encapsulation techniques that create tunnels. That essentially enables route and address isolation, that is independent of underlay and other overlays. Encapsulation is nothing more than adding outer header/s to original payload that is not visible to network devices when in-transit.

- Virtual topology with interconnects between nodes
- Encapsulation (tunnel) creates path virtualization
- Network address overlap and route isolation enabled
- Overlays are operationally independent of underlays

Consider that overlays logically create single point-to-point connections. That same topology has multiple physical connections between switches. The purpose of overlays are to solve limitations inherent with physical switching domains such as STP, routing loops, broadcasts and address overlap. They also enable multi-tenant service, enhanced mobility, seamless connectivity and automation.

Table 2 Underlay vs Overlay

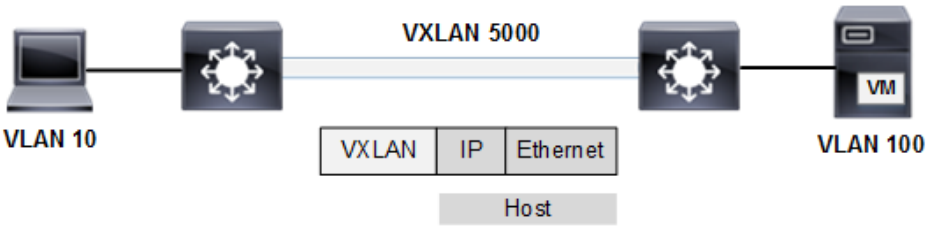
Underlay	Overlay
physical	virtual
single-tenant	multi-tenant
unique address space	overlap address space
native transport	tunneling

Layer 2 Overlay

Within the fabric architecture there is support for Layer 2 and Layer 3 overlays. Layer 2 overlays are designed to emulate a physical topology for the purpose of extending Layer 2 domains. For example, connecting two servers on different switches that are assigned to the same VLAN. The solution is a VXLAN overlay to enable a virtual connection between servers. It is common to have web-based applications with multiple servers that are often in different locations.

- Emulates a physical switching topology with virtual overlay
- Extend Layer 2 domains between switches and locations
- Enable address isolation and overlapping between domains
- Tunnels terminate at leaf switches for campus deployment

Figure 4 VXLAN Fabric Overlay



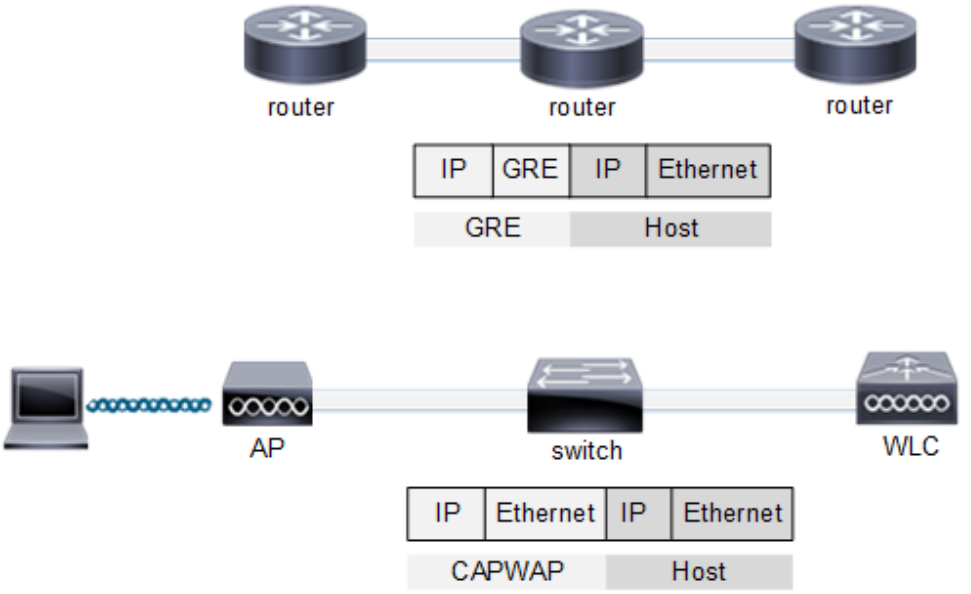
VXLAN is a data plane overlay that encapsulates host packets for communication across fabric. As an overlay, it requires the transport services of a physical underlay infrastructure. In our example, the tunnels are terminated at fabric edge switches. There is a common underlay for data plane forwarding, however the underlay topology is independent of overlay topologies. As a result, underlay and overlay maintain separate data and control planes.

Layer 3 Overlay

Layer 3 overlays enable data plane forwarding across a fabric between different subnets. There is the advantage as well of isolation from the underlay limitations associated with MAC flooding and spanning tree protocol loops. Tunnels are created with encapsulation of host packets. Some examples include VPN, MPLS, GRE, CAPWAP and VRF.

- Routing-based overlay for IP connectivity across fabric
- Isolates broadcast domains to each network device
- IP tunnel terminates at host endpoint or network device
- Logical point-to-point topology between tunnel endpoints

Figure 5 GRE and CAPWAP Overlays



Automation Fundamentals

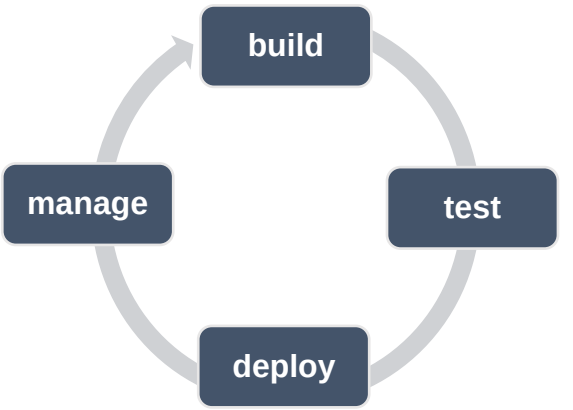
The advent of network programmability and automation tools is radically changing how network infrastructure is managed. Compared with traditional networking, automation has astonishing advantages for physical and virtualized network services. Network automation lowers operational costs, enables deployment agility, and unified policies.

Advantages of Network Automation

- Minimize network outages
- Enable deployment agility
- Lower operational costs
- Unified security policies
- Software compliance

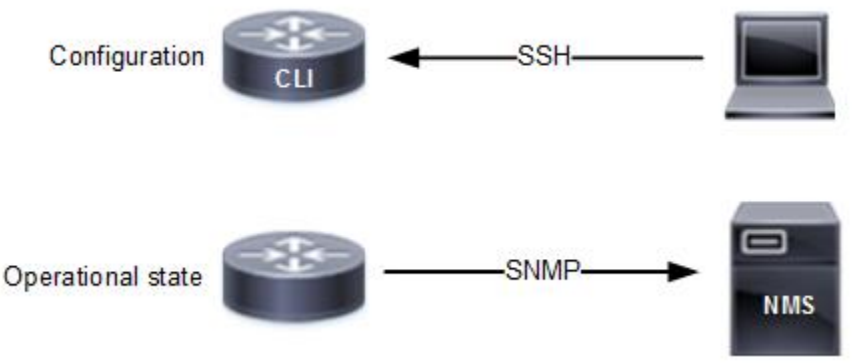
The most common cause of network downtime is user error. There are significantly less errors with configuration changes and deployment of network infrastructure. There is a globally centralized view of the network that is fundamental to SDN architecture. Network administrators can push standard configurations out to new network devices and update configuration on existing infrastructure. The audit of device configuration or software versions for compliance before update is much faster with automation.

Figure 6 Automation Life Cycle



Configuration management tools such as Puppet, Chef and Ansible are used to enable automation for on-premises and cloud-based services. They were developed originally for managing cloud computing and network virtualization infrastructure. Figure 6-6 illustrates how automation is based on quality assurance. There is a build, test and deploy model that minimizes errors and downtime before configuration changes are pushed to devices.

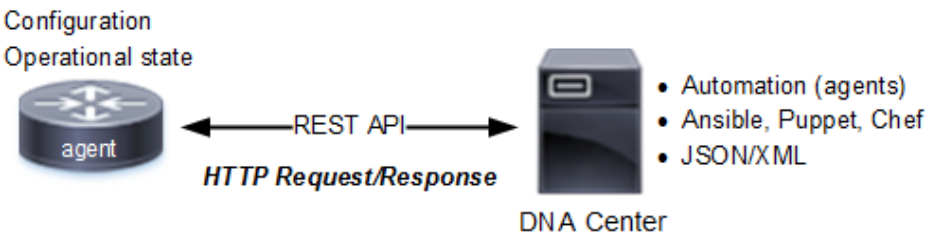
Figure 7 Traditional Networking Management



Previously, traditional networking was based on a silo view where each network device was statically managed separately. Having a centralized, real-time network view is fundamental to automation. There is much more accomplished, in less time and lower cost with minimal network outages.

The new architecture is based on agents that are deployed to network devices. They enable communication with a controller such as Cisco DNA Center via REST APIs. Multiple different automation tools are available such as NETCONF, RESTCONF, Ansible, Puppet and Chef. They are southbound APIs within SDN framework that provide features to automate configuration, software updates and other services.

Figure 8 Controller-Based Management Automation



Common Automation Management Tasks

- Unified infrastructure, software and security policies
- Push new configurations for physical/virtual infrastructure
- Standardize and update existing network device configuration
- Enhanced software compliance and version control
- Maintenance backup of system images and scripts
- Network discovery, detection and analysis
- Programmable scripting instead of manual CLI

Table 3 Traditional vs Automation

Traditional	Automation
CLI	scripting
manual	dynamic
slower	faster
error-prone	assurance
deploy	test and deploy
not scalable	scalable
physical server	physical + virtual machine

Configuration Management Tools

There are various open source configuration management tools that enable automation and orchestration of basic and complex tasks. They were originally developed for cloud computing however they are used to manage on-premises infrastructure as well. Some of the most popular automation tools include Puppet, Chef and Ansible.

Each of them have advantages, disadvantages and specific architecture. Configuration management for network infrastructure is mostly comprised of provisioning, compliance and maintenance tasks. Consider that traditional networking is all based on manual CLI access and SNMP operational monitoring of physical devices. With the advent of virtualization, network administrators are also managing network servers that are deployed as virtual machines (VM). That could include virtual appliances in the cloud or network services at the data center such as TFTP server and wireless LAN controller.

Example Automation Tasks

- Create new VLANs on switches
- Create management interface on switches
- Deploy initial configuration to multiple routers
- Update routers based on new PSIRT security alert
- Backup startup configuration scripts to TFTP server

The primary difference in architecture is how network nodes (client) are updated. Puppet and Chef are based on agents that are installed on clients and communicate with a centralized server (Puppet Master).

Ansible has agentless architecture where no software is installed on client nodes. The agent-based model is called a "pull mode" where clients pull or download a configuration or software update from a centralized server. The "pull mode" of Ansible relies on dynamic polling from a server.

They are open standard tools developed from cloud environments. One of the advantages of each platform is reusable template scripts that have been developed for a variety of common tasks. The protocols from Table 6-4 describe how client and server communicate. Puppet is a full-fledged configuration management tool with monitoring of state consistency. Puppet can also test scripts before making changes in simulation mode. All tools can create automated scripts for provisioning, compliance, and maintenance tasks.

Table 4 Comparing Puppet, Chef, and Ansible

Puppet	Chef	Ansible
agent	agent	agentless
pull	pull	push
HTTPS	SSH	SSH
Ruby	Ruby	Python
modules	recipes	playbook (YAML)
complex	complex	easy

REST API Architecture

The proliferation of web-based applications and cloud computing has led to development of Representational State Transfer (REST) architecture. It is a framework with rules for creating web-based services. It is based on stateless operations (verbs) that are performed on objects (resources) defined with URLs.

Figure 9 REST API Architecture

HTTP Verb	Network Operation
GET	show running-config
POST	configure terminal
PUT	copy run start
DELETE	delete startup-config

REST API is an example of northbound API that enables communication between SDN controller and applications. HTTP requests and responses are sent between machines based on GET, POST, PUT, DELETE verbs. They are used for inter-application communication. The server has no knowledge (stateless) and does not differentiate between single tasks or an entire application. REST API is an application programming interface compliant with REST architecture.

1. **Define Resources:** URL (web page, image, document, video, email)

2. **Assign HTTP Verbs:** GET, POST, PUT, DELETE

3. **Select Encoding Type:** HTML, JSON, or XML data encoding format

For example, you could develop a REST API to rent computer labs where customers request and book time online. Customers would start from the top-level navigation web page to request (GET) lab time. The application then responds (POST) with available times and dates. The customer could book a reservation (POST) time slot for a particular day. The customer then decides to change lab time reserved with a PUT request that updates existing data. There is also DELETE operation to cancel a booking.

Figure 10 RESTFUL API Architecture

HTTP Verb	Operation
POST	Create
GET	Read
PUT	Update
DELETE	Delete

REST API is often comprised of multiple web pages with features that are accessed through HTTP verbs. The data encoding type allow machines to read payload data in a common format. The encoding types for data interchange include JSON, HTML and XML. Communication between client browser and server is via HTML. In addition, server to server or server to device data exchange is encoded with JSON or XML.

API Stack Communication

REST API applications are designed for machine to machine (M2M) communication. The components of an application include HTTP methods (verbs), encoding, network transport and authentication. REST API encryption is provided with HTTPS where desired. The following describes REST API stack communication with HTTP application layer.

- HTTP/S Verbs = GET/POST/PUT/DELETE
- Authentication Method
- Encoding = JSON
- Transport = TCP 80/443
- PHY = Ethernet/Wireless

HTTP Verbs

Verbs are HTTP operations that define some action to read, add or modify resources on a server. The HTTP operations access resources represented as URLs and return payload response to a client, server or network device. Cisco DNA Center is essentially a server that manages physical and virtual network devices.

GET - This retrieve operation only requests to read a resource from the server such as a web page. The response header from a server or network device includes data content, with no state change.

POST - This operation is used to create new data or provide new data. Any client, server or network device can initiate POST operation and response is returned with updated data state.

PUT - This operation is used to send response to update or replace existing data on a server or network device.

DELETE - This operation removes data from a server or network device.

CRUD was primarily developed to manipulate database records for a variety of traditional application platforms. Recently, it has been adapted as well for web-based applications. CRUD methods are mapped to HTTP verbs for creating REST API and compliance with REST architecture.

Table 5 HTTP Verbs vs CRUD Operations

HTTP Verb	CRUD Operation
POST	CREATE
GET	READ
PUT	UPDATE
DELETE	DELETE

You can define a REST API for creating web services based on CRUD operations as a result. For example, consider an online shopping cart where CRUD is used to READ a web page where some CCNA books are listed. The next operation is CREATE to checkout and send payment for selected item. You could then change your shipping location with an UPDATE operation. The DELETE operation is used to remove/cancel a shopping cart session that was started.

JSON Data Encoding

REST does not specify any encoding type when creating a REST API for web services. In fact, there are various encoding types available that enable data interchange for platform independent data sharing. Each data encoding also specifies character sets that are supported. The purpose of encoding is to define a format for data that enable data interchange between disparate systems.

JSON is a readable text-based encoding method comprised of objects, arrays, and name/value pairs. It is based on a standardized syntax that enables data interchange between disparate systems. The following are some primary rules for correct syntax when creating JSON scripts.

- integer number value with double quotes are not allowed
- null value with double quotes are not allowed
- strings are used to represent values such as phone numbers
- square brackets [ ] create an array list within an object
- curly brackets { } create an object with name/value pairs
- comma-separated list of array values or name/value pairs

The following is an example of a JSON object that has the hostname and IP addressing for a data center router. JSON objects are comprised of single or multiple name/value pairs that are separated by commas. For example, name = hostname and value = router-1.

Example 1 JSON Object

```
{
“DC-Routers”: {
“hostname”: “router-1”,
“ip_address” : “192.168.1.1”,
“subnet_mask” : “255.255.255.0”
}
}
```

JSON array is basically a list of items that are associated with an array name. For example, an array called network interfaces could be created with multiple interfaces on a switch line card. An array can also comprise multiple objects, where each list item is an object separated by commas.

There is a single error only with the JSON script. It is a comma after curly bracket of second object }, that is not required. The last object in an array has a matching curly bracket only. The following example illustrates in bold where array starts and ends with square [ ] brackets. It is comprised of a list of network interfaces on a switch.

Example 2 JSON Array

```
{
"hostname": "switch-1",
"interfaces": [
"Loopback0",
"Serial1/0",
"Ethernet1/1",
"Ethernet2/1"
]
}
```

Table 6 Data Encoding Types

JSON	XML	HTML
text-based	text-based	text-based
client-server server-server	server-server	client-server
faster	slower	slower
less secure	more secure	more secure
text and number	multiple data types	multiple data types
key values, arrays	tree structure	tree structure
UTF-8, ASCII	UTF-8, ISO, ASCII	UTF-8, ISO, ASCII
REST API	REST API	REST API

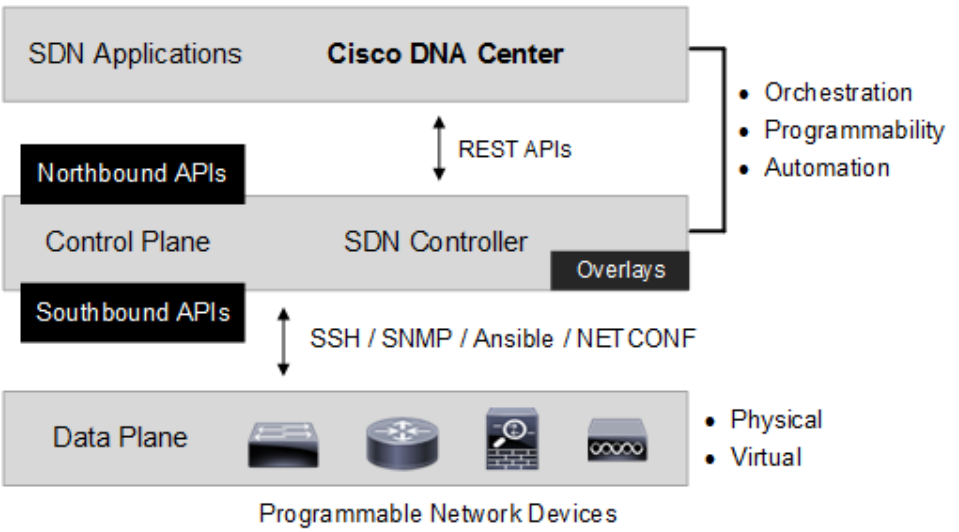
Character Encoding

The original character set standard was ASCII based on a character set with 128 numbers, letters and symbols. It was superseded by UTF-8 with the advent of web-based applications and the need for an expanded character set. In fact, by some estimates, UTF-8 is currently the default character set used for approximately 95% of all web pages. New versions of the same standard now include UTF-16 and UTF-32 character set. The default character set for JSON, XML and HTML is UTF-8.

Cisco DNA Center

Cisco DNA Center is a network management solution that is based on SDN architecture. DNA Center enables orchestration, automation and programmability of wired, wireless, and virtualized services. The level of complexity has increased with virtualization, mobility and on-premises connection to cloud data centers.

Figure 11 Cisco DNA Center Architecture (DNAC)



Cisco DNA Center is a full-fledged management application that includes a Cisco proprietary SDN controller. It provides a global view of all physical and virtual machines (VM) that are centrally managed. The functional components of Cisco DNA Center include design, provision, policy, and assurance. Intent-based REST API modules are enabled for discovery, configuration, automation, and monitoring purposes. That is supported for both fabric and non-fabric infrastructure.

DNA Center is installed on an appliance that is connected to a shared services block at a data center. There is also ISE, DHCP, DNS and NTP server deployed to a shared services block. It is common to also install configuration management tools such as Ansible or NETCONF as well to augment configuration automation tasks.

Table 7 Traditional vs Controller-Based Networking

Traditional	Controller-Based
silo	global
distributed	centralized
physical	logical
static	programmable
single-task	orchestration
local	unified
device	network
trial and error	assurance
point-in-time	real-time

Cisco DNA Center enables northbound REST APIs and workflows to manage fabric and non-fabric devices. REST APIs communicate with network devices and perform functions via HTTP methods (GET, POST, PUT, DELETE). For example, to create a new fabric site would require REST API POST request. Any updates to a new site such as changing fabric site name would use PUT method. GET request is used to read device configuration or collect operational state. JSON is the data encoding supported with Cisco Intent-based REST APIs.

Network discovery is started to populate inventory with all detected network devices. GET method collects information on clients, sites, topology, devices and operational state. It reads resources such as configuration script while POST method creates a new configuration.

Next, policies are defined with configuration settings and security access for each device class and functional roles. The provisioning workflows add network devices to sites, push configuration based on policies, and create fabric domains. Finally there is assurance to enable performance monitoring, operational state and management of all network elements.

CCNA IOS Show Commands

The following is a list of the most common IOS commands associated with questions from the CCNA exam. They are all standard IOS commands used to configure, verify and troubleshoot network connectivity. The IOS commands are based on all topics from the published CCNA exam guidelines.

Cisco CLI Help Facility

Mode Level

The List of commands available from each Cisco device mode is available with question mark **?** from each top level mode prompt.

rommon > **?**
switch > **?**
switch# **?**
switch(config)# **?**
switch(config-if)# **?**

Command Level

The command level **?** provides a list of all commands for that subgroup such as show commands for instance. In addition the question **?** after any IOS command displays syntax options for that specific command. It is a quick reference for correct configuration syntax and commands not supported with the current IOS version.

switch# **show ?**
switch(config)# **vtp mode ?**
switch(config-if)# **?**
switch(config-if)# **show interfaces ?**

Partial Commands

The partial command level question **?** provides a list of all commands that begin with the letters specified. That helps list commands available that start with the same letters.

switch# **c?**

Systems Management

show running-config

Display the current running configuration script on any Cisco device.

show version

Display a variety of information on device configuration including the following:

- IOS version
- license feature set
- configuration register setting
- hardware

show memory

Display the total, used and available memory on a Cisco device.

show process cpu

Display the CPU utilization for a Cisco device at five minute intervals.

dir /all

Display all files and subdirectories for a file systems.

show flash

List the files currently on flash memory including available memory.

erase nvram:

Delete all the files on NVRAM including the startup configuration.

erase startup-config

Delete the startup configuration file on NVRAM.

copy tftp: flash:

Copy IOS image file to local Flash memory

copy nvram:startup-config ftp | tftp | rcp

Backup startup-config to filesystem ftp | tftp | rcp

show users all

Display all inbound connections to the local device including VTY, console and AUX lines.

show terminal

Display terminal settings for the current terminal line and transport protocols allowed for remote management access (SSH, Telnet etc.)

show logging

Verify the logging configuration and where it is enabled/disabled on the network device. List all error messages logged for a specific device.

show ip interface brief

Summarize the operational status (up/up) and IP address assigned to all network interfaces. The Status column is Interface (Layer 1). The Protocol column is Line Protocol (Layer 2). The subnet mask is not displayed with the IP address.

show protocols

Verify operational status (up/up), IP address and subnet mask of all network interfaces.

show interfaces [interface]

Display the operational status (up/up), IP address, configuration settings and errors for a specific switch or router interface.

- operational status
- speed
- duplex
- MTU
- interface errors

Network Access

show vlan brief

Display all configured VLANs, active status and switch ports assigned.

show vlan

Display all configured VLANs, verify active status and any switch ports assigned. There is some additional VLAN information provided as well.

show interface switchport

Display the operational mode and administrative mode for local switch ports and enable status.

show interfaces trunk

Verify the operational status of trunk interfaces and configuration settings:

- switch port members
- allowed VLANs
- native VLAN
- encapsulation type
- trunk mode

show interface port-channel [number]

Verify operational status and errors for an EtherChannel port channel interface.

- IP address
- speed
- duplex
- MTU
- interface errors
- port members

show etherchannel summary

Verify all EtherChannel links configured on switch and operational status.

- operational status
- channel group number
- negotiation protocol (PAgP/LACP)
- switch ports assigned

show spanning-tree vlan [number]

Display spanning tree information for a specific VLAN.

- root bridge
- timers
- STP port types (local interfaces)
- port path cost

show spanning-tree interface [interface]

Display the spanning tree information for a specific switch interface.

- STP port type
- STP port state
- port path cost
- STP timers

show spanning-tree

Display the bridge ID for the local switch and root bridge ID for each VLAN including priority and timer settings.

- local bridge ID, priority and timers
- root bridge priority per VLAN
- root bridge MAC address per VLAN
- priority and path cost for local switch ports

show spanning-tree summary

Display the spanning tree protocol on the switch.

- spanning tree protocol enabled
- root bridge ID for each VLAN
- STP enhancements (PortFast etc.).
- STP port states per VLAN

show mac address-table

Display MAC address, port number and VLAN of each host connected to the local switch.

show cdp neighbor detail

Display all directly connected neighbor devices and confirm Layer 2 connectivity to each neighbor and the following neighbor details.

show cdp

Verify that CDP is enabled, update timer, hold timer and CDP version.

show lldp

Verify that LLDP is enabled and timer settings.

show port-security interface [interface]

Display the port security configuration for a switch port.

IP Connectivity

ping [ip address] [hostname]

Confirms Layer 3 connectivity between source and destination based on ICMP packets.

traceroute [ip address] [hostname]

Confirm the routing path for Layer 3 connectivity between source and destination.

show ip route

Display the routing table for the local router that includes all known subnets, routing protocol, next hop address, metrics and administrative distance..

show ip protocols

Display a variety of settings and configuration for all enabled routing protocols on the router.

show ip ospf interface [interface]

Verify the operational status (up/up) of an OSPF enabled interface including the following.

- IP address
- area assigned
- process ID
- router ID
- network type
- timers

show ip ospf database

Display the OSPF link state database topology that includes links for all OSPF neighbors

show ip ospf neighbor

Verify all OSPF adjacencies established with connected OSPF neighbors.

- neighbor router ID
- neighbor IP address
- adjacency state
- assigned DR/BDR

IP Services

show ip dhcp conflict

Display all IP address conflicts detected on the IOS DHCP server.

show ip dhcp binding

Display IP address and MAC address of DHCP client, lease expiration on the IOS DCHP server.

show ip dhcp pool

Display the pool range of assigned IP addresses, leased addresses and any pending events.

show ip dhcp snooping

Verify that DHCP snooping is enabled along with assigned VLANs and interfaces enabled for snooping.

show ip arp inspection

Display the configuration for ARP inspection including assigned VLAN, active status and counters.

show ip nat translations

Verify the NAT addressing assigned for translating between private and public addressing.

show ntp status

Verify clock synchronization status to an NTP server, IP address of NTP server, stratum and clock signaling.

show standby

Display the HSRP configuration on the local router for the router group configured.

show access-lists

Display all IPv4 access control lists configured on the local router to verify filtering of packets.

***IPv6 Commands**

Replace **ip** with **ipv6** for all IOS show commands.

Host Commands

ipconfig /all

Display host TCP/IP settings including IPv4 address, default gateway, DNS server and MAC address.

ifconfig –a

Display host TCP/IP settings for Linux clients.

telnet [ip address]

Telnet session from a host computer to remotely manage network devices. There is an option to specify IP address or hostname.

ssh –l [username] [ip address]

SSH session from a host computer to remotely manage network devices. There is an option to specify IP address or hostname.

CCNA Configuration Tool

Login to global configuration mode.

router > **enable**
router# **configure terminal**
router(config)#

Encrypt clear text passwords in configuration files.

service password-encryption

Configure enable password cisconet with level 15 privilege.

enable password cisconet

Configure local authentication username admin with privileged EXEC level security and secret password ccnaexam.

username admin privilege 15 secret ccnaexam

Configure local authentication username cisco with user EXEC level security and password cisconet.

username cisco privilege 1 password cisconet

Configure VTY 0 4 default lines to enable login with password cisconet and a timeout of 5 minutes. Enable password is required for Telnet.

line vty 0 4
password cisconet
login
exec-timeout 5

Enable local authentication on VTY 0 4 lines.

line vty 0 4
login local

Configure console port with password cisconet for access security.

line console 0
password cisconet
login

Configure PST timezone on a Cisco device.

clock timezone PST -8

Configure SSH version 2 for management access.

crypto key generate rsa
ip ssh version 2
ip domain-name cisconet.com

Configure Cisco device to only permit inbound SSH connections on default VTY lines.

line vty 0 4
transport input ssh

Configure SNMP community string to read-only access with password cisco. Configure a string with a read/write access and password ccna.

snmp-server community cisco ro
snmp-server community ccna rw

Configure an external syslog server IP address for sending local system messages.

logging on
logging host 192.168.3.1

Configure DNS domain name for network services.

ip domain-name ccna.cisconet.com

Configure DNS server where requests are sent that originate from that Cisco network device.

ip name-server 172.16.1.2

Configure NTP external time server as authoritative time source for Cisco device.

ntp server 172.16.1.1

Enable web-based management of Cisco network devices.

ip http secure-server
ip http authentication local

Configure switch port access mode, assign VLAN 10 and link autonegotiation.

```
interface fastethernet0/1
switchport mode access
switchport access vlan 10
duplex auto
speed auto
```

Configure voice VLAN on a switch access port.

```
interface fastethernet0/1
switchport mode access
switchport voice vlan 10
```

Configure Trunking with native VLAN 999 and allow VLANs 10-12 on a default configuration.

```
interface fastethernet0/1
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 10-12
```

Enable DTP on a switch port to send request frames and negotiate dynamic trunking with neighbor switch.

```
interface fastethernet0/1
switchport mode dynamic desirable
```

Configure LACP active mode on switch port Fa0/1 and Fa0/2 for dynamic EtherChannel negotiation and assign to channel group 1.

```
interface range fastethernet0/1
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active

interface range fastethernet0/2
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active

interface port-channel 1
switchport mode trunk
switchport nonegotiate
```

Configure Layer 3 switch port as a port channel with LACP active mode for dynamic EtherChannel negotiation and assign to port channel 1.

```
interface gigabitethernet0/1
no switchport
channel-group 1 mode active

interface port-channel 1
ip address 192.168.3.1 255.255.255.0
no shutdown
```

Enable Rapid PVST+ globally on a switch.

```
spanning-tree mode rapid-pvst
```

Configure PortFast and BPDU guard on a switch port.

```
interface fastethernet0/1
switchport mode access
switchport access vlan 10
spanning-tree portfast
spanning-tree bpduguard enable
```

Configure Layer 2 switch with a default gateway for Telnet management access.

```
ip default-gateway 172.16.1.3
```

Enable CDP globally on a Cisco network device.

```
cdp run
```

Enable LLDP globally on a Cisco network device.

```
lldp run
```

Enable IPv6 packet forwarding globally on a Cisco network device.

```
ipv6 unicast-routing
```

Enable IPv6 address autoconfiguration.

```
interface fastethernet1/0
ipv6 address autoconfig
```

Configure an IPv6 address that generates host portion identifier from the interface MAC address.

```
interface fastethernet1/0
ipv6 address 2001:db8:3c4d:4::/64 eui-64
```

Configure IPv4 static route to destination 172.16.1.0/24 with next hop 172.16.2.1

ip route 172.16.1.0 255.255.255.0 172.16.2.1

Configure IPv4 default route with next hop of 172.33.1.2

ip route 0.0.0.0 0.0.0.0 172.33.1.2

Configure IPv4 floating static route to destination 192.168.3.0/24 with next hop 192.168.2.2 and administrative distance = 200.

ip route 192.168.3.0 255.255.255.0 192.168.2.2 200

Configure OSPFv2 globally advertising subnet 192.168.0.0/16 to area 0 and 172.16.1.0/24 to area 0.

router ospf 1
router-id 172.16.1.255
network 192.168.0.0 0.0.255.255 area 0
network 172.16.1.0 0.0.0.255 area 0

Configure OSPF on a physical interface and advertise 192.168.1.0/24 subnet to area 10.

interface fastethernet1/1
ip address 192.168.1.1 255.255.255.0
ip ospf 1 area 10
no shutdown

Configure network type on OSPF interface for point-to-point and disable Designated Router (DR) election.

interface fastethernet1/1
ip address 192.168.1.1 255.255.255.0
ip ospf 1 area 0
ip ospf network point-to-point
no shutdown

Configure port security on a switch interface and add MAC address dynamically to running configuration. Limit number of hosts for the switch port to a maximum of one.

interface fastethernet0/1
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1

Enable DHCP snooping for specific VLANs and configure a physical interface as trusted with rate limiting of packets.

ip dhcp snooping
ip dhcp snooping vlan 1,10

interface fastethernet0/1
ip dhcp snooping trust
ip dhcp snooping limit rate 40

Enable dynamic ARP inspection on VLAN 10,11,12.

ip arp inspection vlan 10-12

Configure DHCP relay on a router.

interface fastethernet0/1
ip address 172.16.3.1 255.255.255.0
ip helper-address 172.16.1.2

Configure DHCP relay address on a Layer 3 switch for VLAN 10 hosts.

interface Vlan 10
ip helper-address 172.16.1.2

Configure NAT pool internet with public address 172.33.1.1/24 and **overload** keyword for port address translation. Configure ACL 100 to enable internet access for hosts on 192.168.1.0/24 subnet. Enable NAT on inside and outside interface.

ip nat pool internet 172.33.1.1 172.33.1.1 netmask 255.255.255.0
ip nat inside source list 100 pool internet overload
access-list 100 permit ip 192.168.1.0 0.0.0.255 any

interface gigabitethernet0/0
ip nat inside
interface gigabitethernet0/1
ip nat outside

Configure static NAT between inside local IP address 192.168.1.1 (private) and outside global IP address 200.200.1.1 (internet routable).

ip nat inside source static 192.168.1.1 200.200.1.1

CCNA 200-301: Score Your Best

CCNA certification has become increasingly complex with questions from multiple knowledge domains and topics. The following is a description of the questions types on the CCNA exam.

Multiple Choice

Question that asks the candidate to select the correct answer/s from multiple options.

Drag and Drop

Match a list of items such as protocols or network devices for example, with the correct description.

Fill-in-the-Blank

Determine a word/s to finish a statement so that it is correct.

CCNA Exam Strategy

The following are exam strategy recommendations to score your best on the new CCNA exam.

- The testing center will give you double-sided laminated paper at the beginning of the exam. Request 3-5 of them so you are not interrupting your exam. There is a 15-minute tutorial before the exam starts. Use that time to create your whiteboard notes. It is a collection of facts and figures that you have for quick reference.

- **Create CCNA Whiteboard** - subnetting table, binary table, AD values, port numbers, protocol facts, default settings, wildcard masks, ACL stuff and anything else that you often forget.

- **Pre-exam practice tests** are essential and when designed properly should verify your readiness for the exam. Select practice tests that include all topics with percentages assigned and simulation labs.

- Subnetting is a key aspect of the CCNA exam for many types of questions. It is easy to make mistakes when converting binary and decimal values. Write out the class C subnetting table on paper when the exam starts. Include the binary conversion table as well for quick reference.

- Don’t burn time with a question you could only guess on. Take your best guess and move on to the next question.

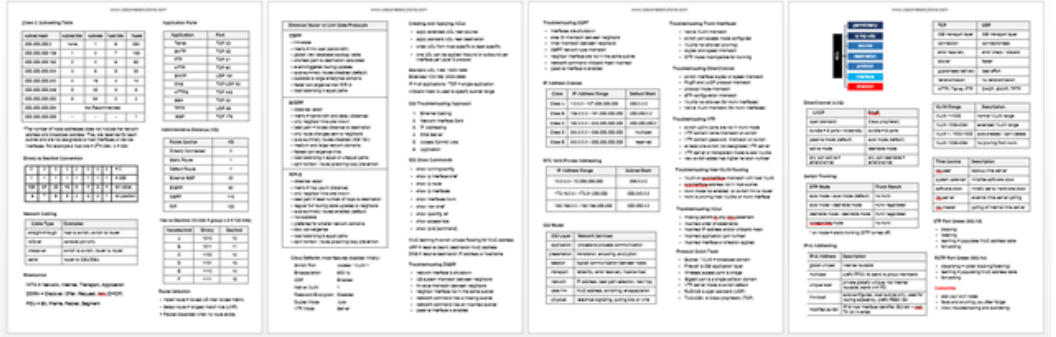
- Verify each answer and **Do not click Next** until you are satisfied with your answer and ready for the next question. There is no review allowed for questions or navigation permitted to a previous question.

- Do not waste time considering your answers from previous questions. There is no back button or end of test question review with CCNA.

- Read each question a couple of times, carefully noting keywords and subtleties to determine what the question is testing.

CCNA Whiteboard

There is a 15-minute tutorial before the CCNA exam starts. You have that time to create your whiteboard notes on laminated paper provided at the testing center. There is a virtual whiteboard provided as well for online testing option. CCNA whiteboard here is an essential study review to do your best. The whiteboard should include subnetting table, binary conversion table, IOS commands, port numbers, wireless, SDN, route selection, AD values, OSPFv2, ACLs, Cisco default settings and anything else you often forget.



www.cisconetsolutions.com