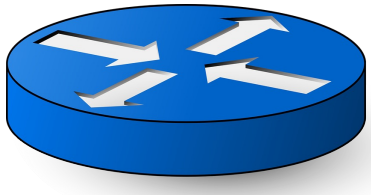
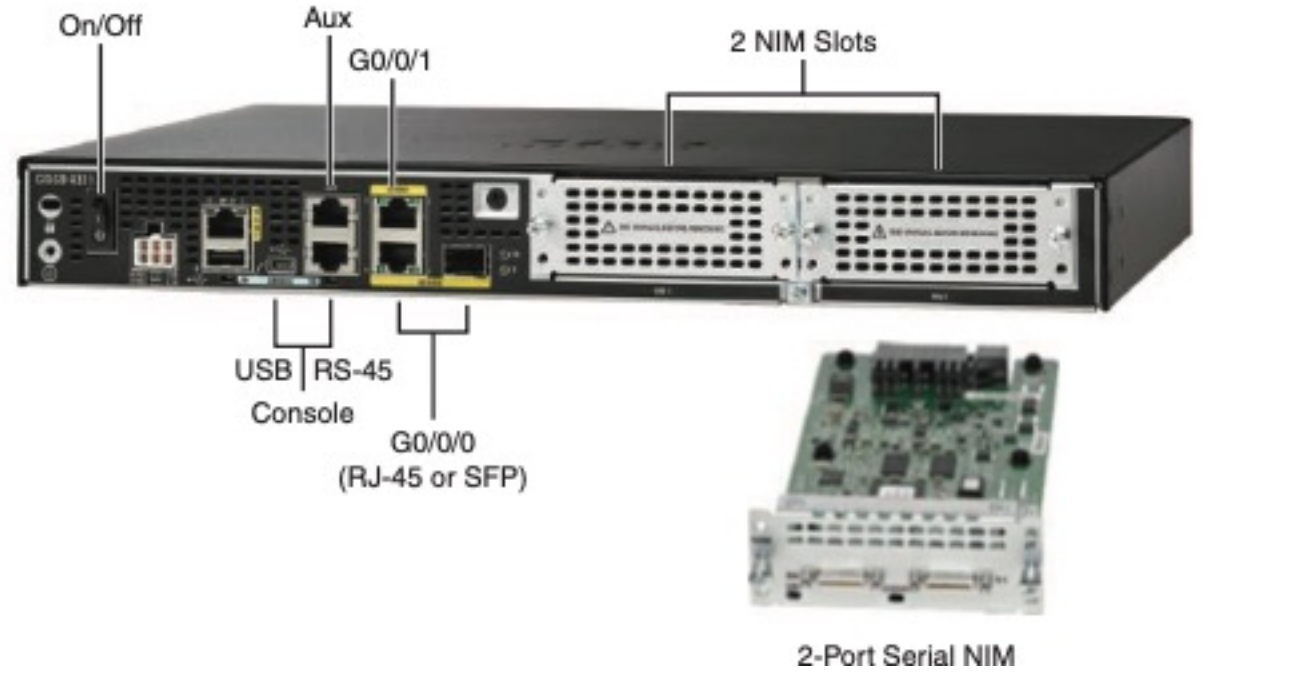


Router

router wont forward broadcast frame

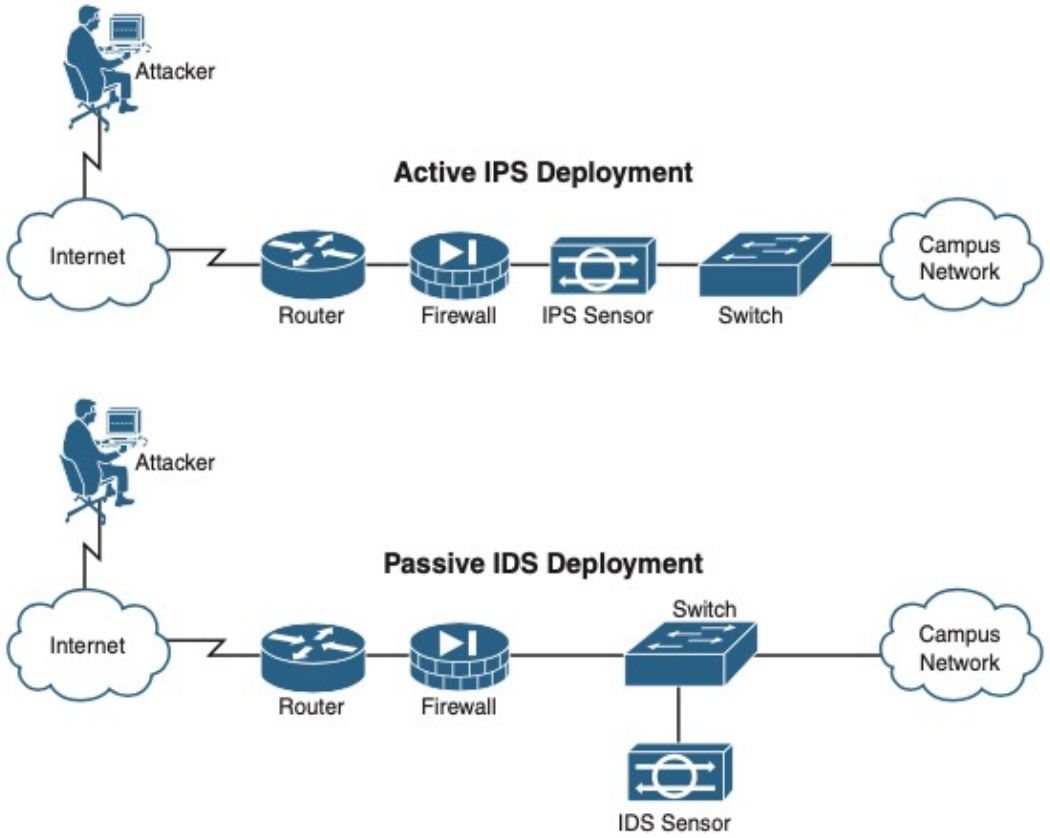
Router Ports Representation

Figure 31-10 Backplane of the Cisco 4321 Integrated Services Router (ISR)

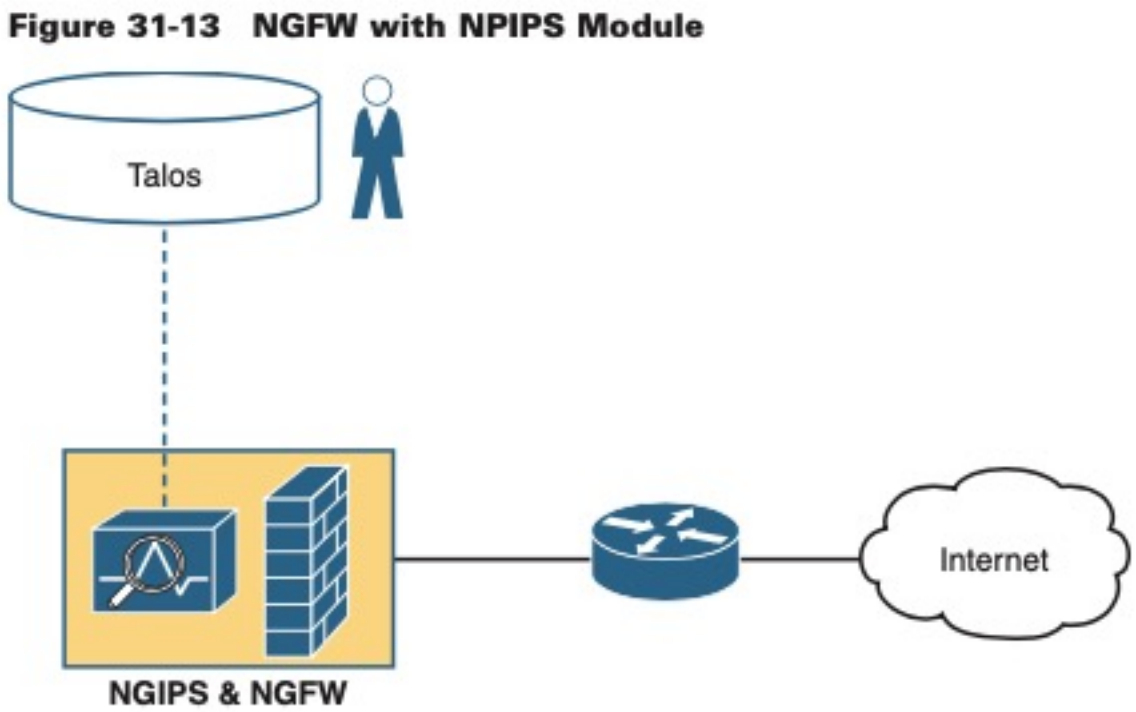


IDS and IPS placement in the Network

Figure 31-12 IPS and IDS Comparison



NEXT GEN Firewalls Placement



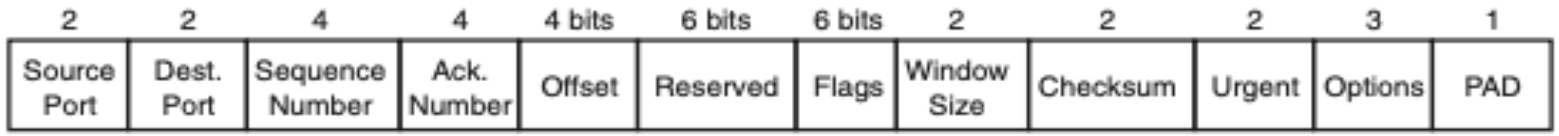
IP Class

Table 11-2 RFC 1918 Private Address Space

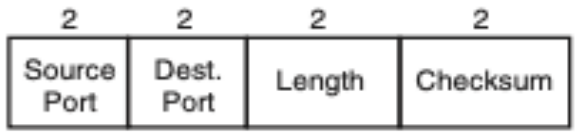
Class of Networks	Private IP Networks	Number of Networks
A	10.0.0.0	1
B	172.16.0.0 through 172.31.0.0	16
C	192.168.0.0 through 192.168.255.0	256

TCP UDP Header

Figure 31-7 TCP and UDP Headers



TCP Header



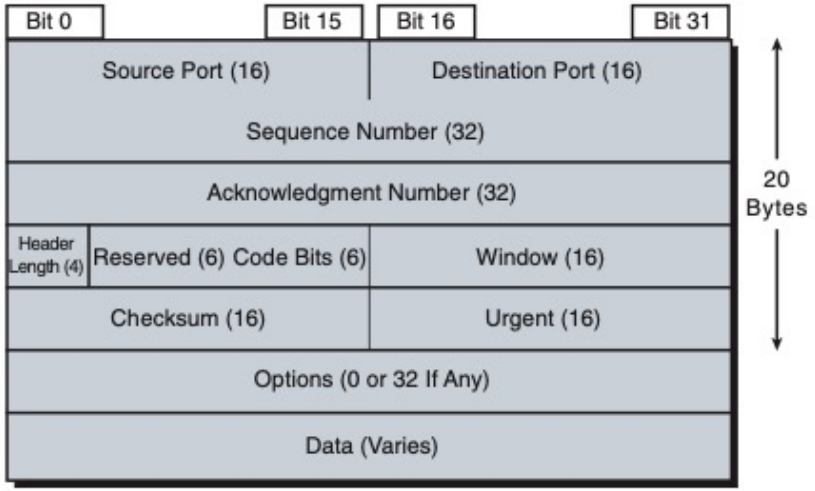
UDP Header

TCP Header

TCP Header

TCP provides error recovery, but to do so, it consumes more bandwidth and uses more processing cycles than UDP. TCP and UDP rely on IP for end-to-end delivery. TCP is concerned with providing services to the applications of the sending and receiving computers. To provide all these services, TCP uses a variety of fields in its header (see Figure 31-2).

Figure 31-2 TCP Header



TCP IP Data Encapsulation

Data Encapsulation Summary

Each layer of the TCP/IP model adds its own header information. As the data travels down through the layers, it is encapsulated with a new header. At the network access layer, a trailer is also added. This encapsulation process is described in five steps:

Step 1. Create and encapsulate the application data with any required application layer headers. For example, the HTTP OK message can be returned in an HTTP header, followed by part of the contents of a web page.

Step 2. Encapsulate the data supplied by the application layer inside a transport layer header. For end-user applications, a TCP or UDP header is typically used.

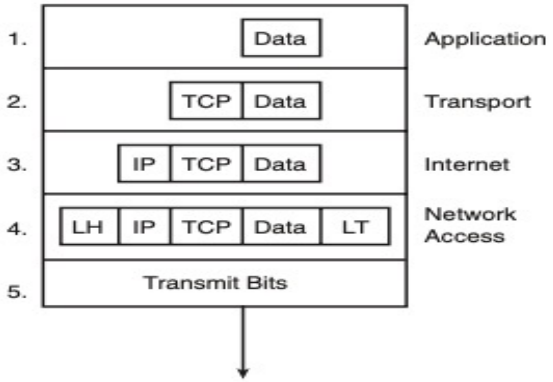
Step 3. Encapsulate the data supplied by the transport layer inside an Internet layer (IP) header. IP is the only protocol available in the TCP/IP network model at the Internet layer.

Step 4. Encapsulate the data supplied by the Internet layer inside a network access layer header and trailer. This is the only layer that uses both a header and a trailer.

Step 5. Transmit the bits. The physical layer encodes a signal onto the medium to transmit the frame.

The numbers in Figure 31-8 correspond to the five steps in the list, graphically showing the same encapsulation process.

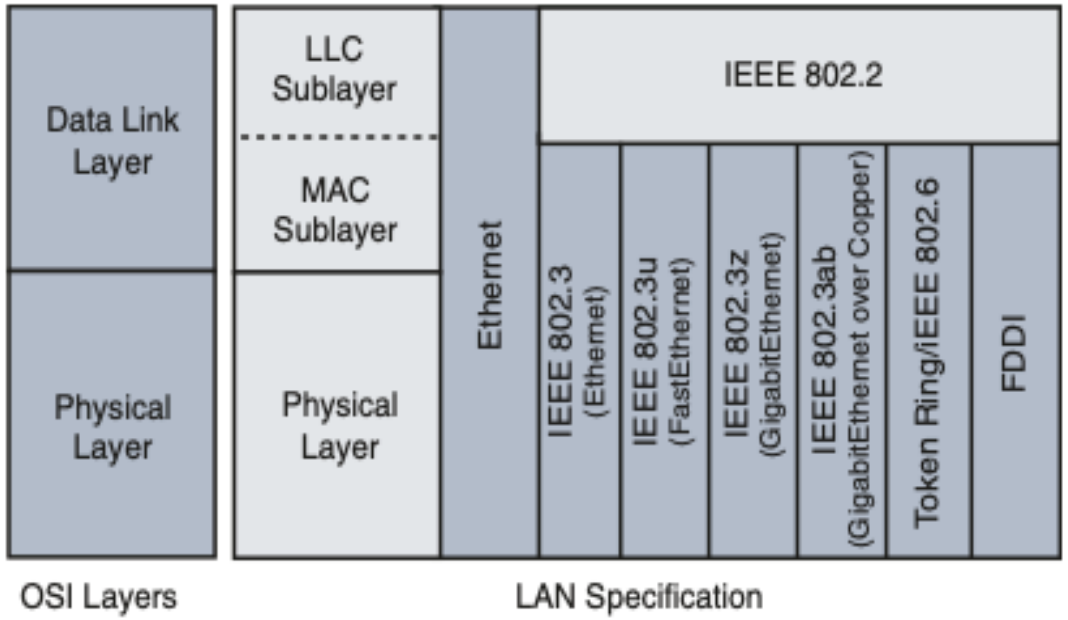
Figure 31-8 Five Steps of Data Encapsulation



NOTE: The letters LH and LT stand for link header and link trailer, respectively, and refer to the data link layer header and trailer.

Ethernet Standard of the OSI

Figure 30-2 Ethernet Standards and the OSI Model



Terminal history Buffer

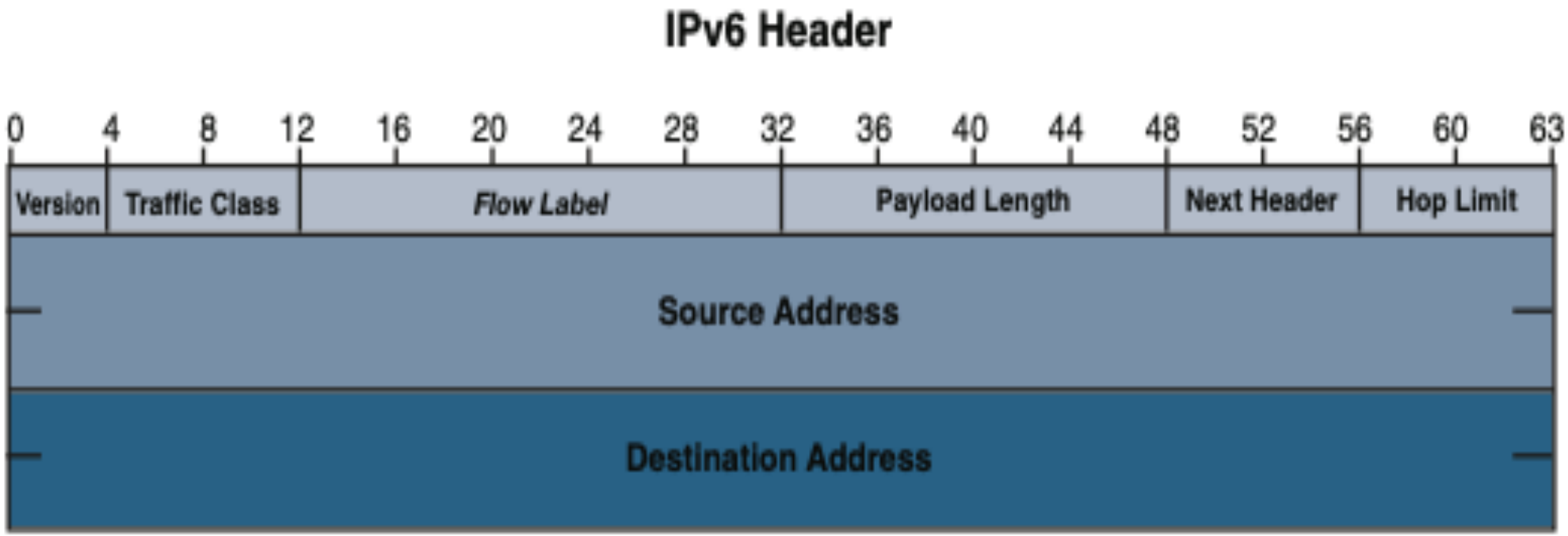
Table 29-3 Command History Buffer Commands

Command Syntax	Description
`switch# show history`	Displays the commands currently stored in the history buffer.
`switch# terminal history`	Enables terminal history. This command can be run from either user or privileged EXEC mode.
`switch# terminal history size 50`	Configures the terminal history size. The terminal history can maintain 0–256 command lines.
`switch# terminal no history size`	Resets the terminal history size to the default value of 20 command lines in Cisco IOS 15.
`switch# terminal no history`	Disables terminal history.

IPV6

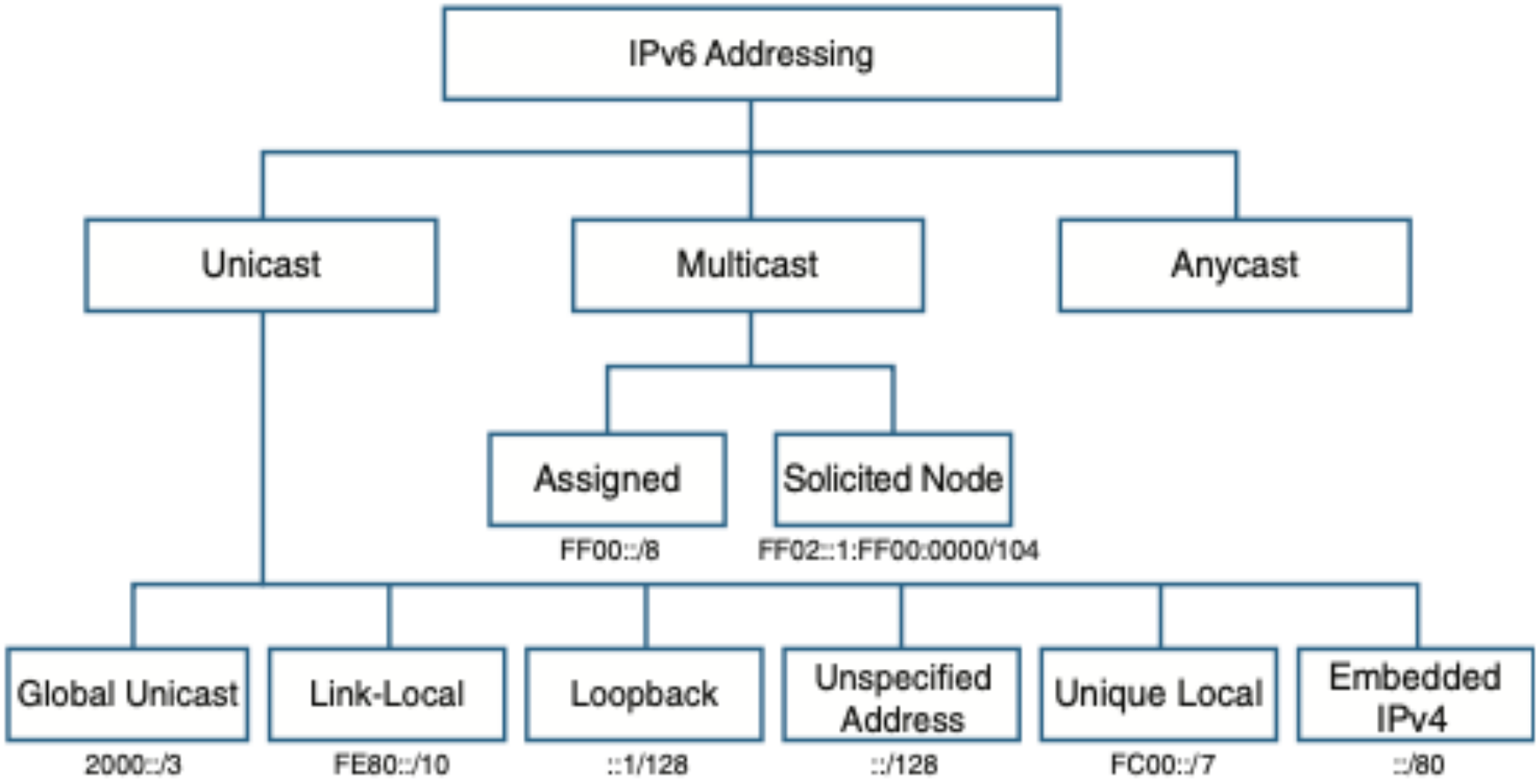
- IPV6 is 128 Bits in length
- IPV6 uses NDP which is the equivalent of ARP
- IPV6 Have the link-local address which is FE80

IPV6 Header


IPv6 Header
0
4
8
12
16
20
24
28
32
36
40
44
48
52
56
60
63
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address

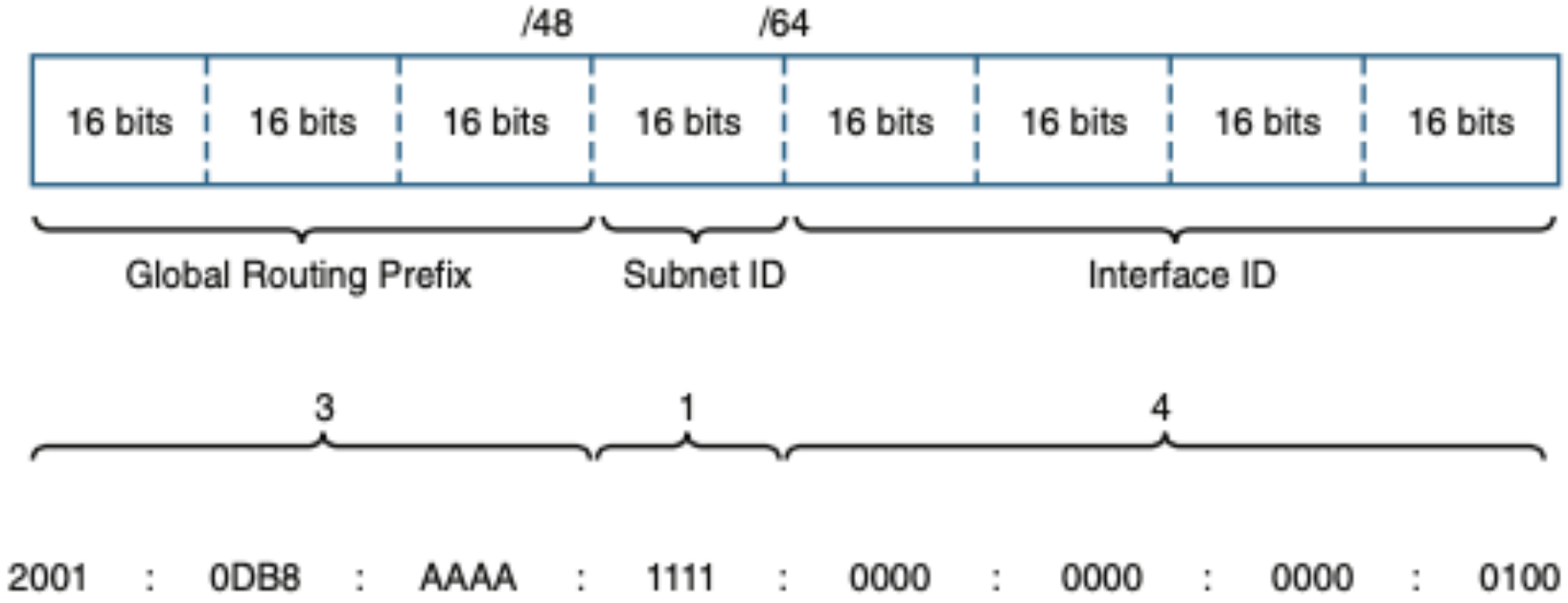
IPV6 Address Type

Figure 27-2 IPv6 Address Types



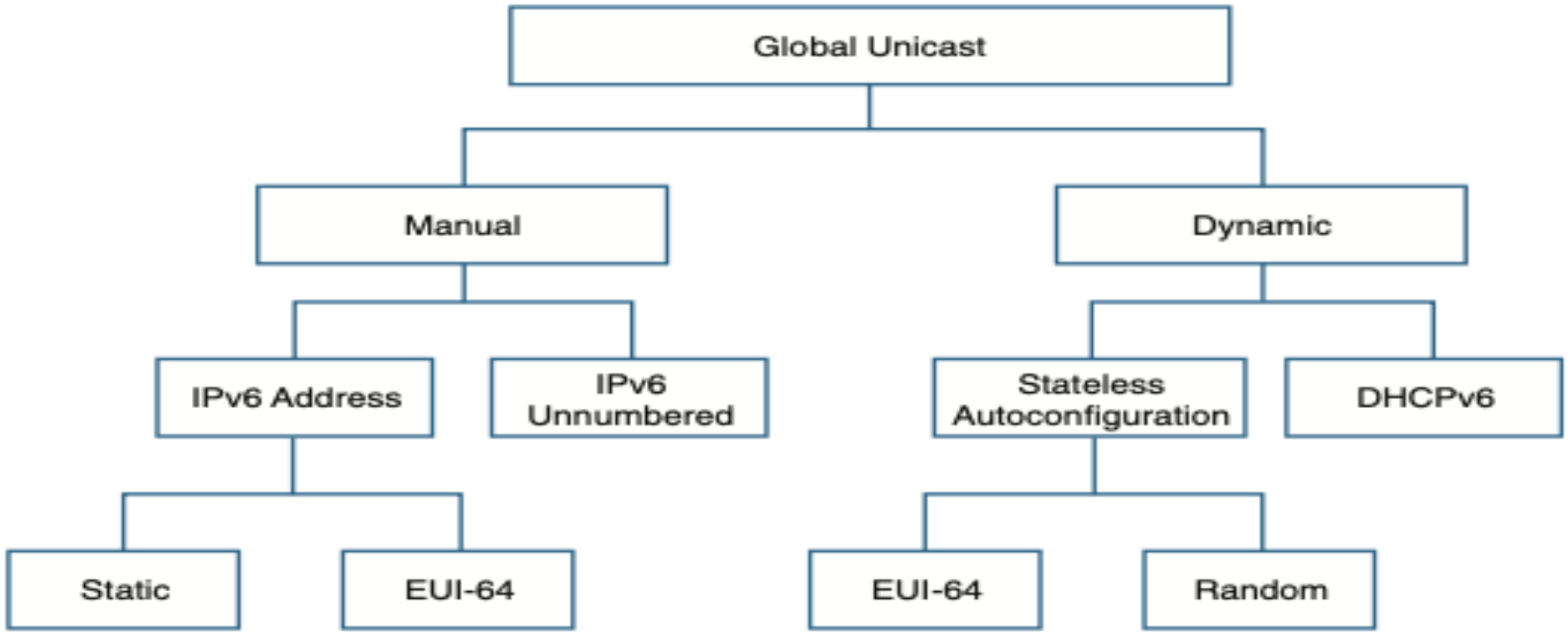
Global Unicast Structure

Figure 27-3 Graziani's 3-1-4 Rule for Remembering the Global Unicast Address Structure



Global unicast Configuration Option

Figure 27-6 Global Unicast Address Configuration Options



Summary of Global Unicast Configuration

Table 27-2 Summary of Global Unicast Configuration Options

Global Unicast	Configuration Option	Description
Manual	Static	Much as with IPv4, the IPv6 address and prefix are statically configured on the interface.
	EUI-64	The prefix is configured manually. The EUI-64 process uses the MAC address to generate the 64-bit interface ID.
	IPv6 unnumbered	Much as with IPv4, an interface can be configured to use the IPv6 address of another interface on the same device.
Dynamic	Stateless address autoconfiguration	SLAAC determines the prefix and prefix length from neighbor discovery router advertisement messages and then creates the interface ID using the EUI-64 method.
	DHCPv6	Much as with IPv4, a device can receive some or all of its addressing from a DHCPv6 server.

IPV6 NDP Functions

Key Topic

Table 25-3 NDP Function Summary

Function	Protocol Messages	Who Discovers Info	Who Supplies Info	Info Supplied
Router discovery	RS and RA	Any IPv6 host	Any IPv6 router	Link-local IPv6 address of router
Prefix/length discovery	RS and RA	Any IPv6 host	Any IPv6 router	Prefix(es) and associated prefix lengths used on local link
Neighbor discovery	NS and NA	Any IPv6 host	Any IPv6 host	Link-layer address (for example, MAC address) used by a neighbor
Duplicate Address Detection	NS and NA	Any IPv6 host	Any IPv6 host	Simple confirmation whether a unicast address is already in use

Summary of IPv6 Address Types

Key Topic

Table 24-5 Summary of IPv6 Address Types and the Commands That Create Them

Type	Prefix/Address Notes	Enabled with What Interface Subcommand
Global unicast	Many prefixes	**ipv6 address** *address/prefix-length* **ipv6 address** *prefix/prefix-length* **eui-64**
Unique Local	FD00::/8	**ipv6 address** *prefix/prefix-length* **eui-64**
Link local	FE80::/10	**ipv6 address** *address* **link-local** Autogenerated by all **ipv6 address** commands Autogenerated by the **ipv6 enable** command
All hosts multicast	FF02::1	Autogenerated by all **ipv6 address** commands
All routers multicast	FF02::2	Autogenerated by all **ipv6 address** commands
Routing protocol multicasts	Various	Added to the interface when the corresponding routing protocol is enabled on the interface
Solicited-node multicast	FF02::1:FF /104	Autogenerated by all **ipv6 address** commands

IPV6 Multicast Scope

as noted in Table 24-4.

Key Topic

Table 24-4 IPv6 Multicast Scope Terms

Scope Name	First Quartet	Scope Defined by...	Meaning
Interface-Local	FF01	Derived by Device	Packet remains within the device. Useful for internally sending packets to services running on that same host.
Link-Local	FF02	Derived by Device	Host that creates the packet can send it onto the link, but no routers forward the packet.
Site-Local	FF05	Configuration on Routers	Intended to be more than Link-Local, so routers forward, but must be less than Organization-Local; generally meant to limit packets so they do not cross WAN links.
Organization-Local	FF08	Configuration on Routers	Intended to be broad, probably for an entire company or organization. Must be broader than Site-Local.
Global	FF0E	No Boundaries	No boundaries.

IPV6 Local-Scope Multicast Address

Table 24-3 Key IPv6 Local-Scope Multicast Addresses

Short Name	Multicast Address	Meaning	IPv4 Equivalent
All-nodes	FF02::1	All-nodes (all interfaces that use IPv6 that are on the link)	224.0.0.1
All-routers	FF02::2	All-routers (all IPv6 router interfaces on the link)	224.0.0.2
All-OSPF, All-OSPF-DR	FF02::5, FF02::6	All OSPF routers and all OSPF-designated routers, respectively	224.0.0.5, 224.0.0.6
RIPng Routers	FF02::9	All RIPng routers	224.0.0.9
EIGRPv6 Routers	FF02::A	All routers using EIGRP for IPv6 (EIGRPv6)	224.0.0.10
DHCP Relay Agent	FF02::1:2	All routers acting as a DHCPv6 relay agent	None

IPV6 Routing Protocols

Table 22-2 IPv6 Routing Protocols

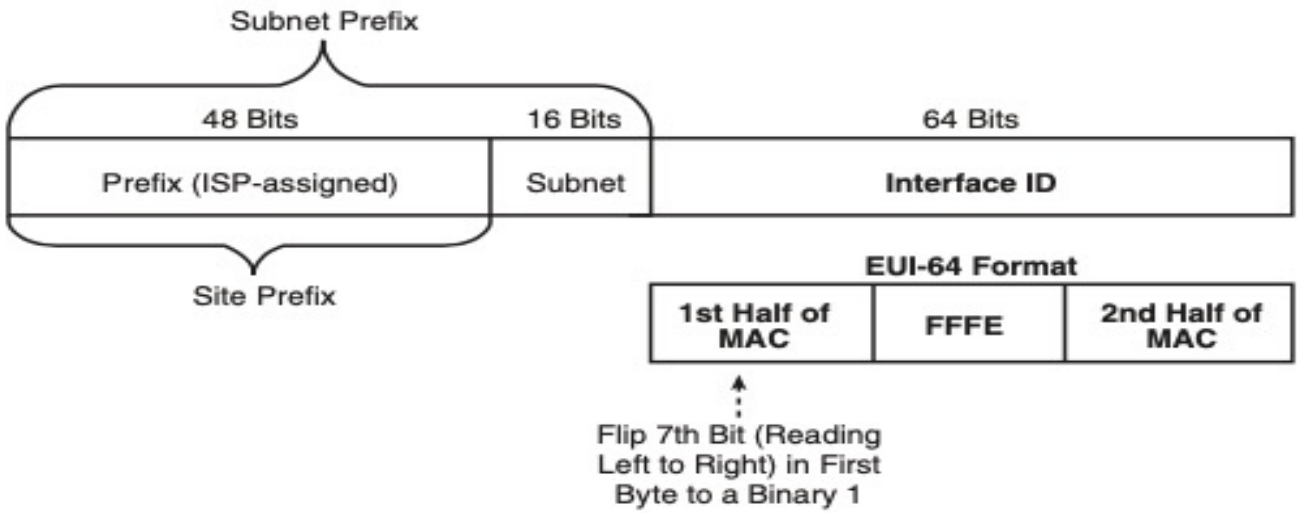
Routing Protocol	Defined By	Notes
RIPng (RIP next generation)	RFC	The "next generation" is a reference to a TV series, *Star Trek: the Next Generation*.
OSPFv3 (OSPF version 3)	RFC	The OSPF you have worked with for IPv4 is actually OSPF version 2, so the new version for IPv6 is OSPFv3.
EIGRPv6 (EIGRP for IPv6)	Cisco	Cisco owns the rights to the EIGRP protocol, but Cisco also now publishes EIGRP as an informational RFC.
MP BGP-4 (Multiprotocol BGP version 4)	RFC	BGP version 4 was created to be highly extendable; IPv6 support was added to BGP version 4 through one such enhancement, MP BGP-4.

IPV6 Format with interface ID and EUI-64

For example, the following two lines list a host's MAC address and corresponding EUI-64 format interface ID, assuming the use of an address configuration option that uses the EUI-64 format:

- **MAC address:** 0034:5678:9ABC
- **EUI-64 interface ID:** 0234:56FF:FE78:9ABC

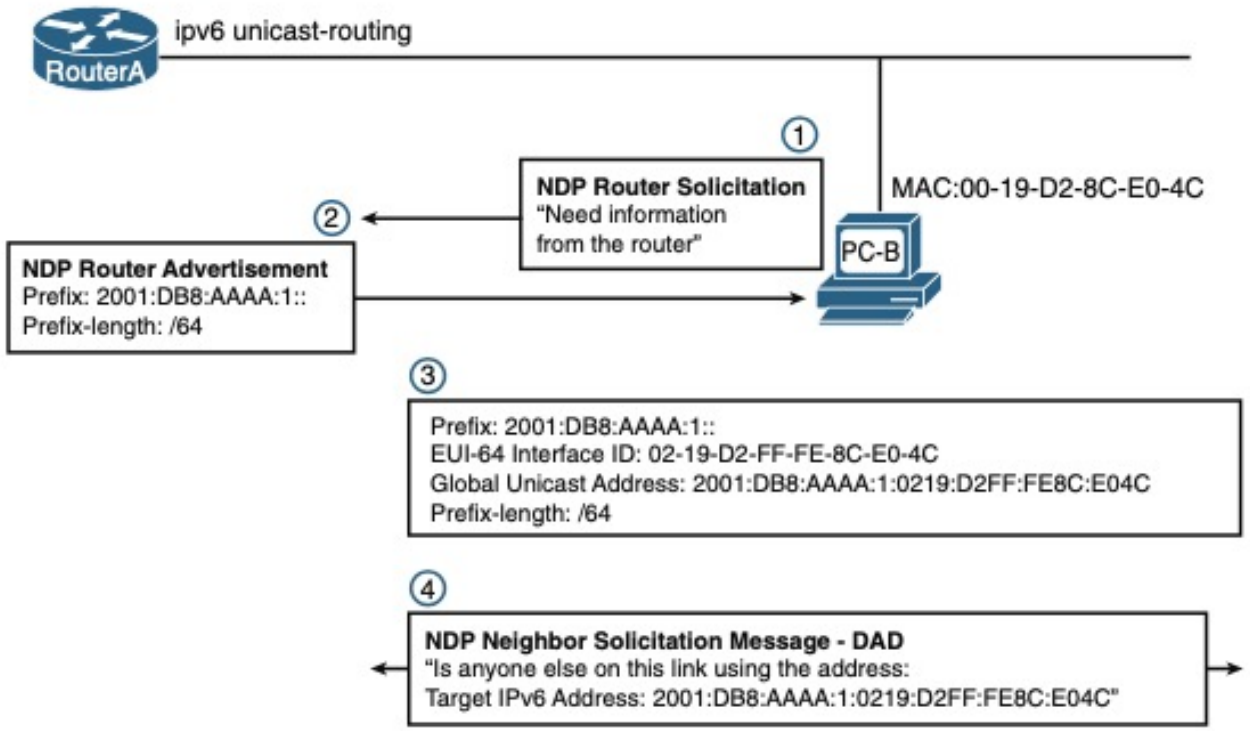
Figure 27-14 IPv6 Address Format with Interface ID and EUI-64



NOTE: To change the seventh bit (reading left to right) in the example, convert hex 00 to binary 00000000, change the seventh bit to 1 (00000010), and then convert back to hex, for hex 02 as the first two digits.

Neighbor Discovery and The SLAAC Process

Figure 27-15 Neighbor Discovery and the SLAAC Process



VPN Comparison

Table 14-4 Comparisons of Site-to-Site and Remote Access VPNs

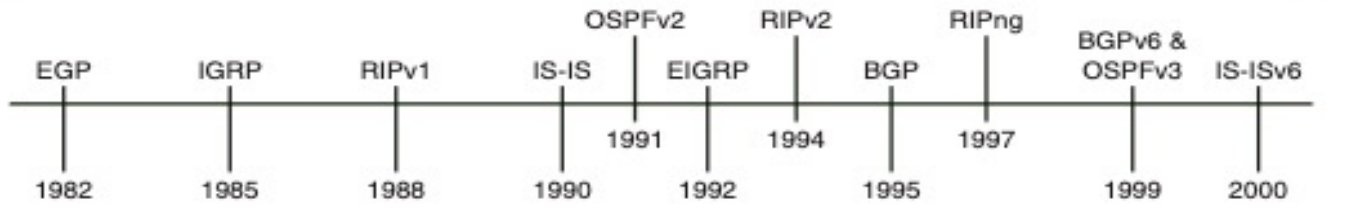
	Remote Access	Site-to-Site
Typical security protocol	TLS	IPsec
Devices supported by one VPN (one or many)	One	Many
Typical use: on-demand or permanent	On-demand	Permanent

Protocols

- RIP and EIGRP are Distance Vector Protocol
- OSPF and IS-IS Are Link State Protocol
- Link state Routing Protocol is Faster than Distance vector
- Lower Metric is considered a Better
- For a static route to be less preferred than a dynamic routing protocol the AD has to be higher

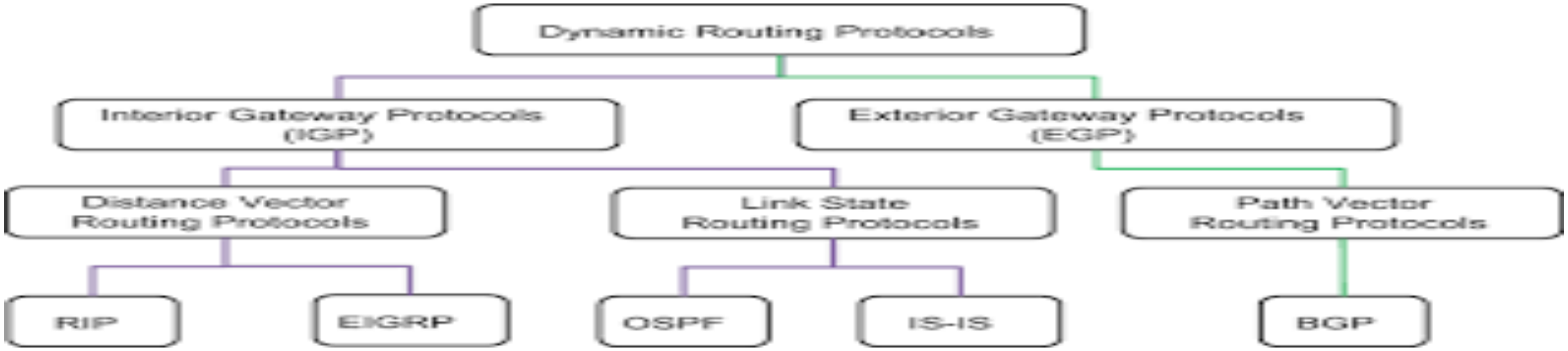
Evolution and Classification of Routing Protocols

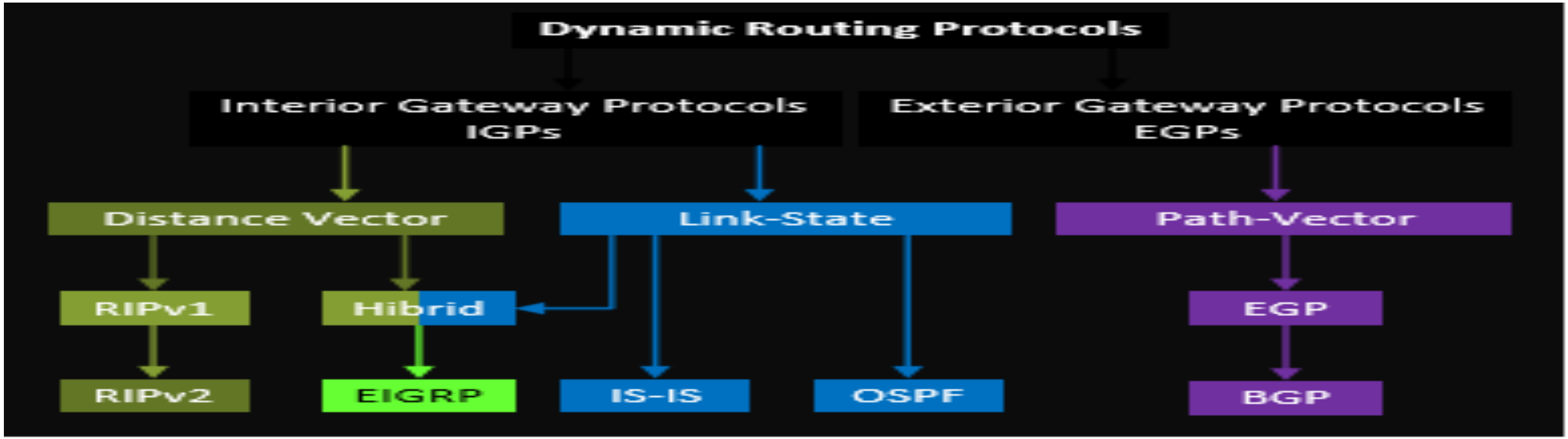
Figure 19-2 Evolution and Classification of Routing Protocols



	Distance Vector Routing Protocols		Link State Routing Protocols		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	MP BGP-4 (IPv6)

Dynamic Routing Protocol





OSPF Neighbors Adjacency Requirements

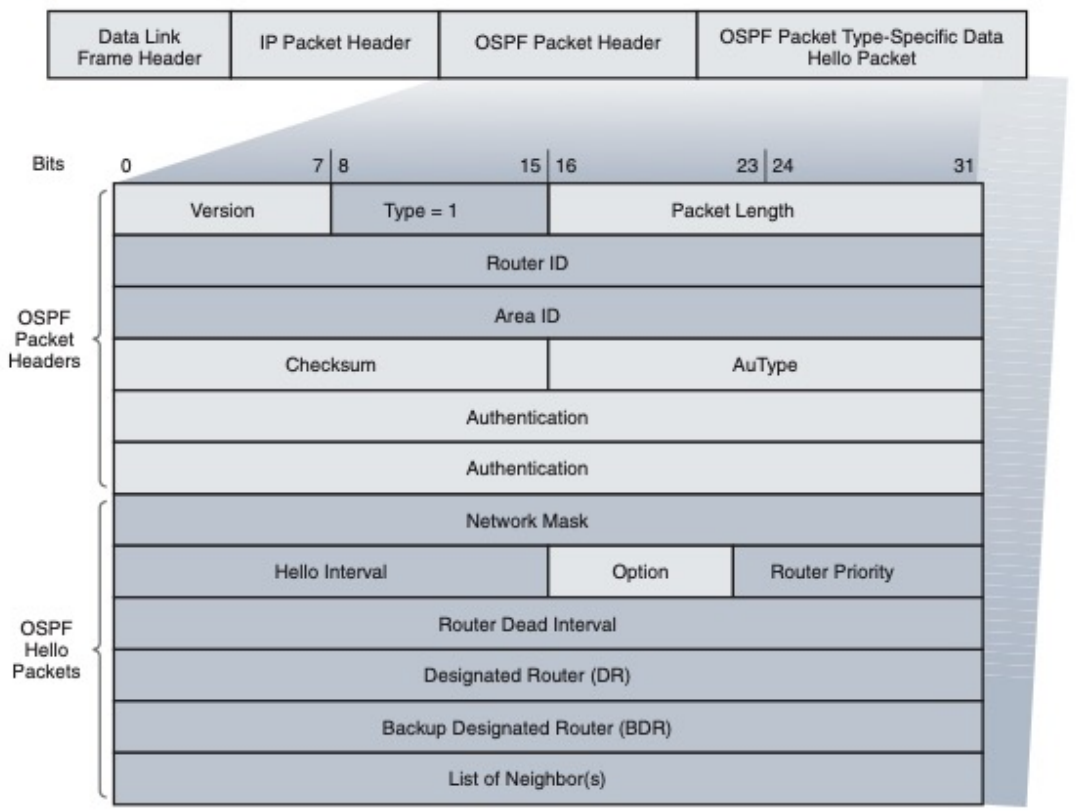
Key Topic

Table 21-3 Neighbor Requirements for OSPF

Requirement	Required for OSPF	Neighbor Missing if Incorrect
Interfaces must be in an up/up state.	Yes	Yes
Access control lists (ACL) must not filter routing protocol messages.	Yes	Yes
Interfaces must be in the same subnet.	Yes	Yes
They must pass routing protocol neighbor authentication (if configured).	Yes	Yes
Hello and hold/dead timers must match.	Yes	Yes
Router IDs (RID) must be unique.	Yes	Yes
They must be in the same area.	Yes	Yes
OSPF process must not be shut down.	Yes	Yes
Neighboring interfaces must use same MTU setting.	Yes	No
Neighboring interfaces must use same OSPF network type.	Yes	No

OSPF Packet Header and Hello types

Figure 14-2 OSPF Packet Header and Hello Packet



OSPF Link State

Link-State Advertisements

LSUs are the packets used for OSPF routing updates. An LSU packet can contain 11 types of LSAs, as Figure 14-3 shows.

Figure 14-3 LSUs Contain LSAs

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them.
2	DBD	Checks for database synchronization between routers.
3	LSR	Requests specific link-state records from router to router.
4	LSU	Sends specifically requested link-state records.
5	LSAck	Acknowledges the other packet types.

The acronyms LSA and LSU are often used interchangeably.

An LSU contains one or more LSAs.

LSAs contain route information for destination networks.

LSA specifics are discussed in CCNP.

LSA Type	Description
1	Router LSAs
2	Network LSAs
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Protocol (BGP)
9, 10, 11	Opaque LSAs

OSPF Types and Key Behaviors

Key Topic

Table 21-2 Two OSPF Network Types and Key Behaviors

Network Type Keyword	Dynamically Discovers Neighbors	Uses a DR/BDR
broadcast	Yes	Yes
point-to-point	Yes	No

OSPF Equal Cost

Table 20-3 Faster Interfaces with Equal OSPF Costs

Interface	Interface Default Bandwidth (Kbps)	Formula (Kbps)	OSPF Cost
Serial	1544 Kbps	100,000 / 1544	64
Ethernet	10,000 Kbps	100,000 / 10,000	10
Fast Ethernet	100,000 Kbps	100,000/100,000	1
Gigabit Ethernet	1,000,000 Kbps	100,000/1,000,000	1
10 Gigabit Ethernet	10,000,000 Kbps	100,000/10,000,000	1
100 Gigabit Ethernet	100,000,000 Kbps	100,000/100,000,000	1

OSPF Design Terminology

Key Topic

Table 19-7 OSPF Design Terminology

Term	Description
Area Border Router (ABR)	An OSPF router with interfaces connected to the backbone area and to at least one other area
Backbone router	A router connected to the backbone area (includes ABRs)
Internal router	A router in one area (not the backbone area)
Area	A set of routers and links that shares the same detailed LSDB information, but not with routers in other areas, for better efficiency
Backbone area	A special OSPF area to which all other areas must connect—area 0
Intra-area route	A route to a subnet inside the same area as the router
Interarea route	A route to a subnet in an area of which the router is not a part

OSPF Network States and their Meanings

Table 19-5 Stable OSPF Neighbor States and Their Meanings

Neighbor State	Term for Neighbor	Term for Relationship
2-way	Neighbor	Neighbor Relationship
Full	Adjacent Neighbor Fully Adjacent Neighbor	Adjacency

OSPF Similarities

Similarities Between OSPFv2 and OSPFv3

OSPFv3 operates much like OSPFv2. Table 14-2 summarizes the operational features that OSPFv2 and OSPFv3 share.

Table 14-2 OSPFv2 and OSPFv3 Similarities

Feature	OSPFv2 and OSPFv3
Link state	Yes
Routing algorithm	SPF
Metric	Cost
Areas	Support the same two-level hierarchy
Packet types	Use the same hello, DBD, LSR, LSU, and LSAck packets
Neighbor discovery	Transition through the same states using hello packets
LSDB synchronization	Exchange contents of their LSDB between two neighbors
DR and BDR	Use the same function and election process
Router ID	Use a 32-bit router ID and the same process in determining the 32-bit router ID

OSPF Differences

Differences Between OSPFv2 and OSPFv3

Table 14-3 lists the major differences between OSPFv2 and OSPFv3.

Table 14-3 OSPFv2 and OSPFv3 Differences

Feature	OSPFv2	OSPFv3
Advertising	IPv4 networks	IPv6 prefixes
Source address	IPv4 source address	IPv6 link-local address
Destination address	Choice of Neighbor IPv4 unicast address 224.0.0.5, all-OSPF-routers multicast address 224.0.0.6, DR/BDR multicast address	Choice of Neighbor IPv6 link-local address FF02::5, all-OSPFv3-routers multicast address FF02::6, DR/BDR multicast address
Advertising networks	Configured using the **network** router configuration command	Configured using the **ipv6 ospf area** interface configuration command
IP unicast routing	IPv4 unicast routing enabled by default	Requires configuration of the **ipv6 unicast-routing** global configuration command
Authentication	Plain text and MD5	IPsec

Multiarea OSPF Design Terminology

Table 14-4 Multiarea OSPF Design Terminology

Term	Description
Area border router (ABR)	An OSPF router with interfaces connected to the backbone area and to at least one other area.
Backbone router	A router connected to the backbone area (includes ABRs).
Internal router	A router in one area (not the backbone area).
Autonomous system boundary router (ASBR)	A router that has at least one interface connected to an external network. An external network is a network that is not part of the routing domain, such as EIGRP, BGP, or one with static routing to the Internet, as Figure 14-5 shows.

Term	Description
Area	A set of routers and links that shares the same detailed LSDB information—but not with routers in other areas—for better efficiency
Backbone area	A special OSPF area to which all other areas must connect, such as Area 0
Intra-area route	A route to a subnet inside the same area as the router
Interarea route	A route to a subnet in an area the router is not a part of

OSPF Link Types

Link Type	Link ID (This applies to individual Links)
Point-to-Point	Neighbor Router ID
Link to transit network	Interface address of DR
Link to stub network (In case of loopback mask is 255.255.255.255)	Network/subnet number
Virtual Link	Neighbor Router ID

The **Link Data** is the IP address of the link, except for stub network where the link data is the network mask.

Link Type	Link Data
Stub network	Network Mask
Other networks (applies to router links only)	Router - associated IP interface address

OSPF Link Cost value

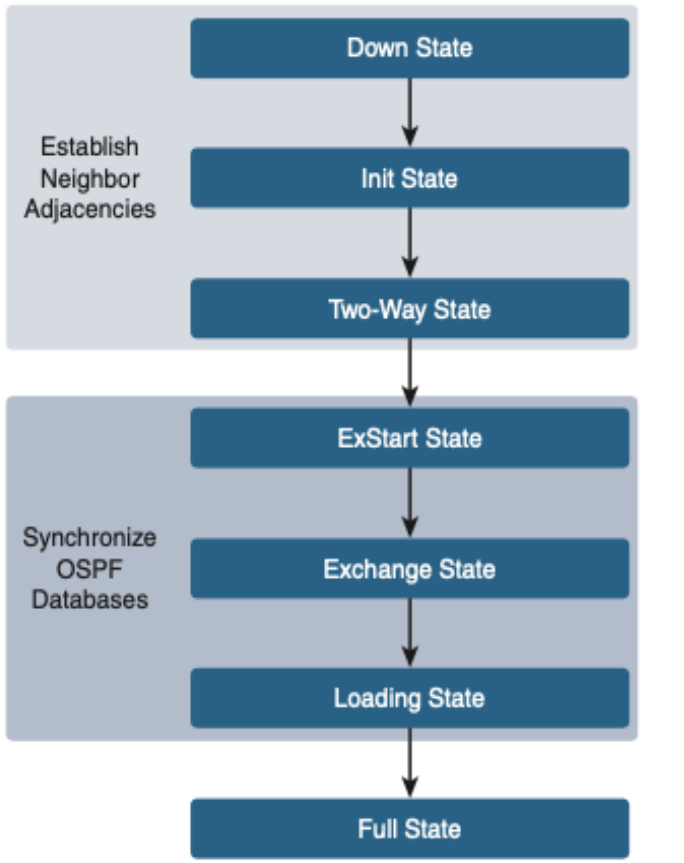
Table 13-2 Cisco Default OSPF Cost Values

Interface Type	10^8/bps = Cost	Cost
10 Gigabit Ethernet (10 Gbps)	10^8/10,000,000,000 bps = 1	1
Gigabit Ethernet (1 Gbps)	10^8/1,000,000,000 bps = 1	1
Fast Ethernet (100 Mbps)	10^8/100,000,000 bps = 1	1
Ethernet (10 Mbps)	10^8/10,000,000 bps = 10	10

Interface Type	10^8/bps = Cost	Cost
T1 (1.544 Mbps)	10^8/1,544,000 bps = 64	64
128 kbps	10^8/128,000 bps = 781	781
64 kbps	10^8/64,000 bps = 1562	1562

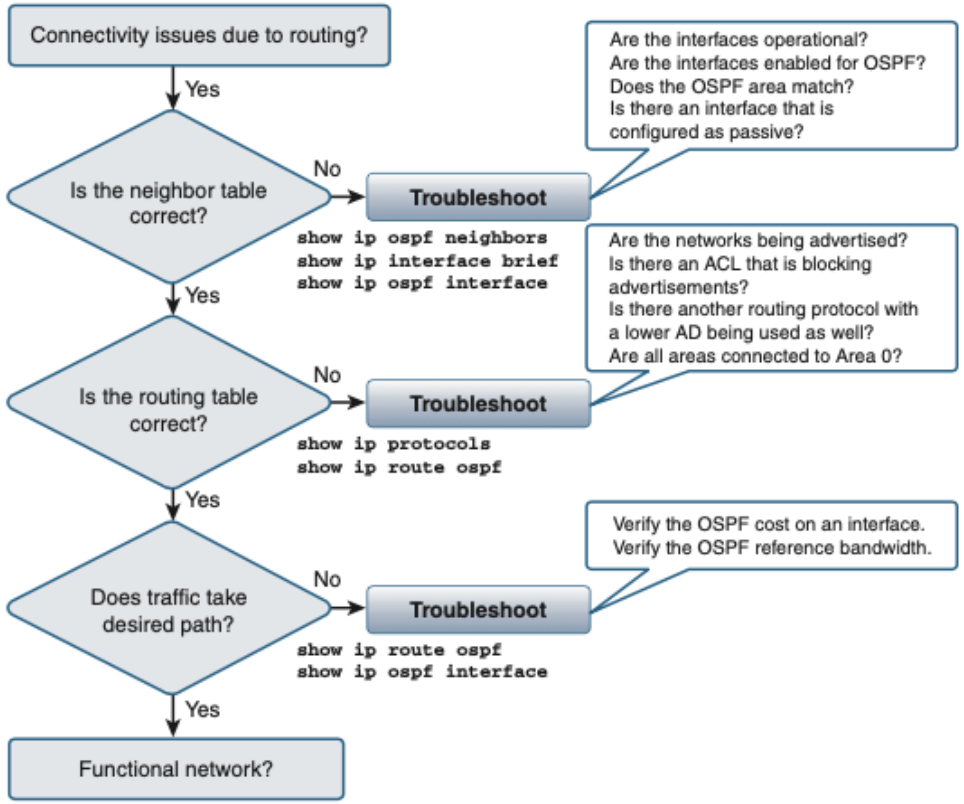
OSPF STATES

Figure 12-3 Transitioning Through the OSPF States



Systematic Resource For TSHOOT OSPF V2

Figure 12-4 Systematic Method for Troubleshooting OSPFv2



Default Administrative Distance

Table 19-4 Default Administrative Distances

Route Type	Administrative Distance
Connected	0
Static	1
BGP (external routes [eBGP])	20
EIGRP (internal routes)	90
IGRP	100
OSPF	110

Administrative Distances

Route Type	Administrative Distance
IS-IS	115
RIP	120
EIGRP (external routes)	170
BGP (internal routes [iBGP])	200
DHCP default route	254
Unusable	255

Routing Protocol Comparison

Table 19-3 Interior IP Routing Protocols Compared

Feature	RIPv2	EIGRP	OSPF
Classless/sends mask in updates/supports VLSM	Yes	Yes	Yes
Algorithm (DV, advanced DV, LS)	DV	Advanced DV	LS
Supports manual summarization	Yes	Yes	Yes
Cisco-proprietary	No	Yes[1]	No
Routing updates are sent to a multicast IP address	Yes	Yes	Yes
Convergence	Slow	Fast	Fast

IP IGP Metrics

Key Topic

Table 19-2 IP IGP Metrics

IGP	Metric	Description
RIPv2	Hop count	The number of routers (hops) between a router and the destination subnet
OSPF	Cost	The sum of all interface cost settings for all links in a route, with the cost defaulting to be based on interface bandwidth
EIGRP	Calculation based on bandwidth and delay	Calculated based on the route's slowest link and the cumulative delay associated with each interface in the route

HSRP

Key Topic

Table 12-2 Three FHRP Options

Acronym	Full Name	Origin	Redundancy Approach	Load Balancing Per...
HSRP	Hot Standby Router Protocol	Cisco	active/standby	subnet
VRRP	Virtual Router Redundancy Protocol	RFC 5798	active/standby	subnet
GLBP	Gateway Load Balancing Protocol	Cisco	active/active	host

HSRP Features

Table 24-3 HSRP Version 1 and Version 2 Features

HSRP Feature	Version 1	Version 2
Group numbers supported	0–255	0–4095
Authentication	None	MD5
Multicast addresses	IPv4: 224.0.0.2	IPv4: 224.0.0.102 IPv6: FF02::66
Virtual MAC ranges	0000.0C07.AC00 to 0000.0C07.ACFF	IPv4: 0000.0C9F.F000 to 0000.0C9F.FFFF IPv6: 0005.73A0.0000 to 0005.73A0.0FFF

NOTE: The last three hexadecimal digits of the virtual MAC address indicate the configured group number. Group numbers are important for more advanced HSRP configurations, which are beyond the scope of the CCNA exam.

ACL Types

- Standard numbered ACLs (1–99)
- Extended numbered ACLs (100–199)
- Additional ACL numbers (1300–1999 standard, 2000–2699 extended)
- Named ACLs
- Improved editing with sequence numbers

ACL Application Consideration

- Place extended ACLs as close as possible to the source of the packets that will be filtered. Filtering close to the source of the packets saves some bandwidth.
- Remember that all fields in one **access-list** command must match a packet for the packet to be considered to match that **access-list** statement.
- Use numbers of 100–199 and 2000–2699 on the **access-list** commands; no one number is inherently better than another.

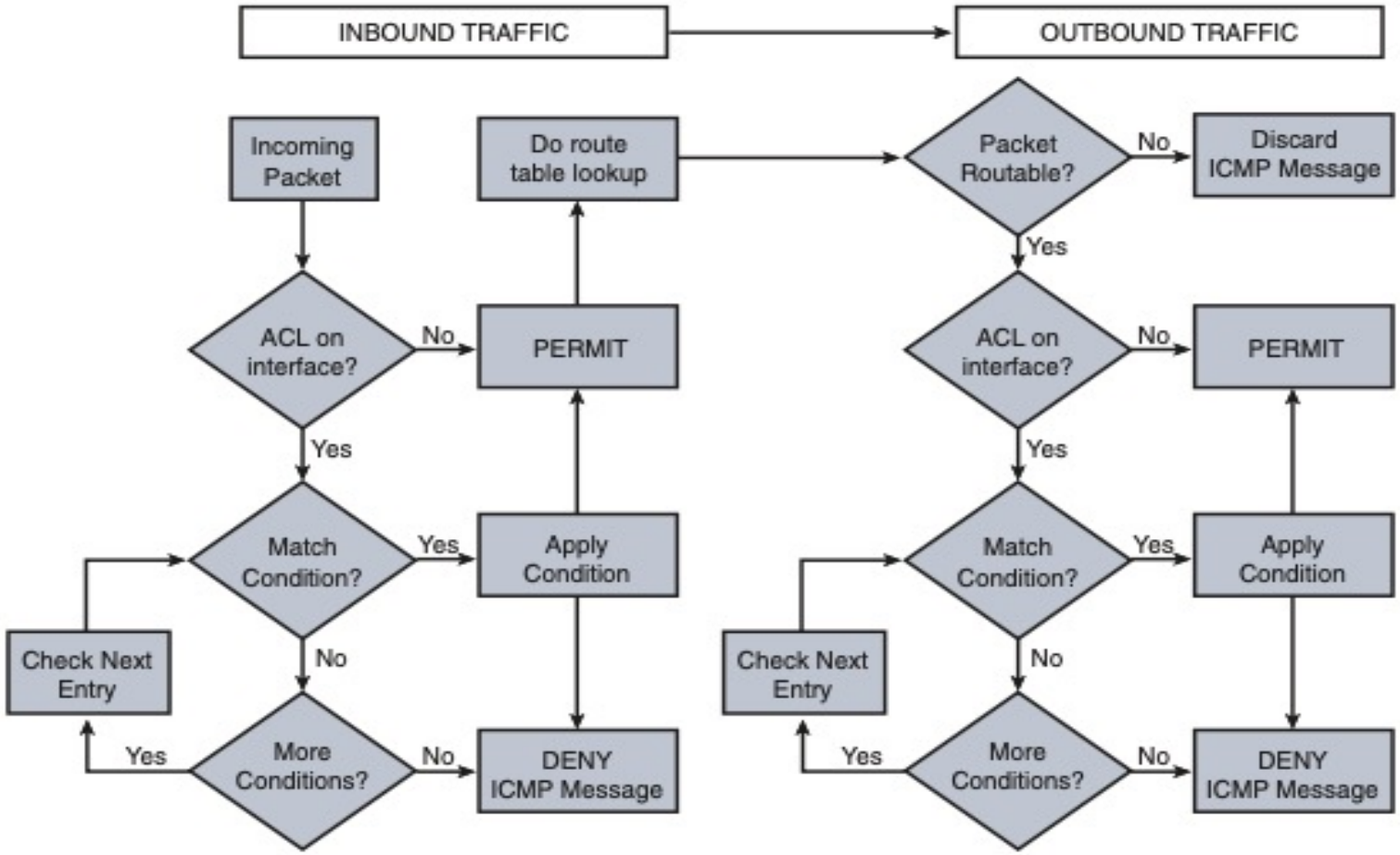
- Using names instead of numbers to identify the ACL, making it easier to remember the reason for the ACL
- Using ACL subcommands, not global commands, to define the action and matching parameters
- Using ACL editing features that allow the CLI user to delete individual lines from the ACL and insert new lines

Topic

- Place extended ACLs as close as possible to the source of the packet. This strategy allows ACLs to discard the packets early.
- Place standard ACLs as close as possible to the destination of the packet. This strategy avoids the mistake with standard ACLs (which match the source IPv4 address only) of unintentionally discarding packets that did not need to be discarded.
- Place more specific statements early in the ACL.
- Disable an ACL from its interface (using the **no ip access-group** interface subcommand) before making changes to the ACL.

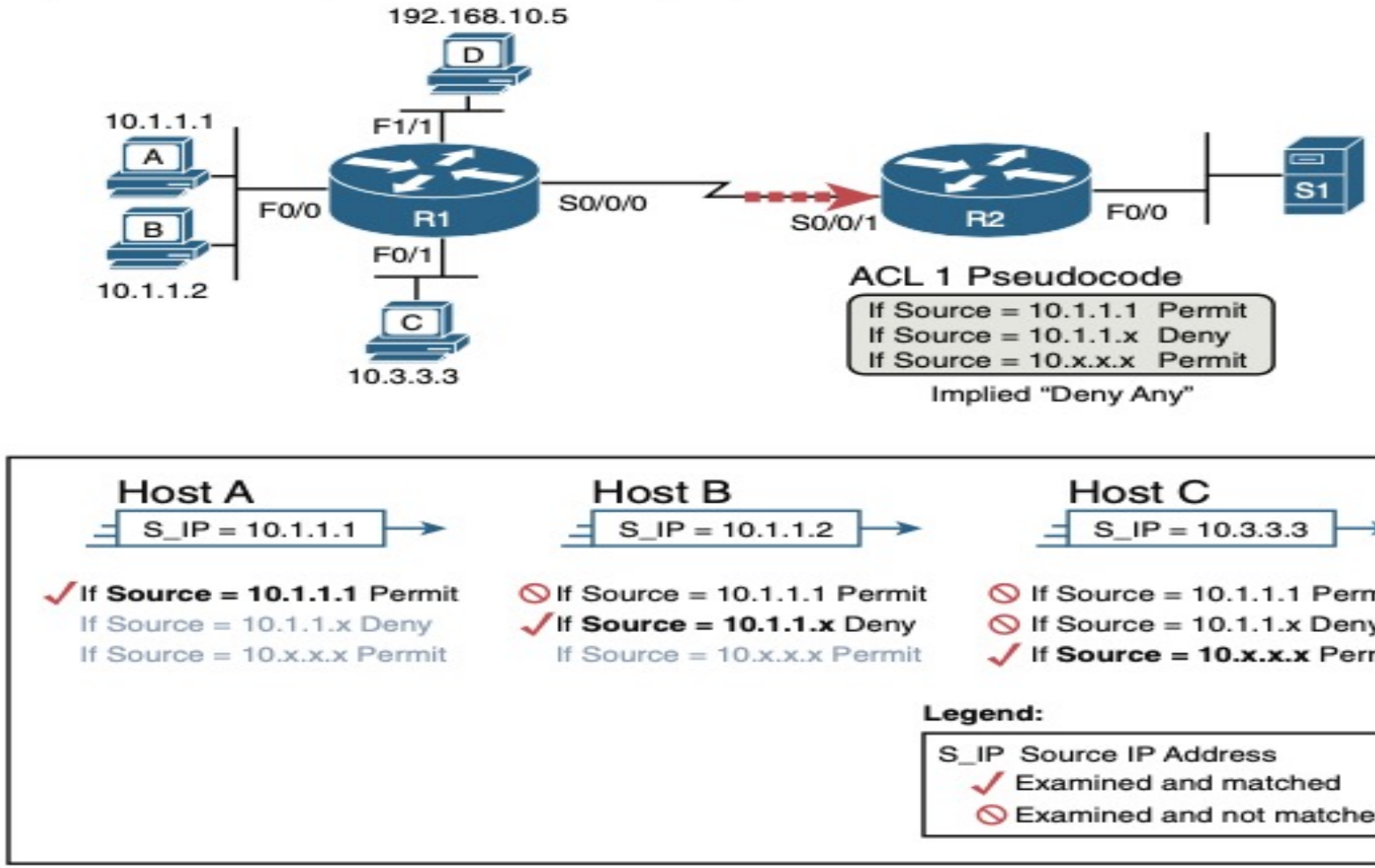
ACL interface Processing for Inbound outbound Traffic

Figure 10-1 ACL Interface Processing for Inbound and Outbound Traffic



ACL Matching logic example

Figure 10-2 Example of ACL Matching Logic



Compared iPV4 and IPV6 ACL

Table 9-2 IPv4 and IPv6 ACLs

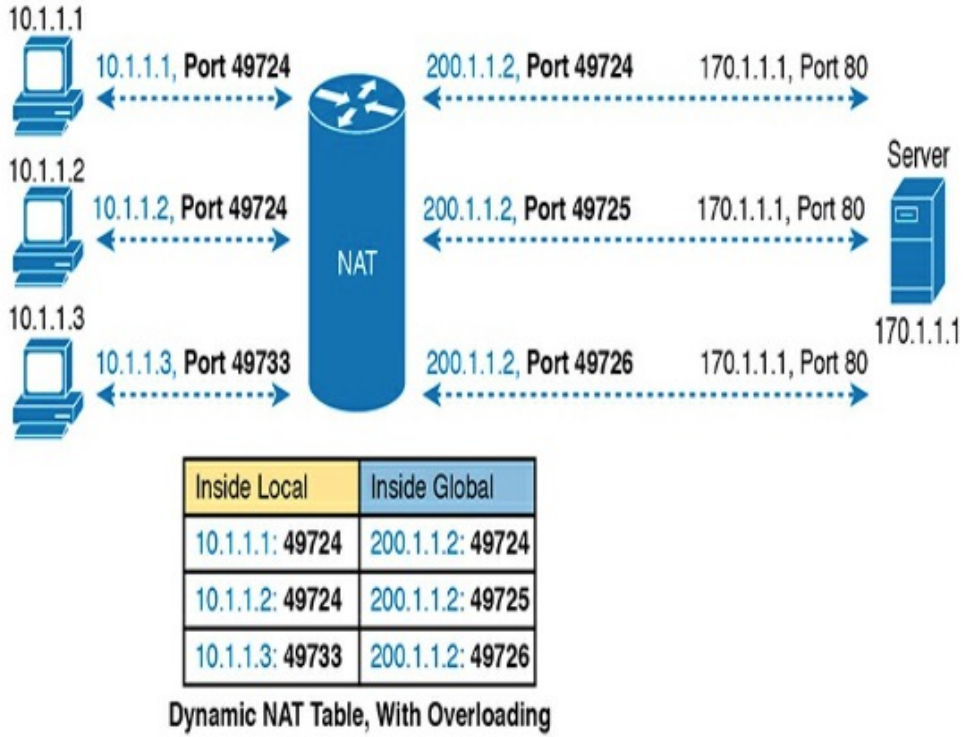
Feature	IPv4 Only	IPv6 Only	Both
Match source and/or destination address			X
Match host addresses or subnets/prefixes			X
Applied directionally on an interface			X
Match TCP or UDP source and/or destination ports			X
Match ICMP codes			X

Feature	IPv4 Only	IPv6 Only	Both
Include implicit deny at end of ACL			X
Match IPv4 packets only	X		
Match IPv6 packets only		X	
Use numbers to identify the ACL	X		
Use names to identify the ACL			X
Include some implicit **permit** statements at end of ACL		X	

NAT

Term	Values in Figures	Meaning
Inside local	10.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective: it is inside the enterprise. **Local:** Means not global; that is, local. It is the address used for that host while the packet flows in the local enterprise rather than the global Internet. **Alternative:** Think of it as inside private, because this address is typically a private address.
Inside global	200.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective. **Global:** Means global as in the global Internet. It is the address used for that host while the packet flows in the Internet. **Alternative:** Think of it as inside public, because the address is typically a public IPv4 address.
Outside global	170.1.1.1	With source NAT, the one address used by the host that resides outside the enterprise, which NAT does not change, so there is no need for a contrasting term. **Alternative:** Think of it as outside public, because the address is typically a public IPv4 address.
Outside local	—	This term is not used with source NAT. With destination NAT, the address would represent a host that resides outside the enterprise, but the address used to represent that host as packets pass through the local enterprise.

NAT OVERLOAD



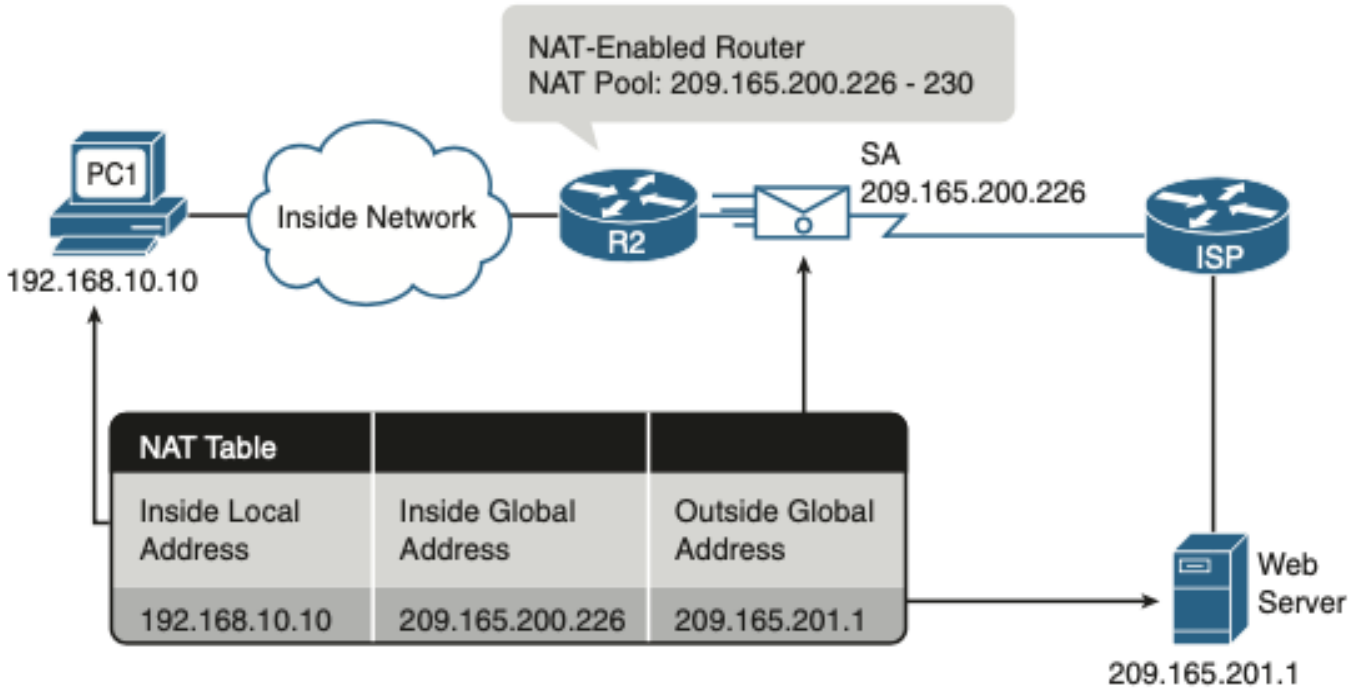
Inside Local	Inside Global
10.1.1.1: **49724**	200.1.1.2: **49724**
10.1.1.2: **49724**	200.1.1.2: **49725**
10.1.1.3: **49733**	200.1.1.2: **49726**

Dynamic NAT Table, With Overloading

Figure 10-8 *NAT Overload (PAT)*

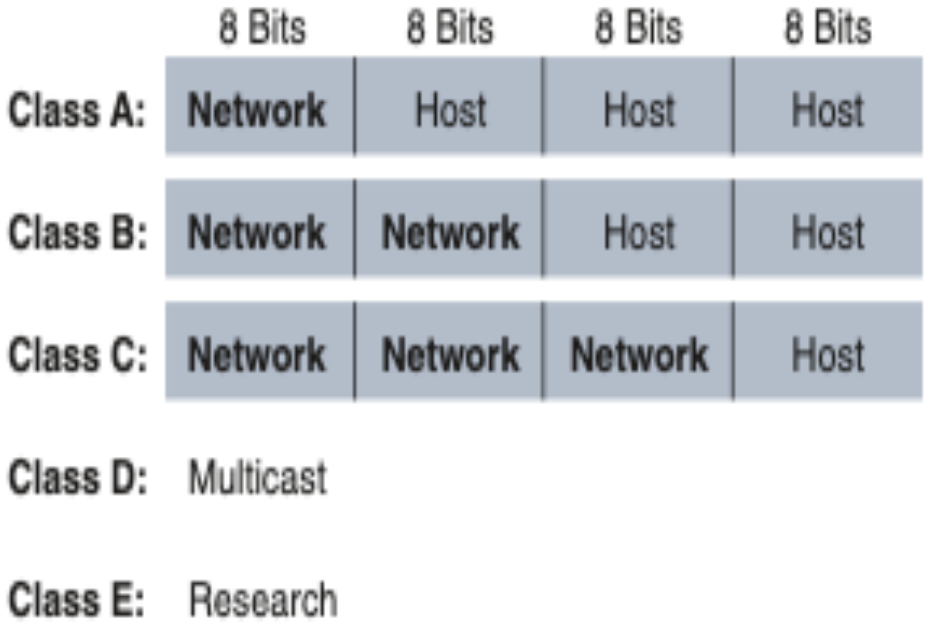
NAT Inside Local and global

Figure 8-2 NAT Terminology



Network Host Boundary for Each class

Figure 28-2 Network/Host Boundary for Each Class of IPv4 Address



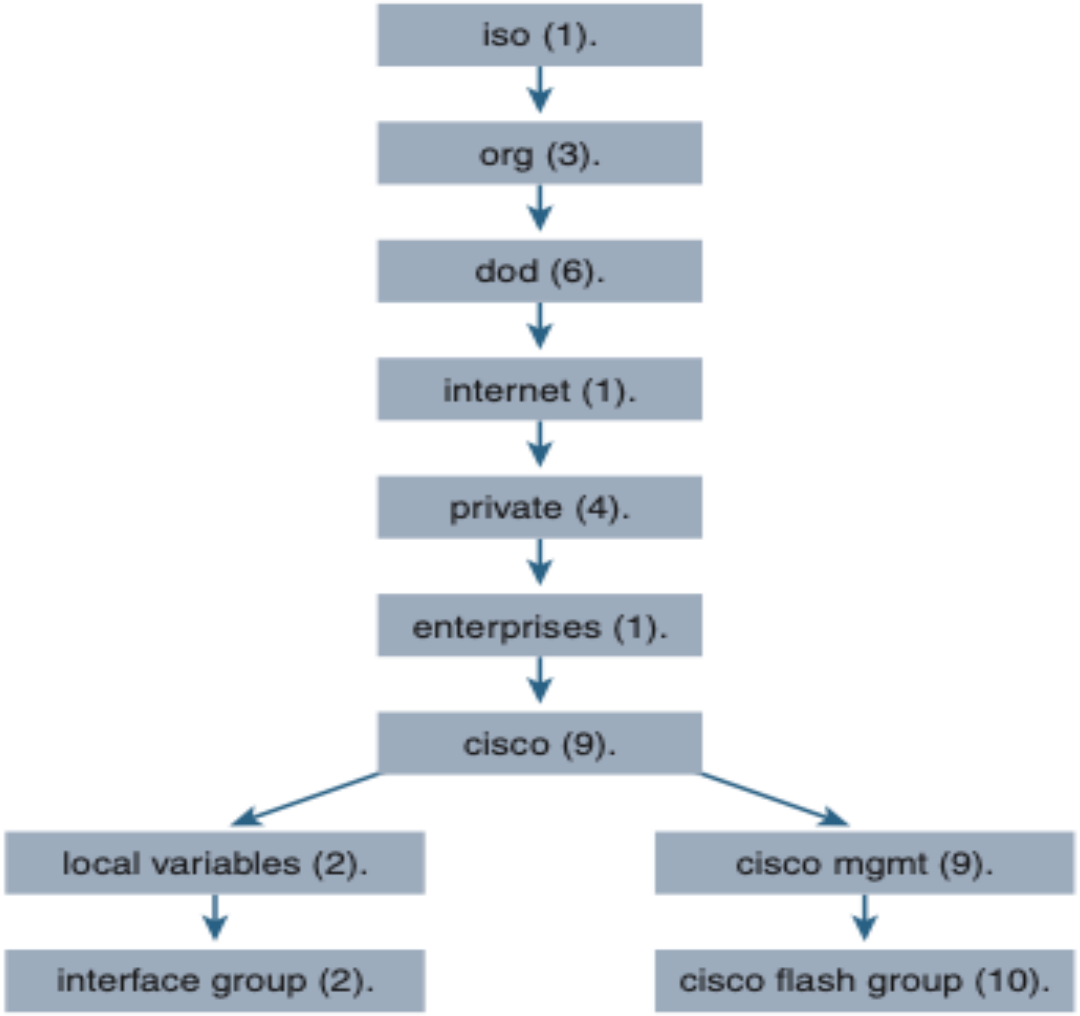
SNPM Operation

Table 4-1 get and set SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table. The SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
get-bulk-request	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (This works only with SNMPv2 or later.)
get-response	Replies to a **get-request**, **get-next-request**, or **set-request** sent by an NMS.
set-request	Stores a value in a specific variable.

MIB Object ID

Figure 4-1 Management Information Base Object IDs



Syslog Message Format

Table 4-3 describes the fields in a syslog message.

Table 4-3 Syslog Message Format

Field	Explanation
`seq no`	Sequence number stamped on the log message. Appears only if the **service sequence-numbers** global configuration command is configured.
`timestamp`	Date and time of the message or event. Appears only if the **service timestamps** global configuration command is configured.
`facility`	The facility to which the message refers.
`severity`	Single-digit code from 0 to 7 indicating the severity of the message.
`MNEMONIC`	Text string that uniquely describes the message.
`description`	Text string containing detailed information about the event being reported.

Syslog Severity Level

Table 4-2 Syslog Severity Level

Severity Name	Severity Level	Explanation
Emergency	Level 0	System unusable
Alert	Level 1	Immediate action needed
Critical	Level 2	Critical condition
Error	Level 3	Error condition
Warning	Level 4	Warning condition
Notification	Level 5	Normal but significant condition
Informational	Level 6	Informational message
Debugging	Level 7	Debugging message

Switch

- Layer 2 Switch

Forward Packets Based on Destination MAC Address

switches receive broadcast frame flooded to all of the ports except the one that received the broadcast frame

VLANS from 1 to 1005 exist in switches by default can not be deleted

Traffic from multiple VLANs can be allowed over a trunk link

Traffic Types

Table 26-1 Traffic Types

Traffic Type	Description
Network management	Many types of network management traffic can be present on the network. To make network troubleshooting easier, some designers assign a separate VLAN to carry certain types of network management traffic.
IP telephony	Two types of IP telephony traffic exist: signaling information between end devices and the data packets of the voice conversation. Designers often configure the data to and from the IP phones on a separate VLAN designated for voice traffic so that they can apply quality-of-service measures to give high priority to voice traffic.
IP multicast	Multicast traffic can produce a large amount of data streaming across the network. Switches must be configured to keep this traffic from flooding to devices that have not requested it, and routers must be configured to ensure that multicast traffic is forwarded to the network areas where it is requested.
Normal data	Normal data traffic is typical application traffic that is related to file and print services, email, Internet browsing, database access, and other shared network applications.
Scavenger class	Scavenger class includes all traffic with protocols or patterns that exceed their normal data flows. Applications assigned to this class have little or no contribution to the organizational objectives of the enterprise and are typically entertainment oriented.

Lan Switch Interface Status Code

Table 29-6 LAN Switch Interface Status Codes

Line Status	Protocol Status	Interface Status	Typical Root Cause
Administratively down	Down	disabled	The interface is configured with the **shutdown** command.
Down	Down	notconnect	No cable exists, the cable is bad, incorrect cable pinouts are used, the two connected devices have mismatched speeds, or the device on the other end of the cable is powered off or the other interface is shut down.
Up	Down	notconnect	An interface up/down state is not expected on LAN switch interfaces. This indicates a Layer 2 problem on Layer 3 devices.
Down	Down (err-disabled)	err-disabled	Port security has disabled the interface. The network administrator must manually reenable the interface.
Up	Up	connect	The interface is working.

Common Lan Problem Indicator

Table 29-7 Common LAN Layer 1 Problem Indicators

Type of Problem	Counter Values Indicating This Problem	Common Root Causes
Excessive noise	Many input errors, few collisions	Wrong cable category (Cat5, Cat5E, Cat6), damaged cables, EMI
Collisions	More than roughly 0.1% of all frames are collisions	Duplex mismatch (seen on the half-duplex side), jabber, DoS attack
Late collisions	Increasing late collisions	Collision domain or single cable too long, duplex mismatch

TCP VS UDP

TCP	UDP
Secure	Unsecure
Connection-Oriented	Connectionless
Slow	Fast
Guaranteed Transmission	No Guarantee
Used by Critical Applications	Used by Real-Time Applications
Packet Reorder Mechanism	No Reorder Mechanism
Flow Control	No Flow Control
Advanced Error Checking	Basic Error Checking (Checksum)
20 Bytes Header	8 Bytes Header
Acknowledgement Mechanism	No Acknowledgement
Three-Way Handshake	No Handshake Mechanism
DNS, HTTPS, FTP, SMTP etc.	DNS, DHCP, TFTP, SNMP etc.

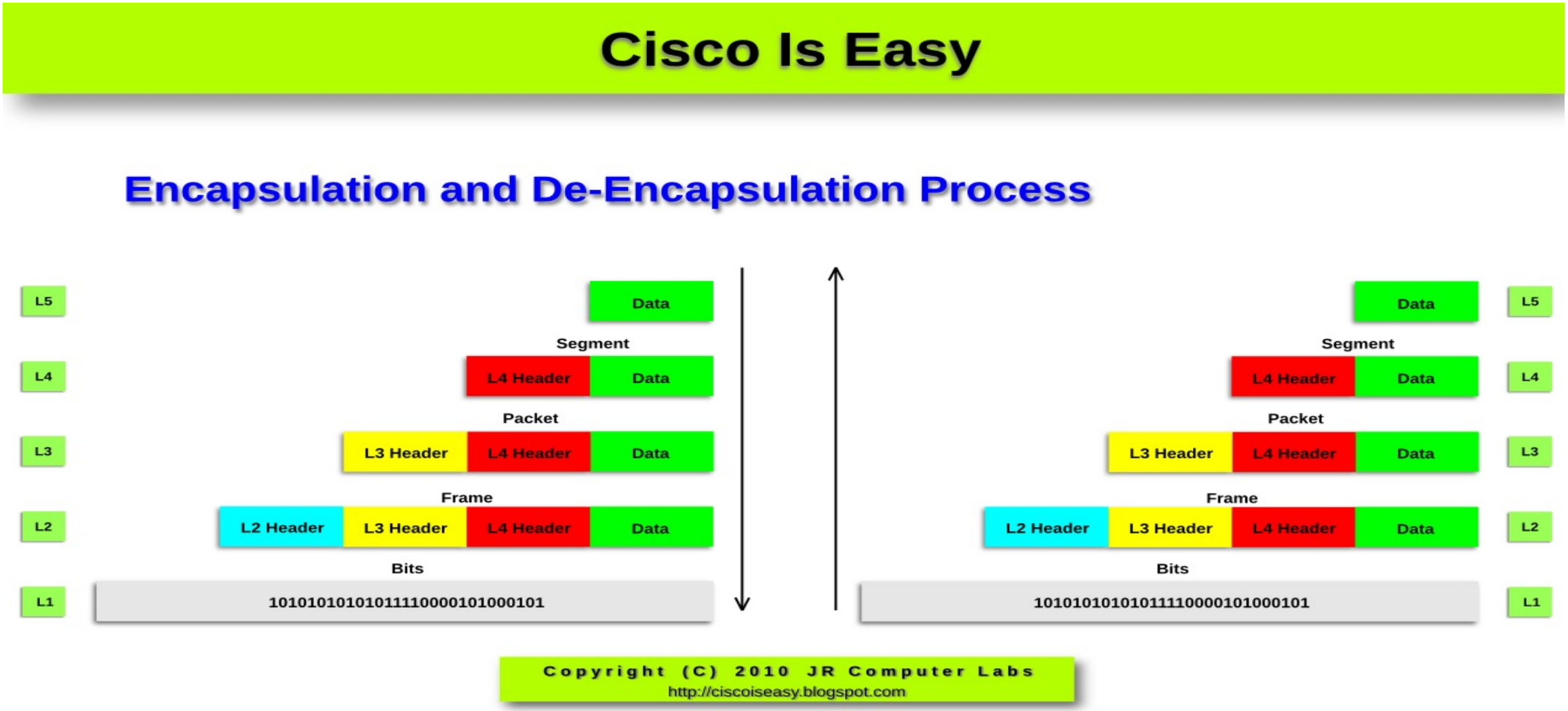
TCP UDP Protocols

Application	Protocol	Port Number
File Transfer Protocol FTP Client	TCP	20
File Transfer Protocol FTP Server	TCP	21
Secure Shell SSH	TCP	22
Telnet	TCP	23
Simple Mail Transport Protocol SMTP	TCP	25
Domain Name System DNS	UDP / TCP	53
Dynamic Host Configuration Protocol DHCP	UDP	67,68
Trivial File Transfer Protocol TFTP	UDP	69
Hypertext Transfer Protocol HTTP	TCP	80
Post Office Protocol 3 POP3	TCP	110
Simple Network Management Protocol SNMP	UDP	161
Hypertext Tranfer Protocol Secure HTTPS	TCP	443

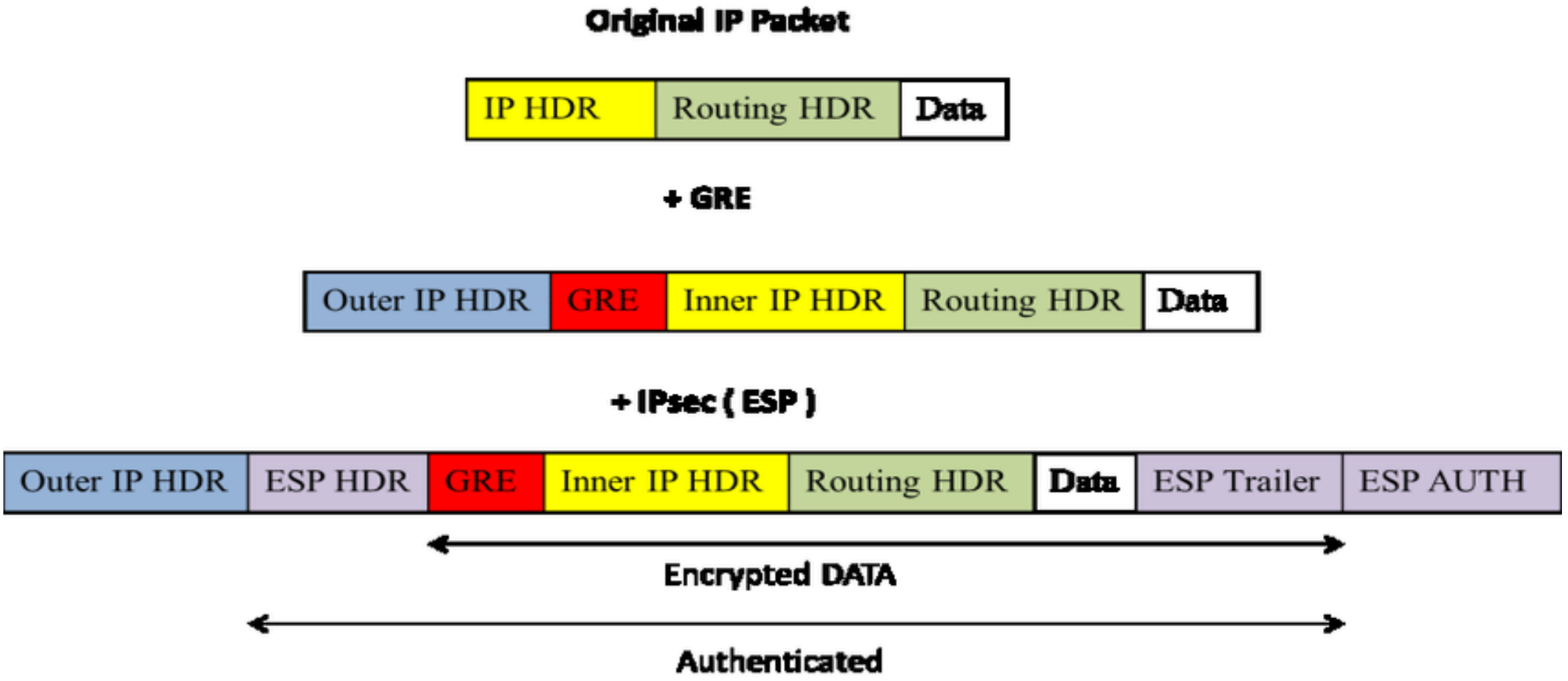
BPDU Structure

- Ipv4 packet structure the fields of the ipv4 header
- combination of data and layer 4 header is called a segment
- combination of data layer 4 header layer 3 header is called Packet

Encapsulation Decapsulation Process



GRE IPSEC Encapsulation of a Packet



- AutoMDIX allows devices to detect which pin their neighbors are on and adjust the pins
- vlan tagging switches will tag all vlan over the trunk port
- ISL and 802.1q are the 2 protocol for trunking ISL is cisco propietary 802.1q is industry standard ISL is no longer used
- 802.1q tag is inserted in a field between the ethernet header the tag is 4 bytes or 32 bit
- 802.1q has a featured called the native vlan wich is vlan 1 by default
- when a switch received a untagged frame it will asume it belongs to the native vlans

Switch Operation

- DTP is a Cisco proprietary protocol that allows interfaces to negotiate trunks
- For security considerations dtp should be disabled in all interfaces
- Switch port in dynamic desirable will activate negotiate to form a trunk with other switches
- a switch in dynamic auto will not actively try to form a trunk but just passible
- static access means a static port that belongs to a vlan wich doesnt change
- a switch in dynamic auto will form a trunk with the other switches if the other switch is in dynamic desirable
- a switch port in access mode will stop dtp from sending dtp frames

- VTP allows to configure vlans on a central server switch
- 3 vtp mode that switches operates server client and transparent
- server mode switches can add modified or delete vlans
- vtp advertisement are sent only on trunk ports
- vtp client cannot add modified or delete vlans they just syncronized with the highest revision
- for switches to syncronize among devices they need to have the same domain name
- switches in transparent mode doesn not participate in the vtp domain it have its own database it just forward vtp information if they are in the same domain

VTP

Key Topic

Table 8-3 Expected Trunking Operational Mode Based on the Configured Administrative Modes

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

Administrative Mode with Switch port Mode Command

Key Topic

Table 8-2 Trunking Administrative Mode Options with the **switchport mode** Command

Command Option	Description
access	Always act as an access (nontrunk) port
trunk	Always act as a trunk port
dynamic desirable	Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking
dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking

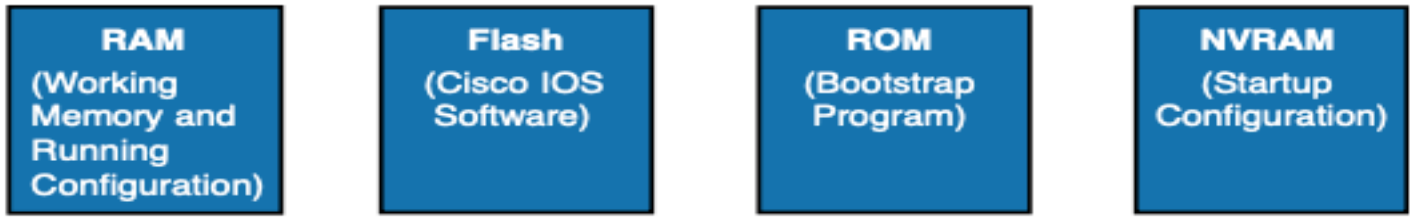
Lan Switches Interfaces Code

Key Topic

Table 7-2 LAN Switch Interface Status Codes

Line Status	Protocol Status	Interface Status	Typical Root Cause
administratively down	down	disabled	The **shutdown** command is configured on the interface.
down	down	notconnect	No cable; bad cable; wrong cable pinouts; speed mismatch; neighboring device is (a) powered off, (b) **shutdown**, or (c) error disabled.
up	down	notconnect	Not expected on LAN switch physical interfaces.
down	down (err-disabled)	err-disabled	Port security has disabled the interface.
up	up	connected	The interface is working.

Switches Memory Types and IOS



Key Topic

Table 4-5 Names and Purposes of the Two Main Cisco IOS Configuration Files

Configuration Filename	Purpose	Where It Is Stored
startup-config	Stores the initial configuration used anytime the switch reloads Cisco IOS.	NVRAM
running-config	Stores the currently used configuration commands. This file changes dynamically when someone enters commands in configuration mode.	RAM

EtherChannel Formation

Will an EtherChannel Form?

LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

PAGP Mode

Table 24-1 PAgP Mode Settings

Sw1	Sw2	Channel Established?
On	On	Yes
Auto/Desirable	Desirable	Yes
On/Auto/Desirable	Not configured	No
On	Desirable	No
Auto/On	Auto	No

LACP Mode

Table 24-2 LACP Mode Settings

Sw1	Sw2	Channel Established?
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not configured	No
On	Active	No
Passive/On	Passive	No

NOTE: For both the PAgP and LACP protocols, the on mode creates the EtherChannel configuration unconditionally, without PAgP or LACP dynamic negotiation. You should probably memorize the mode settings for both PAgP and LACP in preparation for the CCNA exam.

EtherChannel Load Distribution

Table 10-4 EtherChannel Load Distribution Methods

Configuration Keyword	Math Uses...	Layer
src-mac	Source MAC address	2
dst-mac	Destination MAC address	2
src-dst-mac	Both source and destination MAC	2
src-ip	Source IP address	3
dst-ip	Destination IP address	3
src-dst-ip	Both source and destination IP	3
src-port	Source TCP or UDP port	4
dst-port	Destination TCP or UDP port	4
src-dst-port	Both source and destination TCP or UDP port	4

STP

- STP is a layer 2 protocol
- Classic STP is an industry-standard protocol STP prevents layer 2 loops by placing the ports in a blocking state
- VTP enable hello BPDU out of every interface every 2 seconds
- The switch with the lowest bridge ID is elected the root bridge
- in the root bridge, all ports are forwarding
- For a tight breaker the MAC address is used the lowest MAC address will break the thigh
- All switches have 3267 as the default ID

- PVST run a different stp instance per vlan one interface could be forwarding in one vlan and blocking in the other
- all interfaces in the root bridge are designated ports
- when switch boots its a root bridge it will give its position up if it receives a higher BPDU wich mean the lowest ID
- there is one root port on each switch except for the root bridge
- the lowest port ID is the root Port
- each port has a default number of 128
- Blocking and forwarding are stable states
- Listening and learning are transitioning state
- none designated ports are in blocking states
- interfaces in the blocking states does not send traffic but they do receive BPDU
- only designated and root port enter in a forwarding state

The most common spanning tree protocols

PROTOCOL	IEEE STANDARD	SWITCH	DESCRIPTION
Spanning Tree Protocol (STP)	IEEE 802.1D	stp	The original STP version
Rapid STP (RSTP)	IEEE 802.1w	rstp	An evolution of STP 802.1D that addresses the STP convergence time gap issue with enhanced BPDU exchange
Multiple STP (MSTP)	IEEE 802.1s	mstp	A format for mapping multiple VLANs into the same spanning tree to reduce processing on the switch
Per-VLAN Spanning Tree (PVST+)	Cisco protocol based on 802.1D	pvst	An 802.1D enhancement that provides a separate STP instance for each VLAN configured in the network
Rapid PVST+	Cisco protocol based on 802.1w	rapid-pvst	An 802.1w enhancement that provides a separate STP instance for each VLAN, enabling faster convergence times

STP Standard

Key Topic

Table 10-2 STP Standards and Configuration Options

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

STP Port States

Key Topic

Table 9-10 Port States Compared: STP and RSTP

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

STP Port Roles

are instructive about how RSTP works. Table 9-9 lists these RSTP port roles.

Key Topic

Table 9-9 Port Roles in RSTP

Function	Port Role
Port that begins a nonroot switch's best path to the root	Root port
Port that replaces the root port when the root port fails	Alternate port
Switch port designated to forward onto a collision domain	Designated port
Port that replaces a designated port when a designated port fails	Backup port
Port that is administratively disabled	Disabled port

STP Timers

Key Topic

Table 9-7 STP Timers

Timer	Default Value	Description
Hello	2 seconds	The time period between Hellos created by the root.
MaxAge	10 times Hello	How long any switch should wait, after ceasing to hear Hellos, before trying to change the STP topology.
Forward delay	15 seconds	Delay that affects the process that occurs when an interface changes from blocking state to forwarding state. A port stays in an interim listening state, and then an interim learning state, for the number of seconds defined by the forward delay timer.

STP Default Port Cost

Key Topic

Table 9-6 Default Port Costs According to IEEE

Ethernet Speed	IEEE Cost: 1998 (and Before)	IEEE Cost: 2004 (and After)
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	N/A	200
1 Tbps	N/A	20

STP/RSTP Reason for Forwarding or Blocking

Key Topic

Table 9-3 STP/RSTP: Reasons for Forwarding or Blocking

Characterization of Port	STP State	Description
All the root switch's ports	Forwarding	The root switch is always the designated switch on all connected segments.
Each nonroot switch's root port	Forwarding	The port through which the switch has the least cost to reach the root switch (lowest root cost).
Each LAN's designated port	Forwarding	The switch forwarding the Hello on to the segment, with the lowest root cost, is the designated switch for that segment.
All other working ports	Blocking	The port is not used for forwarding user frames, nor are any frames received on these interfaces considered for forwarding.

STP variety

Table 25-3 Features of STP Varieties

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s, Cisco	Medium or high	Fast	Per instance

Port State

Table 25-4 PVST Port States

Operation Allowed	Blocking	Listening	Learning	Forwarding	Disabled
Can receive and process BPDUs	Yes	Yes	Yes	Yes	No
Can forward data frames received on the interface	No	No	No	Yes	No
Can forward data frames switched from another interface	No	No	No	Yes	No
Can learn MAC addresses	No	No	Yes	Yes	No

STP RSTP Port States

Table 25-5 RSTP and STP Port States

Operational State	STP State (802.1D)	RSTP State (802.1w)	Forwards Data Frames in This State?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	No
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

RSTP and STP Port Roles

Table 25-6 RSTP and STP Port Roles

RSTP Role	STP Role	Definition
Root port	Root port	A single port on each nonroot switch in which the switch hears the best BPDU out of all the received BPDUs
Designated port	Designated port	Of all switch ports on all switches attached to the same segment/collision domain, the port that advertises the "best" BPDU
Alternate port	—	A port on a switch that receives a suboptimal BPDU
Backup port	—	A nondesignated port on a switch that is attached to the same segment/collision domain as another port on the same switch
Disabled	—	A port that is administratively disabled or that is not capable of working for other reasons

Key Topic

Table 8-3 Expected Trunking Operational Mode Based on the Configured Administrative Modes

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use[1]	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use[1]	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

[1] When two switches configure a mode of "access" on one end and "trunk" on the other, problems occur. Avoid this combination.

Trunk Negotiation Results

Table 26-2 summarizes the results of DTP negotiations based on the different DTP configuration commands on local and remote ports.

Table 26-2 Trunk Negotiation Results Between a Local Port and a Remote Port

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

Forwarding and Blocking Ports

Table 25-1 STP: Reasons for Forwarding or Blocking

Characterization of Port	STP State	Description
All the root switch's ports	Forwarding	The root switch is always the designated switch on all connected segments.
Each nonroot switch's root port	Forwarding	This is the port through which the switch has the least cost to reach the root switch.
Each LAN's designated port	Forwarding	The switch forwarding the lowest-cost BPDU onto the segment is the designated switch for that segment.
All other working ports	Blocking	The port is not used for forwarding frames, nor are any frames received on these interfaces considered for forwarding. BPDUs are still received.

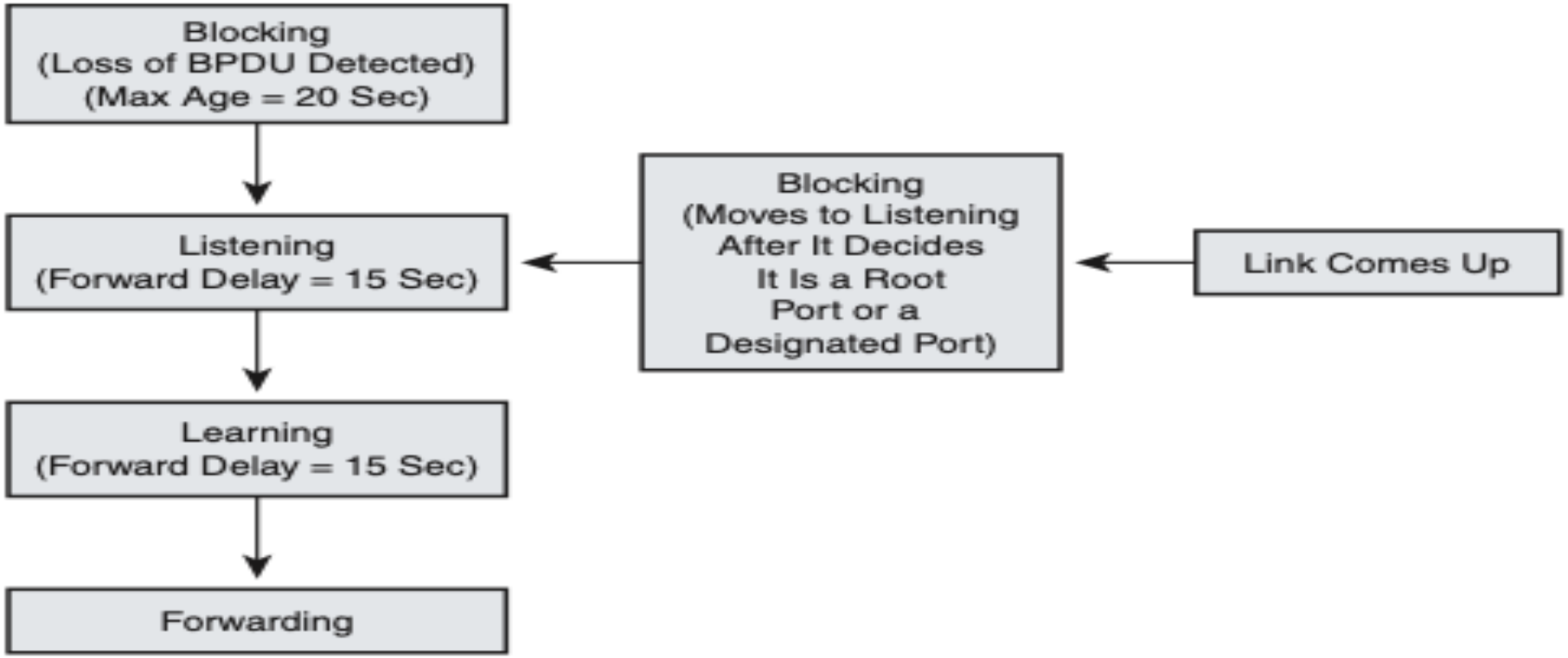
Port Cost

Table 25-2 Default IEEE Port Costs

Ethernet Speed	Original IEEE Cost	Revised IEEE Cost
10 Mbps	100	100
100 Mbps	10	19
1 Gbps	1	4
10 Gbps	1	2

Port States

Figure 25-3 Spanning Tree Port States



A fifth state, disabled, occurs either when a network administrator manually disables the port or when a security violation disables the port.

Layer 3 Switch

- Routes Traffics

Routes Traffic Similar to a router when enabling routing Mode

Port Security Violations

Table 6-2 Actions When Port Security Violation Occurs

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

CDP Commands

Table 9-3 show cdp Commands That List Information About Neighbors

Command	Description
show cdp neighbors [*type number*]	Lists one summary line of information about each neighbor or just the neighbor found on a specific interface if an interface was listed
show cdp neighbors detail	Lists one large set (approximately 15 lines) of information, one set for every neighbor
show cdp entry *name*	Lists the same information as the **show cdp neighbors detail** command, but only for the named neighbor (case sensitive)

CDP Defaults

Table 5-1 CDP Defaults

Parameter	Default
CDP	Enabled globally and on all interfaces
CDP version	Version 2
CDP timer	60 seconds
CDP holdtime	180 seconds

LLDP Commands

Topic

- **[no] lldp run:** A global configuration command that sets the default mode of LLDP operation for any interface that does not have more specific LLDP subcommands (**lldp transmit**, **lldp receive**). The **lldp run** global command enables LLDP in both directions on those interfaces, while **no lldp run** disables LLDP.
- **[no] lldp transmit:** An interface sub-command that defines the operation of LLDP on the interface regardless of the global [**no**] **lldp run** command. The **lldp transmit** interface subcommand causes the device to transmit LLDP messages, while **no lldp transmit** causes it to not transmit LLDP messages.
- **[no] lldp receive:** An interface subcommand that defines the operation of LLDP on the interface regardless of the global **[no] lldp run** command. The **lldp receive** interface subcommand causes the device to process received LLDP messages, while **no lldp receive** causes it to not process received LLDP messages.

LLDP Defaults

Table 5-2 LLDP Defaults

Parameter	Default
LLDP	Disabled globally and on all interfaces
LLDP timer	30 seconds
LLDP holdtime	120 seconds
LLDP reinitialization delay	2 seconds

NOTE: The reinitialization delay is the number of seconds the device waits after LLDP is disabled on a port before it accepts a configuration to reenable LLDP.

POE

- Power policing prevents a POE to take to much power
- solution to prevent tail drop is random early detection

QOS

- NBAR performs a deep packet inspection beyond TCP all the way up to layer 7
- Classification gives priority To traffic over others
- PCP field is in the trunk is referred to as COS
- in the ipv4 Header, there is a byte called TOS type of service
- standard IPP marking is Similar to PPC
- DF default forwarding is the marking for Best Effort
- EF expedited forwarding is for the required low-loss
- AF Assure Forwarding highest packets will be forwarded compared to low packets
- Low Latency Queuing creates a priority Que
- QOS Platinum should be used for voice silver is the best effort by default gold for video traffic bronze is the lowest option for Background traffic

QOS Clasifiers

Topic

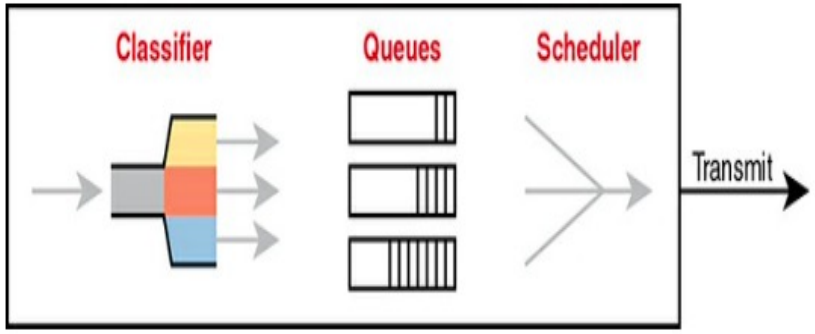


Figure 11-14 *Queuing Components*

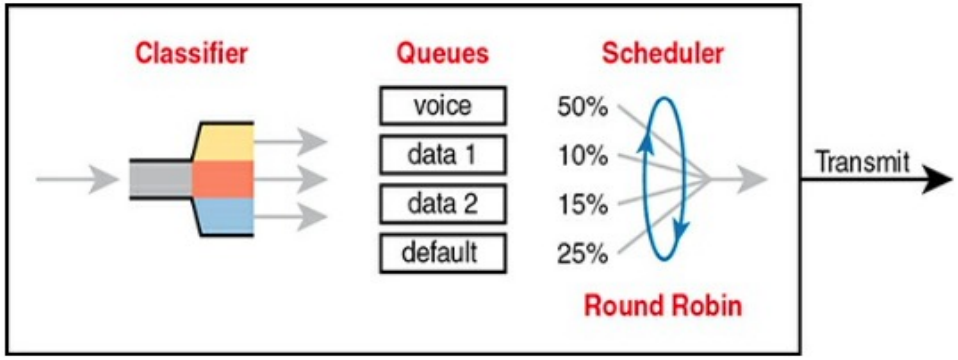
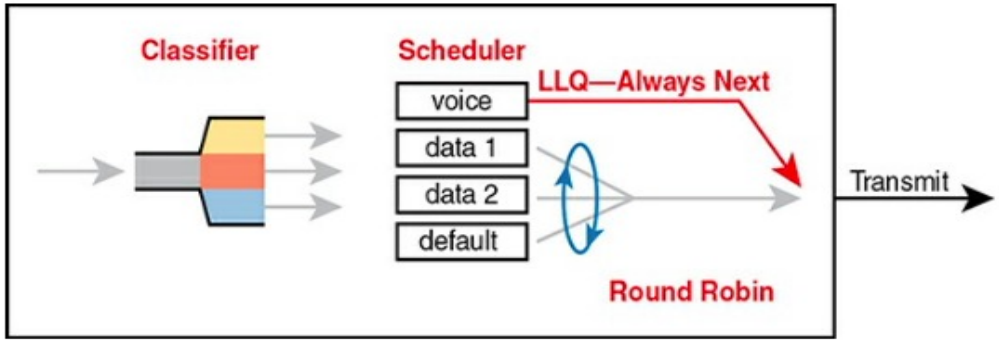


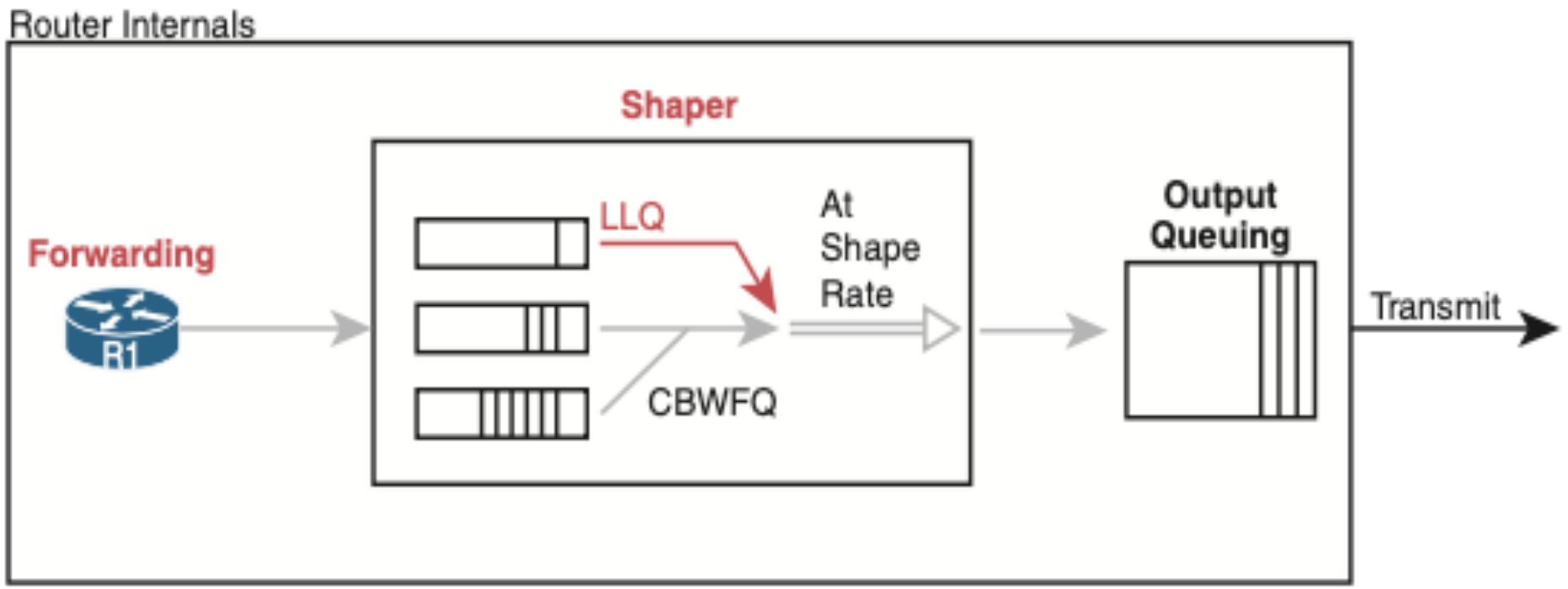
Figure 11-16 *Round Robin Not Good for Voice Delay (Latency) and Jitter*

Topic



QOS WITH LLQ and CBWFQ

Figure 6-10 Shaping with LLQ and CBWFQ

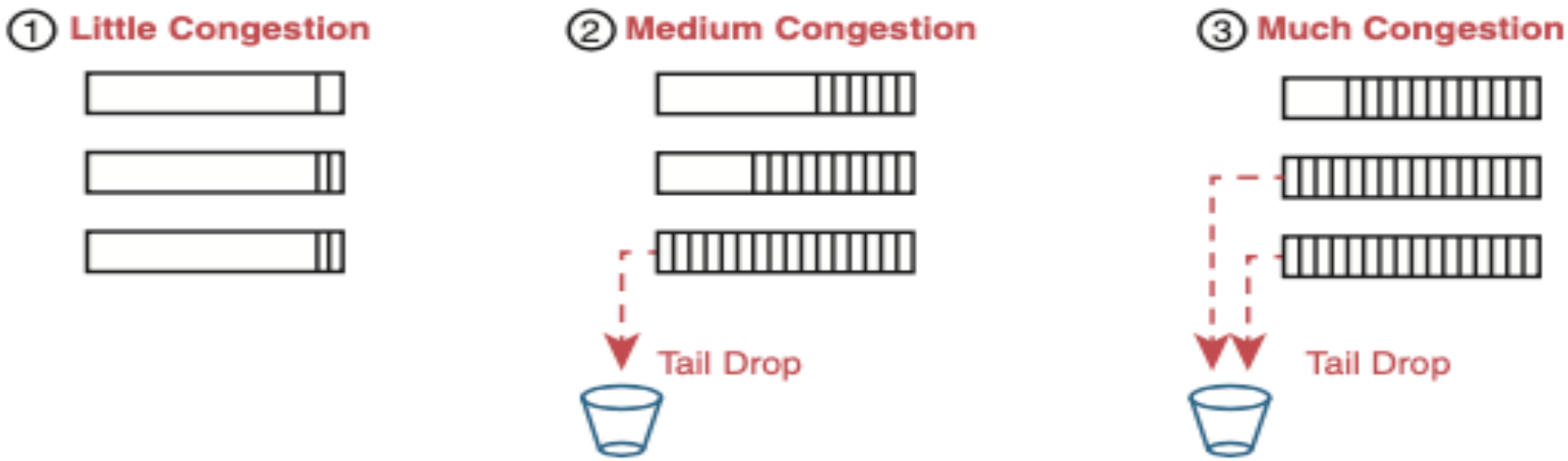


QOS and TCP

QoS and TCP

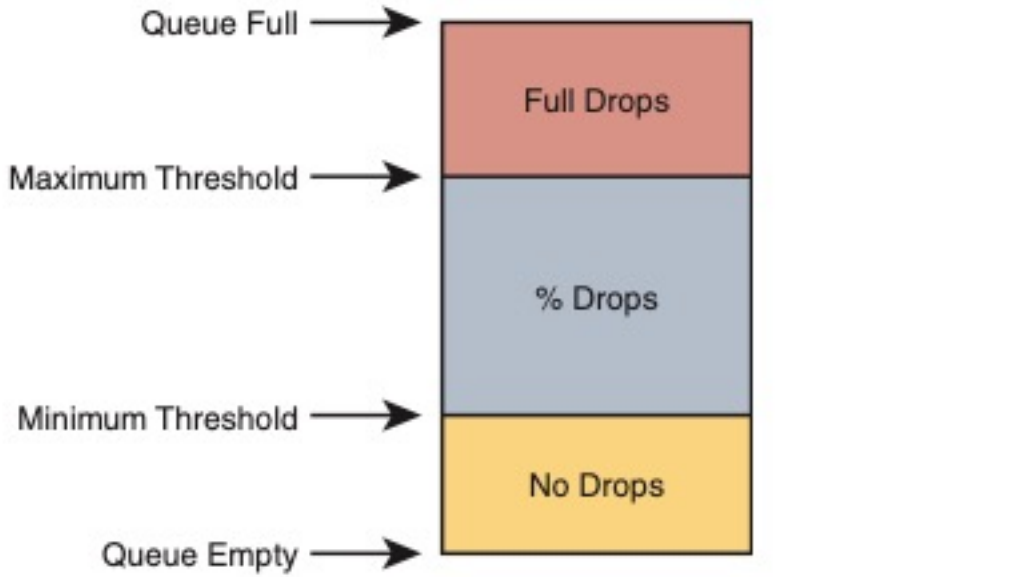
Without congestion-avoidance tools, tail drop can occur (see Figure 6-11).

Figure 6-11 Tail Drop Example



QOS Queue Threshold Discarding TCP Packets

Figure 6-12 Queue Thresholds for Discarding TCP Packets



QOS Characteristics of Major traffic and Tools

Figure 6-1 Characteristics of Major Traffic Types

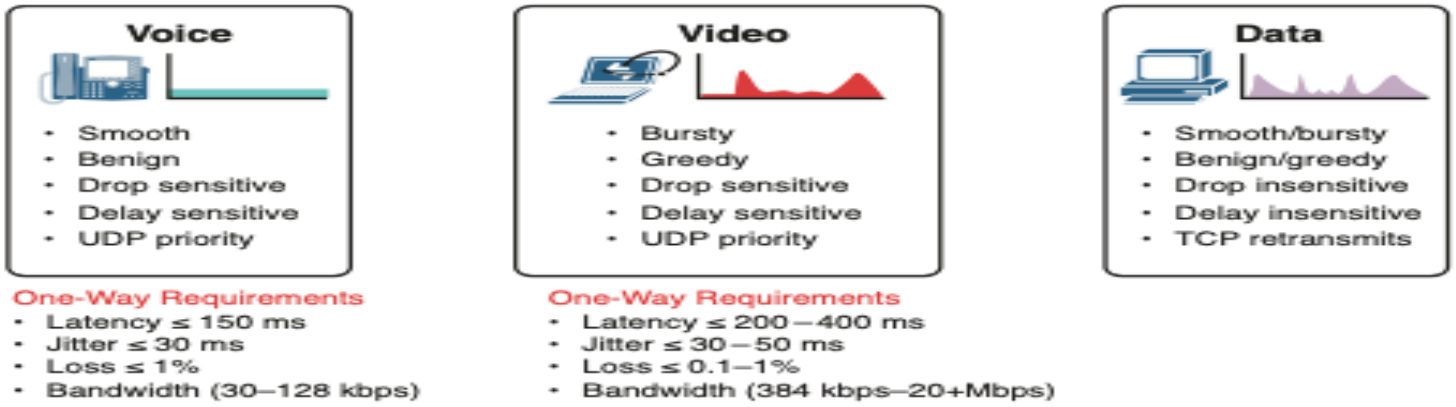
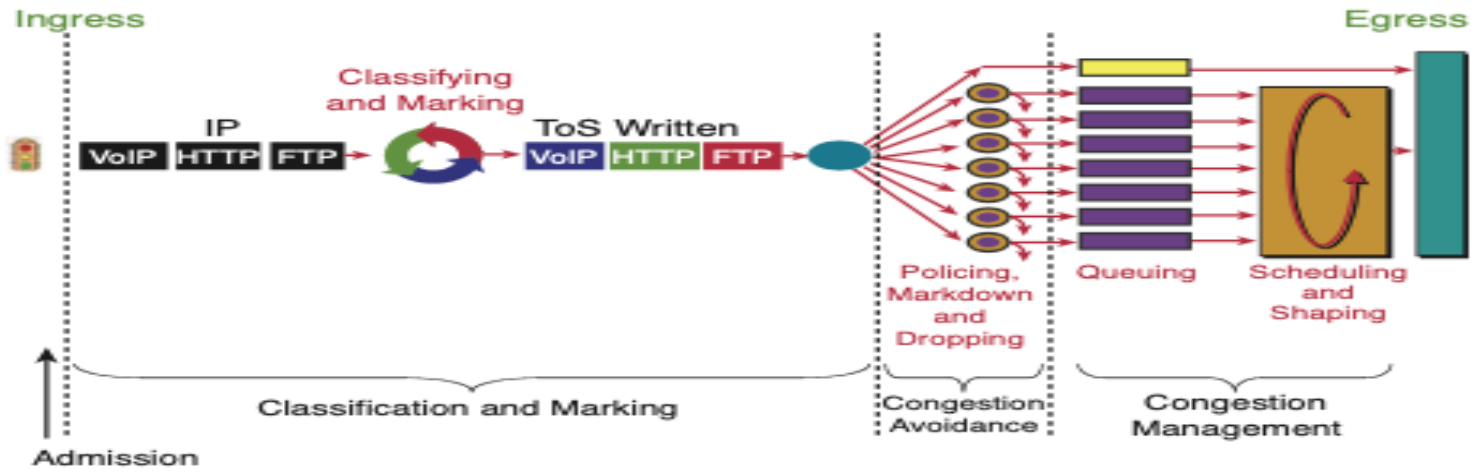


Figure 6-2 shows the sequence of QoS events as traffic is forwarded out an interface.

Figure 6-2 Overview of QoS Tools



ToS and Traffic Class in IPV4 and IPV6 Field

Figure 6-3 The ToS and Traffic Class Fields in IPv4 and IPv6

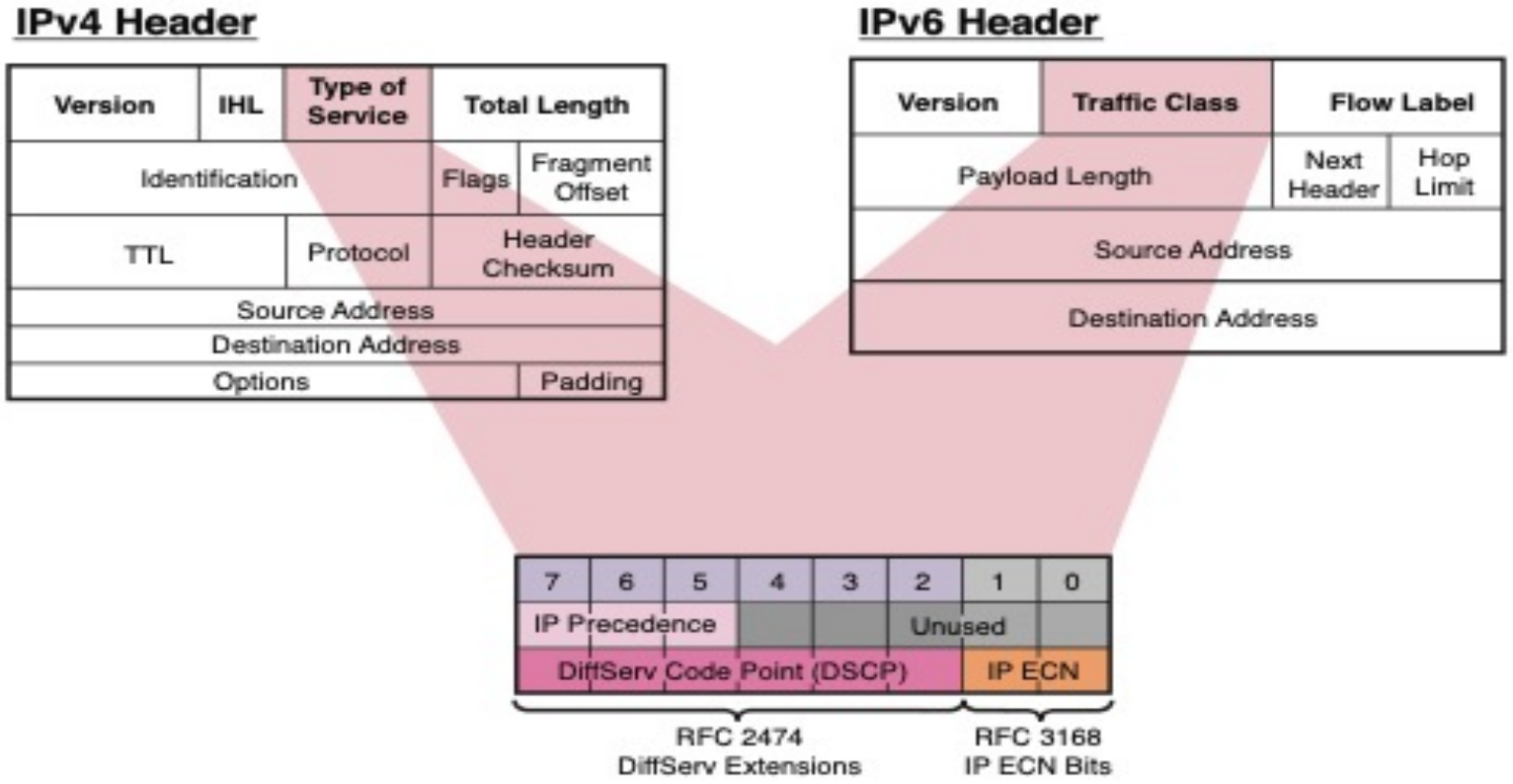
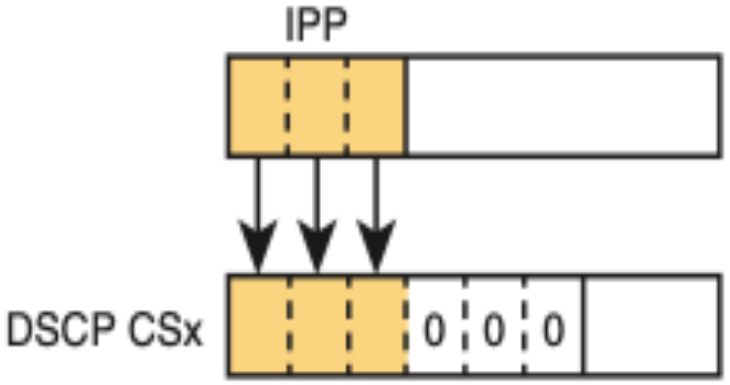


Figure 6-3 highlights the Differentiated Services Code Point (DSCP) bits, which are the core of the Differentiated Services (DiffServ) model for QoS. QoS tools can use the 2 bits allotted for IP Explicit Congestion Notification (ECN) to inform downstream routers of congestion in the traffic flow.

QOS Class Selector Value

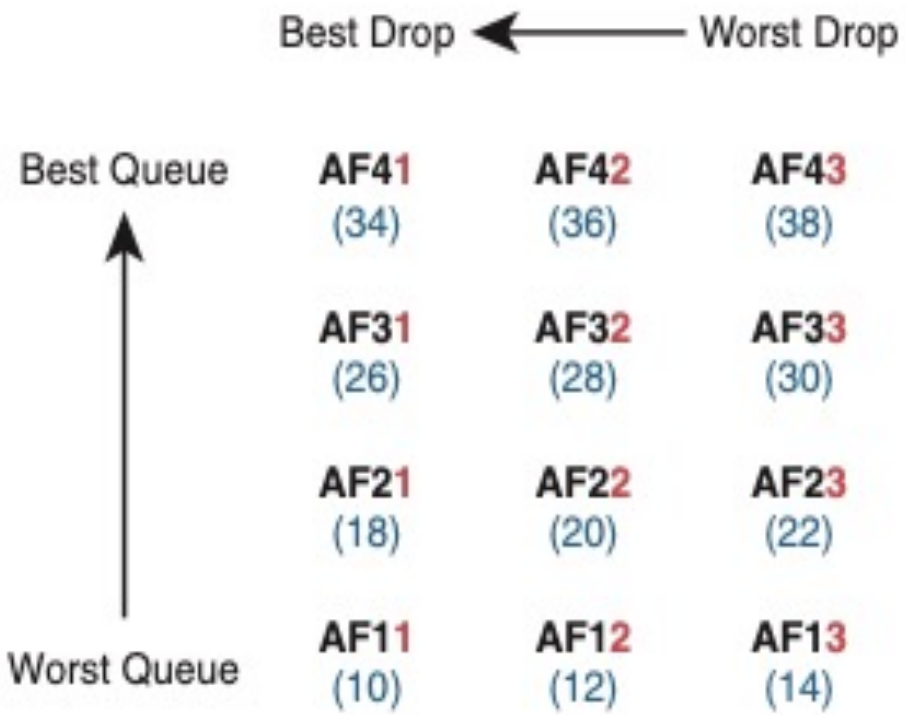
Figure 6-4 The Class Selector Values



IPP	CS	Decimal DSCP
0	CS0	0
1	CS1	8
2	CS2	16
3	CS3	24
4	CS4	32
5	CS5	40
6	CS6	48
7	CS7	56

AF DSCP Values

Figure 6-6 AF DSCP Values



Qos Marking Example

Figure 6-5 CoS Marking Example

Additional fields that can be marked for QoS include the Traffic Identifier (TID) field in the 802.11 frame and the EXP field in MPLS. Table 6-1 lists all the QoS fields.

Table 6-1 QoS Marking Fields

Field	Name Header(s)	Length (bits)	Where Used
DSCP	IPv4, IPv6	6	End-to-end packet
IPP	IPv4, IPv6	3	End-to-end packet
CoS	802.1Q	3	Over VLAN trunk
TID	802.11	3	Over Wi-Fi
EXP	MPLS Label	3	Over MPLS WAN

NOTE: The MPLS EXP field was renamed the Traffic Class field in RFC 5462. However, EXP is still commonly used. The EXP name comes from the designation "experimental use."

Syslog Severity Levels

Keyword	Numeral	Description	
Emergency	0	System unusable	Severe
Alert	1	Immediate action required	
Critical	2	Critical Event (Highest of 3)	Impactful
Error	3	Error Event (Middle of 3)	
Warning	4	Warning Event (Lowest of 3)	
Notification	5	Normal, More Important	Normal
Informational	6	Normal, Less Important	
Debug	7	Requested by User Debug	Debug

Figure 9-3 *Syslog Message Severity Levels by Keyword and Numeral*

Security

Table 4-4 Summary of Human Security Vulnerabilities

Attack Type	Goal
Social engineering	Exploits human trust and social behavior
Phishing	Disguises a malicious invitation as something legitimate
Spear phishing	Targets group of similar users
Whaling	Targets high-profile individuals
Vishing	Uses voice calls
Smishing	Uses SMS text messages
Pharming	Uses legitimate services to send users to a compromised site
Watering hole	Targets specific victims who visit a compromised site

Security Terms

Table 11-1 Security Terms

Term	Description
Assets	Anything of value to the organization, including people, equipment, resources, and data.
Vulnerability	A weakness in a system or its design that could be exploited by a threat.
Threat	A potential danger to a company's assets, data, or network functionality.
Exploit	A mechanism that takes advantage of a vulnerability.
Mitigation	The process of taking countermeasures to reduce the likelihood or severity of a potential threat or risk.
Risk	The likelihood of a threat exploiting the vulnerability of an asset, with the aim of negatively affecting an organization.

Data Loss Vector

Table 11-2 Data Loss Vectors

Vector	Description
Email/social networking	Intercepted email or IM messages could be captured and reveal confidential information.
Unencrypted devices	If data is not stored using an encryption algorithm, the thief may be able to retrieve valuable confidential data.
Cloud storage devices	Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
Removable media	An employee could perform an unauthorized transfer of data to a USB drive or a USB drive containing valuable corporate data could be lost.
Hard copy	Confidential data should be shredded when no longer required.
Improper access control	Passwords or weak passwords that have been compromised can provide a threat actor with easy access to corporate data.

Pentest Tools

Table 11-3 Types of Penetration Tools

Tool	Description
Password crackers	Password cracking tools are often referred to as password recovery tools and can be used to crack or recover a password. Password crackers repeatedly make guesses in order to crack the password.
Wireless hacking tools	Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities.
Network scanning and hacking tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports.

Tool	Description
Packet crafting tools	These tools are used to probe and test a firewall's robustness using specially crafted forged packets.
Packet sniffers	These tools are used to capture and analyze packets in traditional Ethernet LANs or WLANs.
Rootkit detectors	This is a directory and file integrity checker used by white hats to detect installed rootkits.
Forensic tools	These tools are used by white hat hackers to sniff out any trace of evidence existing in a computer.
Debuggers	These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware.
Hacking operating systems	These are specially designed operating systems preloaded with tools optimized for hacking.
Encryption tools	Encryption tools use algorithm schemes to encode data to prevent unauthorized access to the encrypted data.
Vulnerability exploitation tools	These tools identify whether a remote host is vulnerable to security attack.
Vulnerability scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan virtual machines (VMs), devices brought to work by individuals in a bring-your-own-device (BYOD) situation, and client databases.

Attacks Types

Table 11-4 Common Types of Attacks

Attack Type	Description
Eavesdropping attack	A threat actor captures and "listens" to network traffic. This attack is also referred to as *sniffing* or *snooping*.
Data modification attack	If threat actors have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.
IP address spoofing attack	A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
Password-based attacks	A threat actor who discovers a valid user account has the same rights as the real user. A threat actor can use a valid account to obtain lists of other users or network information, change server and network configurations, and modify, reroute, or delete data.
Denial of service attack	A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can flood a computer or an entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

Attack Type	Description
Man-in-the-middle attack	This attack occurs when threat actors have positioned themselves between a source and destination. They can actively monitor, capture, and control the communication transparently.
Compromised-key attack	If a threat actor obtains a secret key, that key is referred to as a *compromised key*. A compromised key can be used to gain access to secured communication without the sender or receiver being aware of the attack.
Sniffer attack	A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If packets are not encrypted, a sniffer provides a full view of the data inside the packet.

Malware Types

Table 4-3 Summary of Malware Types

Characteristic	Trojan Horse	Virus	Worm
Packaged inside other software	Yes	No	No
Self-injected into other software	No	Yes	No
Propagates automatically	No	No	Yes

Other Types of Malware

Table 11-5 Other Types of Malware

Malware	Description
Adware	Adware is usually distributed by downloading online software. Adware can display unsolicited advertising using popup web browser windows or new toolbars, or it can unexpectedly redirect a user from a web page to a different website. Popup windows may be difficult to control as new windows can pop up faster than the user can close them.
Ransomware	Ransomware typically denies a user access to his or her files by encrypting the files and then displaying a message demanding a ransom for the decryption key. Users without up-to-date backups must pay the ransom to decrypt their files. Payment is usually made using wire transfer or cryptocurrencies such as bitcoin.

Malware	Description
Rootkit	Threat actors use rootkits to gain administrator account–level access to a computer. They are very difficult to detect because they can alter firewall, antivirus protection, system files, and even OS commands to conceal their presence. A rootkit can provide a backdoor to threat actors, giving them access to the PC and allowing them to upload files and install new software to be used in a distributed DoS (DDoS) attack. Special rootkit removal tools must be used to remove them, or a complete OS re-install may be required.
Spyware	Spyware is similar to adware but is used to gather information about the user and send it to threat actors without the user's consent. Spyware can be a low threat, gathering browsing data, or it can be a high threat, capturing personal and financial information.

Recon Attacks Techniques

Table 11-6 Reconnaissance Attack Techniques

Technique	Description
Perform an information query of a target	The threat actor looks for initial information about a target. Various tools can be used, including a Google search, the organization's website, and whois.
Initiate a ping sweep of the target network	The information query usually reveals the target's network address. The threat actor can then initiate a ping sweep to determine which IP addresses are active.
Initiate a port scan of active IP addresses	A port scan can be used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Run vulnerability scanners	A vulnerability scanner can query the identified ports to determine the type and version of the application and operating system running on the host. Examples of such tools include Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.
Run exploitation tools	The threat actor attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist, including Metasploit, Core Impact, sqlmap, Social-Engineer Toolkit, and Netsparker.

Types of access Attacks

Table 11-7 Types of Access Attacks

Access Attack	Description
Password attack	The threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.
Spoofing attack	The threat actor has a device pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.
Trust exploitation	The threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
Port redirection	The threat actor uses a compromised system as a base for attacks against other targets.
Man-in-the-middle attack	The threat actor is positioned between two legitimate entities in order to read or modify the data that passes between the two parties.
Buffer overflow attack	The threat actor exploits the buffer memory and overwhelms it with unexpected values. This usually renders the system inoperable, creating a DoS attack.

Types of Social Engineering Attacks

Table 11-8 Types of Social Engineering Attacks

Social Engineering Attack	Description
Pretexting	An attack in which a threat actor pretends to need personal or financial data to confirm the identity of the target.
Phishing	An attack in which a threat actor sends fraudulent email that is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on his or her device or into sharing personal or financial information.
Spear phishing	An attack in which a threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Unsolicited email, also known as junk mail, that often contains harmful links, malware, or deceptive content.

Social Engineering Attack	Description
Something for something	Sometimes called *quid pro quo*, an attack in which a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	An attack in which a threat actor leaves a malware-infected flash drive in a public location. A victim finds the drive and inserts it into a laptop, unintentionally installing malware.
Impersonation	An attack in which a threat actor pretends to be someone he or she is not to gain the trust of a victim.
Tailgating	An attack in which a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	An attack in which a threat actor inconspicuously looks over someone's shoulder to steal passwords or other information.
Dumpster diving	An attack in which a threat actor rummages through trash bins to discover confidential documents.

Types of IP Attacks

Table 11-9 Types of IP Attacks

IP Attack Technique	Description
ICMP attacks	Threat actors use Internet Control Message Protocol (ICMP) echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
Amplification and reflection attack	Threat actors attempt to prevent legitimate users from accessing information or services using DoS and DDoS attacks. In one type of amplification and reflection attack, the threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim. Therefore, these hosts all reply to the spoofed IP address of the victim and overwhelm it.
Address spoofing attack	Threat actors spoof the source IP address in an IP packet to perform blind spoofing or non-blind spoofing. In non-blind spoofing, the threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also be done to hijack an authorized session. In blind spoofing, the threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.
Man-in-the-middle (MITM) attack	Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They can eavesdrop by inspecting captured packets or alter packets and forward them to their original destination.
Session hijacking	Threat actors gain access to the physical network and then use an MITM attack to hijack a session.

- **User awareness:** All users should be made aware of the need for data confidentiality to protect corporate information, as well as their own credentials and personal information. They should also be made aware of potential threats, schemes to mislead, and proper procedures to report security incidents. Users should also be instructed to follow strict guidelines regarding data loss. For example, users should not include sensitive information in emails or attachments, should not keep or transmit that information from a smartphone, or store it on cloud services or removable storage drives.
- **User training:** All users should be required to participate in periodic formal training so that they become familiar with all corporate security policies. (This also implies that the enterprise should develop and publish formal security policies for its employees, users, and business partners to follow.)
- **Physical access control:** Infrastructure locations, such as network closets and data centers, should remain securely locked. Badge access to sensitive locations is a scalable solution, offering an audit trail of identities and timestamps when access is granted. Administrators can control access on a granular basis and quickly remove access when an employee is dismissed.

Commands and Encoding Types for the **username secret** Command

Table 5-3 Commands and Encoding Types for the **username secret** Command

Command	Type	Algorithm
username *name* [**algorithm-type md5**] **secret** *password*	5	MD5
username *name* **algorithm-type sha256 secret** *password*	8	SHA-256

Actions that switch port will take

Table 20-2 Actions When Port Security Violation Occurs

Option on the switchport port-security violation Command	protect	restrict	shutdown
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface, discarding all traffic	No	No	Yes

Port Security Example

Example 20-5 Port Security Configuration Example

```
S1(config)# interface range fa 0/5 - fa 0/24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport port-security
S1(config-if-range)# switchport port-security maximum 3
S1(config-if-range)# switchport port-security violation restrict
S1(config-if-range)# switchport port-security mac-address sticky
```

Parameters for Port Security Aging

```
Switch(config-if)# switchport port-security aging { static | time time |
  type {absolute | inactivity}}
```

Table 20-3 describes the parameters for this command.

Table 20-3 Parameters for the *port-security aging* Command

Parameter	Description
`static`	Enable aging for statically configured secure addresses on this port.
`time` *time*	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
`type absolute`	Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
`type inactivity`	Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

WIRELESS

- Type of Wireless Connection

WEP WPA WAP2

RF is an electromagnetic frequency

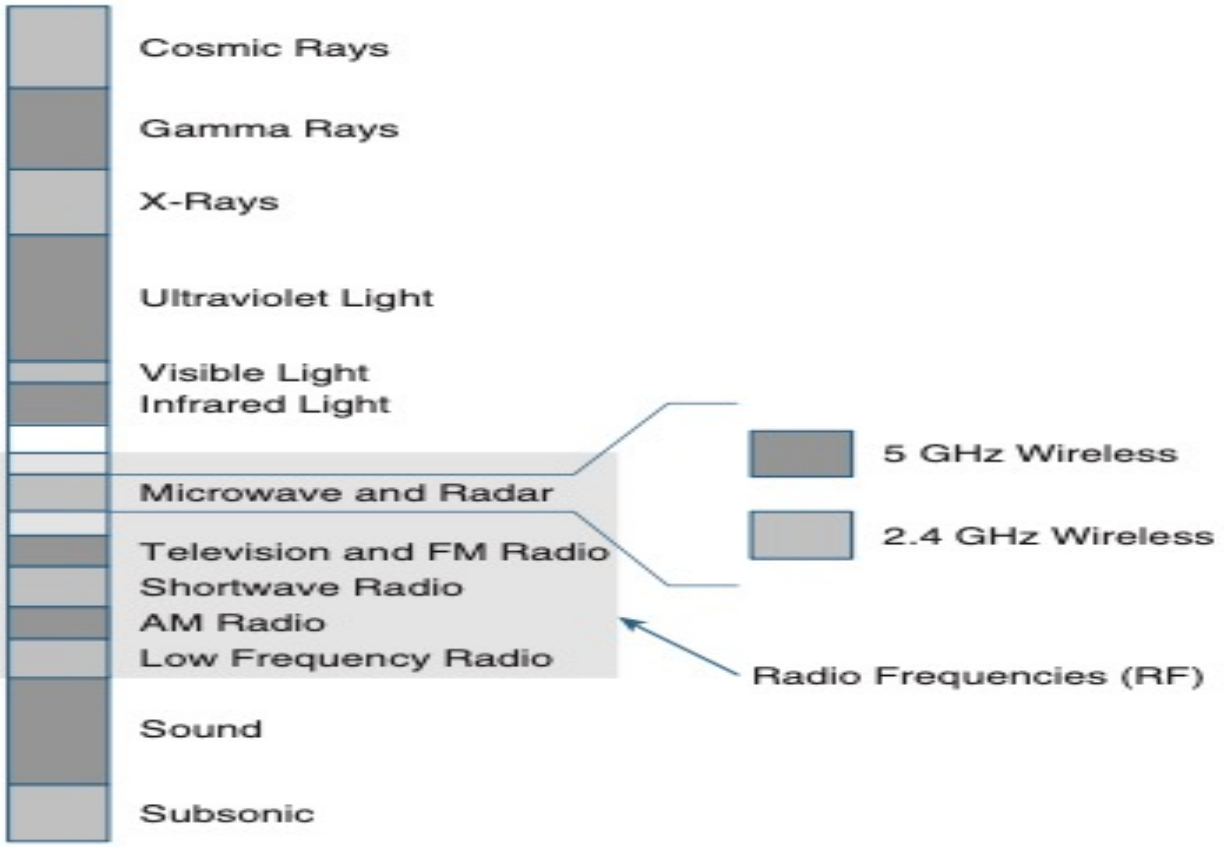
CSMA/CD is used in wired connections to recover collision CSMA/CA is used in wireless to avoid collision

Wi-Fi use 2 bands 2.4 ghz and 5 ghz

RF Spectrum

Figure 22-1 RF Spectrum

Frequency (Hz)	Frequency Notation
10^{21}	
10^{20}	
10^{19}	
10^{18}	
10^{17}	
10^{16}	
10^{15}	
10^{14}	
10^{13}	
10^{12}	
10^{11}	100 GHz
10^{10}	10 GHz
10^{9}	1 GHz
10^{8}	100 MHz
10^{7}	10 MHz
10^{6}	1 MHz
10^{5}	100 kHz
10^{4}	10 kHz
10^{3}	1 kHz
10^{2}	100 Hz
10^{1}	10 Hz
0	0 Hz



2.4 and 5GHZ Channel

Figure 22-2 2.4-GHz Channels

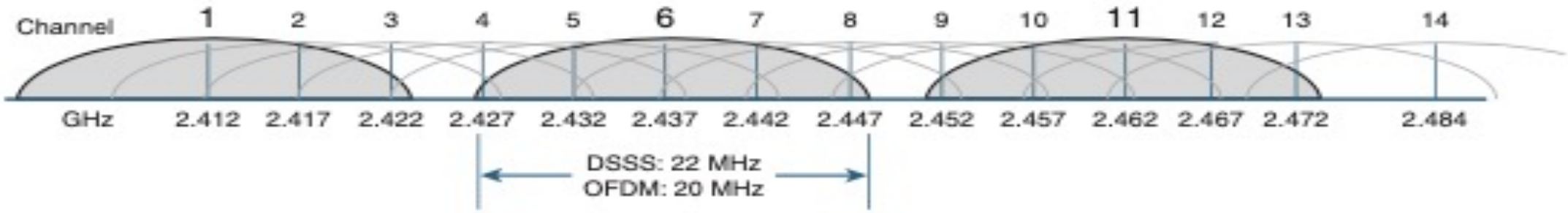
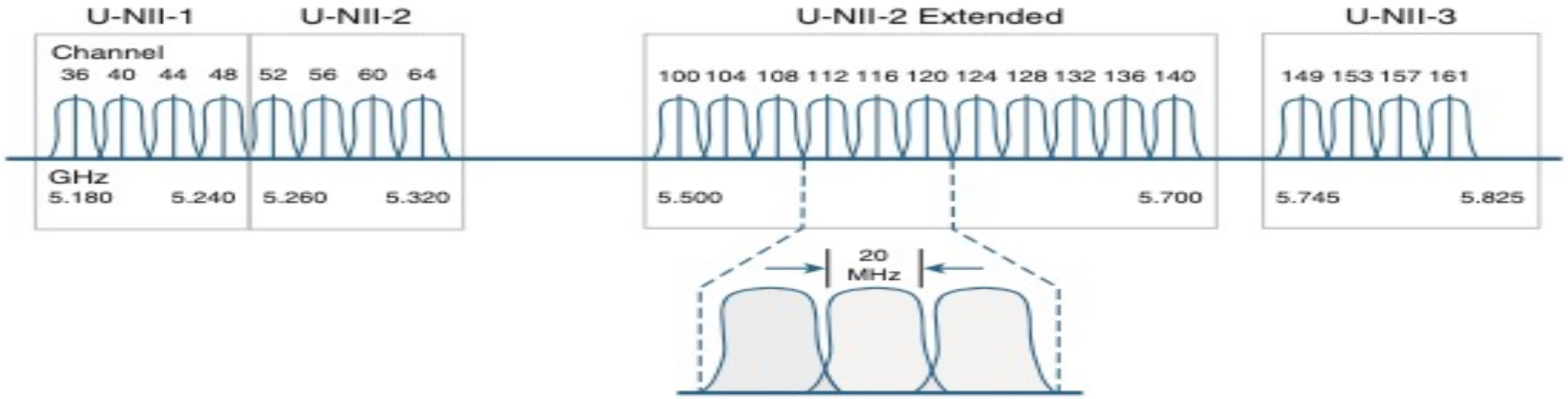


Figure 22-3 5-GHz Channels



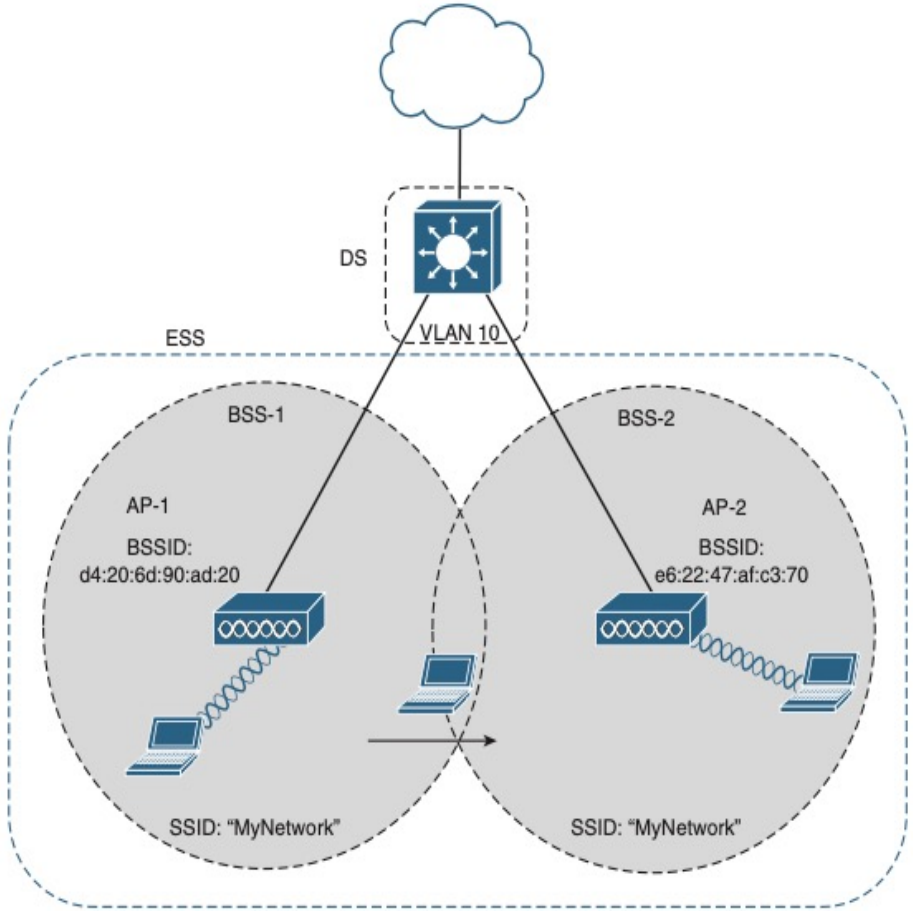
802.11 Standards

Table 22-1 Summary of 802.11 Standards

IEEE WLAN Standard	Radio Frequency	Description
802.11	2.4 GHz	Speeds of up to 2 Mbps
802.11a	5 GHz	Speeds of up to 54 Mbps Small coverage area Less effective at penetrating building structures Not interoperable with 802.11b and 802.11g
802.11b	2.4 GHz	Speeds of up to 11 Mbps Longer range than 802.11a Better able to penetrate building structures
802.11g	2.4 GHz	Speeds of up to 54 Mbps Backward compatible with 802.11b with reduced bandwidth capacity
802.11n	2.4 GHz 5 GHz	Data rates ranging from 150 Mbps to 600 Mbps with a distance range of up to 70 m (230 feet) APs and wireless clients require multiple antennas using MIMO technology Backward compatible with 802.11a/b/g devices with limiting data rates
802.11ac	5 GHz	Provides data rates ranging from 450 Mbps to 1.3 Gbps (1300 Mbps) using MIMO technology Up to eight antennas can be supported Backward compatible with 802.11a/n devices with limiting data rates
802.11ax	2.4 GHz 5 GHz	Released in 2019 (latest standard) Also known as High-Efficiency Wireless (HEW) Higher data rates and increased capacity Handles many connected devices Improved power efficiency 1 GHz and 7 GHz capable when those frequencies become available

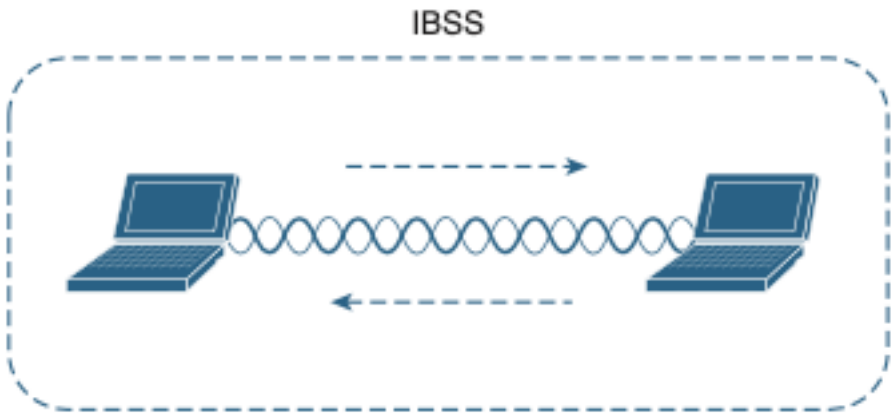
Wireless Topology ESS Infrastructure Mode

Figure 22-4 Example of ESS Infrastructure Mode



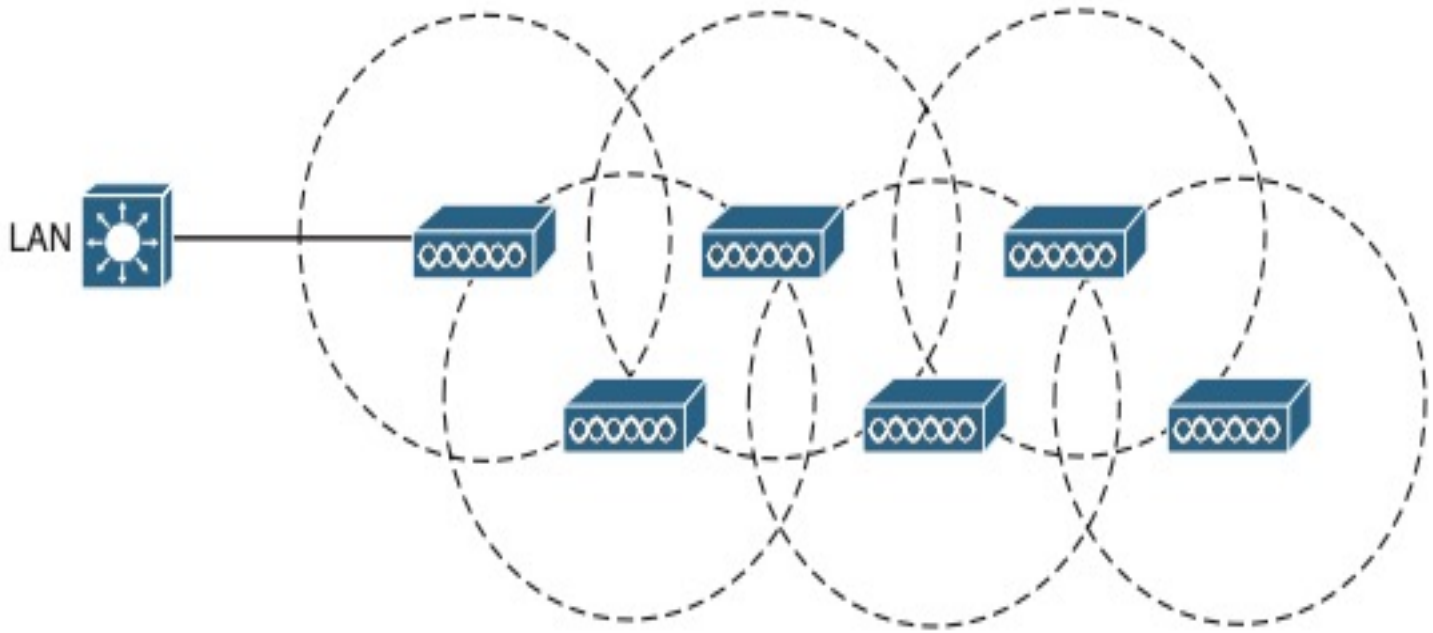
IBSS Topology

Figure 22-5 802.11 Independent Basic Service Set



Mesh Topology

Figure 22-6 Example of a Wireless Mesh Network

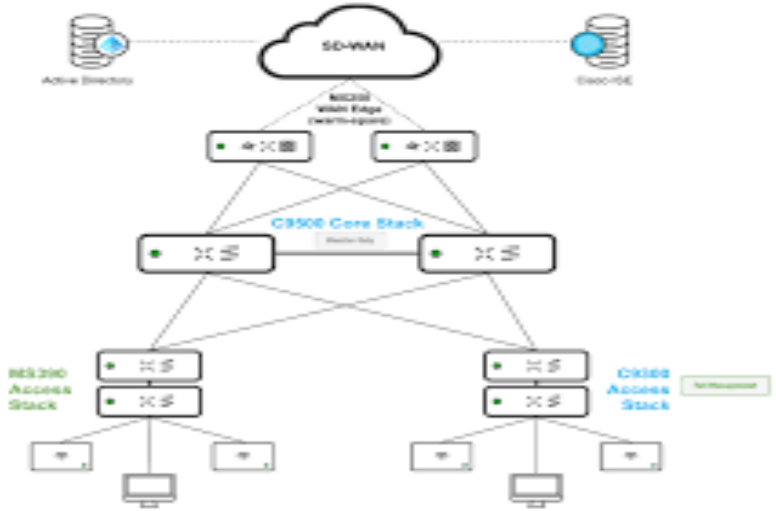


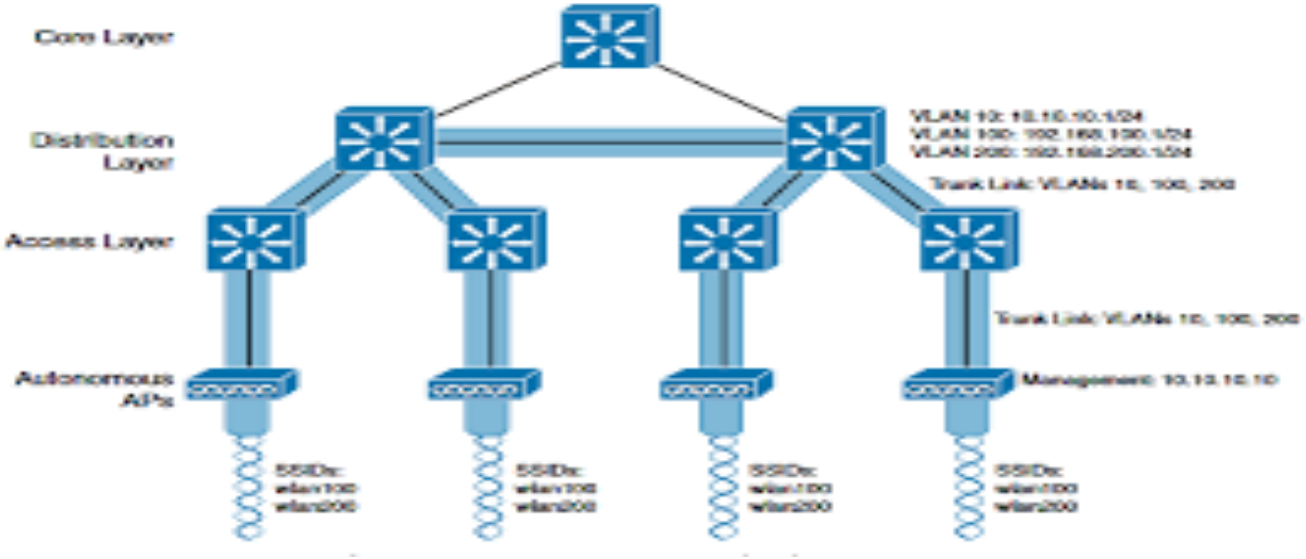
- Wi-Fi 6 has expanded to the 6GHZ band
- channel bonding can be used to combine the channel
- IBSS is a wireless connection in which 2 devices connect directly without using an AP This is called ad-hoc
- BSS clients connect to each other Via AP but not directly with each other
- When you move between AP in an extended service set is called Roaming
- MBSS (Mesh Basic Set Service) is used when is difficult to run an ethernet connection to the AP
- MBSS in Repeater Mode can extend the range

Wireless Architecture

- Beacons are sent periodically to AP to advertise BSS
- There are 3 types of wireless LAN deployment Autonomous Lightweight and cloud
- Autonomous AP does not rely on a WLC (Wireless LAN controller) they are configured individually This is fine for Small Network
- a Wireless LAN architecture with Controller a CAPWAP tunnel is created
- WLC provide channel assignment
- In sniffer mode the AP is dedicated to capturing packets it doesn't BSS for the Client

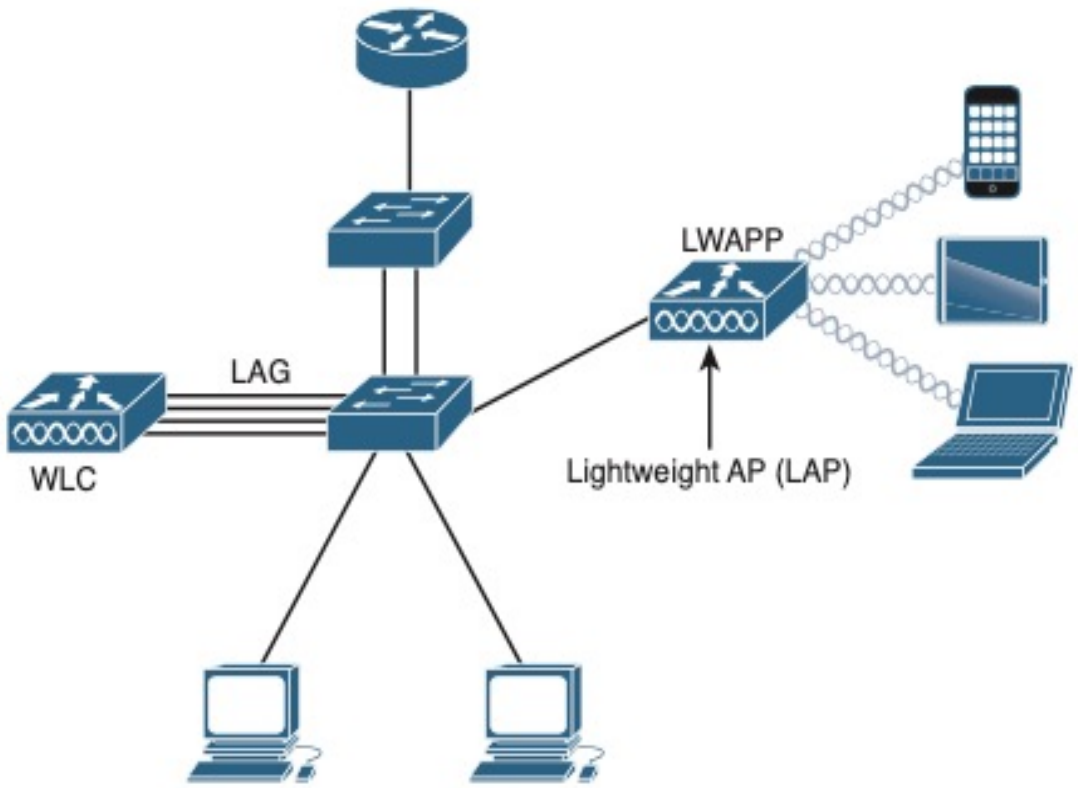
- Cloud base architecture is between Autonomous AP and split architecture one example is Meraki
- Lightweight AP Are Managed By a Centralized controller Cloud Base AP is Managed by a Central Device like Cisco Meraki



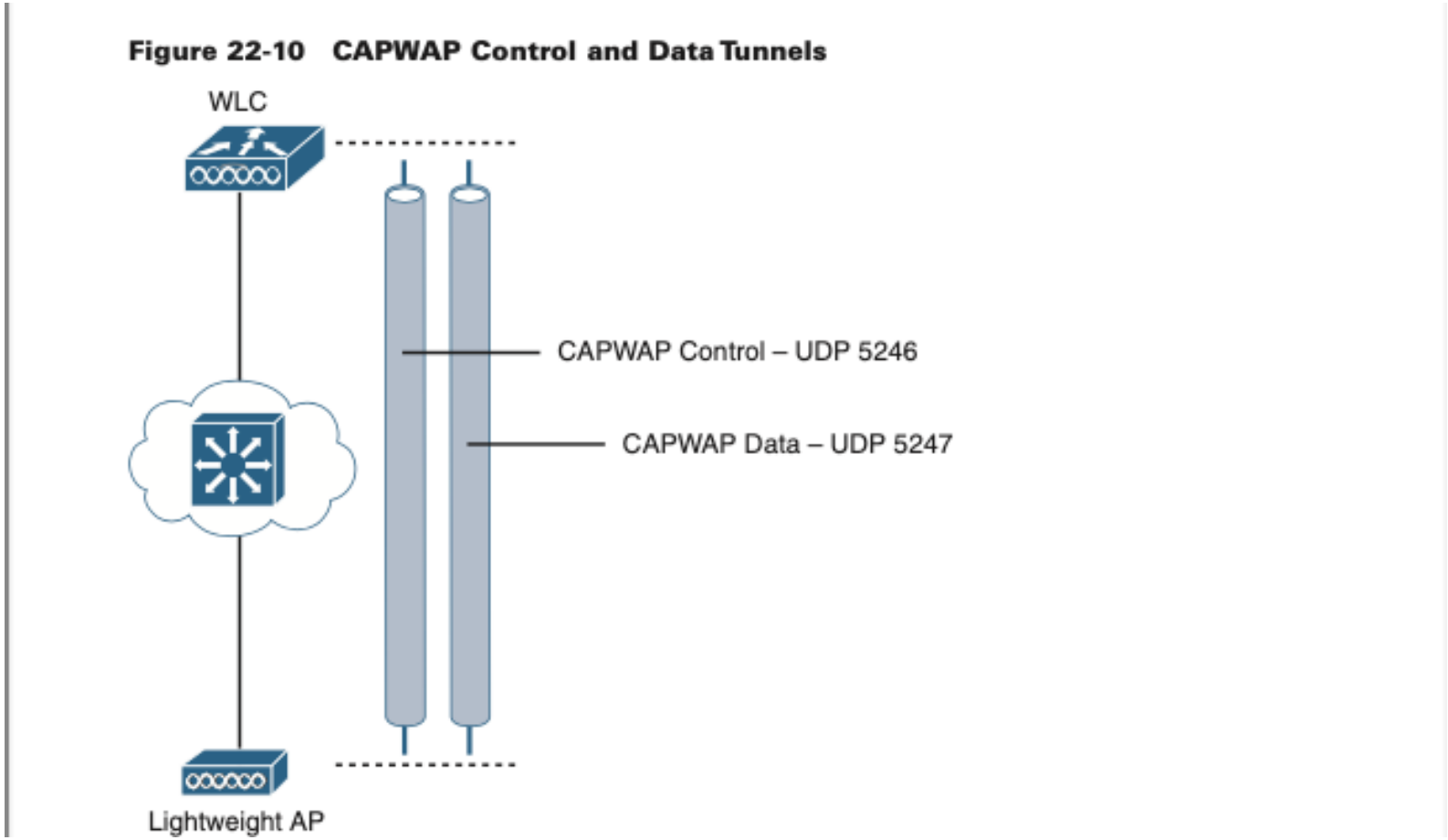


Controller Based AP Architecture

Figure 22-9 Controller-Based AP Architecture

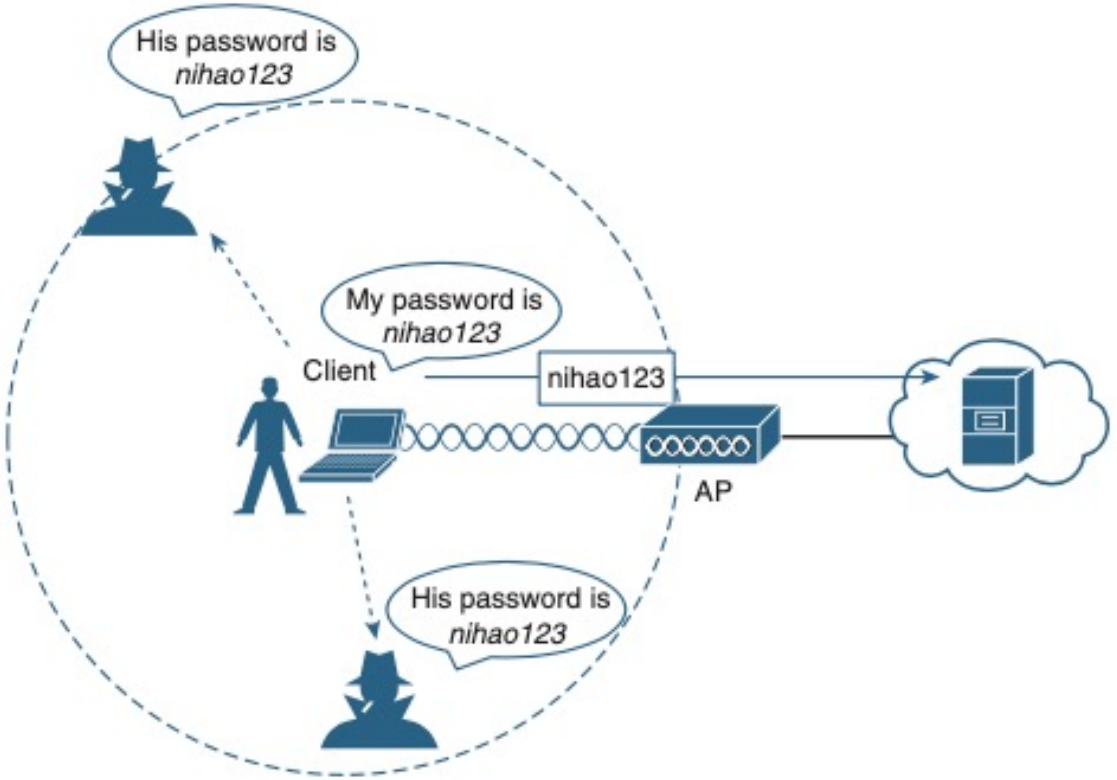


Capwap Control and Data Tunnel



Open Wireless Network

Figure 22-11 Open Wireless Network



Shared Key Authentication Method

Table 22-3 Shared Key Authentication Methods

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. However, the key never changes when exchanging packets. This makes WEP easy to hack. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.

Authentication Method	Description
WPA2	The current industry standard for securing wireless networks. It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	The next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF). However, devices with WPA3 are not yet readily available.

Split Mac Function of the AP and WLC

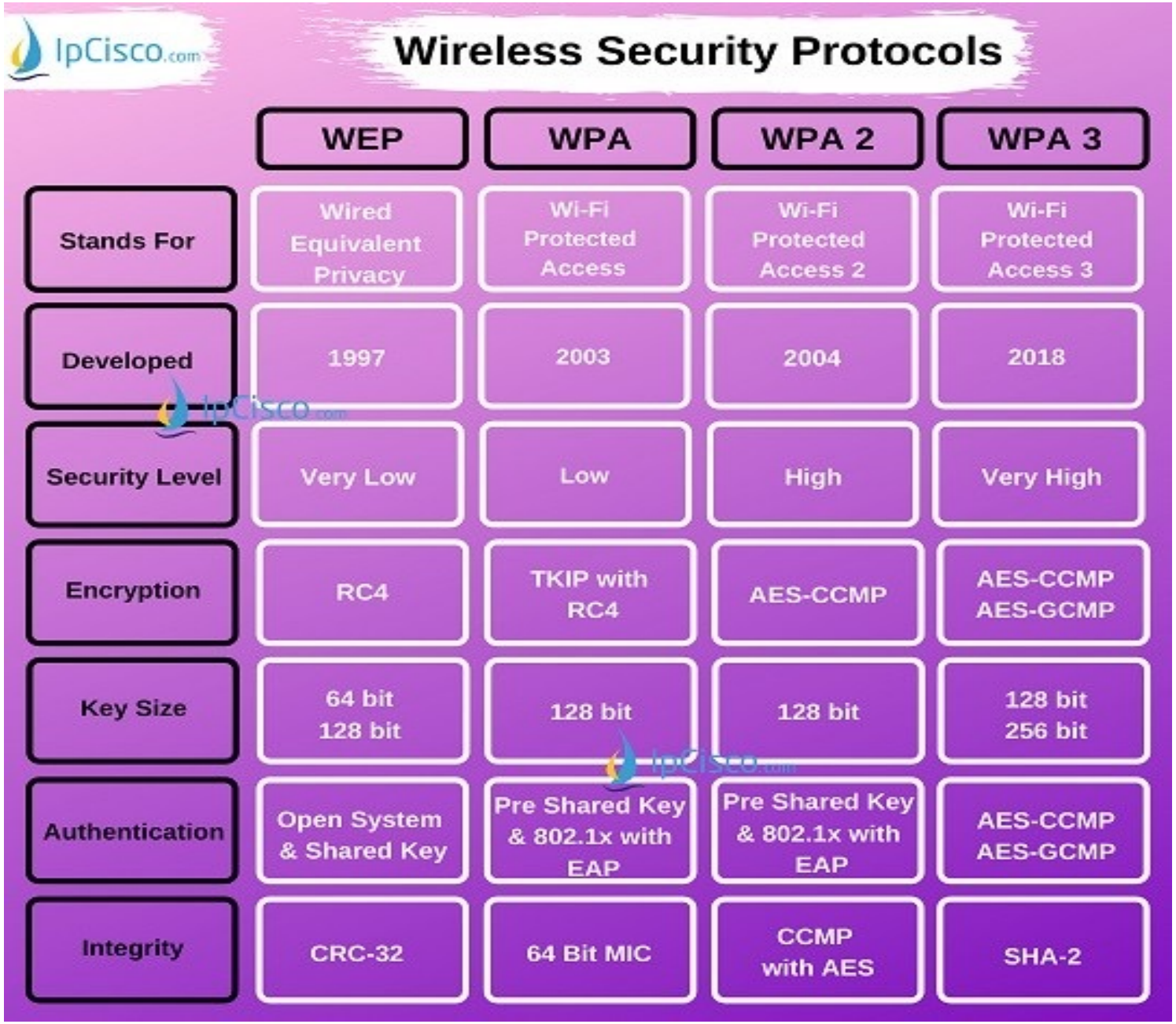
Table 22-2 Split-MAC Functions of the AP and WLC

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgments and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

Wireless Encryption

- all client must be authenticated before they can join the SSID
- integrity ensured the message is not modified in transit for that a MIC is added
- Open authentication is the first standard client sends the request and the AP accepts all is not secure
- WEP is another way of authentication it provides encryption it uses RC4 wep is not secured regardless of the lenght of the Key
- EAP is a framework where other methods are based on
- in EAP used authenticator authentication server and the suplicant

- LEAP is the improvement for for WEP is vulnerable and is not used anymore
- EAP-TLS required certification in the client and the server
- TKIP is based on WEP but has more security Features TKIP is more Secure than WEP
- CCMP is more secure it uses WPA2 it uses AES for counter mode
- GCMP is more secure and more efficient than CCMP it is used in Wi-Fi protected 3
- PSK is used to generate encryption KEy
- all 3 WPA use personal and enterprise mode
- SAE protects the 4 way handshake using Personal Mode
- WLC only supports static LAG and the port is supposed to be configured to mode on


IpCisco.com
Wireless Security Protocols
WEP
WPA
WPA 2
WPA 3
Stands For
Wired Equivalent Privacy
Wi-Fi Protected Access
Wi-Fi Protected Access 2
Wi-Fi Protected Access 3
Developed
1997
2003
2004
2018
Security Level
Very Low
Low
High
Very High
Encryption
RC4
TKIP with RC4
AES-CCMP
AES-CCMP AES-GCMP
Key Size
64 bit 128 bit
128 bit
128 bit
128 bit 256 bit
Authentication
Open System & Shared Key
Pre Shared Key & 802.1x with EAP
Pre Shared Key & 802.1x with EAP
AES-CCMP AES-GCMP
Integrity
CRC-32
64 Bit MIC
CCMP with AES
SHA-2

Wireless Characteristics

Key Topic

Table 26-3 Basic Characteristics of Some IEEE 802.11 Amendments

Amendment	2.4 GHz	5 GHz	Max Data Rate	Notes
802.11-1997	Yes	No	2 Mbps	The original 802.11 standard ratified in 1997
802.11b	Yes	No	11 Mbps	Introduced in 1999
802.11g	Yes	No	54 Mbps	Introduced in 2003
802.11a	No	Yes	54 Mbps	Introduced in 1999
802.11n	Yes	Yes	600 Mbps	HT (high throughput), introduced in 2009
802.11ac	No	Yes	6.93 Gbps	VHT (very high throughput), introduced in 2013
802.11ax	Yes	Yes	4x 802.11ac	High Efficiency Wireless, Wi-Fi6; expected late 2019; will operate on other bands too, as they become available

Authentication and Encryption Comparison

Key Topic

Table 28-2 Comparing WPA, WPA2, and WPA3

Authentication and Encryption Feature Support	WPA	WPA2	WPA3*
Authentication with **Pre-Shared Keys?**	Yes	Yes	Yes
Authentication with **802.1x?**	Yes	Yes	Yes
Encryption and MIC with **TKIP?**	Yes	No	No
Encryption and MIC with **AES and CCMP?**	Yes	Yes	No
Encryption and MIC with **AES and GCMP?**	No	No	Yes

Wireless Security Mechanism

Key Topic

Table 28-3 Review of Wireless Security Mechanisms and Options

Security Mechanism	Type		Type Expansion	Credentials Used
Authentication Methods	Open		Open Authentication	None, other than 802.11 protocol
	WEP		Wired Equivalent Privacy	Static WEP keys
	802.1x/EAP (Extensible Authentication Protocol)	LEAP	Lightweight EAP	Deprecated; uses dynamic WEP keys
		EAP-FAST	EAP Flexible Authentication by Secure Tunneling	Uses protected access credential (PAC)
		PEAP	Protected EAP	AS authenticated by digital certificate
		EAP-TLS	EAP Transport Layer Security	Client and AS authenticated by digital certificate
Privacy & Integrity Methods	TKIP		Temporal Key Integrity Protocol	N/A
	CCMP		Counter/CBC-MAC Protocol	N/A
	GCMP		Galois/Counter Mode Protocol	N/A

L2 Wireless Lan Security

scheme to use. Table 29-2 lists the types that are available.

Key Topic

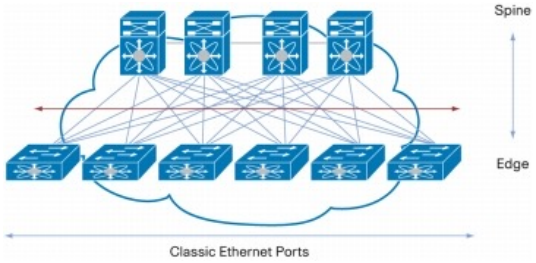
Table 29-2 Layer 2 WLAN Security Type

Option	Description
None	Open authentication
WPA+WPA2	Wi-Fi protected access WPA or WPA2
802.1x	EAP authentication with dynamic WEP
Static WEP	WEP key security
Static WEP + 802.1x	EAP authentication or static WEP
CKIP	Cisco Key Integrity Protocol
None + EAP Passthrough	Open authentication with remote EAP authentication

Frequency Unit

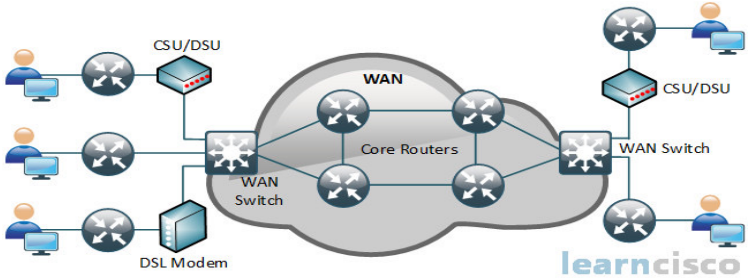
Table 26-2 Frequency Unit Names

Unit	Abbreviation	Meaning
Hertz	Hz	Cycles per second
Kilohertz	kHz	1000 Hz
Megahertz	MHz	1,000,000 Hz
Gigahertz	GHz	1,000,000,000 Hz



Design

- TIER 3 TIER 2
- Tier 2 design includes the core and distribution Together is called the collapse design
- Tier 3 design is set up in the following way Core Distribution and Access
- Spine leaf Design All of the Spine is connected to Leaf switches Leaf switches cannot be connected to leaf switches Spine switches cannot be connected to spine Switches



WAN TECHNOLOGIES

- SITES TO SITES

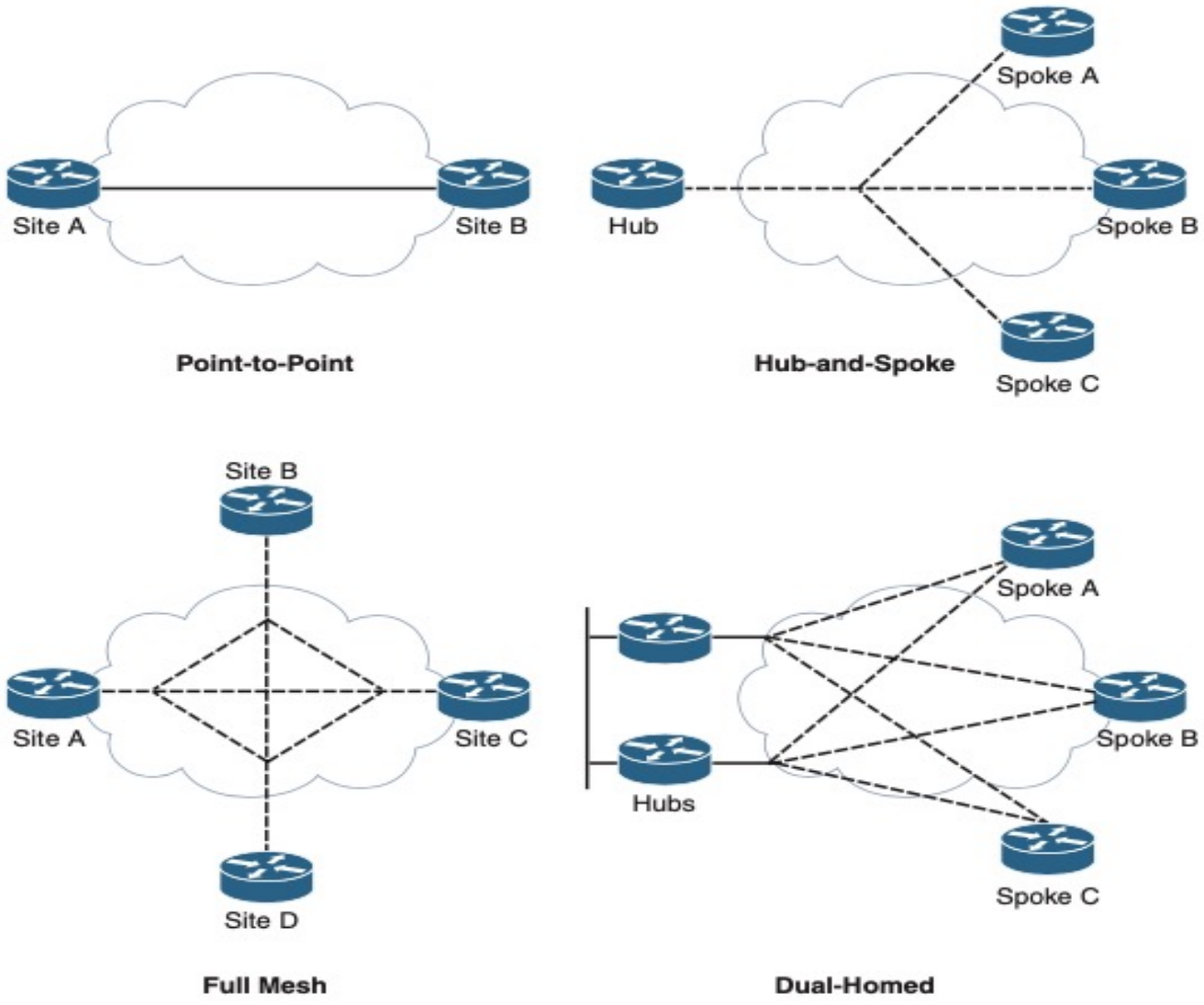
CE and PE
hub and spoke the central site is called the hub the branches connected are called the spoke traffic can be controlled which one can enter and can not

MPLS are shared networks the label switching allows VPN to separated traffic between router

CE mean costumer routers PE routers are provider router and the P

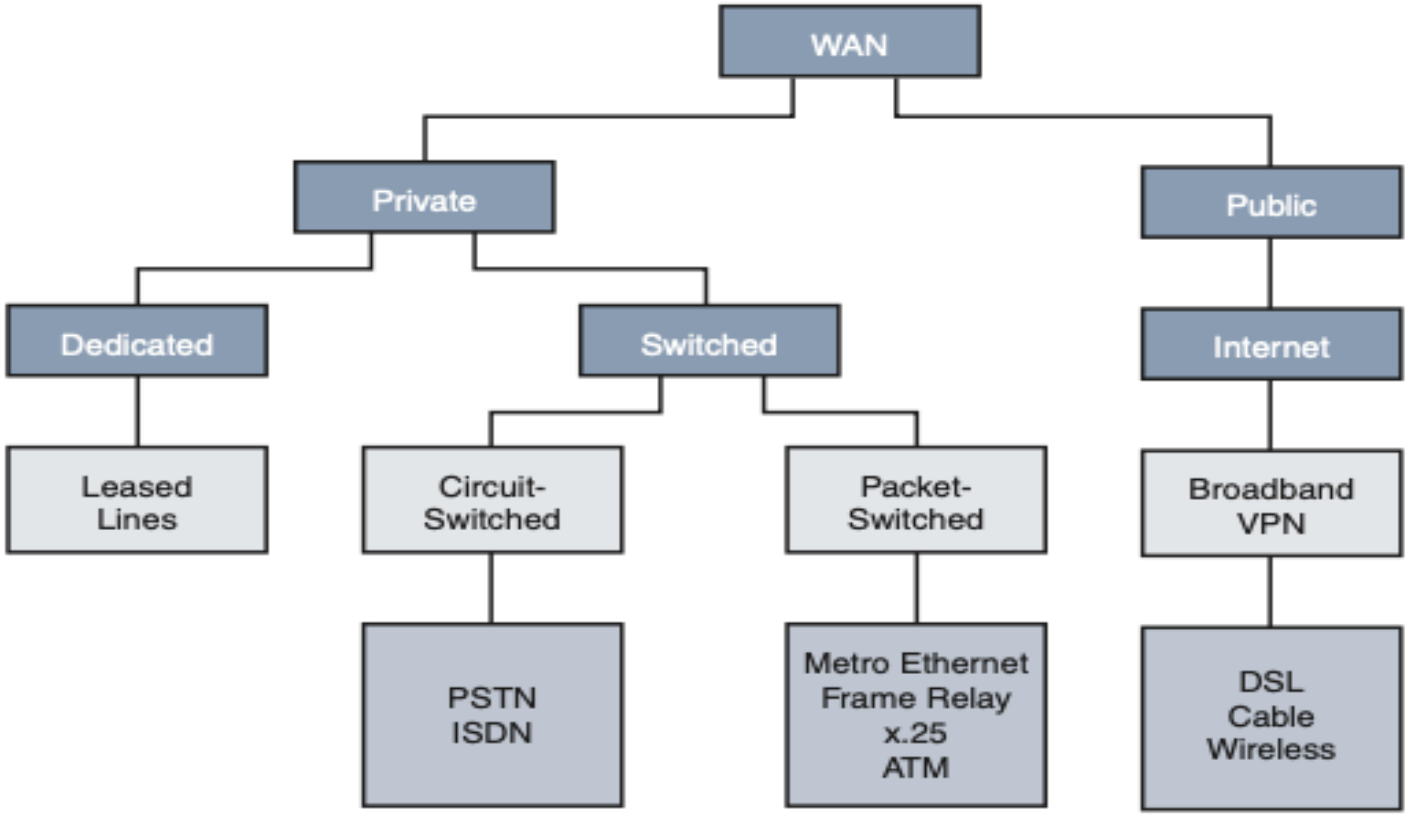
WAN Topology

Figure 7-1 WAN Topology Options



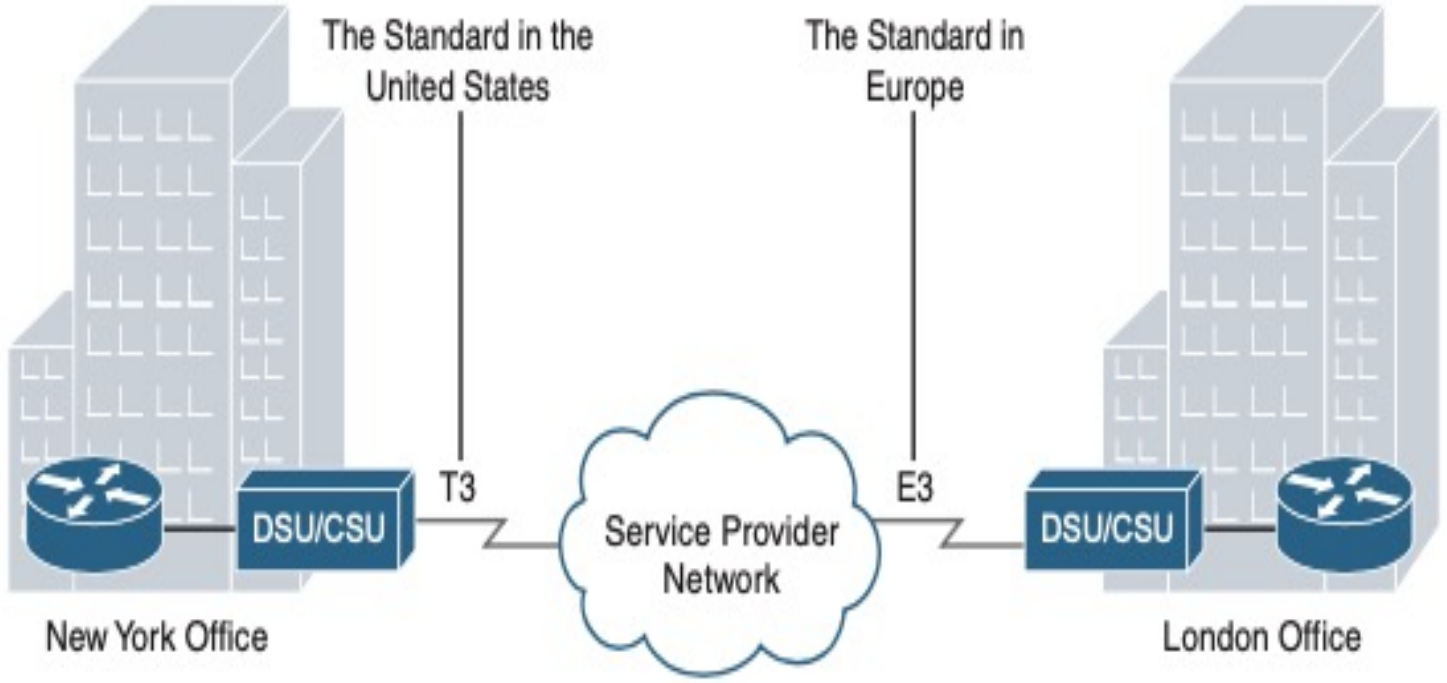
WAN Link Connections

Figure 7-2 WAN Link Connection Options



WAN Leased Line

Figure 7-3 Leased Lines



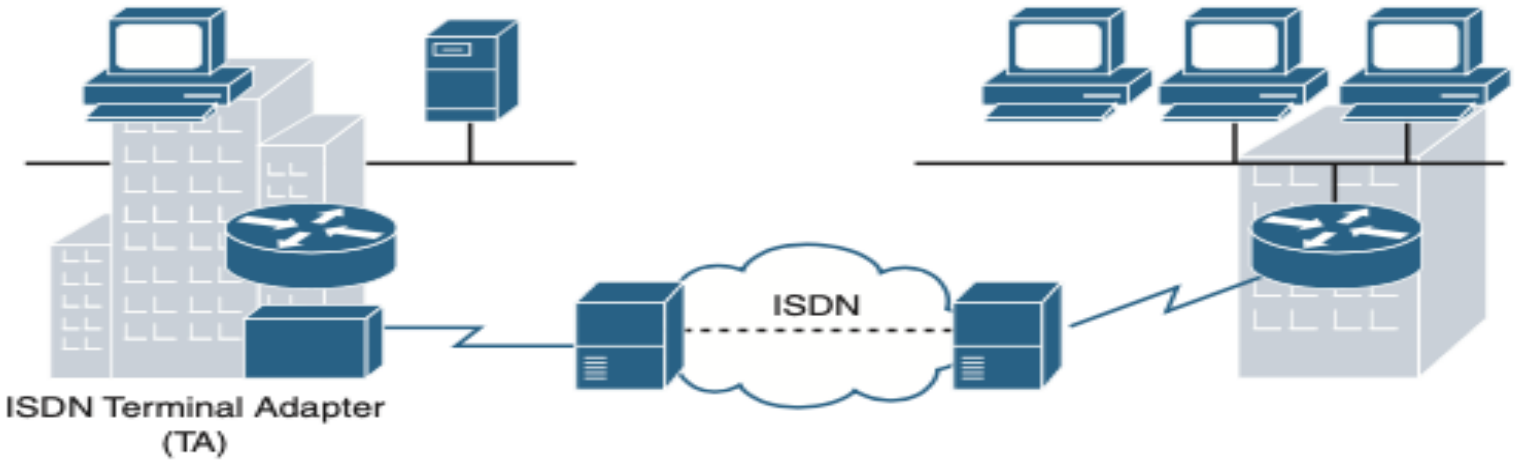
Leased Lines Type and Capacity

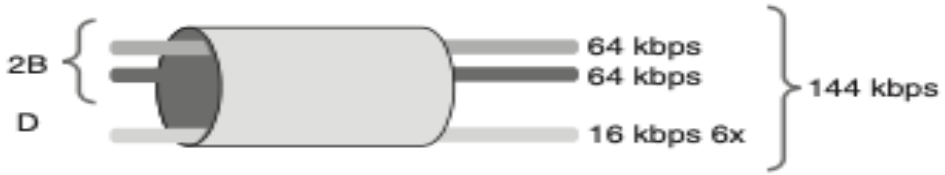
Table 7-1 Leased Line Types and Capacities

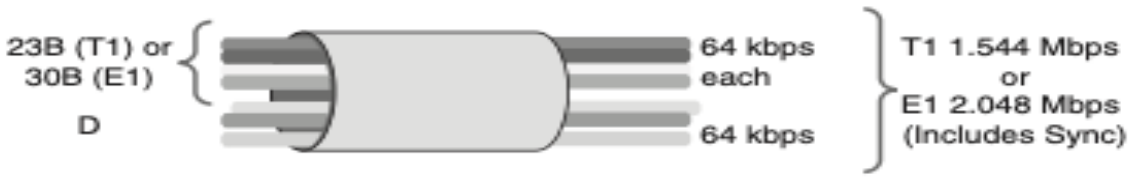
Line Type	Bit-Rate Capacity	Line Type	Bit-Rate Capacity
56k	56 kbps	OC-9	466.56 Mbps
64k	64 kbps	OC-12	622.08 Mbps
T1	1.544 Mbps	OC-18	933.12 Mbps
E1	2.048 Mbps	OC-24	1244.16 Mbps
J1	2.048 Mbps	OC-36	1866.24 Mbps
E3	34.064 Mbps	OC-48	2488.32 Mbps
T3	44.736 Mbps	OC-96	4976.64 Mbps
OC-1	51.84 Mbps	OC-192	9953.28 Mbps
OC-3	155.54 Mbps	OC-768	39,813.12 Mbps

ISDN Network

Figure 7-4 ISDN Network Infrastructure and PRI/BRI Line Capacity

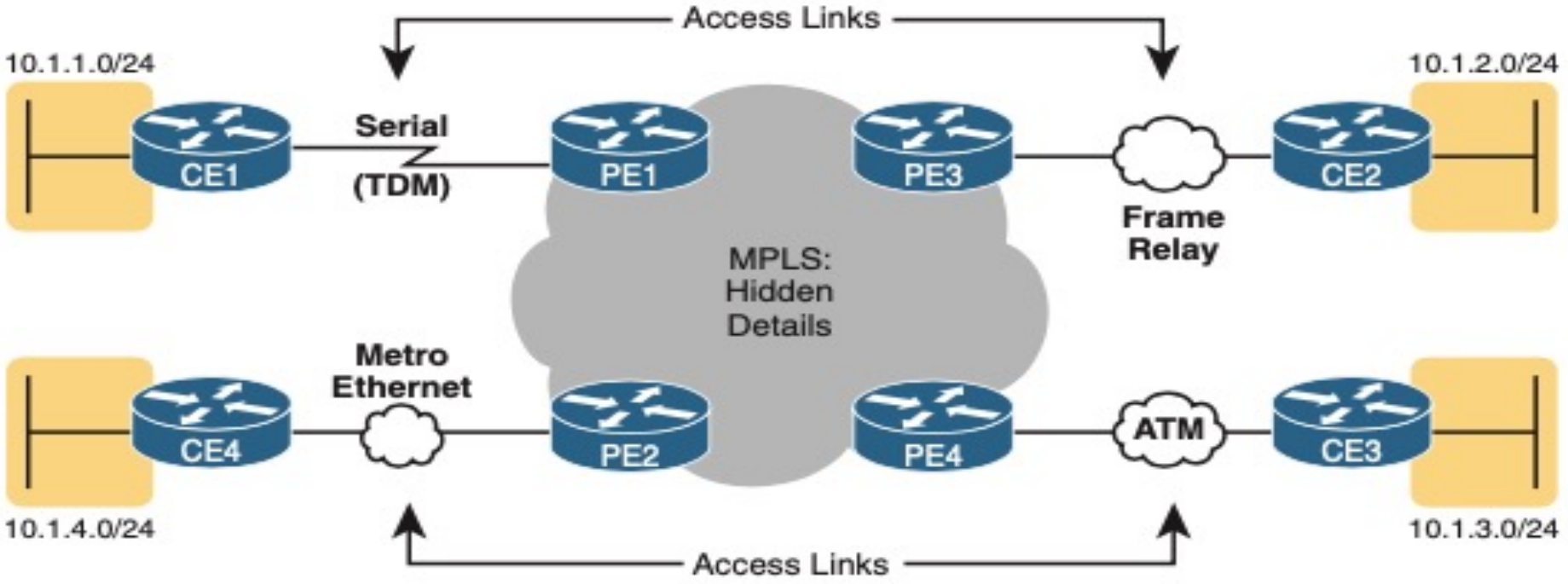






MPLS

Figure 7-5 Popular MPLS Connection Options

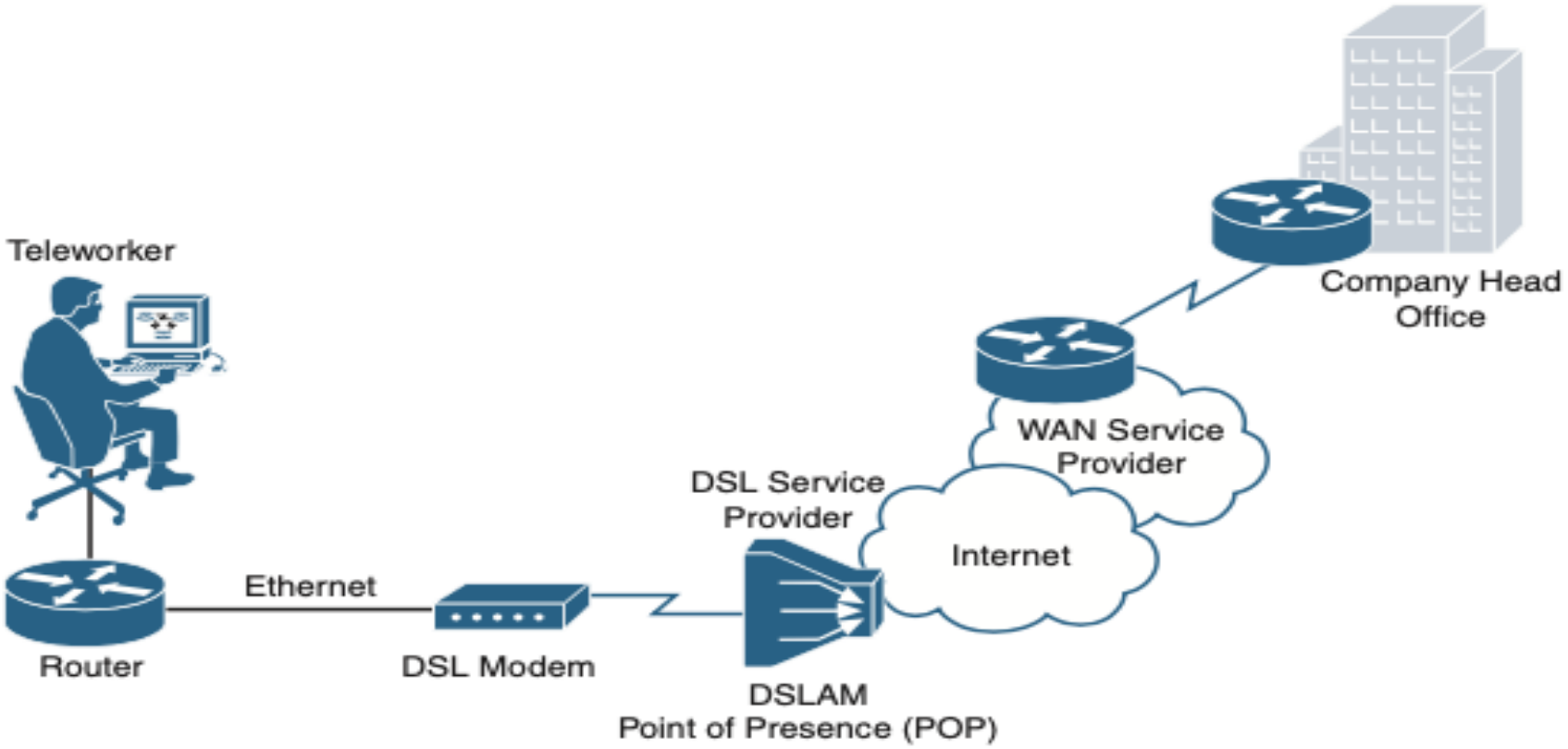


In Figure 7-5, CE refers to the customer edge routers. PE is the provider edge routers that add and remove labels.

NOTE: MPLS is primarily a service provider WAN technology.

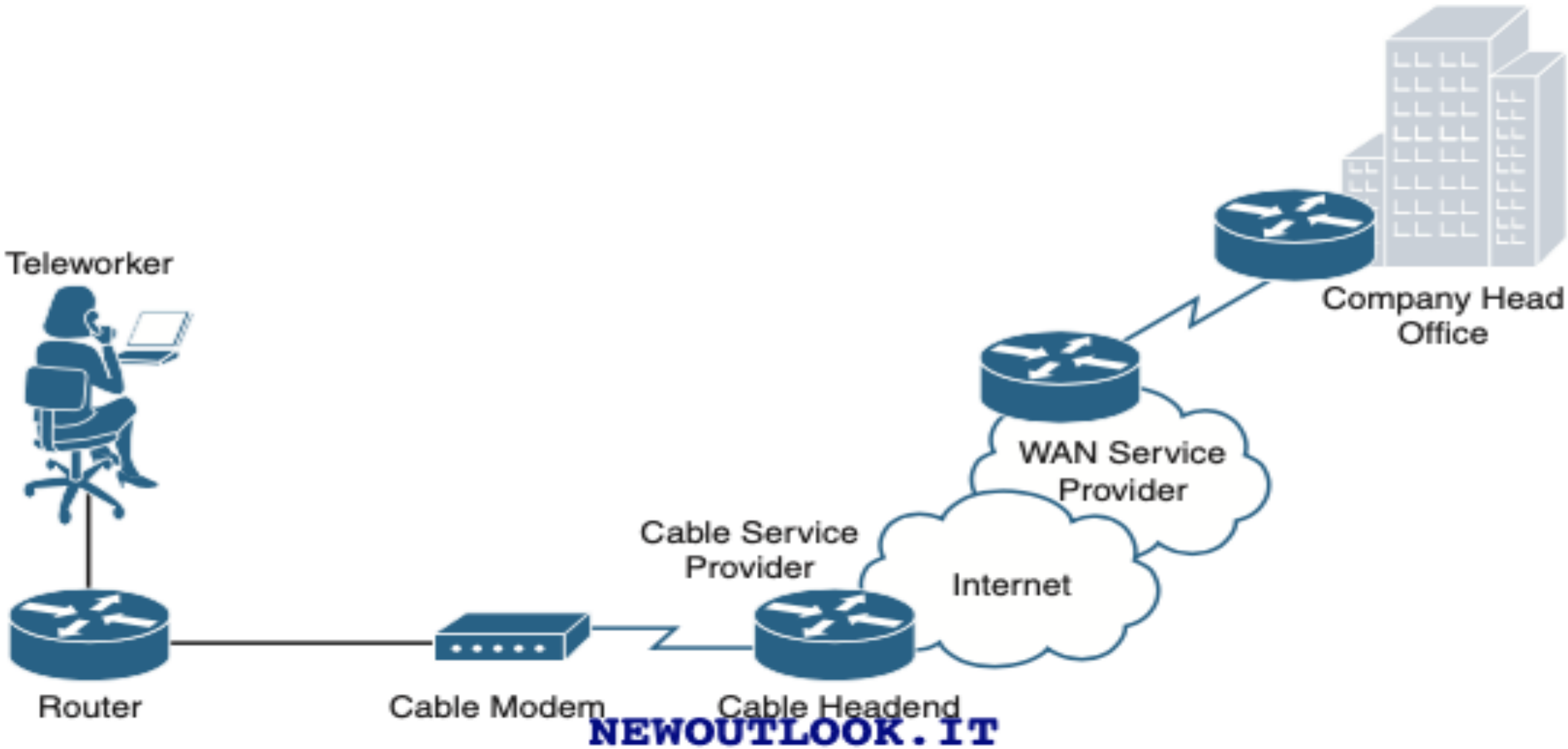
DSL

Figure 7-6 Teleworker DSL Connection



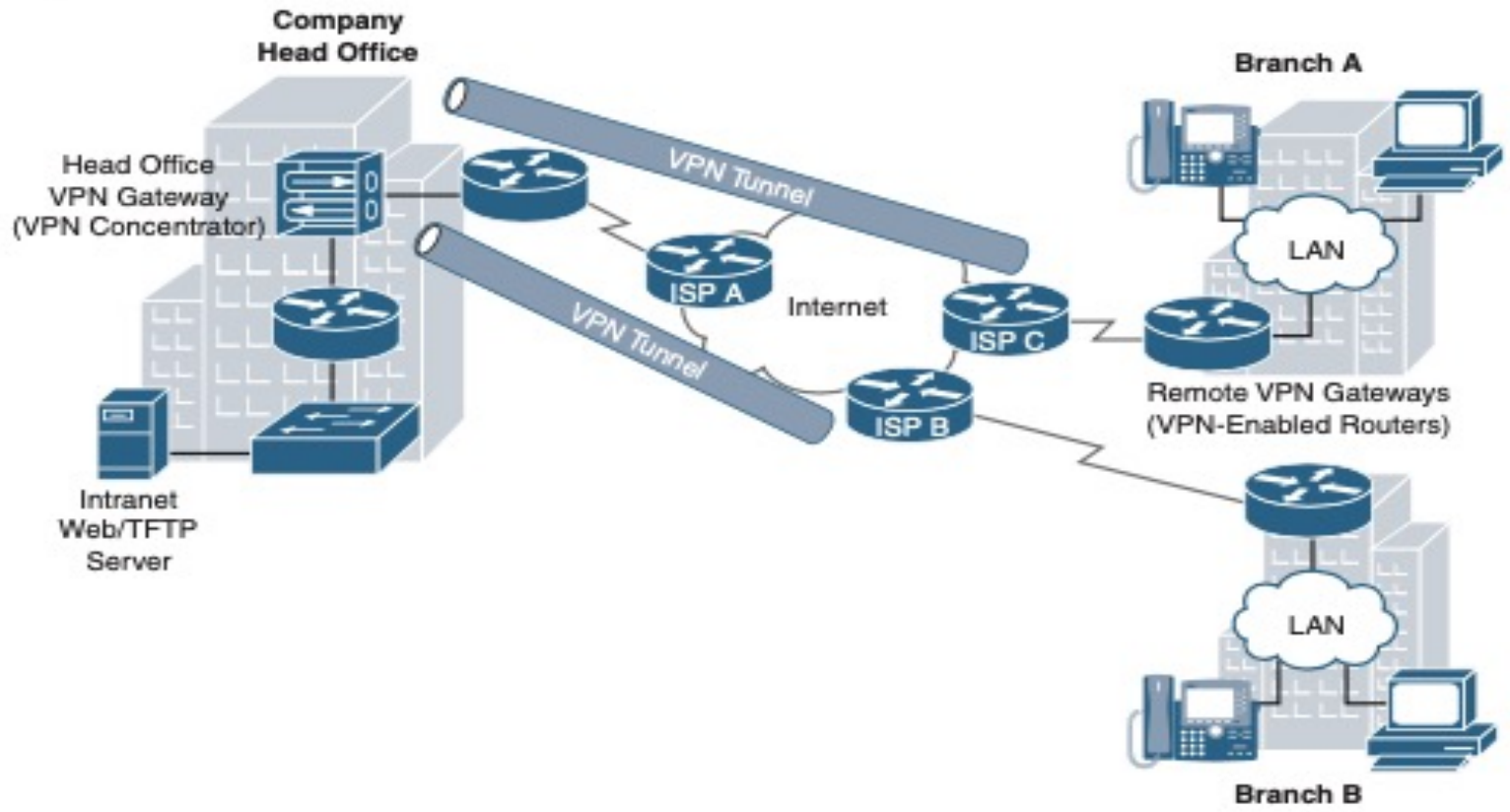
Cable Modem

Figure 7-7 Teleworker Cable Modem Connection

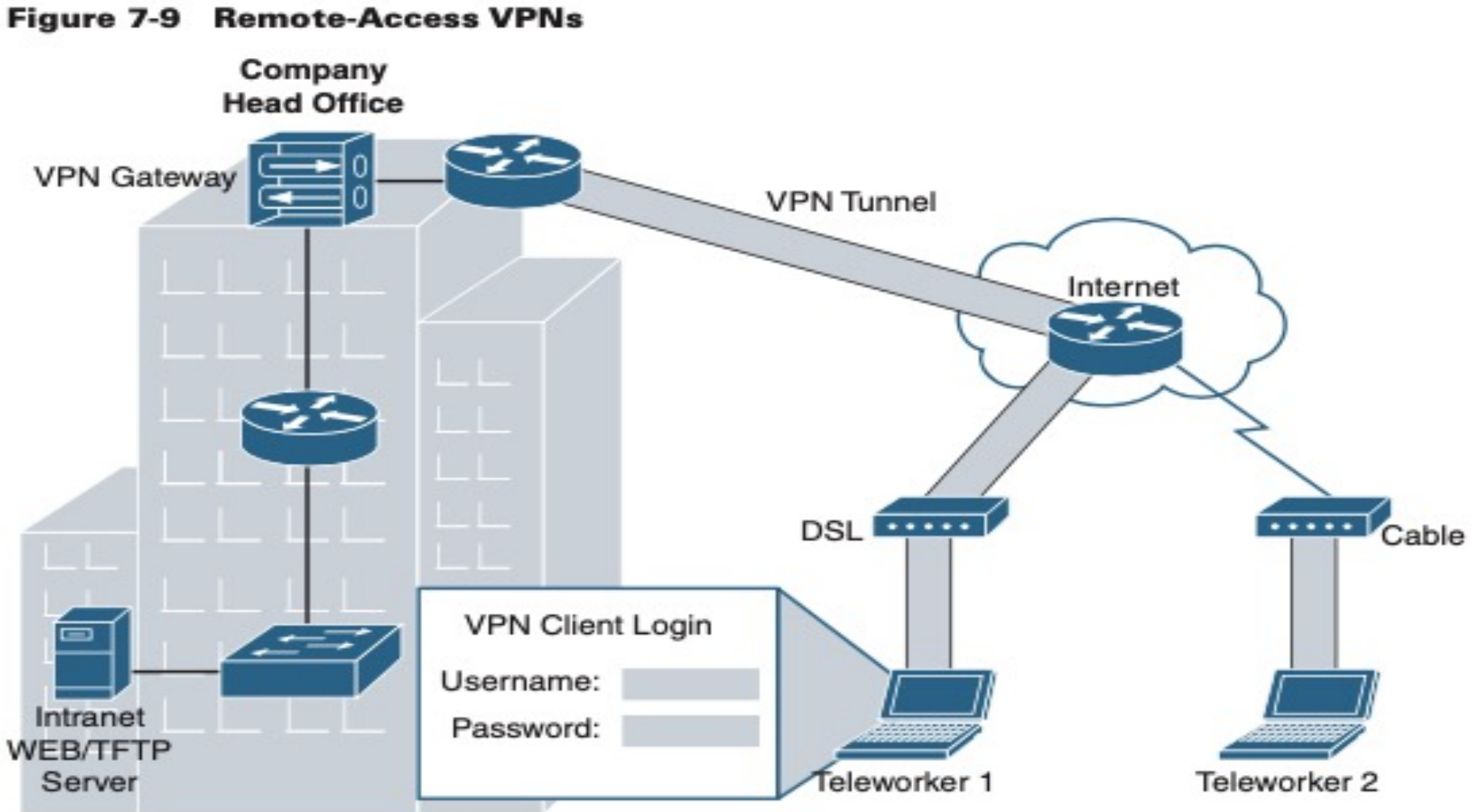


Site to Site VPN

Figure 7-8 Site-to-Site VPNs

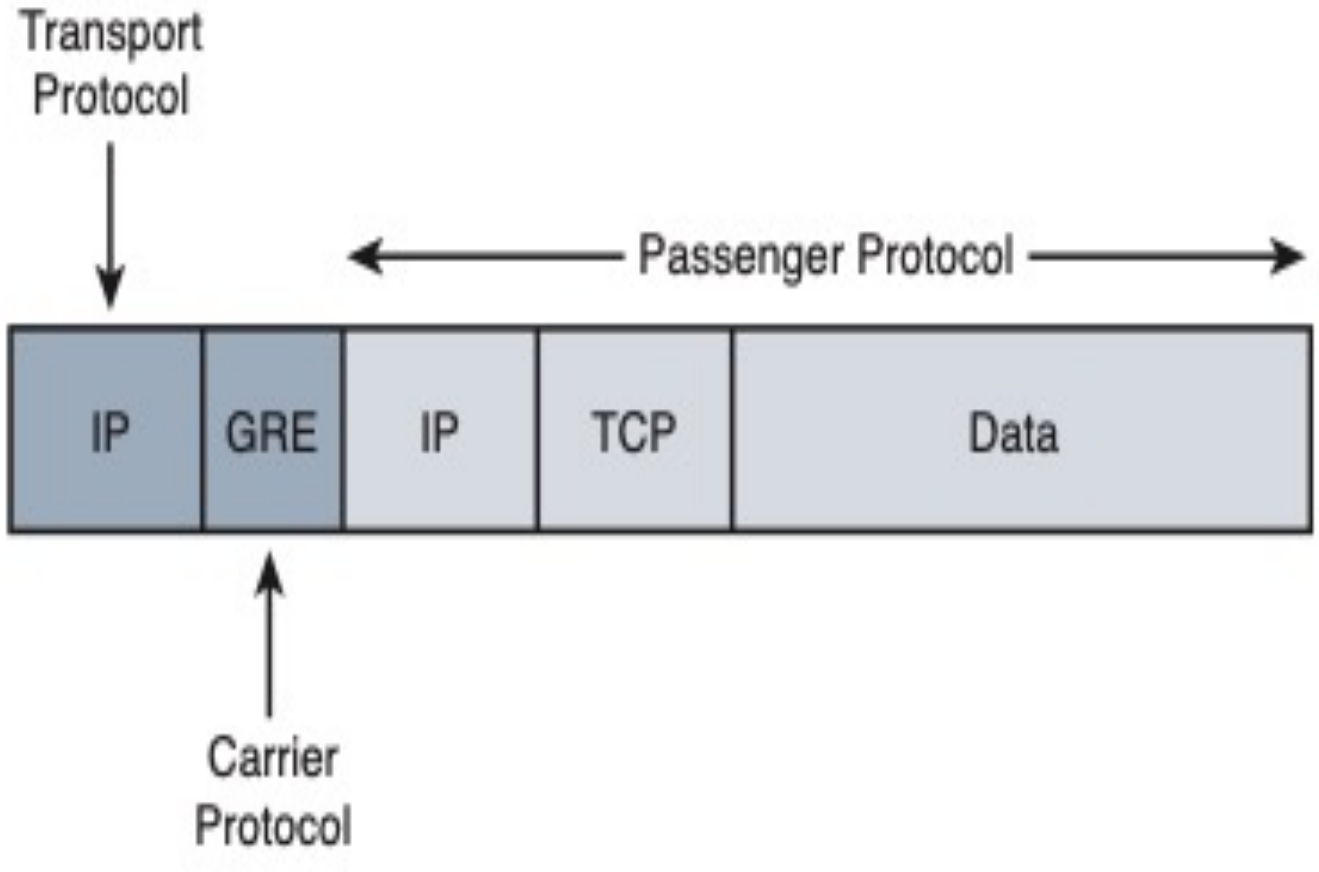


Remote Access VPN



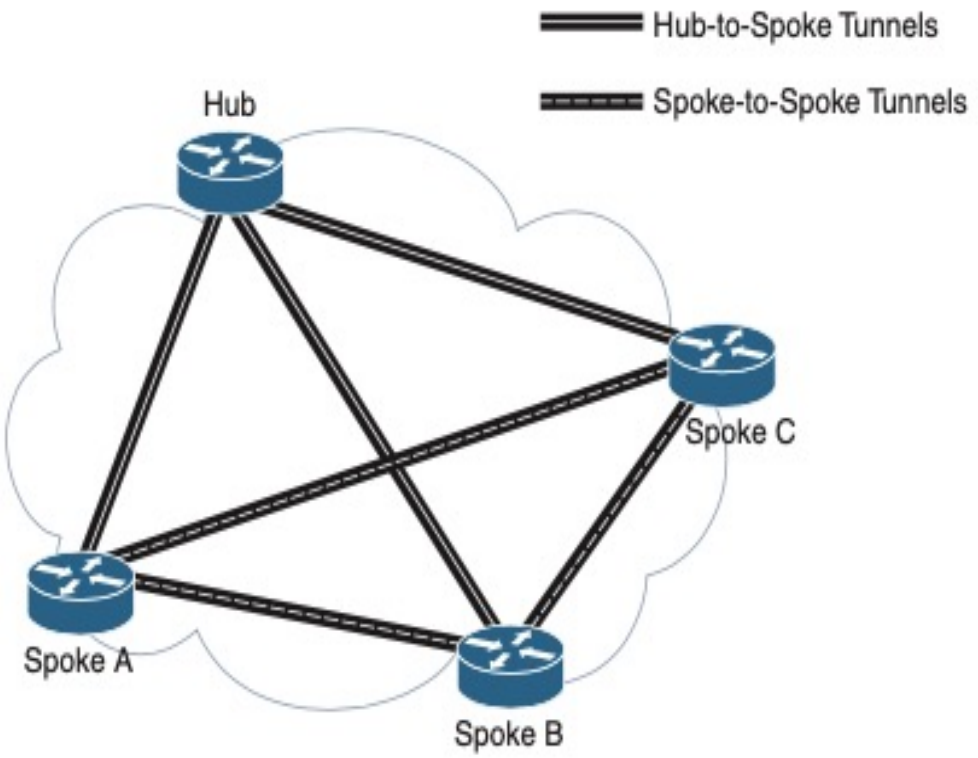
Transport Carrier and Passenger Protocol

Figure 7-10 Transport, Carrier, and Passenger Protocols



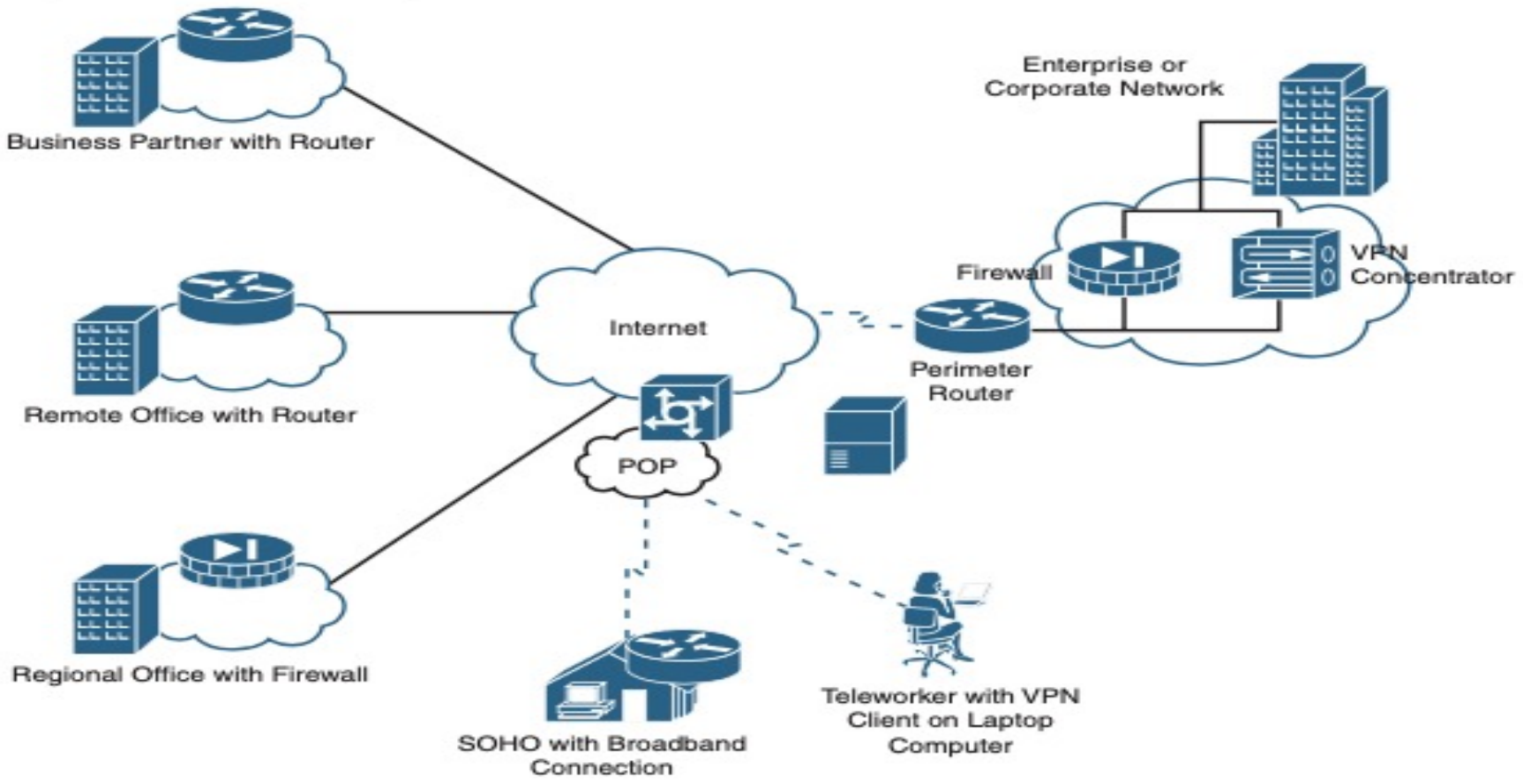
DMVPN Topology

Figure 7-11 DMVPN Sample Topology



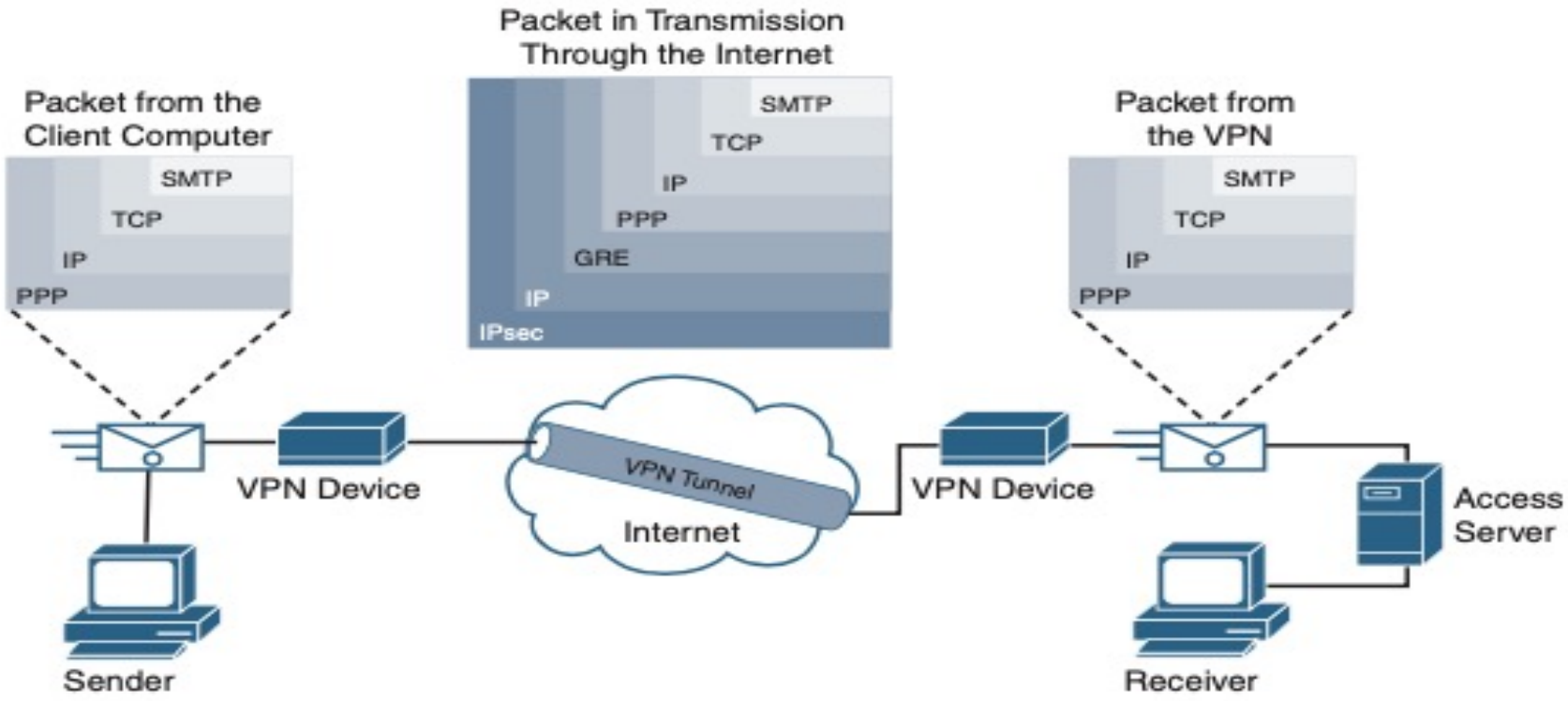
VPN Components

Figure 7-12 VPN Components



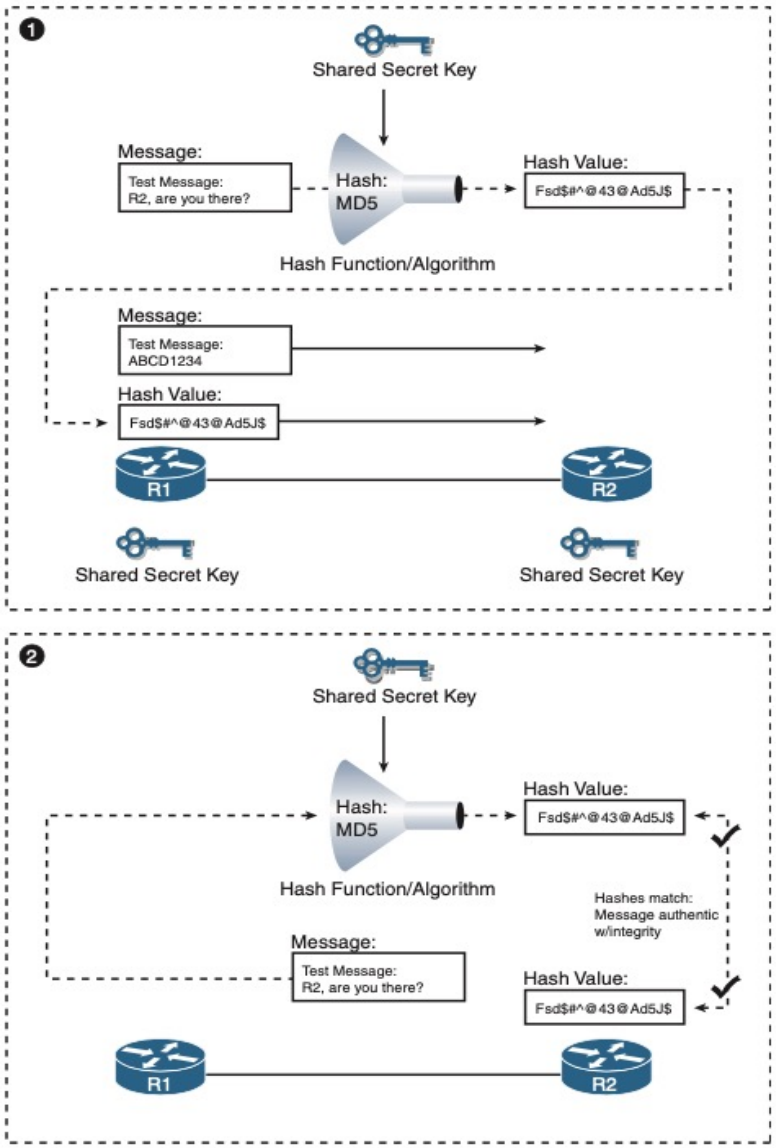
Packet Encapsulation in a VPN

Figure 7-13 Packet Encapsulation in a VPN Tunnel



Create and Verify Message Digest

Figure 7-14 Creating and Verifying a Message Digest



IPSEC and SSL Comparison for Remote Access

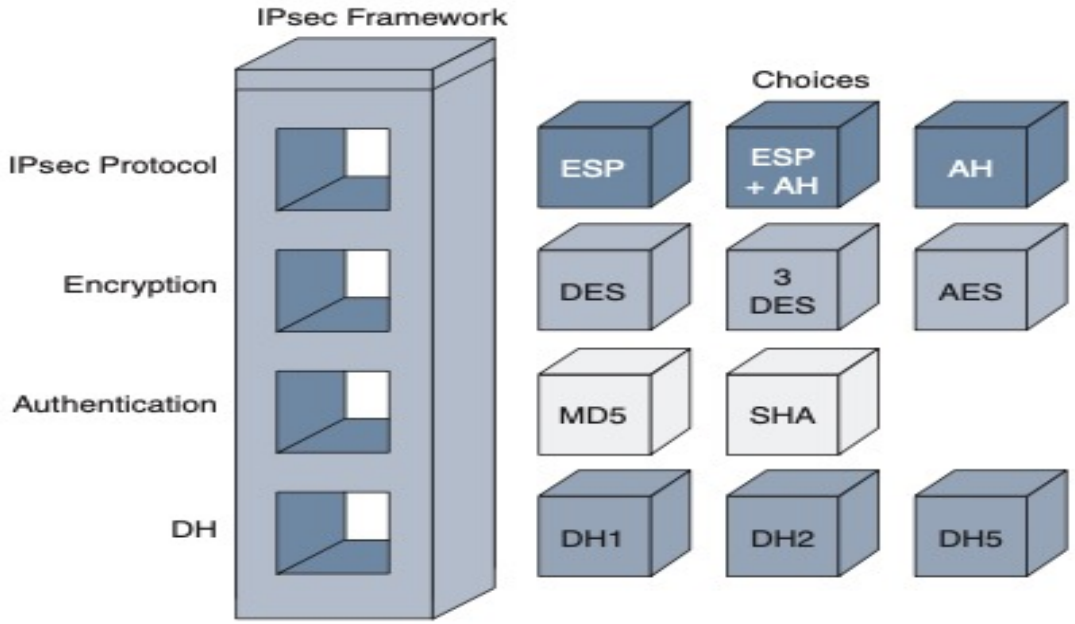
Table 7-3 IPsec and SSL for Remote Access

Feature	IPsec	SSL
Applications supported	Extensive—All IP-based applications are supported.	Limited—Only web-based applications and file sharing are supported.
Authentication strength	Strong—Uses two-way authentication with shared keys or digital certificates.	Moderate—Using one-way or two-way authentication.
Encryption strength	Strong—Uses key lengths from 56 bits to 256 bits.	Moderate to strong—With key lengths from 40 bits to 256 bits.
Connection complexity	Medium—Requires that a VPN client be pre-installed on a host.	Low—Requires a web browser only on a host.
Connection option	Limited—Only specific devices with specific configurations can connect.	Extensive—Any device with a web browser can connect.

IPSEC Framework

- Choose an IPsec protocol.
- Choose the encryption algorithm that is appropriate for the desired level of security.
- Choose an authentication algorithm to provide data integrity.
- The last square is the Diffie-Hellman (DH) algorithm group, which establishes the sharing of key information between peers. Choose which group to use: DH1, DH2, or DH5.

Figure 7-15 IPsec Framework



Choosing WAN Link Option

Choosing a WAN Link Option

Table 7–2 compares the advantages and disadvantages of the various WAN connection options reviewed.

Table 7-2 Choosing a WAN Link Connection

Option	Description	Advantages	Disadvantages	Sample Protocols
Leased line	Point-to-point connection between two LANs.	Most secure	Expensive	PPP, HDLC, SDLC
Circuit switching	Dedicated circuit path created between endpoints. The best example is dialup connections.	Inexpensive	Call setup	PPP, ISDN
Packet switching	Devices transporting packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable-length packets are transmitted over PVCs or SVCs.	Highly efficient use of bandwidth	Shared media across link	Frame Relay, MetroE
Internet	Connectionless packet switching using the Internet as the WAN infrastructure. Uses network addressing to deliver packets. Because of security issues, VPN technology must be used.	Least expensive, globally available	Least secure	DSL, cable modem, wireless

- MPLS label use MPLS label to decide where to send the router
- when forming LAYER 3 VPN in MPLS a routing protocol can be used or a static route can be set between the CE and PE
- When using LAYER 2 VPN the connection will be transparent to the customer
- IPSEC does not support broadcast or Multicast
- GRE creates tunnel like IPSEC but it does not encrypt the original packet so its not secured but it encapsulated broadcast and multicast
- DMVPN is a cisco develop product that allows you to create a full mesh VPN
- remote to site VPN use TLS
- VPN Client software like cisco anyconnect are installed on end devices then the end devices create a tunnel to the remote device

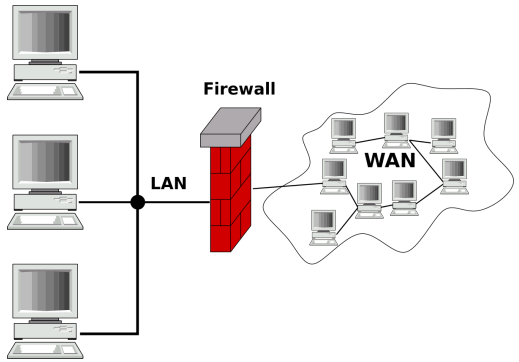
Metro Ethernet

Metro Ethernet Access

Name	Speed	Distance
100BASE-LX10	100 Mbps	10 Km

Technet24

Ethernet Line Service	E-Line	Point-to-point	Two customer premise equipment (CPE) devices can exchange Ethernet frames, similar in concept to a leased line.
Ethernet LAN Service	E-LAN	Full mesh	This service acts like a LAN, in that all devices can send frames to all other devices.
Ethernet Tree Service	E-Tree	Hub and spoke; partial mesh; point-to-multipoint	A central site can communicate to a defined set of remote sites, but the remote sites cannot communicate directly.



Firewalls

- Firewalls forward traffic based on rules it controls what enters into the network or goes out

Firewalls Types

Topic

- **Traditional firewall:** An NGFW performs traditional firewall features, like stateful firewall filtering, NAT/PAT, and VPN termination.
- **Application Visibility and Control (AVC):** This feature looks deep into the application layer data to identify the application. For instance, it can identify the application based on the data, rather than port number, to defend against attacks that use random port numbers.
- **Advanced Malware Protection:** NGFW platforms run multiple security services, not just as a platform to run a separate service, but for better integration of functions. A network-based antimalware function can run on the firewall itself, blocking file transfers that would install malware, and saving copies of files for later analysis.
- **URL Filtering:** This feature examines the URLs in each web request, categorizes the URLs, and either filters or rate limits the traffic based on rules. The Cisco Talos security group monitors and creates reputation scores for each domain known in the Internet, with URL filtering being able to use those scores in its decision to categorize, filter, or rate limit.
- **NGIPS:** The Cisco NGFW products can also run their NGIPS feature along with the firewall.

- **Traditional IPS:** An NGIPS performs traditional IPS features, like using exploit signatures to compare packet flows, creating a log of events, and possibly discarding and/or redirecting packets.
- **Application Visibility and Control (AVC):** As with NGFWs, an NGIPS has the ability to look deep into the application layer data to identify the application.
- **Contextual Awareness:** NGFW platforms gather data from hosts —OS, software version/level, patches applied, applications running, open ports, applications currently sending data, and so on. Those facts inform the NGIPS as to the often more limited vulnerabilities in a portion of the network so that the NGIPS can focus on actual vulnerabilities while greatly reducing the number of logged events.
- **Reputation-Based Filtering:** The Cisco Talos security intelligence group researches security threats daily, building the data used by the Cisco security portfolio. Part of that data identifies known bad actors, based on IP address, domain, name, or even specific URL, with a reputation score for each. A Cisco NGIPS can perform reputation-based filtering, taking the scores into account.
- **Event Impact Level:** Security personnel need to assess the logged events, so an NGIPS provides an assessment based on impact levels, with characterizations as to the impact if an event is indeed some kind of attack.

Cabling

- Straight Through Crossover ethernet cables
- Crossover cable is used to connect switch to switch and router to Router
- Straight Through Cable is used to connect PC to a switch or Router
- Copper UTP Cable can be used up to 100 meter
- Standards for Fiber Cable 100 base lx speed 1gbs multimode or single mode up 550 km standard 802.3z

- 10gbase -SR 10GBS MULTIMODE 400 KM standard 802.ae
- 10GBASE-LR 10GBS SINGLE MODE 10KM standard 802.ae
- 10BASE-ER 10GBS SINGLE MODE 30 KM standard 802.ae
- Crossover cable is used to connect switch to switch and router to Router
- Straight Through Cable is used to connect the PC to a switch or Router
- Copper UTP Cable can be used up to 100 meter
- 10 base t is 10 m 100 base t is 100 meter 1000 base t is 100 meter 10 g base t 100 meter
- 10 base T fast ethernet cable use 2 pair of cable or only 4 fair pair pin position at 1 and 2 switches receive data in PIN and 1 and 2

- on the switch pin 3 and 6 is used to transmit data on the PC 3 and 6 is used to receive Data
- on a router transmit data on pin 1 and 2 and receive in 3 and 6

Table 2-4 A Sampling of IEEE 802.3 10-Gbps Fiber Standards

Standard	Cable Type	Max Distance*
10GBASE-S	MM	400m
10GBASE-LX4	MM	300m
10GBASE-LR	SM	10km
10GBASE-E	SM	30km

* The maximum distances are based on the IEEE standards with no repeaters

Key Topic

Table 2-2 Examples of Types of Ethernet

Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

Cabling Comparison

Key Topic

Table 2-5 Comparisons Between UTP, MM, and SM Ethernet Cabling

Criteria	UTP	Multimode	Single-Mode
Relative Cost of Cabling	Low	Medium	Medium
Relative Cost of a Switch Port	Low	Medium	High
Approximate Max Distance	100m	500m	40km
Relative Susceptibility to Interference	Some	None	None
Relative Risk of Copying from Cable Emissions	Some	None	None

Types of Ethernet

Table 30-1 Today's Most Common Types of Ethernet

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10 Mbps	10BASE-T	802.3	Copper, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	802.3u	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-LX	802.3z	Fiber, 550 m
Gigabit Ethernet	1000 Mbps	1000BASE-T	802.3ab	Copper, 100 m
10GigE (Gigabit Ethernet)	10 Gbps	10GBASE-T	802.3an	Copper, 100 m
10GigE (Gigabit Ethernet)	10 Gbps	10GBASE-S	802.3ae	Fiber, 400 m

Devices that Transmit in different Pin Pairs

Table 30-2 10BASE-T and 100BASE-TX Pin Pairs Used

Devices That Transmit on 1,2 and Receive on 3,6	Devices That Transmit on 3,6 and Receive on 1,2
PC NICs	Hubs
Routers	Switches
Wireless access points (Ethernet interfaces)	—
Networked printers (printers that connect directly to the LAN)	—

Ethernet Frames

Figure 30-7 Ethernet Frame Formats

DIX

Preamble 8	Destination 6	Source 6	**Type** 2	Data and Pad 46 – 1500	FCS 4

IEEE 802.3 (Original)

Preamble 7	**SFD** 1	Destination 6	Source 6	**Length** 2	Data and Pad 46 – 1500	FCS 4

IEEE 802.3 (Revised 1997)

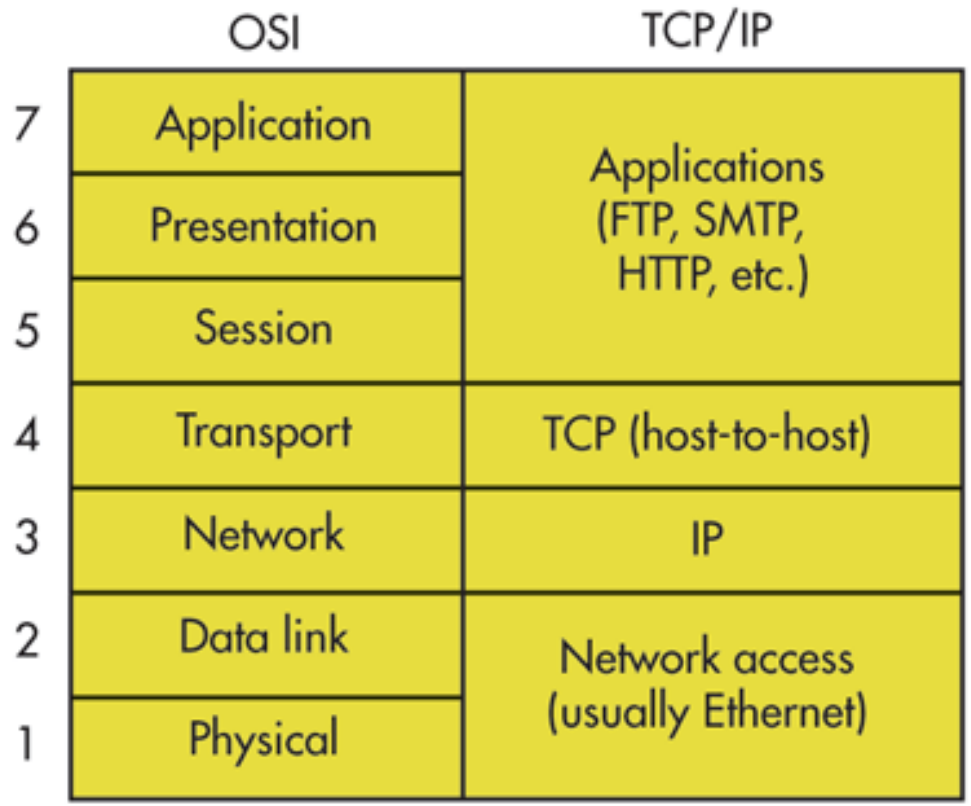
Bytes	**Preamble** 7	**SFD** 1	Destination 6	Source 6	**Length/ Type 2**	Data and Pad 46 – 1500	FCS 4

Ethernet Field Description

Table 30-3 IEEE 802.3 Ethernet Field Descriptions

Field	Field Length, in Bytes	Description
Preamble	7	Synchronization
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC field
Destination MAC Address	6	Identifies the intended recipient of this frame
Source MAC Address	6	Identifies the sender of this frame
Length	2	Defines the length of the data field of the frame (either length or type is present, but not both)
Type	2	Defines the type of protocol listed inside the frame (either length or type is present, but not both)
Data and Pad	46–1500	Holds data from a higher layer, typically a Layer 3 PDU (generic) and often an IP packet
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine whether the frame experienced transmission errors

OSI


OSI
TCP/IP
7
Application
6
Presentation
5
Session
Applications
(FTP, SMTP,
HTTP, etc.)
4
Transport
TCP (host-to-host)
3
Network
IP
2
Data link
1
Physical
Network access
(usually Ethernet)

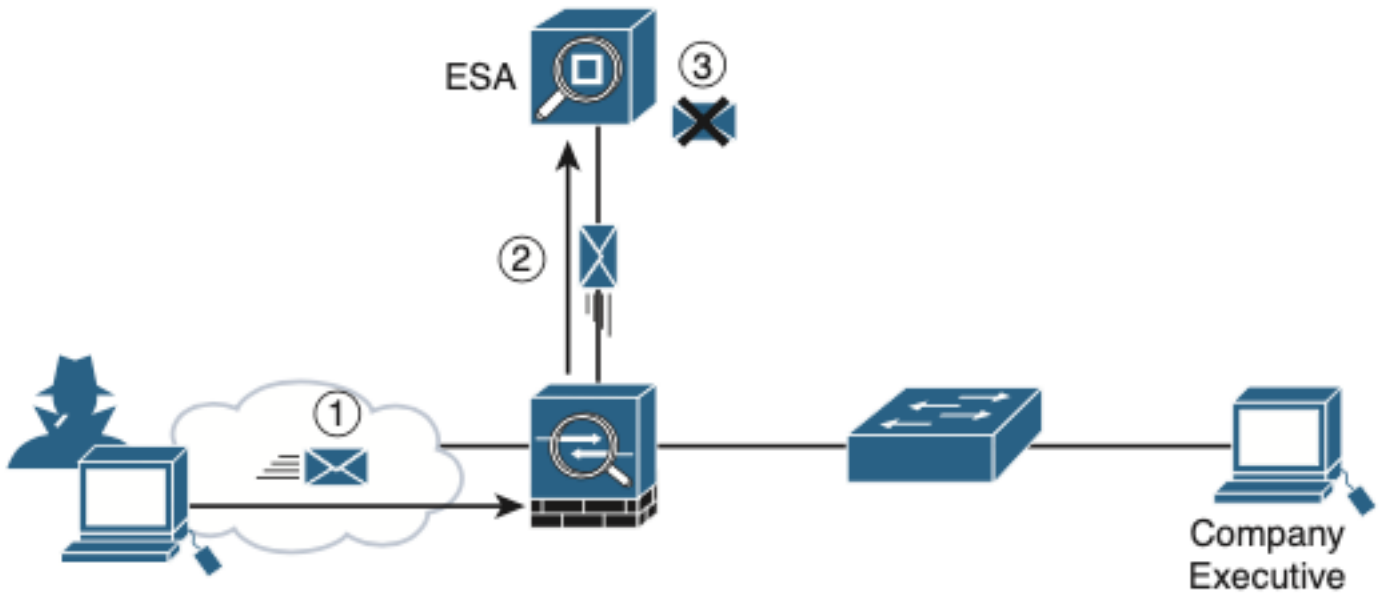
TCP/IP Architectural and Protocol

Table 1-2 TCP/IP Architectural Model and Example Protocols

TCP/IP Architecture Layer	Example Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Internet	IP, ICMP
Data Link & Physical	Ethernet, 802.11 (Wi-Fi)

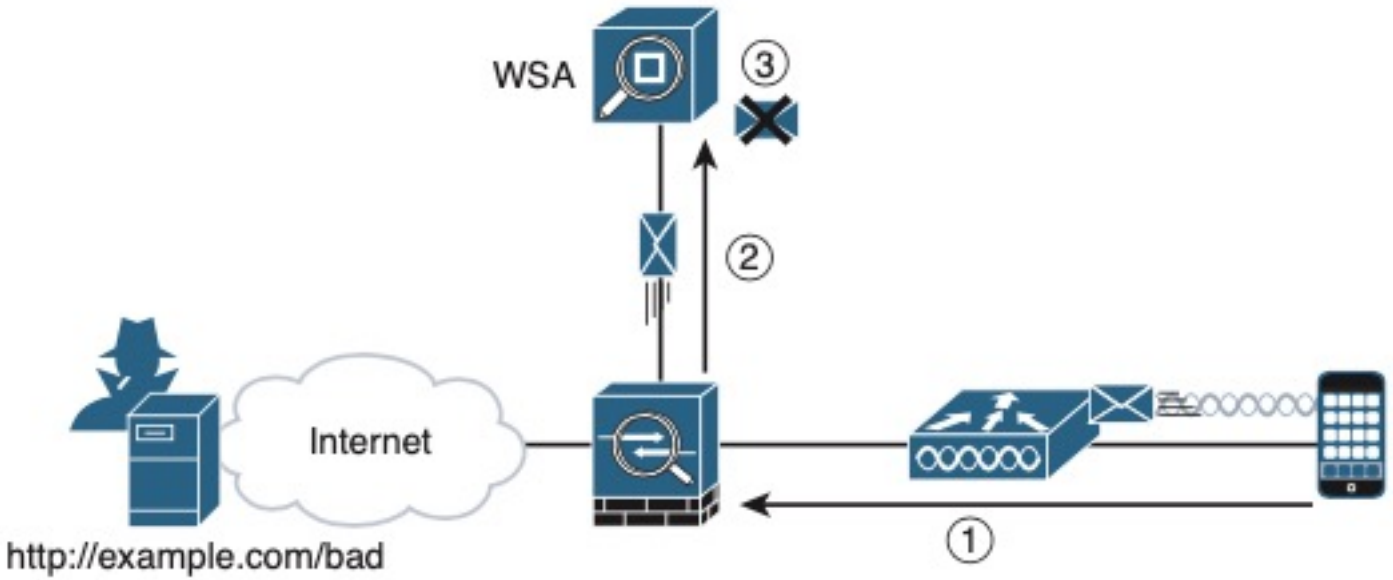
Security Cisco ESA Discard Emails

Figure 20-1 Cisco ESA Discards Bad Emails



Cisco WSA

Figure 20-2 Cisco WSA Discard Packet Destined for a Blacklisted Site



Local Password Only Authentication

Example 20-1 Local Password Only Authentication

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

Local Username and Password Authentication

Example 20-2 Local Username/Password Authentication

```
R1(config)# username allanj secret 31daysCCNA
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# no password
R1(config-line)# line vty 0 15
R1(config-line)# login local
R1(config-line)# no password
```

```
S1# telnet 10.10.10.1
```



```
Trying 10.10.10.1 ...Open


User Access Verification

Username: allanj
Password:
R1> enable
Password:
R1# show run | include username
username allanj secret 5 $1$mERr$e/edsAr7D0CyM/z3tMvyL/
R1#
```

Remote SSH Configuration

Example 20-3 Configuring SSH Remote Access on a Switch

```
S1# show ip ssh
SSH Disabled-version 1.99
%Please create RSA keys to enable SSH (of at least 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries:3
S1# conf t
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
   General Purpose Keys. Choosing a key modulus greater than 512 may take
   a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)
```



```
*Mar 1 02:20:18.529: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# username allanj secret 31daysCCNA
!The following commands are optional SSH configurations.
S1(config)# ip ssh version2
S1(config)# ip ssh authentication-retries 5
S1(config)# ip ssh time-out 60
S1(config)# end
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 5
S1#
```

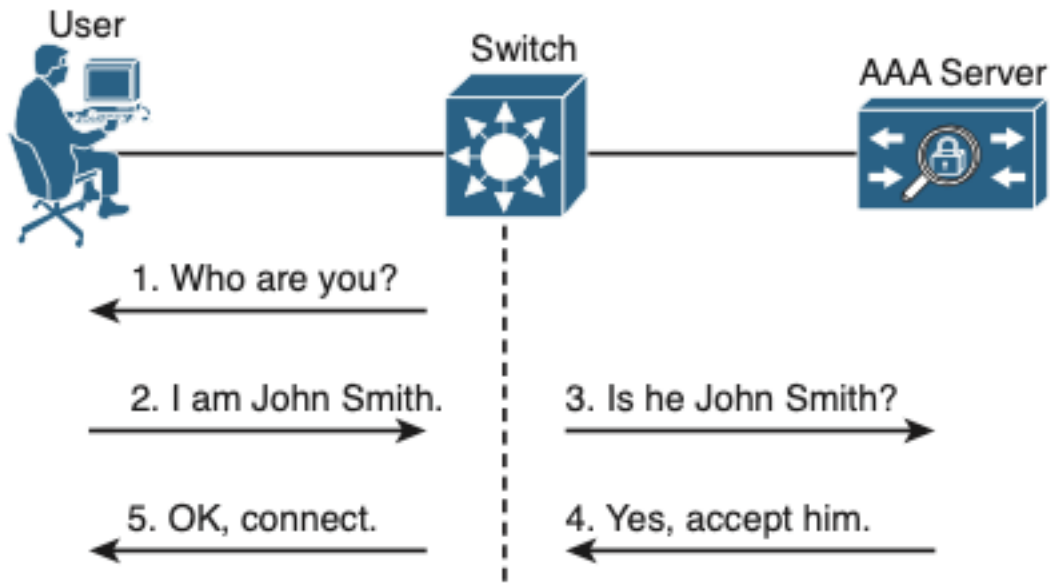
Comparison Between TACAS+ and Radius

Table 20-1 Comparison of TACACS+ and RADIUS

Feature	TACACS+	RADIUS
Most often used for	Network devices	Users
Transport protocol	TCP	UDP
Authentication port number(s)	49	1645, 1812
Protocol encrypts the password	Yes	Yes
Protocol encrypts entire packet	Yes	No
Supports function to authorize each user to a subset of CLI commands	Yes	No
Defined by	Cisco	RFC 2865

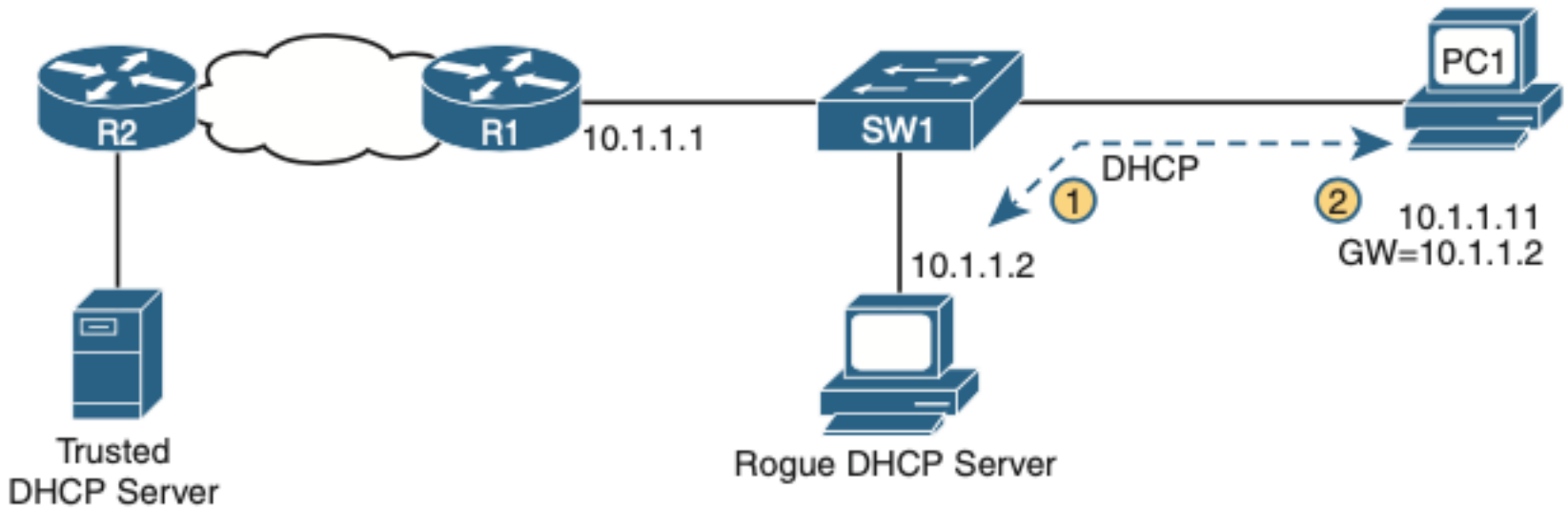
Simplified View of a AAA Server

Figure 20-3 A Simplified View of AAA



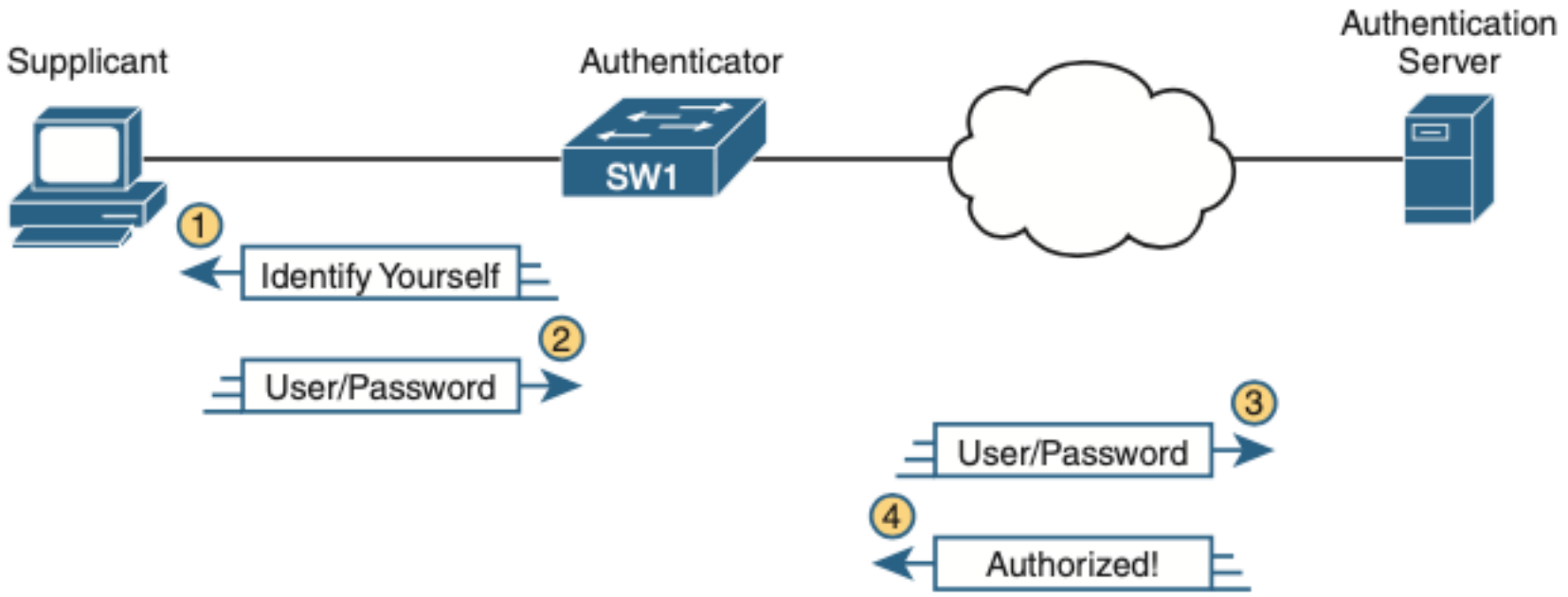
802.1x Role

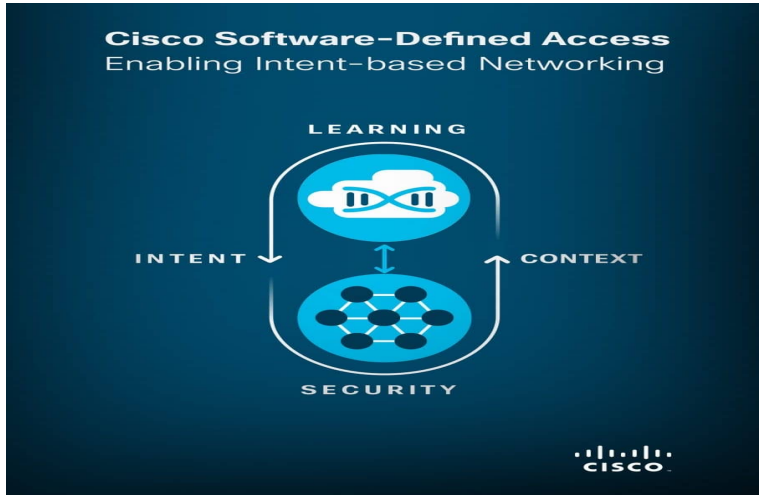
Figure 20-4 802.1X Roles



802.1x Authentication Flow

Figure 20-5 802.1X Authentication Flows



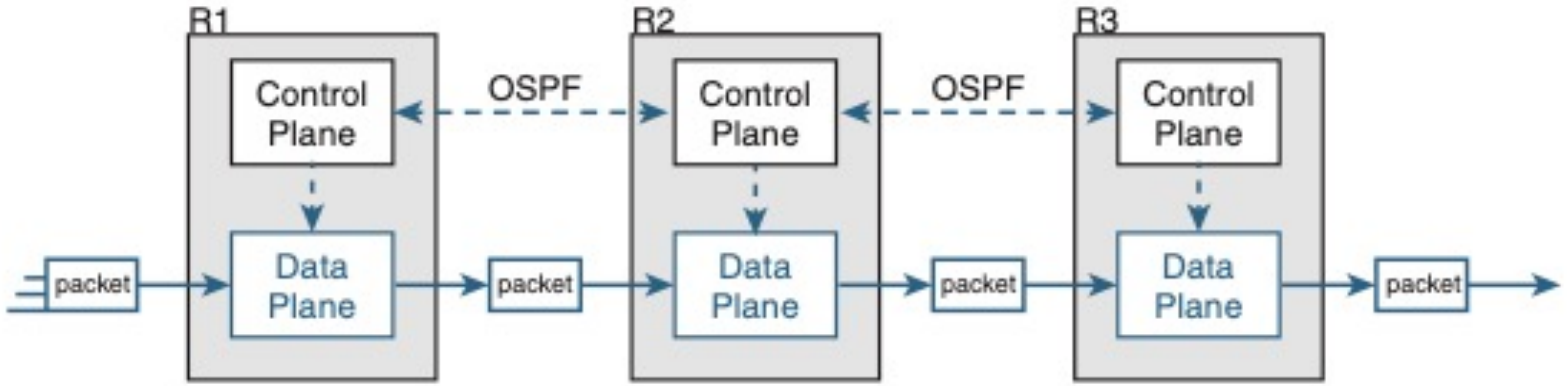


Automation and Programmability

- XML YANG YAML
- HTTPS uses CRUD API and HTTP uses Rest API as the communication protocol
- SDN is a approach to network that centralized the control plane in a controller
- Data serialization is the process of storing data in a file

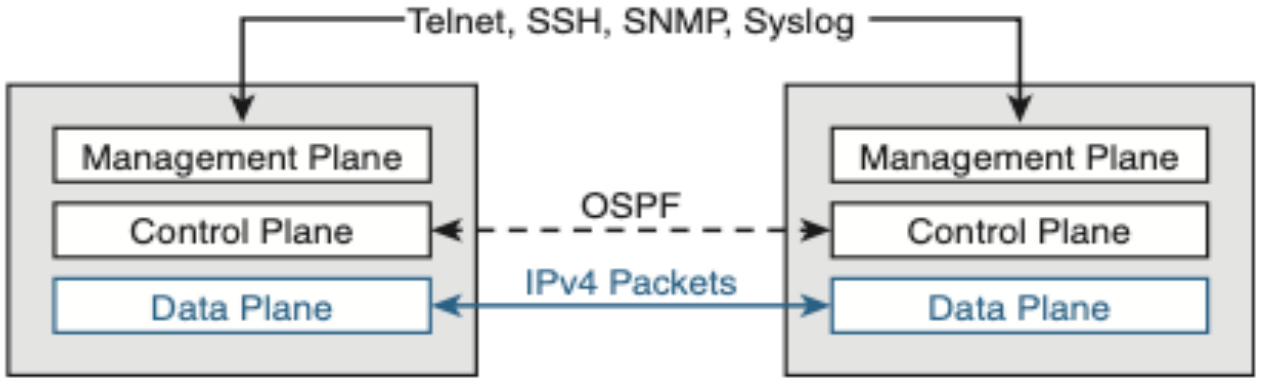
Control and Data Plane

Figure 3-6 Control and Data Plane Example



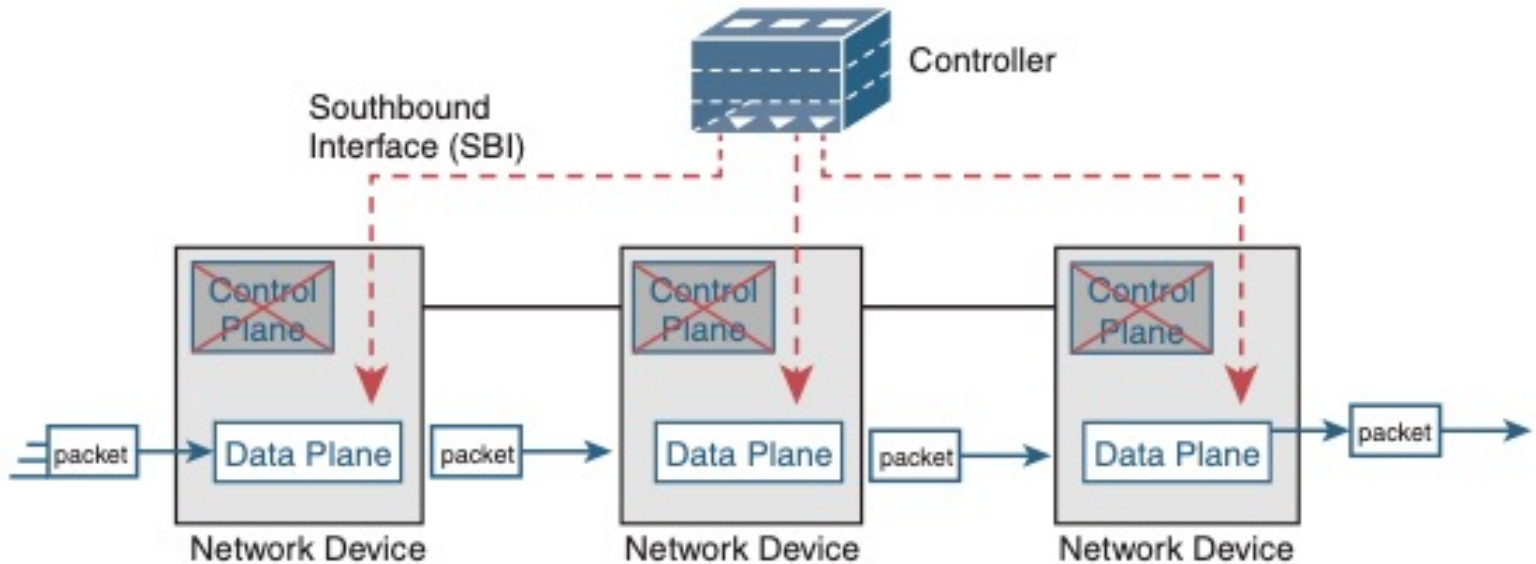
Management Plane

Figure 3-7 Management Plane Example



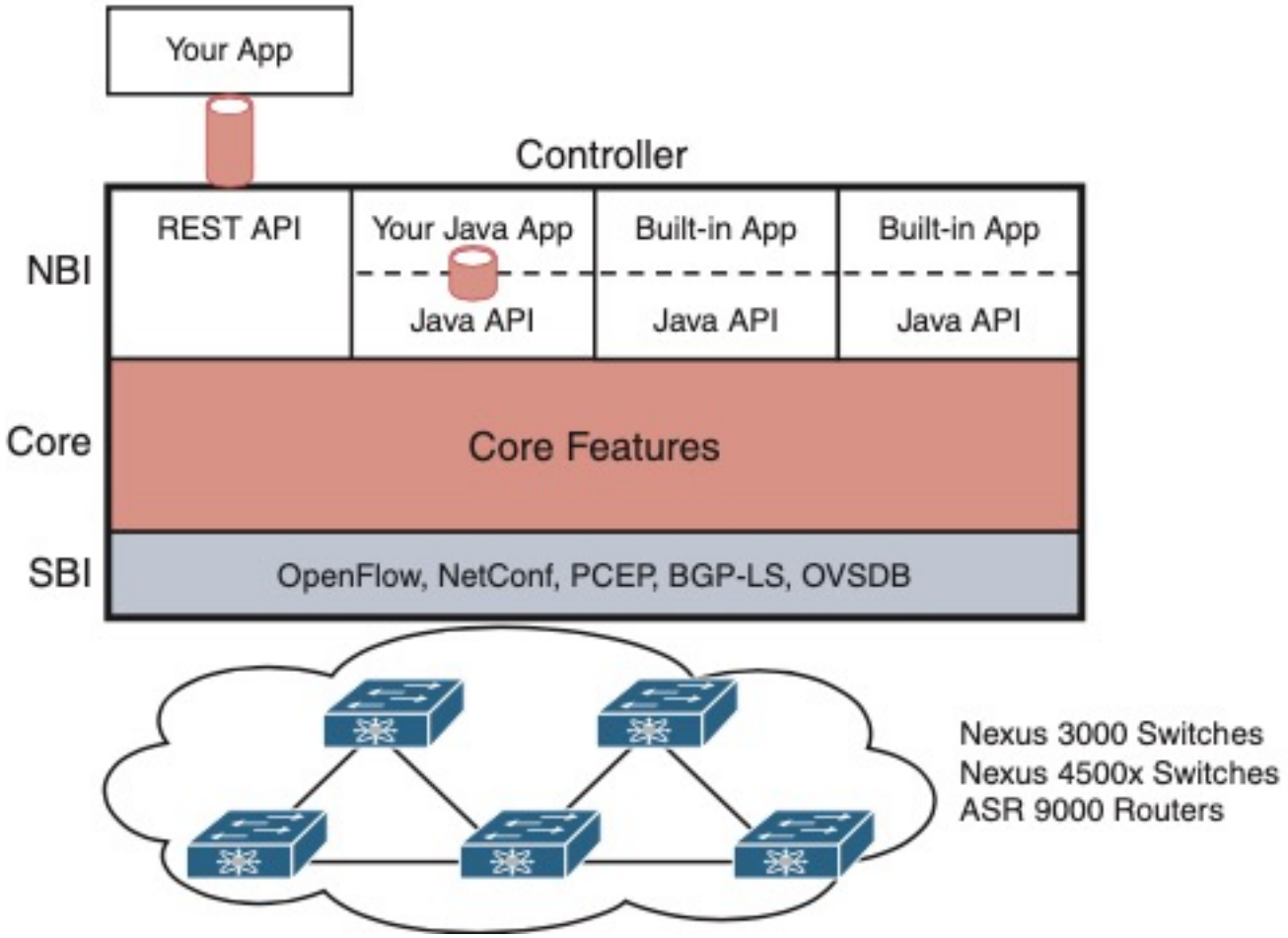
Centralized Controller and Distributed Data Plane

Figure 3-8 Centralized Controller and Distributed Data Plane

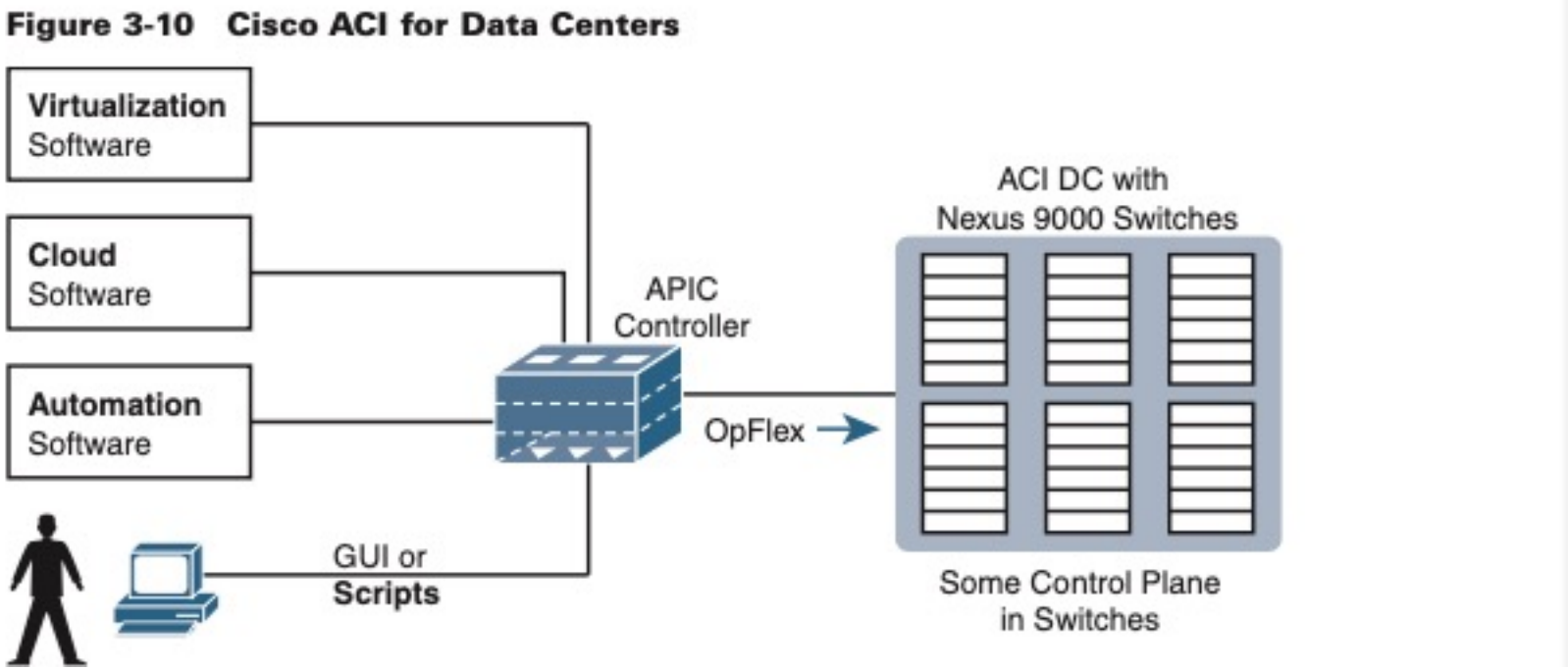


Open daylight Controller

Figure 3-9 ONF OpenDaylight Controller

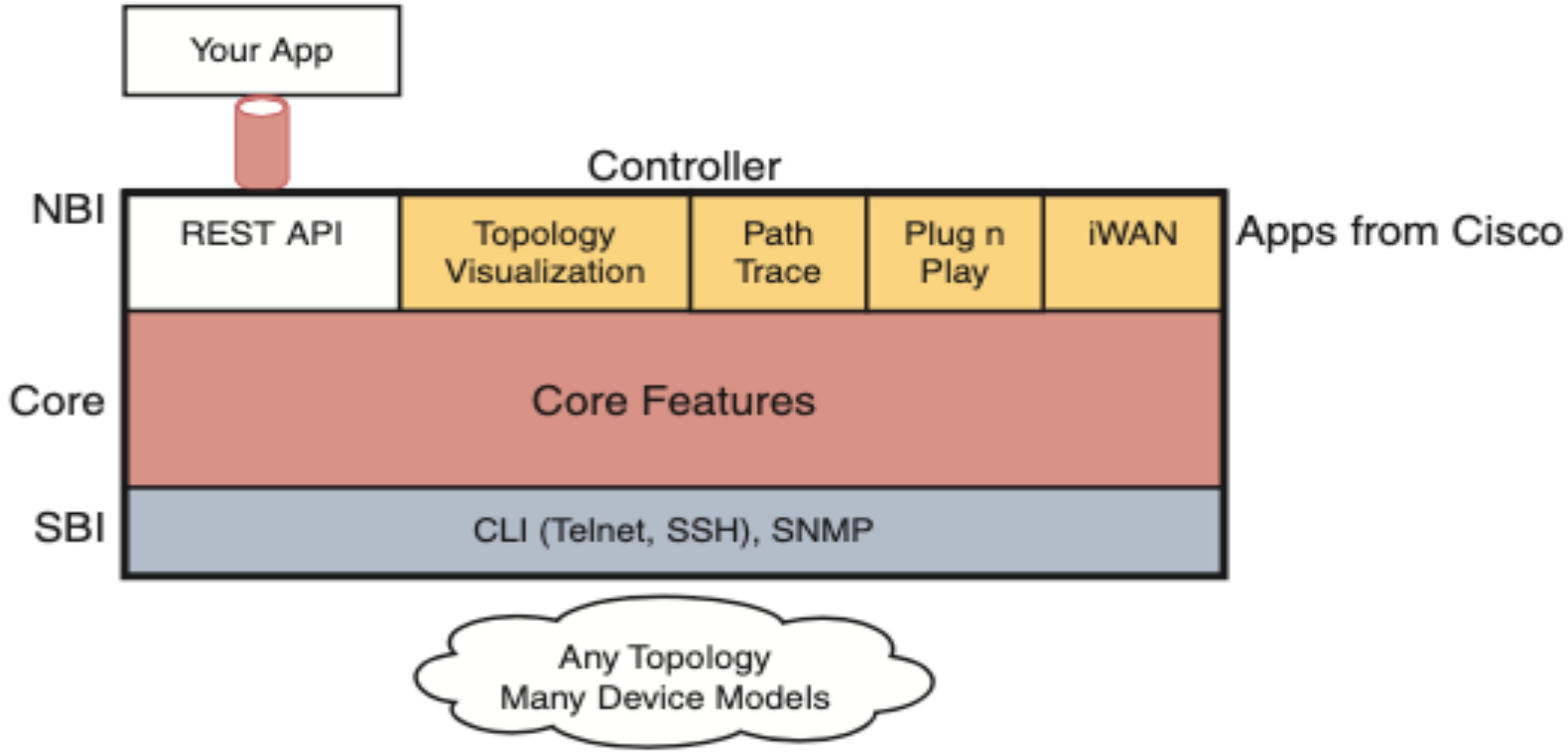


Cisco ACI for Data Center



APIC-EM Controller

Figure 3-12 APIC-EM Controller

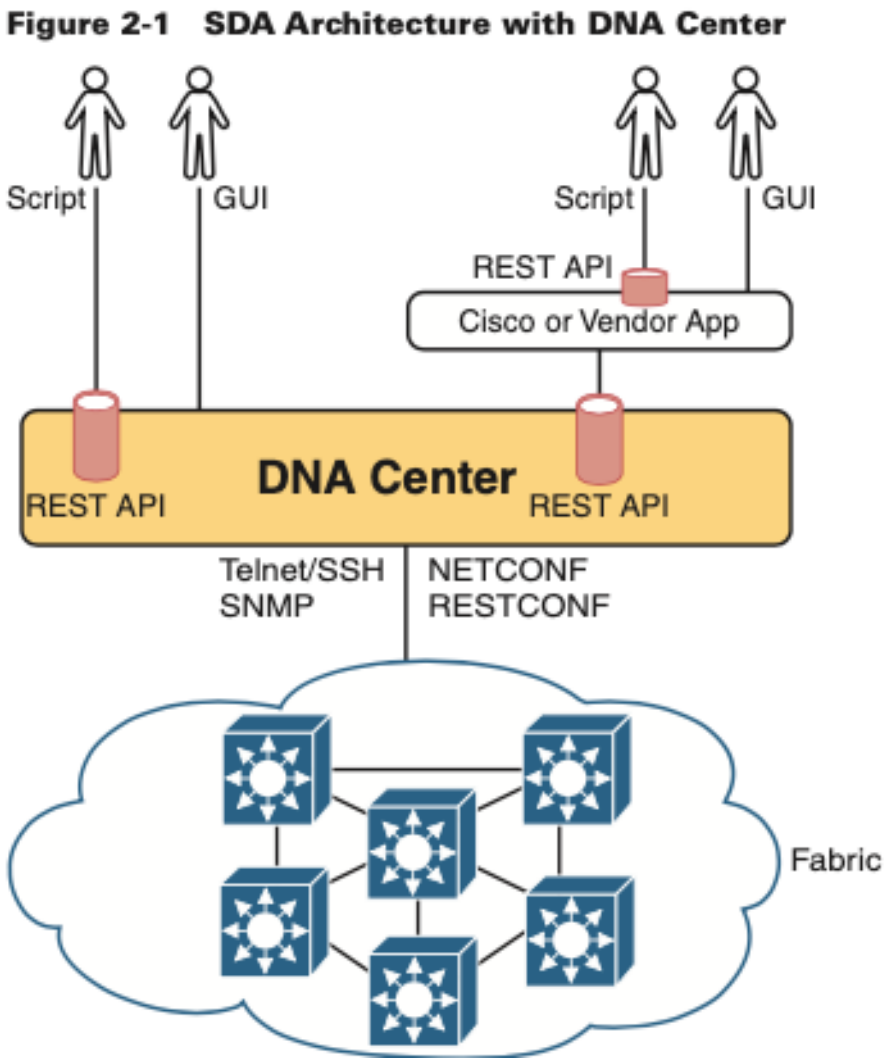


Comparing 3 SDN Controller

Table 3-1 Comparing Characteristics of Three SDN Controllers

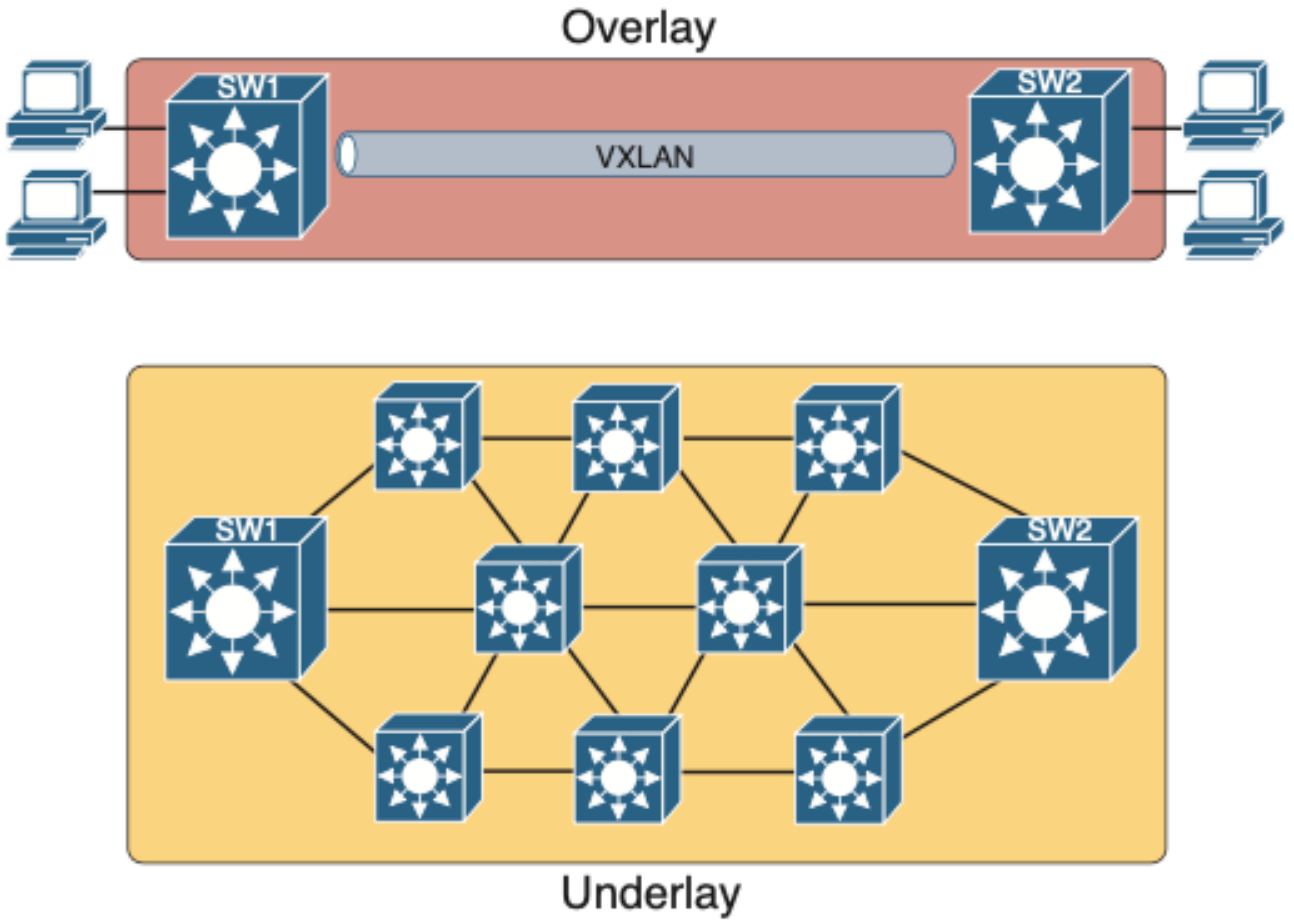
Characteristic	OpenDaylight, Cisco OSC	APIC	APIC-EM
Changes how the device control plane works compared to in traditional networking	Yes	Yes	No
Creates a centralized point from which humans and automation control the network	Yes	Yes	Yes
Determines the degree to which the architecture centralizes the control plane	Mostly	Partially	Not at all
Determines the SBIs used	OpenFlow	OpFlex	CLI, SNMP
Identifies the organization that is the primary definer/owner	ONF	Cisco	Cisco

SDA Architecture with DNA Center



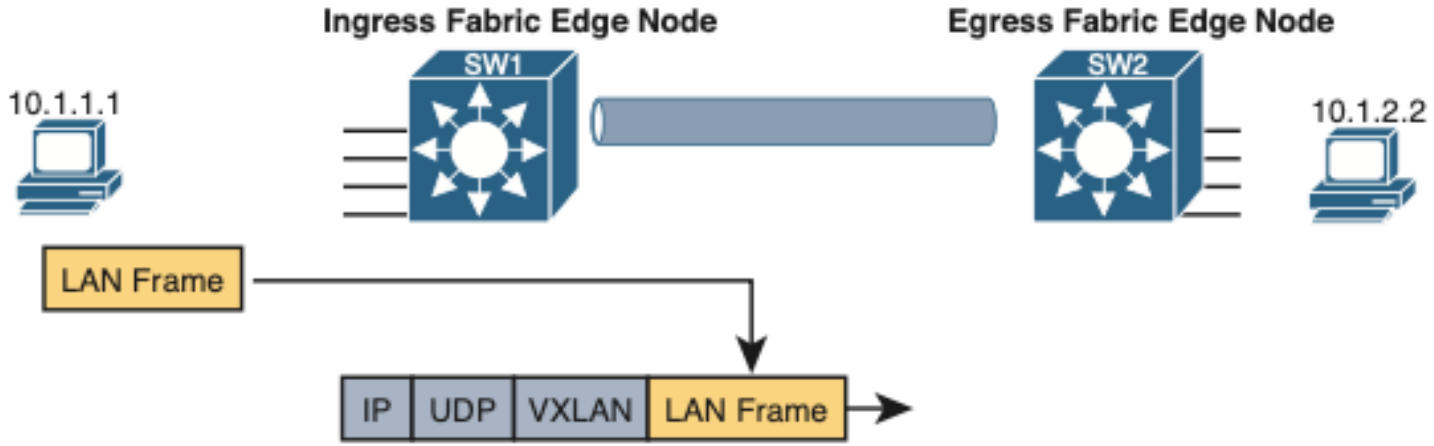
Overlay and Underlay

Figure 2-2 Overlay and Underlay



VXLAN Tunneling Operation

Figure 2-3 VXLAN Tunneling Protocol Operation



The VXLAN tunnel in the overlay works like this:

Step 1. An endpoint sends a frame.

Step 2. The frame is encapsulated in the VXLAN tunneling specification.

Step 3. The frame is forwarded to the underlay fabric.

Step 4. The other nodes in the underlay forward the frame based on the VXLAN tunnel details.

Step 5. The last SDA node removes the VXLAN details.

Step 6. The frame is forwarded to the destination endpoint.

Data Format Comparison

Table 1-1 Data Format Comparison

Data Format	Origin/Definition	Central Purpose	Common Use
JSON	JavaScript (JS) language; RFC 8259	General data modeling and serialization	REST APIs
XML	World Wide Web Consortium (W3C.org)	Data-focused text markup, which allows data modeling	REST APIs, web pages
YAML	YAML.org	General data modeling	Ansible

- Jason allows to representation Variables with text Variables are containers that store Values
- JSON can be used to store Data and Exchange Data
- in JSON white space is insignificant they don’t change the meaning of the data
- A string is a text value surrounded by double quotes
- number is a numeric value is not surrounded by quotes
- A Boolean is a data type that can be only true or False
- A null is the absence of data value
- objects are surrounded by double quotes a key which is String is surrounded by double quotes as well
- The key and the value are separated by a comma
- Objects within objects is called nested objects
- an A Array is a series of values separated by comma

Jason Output

Example 1-2 JSON Output

```
{
    "ietf-interfaces:interface": {
          "name": "GigabitEthernet0/0/0",
          "description": "Wide Area Network",
          "enabled": true,
          "ietf-ip:ipv4": {
              "address": [
                  {
                      "ip": "172.16.0.2",
                      "netmask": "255.255.255.0"
                  }
              ]
           }
    }
}
```

XML

- Like Jason white space means nothing
- the key is tagged with the value in the middle
- XML is quite similar to HTML it uses tagges
- YAML is another serialization data language
- YAML is used by ansible
- in YAML white space is significant YAML Start with 3 Hifens ---

Underlay and Overlay

- the underlay is the physical underlining like physical devices underlay is a bunch of switches
- the overlay is the virtual physical network built on top of the physical network
- SDA uses a protocol called VXLAN to Build tunnels fabric is the term we use for the overlay and underlay as a hole
- the edge nodes connect to the end host and the Border nodes connect devices outside the SD-Access example connecting to wan devices

- Configuration Management tools like Ansible Puppet and Chef allow us to do massive configurations of devices
- Ansible is written in Python Ansible is agentless Ansible uses ssh to connect to devices make configuration changes get information etc ansible uses a push model Ansible server called the control mode playbook is the blueprint of the task and these files are written in YAML you also need the inventory file and templates
- Puppet and chef use the Pull Model
- Puppet is written in Ruby puppet is agent-based the server is called Puppet Master and uses TCP 8140 and use Pull Model
- Chef like Puppet is agent-based and use a pull Mode TCP port 1002 Chef File uses DSL Which is a proprietary Language written in Ruby
- Puppet and chef both communicate using HTTP
- devices that communicate between the SBI are netconf and Restconf

API Comparison

Table 18-2 Comparing CRUD Actions to REST Verbs

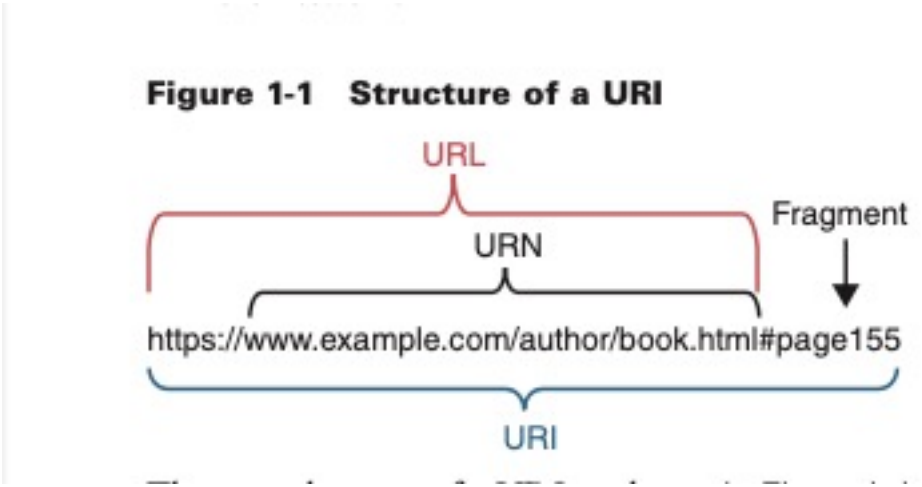
Action	CRUD Term	REST (HTTP) Verb
Create new data structures and variables	Create	POST
Read (retrieve) variable names, structures, and values	Read	GET
Update or replace values of some variable	Update	PATCH, PUT
Delete some variables and data structures	Delete	DELETE

HTTP Restful Operation

Table 1-2 HTTP Methods and RESTful Operation

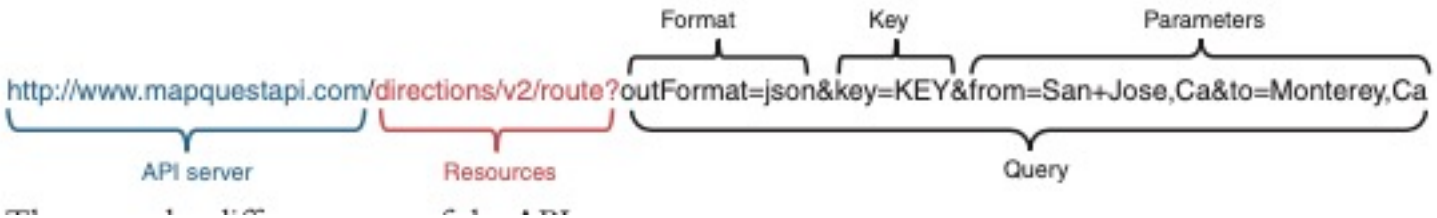
HTTP Method	RESTful Operation
POST	Create
GET	Read
PUT/PATCH	Update
DELETE	Delete

URI Structure



Restful API Request

Figure 1-2 RESTful API Request to the MapQuest API Server



Jason Payload Received form a API Request

Example 1-4 JSON Payload Received from an API Request


```
{
  "route": {
    "hasTollRoad": false,
    "hasBridge": true,
    "boundingBox": {
      "lr": {
        "lng": -121.667061,
        "lat": 36.596809
      },
      "ul": {
        "lng": -121.897125,
        "lat": 37.335358
      }
    },
    "distance": 71.712,
    "hasTimedRestriction": false,
    "hasTunnel": false,
    "hasHighway": true,
    "computedWaypoints": [],
    "routeError": {
      "errorCode": -400,
      "message": ""
    },
(output omitted)
```

Ansible Puppet and Chef Comparison

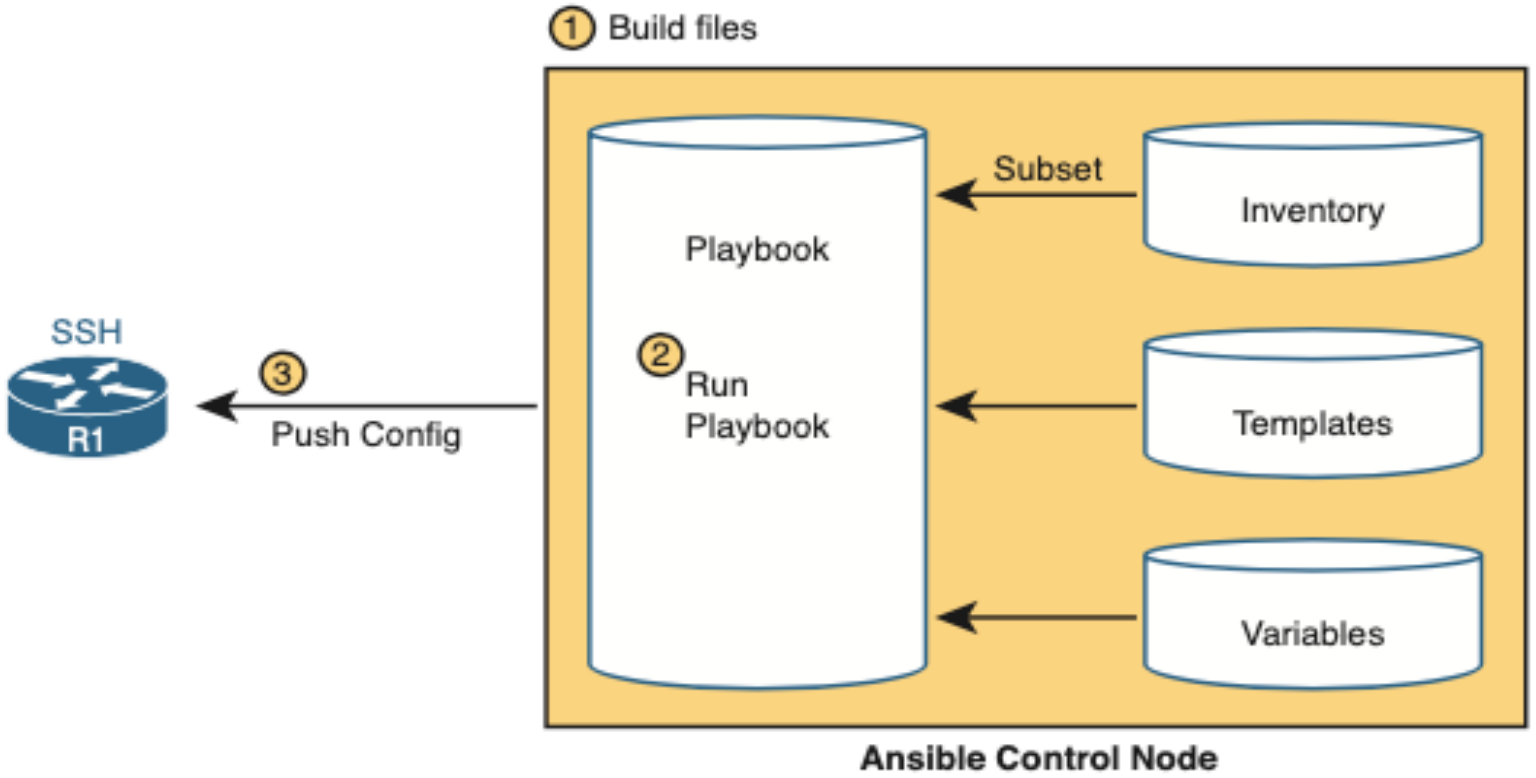
Table 19-2 Comparing Ansible, Puppet, and Chef

Action	Ansible	Puppet	Chef
Term for the file that lists actions	Playbook	Manifest	Recipe, Runlist
Protocol to network device	SSH, NETCONF	HTTP (REST)	HTTP (REST)
Uses agent or agentless model	Agentless	Agent*	Agent
Push or pull model	Push	Pull	Pull

* Puppet can use an in-device agent or an external proxy agent for network devices.

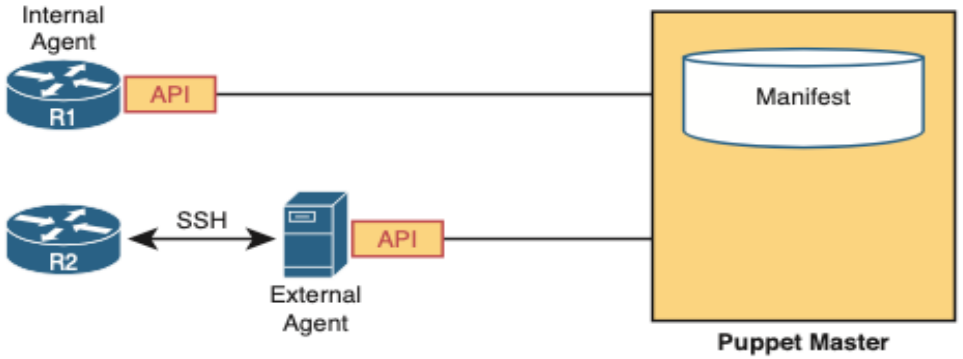
Ansible Push Model

Figure 1-3 Ansible Push Model



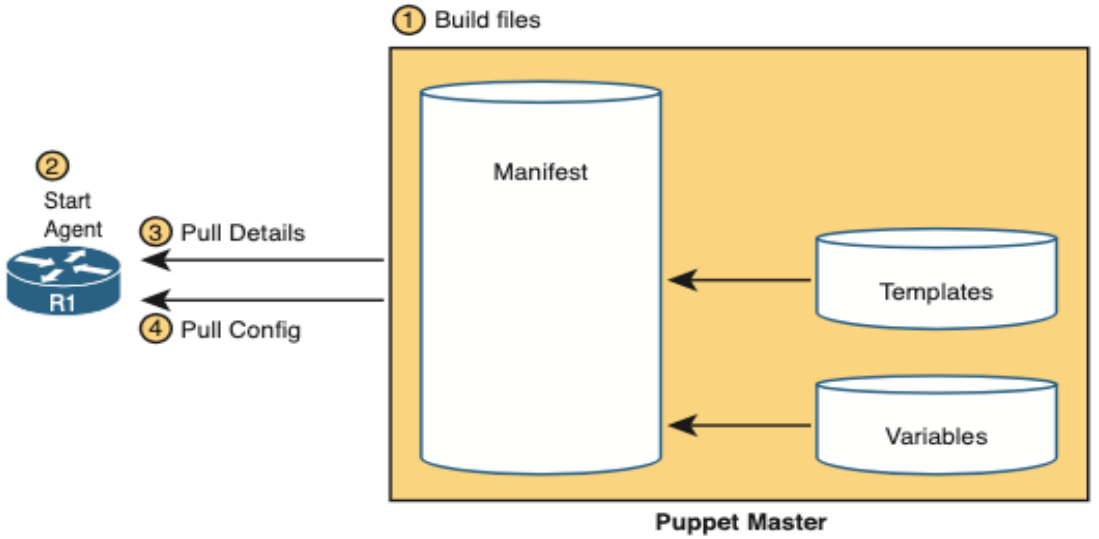
Puppet Model

Figure 1-4 Agent-Based or Agentless Operation for Puppet



Puppet uses a pull model to get a configuration to appear in the device, as shown in Figure 1-5.

Figure 1-5 Puppet Pull Model



Ansible Puppet and Chef Comparison

Table 1-3 Anisble, Puppet, and Chef Comparison

Feature	Ansible	Puppet	Chef
Term for the file that lists actions	Playbook	Manifest	Recipe, runlist
Protocol used to communicate with network devices	SSH, NETCONF	HTTP (REST)	HTTP (REST)
Uses agent or agentless model?	Agentless	Agent*	Agent
Uses a push or pull model?	Push	Pull	Pull

* Puppet can use an in-device agent or an external proxy agent for network devices.