Table of Contents

C1: IP Static Routing

Static Routes

Command:

ip route [network-address[[subnet-mask] {[next-hop-ip] | [exit-interface] [ip-address]} [administrative-distance]

Type	**Details**
Standard Static Route	IPv4 Standard Static Route e.g. *ip route 172.16.1.0 255.255.255.0 172.16.2.2* *ip route 172.16.1.0 255.255.255.0 s0/0/1* *ip route 172.16.1.0 255.255.255.0 s0/0/1 172.16.2.2* IPv6 Standard Static Route e.g. *ipv6 unicast-routing* *ipv6 route 2001:db8:acad:1::/64 2001:db8:acad:2::2* *ipv6 route 2001:db8:cafe:1::/64 2001:db8:acad:2::2* *ipv6 route 2001:db8:cafe:2::/64 2001:db8:acad:2::2*
Default Static Route	Used as **Gateway of Last Resort** which can match all packets, represents **any network** that is not in the routing table. IPv4 Default Static Route *ip route 0.0.0.0 0.0.0.0 {ip-address | exit-interface}*

	e.g. *ip route 0.0.0.0 0.0.0.0 172.16.2.2* <u>IPv6 Default Static Route</u> *ip route ::/0 {ipv6-address | exit-interface}* e.g. *ipv6 route ::/0 2001:db8:acad:2::2*
Floating Static Route	• Provide a **backup path** to a primary static or dynamic route • Only **used when the primary route is not available** • Configured with **higher administrative distance** than the primary route (Router will choose the path with lowest AD when **static route has AD of 1** by default) <u>IPv4 Floating Static Route</u> *ip route 0.0.0.0 0.0.0.0 172.16.2.2 (main route)* *ip route 0.0.0.0 0.0.0.0 10.10.10.2 5 (backup route - floating static route)* <u>IPv6 Floating Static Route</u> *ip route ::/0 201:db8:acad:2::2 (main route)* *ip route ::/0 2001:db8:feed:10::2 5 (backup route - floating static route)*
Summary Static Route	• Reduce number of routes in routing table • Minimizing route updates

- Reduces memory and CPU utilization
- Faster routing table lookups

Steps

1. Write out the **network addresses** to be summarized in **binary**.

   192.168.1.0 = 1100 0000 . 1010 1000 . 0000 0001 . 0000 0000

   192.168.2.0 = 1100 0000 . 1010 1000 . 0000 0010 . 0000 0000

   192.168.3.0 = 1100 0000 . 1010 1000 . 0000 0011 . 0000 0000

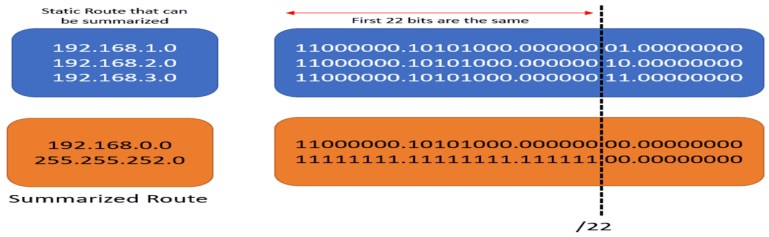
2. Find the **subnet mask** for summarization. Start with the far left bit, going to the right, finding all the bits that match **until we reach the unmatching column**. This signifies the summary boundary.

3. Count the **number of far-left matching bits**. The number identifies the subnet mask, in slash notation, for the summarized route.

   Number of far-left matching bits = 22

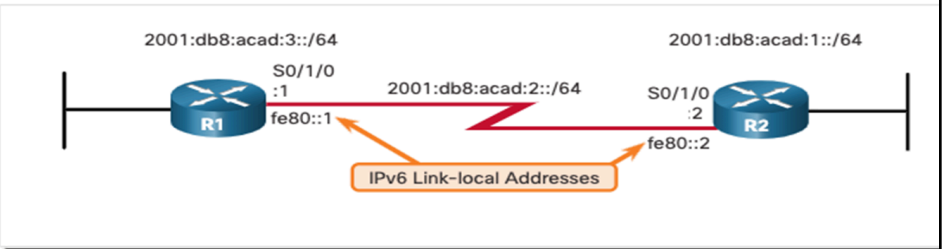
   Subnet mask = /22 or 255.255.252.0

4. To find the network address for summarization, copy the matching bits and **add all 0 bits to the end to make 32 bits**.

Next-Hop Options

Options	**Explanation**
Next-Hop Static Route	Only the **next-hop IP address** is specified e.g. *ip route 172.16.1.0 255.255.255.0 172.16.2.2*
Directly Connected Static Route	Only the **router exit interface** is specified e.g. *ip route 172.16.1.0 255.255.255.0 s0/0/1*
Fully Specified Static Route	The **next-hop IP address** and **exit interface** are specified e.g. *ip route 172.16.1.0 255.255.255.0 s0/0/1 172.16.2.2* *** If the IPv6 static route uses an IPv6 link-local address as the next-hop address, use a fully specified static route.** *ipv6 route 2001:db8:acad:1::/64 s0/1/0 fe80::2*

<table>
<tr>
<td></td>
<td>


</td>
</tr>
<tr>
<td>Static Host Route</td>
<td>

IPv4 address with 32-bit mask or IPv6 address with 128-bit mask
Can be added to the routing table via:

Automatically installed when an IP address is configured on the route
Configured as a static host route
Host route automatically obtained through other methods such as EIGRP and OSPF

<u>IPv4 Static Host Route</u>
ip route 209.165.200.238 255.255.255.255 198.51.100.2

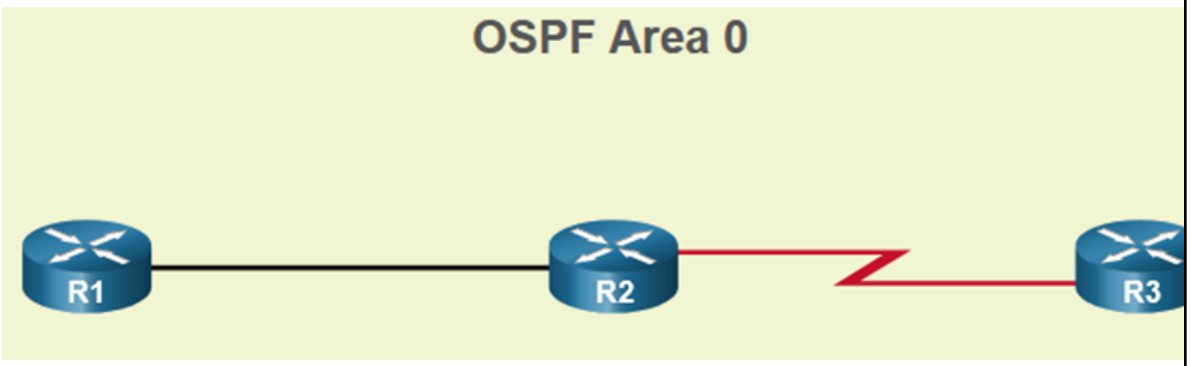
<u>IPv6 Static Host Route</u>
ip route 2001:db8:acad:2::238/128 2001:db8:acad:1::2

<u>IPv6 Static Host Route with Link-Local Next-Hop</u>
Must specify interface type and interface number
ipv6 route 2001:db8:acad:2::238/128 serial 0/1/0 fe80::2
</td>
</tr>
</table>

C2: Single-Area OSPFv2

- **Link-state protocol** that was developed as an alternative for the distance vector Routing Information Protocol (RIP)
- Offers **faster convergence** (quickly update routing table so they agree on the correct network paths again) and **scales to much larger network** implementations
- Uses the concepts of **areas** where network administrators can **divide the routing domain into distinct areas** that help control routing update traffic

OSPF Implementation



Method	Explanation
Single-Area OSPF	• All routers are in one area. Best practice is to use area 0.
Multiarea OSPF	• OSPF is implemented using multiple areas, in a hierarchical fashion • All areas must connect to the backbone area (area 0) • Routers interconnecting the areas are referred to as Area Border Routers (ABRs)

MultiArea OSPF Advantages

Advantages	Explanation
Smaller routing tables	• Tables are smaller because there are fewer routing table entries • Network addresses can be summarized between areas • Route summarization is not enabled by default
Reduced link-state update overhead	• Designing multiarea OSPF with smaller areas minimizes processing and memory requirements
Reduced frequency of SPF calculations	• Multiarea OSPF localize the impact of a topology change within an area • e.g. it minimizes routing update impact because LSA flooding stops at the area boundary

OSPF Challenges

Multiaccess networks can create two challenges for OSPF regarding the flooding of LSAs:

Challenge	Explanation
Creation of multiple adjacencies 邻接关系	• Ethernet networks could potentially interconnect many OSPF routers over a common link • Creating adjacencies with every router would lead to an excessive number of LSAs exchanged between routers on the same network
Extensive flooding of LSAs	• Link-state routers flood their LSAs any time OSPF is initialized, or when there is a change in the topology • This flooding can become excessive

Router ID

<table>
<tr><td colspan="2">

- OSPF router ID is a 32-bit value represented as an IPv4 address
- Used to uniquely identify an OSPF router, and all OSPF packets include the router ID of the originating router
- Every router requires a router ID to participate in OSPF domain
- The router ID is used by OSPF-enabled router to:

</td></tr>
<tr><td>Participate in the synchronization of OSPF databases</td><td>

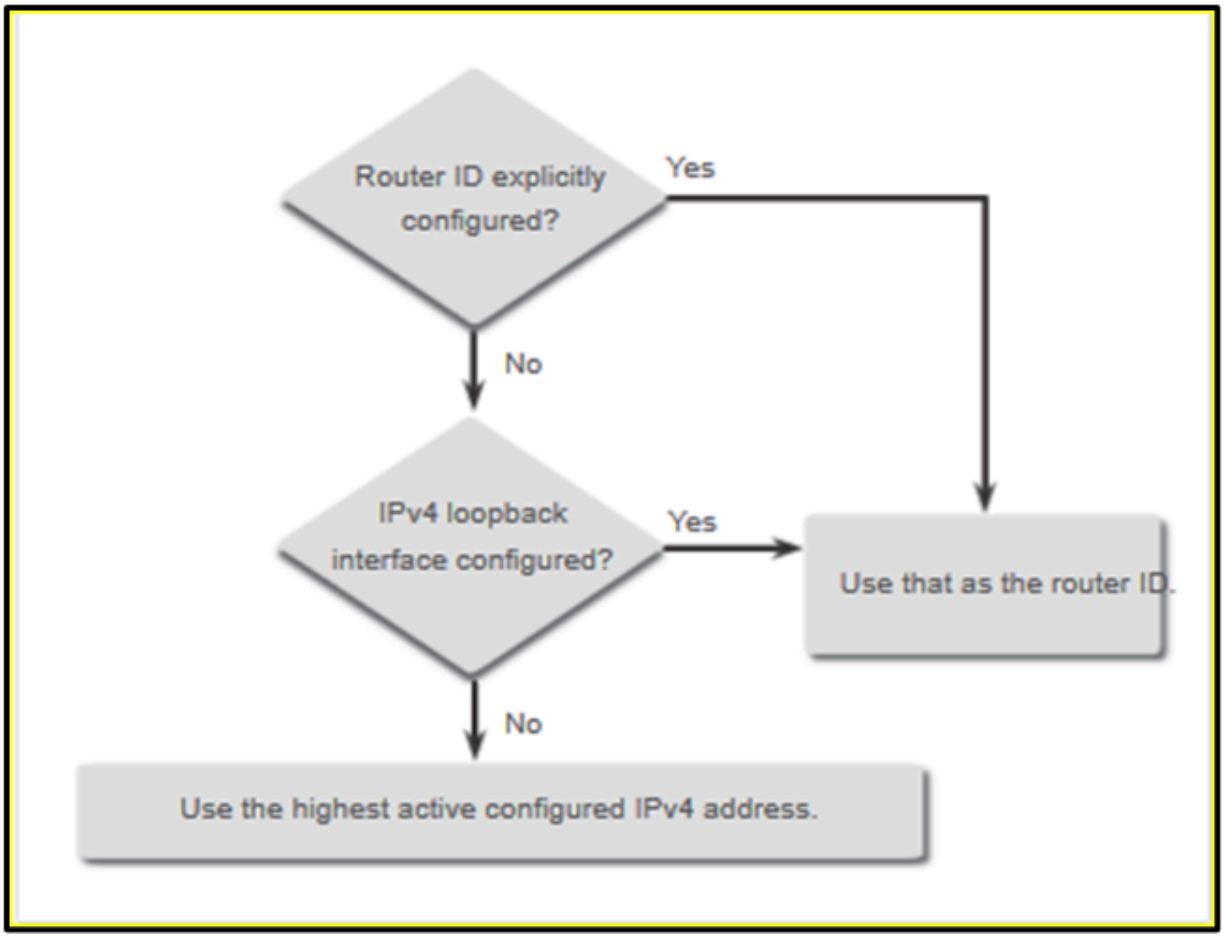
- During the Exchange State, the router with the highest router ID will send their database descriptor (DBD) packets first

</td></tr>
<tr><td>Participate in the election of the designated router (DR)</td><td>

- In a multiaccess LAN environment, the router with the highest router ID is elected the DR
- The routing device with the second highest router ID is elected the backup designated router (BDR).

</td></tr>
</table>

Router ID Order of Precedence



1. The router ID is explicitly configured using the OSPF ***router-id*** *rid* router configuration mode command. This is the recommended method to assign a router ID.
2. The router chooses the **highest IPv4 address** of any of the configured **loopback interfaces**.
3. The router chooses the **highest active IPv4 address** of any of its physical interfaces.

Configure Loopback Interface as Router ID

interface Loopback 1

ip address 1.1.1.1 255.255.255.255

```
R1(config-if)# interface Loopback 1
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Explicitly Configure a Router ID

router ospf 10

router-id 1.1.1.1

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
*May 23 19:33:42.689: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Modify Router ID

clear ip ospf process: Reset router ID

```
R1# show ip protocols | include Router ID
Router ID 10.10.1.1
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
R1(config-router)# end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
*Jun 6 01:09:46.975: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
*Jun 6 01:09:46.981: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from LOADING
to FULL, Loading Done *
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Point-to-Point OSPF Networks

network [network-address] [wildcard-mask] area [area-id] e.g. *router ospf 10* *network 10.10.1.0 0.0.0.255 area 0* *network 10.1.1.4 0.0.0.3 area 0* *network 10.1.1.12 0.0.0.3 area 0*	Specify the interfaces that belong to a point-to-point network
ip ospf [process-id] area [area-id] e.g. *interface g0/0/0* *ip ospf 10 area 0* *interface g0/0/1* *ip ospf 10 area 0*	Configure OSPF directly on specific interface

Passive Interface

- OSPF messages only need to be sent out interfaces that are connecting to other OSPF-enabled routers
- Sending out unneeded messages on a LAN affects the network:

Impact	**Explanation**
Inefficient use of bandwidth	• Available bandwidth is consumed transporting unnecessary messages

Inefficient use of resources	• All devices on the LAN must process and eventually discard the message
Increased security risk	• Without additional OSPF security configurations, OSPF messages can be intercepted with packet sniffing software • Routing updates can be modified and sent back to the router, corrupting the routing table with false metrics that misdirect traffic

Solution

router ospf [process-id] *passive-interface [interface]*	Prevent the transmission of routing messages through a specific router interface but still allow that network to be advertised to other routers

Disable DR/BDR Election Process

- The DR/BDR election process is unnecessary when there are only two routers on the point-to-point network.
- The router will have designated the network type as BROADCAST

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
        0           1        no           no          Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.1.1.6
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.1.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
```

interface [interface] *ip ospf network*	• Change to point-to-point network • apply this command on all interfaces that need to

point-to-point	disable DR/BDR election process

Multiaccess OSPF Networks

State of Neighbors in Multiaccess Networks

State	**Explanation**
FULL/DROTHER	• This is a DR or BDR router that is fully adjacent with a non-DR or BDR router • These two neighbors can exchange Hello packets, updates, queries, replies and acknowledgments
FULL/DR	• The router is fully adjacent with the indicated DR neighbor • These two neighbors can exchange Hello packets, updates, queries, replies and acknowledgments
FULL/BDR	• The router is fully adjacent with the indicated BDR neighbor • These two neighbors can exchange Hello packets, updates, queries, replies and acknowledgments
2-WAY/DROTHER	• The non-DR or BDR router has a neighbor relationship with another non-DR or BDR router • These two neighbors exchange Hello packets

Default DR/BDR Election Process

1. The routers in the network elect the router with the **highest interface priority** as the **DR**. The router with the **second highest interface priority** becomes the **BDR**.
    - The priority can be configured to be any number between 0 - 255.
    - If the interface priority value is set to 0, that interface cannot be elected as DR nor BDR.

- The **default priority** of multiaccess broadcast interfaces is **1**.

2. If the **interface priorities are equal**, then the router with the **highest router ID** is elected the **DR**. The router with the **second highest router ID** is the **BDR**.
    - The **election process takes place** when the **first router with an OSPF-enabled interface is active** on the network. If all of the routers on the network have not finished booting, it is possible that a router with a lower router ID becomes the DR.
    - The **addition of a new router does not initiate a new election** process.

Setting Interface Priority

interface [interface]

ip ospf priority [0-255]

clear ip ospf process

- A value of 0 does not become a DR or BDR
- A value of 1 to 255 may make the router becomes the DR or BDR

Cisco OSPF Cost Metric

- Routing protocols use metrics to determine the best path of a packet across a network
- OSPF uses cost as a metric, a lower cost indicates a better path
- Cisco cost of interface is inversely proportional to the bandwidth of the interface (higher bandwidth, lower cost)

Cost = reference bandwidth / interface bandwidth

Default reference bandwidth is 10^8 (100,000,000):

Cost = 100,000,000 bps / interface bandwidth in bps

- Adjust the reference bandwidth with the ***auto-cost reference bandwidth [Mbps]*** command on each OSPF router

- Manually set OSPF cost value with ***ip ospf cost [cost]*** command on necessary interfaces

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	0.01 = 1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	0.1 = 1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	1

Same Costs due to reference bandwidth

Adjust Reference Bandwidth

- OSPF cost assigned to a Gigabit Ethernet interface with the default reference bandwidth of 100,000,000 bps would equal to 1 since the nearest integer for 0.1 is 0 instead of 1.
- Cost = 100,000,000 bps / 1,000,000,000 = 1
- All interfaces faster than Fast Ethernet will have the same cost value of 1 as a Fast Ethernet interface
- e.g.
    - Adjust cost for Gigabit Ethernet: *auto-cost reference-bandwidth 1000*
    - Adjust cost for 10 Gigabit Ethernet: *auto-cost reference-bandwidth 10000*
    - Return to default reference bandwidth: *auto-cost reference-bandwidth 100*

- OSPF Cost Table

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	10,000,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	10,000,000,000	÷	1,000,000,000	10
Fast Ethernet 100 Mbps	10,000,000,000	÷	100,000,000	100
Ethernet 10 Mbps	10,000,000,000	÷	10,000,000	1000

Hello and Dead Intervals

Hello Interval	• How often OSPF routers send hello packets to establish and maintain neighbor relationships • Set Hello intervals: *ip ospf hello-interval [seconds]* • Reset Hello intervals: *no ip ospf hello-interval*
Dead interval	• The time a router waits to receive a hello packet from a neighbor before declaring that neighbor as down • Set Dead intervals: *ip ospf dead-interval [seconds]* • Reset Dead intervals: *no ip ospf dead-interval*

Propagate Default Static Route

```
R2(config)# interface lo1
R2(config-if)# ip address 64.100.0.1 255.255.255.252
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

Default Static Route	*ip route 0.0.0.0 0.0.0.0 [next-hop-address | exit-interface]*
Instruct specific router to be the source of default route information and propagate the default static route in OSPF updates	*default-information originate*

C3: ACL Concepts

- ACL is a series of IOS commands that are used to filter packets based on information found in the packet header.
- Refer to Workbook for ACL commands☺️

Types of ACLs

Type	**Explanation**
Standard ACLs	• ACLs only filter at Layer 3 using the source IPv4 address only
Extended ACLs	• ACLs filter at Layer 3 using the source and / or destination IPv4 address • They can also filter at Layer 4 using TCP, UDP ports and optional protocol type information for finer control

ACL Operation

Inbound ACL	• Filters packet before they are routed to the outbound interface • Efficient because it saves the overhead of routing lookups if the packet is discarded
Outbound ACL	• Filter packets after being routed, regardless of the inbound interface

<u>Selection of Filtering Incoming or Outgoing Packets</u>

Access lists on **incoming port**	• Requires less CPU processing • Filters and denies packets before the router has to make a routing decision

Access lists on **outgoing port**	• Are outbound by default unless otherwise specified • Increases the CPU processing time because the routing decision is made and the packet switched to the correct outgoing port before it is tested against the ACL

Common Protocols in Extended ACL

Transport Layer Protocol	**Protocol**	**Port Number**	**Keyword**
TCP	FTP	20 (data), 21 (login) * both needed (2 statements)	ftp-data (20) ftp (21)
	SSH	22	-
	Telnet	23	telnet
	SMTP	25	smtp
	HTTP	80	www
	POP3	110	pop3
	HTTPS	443	-
UDP	DNS	53	domain
	DHCP	67 (server → client) 68 (client → server) * both needed (2	bootps (67) bootpc (68)

		statements)	
	TFTP	69	tftp
	SNMP	161	snmp
ICMP	**For ping**		

C4: Network Security Concepts

Current State of Cybersecurity

Current State of Affairs

Security Terms	**Description**
Assets	• Anything of value to the organization • Includes people, equipment, resources and data
Vulnerability	• 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
Mitigation	• Counter-measure that reduces the likelihood or security of a potential threat or risk • Network security involves multiple mitigation techniques
Risk	• Likelihood of a threat to exploit the vulnerability of an asset, with the aim of negatively affecting an organization • Risk is measured using the probability of the occurrence of an event and its consequences

Data Loss *

Data loss or data exfiltration: **Situation when data is intentionally or unintentionally lost, stolen or leaked to the outside world** Consequences:

- **Brand damage and loss of reputation**
- **Loss of competitive advantage**
- **Loss of customers**
- **Loss of revenue**
- **Litigation 诉讼 / legal action resulting in fines and civil penalties 民事处罚**
- **Significant cost and effort to notify affected parties and recover from breach**

Data Loss Vectors	**Description**
Email / Social Networking	Intercepted email or IM messages **即时通讯信息** could be captured and reveal confidential information
Unencrypted Devices	If the data is not stored using an encryption algorithm, then the thief can 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	One risk is that an employee could perform an unauthorized transfer of data to a USB drive Another risk is that a USB drive containing valuable corporate data could be lost
Hard Copy	Confidential data should be shredded **被粉碎** when no longer required
Improper Access Control	Passwords or weak passwords which have been compromised can provide a threat actor with easy access to corporate data

Threat Actors

Type of Hackers

Hacker Type	Description
White Hat Hackers	• Ethical hackers who **use their programming skills for good, ethical and legal purposes** • **Security vulnerabilities are reported to developers** for them to fix before the vulnerabilities can be exploited
Gray Hat Hackers	• Individuals who **commit crimes and do arguably unethical things**, but **not for personal gain or to cause damage** • May **disclose a vulnerability to the affected organization** after having compromised their network
Black Hat Hackers	• Unethical criminals who **compromise computer and network security for personal gain**, or for malicious reasons such as **attacking networks**

Hacking Terms

Hacking Term	Description
Script Kiddies	• Teenagers or inexperienced hackers running existing scripts, tools and exploits to cause harm but typically not for profit
Vulnerability Broker	• Usually are gray hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards
Hacktivists	• Gray hat hackers who publicly protest 抗议 organizations or governments by posting articles, videos, leaking sensitive information and performing network attacks

Cyber criminals	• Black hat hackers who are either self-employed or working for large cybercrime organizations
State-Sponsored 国家支持的黑客活动	• Either white hat or black hat hackers who steal government secrets, gather intelligence and sabotage networks • Their targets are foreign governments, terrorist groups and corporations • Most countries in the world participate to some degree in state-sponsored hacking

Threat Actor Tools

Penetration Testing Tool	**Description**
Password Crackers	• **Password recovery tools** which can be used to track or recover a password • **Make guesses** to crack the password • e.g. John the Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack and Medusa
Wireless Hacking Tools	• Used to intentionally **hack into a wireless network** to detect security vulnerabilities • e.g. Aircrack-ng, InSSIDer, KisMAC, Firesheep and ViStumbler
Network Scanning and Hacking Tools	• Used to **probe** 探测 **network devices, servers and hosts for open TCP or UDP ports** • e.g. Nmap, SuperScan, Angry IP Scanner and NetScanTools

Packet Crafting Tools	• Used to **probe and test a firewall's robustness** using **specially crafted forged packets** 伪造数据包 • e.g. Hping, Scapy, Socat, Yersinia, Nping and Nemesis
Packet Sniffers	• Used to **capture and analyze packets within traditional Ethernet LANs or WLANs** • e.g. Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy and SSLstrip

* More penetration testing tool in lecture note pg15

Attack Types

Attack Type	**Description**
Eavesdropping Attack	• Happen when a threat actor **captures and "listens" to network traffic** • 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	• If threat actors **discover a valid user account**, the threat actors have the same rights as the real user • Threat actors could **use that valid account to obtain lists of other users**, network information, change server and network configuration, and modify, reroute or delete data

Denial of Service Attack	• **Prevents normal use of a computer or network by valid users** • **Flood a computer or the entire network with traffic** until a shutdown occurs because of the **overload** • Block traffic, which results in a loss of access to network resources by authorized users
Man-in-the-Middle Attack	• Occurs when threat actors have **positioned themselves between a source and destination** • 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 a 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 the packets are not encrypted, a sniffer provides a full view of the data inside the packet

Malware

Type of Malware	**Description**
Virus	• **Requires human action to propagate** and **infect other computers** • Virus hides by **attaching itself to computer code, software or**

	documents on the computer ● When **opened**, the **virus executes** and infects the computer ● **Alter, corrupt, delete files or erase entire drives** ● Cause computer booting issues and corrupt applications ● Capture and send sensitive information to threat actors ● Access and use email accounts to spread ● Lay dormant until summoned by the threat actor 处于休眠状态, 直到被威胁制造者召唤
Adware	● **Distributed by downloading online software** ● **Display unsolicited** 未经请求 **advertising using pop-up web browser windows**, new toolbars or unexpectedly redirect a webpage to a different website ● Pop-up windows may be difficult to control as new windows can pop-up faster than the user can close them
Ransomware	● **Denies a user access to their 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 crypto currencies such as Bitcoin
Rootkit	● Used by threat actors to **gain administrator account-level access to a computer** ● **Very difficult to detect** because they can **alter firewall, antivirus protection, system files and even OS commands** to conceal their presence ● **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 DDoS attack • Special rootkit removal tools must be used to remove them, or a complete OS re-install may be required
Spyware	• Like adware but used to **gather information about the user** and **send to threat actors** without the user's consent • Can be a low threat, gathering browsing data, or it can be high threat capturing personal and financial information
Worm	• **Self-replicating program** that **propagates automatically without user actions** by **exploiting vulnerabilities in legitimate software** • Uses the network to search for other victims with the same vulnerability • Slow or disrupt network operations

Common Network Attacks

Reconnaissance Attacks

Reconnaissance attacks: **Unauthorized discovery and mapping of systems, services or vulnerabilities**	
Technique	**Description**
Perform an information query of a target	• Threat actor is looking for **initial information about a target** • Various tools can be used such as Google search, organizations website, whois and more
Initiate a ping sweep of the target network	• Information query **reveals the target's network address** • Threat actor can initiate a **ping sweep to determine**

	which IP addresses are active
Initiate a port scan of active IP addresses	• **Determine which ports or services are available** • Port scanners such as Nmap, SuperScan, Angry IP Scanner and NetScanTools
Run vulnerability scanners	• **Query the identified ports to determine the type and version of the application and operating system** that is running on the host • Tools such as Nipper, Core Impact, Nessus, SAINT and Open VAS
Run Exploitation tools	• Threat actor attempts to **discover vulnerable services that can be exploited** • Vulnerability exploitation tools such as MetaSploit, Core Impact, Sqlmap, Social Engineer Toolkit and NETsparker

Access Attacks

- **Exploit known vulnerabilities in authentication services, FTP services and Web services**
- **Gain entry to web accounts, confidential databases and other sensitive information**
- Used on network devices and computers to **retrieve data, gain access, or to escalate access privileges to administrator status**

Type	**Description**
Password Attacks	• **Discover critical system password** using various methods • Can be launched using various **password cracking tools**
Spoofing Attacks	• **Pose as another device by falsifying data**

	• e.g. IP spoofing, MAC spoofing and DHCP spoofing

Social Engineering Attacks *

• Access attack that attempts to **manipulate individuals into performing actions or divulging 泄露 confidential information**	
Social Engineering Attack	**Description**
Pretexting	**Pretends to need personal or financial data** to confirm the identity of the recipient
Phishing	**Sends fraudulent email which is disguised as being from a legitimate, trusted source** to trick the recipient into **installing malware** on their device, or to **share personal or financial information**
Spear phishing	**Creates a targeted phishing attack** tailored for a specific individual or organization
Spam	A.k.a. junk mail, this is **unsolicited email which often contains harmful links, malware or deceptive 欺骗性 content**
Something for Something	A.k.a. "Quid pro quo", this is when a **threat actor requests personal information from a party in exchange for something such as a gift**
Baiting	• Leaves a **malware infected flash drive in a public location** • A victim finds the drive and unsuspectingly **inserts it into their laptop, unintentionally installing malware**
Impersonation	**Pretends to be someone they are not to gain the trust of a victim**

Tailgating	Quickly **follows an authorized person into a secure location to gain access to a secure area**
Shoulder surfing	Inconspicuously **looks over someone's shoulder to steal their passwords or other information**
Dumpster diving	**Rummages 翻找 through trash bins to discover confidential documents**

DoS and DDoS Attacks

DoS Attacks	**Distributed DoS Attack (DDoS)**
Interrupt communication and **cause significant loss of time and money**	Similar to DoS attack, but it **originates from multiple coordinated sources**
Relatively **simple to conduct**, even by unskilled threat actor	

Type of DoS Attack	**Explanation**
Overwhelming Quantity of Traffic	• **Sends an enormous quantity of data** at a rate that the **network, host or application cannot handle** • Causes **transmission and response times to slow down** • **Crash** a device or service
Maliciously Formatted Packets	• **Sends a maliciously formatted packet to a host or application** and the **receiver is unable to handle it** • Causes the receiving device to **run very slowly or crash**

IP Vulnerabilities and Threats

IP Attack Techniques

IP Attack Techniques	Description
ICMP attacks	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 attacks	Attempt to **prevent legitimate users from accessing information or services using DoS and DDoS attacks**
Address spoofing attacks	**Spoof the source IP address in an IP packet** to perform blind spoofing or non-blind spoofing
Man-in-the-middle attack (MITM)	Threat actors **position themselves between a source and destination** to transparently **monitor, capture and control the communication** Eavesdrop by inspecting captured packets, or alter packets and forward them to their original destination
Session hijacking	**Gain access to the physical network, and then use an MITM attack to hijack a session**

ICMP Attacks

Launch information-gathering attacks to:

- **map out a network topology, discover which hosts are active (reachable)**
- **identify the host operating system (OS fingerprinting)**
- **determine the state of a firewall**

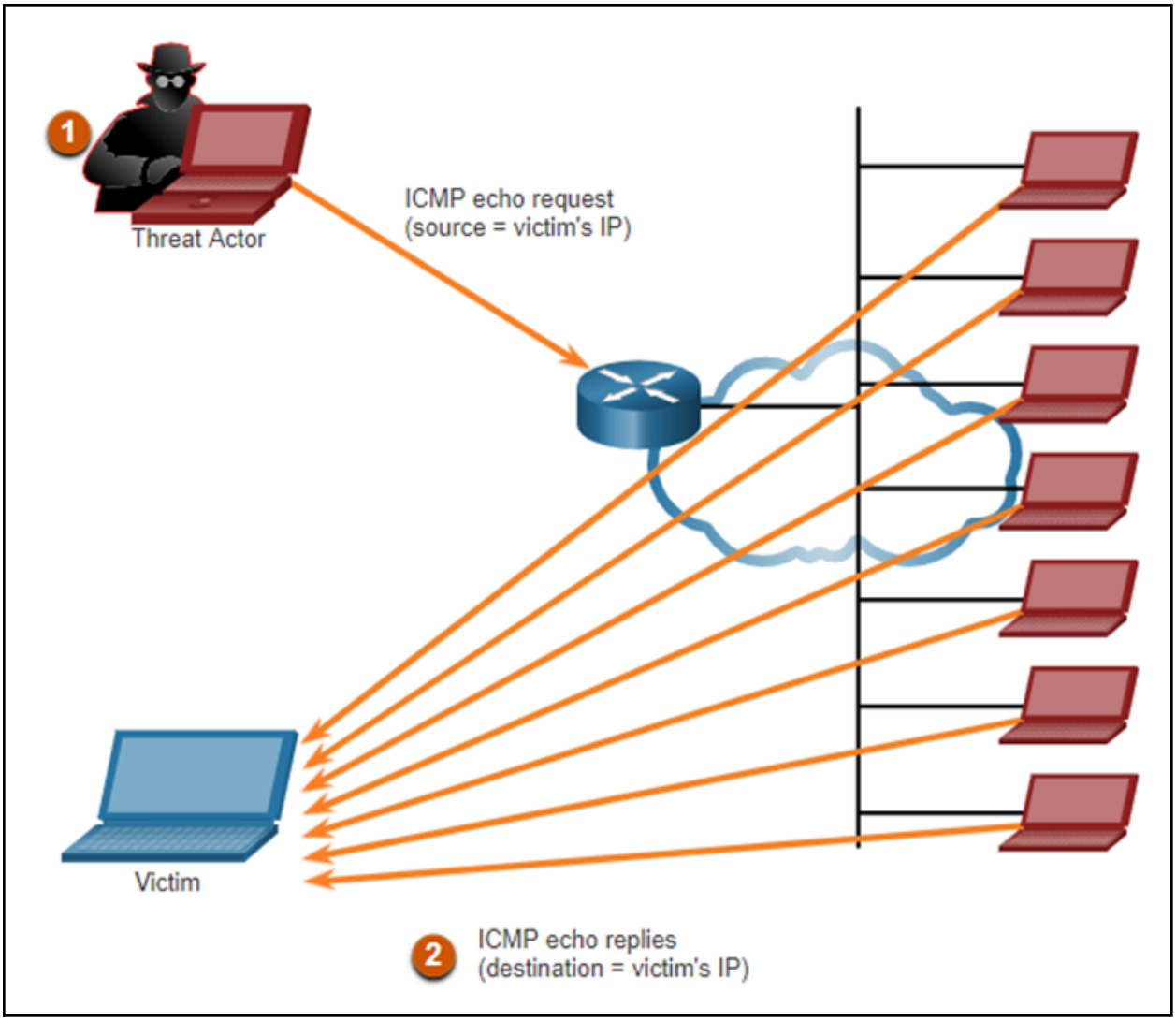
Prevention:

- Networks should have **strict ICMP access control list (ACL) filtering on the network edge** to **avoid ICMP probing** from the Internet
- Uses **security devices such as firewalls and intrusion detection systems (IDS)** to **detect attacks** and **generate alerts to security analysis**

ICMP Messages used by Hackers	**Description**
ICMP echo request and echo reply	This is used to perform **host verification** and **DoS attacks**
ICMP unreachable	This is used to perform **network reconnaissance** and **scanning attacks**
ICMP mask reply	This is used to **map an internal IP network**
ICMP redirects	This is used to **lure** 引诱 **a target host into sending all traffic through a compromised device** and **create a MITM attack**
ICMP router discovery	This is used to **inject bogus route entries into the routing table of a target host**

Amplification and Reflection Attacks

- **Smurf attack** is used to **overwhelm a target host**
- Threat actors use **resource exhaustion attacks** to either to **crash a target host** or to **consume the resources of a network**



Address Spoofing Attacks

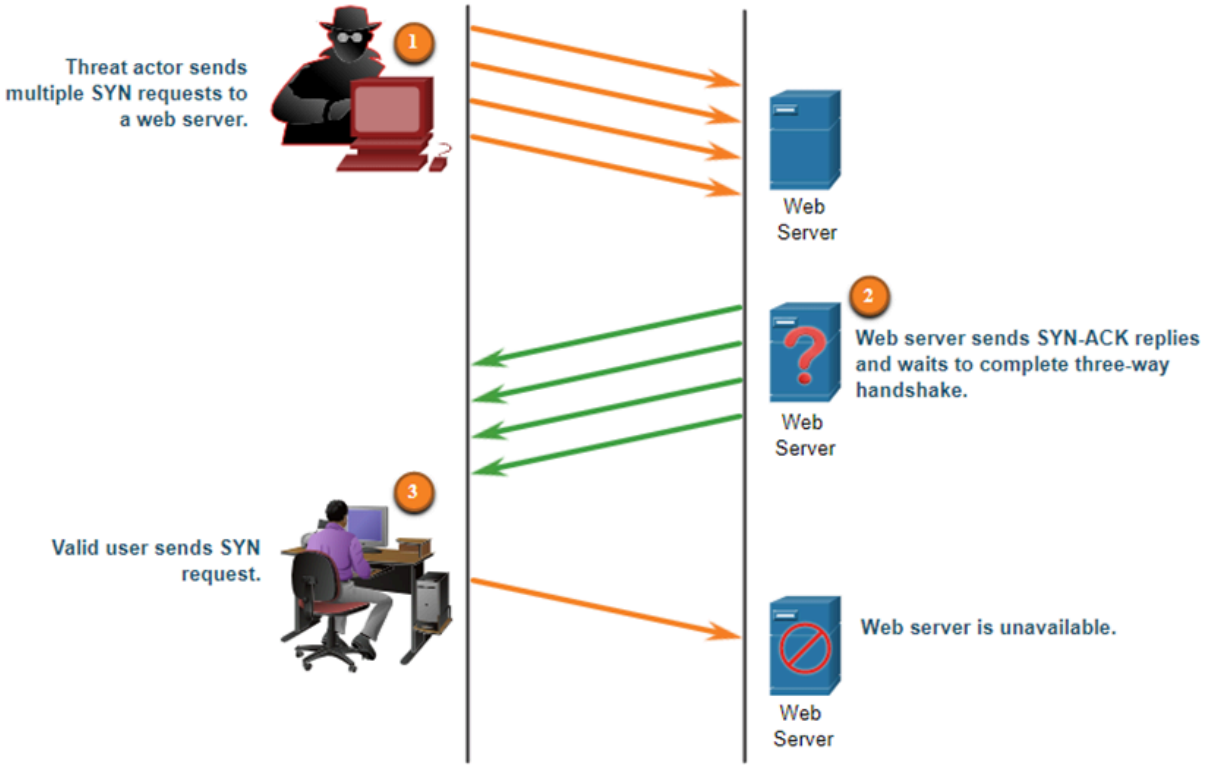
- Occur when a threat actor **creates packets with false source IP address information** to either **hide the identity of the sender**, or to **pose as another legitimate user**
- Spoofing is usually incorporated into another attack such as Smurf attack
- Spoofing attacks can be non-blind or bind

Non-blind spoofing	• Threat actor **can see the traffic that is being sent between the host and the target** • **Determine the state of a firewall and sequence-number prediction** • Can **hijack an authorized session**
Blind spoofing	• Threat actor **cannot see the traffic that is being sent**

	between the host and the target • **Used in DoS attacks**

TCP and UDP Vulnerabilities

TCP SYN Flood Attack



1. The **threat actor sends multiple SYN requests to a web server**.
2. The **web server replies with SYN-ACKs for each SYN request** and **waits to complete the three-way handshake**. The **threat actor does not respond to the SYN-ACKs**.
3. A **valid user cannot access the web server** because the web server has **too many half-opened TCP connections**.

UDP Flood Attacks

- Threat actor uses a tool like UDP Unicorn or Low Orbit Ion Cannon
- These tools **send a flood of UDP packets**, often **from a spoofed host to a server on the subnet**
- The **program will sweep through all the known ports trying to find closed ports**
- This will cause the **server to reply with an ICMP port unreachable message**.
- Because there are **many closed ports on the server**, this **creates a lot of traffic on the segment which uses up most of the bandwidth**
- Result is similar to DoS attack

Network Security Best Practices

Defense-in-Depth Approach

- Requires a combination of networking devices and services working together
- Ensure secure communications across both public and private networks
- To secure devices including routers, switches, servers and hosts

1. Several security devices and services are implemented
    - VPN
    - ASA Firewall
    - IPS
    - ESA/WSA
    - AAA Server

2. All network devices including the router and switches are hardened, which means that they have been secured to prevent threat actors from gaining access and tampering with the devices

3. You must also secure data as it travels across various links. This may include internal traffic but it is more important to protect the data that travels outside of the organization to branch sites, telecommuter sites and partner sites

Content Security Devices

Cisco Email Security Appliance (ESA)	• Special device designed to **monitor Simple Mail Transfer Protocol (SMTP)** • Cisco ESA is constantly **updated by real-time feeds from the Cisco Talos** • **Threat intelligence data is pulled by the Cisco ESA every three to five minutes**
Cisco Web Security Appliance (WSA)	• **Mitigation technology for web-based threats** • **Combines advanced malware protection, application visibility and control, acceptable use policy controls and reporting** • Provides complete **control over how users access the Internet** • Perform **blacklisting of URLs**, **URL-filtering**, **malware scanning**, **URL categorization**, **web application filtering** and **encryption and decryption of web traffic**

C5: NAT for IPv4

NAT64

- NAT for IPv6 is used to **transparently provide access between IPv6-only and IPv4-only networks**
- It is not used as a form of private IPv6 to global IPv6 translation
- NAT for IPv6 should not be used as a long-term strategy, but as a temporary mechanism to **assist in the migration from IPv4 to IPv6**

C7: VPN and IPsec Concepts

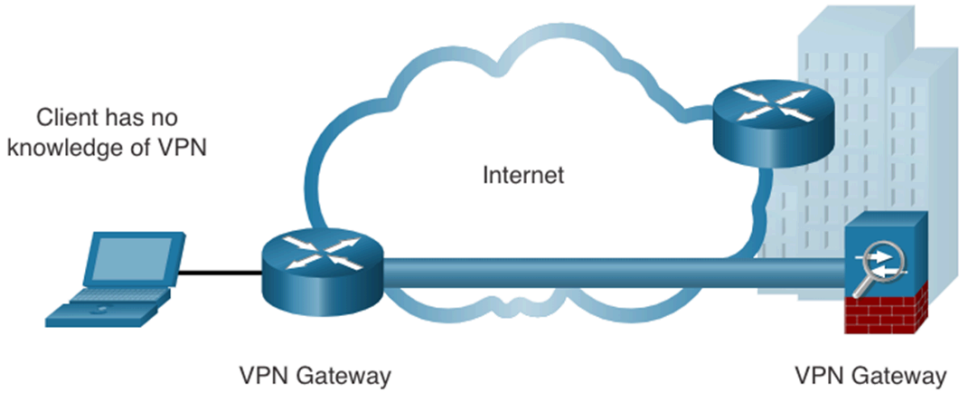
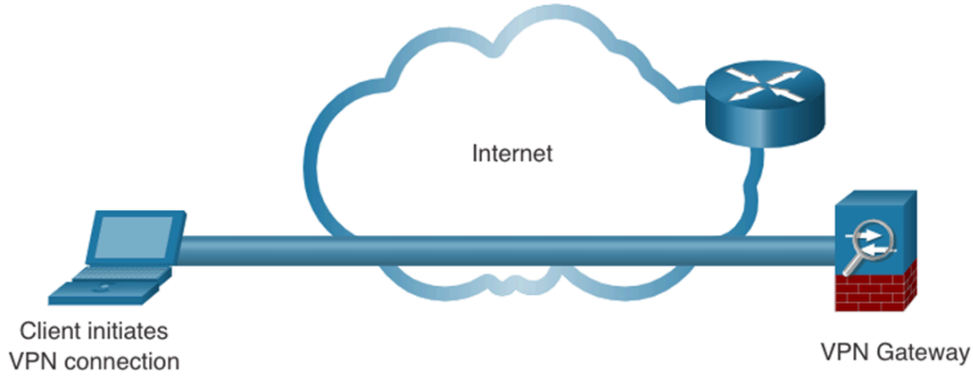
Virtual Private Networks

- Virtual private networks (VPNs) to **create end-to-end private network connections**.
- VPN is virtual in that it **carries information within a private network**, but that **information is actually transported over a public network**
- A VPN is private in that the **traffic is encrypted to keep the data confidential** while it is **transported across the public network**

Benefit	**Description**
Cost Savings	Organizations can use VPNs to **reduce their connectivity costs** while simultaneously **increasing remote connection bandwidth**
Security	**Encryption** and **authentication protocols protect data from unauthorized access**
Scalability	VPNs **allow organizations to use the internet**, making it **easy to add new users without adding significant infrastructure**
Compatibility	• VPNs can be **implemented across a wide variety of WAN link options** including broadband technologies • **Remote workers can use these high-speed connections to gain secure access to corporate network**

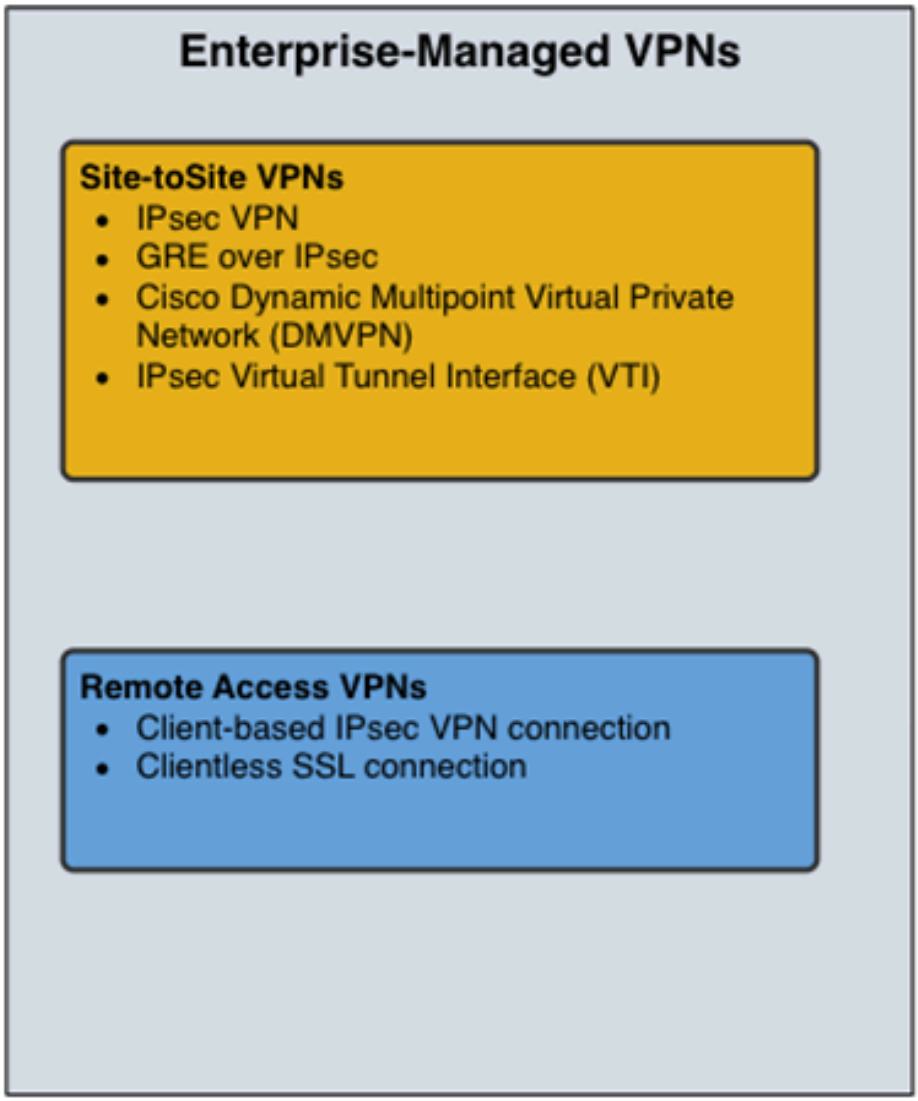
Site-to-Site and Remote Access VPNs

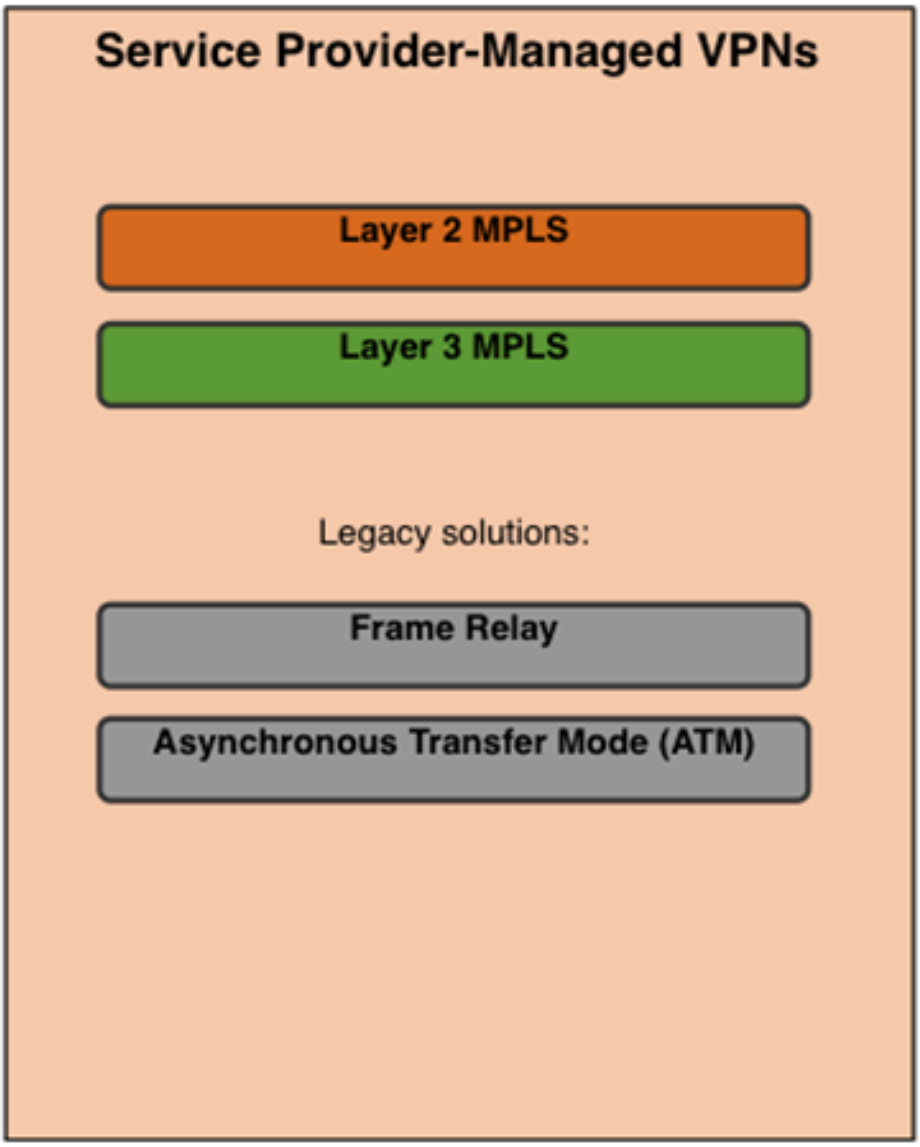
Site-to-Site VPN	• A site-to-site VPN is **terminated on VPN gateways** • **VPN traffic is only encrypted between gateways** • **Internal hosts have no knowledge that a VPN is being used**

	
Remote-Access VPN	• A remote-access VPN is **dynamically created to establish a secure connection between a client and a VPN terminating device** 

Enterprise and Service Provider VPNs

Enterprise VPNs	• Common solution for **securing enterprise traffic across the internet** • **Site-to-site and remote access VPNs are created and managed by the enterprise using IPsec and SSL VPNs**

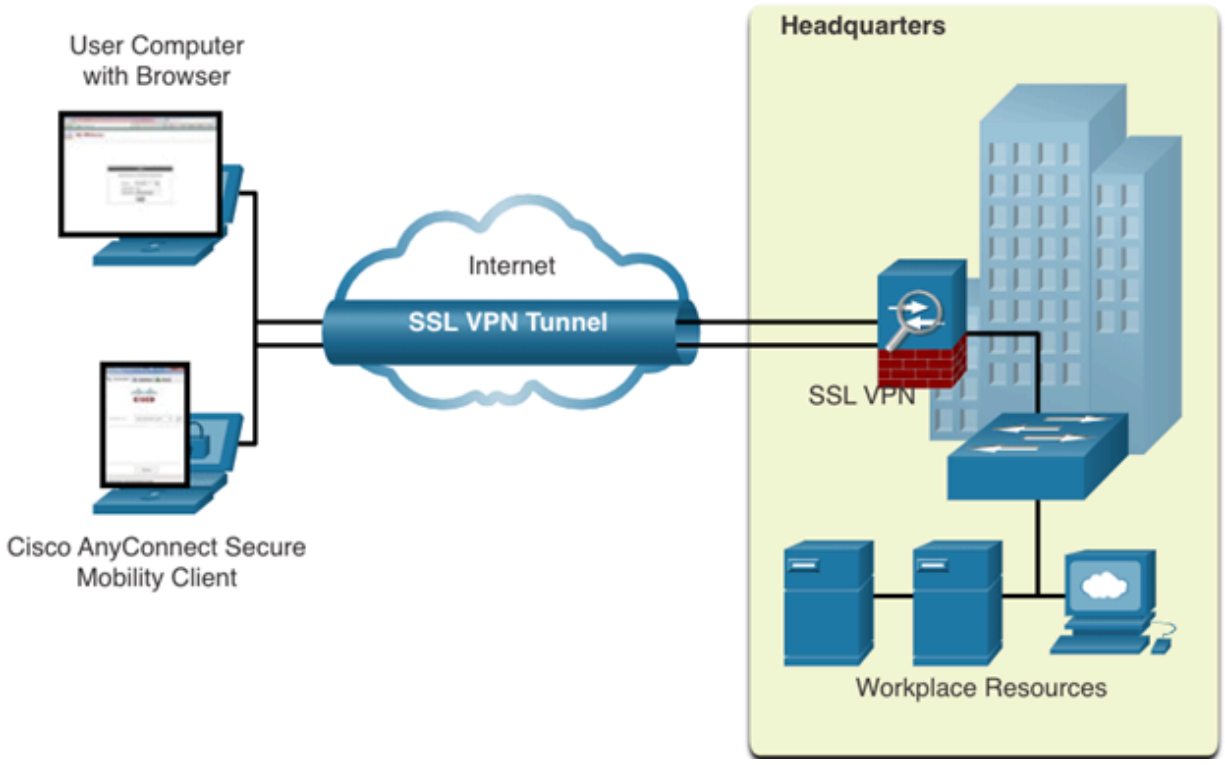
	
Service Provider VPNs	• **Created and managed by the provider network** • The provider uses **Multiprotocol Label Switching (MPLS) at Layer 2 or Layer 3** to **create secure channels between an enterprise's sites**, effectively **segregating 隔离 the traffic from other customer traffic**



Types of VPNs

Remote-Access VPNs

- Let **remote and mobile users securely connect to the enterprise**
- **Enabled dynamically by the user** when required and can be **created using either IPsec or SSL**



Clientless VPN connection	The **connection is secured using a web browser SSL connection**
Client-based VPN connection	**VPN client software** such as Cisco AnyConnect Secure Mobility Client must be **installed on the remote user's end device**

SSL VPNs

- SSL uses the **public key infrastructure** and **digital certificates** to **authenticate peers**
- Type of VPN method implemented based on access requirements of the users and organization's IT processes

Feature	**IPsec**	**SSL**
Application supported	**Extensive** - All IP-based applications	**Limited** - Only web-based applications and file sharing
Authentication strength	**Strong** - Two-way authentication with shared keys or digital certificates	**Moderate** - One-way or two-way authentication
Encryption	**Strong** - Key lengths 56 - 256 bits	**Moderate to strong** - Key lengths

strength		40 - 256 bits
Connection complexity	**Medium** - Requires VPN client installed on a host	**Low** - Requires web browser on a host
Connection option	**Limited** - Only specific devices with specific configurations can connect	**Extensive** - Any device with a web browser can connect

Site-to-Site IPsec VPNs

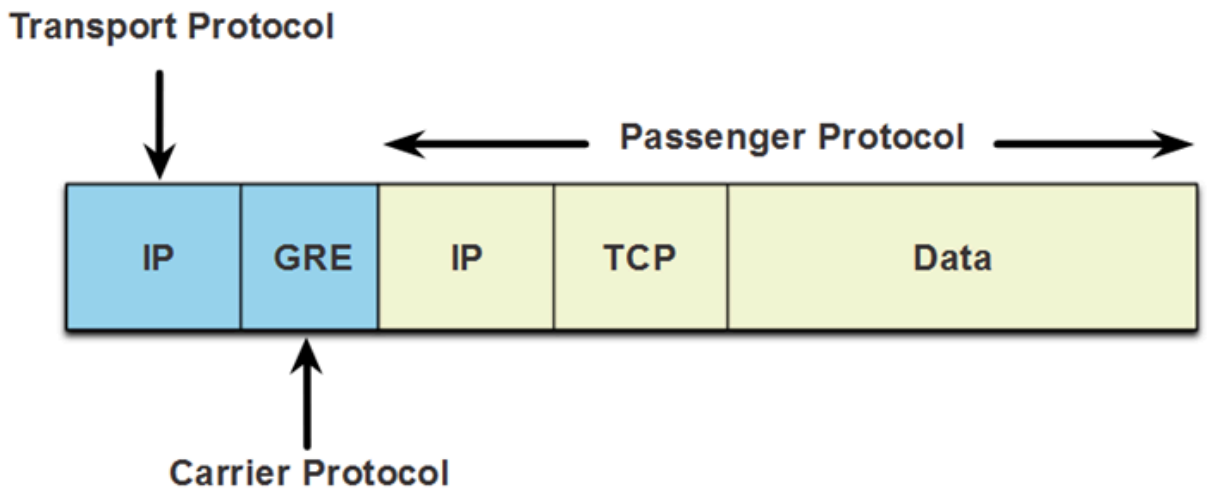
- Site-to-site VPNs **connect networks across an untrusted network** such as the internet
- **End hosts send and receive normal unencrypted TCP/IP traffic through a VPN gateway**
- The **VPN gateway encapsulates and encrypts outbound traffic from a site** and **sends the traffic through the VPN tunnel to the VPN gateway at the target site**
- The **receiving VPN gateway strips the headers**, **decrypts the content** and **relays the packet toward the target host inside its private network**

GRE over IPsec

- Generic Routing Encapsulation (GRE) is a **non-secure site-to-site VPN tunneling protocol**
- A GRE tunnel can **encapsulate various network layer protocols** as well as multicast and broadcast traffic
- GRE **does not by default support encryption**; and therefore, it does **not provide a secure VPN tunnel**
- A **GRE packet can be encapsulated into an IPsec packet** to **forward it securely to the destination VPN gateway**
    - **Standard IPsec VPNs** (non-GRE) can only **create secure tunnels for unicast traffic**
    - **Encapsulating GRE into IPsec** allows **multicast routing protocol updates to be secured through a VPN**

Terms used to describe the encapsulation of GRE over IPsec tunnel:	
Passenger protocol	• This is the **original packet that is to be encapsulated by GRE** • It could be an **IPv4 or IPv6 packet**, a **routing update** and more

Carrier protocol	GRE is the **carrier protocol that encapsulates the original passenger packet**
Transport protocol	• This is the **protocol that will actually be used to forward the packet** • This could be **IPv4 or IPv6**



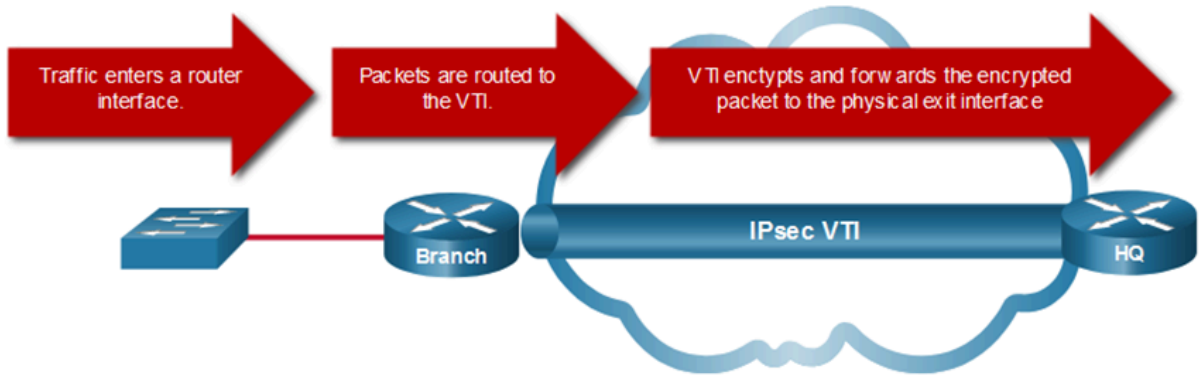
Dynamic Multipoint VPNs

Key Point	Description
Definition	DMVPN is a Cisco software solution for **building multiple VPNs in an easy, dynamic, and scalable manner**.
Purpose	**Simplifies VPN tunnel configuration** and **provides a flexible option to connect a central site with branch sites**.
Topology Type	Uses a **hub-and-spoke configuration** to establish a full mesh topology.
Connection Setup	Spoke sites establish secure VPN tunnels with the hub site.
Tunnel Configuration	Each site is configured using Multipoint Generic Routing Encapsulation (mGRE).
mGRE Function	Allows a single GRE interface to dynamically support multiple IPsec tunnels.
Spoke-to-Spoke	Spoke sites can obtain information about each other and build

Communication	direct tunnels between themselves.

IPsec Virtual Tunnel Interface

- IPsec Virtual Tunnel Interface (VTI) **simplifies the configuration process required to support multiple sites and remote access**
- IPsec VTI configurations are **applied to a virtual interface** instead of static mapping the IPsec sessions to a physical interface
- IPsec VTI is capable of **sending and receiving both IP unicast and multicast encrypted traffic**. Therefore, routing protocols are automatically supported without having to configure GRE tunnels
- IPsec VTI can be **configured between sites or in a hub-and-spoke topology**



Service Provider MPLS VPNs

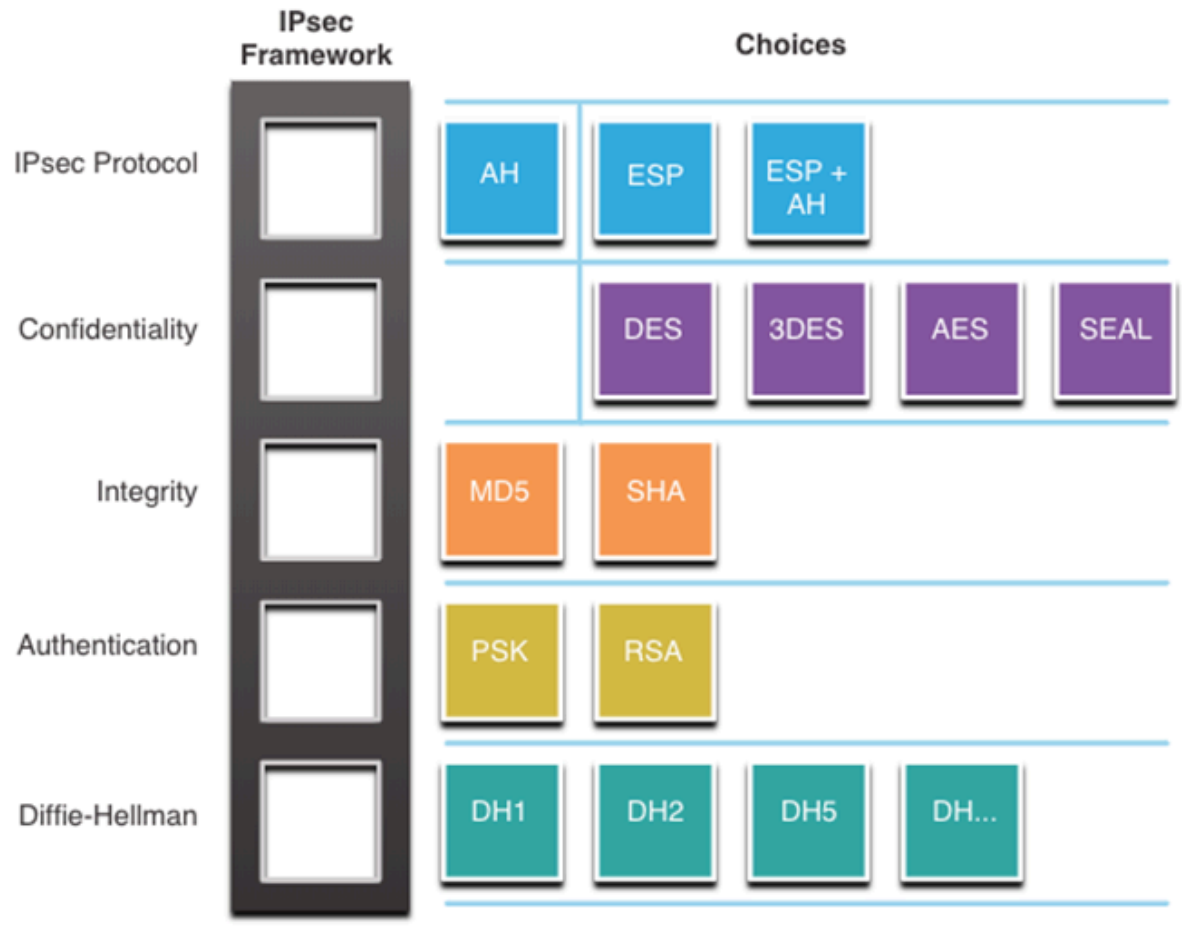
- Traffic is forwarded through the MPLS backbone using labels
- Traffic is secure because service provider customers cannot see each other's traffic
- MPLS provides clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider

2 types of MPLS VPN solutions supported by service providers:

Layer 3 MPLS VPN	• The **service provider participates in customer routing** by **establishing a peering between the customer's routers and the provider's routers**
Layer 2 MPLS VPN	• The **service provider is not involved in the customer routing** • Instead, the **provider deploys a Virtual Private LAN**

	Service (VPLS) to emulate an Ethernet multiaccess LAN segment over the MPLS network • **No routing is involved** • The **customer's routers effectively belong to the same multiaccess network**

IPsec



- IPsec is an IETF standard that **defines how a VPN can be secured across IP networks**
- IPsec is **not bound to any specific rules for secure communications**
- IPsec can easily **integrate new security technologies without updating existing IPsec standards**
- The open slots in the IPsec framework can be filled with any of the choices that are available for that IPsec function to create a unique security association (SA)
- Choosing the IPsec protocol encapsulation is the first building block of the framework

<table>
<tr><td colspan="2">

IPsec encapsulates packets using Authentication Header (AH) or Encapsulation Security Protocol (ESP)
The choice of AH or ESP establishes which other building blocks are available

AH is appropriate only when confidentiality is not required or permitted
ESP providers both confidentiality and authentication

IPsec protects and authenticates IP packets between source and destination and providers these essential security functions:

</td></tr>
<tr><td>Confidentiality</td><td>

The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm
Number of possibilities to try to hack the key is a function of the length of the key (the shorter the key, the easier it is to break)
Encryption algorithms applied in symmetric key cryptosystems:

DES uses a 56-bit key
3DES uses 3 independent 56-bit encryption keys per 64-bit block
AES offers 3 different key lengths: 128 bits, 192 bits, and 256 bits
SEAL is a stream cipher, which means it encrypts data continuously rather than encrypting blocks of data. SEAL uses a 160-bit key

</td></tr>
<tr><td>Integrity</td><td>

Data integrity means that the data has not changed in transit
Hashed Message Authentication Code (HMAC) is a data integrity algorithm that guarantees the integrity of the message using a hash value
Message-Digest 5 (MD5) uses a 128-bit shared-secret key. MD5 is no longer secure and should be avoided
Secure Hash Algorithm (SHA0 uses a 160-bit secret key and are more secure

</td></tr>
<tr><td>Origin authentication</td><td>2 IPsec peer authentication methods:

Pre-shared key (PSK)

PSK value is entered into each peer manually
Easy to configure manually
Does not scale well
Must be configured on every peer

Rivest, Shamir, and Adleman (RSA)

Authentication uses digital certificates to authenticate

</td></tr>
</table>

	the peers ○ Each peer must authenticate its opposite peer before the tunnel is considered secure
Diffie-Hellman	● DH **allows two peers to establish a shared secret key over an insecure channel** ● Variations of DH key exchange are specified as DH groups: ○ DH groups 1, 2 and 5 should no longer be used ○ DH groups 14, 15 and 16 use larger key sizes with 2048 bits, 3072 bits, and 4096 bits, respectively ○ DH groups 19, 20, 21 and 24 with respective key sizes of 256 bits, 384 bits, 521 bits and 2048 bits support Elliptical Curve Cryptography (ECC), which reduces the time needed to generate keys

C8: WAN Concepts

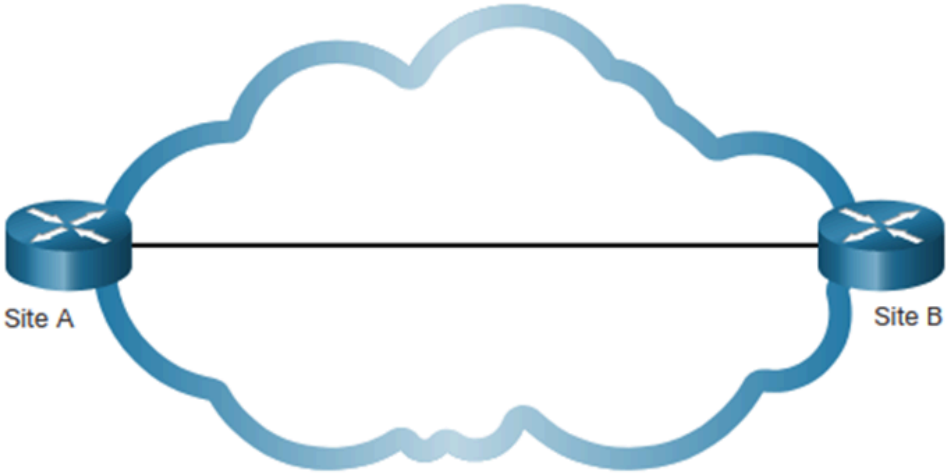
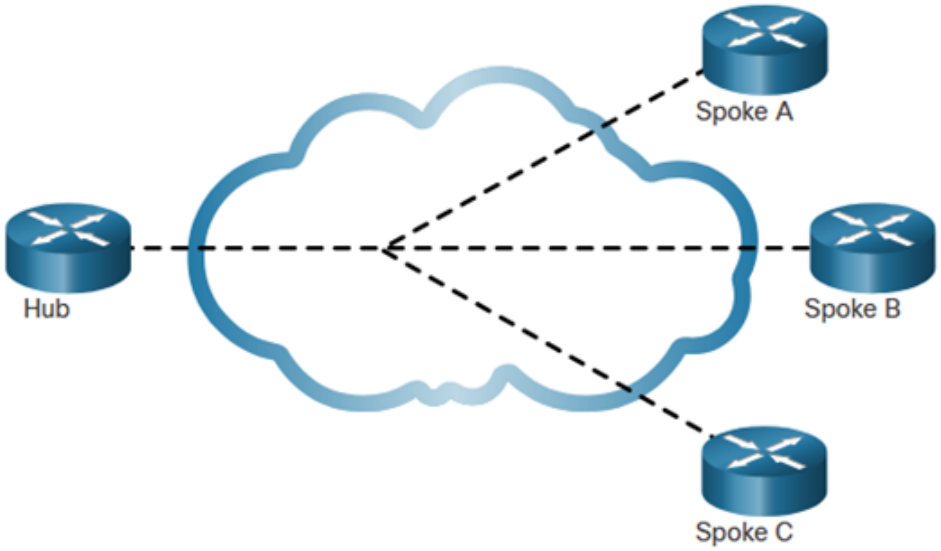
Purpose of WANs

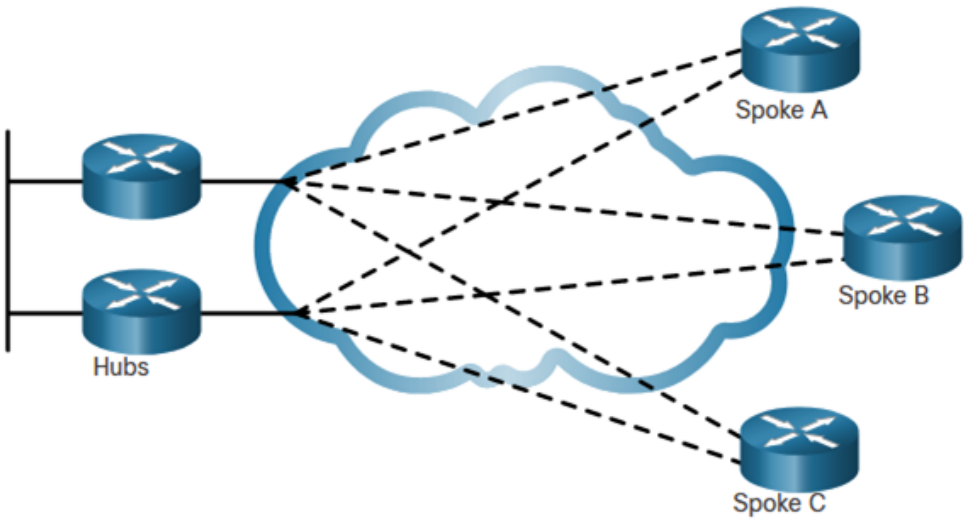
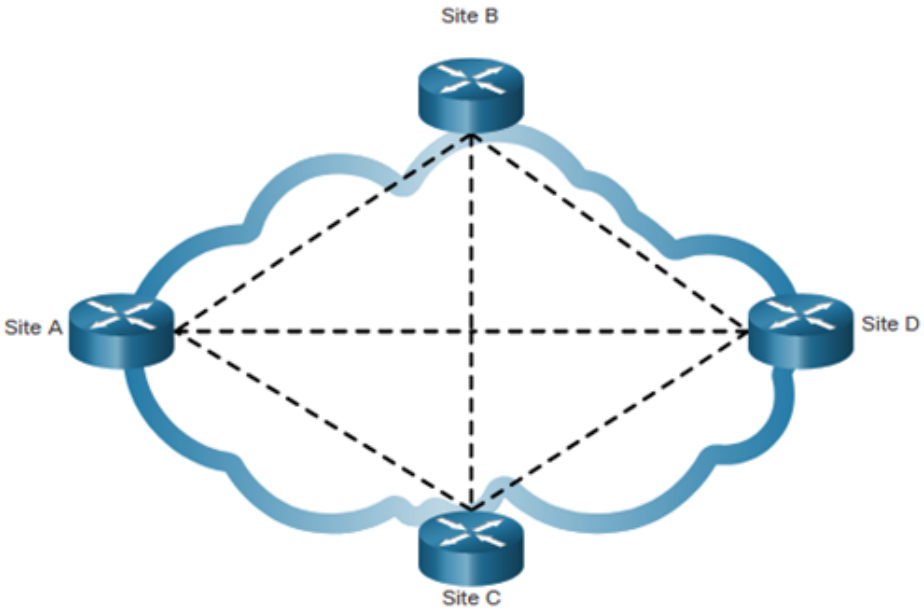
WAN is a **telecommunications network that spans over a relatively large geographical area** and is required to **connect beyond the boundary of the LAN**	
Local Area Networks (LANs)	**Wide Area Networks (WANs)**
LANs provide networking services within a **small geographic area**	WANs provide networking services over **large geographic areas**
LANs are used to **interconnect local computers, peripherals and other devices**	WANs are used to **interconnect remote users, networks and sites**
A LAN is **owned and managed by an organization or home user**	WANs are **owned and managed by internet service, telephone, cable and satellite providers**
Other than the network infrastructure costs, there is **no fee to use a LAN**	WAN services are **provided for a fee**
LANs provide **high bandwidth speeds** using **wired Ethernet** and **Wi-Fi services**	WANs providers offer l**ow to high bandwidth speeds**, over **long distances**

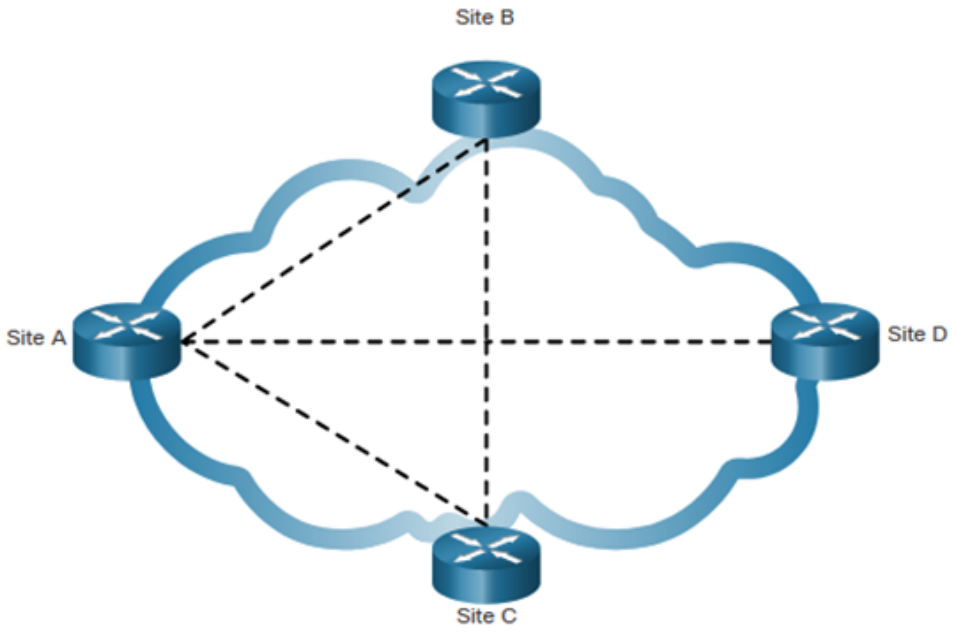
• Private WAN is a connection that is dedicated to single customer
  ○ **Guaranteed service level**
  ○ **Consistent bandwidth**
  ○ **Security**
• Public WAN connection is provided by an ISP or telecommunications service provider using the internet (Service levels and bandwidth may vary, and the shared connections do not guarantee security)	

WAN Topologies (5)

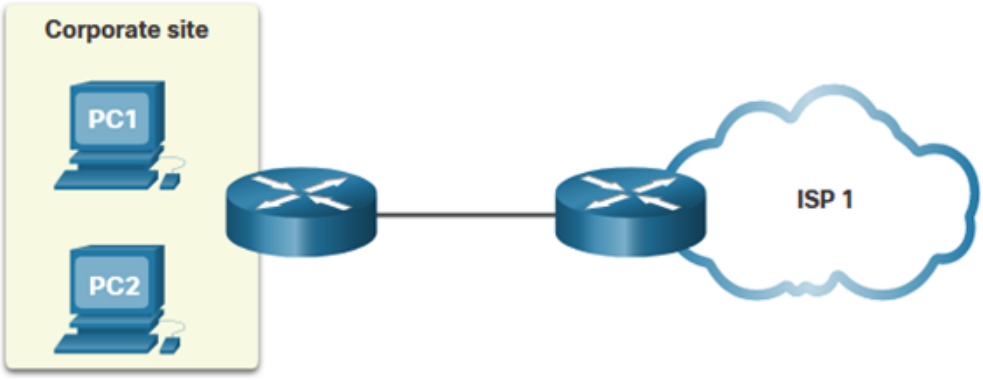
Point-to-Point Topology	• Employs a **point-to-point circuit between two endpoints** • Involves a **Layer 2 transport service through the service provider network** • The point-to-point connection is **transparent to the customer network** • It may become expensive if many point-to-point connections are

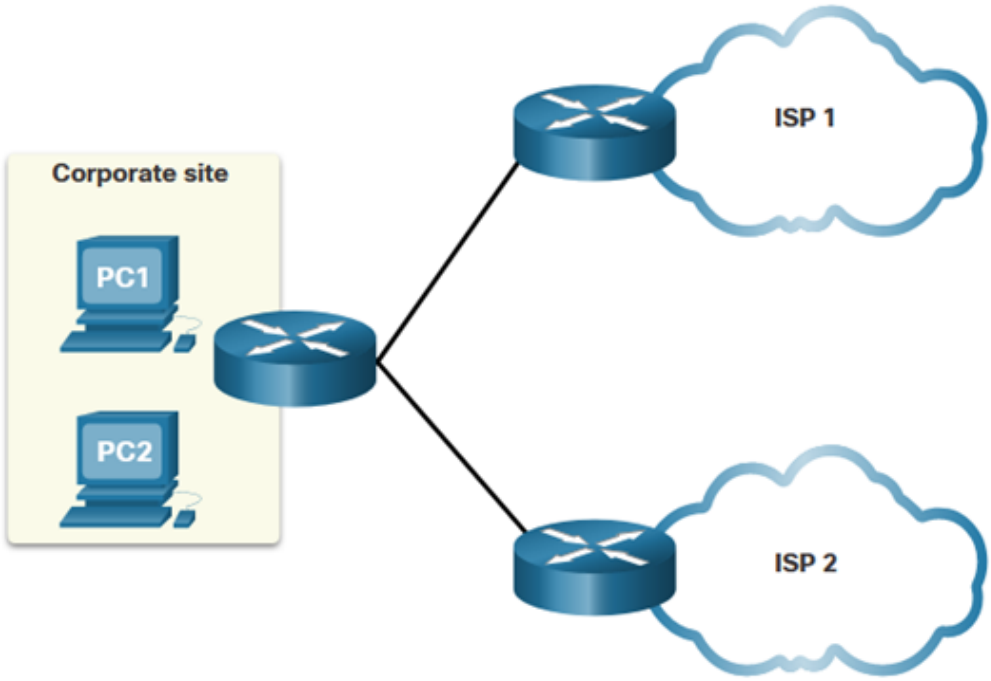
	required 
Hub-and-Spoke Topology	• **Enables a single interface on the hub router to be shared by all spoke circuits** • **Spoke routers can be interconnected through the hub router using virtual circuits and routed subinterfaces** • **Spoke routers** can only **communicate with each other through the hub router** • The hub router represents a single point of failure. If it fails, inter-spoke communication also fails 
Dual-homed Topology	• Offers **enhanced network redundancy, load balancing, distributed computing and processing**, and the ability to **implement backup service provider connections** • **More expensive** to implement than single-homed topologies.

	This is because they **require additional networking hardware** such as additional routers and switches • More difficult to implement because they require additional and more complex configurations 
Fully Meshed Topology	• **Uses multiple virtual circuits to connect all sites** • The **most fault-tolerant** topology 
Partially Meshed Topology	• **Connects many but not all sites**

Carrier Connections

Single-Carrier Connection	• Single-carrier connection is when an **organization connects to only one service provider** • An **service level agreement (SLA) is negotiated between the organization and the service provider** 
Dual-Carrier Connection	• Dual-carrier connection **provides redundancy and increases network availability** • The **organization negotiates separate SLAs with two different service providers**

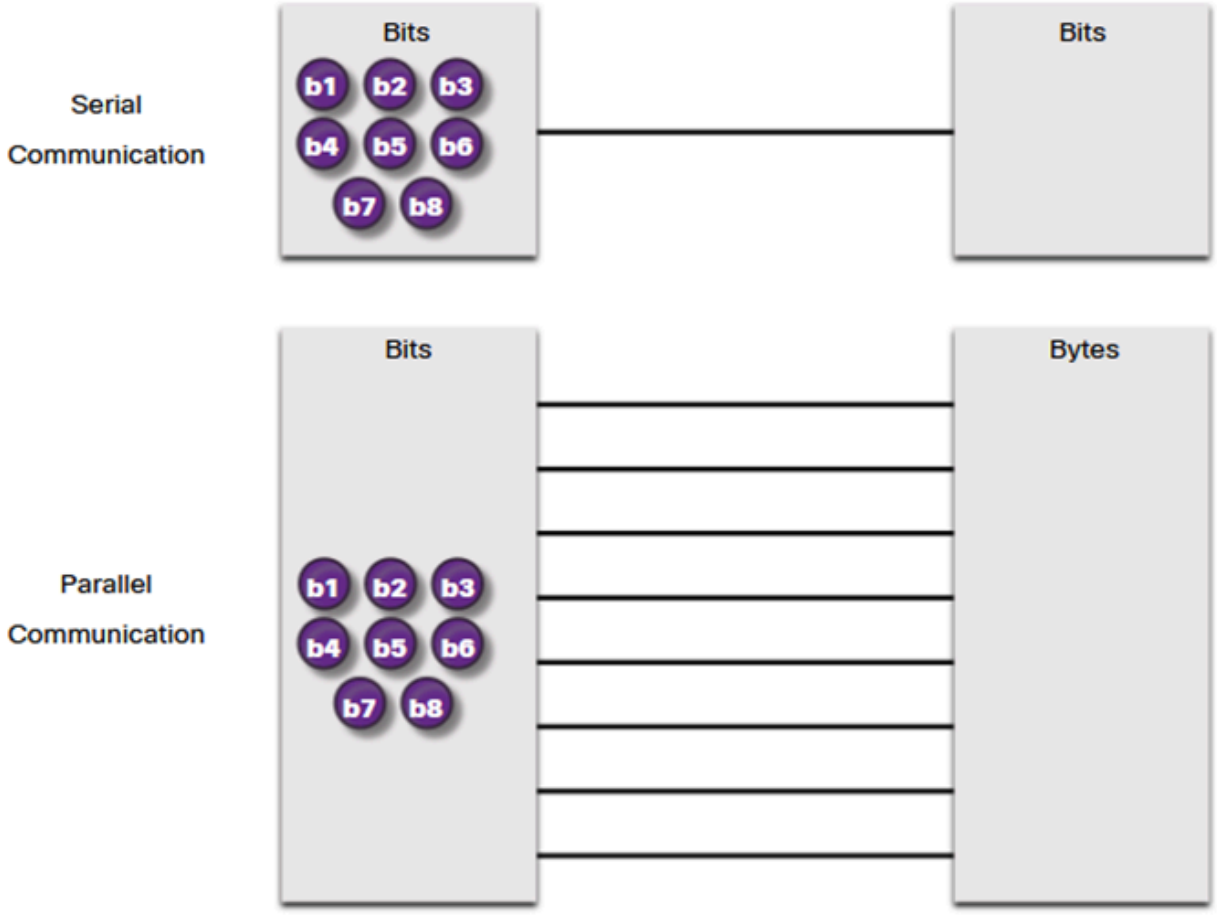
Evolving Networks

Small Network	• SPAN, a small fictitious company, started with a few employees in a small office • Uses a single LAN connected to a wireless router for sharing data and peripherals • Connection to the internet is through a common broadband service called Digital Subscriber Line (DSL) • IT support is contracted from the DSL provider
Campus Network	• Within a few years SPAN grew and required several floors of a building • The company now required a Campus Area Network (CAN) • A firewall secures internet access to corporate users • In-house IT staff to support and maintain the network
Branch Network	• A few years later, the company expanded and added a branch site in the city, and the remote and regional sites in other cities • The company now required a metropolitan area network (MAN) to interconnect sites within the city • To connect to the central office, branch offices in nearby cities used private dedicated lines through their local service

	provider
Distributed Network	• SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide • Site-to-site and remote access Virtual Private Networks (VPNs) enable the company to use the internet to connect easily and securely with employees and facilities around the world

Serial Communication

- Serial communication **transmits bits sequentially over a single channel**
- Parallel communications **simultaneously transmit several bits using multiple wires**
- As the **cable length increases**, the **synchronization timing between multiple channels becomes more sensitive to distance**. For this reason, **parallel communication is limited to very short distances**



Circuit-Switched Communication

- Circuit-switched network **establishes a dedicated circuit (or channel) between endpoints before the users can communicate**
- **Establishes a dedicated virtual connection through the service provider network before communication can start**
- **All communications uses the same path**
- The two most common types of circuit-switched WAN technologies are the public switched telephone network (PSTN) and the legacy Integrated Services Digital Network (ISDN)

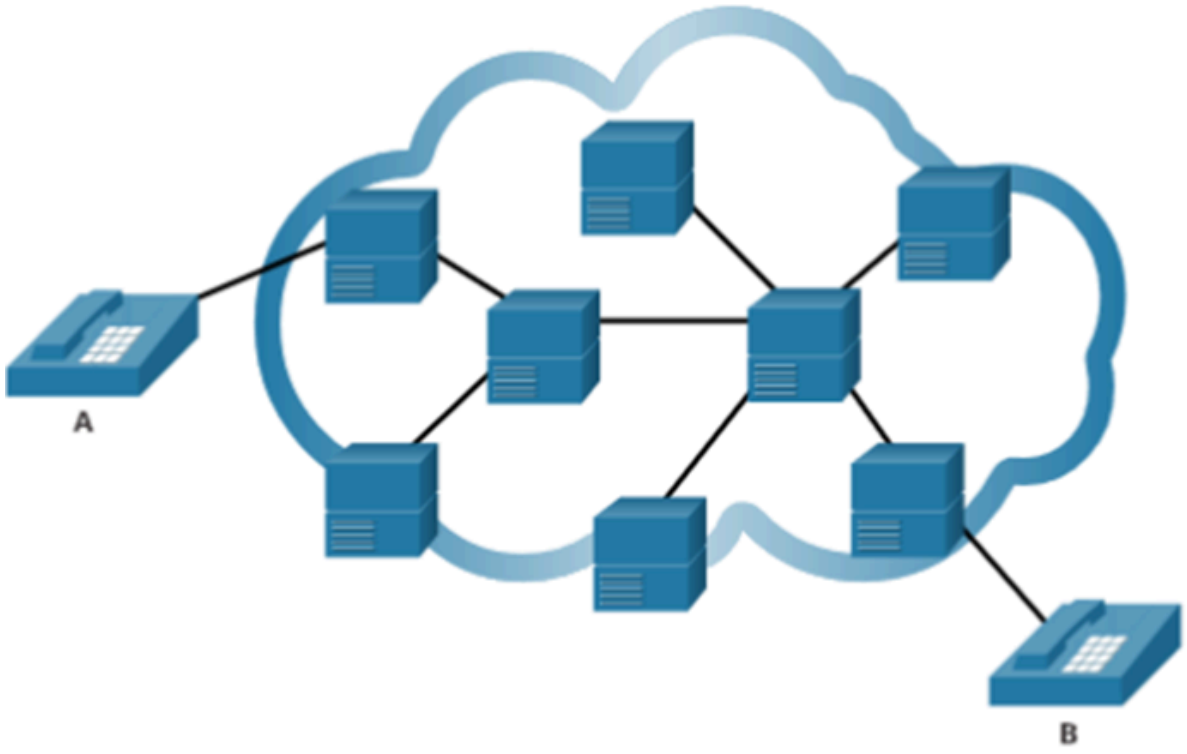
Definition: A dedicated communication path is established between two endpoints for the duration of the session.

✅ **Key Characteristics:**

- **Fixed path**: Once the circuit is established, all data follows the same route.
- **Continuous connection**: Resources are reserved for the entire session.
- **Used in**: Traditional telephone networks (e.g., landline calls).
- **Latency**: Low and predictable.
- **Efficiency**: Less efficient — the circuit remains reserved even when no data is being transmitted.

📞 **Example:**

- Making a phone call on a landline: a dedicated line is reserved between you and the person you're calling.



- Network communication most commonly implemented using packet-switched communication
- **Segments traffic data into packets that are routed over a shared network**
- Much **less expensive** and **more flexible than circuit switching**
- Common types of packet-switched WAN technologies are:
    - Ethernet WAN (Metro Ethernet)
    - Multiprotocol Label Switching (MPLS)
    - Frame Relay
    - Asynchronous Transfer Mode (ATM)

Definition: Data is broken into packets and each packet is sent independently through the network.

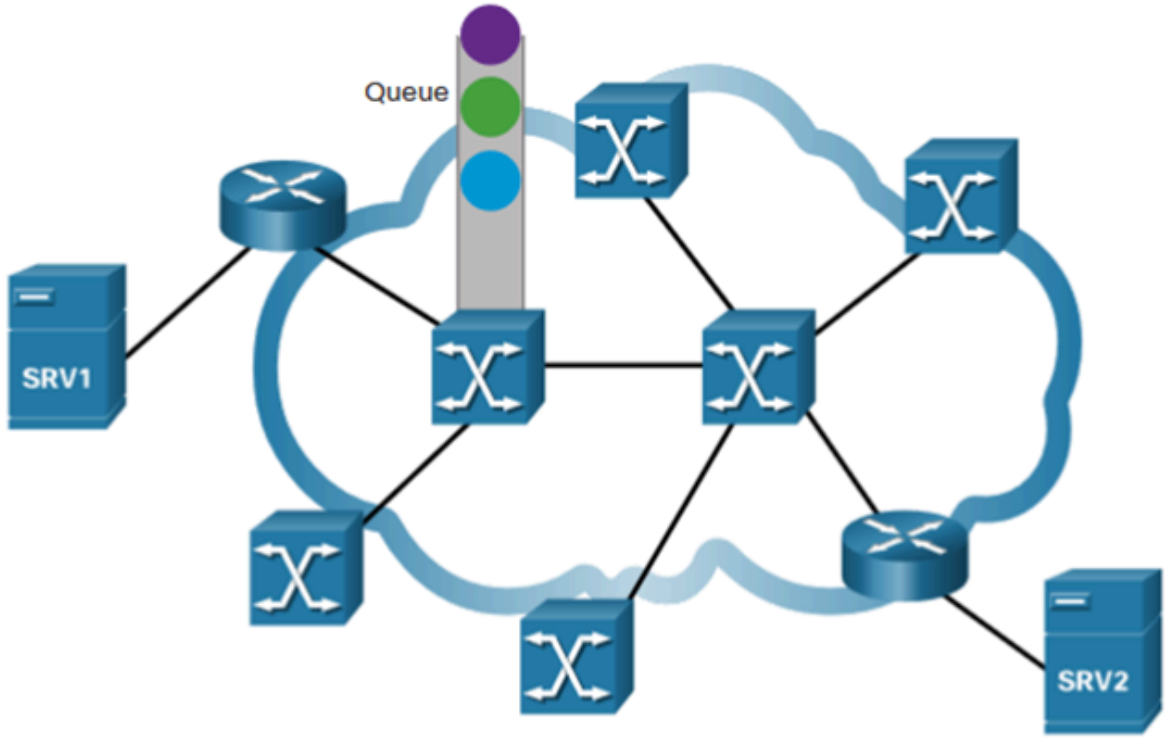
✅ **Key Characteristics:**

- **Dynamic routing**: Packets may take different paths to reach the destination.
- **No dedicated path**: Network resources are shared among users.
- **Used in**: Internet, email, VoIP, streaming.
- **Latency**: Can vary depending on network congestion.
- **Efficiency**: Highly efficient — resources are used only when data is being

transmitted.

🌐 **Example:**

- Sending an email or browsing a website: data is split into packets and routed through various paths to reach the server.



Traditional WAN Connectivity

Leased Lines

- **Point-to-point lines could be leased from a service provider** called as "leased lines"
- The term refers to the fact that **organization pays a monthly lease fee to a service provider to use the line**
- 2 systems used to define digital capacity of a copper media serial link:
  - T-carrier
  - E-carrier

Advantages

Simplicity	Point-to-point communication links require **minimal expertise to install and maintain**
Quality	Point-to-point communication links usually offer **high quality service, if they have adequate bandwidth**
Availability	• **Constant availability** is essential for some applications such as e-commerce • Point-to-point communication links provide **permanent, dedicated capacity** which is required for VoIP or Video over IP
Disadvantages	
Cost	• Point-to-point links are generally the **most expensive type of WAN access** • The cost of leased line solutions can become significant when they are used to **connect many sites over increasing distances**
Limited flexibility	WAN traffic is often variable, and leased lines have a fixed capacity, so that the **bandwidth of the line seldom matches the need exactly**

Circuit-Switch Options

- Circuit-switched connections are provided by Public Service Telephone Network (PSTN) carriers
- The local loop connecting the CPE to the CO is copper media
- There are 2 traditional circuit-switched options:
    - Public Service Telephone Network (PSTN)
    - Integrated Services Digital Network (ISDN)

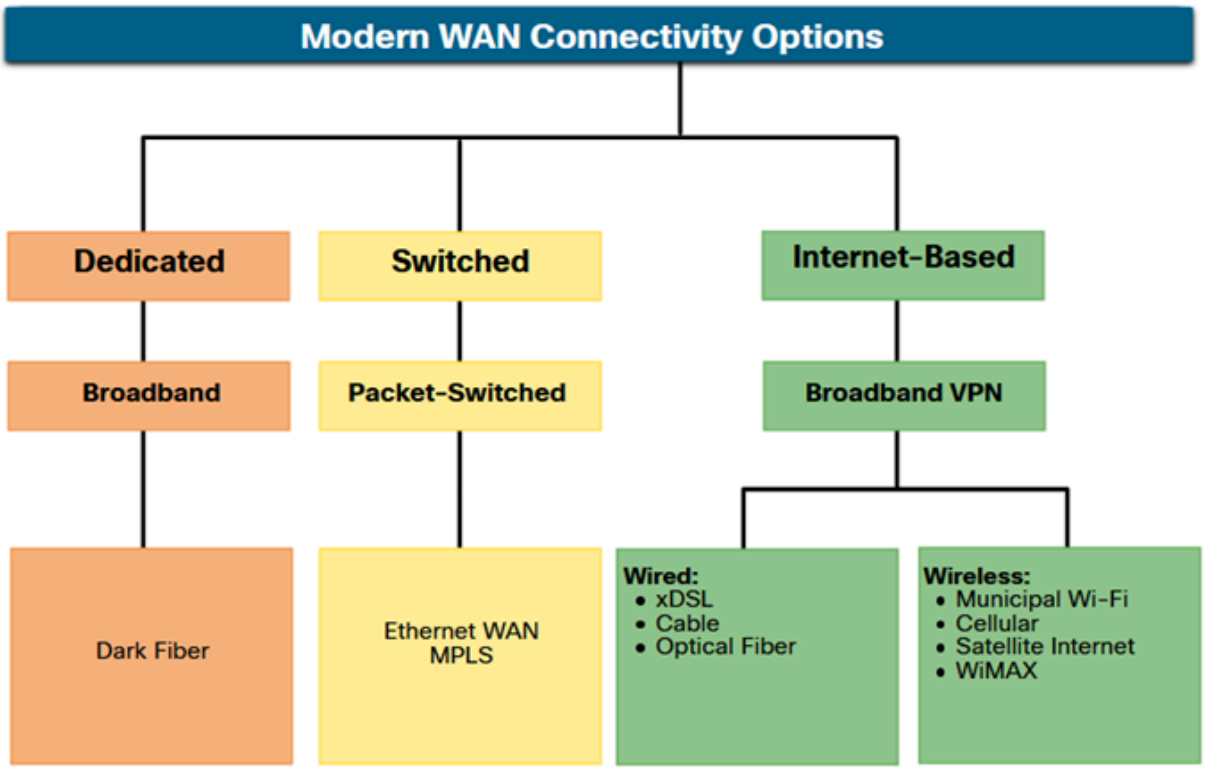
Public Service Telephone Network (PSTN)	• Dialup WAN access uses the PSTN as its WAN connection • Traditional local loops can transport binary computer data through the voice telephone network using a voiceband modem • THe physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 kbps
Integrated Services Digital Network (ISDN)	• ISDN is a circuit-switching technology that enables the PSTN local loop to carry digital signals • This provide higher capacity switched connections

	than dialup access ● ISDN provides for data rates from 45 Kbps to 2.048 Mbps

Packet-Switch Options

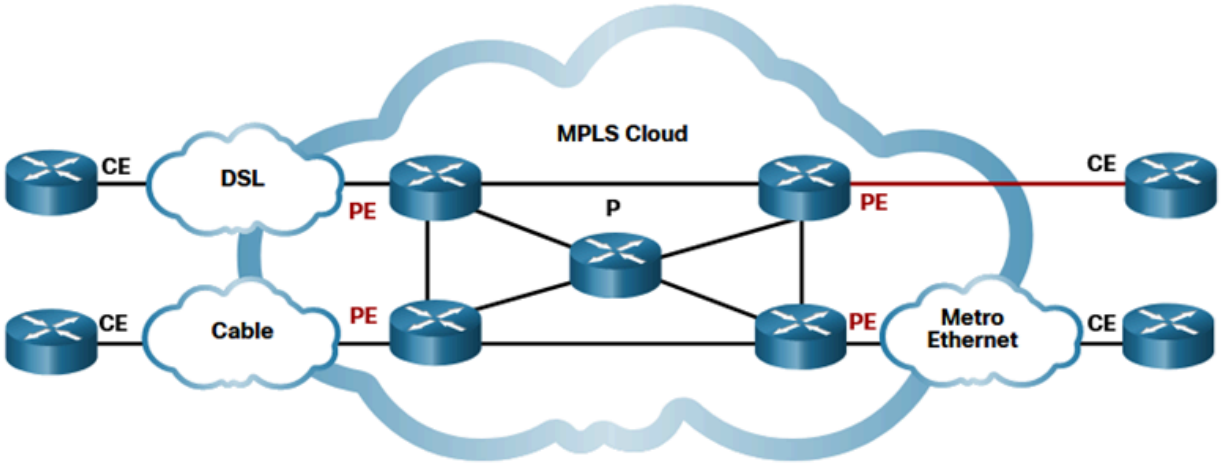
● Packet switching segments data into packets that are routed over a shared network ● It allows many pairs of nodes to communicate over the same channel ● There are 2 traditional (legacy) circuit-switched options: ○ Frame Relay ○ synchronous Transfer Mode (ATM)	
Frame Relay	● Frame Relay is a simple Layer 2 non-broadcast multi-access (NBMA) WAN technology that is used to interconnect enterprise LANs ● Frame Relay created PVCs which are uniquely identified by a data-link connection identifier (DLCI)
Asynchronous Transfer Mode (ATM)	● Asynchronous Transfer Mode (ATM) technology is capable of transferring voice, video and data through private and public networks ● ATM is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes

Modern WAN Connectivity



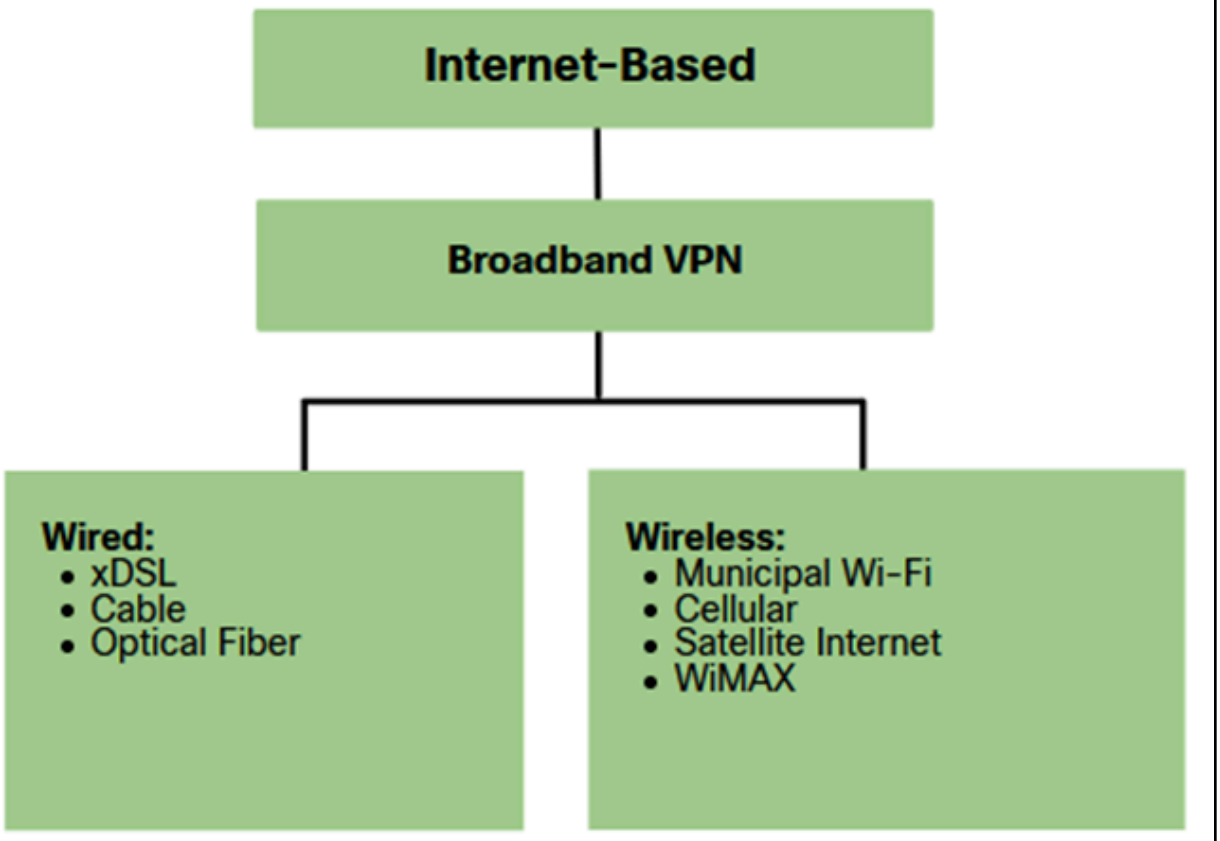
Dedicated broadband	• **Fiber can installed independently by an organization** to **connect remote locations directly together** • **Dark fiber** can be **leased or purchased from a supplier**
Packet-switched	• **Metro Ethernet**: replacing many traditional WAN options • **MPLS**: enables sites to connect to the provider regardless of its access technologies
Internet-based broadband	• Organizations are now commonly using the global internet infrastructure for WAN connectivity

MPLS



- Multiprotocol Label Switching (MPLS) is a high-performance service provider WAN routing technology to **interconnect clients without regard to access method or payload**
- MPLS **supports a variety of client access methods** (e.g. Ethernet, DSL, Cable, Frame Relay)
- MPLS can **encapsulate all types of protocols including IPv4 and IPv6 traffic**
- An **MPLS router can be a customer edge (CE) router, provider edge (PE) router, or an internal provider (P) router**
- MPLS routers are label switched routers (LSRs). They **attach labels to packers that are then used by other MPLS routers to forward traffic**
- MPLS **provides services for QoS support, traffic engineering, redundancy and VPNs**

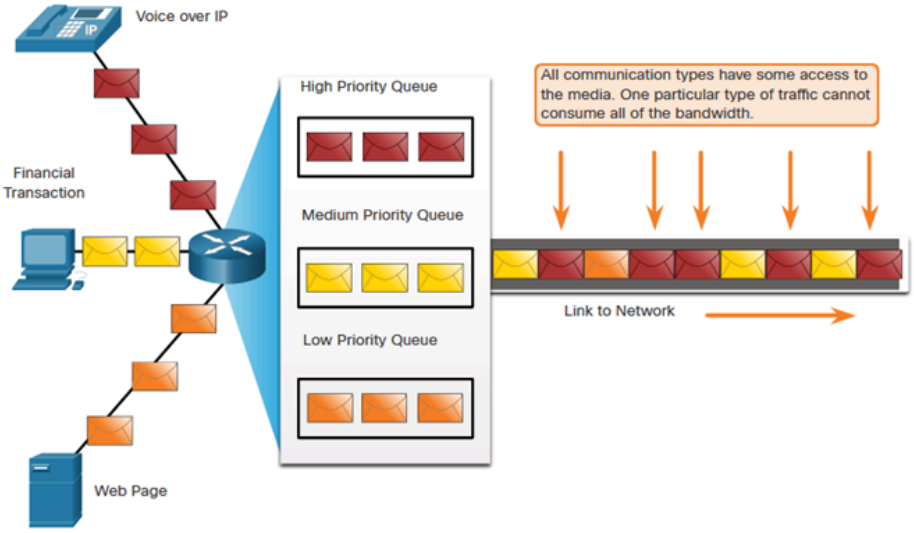
Internet-Based Connectivity

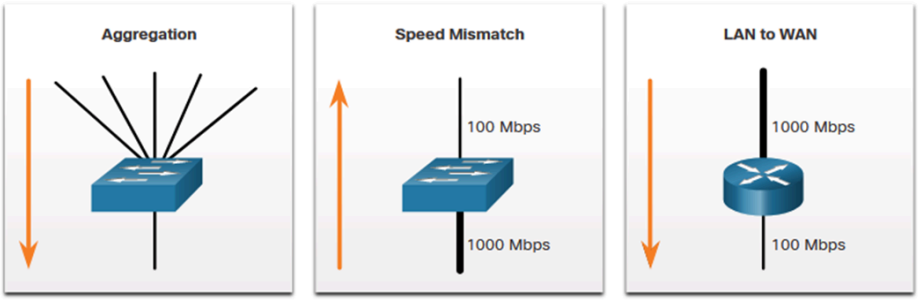


Wired Options	• Wired options use **permanent cabling** (e.g. copper or fiber) • To **provide consistent bandwidth**, and **reduce error rates and latency** • e.g. DSL, cable connections, and optical fiber networks
Wireless Options	• Wireless options are **less expensive** to implement compared to other WAN connectivity options because they **use radio waves instead of wired media to transmit data** • e.g. cellular 3G/4G/5G or satellite internet services • Wireless signals can be **negatively affected by** factors such as **distance from radio towers**, **interference from other source and weather**

C9: QoS Concepts

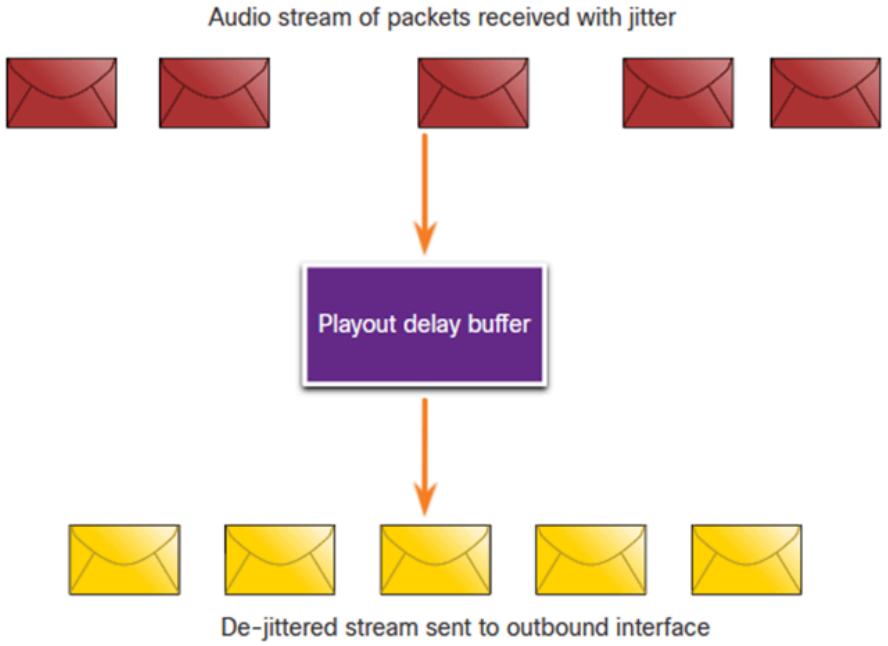
Network Transmission Quality

Prioritizing Traffic	• When traffic volume is greater than what can be transported across the network, devices queue (hold) the packets in memory until resources become available to transmit them • Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed • If the number of packets to be queued continues to increases, the memory within the device fills up and packets are dropped • One QoS technique that can help with this problem is to classify data into multiple queues 
Bandwidth, Congestion, Delay, and Jitter	• Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps) • Network congestion causes delay. An interface experiences congestion when it is presented with more traffic than it can handle. Network congestion points are ideal candidates for QoS mechanisms • The typical congestion points are aggregation, speed mismatch and LAN to WAN



- Delay or latency refers to the time it takes for a packet to travel from the source to the destination
    - Fixed delay is the amount of time a specific process takes, such as how long it takes to place a bit on the transmission media
    - Variable delay takes an unspecified amount of time and is affected by factors such as how much traffic is being processed
    - Jitter is the variation of delay of received packets

Delay	**Description**
Code delay	The fixed amount of time it takes to compress data at the source before transmitting to the first internetworking device, usually a switch
Packetization delay	The fixed time it takes to encapsulate a packet with all the necessary header information
Queuing delay	The variable amount of time a frame or packet waits to be transmitted on the link
Serialization delay	The fixed amount of time it takes to transmit a frame onto the wire
Propagation delay	The variable amount of time it takes for the frame to travel between the source and destination
De-jitter delay	The fixed amount of time it takes to buffer a flow of packets and then send them out in

<table>
<tr><td></td><td><table><tr><td></td><td>evenly spaced intervals</td></tr></table></td></tr>
<tr><td>Packet Loss</td><td>Without QoS mechanisms, time-sensitive packets such as real-time video and voice, are dropped with the same frequency as data that is not time-sensitive
When a router receives a Real-Time Protocol (RTP) digital audio stream for Voice over IP (VoIP), it compensates for the jitter that is encountered using a playout delay buffer
The playout delay buffer buffers these packets and then plays them out in a steady stream
If the jitter is so large that it causes packets to be received out of the range of the play out buffer, the out-of-range packets are discarded and dropouts are heard in the audio
For losses as small as one packet, the digital signal processor (DSP) interpolates what it thinks the audio should be and no problem is audible to the user
When jitter exceeds what the DSP can do to make up for the missing packets, audio problems are heard 
</td></tr>
</table>

Traffic Characteristics

Voice

- Voice traffic is **predictable** and **smooth** and **very sensitive to delays** and **dropped packets**
- Voice packets must receive a **higher priority than other types of traffic**
- Cisco products use the RTP port range 16384 to 32767 to prioritize voice traffic
- Voice can **tolerate a certain amount of latency, jitter and loss without any noticeable effects**
- **Latency** should be **no more than 150 milliseconds (ms)**
- **Jitter** should be **no more than 30 ms**, and **packet loss no more than 1%**
- Voice traffic requires **at least 30 Kbps of bandwidth**

Voice Traffic Characteristics	**One-Way Requirements**
• Smooth • Benign 良性 • Drop sensitive • Delay sensitive • UPD priority	• Latency <= 150 ms • Jitter <= 30 ms • Loss <= 1% • Bandwidth (30 - 128 Kbps)

Video

- Video traffic tends to be **unpredictable**, **inconsistent and bursty** 突发. Compared to voice, video is **less resilient to loss** 抗丢失能力 and has a **higher volume of data per packet**
- The **number and size of video packets varies every 33 ms** based on the content of the video
- **UDP ports** such as 554, are used for the Real-Time Streaming Protocol (RSTP) and should be given **priority over other, less delay-sensitive, network traffic**
- **Latency** should be **no more than 400 milliseconds (ms)**. **Jitter** should be **no more than 50 ms**, and **video packet loss should be no more than 1%**. Video traffic requires **at least 384 Kbps of bandwidth**

Video Traffic Characteristics	**One-Way Requirements**
• Bursty • Greedy • Drop sensitive • Delay sensitive • UPD priority	• Latency <= 200 - 400 ms • Jitter <= 30 - 50 ms • Loss <= 0.1 - 1% • Bandwidth (384 Kbps - 20 Mbps)

Data

- Data applications that have **no tolerance for data loss**, such as email and web pages, **use TCP to ensure that if packets are lost in transit, they will be resent**
- Data traffic can be **smooth** or **bursty**
- Network control traffic is usually **smooth** and **predictable**
- Some TCP applications can consume a large portion of network capacity. FTP will consume as much bandwidth as it can get when you download a large file such as movie or game

Data Traffic Characteristics

- Smooth / bursty
- Benign / greedy
- Drop insensitive
- Delay insensitive
- TCP Retransmits

- Data traffic is relatively **insensitive to drops and delays** compared to voice and video
- Quality of Experience or QoE is important to consider with data traffic
    - Does the data come from an interactive application?
    - Is the data mission critical?

Factor	Mission Critical	Not Mission Critical
Interactive	**Prioritize for the lowest delay of all data traffic** and strive for a **1 to 2 second response time**	Applications could **benefit from lower delay**
Not interactive	**Delay can vary greatly** as long as the **necessary minimum bandwidth is supplied**	**Gets any leftover bandwidth after all voice, video and other data application needs are met**

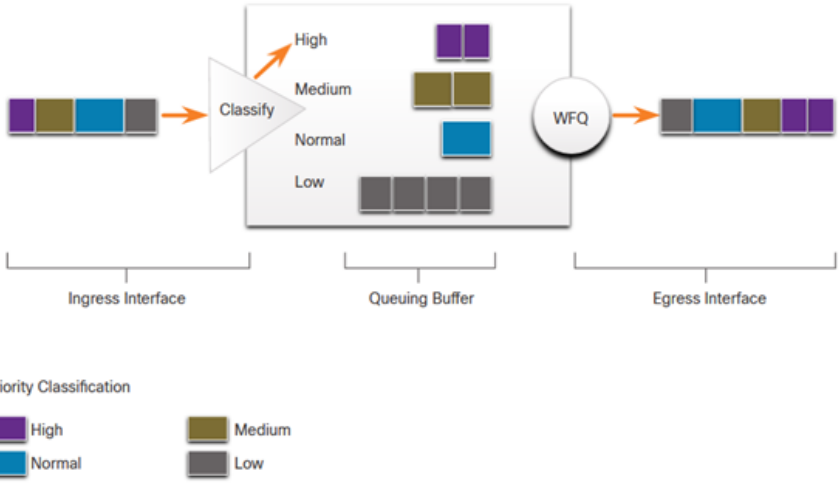
Comparison between Voice, Video and Data Traffic

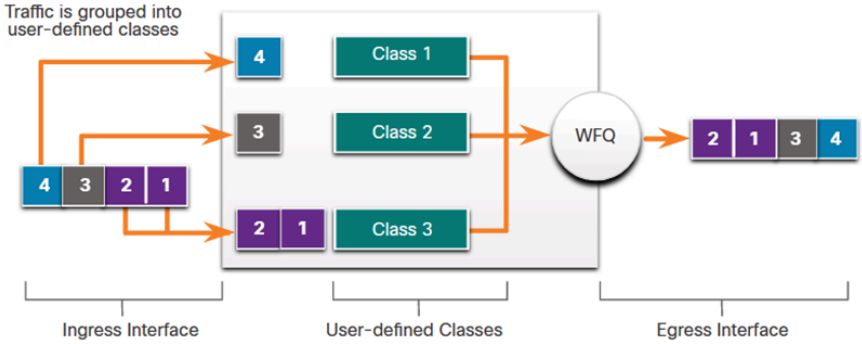
Feature	Voice Traffic	Video Traffic	Data Traffic
Traffic Nature	Predictable and smooth	Unpredictable, inconsistent, and bursty	Can be smooth or bursty
Sensitivity	Very sensitive to delay and packet	Less resilient to loss, but still	Relatively insensitive to delay and loss

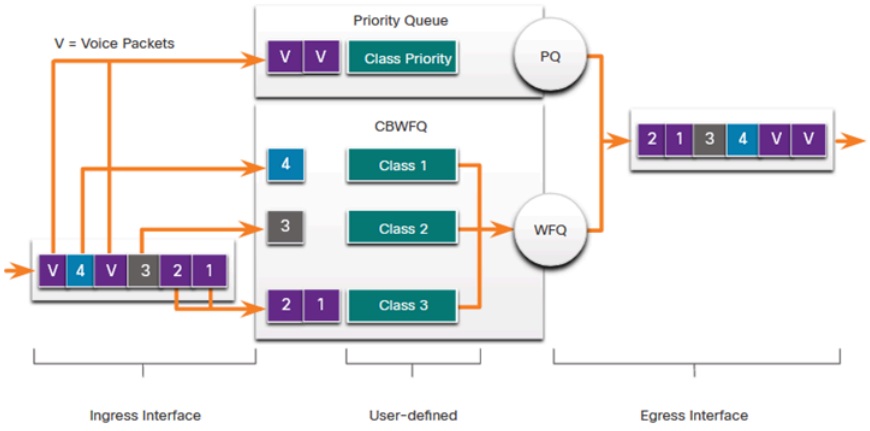
	loss	delay-sensitive	
Protocol / Ports	Uses RTP (UDP ports **16384–32767**)	Uses RSTP (UDP port **554**)	Uses **TCP** (e.g., HTTP, FTP, Email)
Priority Level	Must receive **highest priority**	Should be prioritized over less delay-sensitive traffic	Lower priority compared to voice and video
Latency Limit	≤ **150 ms**	≤ **400 ms**	Not strict
Jitter Limit	≤ **30 ms**	≤ **50 ms**	Not critical
Packet Loss Tolerance	≤ **1%**	≤ **1%**	Handled by TCP retransmission
Bandwidth Requirement	≥ **30 Kbps**	≥ **384 Kbps**	Varies (depends on application)
Typical Behavior	Smooth and consistent packet flow	Bursty, varies every 33 ms depending on video content	May consume large bandwidth (e.g., FTP downloads)
Example Applications	VoIP, IP Phones	Video conferencing, streaming	Email, web browsing, file transfer

Queuing Algorithms

• Queuing is a congestion management tool that can buffer, prioritize, and if required, reorder packets before being transmitted to the destination	
First-In, First-Out (FIFO)	• First In First Out (FIFO) queuing **buffers and forwards packets in the order of their arrival** • FIFO has **no concept of priority or classes of traffic and consequently**, makes no decision about packet priority • There is **only one queue**, and **all packets are treated equally** • **Packets are sent out an interface in the order in which they arrive**

	
Weighted Fair Queuing (WFQ)	• Weighted Fair Queuing (WFQ) is an **automated scheduling method that provides fair bandwidth allocation to all network traffic** • WFQ **applies priority, or weights, to identified traffic**, **classifies it into conversations or flows**, and then **determines how much bandwidth each flow is allowed relative to other flows** • WFQ **classifies traffic into different flows based on source and destination IP addresses, MAC addresses, port numbers, protocol, and Type of Service (ToS) value** • WFQ is **not supported with tunneling and encryption** because these features **modify the packet content information required by WFQ for classification** 
Class-Based Weighted Fair Queuing (CBWFQ)	• CBWFQ extends the standard WFQ functionality to provide support for **user-defined traffic classes** • Traffic classes are defined based on match criteria including protocols, access control lists (ACLs), and input interfaces

	• Packets satisfying the match criteria for a class constitute the traffic for that class • A **FIFO queue is reserved for each class,** and traffic belonging to a class is directed to the queue for that class • A class can be assigned characteristics, such as bandwidth, weight and maximum packet limit. The bandwidth assigned to a class is the guaranteed bandwidth delivered during congestion • Packets belonging to a class are subject to the bandwidth and queue limits, which is the maximum number of packets allowed to accumulate in the queue, that characterize the class • **After a queue has reached its configured queue limit, adding more packets to the class causes tail drop or packet drop** to take effect, depending on how class policy is configured • **Tail drop discards any packet that arrives at the tail end of a queue** that has completely used up its packet-holding resources • This is the default queuing response to congestion. Tail drop treats all traffic equally and does not differentiate between classes of service 
Low Latency Queuing (LLQ)	• LLQ feature **brings strict priority queuing (PQ) to CBWFQ** • Strict PQ **allows delay-sensitive packets** such as voice to be **sent before packets in other queues** • LLQ allows delay-sensitive packets such as voice to be sent first (before packets in other queues), giving delay-sensitive packets preferential treatment over other traffic • **Cisco recommends that only voice traffic be directed**

	to the priority queue 

QoS Models

- 3 models for implementing QoS. QoS is implemented in a network using either IntServ or DiffServ
    - **IntServ** provides the **highest guarantee of QoS**, it is very **resource-intensive**, and therefore, **not easily scalable**
    - **DiffServ** is **less resource-intensive** and **more scalable**
    - IntServ and DiffServ are sometimes co-deployed in network QoS implementations

Best-Effort Model

- **Not an implementation as QoS** is not explicitly configured
- Use when **QoS is not required**
- Basic design of the internet is **best-effort packet delivery** and provides **no guarantees** 互联网的基本设计是尽力传送数据包，不提供任何保证
- It **treats all network packets in the same way**, so an emergency voice message is treated the same way that a digital photograph attached to an email is treated

Benefits	**Drawbacks**
The model is the **most scalable**	There are **no guarantees of delivery**
Scalability is only limited by available bandwidth, in which case all traffic is equally affected	**Packets will arrive whenever they can and in any order possible**, if they arrive at all
No special QoS mechanisms are required	**No packets have preferential treatment**

It is the **easiest** and **quickest** model to deploy	**Critical data is treated the same** as casual email is treated

Integrated Services (IntServ)

- **Provides very high QoS to IP packets with guaranteed delivery**
- Defines a signaling process for applications to **signal to the network that they require special QoS for a period** and that **bandwidth should be reserved**
- IntServ can **severely limit the scalability of a network**
- IntServ **delivers the end-to-end QoS that real-time applications require**
- Explicitly manages network resources to provide QoS to individual flows or streams, sometimes called microflows
- Uses **resource reservation** and **admission-control mechanisms** 准入控制机制 as building blocks to establish and maintain QoS
- Uses a connection-oriented approach. Each individual communication must explicitly specify its traffic descriptor and requests resources to the network
- The edge router performs **admission control** to **ensure that available resources are sufficient in the network**
- In the IntServ model, the application requests a specific kind of service from the network before sending data
- The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements
- IntServ uses the **Resource Reservation Protocol (RSVP)** to **signal the QoS needs of an application's traffic along devices in the end-to-end path through the network**
- If network devices along the path can reserve the necessary bandwidth, the originating application can begin transmitting. If the requested reservation fails along the path, the originating application does not send any data

🔧 How IntServ Works

1. **Resource Reservation**
    - Applications **request specific QoS** before sending data.
    - The network **reserves bandwidth and resources** for that flow.
2. **Signaling with RSVP**
    - Uses the **Resource Reservation Protocol (RSVP)** to signal QoS requirements across the network.
    - RSVP messages travel from the sender to the receiver, asking each router along the path to reserve resources.

3. **Admission Control**
    - Routers perform **admission control** to decide whether they can meet the requested QoS.
    - If any router cannot reserve the required resources, the request is denied.
4. **Microflow-Based**
    - IntServ manages **individual flows** (called microflows), not aggregated traffic.
    - Each flow is tracked and managed separately.
5. **Connection-Oriented Behavior**
    - Although IP is connectionless, IntServ behaves like a **connection-oriented system**, requiring setup before data transmission.

Benefits	**Drawbacks**
● Explicit end-to-end resource admission control 明确的端到端资源准入控制 ● Per-request policy admission control 每请求策略准入控制 ● Signaling of dynamic port numbers	● Resource intensive due to the stateful architecture requirement for continuous signaling ● Flow-based approach not scalable to large implementations such as the internet

Differentiated Services (DiffServ)

- **Provides high scalability and flexibility in implementing QoS**
- **Network devices recognize traffic classes** and **provide different levels of QoS to different traffic classes**
- The differentiated services (DiffServ) QoS model specifies a simple and scalable mechanism for classifying and managing network traffic
- It is not end-to-end QoS strategy because it cannot **enforce end-to-end guarantees**
- **Hosts forward traffic to a router** which **classifies the flows into aggregates (classes)** and **provides the appropriate QoS policy for the classes**
- **Enforces and applies QoS mechanisms on a hop-by-hop basis**, uniformly **applying global meaning to each traffic class** to provide both flexibility and scalability
- DiffServ **divides network traffic into classes based on business requirements**. Each of the classes can then be **assigned a different level of service**
- As the packets traverse a network, each of the network devices identifies the

packet class and services the packet according to that class
- It is possible to choose many levels of service with DiffServ

🔧 How DiffServ Works

1. **Traffic Classification**
    - Packets are marked with a **Differentiated Services Code Point (DSCP)** in the IP header.
    - This marking defines the **class of service** the packet belongs to.
2. **Aggregation**
    - Instead of managing individual flows (like IntServ), DiffServ groups traffic into **aggregates** (classes).
    - Examples: voice class, video class, best-effort class.
3. **Hop-by-Hop QoS Enforcement**
    - Each router along the path reads the DSCP value and applies the appropriate QoS policy.
    - This includes prioritization, bandwidth allocation, and queuing.
4. **No End-to-End Guarantee**
    - DiffServ does **not reserve resources** across the network.
    - QoS is applied **locally at each hop**, so there's **no absolute guarantee** of service quality.

Benefits	Drawbacks
• Highly scalable • Provides many different levels of quality	• No absolute guarantee of service quality • Requires a set of complex mechanisms to work in concert throughout the network

QoS Implementation Techniques

Avoiding Packet Loss

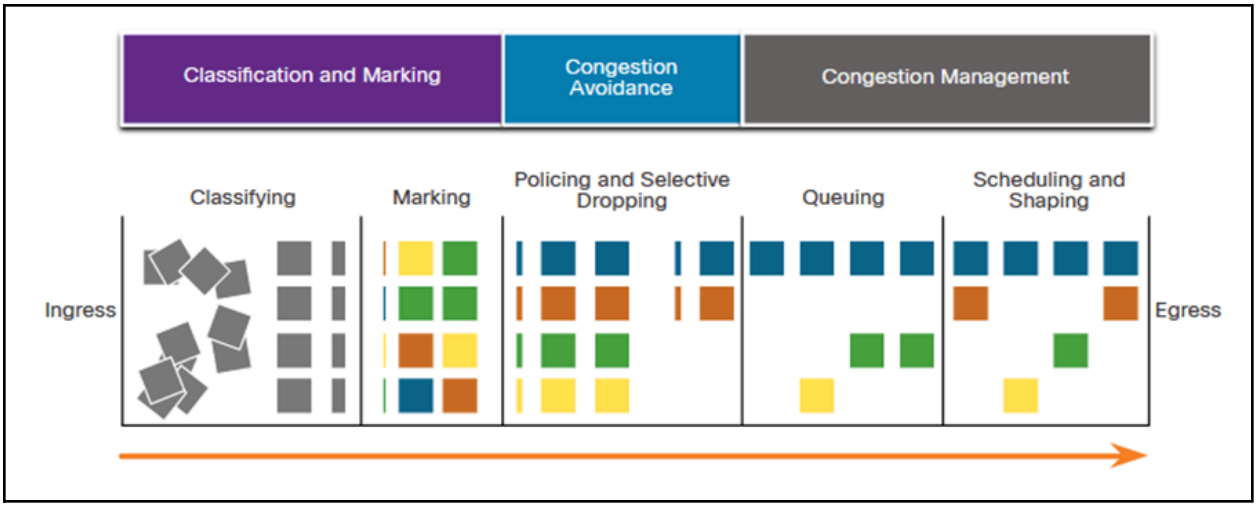
Approaches can prevent drops in sensitive applications:
- **Increase link capacity to ease or prevent congestion**

- **Guarantee enough bandwidth** and **increase buffer space** to **accommodate bursts of traffic from fragile flows**. WFQ, CBWFQ and LLQ can guarantee bandwidth and provide prioritized forwarding to drop-sensitive applications
- **Drop lower-priority packets before congestion occurs**. Cisco IOS QoS provides queueing mechanisms, such as weighted random early detection (WRED), that start dropping lower-priority packets before congestion occurs

QoS Tools	Description
Classification and marking tools	• Sessions, or flows, are analyzed to determine what traffic class they belong to • When the traffic class is determined, the packets are marked
Congestion avoidance tools	• Traffic classes are allotted 分配 portions of network resources, as defined by the QoS policy • The QoS policy also identifies how some traffic may be selectively dropped, delayed or re-marked to avoid congestion • The primary congestion avoidance tool is WRED and is used to regulate TCP data traffic in a bandwidth-efficient manner before tail drops caused by queue overflows occur 主要的拥塞避免工具是 WRED，用于在队列溢出导致尾丢弃之前，以节省带宽的方式调节 TCP 数据流量
Congestion management tools	• When traffic exceeds available network resources, traffic is queued to await availability of resources • Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms

Sequence of QoS tools used when applied to packet flows:

- **Ingress packets are classified** and their respective **IP header is marked**
- To avoid congestion, **packets are then allocated resources based on defined policies**
- **Packets are then queued** and **forwarded out the egress interface based on their defined QoS shaping and policing policy**



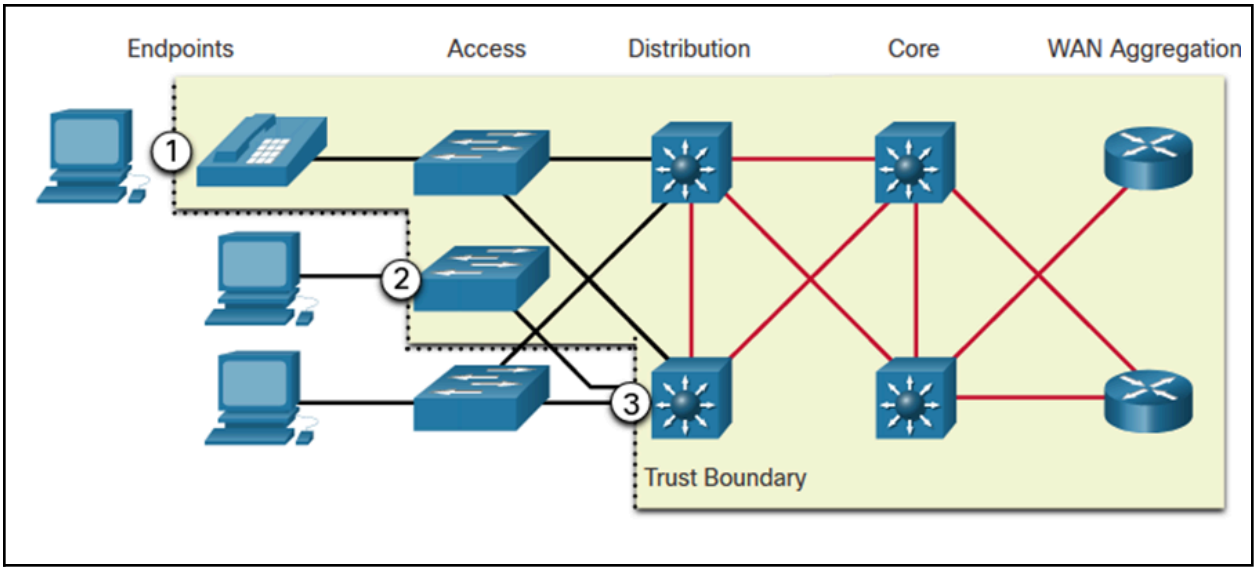
DSCP Values

The 64 DSCP values are organized into 3 categories:	
Best-Effort (BE)	This is the default for all IP packets, The DSCP value is 0. The per-hop behavior is normal routing. When a router experiences congestion, these packets will be dropped. No QoS plan is implemented
Expedited Forwarding (EF)	RFC 3246 defines EF as the DSCP decimal value 46 (binary 101110). The first 3 bits (101) map directly to the Layer 2 CoS value 5 used for voice traffic. At layer 3, Cisco recommends that EF only be used to mark voice packets
Assured Forwarding (AF)	RFC 2597 defines AF to use the 5 most significant DSCP bits to indicate queues and drop preference

Trust Boundaries

Traffic should be classified and marked as close to its source as technically and administratively feasible. This defines the trust boundary.

1. Trusted endpoints have the capabilities and intelligence to mark application traffic to the appropriate Layer 2 CoS and / or Layer 3 DSCP values
2. Secure endpoints can have traffic marked at the Layer 2 switch
3. Traffic can also be marked at Layer 3 switches / routers



Congestion Avoidance

- They **monitor network traffic loads** in an effort to **anticipate and avoid congestion** at common network and internetwork bottlenecks before congestion becomes a problem
- They **monitor the average depth of the queue**. When the **queue is below the minimum threshold**, there are **no drops**. As the **queue fills up to the maximum threshold**, a **small percentage of packets are dropped**. When the **maximum threshold is passed**, **all packets are dropped**

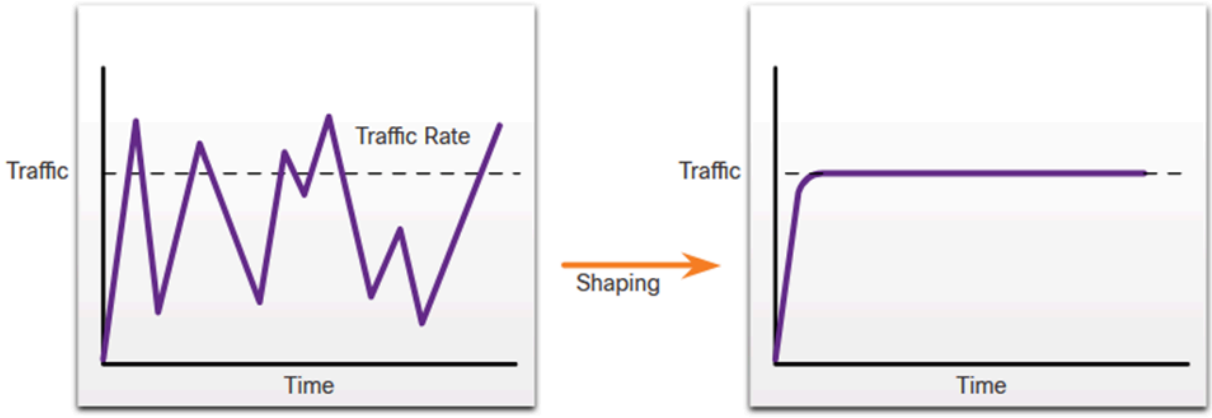
- Some congestion avoidance techniques provide preferential treatment for which packets get dropped
    - **Weighted random early detection (WRED)** allows for congestion on network interfaces by **providing buffer management** and **allowing TCP traffic to decrease**, or **throttle back** 节流, before buffers are exhausted
    - WRED helps **avoid tail drops** and **maximizes network use** and **TCP-based application performance**

Shaping and Policing

Traffic shaping and traffic policing are two mechanisms provided by Cisco IOS QoS software to prevent congestion

- **Traffic shaping retains excess packets in a queue** and then **schedules the excess for later transmission over increments of time**. Traffic shaping results in a **smoothed packet output rate**
- **Shaping** is an **outbound concept**; **packets going out an interface get queued**

and can be shaped. In contrast, **policing is applied to inbound traffic on an interface**



Policing is applied to inbound traffic on an interface. Policing is commonly implemented by service providers to **enforce a contracted customer information rate (CIR)**. However, the service provider may also **allow bursting over the CIR if the service provider's network is not currently experiencing congestion**

QoS Policy Guidelines

QoS policies must **consider the full path from source to destination**

A few guidelines that help ensure the best experience for end users includes the following:

- **Enable queuing at every device in the path between source and destination**
- **Classify and mark traffic as close the source as possible**
- **Shape and police traffic flows as close to their sources as possible**