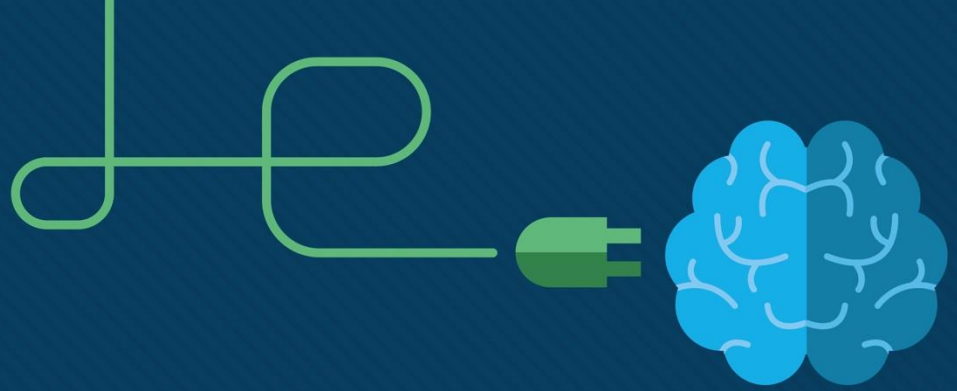


Module 4
WAN Concepts

ITNET04

WAN Connectivity

Module Objectives

Module Title: WAN Concepts

Module Objectives:

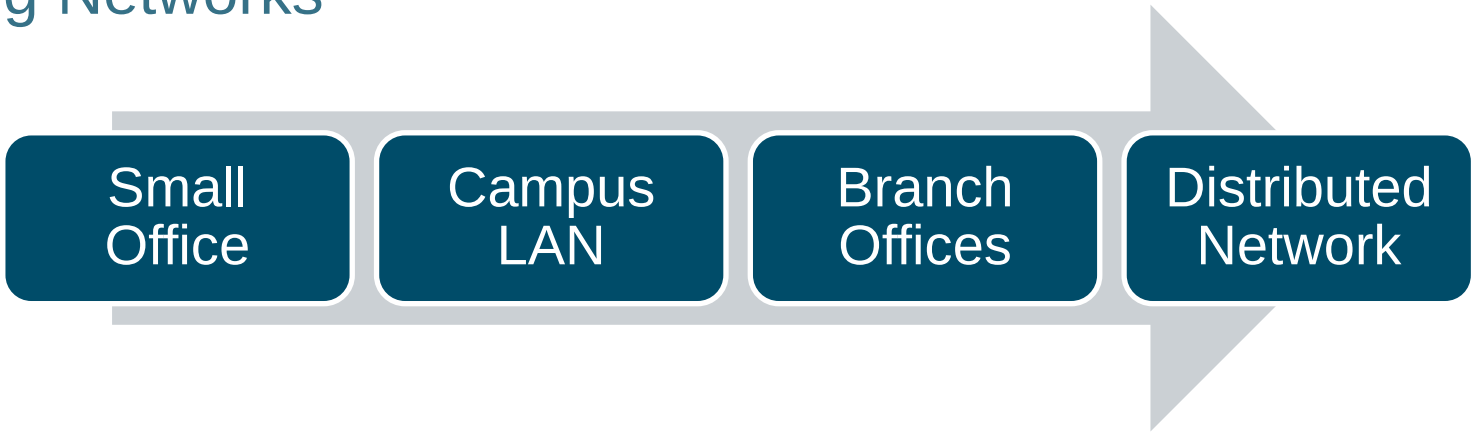
- Explain the purpose of a WAN and how it operates
- Compare WAN connectivity options for small to medium-sized business networks.
- Select WAN access technologies to satisfy business requirements.

Module References:

- CCNAv7 ENSA– Module 7

1.1 WAN Technologies Overview

Evolving Networks

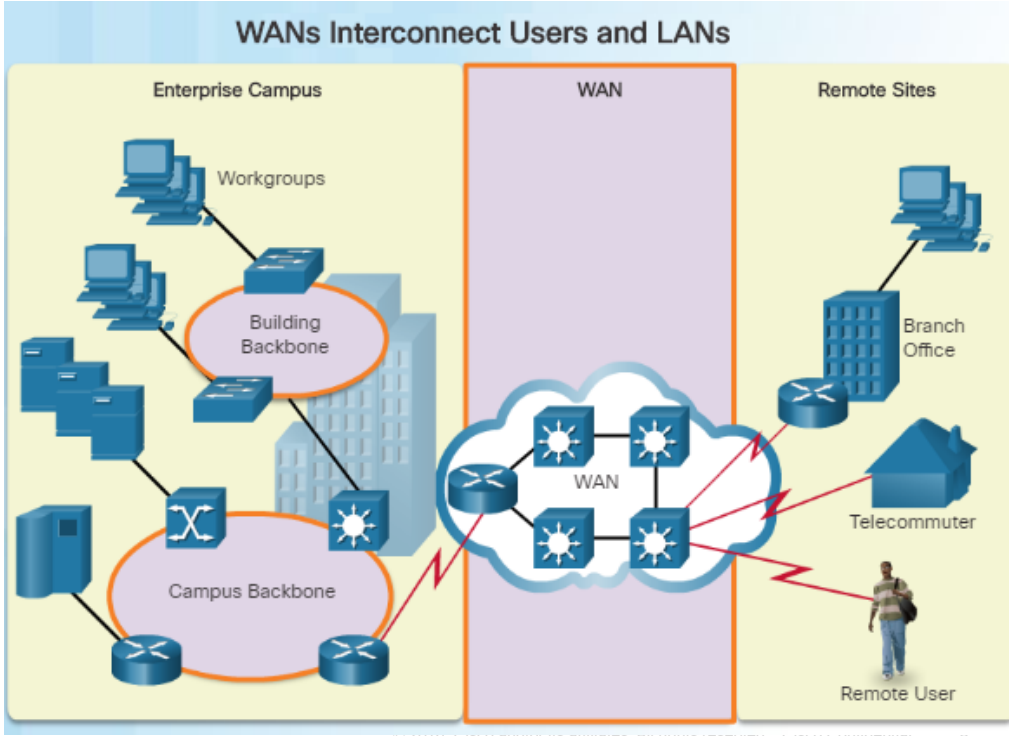


- Companies often start out as small offices and can continue growing until they span multiple offices in various geographic locations
- Throughout their growth, companies expect their networks to scale accordingly
- Company sites often need to stay connected, while simultaneously perform optimally and deliver an increasing array of services and applications to support productivity and profitability.

Why a WAN?

A WAN operates beyond the geographic scope of a LAN and is required to connect beyond the boundaries of the LAN

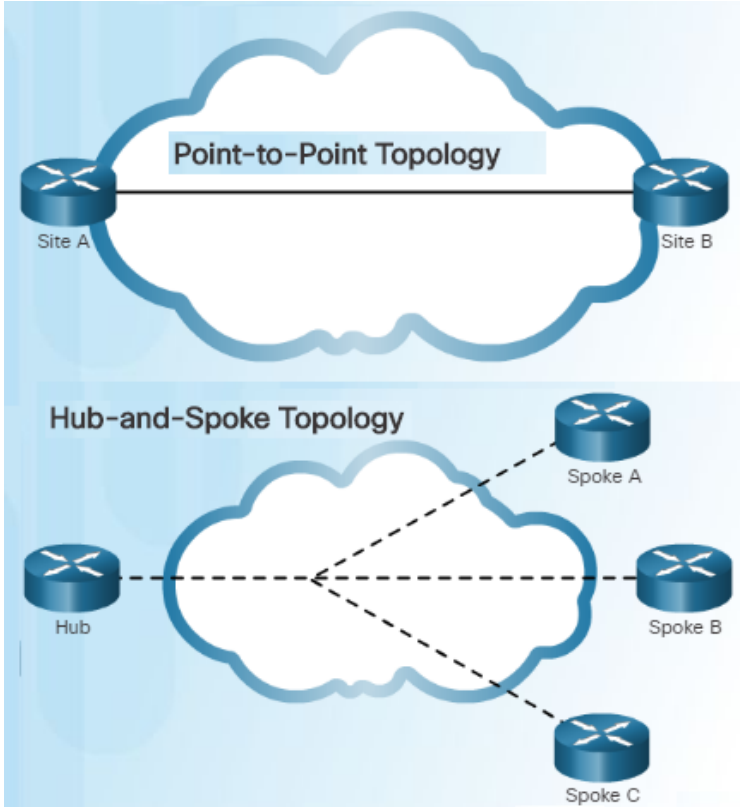
- WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.
- A WAN is owned by a service provider whereas a LAN is typically owned by an organization.
- An organization must pay a fee to use the WAN service provider's network services to connect remote sites.
- WANs providers offer low to high bandwidth speeds, over long distances.



Are WANs Necessary?

- Without WANs, LANs would be a series of isolated networks.
- As organizations expand, businesses require the ability to communicate between geographically separated sites. For example:
  - Regional or branch offices of an organization need to be able to communicate and share data with the central site.
  - Organizations need to share information with other customer organizations.
  - Employees who travel on company business frequently need to access the corporate network.
- In addition, consumers now commonly communicate over the Internet with banks, stores, and other providers of goods and services.

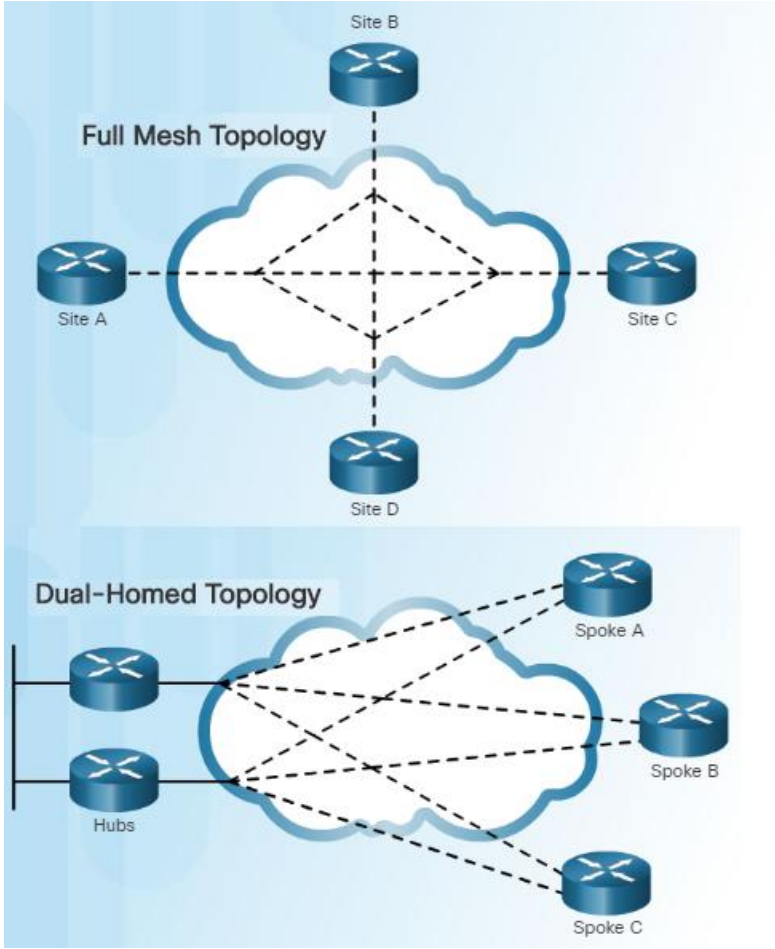
WAN Topologies



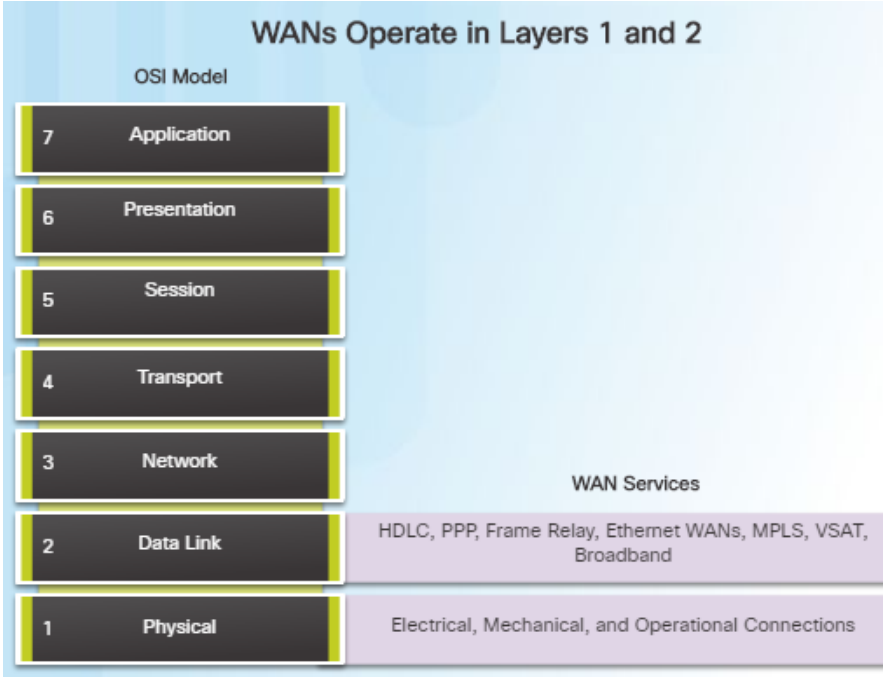
- Interconnecting multiple sites across WANs can involve a variety of service provider technologies and WAN topologies. There are four Common WAN topologies.
- Point-to-Point topology
  - Employs a point-to-point circuit between two endpoints
  - Typically involves a dedicated leased-line connection such as a T1/E1 line.
  - Transparent to the customer network and appears to be a direct physical link between two endpoints
- Hub-and-Spoke
  - Applicable when a private network connection between multiple sites is required
  - A single interface to the hub can be shared by all spoke circuits.
  - Spoke sites can be interconnected through the hub site using virtual circuits and routed subinterfaces at the hub.

WAN Topologies (Cont.)

- Full Mesh
  - A disadvantage of the hub-and-spoke topology is that all communication has to go through the hub.
  - With a full mesh topology using virtual circuits, any site can communicate directly with any other site.
  - A disadvantage is the large number of virtual circuits that need to be configured and maintained.
- Dual-homed Topology
  - Provides redundancy and load balancing however they are more expensive to implement than single-homed topologies.
  - Requires additional networking hardware including routers and switches.
  - More difficult to implement since they require complex configurations.

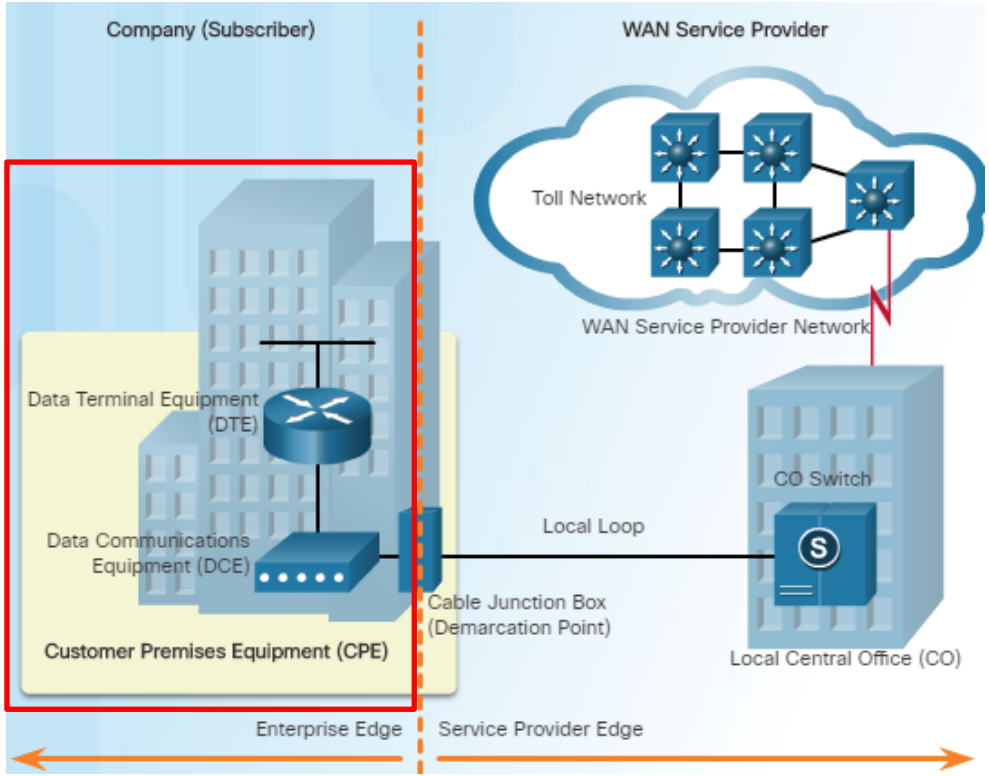


WANs in the OSI Model



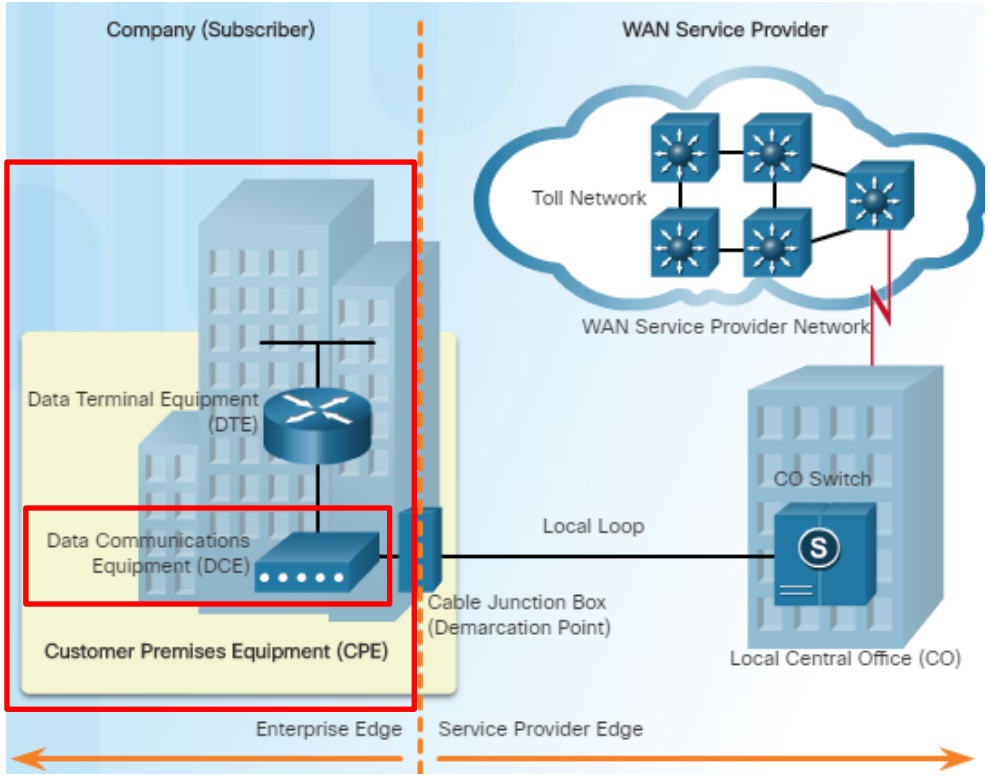
- WAN operations focus primarily on the physical and data link layer of the OSI Model.
- Data link layer requirements include physical addressing, flow control and encapsulation.
- WAN access standards are defined and managed by a number of recognized authorities:
  - TIA/EIA (Telecommunications Industry Association and the Electronic Industries Alliance)
  - ISO (International Organization for Standardization)
  - IEEE (Institute of Electrical and Electronics Engineers)
- Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connects to the services of a communications service provider.
- Layer 2 protocols define how data is encapsulated and the mechanisms for transferring the resulting frames.

Common WAN Terminology



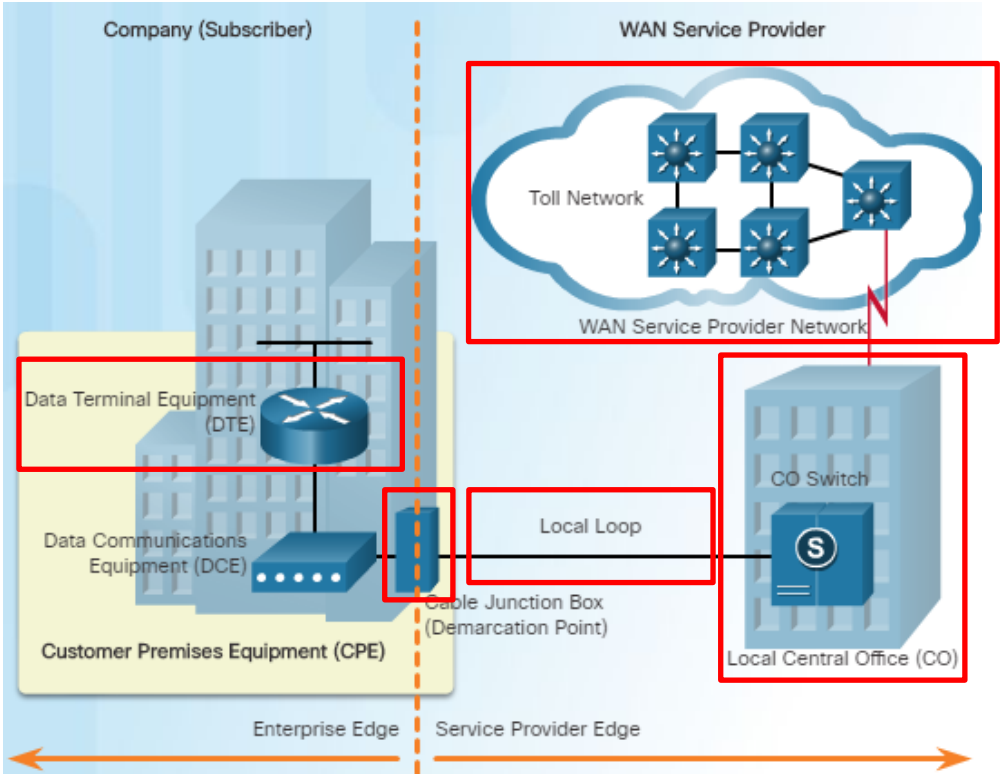
- One primary difference between a WAN and a LAN is that a company must subscribe to an outside WAN service provider to use WAN carrier network services.
- Terminology commonly used to describe WAN connections:
  - **Customer Premises Equipment (CPE)** – Consists of devices and inside wiring located on the enterprise edge connecting to a carrier

Common WAN Terminology



- One primary difference between a WAN and a LAN is that a company must subscribe to an outside WAN service provider to use WAN carrier network services.
- Terminology commonly used to describe WAN connections:
  - **Customer Premises Equipment (CPE)** – Consists of devices and inside wiring located on the enterprise edge connecting to a carrier
  - **Data Communications Equipment (DCE)** – Also called circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.

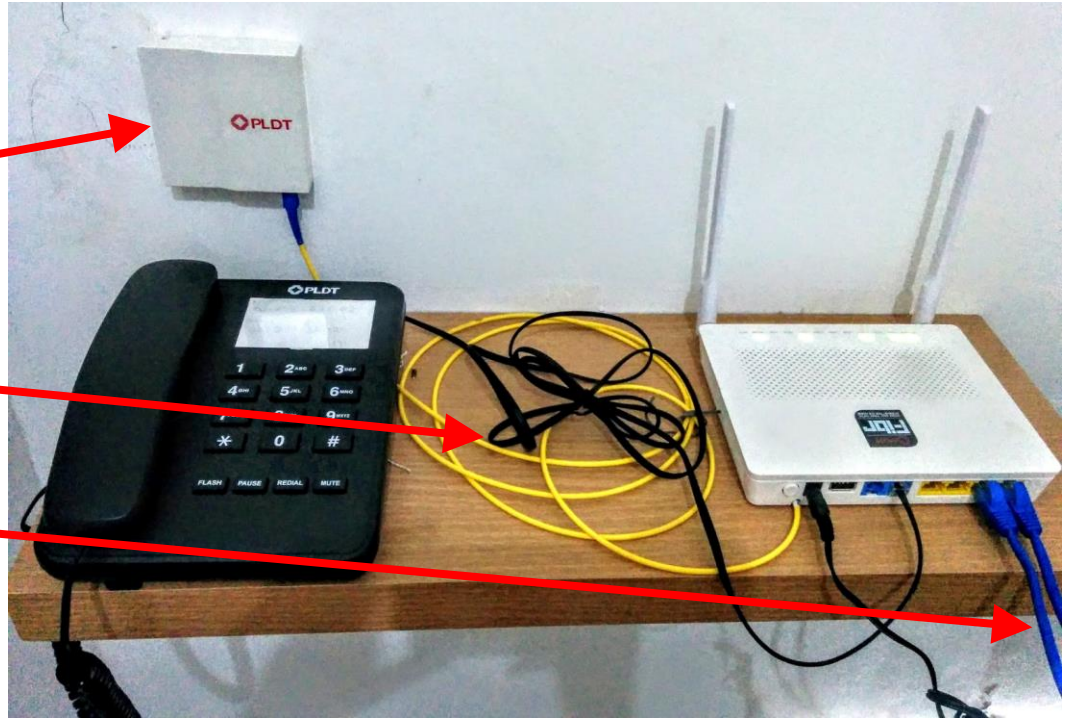
Common WAN Terminology (Cont.)



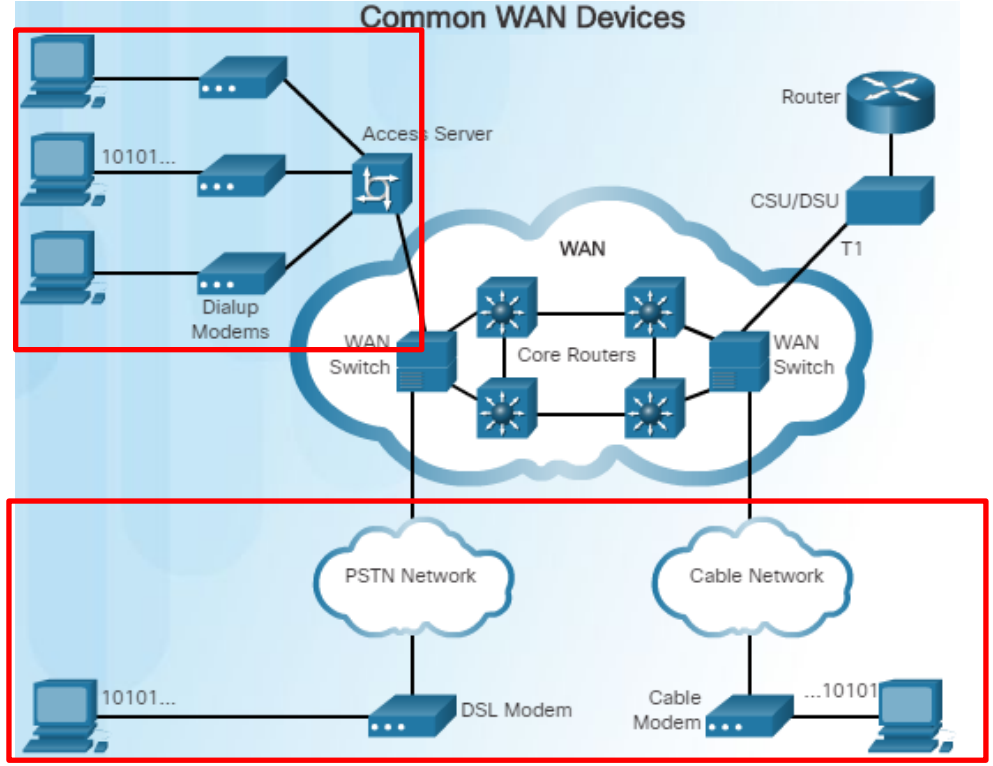
- **Data Terminal Equipment (DTE)** – The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.
- **Demarcation Point** – This is a point established in a building to separate customer equipment from service provider equipment.
- **Local Loop ("last mile")** – The actual copper or fiber cable that connects the CPE to the CO of the service provider.
- **Central Office (CO)** – The CO is the local service provider facility or building that connects the CPE to the provider network.
- **Toll network** – This consists of the long-haul, all-digital, fiber-optic communications lines and other equipment inside the WAN provider network.

WAN Terminology - Local Setting

- **Where is the demarcation point?**

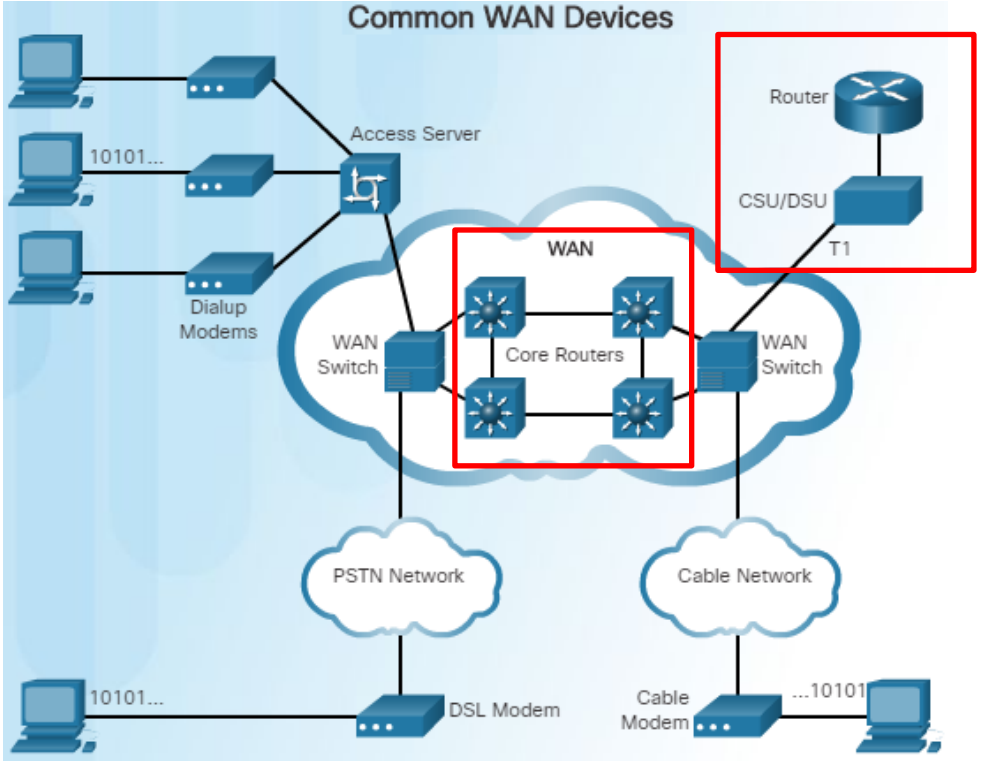


WAN Devices



- There are many types of devices that are specific to WAN environments:
  - **Dialup modem** – Legacy WAN technology that converts (modulates) the digital signals produced by a computer into voice frequencies which are transmitted over the analog lines of the public telephone network to another modem for demodulation.
  - **Access server** – Legacy technology where the server controls and coordinates dialup modem, dial-in and dial-out user communications.
  - **Broadband modem** – A type of digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem, but use higher broadband frequencies and transmission speeds.

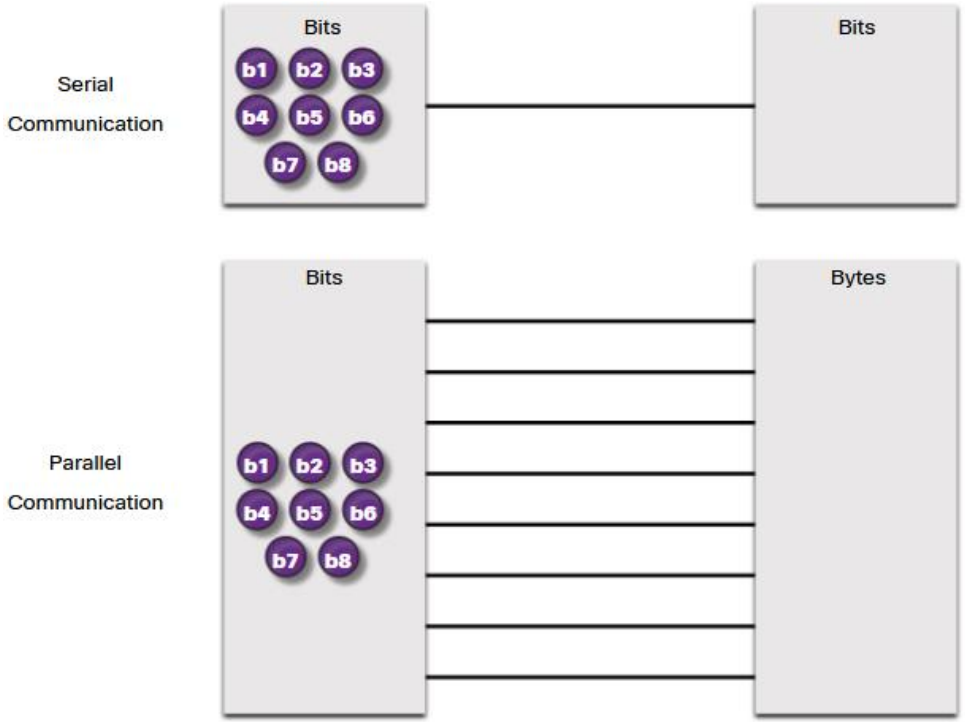
WAN Devices (Cont.)



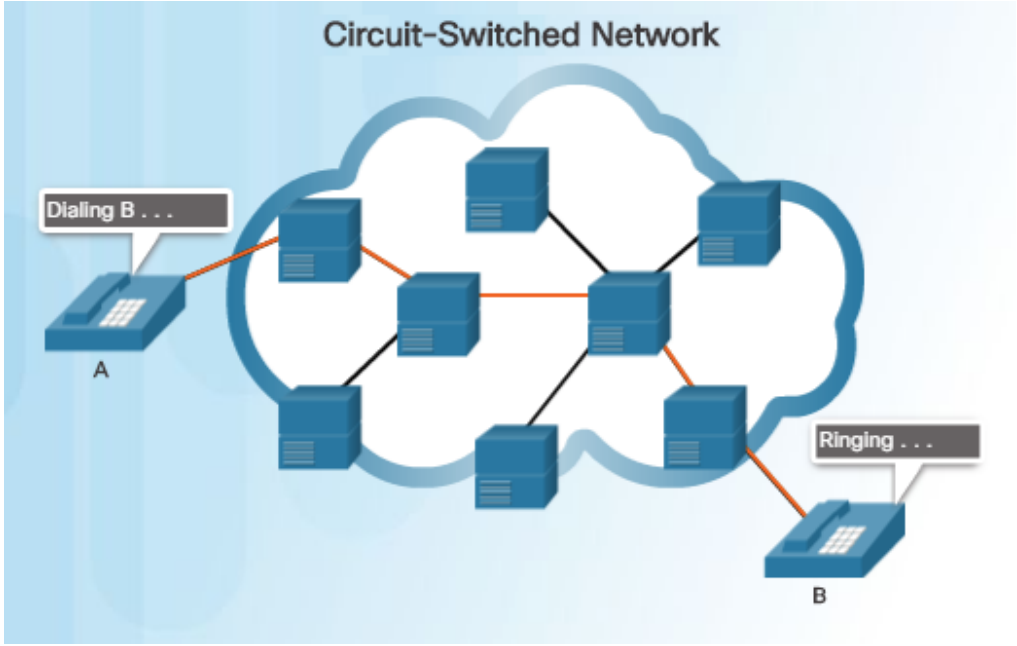
- **CSU/DSU** - Digital-leased lines require a CSU and a DSU. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts line frames into frames that the LAN can interpret and vice versa.
- **Router** – Provides internetworking and WAN access interface ports that are used to connect to the service provider.
- **Core router/Multilayer switch** – A router or multilayer switch that resides within the middle or backbone of the WAN.

Serial Communication

- Almost all network communications occur using a serial communication delivery. Serial communication transmits bits sequentially over a single channel.
- In contrast, 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

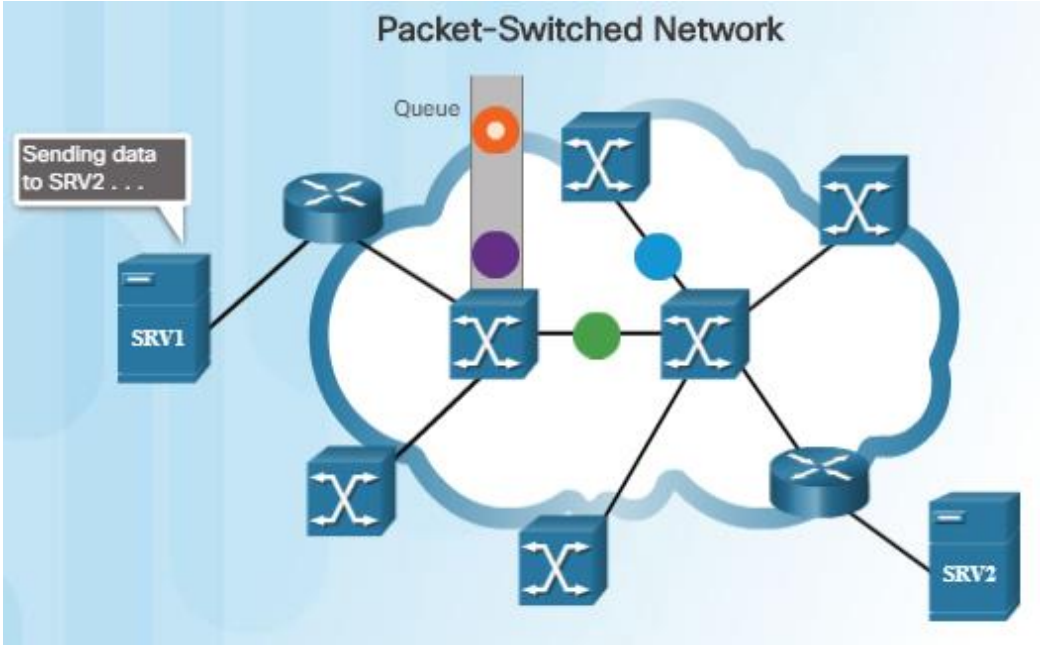


Circuit Switching



- A circuit-switched network is one that establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate.
  - Dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver.
  - Communication can't start until the connection is established through the service provider network.
- Dialing a number to make a call is an example of circuit switching technology.
- The two most common types of circuit-switched WAN technologies
  - Public switched telephone network (PSTN)
  - Integrated Services Digital Network (ISDN).

Packet Switching



Network communication is commonly implemented using packet-switching

- Segments traffic data into packets that are routed over a shared network.
- A circuit does not need to be established and many pairs of nodes can communicate over the same channel.
- Much less expensive and more flexible than circuit switching but more prone to latency and jitter
- Common types of packet-switched WAN technologies are:
  - Ethernet WAN (Metro Ethernet),
  - Multiprotocol Label Switching (MPLS)
  - Frame Relay
  - Asynchronous Transfer Mode (ATM).

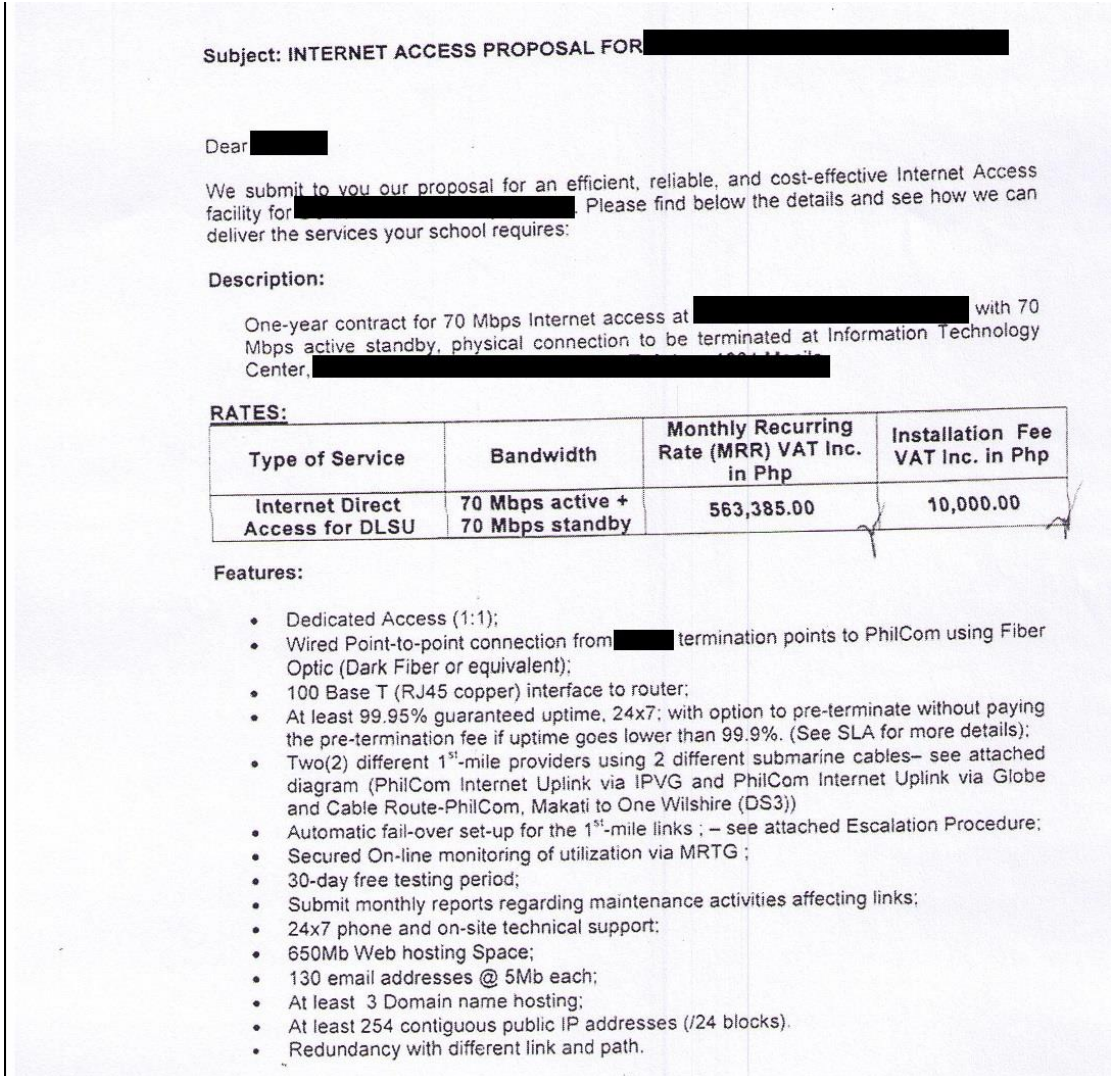
SDH, SONET, and DWDM

- Service provider networks use fiber-optic infrastructures to transport user data between destinations. Fiber-optic cable is far superior to copper cable for long distance transmissions due to its much lower attenuation and interference.
- There are two optical fiber OSI layer 1 standards available to service providers that define how to transfer multiple data, voice, and video communications over optical fiber using lasers or light-emitting diodes (LEDs) over great distances.
  - **SDH** - Synchronous Digital Hierarchy (SDH) is a global standard for transporting data over fiber-optic cable.
  - **SONET** - Synchronous Optical Networking (SONET) is the North American standard that provides the same services as SDH.
  - **DWDM -** Dense Wavelength Division Multiplexing (DWDM) is a newer technology that increases the data-carrying capacity of SDH and SONET by simultaneously sending multiple streams of data (multiplexing) using different wavelengths of light.

WAN Operations

ISP Connectivity Options

- An organization usually signs a service level agreement (SLA) with a service provider. The SLA outlines the expected services relating to the reliability and availability of the connection.
- The service provider may or may not be the actual carrier. A carrier owns and maintains the physical connection and equipment between the provider and the customer. Typically, an organization will choose either a single-carrier or dual-carrier WAN connection.



Subject: INTERNET ACCESS PROPOSAL FOR [redacted]

Dear [redacted]

We submit to you our proposal for an efficient, reliable, and cost-effective Internet Access facility for [redacted]. Please find below the details and see how we can deliver the services your school requires:

Description:

One-year contract for 70 Mbps Internet access at [redacted] with 70 Mbps active standby, physical connection to be terminated at Information Technology Center, [redacted]

RATES:

Type of Service	Bandwidth	Monthly Recurring Rate (MRR) VAT Inc. in Php	Installation Fee VAT Inc. in Php
Internet Direct Access for DLSU	70 Mbps active + 70 Mbps standby	563,385.00	10,000.00

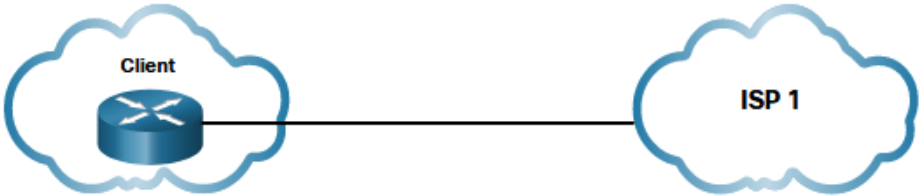
Features:

- Dedicated Access (1:1);
- Wired Point-to-point connection from [redacted] termination points to PhilCom using Fiber Optic (Dark Fiber or equivalent);
- 100 Base T (RJ45 copper) interface to router;
- At least 99.95% guaranteed uptime, 24x7; with option to pre-terminate without paying the pre-termination fee if uptime goes lower than 99.9%. (See SLA for more details);
- Two(2) different 1st-mile providers using 2 different submarine cables– see attached diagram (PhilCom Internet Uplink via IPVG and PhilCom Internet Uplink via Globe and Cable Route-PhilCom, Makati to One Wilshire (DS3))
- Automatic fail-over set-up for the 1st-mile links ; – see attached Escalation Procedure;
- Secured On-line monitoring of utilization via MRTG ;
- 30-day free testing period;
- Submit monthly reports regarding maintenance activities affecting links;
- 24x7 phone and on-site technical support;
- 650Mb Web hosting Space;
- 130 email addresses @ 5Mb each;
- At least 3 Domain name hosting;
- At least 254 contiguous public IP addresses (/24 blocks).
- Redundancy with different link and path.

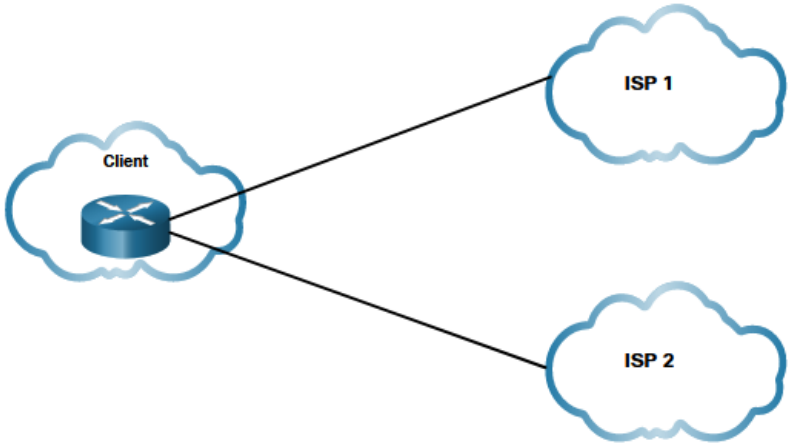
ISP Connectivity Options

There are different ways an organization can connect to an ISP. The choice depends on the needs and budget of the organization.

- **Single-homed** –Single connection to the ISP using one link. Provides no redundancy and is the least expensive solution.



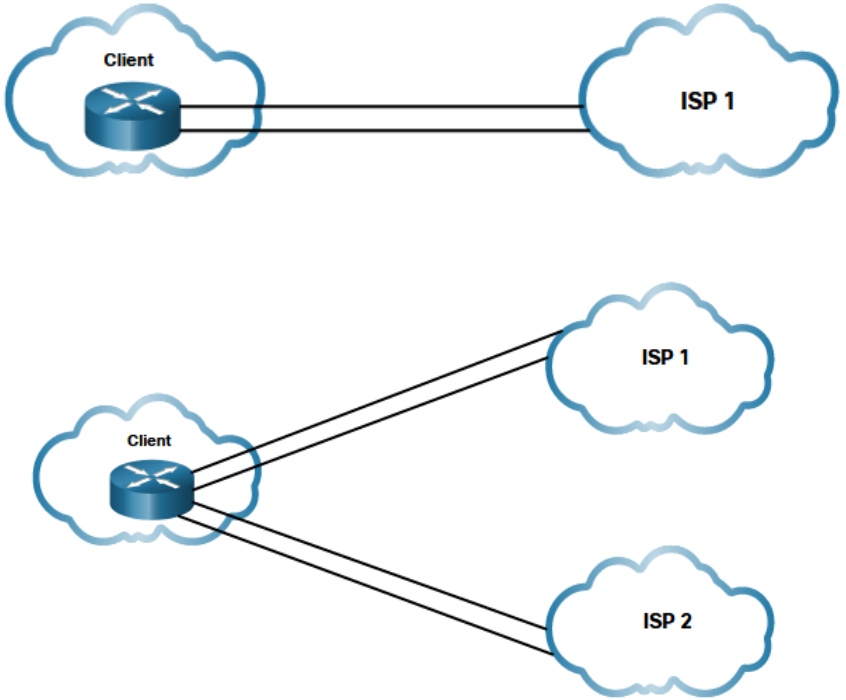
- **Multihomed** -The client connects to two different ISPs. This design provides increased redundancy and enables load-balancing, but it can be expensive.



ISP Connectivity Options

There are different ways an organization can connect to an ISP. The choice depends on the needs and budget of the organization.

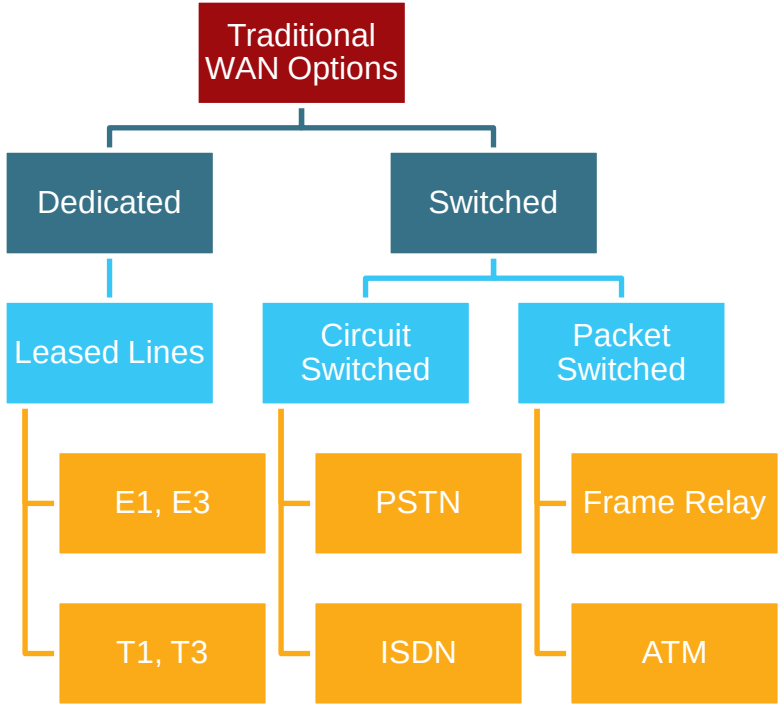
- **Dual-homed** - Connects to the same ISP using two links. Provides both redundancy and load balancing. However, the organization loses internet connectivity if the ISP experiences an outage.
- **Dual-multihomed** - Most resilient topology but most expensive option. The client connects with redundant links to multiple ISPs. This topology provides the most redundancy possible.



4.2. Traditional WAN Connectivity

Traditional WAN Connectivity Options

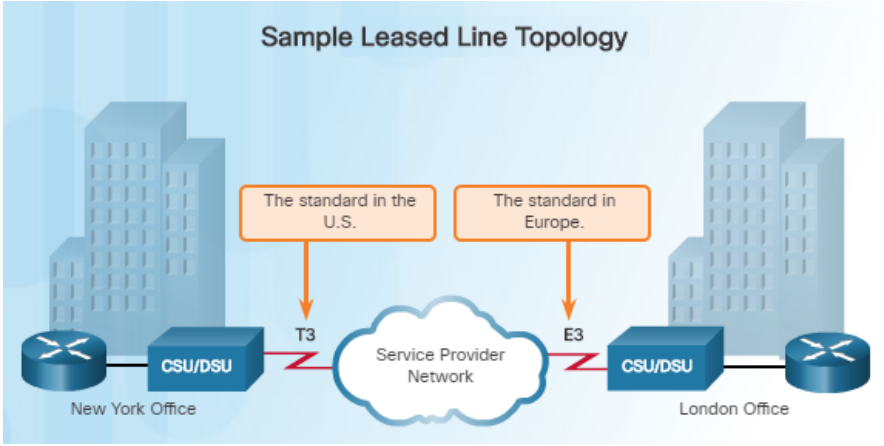
- When LANs appeared in the 1980s, organizations began to see the need to interconnect with other locations.
- To do so, they needed their networks to connect to the local loop of a service provider.
- This was accomplished by using dedicated lines, or by using switched services from a service provider.



Leased Lines

Point-to-point lines could be leased from a service provider and were called “leased lines”. The term refers to the fact that the organization pays a monthly lease fee to a service provider to use the line.

- Leased lines vary in price priced based on the bandwidth required and the distance between the two connected points.



- There are two systems used to define the digital capacity of a copper media serial link:
  - **T-carrier** - Used in North America, T-carrier provides T1 links supporting bandwidth up to 1.544 Mbps and T3 links supporting bandwidth up to 43.7 Mbps.
  - **E-carrier** – Used in Europe, E-carrier provides E1 links supporting bandwidth up to 2.048 Mbps and E3 links supporting bandwidth up to 34.368 Mbps.

Leased Lines

The table summarizes the advantages and disadvantages of leased lines.

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.

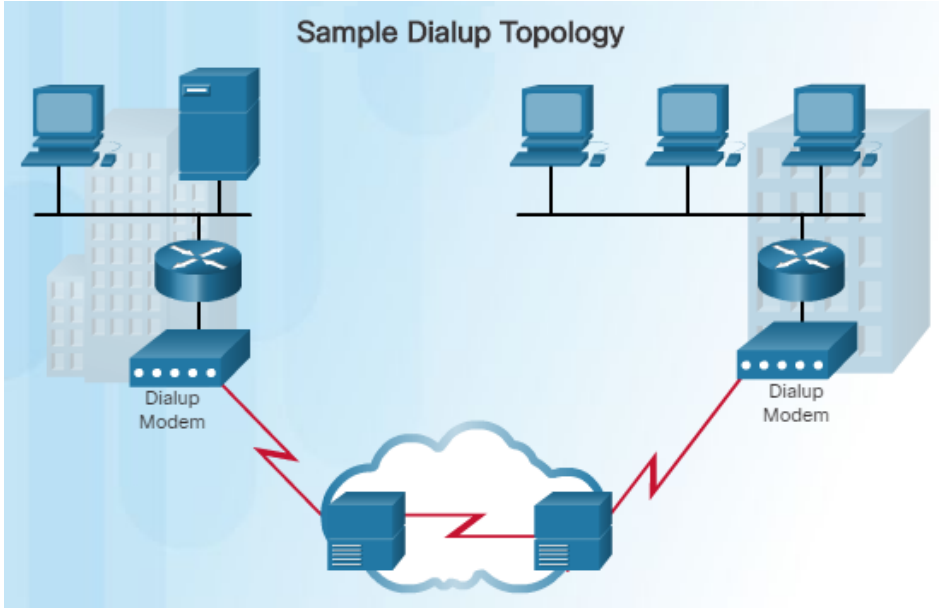
Disadvantages	
Cost	Point-to-point links are generally the most expensive type of WAN access. The cost of leased line solutions can become significant when they are used to connect many sites over increasing distances.
Limited flexibility	WAN traffic is often variable, and leased lines have a fixed capacity, 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.

Dialup

- Traditional local loops can transport binary computer data through the voice telephone network using a voiceband modem.
- A modem modulates the binary data into an analog signal at the source and demodulates the analog signal to binary data at the destination.
- The physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 kbps.

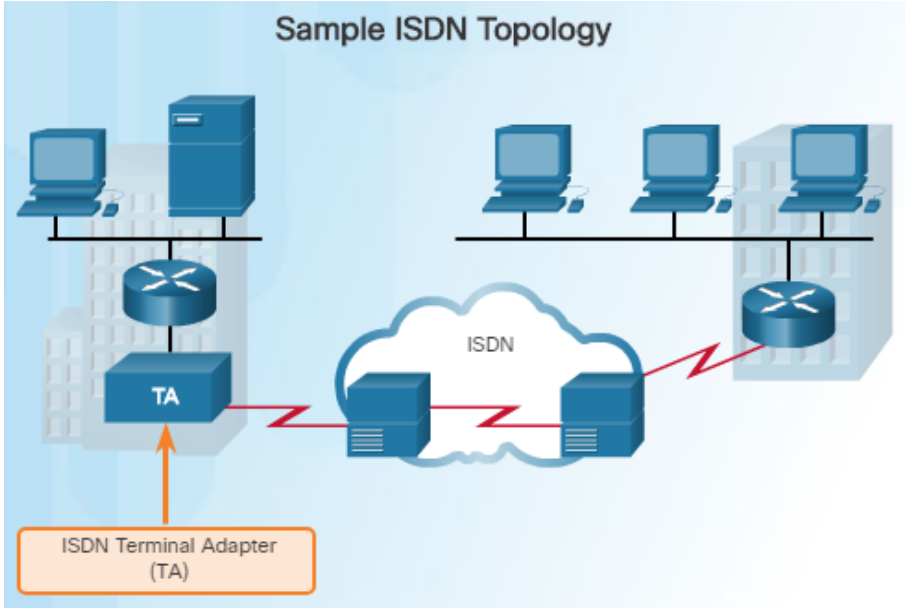


Circuit-Switch Options

Circuit-switched connections are provided by Public Service Telephone Network (PSTN) carriers. The local loop connecting the CPE to the CO is copper media.

Integrated Services Digital Network (ISDN)

- ISDN is a circuit-switching technology that enables the PSTN local loop to carry digital signals.
- Allows two or more signals, or bit streams, to be transferred as subchannels in one communication channel.
- Provided higher capacity switched connections than dialup access – from 45 Kbps to 2.048 Mbps.

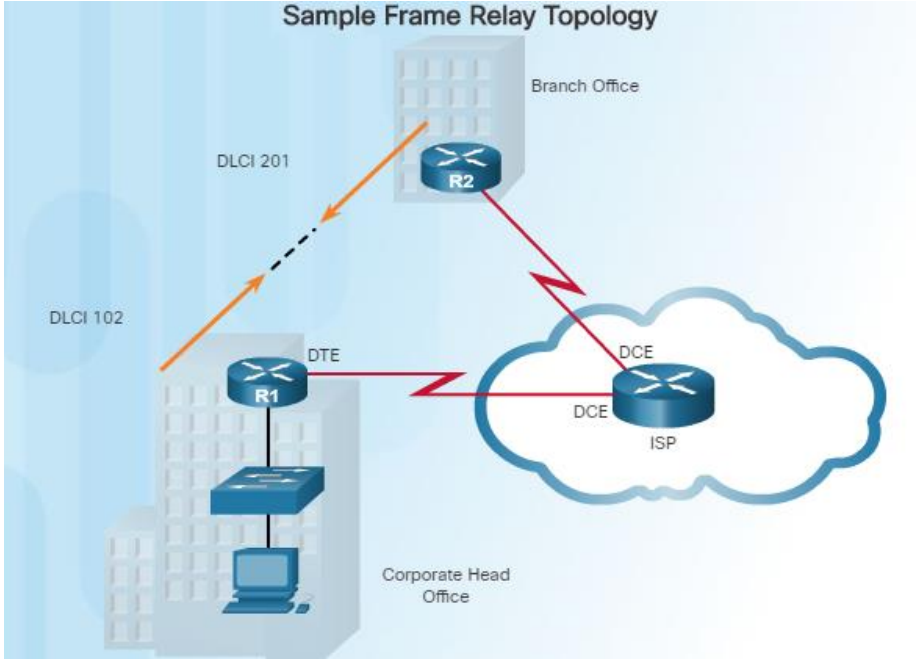


Packet-Switch Options

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.

Frame Relay

- Frame Relay is a simple Layer 2 non-broadcast multi-access (NBMA) WAN technology that is used to interconnect enterprise LANs.
- Creates virtual circuits which are uniquely identified by a data-link connection identifier (DLCI).
- An edge router can use a single physical interface to support multiple virtual circuits connecting to different sites
- Provided higher capacity switched connections than dialup access – from 45 Kbps to 2.048 Mbps.

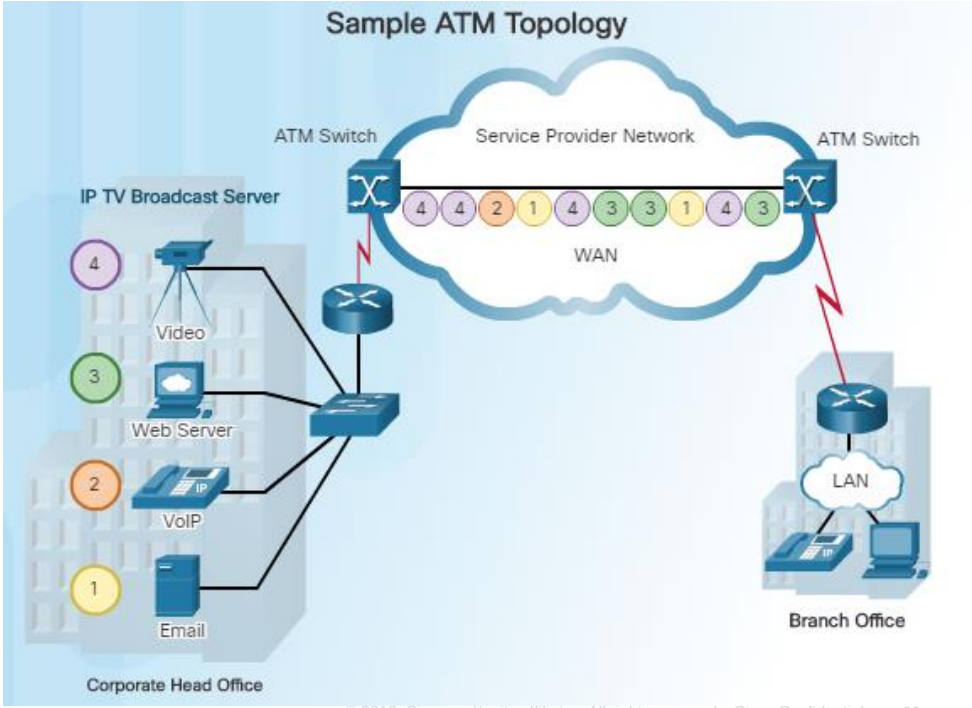


Packet-Switch Options

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.

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.

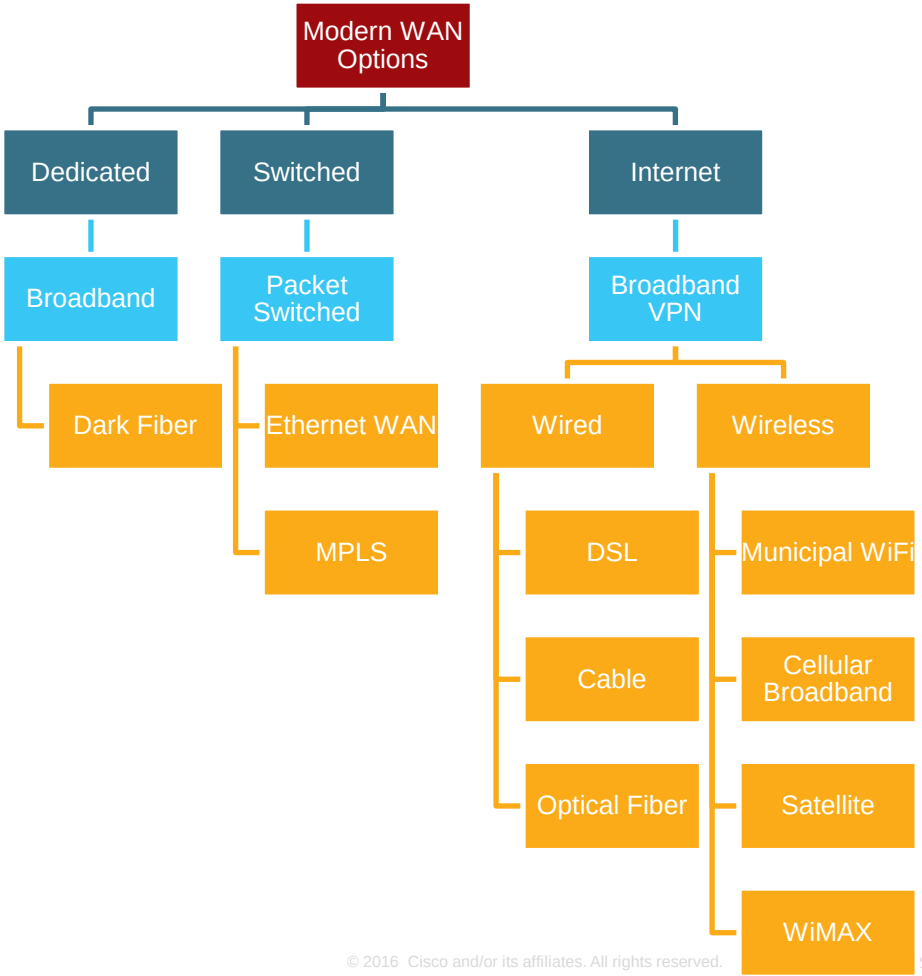


4.3. Modern WAN Connectivity

Modern WANs

Modern WANS have more connectivity options than traditional WANs.

- Enterprises now require faster and more flexible WAN connectivity options.
- Traditional WAN connectivity options have rapidly declined in use because they are either no longer available, too expensive, or have limited bandwidth.

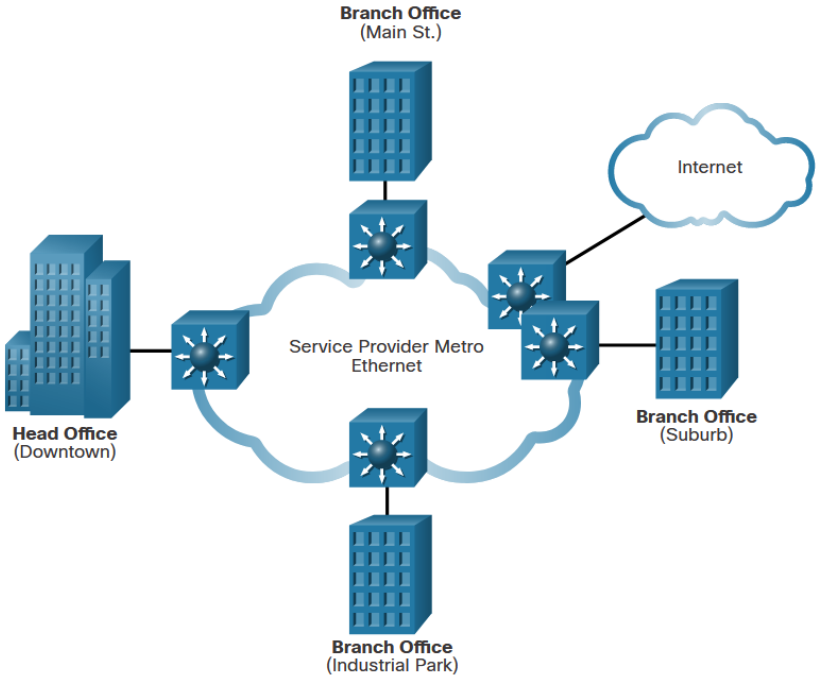


Dedicated Broadband

- Dedicated broadband commonly refers to fiber cabling that is installed independently by an organization to connect remote locations directly together.
- Dark fiber can be also leased or purchased from a service provider. This refers to fiber cabling that are already preinstalled but are not yet in use
- Suitable for organizations that require high security and high bandwidth point-to-point communications, and full control of their network infrastructure

Ethernet WAN

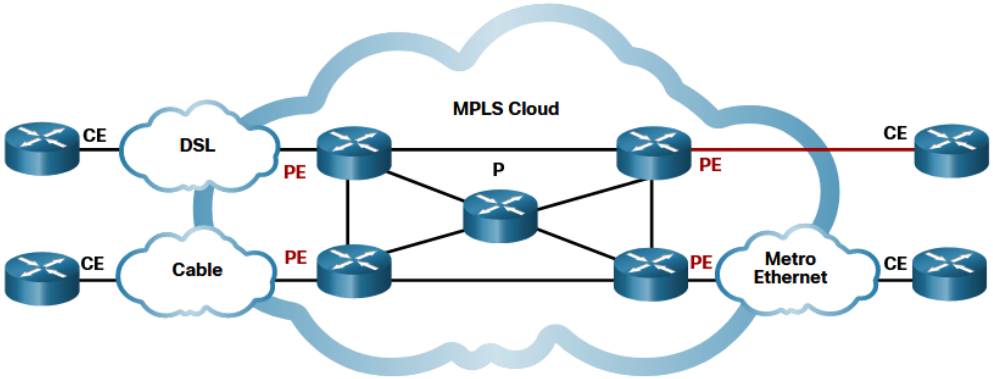
- Ethernet WANs have gained in popularity and are now commonly being used to replace the traditional WAN links
- Service providers offer Ethernet WAN service using fiber-optic cable which can reach distances of up to 5 km.
- The Ethernet WAN service can go by many names, including the following:
  - Metropolitan Ethernet (Metro E)
  - Ethernet over MPLS (EoMPLS)
  - Virtual Private LAN Service (VPLS)
- Benefits of Ethernet WAN are:
  - Reduced expenses and administration
  - Easy integration with existing networks
  - Enhanced business productivity



Multiprotocol Label Sswitching

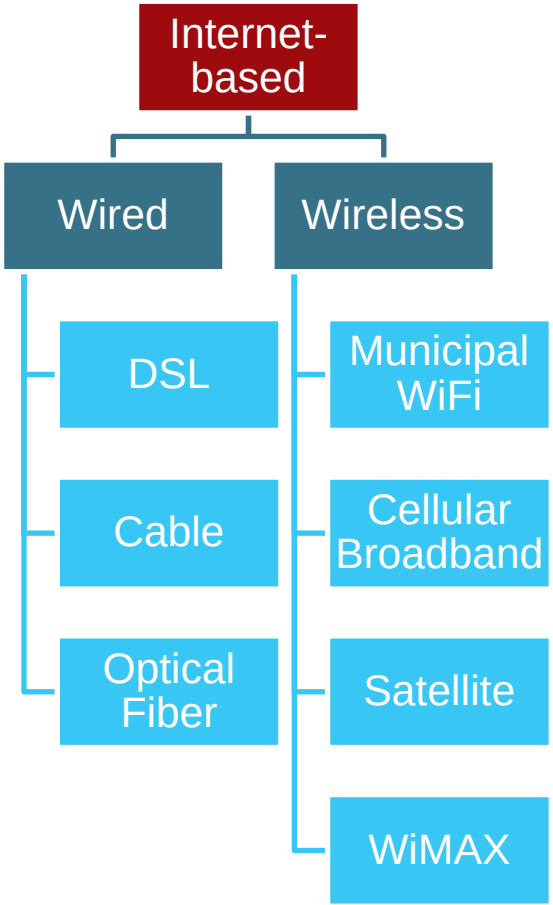
Multiprotocol Label Switching (MPLS) is a high-performance service provider WAN routing technology to interconnect clients without regard to access method or payload.

- Supports a variety of client access methods (e.g., Ethernet, DSL, Cable, Frame Relay).
- Can encapsulate all types of protocols including IPv4 and IPv6 traffic.
- An MPLS router can be a customer edge (CE) router, a provider edge (PE) router, or an internal provider (P) router.
- MPLS routers are label switched routers (LSRs). They attach labels to packets that are then used by other MPLS routers to forward traffic.



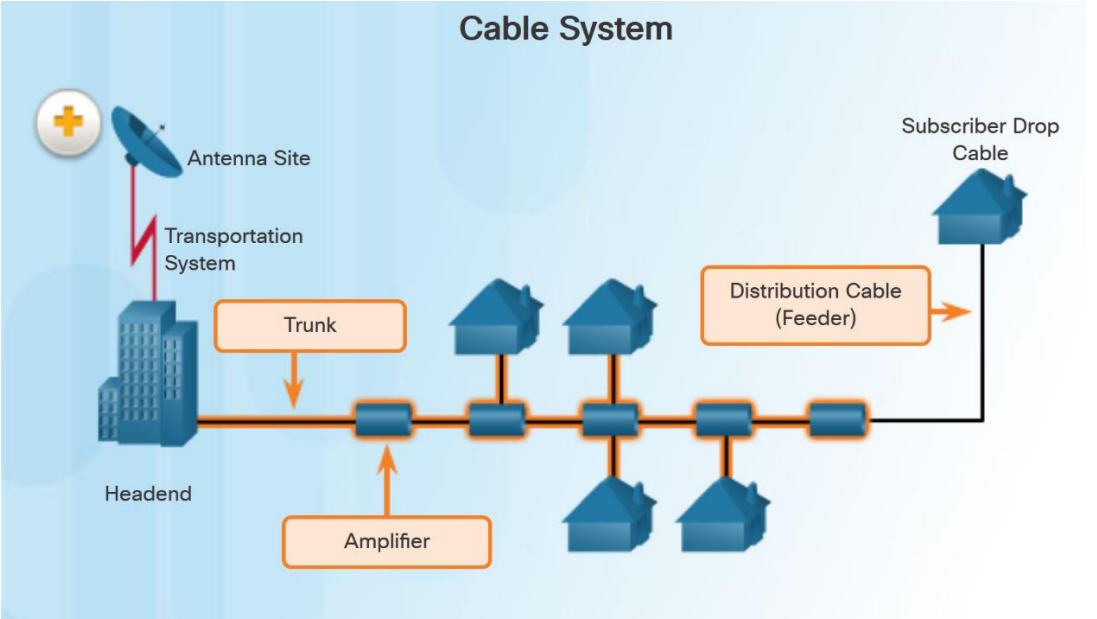
Internet-Based Connectivity

- Internet-based connections are classified as public WAN connections because they share infrastructure and resources with other subscribers of an ISP
- Are also called ‘Broadband Internet’ which refers to always-on high-speed Internet connections, usually offering bandwidths that exceed 200 kbps in at least one direction
- Several technologies available, the most common are:
  - Cable
  - Digital Subscriber Line (DSL)
  - Fiber
  - Wireless (Cellular, Satellite, Municipal WiFi)



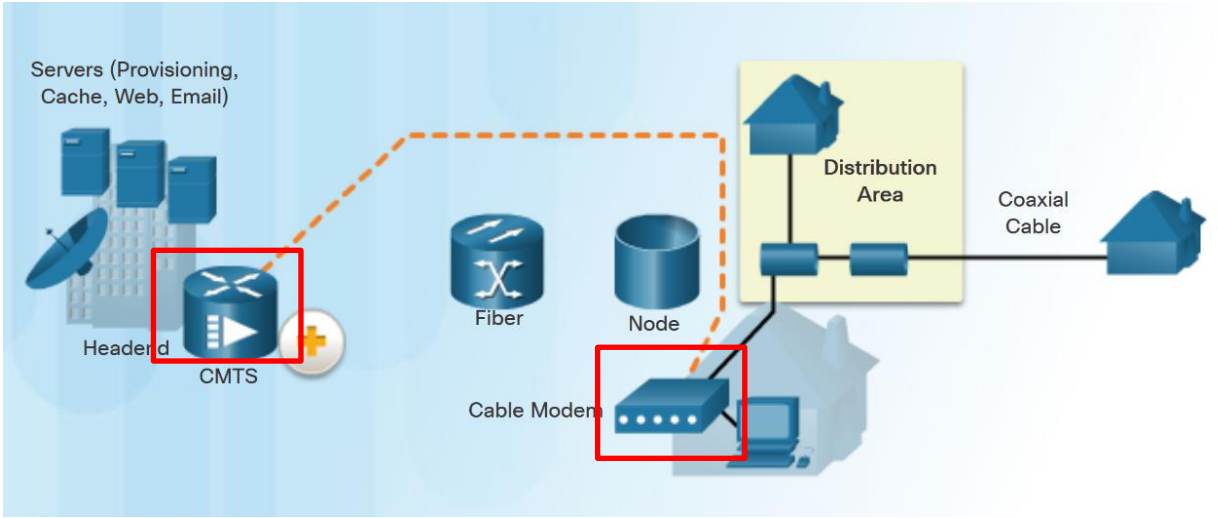
Cable Technology

- Cable system uses a coaxial cable that carries radio frequency (RF) signals across the network to provide Internet access, digital cable television, and telephone service.
- Hybrid fiber-coaxial (HFC) network enables high-speed data.
- The Data over Cable Service Interface Specification (DOCSIS) is the standard for carrying high-bandwidth data over an existing cable system
- Is considered a shared medium so subscribers on the same cable share bandwidth



Cable Technology

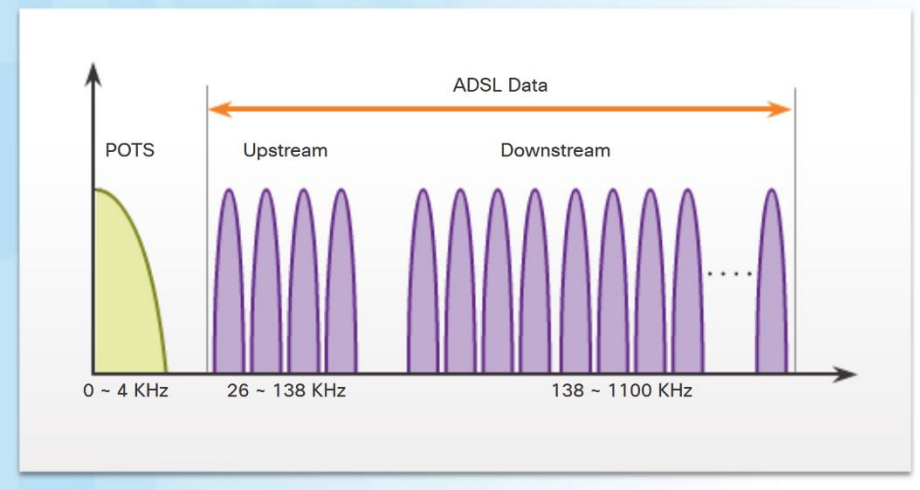
- Two types of equipment are required to send signals upstream and downstream on a cable system:



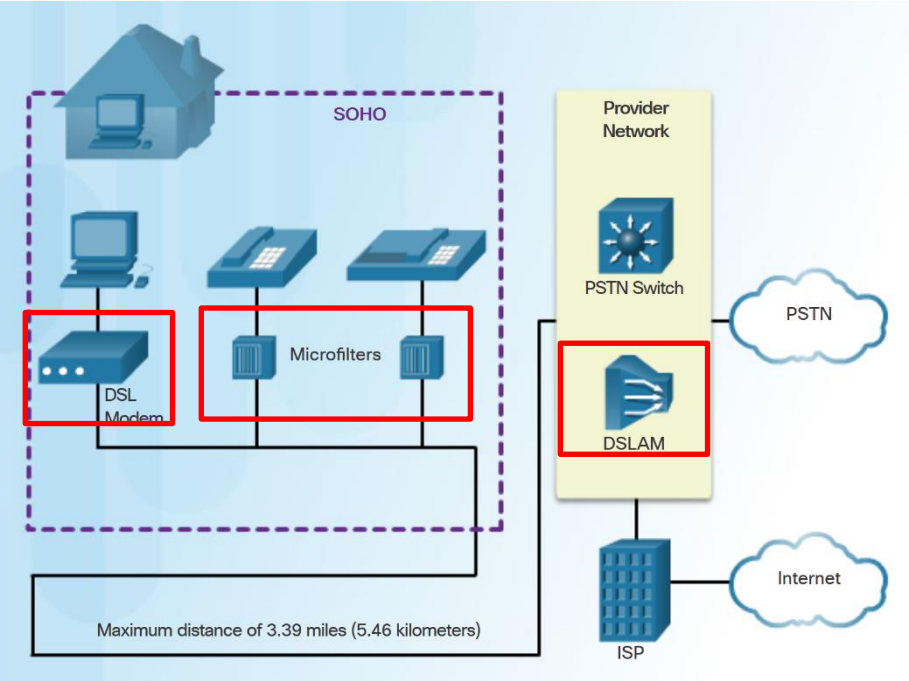
- Cable Modem Termination System (CMTS) at the headend of the cable operator. The headend is a router with databases for providing Internet services to cable subscribers.
- Cable Modem (CM) on the subscriber end.

Digital Subscriber Line

- DSL is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers.
  - Asymmetric DSL (ADSL) provides higher downstream bandwidth to the user than upload bandwidth.
  - Symmetric DSL (SDSL) provides the same capacity in both directions.
  - Very High Speed DSL (VDSL) also provides higher downstream than upstream bandwidth but has higher capacity than ADSL
- DSL data rates are affected by distance from the central office. For satisfactory service, the local loop length must be less than 5.5 km (assuming all copper infrastructure and without repeater).



Digital Subscriber Line



- The DSL connection is set up between the customer premises equipment (CPE) and the DSL access multiplexer (DSLAM) device located at the Central Office (CO).
- Key components in the DSL connection:
  - Transceiver - Usually a modem in a router which connects the computer of the teleworker to the DSL.
  - Microfilter – Connected to the same line to filter out the voice signal for connection to a telephone
  - DSLAM - Located at the CO of the carrier, it combines individual DSL connections from users into one high-capacity link to an ISP.

Digital Subscriber Line

DSL Modem

Microfilter

DSLAM Cabinet

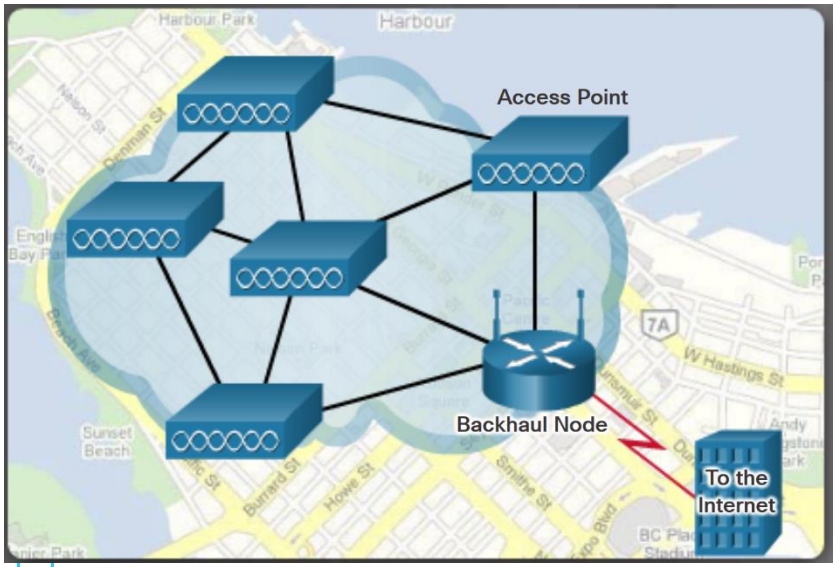
- The DSL connection is set up between the customer premises equipment (CPE) and the DSL access multiplexer (DSLAM) device located at the Central Office (CO).
- Key components in the DSL connection:
  - Transceiver - Usually a modem in a router which connects the computer of the teleworker to the DSL and converts Ethernet to DSL signals.
  - Microfilter – Connected to the same line to filter out the voice signal for connection to a telephone
  - DSLAM - Located at the CO of the carrier, it combines individual DSL connections from users into one high-capacity link to an ISP.
- Advantage of DSL over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM.

Optical Fiber

- Uses an Optical Distribution Network from the central office until the customer premises and is currently the broadband technology offering the highest data rates
- Many municipalities, cities, and providers install fiber-optic cable to the user location. This is commonly referred to as Fiber to the x (FTTx) and includes the following:
  - Fiber to the Home (FTTH) - Fiber reaches the boundary of the residence and subscribers use an Optical Network Unit /Terminal (ONU or ONT) to connect to the network
  - Fiber to the Building (FTTB) - Fiber reaches the boundary of the building with the final connection to the individual living space being made via alternative means.
  - Fiber to the Node/Neighborhood (FTTN) – Optical cabling reaches an optical node that converts optical signals to a format acceptable for twisted pair or coaxial cable to the premise.

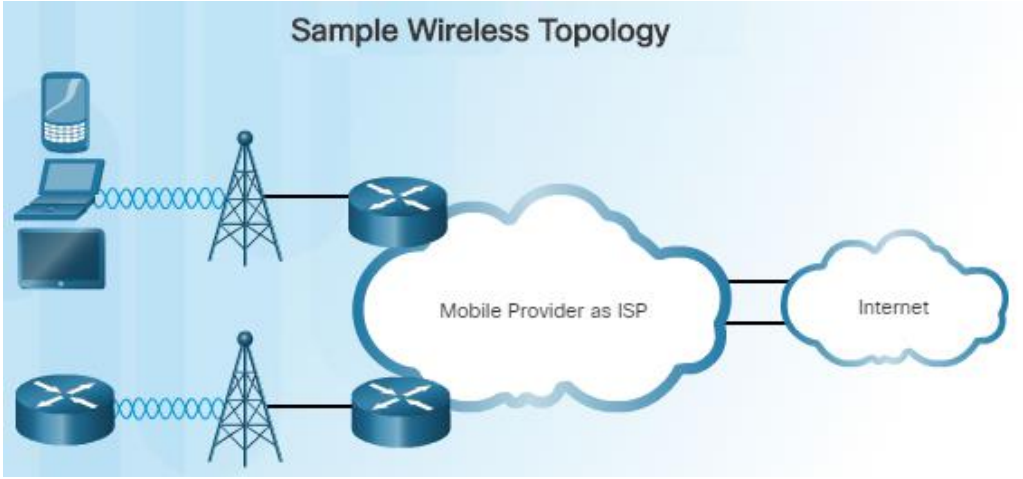
Wireless Internet-Based Broadband

- 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.
- Wireless signals can be negatively affected by factors such as distance from radio towers, interference from other sources and weather.



- **Municipal Wi-Fi** - Most municipal wireless networks use a mesh of interconnected access points as shown in figure.
- **Cellular/mobile** - Mobile phones use radio waves to communicate through nearby cell towers. Cellular speeds continue to increase.
- **Satellite Internet** - Used in locations where land-based Internet access is not available.
- **WiMAX -** has largely been replaced by LTE for mobile access, and cable or DSL for fixed access.

Cellular Broadband



- Cellular service is a wireless broadband technology used to connect users and remote locations where no other WAN access technology is available.
- Mobile device has a small radio antenna, and the provider has a much larger antenna sitting at the top of the tower somewhere within kilometers of the device.

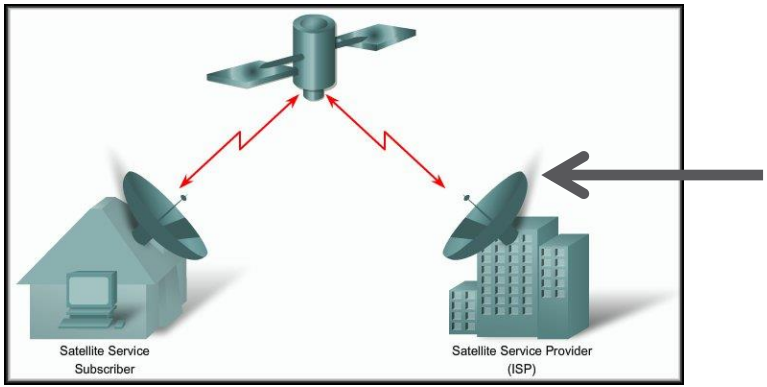
- There are two common cellular industry terms:
  - 3G/4G/5G Wireless – Abbreviation for 3rd, 4th, and 5th generation cellular access.
  - Long-Term Evolution (LTE) – Refers to the current popular mobile broadband standard used. It is considered to be a fourth generation (4G) technology.

Cellular Broadband

Generation	1G	2G	2.5G	3G	3.5G	4G	5G
Start	1970-1980	1990-2000	2001-2004	2004-2005	2006-2010	2011-Now	Soon (2020)
Data Bandwidth	2 Kbps	64 Kbps	144 Kbps	2 Mbps	More than 2 Mbps	1 Gbps	more than 1 Gbps
Technology	Analog Cellular	Digital Cellular	GPRS, EDGE, CDMA	CDMA 2000 (1xRT, EVDO) UMTS, EDGE	EDGE. Wi-Fi	WiMax LTE Wi-Fi	wwww
Service	Voice	Digital Voice, SMS,Higher Capacity Packet Size Data	SMS, MMS	Integrated High Quality Audio, Video & Data	Integrated High Quality Audio, Video & Data	Dynamic Information access, Wearable Devices	Dynamic Information access, Wearable Devices with AI Capabilities
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	Packet	All Packet	All Packet	All Packet
Core Network	PSTN	PSTN	PSTN	Packet N/W	Internet	Internet	Internet

Satellite Internet

- Used in locations where land-based Internet access is not available, or for temporary installations that are continually on the move.
- 3 ways to connect to Internet using satellites:
  - One-way multicast are used for IP multicast-based data, audio, and video distribution.
  - One-way terrestrial return use traditional dialup access to send outbound data through a modem and receive downloads from the satellite.
  - Two-way satellite sends data from remote sites via satellite to a hub. The hub then sends the data to the Internet.



VPN Technology

VPNs can be used to address security concerns incurred when a remote office worker uses broadband services to access the corporate WAN over the internet.

A VPN is an encrypted connection between private networks over a public network. VPN tunnels are routed through the internet from the private network of the company to the remote site or employee host.

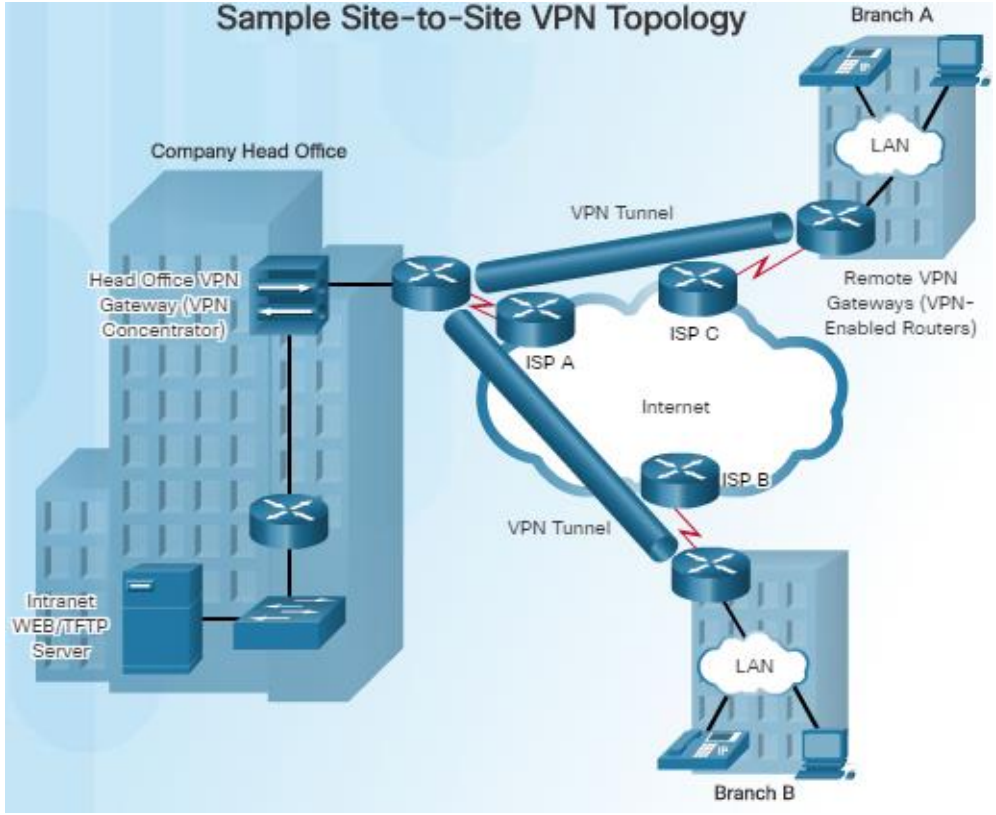
There are several benefits to using VPN:

- **Cost savings** - Eliminates expensive, dedicated WAN links and modem banks.
- **Security** - Advanced encryption and authentication protocols protect data from unauthorized access.
- **Scalability** - Corporations can add large amounts of capacity without adding significant infrastructure.
- **Compatibility with broadband technology** - Supported by broadband service providers such as DSL and cable.

VPNs are commonly implemented as the following:

- **Site-to-site VPN** - VPN settings are configured on routers. Clients are unaware that their data is being encrypted.
- **Remote Access** - The user is aware and initiates remote access connection. For example, using HTTPS in a browser to connect to your bank. Alternatively, the user can run VPN client software on their host to connect to and authenticate with the destination device.

Virtual Private Network Technology



- A VPN is an encrypted connection between private networks over a public network, such as the Internet.
- Due to security risks of sending sensitive data over the public Internet infrastructure,, VPNs can be used to address security concerns incurred when a remote office worker uses broadband services to access the corporate WAN over the internet
- Instead of using a dedicated WAN connection, a VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the private network of the company to the remote site or employee host.

Virtual Private Network Technology

There are several benefits to using VPN:

- **Cost savings** - Eliminates expensive, dedicated WAN links and modem banks.
- **Security** - Advanced encryption and authentication protocols protect data from unauthorized access.
- **Scalability** - Corporations can add large amounts of capacity without adding significant infrastructure.
- **Compatibility with broadband technology** - Supported by broadband service providers such as DSL and cable.

What Did You Learn In This Module?

- A Wide Area Network (WAN) is required to connect beyond the boundary of the LAN.
  - A private WAN is a connection that is dedicated to a single customer.
  - A public WAN connection is typically provided by an ISP or telecommunications service provider using the internet.
- WANs are implemented using the following logical topologies: Point-to-Point, Hub-and-Spoke, Dual-homed, Mesh
- Modern WAN standards cover Layer 1 and Layer 2 specifications
  - Layer 1 protocol standards define how to transfer data over optical fiber using lasers or LEDs (SDH, SONET, and DWDM)
  - Layer 2 protocols define how data will be encapsulated into a frame (broadband, wireless, Ethernet WAN, MPLS, Frame Relay, ATM etc)
- ISP connectivity options include single-homed, dual-homed, multihomed, and dual-multihomed.

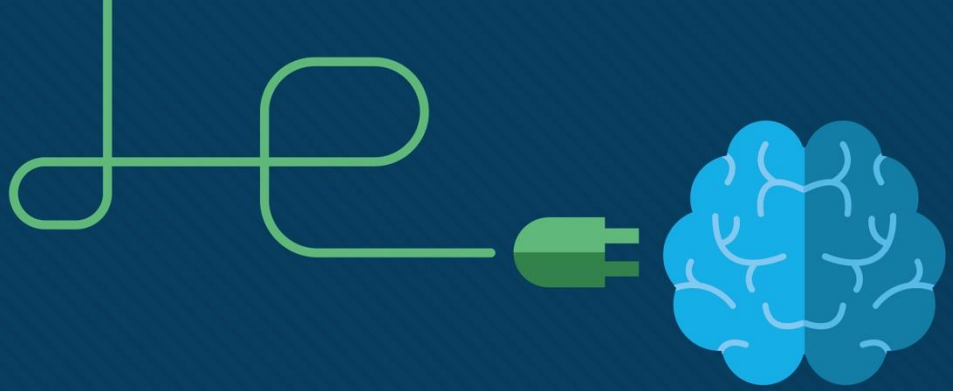
What Did You Learn In This Module?

- Leased lines are a traditional connectivity option that provided a direct point-to-point link between 2 sites.
- Circuit-switching establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate.
  - Dialup used the PSTN to carry low bandwidth analog data transfers
  - ISDN enabled the PSTN local loop to carry digital signals.
- Packet switching segments data into packets that are routed over a shared network.
  - Frame Relay is a simple Layer 2 NBMA WAN technology used to interconnect enterprise LANs.
  - ATM technology is capable of transferring voice, video, and data through private and public networks using a cell-based architecture
- Modern WAN connectivity options include dedicated broadband, Ethernet WAN and MPLS (packet-switched), along with various wired and wireless version of internet-based broadband.
- MPLS is a high-performance service provider WAN routing technology to interconnect clients. MPLS supports a variety of client access methods

Module Summary

What Did You Learn In This Module?

- Internet-based broadband connectivity is an alternative to using dedicated WAN options.
  - Cable - Uses the cable TV network to carry data. Bandwidth is shared by many users. therefore, data rates are often slow during high-usage hours in areas with over-subscription.
  - DSL - Uses telephone lines to carry data. Has limited bandwidth that is distance sensitive
  - Fiber - This option uses optical fiber infrastructure and is currently the fastest wires option available.
  - Cellular/Mobile - Uses the cellular phone network which can reach high speeds with modern 4G/5G technology. With this option, coverage is often the main issue
  - Municipal Wi-Fi - Uses a mesh Wi-Fi network deployed in a city or municipality.
  - Satellite - This option is expensive and provides limited capacity per subscriber. Typically used when no other option is available.
- VPN enable secure routing of data through the internet from the private network of the company to the remote site or employee host using encryption.



Module 5
Network Address Translation

ITNET04

WAN Connectivity

Module Objectives

Module Title: Network Address Translation

Module Objectives:

- Explain the purpose and function of NAT.
- Explain the operation of different types of NAT.
- Configure static NAT, dynamic NAT, port address translation ad port forwarding
- Describe NAT for IPv6.

Module References:

- CCNAv7 ENSA– Module 6

5.1 NAT Characteristics

Recall: Pv4 Address Space

The IPv4 address space includes public and private IP address ranges

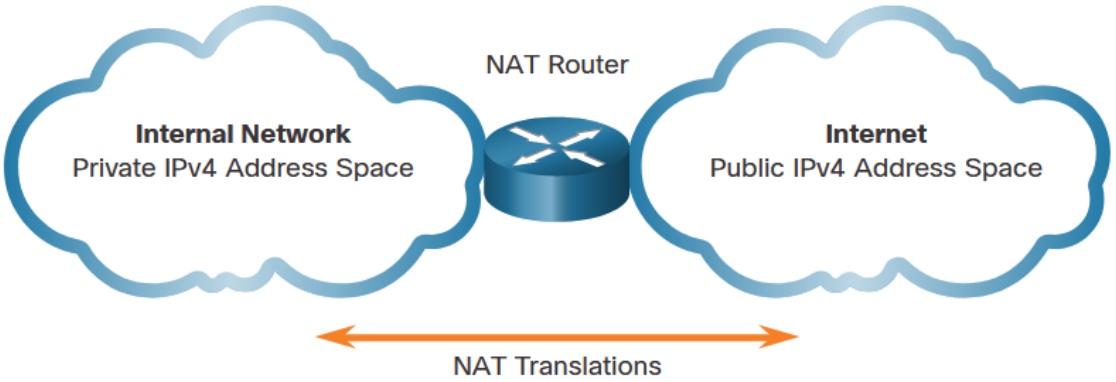
- **Public address**
  - Are guaranteed to be unique once assigned and are hence routable over the Internet
  - Need to be leased from Internet registries or ISPs – must be paid for
- **Private addresses (RFC 1918)**
  - Can be freely used by anyone at no cost
  - No guarantee of uniqueness and so are not routed over the Internet

Class	Private Address Range	CIDR Prefix
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

- Two Issues:
  - Too costly for organizations to provide a public address to each host that needs to access the Internet
  - Not enough public addresses to allow organizations to provide one to each network host.
- Networks need a mechanism that allows them to use private addresses while still being capable of accessing the Internet

What is Network Address Translation?

- Network Address Translation (NAT) provides the translation of private addresses to public addresses when needed.
- NAT typically operates on the border router of a network.
- The primary use is to conserve public IPv4 addresses but also has the added effect of hiding internal IPv4 addresses from outside networks.

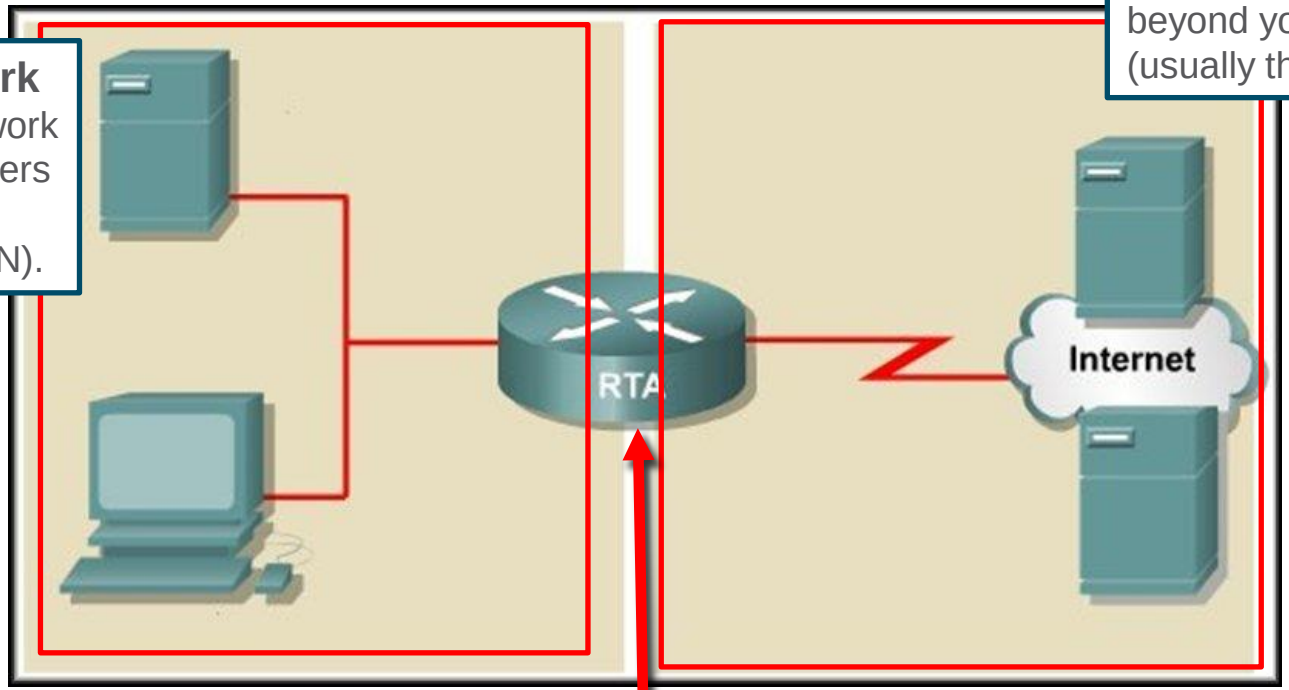


NAT Terminology

- Some terminologies used in NAT:

Inside Network
Refers to a network within your borders (usually the organization LAN).

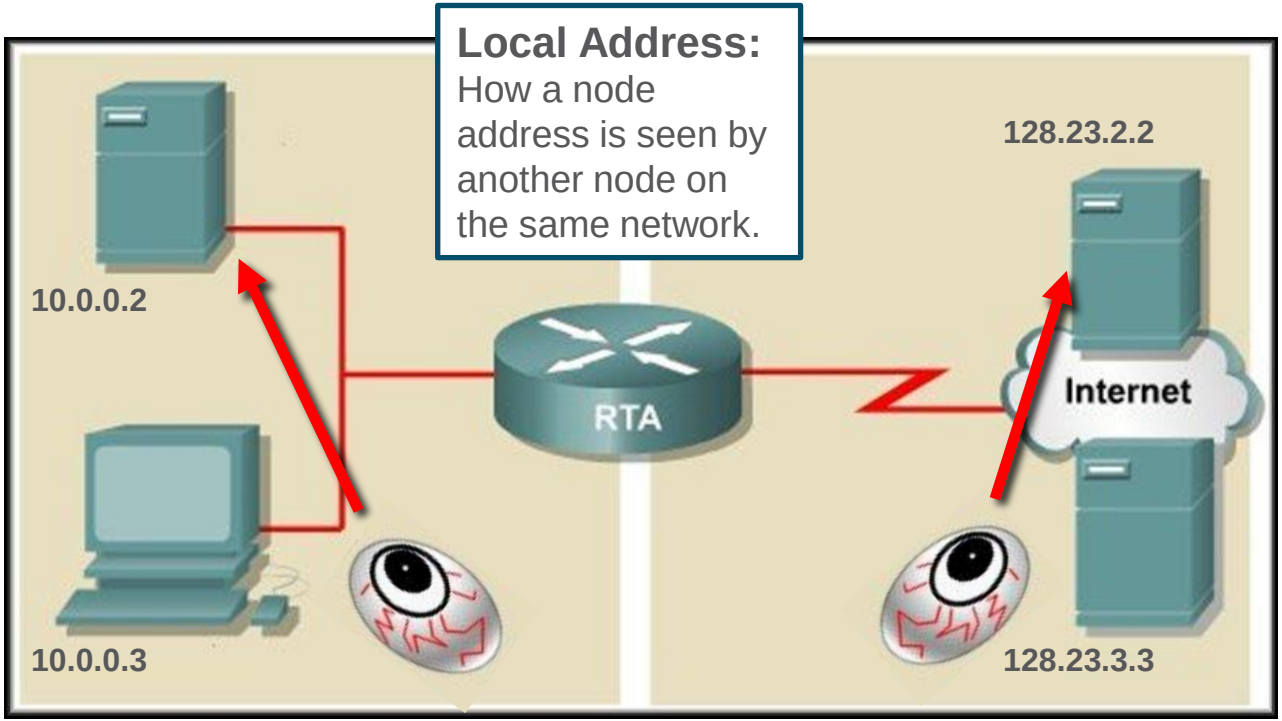
Outside Network
Refers to a network beyond your borders (usually the Internet).



Border Router

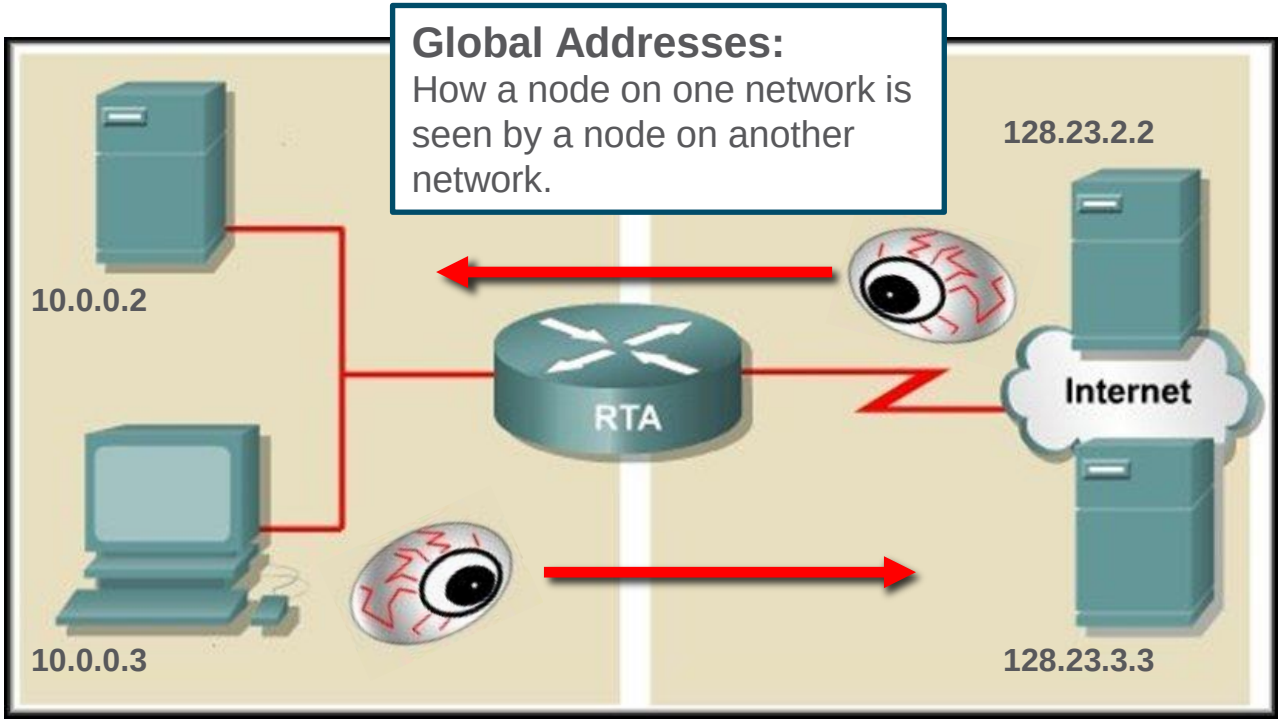
NAT Terminology

- Some terminologies used in NAT:



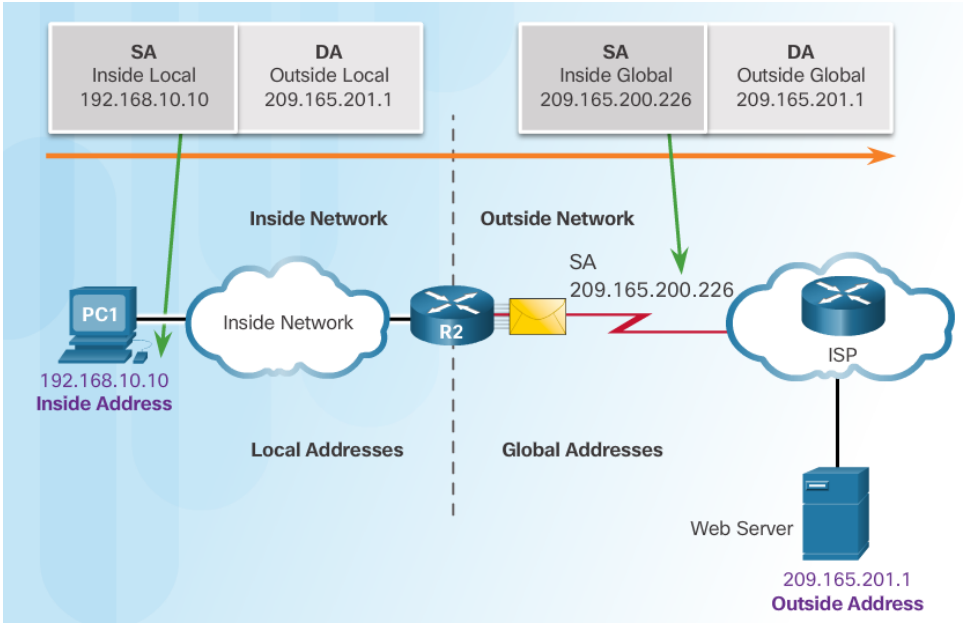
NAT Terminology

- Some terminologies used in NAT:



NAT Terminology

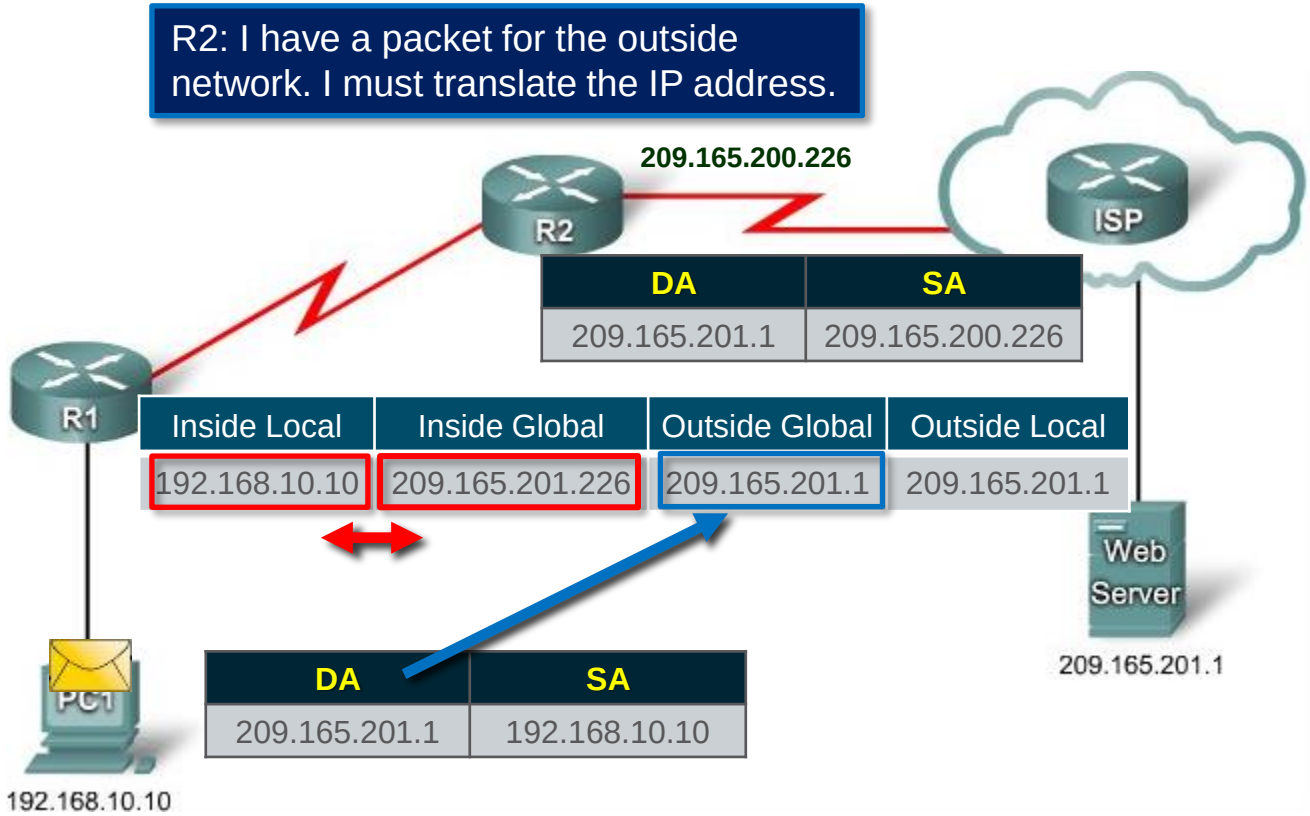
- Inside Local Address:
  - An IP address (usually private) assigned to a host on an inside network.
- Inside Global Address:
  - A valid public address that the host on the inside network is assigned as it exits the router that performs NAT.
- Outside Global Address:
  - A reachable IP address assigned to a host on the Internet.
- *Outside Local Address:*
  - A local address assigned to a host on an outside network. (*Use beyond the scope of this course).*



How NAT Works

Sending PC1 → Server

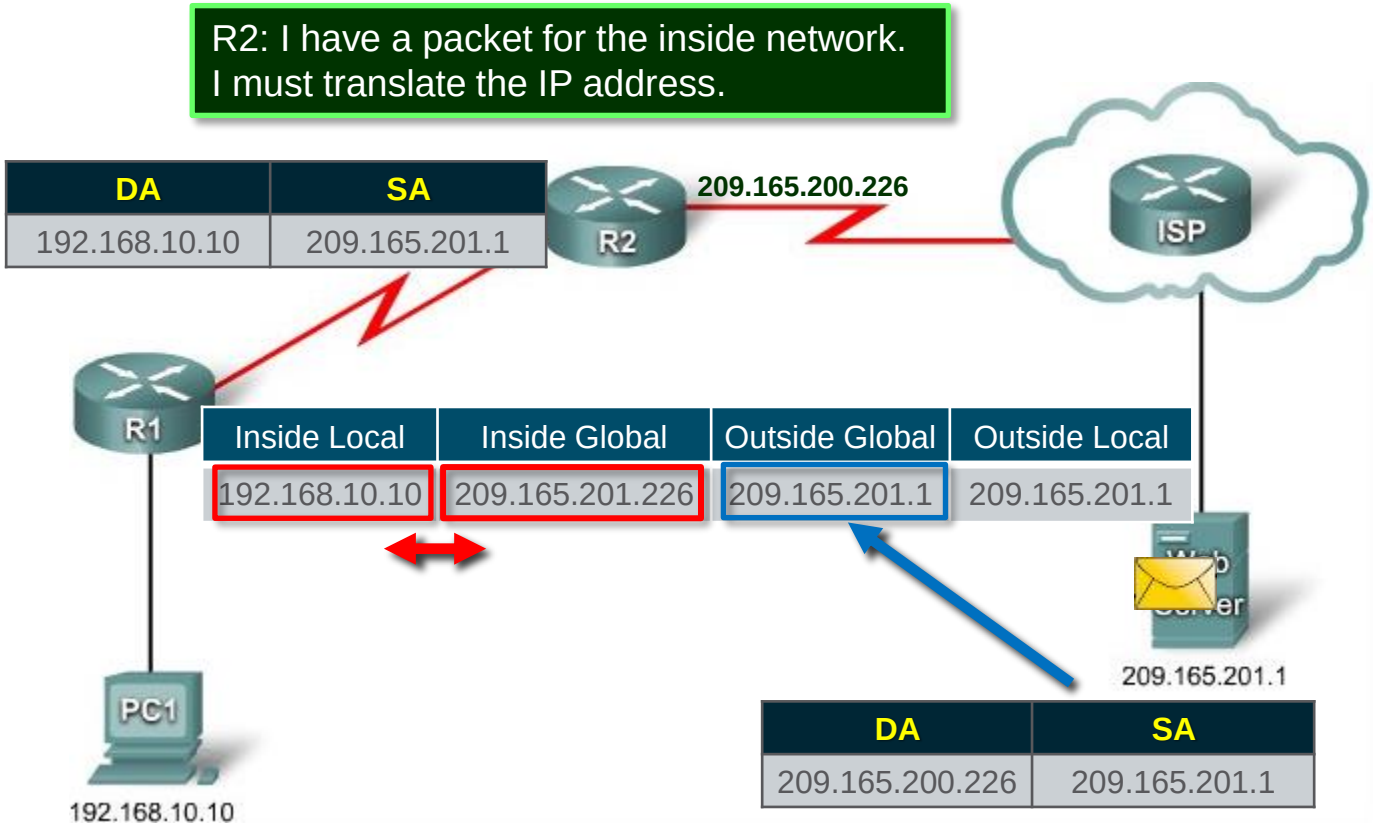
1. PC1 sends a packet for the web server.
2. R2 receives the packet and reads the source address to determine if it needs translation.
3. R2 adds mapping of the local to global address to an internal translation table.
4. R2 sends the packet with the translated source address toward the destination.



How NAT Works

Receiving Server → PC1

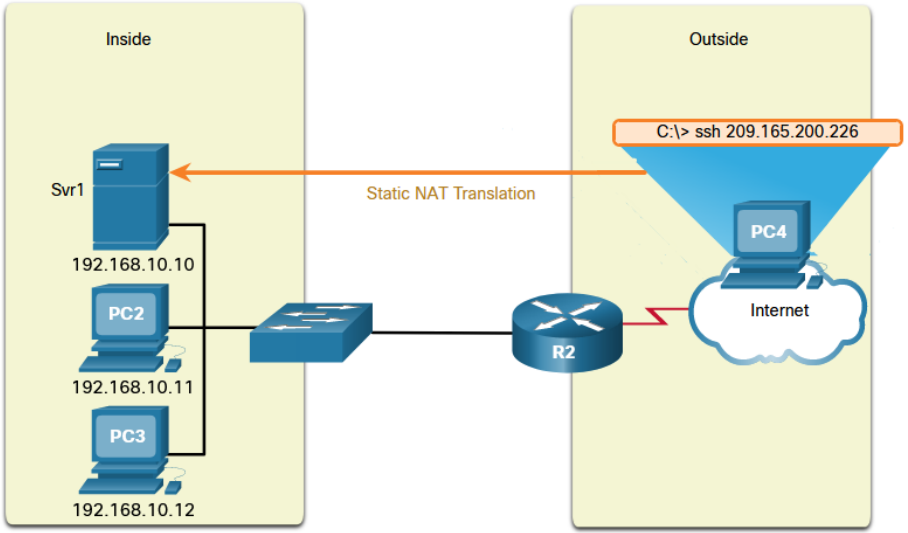
5. The web server responds with a packet addressed to the inside global address of PC1
6. R2 receives the packet with destination address and checks the NAT table and finds an entry for this mapping.
7. R2 uses this information and translates the inside global address to the inside local address then forwards the packet toward PC1.



5.2 Static NAT

Static NAT Overview

- **Static NAT** uses a 1-to-1 mapping of local and global addresses configured by the network administrator that remain constant.
- Allows external devices to initiate connections to internal devices using the statically assigned public address.
  - Useful for web servers or devices that must have a consistent address that is accessible from the Internet (e.g. company web server).
  - It is also useful for devices that must be accessible by authorized personnel when offsite.
- **Note:** Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

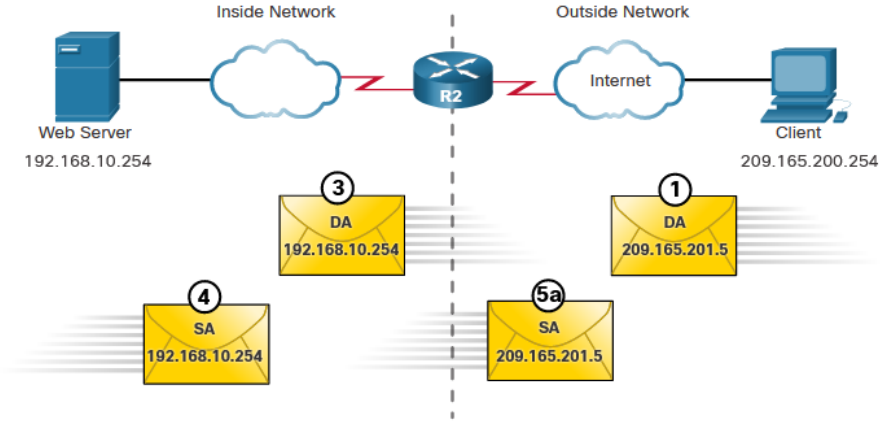


Static NAT Table	
Inside Local Address	**Inside Global Address - Addresses reachable via R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Analyze Static NAT

The static NAT translation process between a client and the a web server:

1. The client sends a packet to the web server.
2. R2 receives packets from the client on its NAT outside interface and checks its NAT table.
3. R2 translates the inside global address of to the inside local address and forwards the packet towards the web server.
4. The web server receives the packet and responds to the client using its inside local address.
5. (a) R2 receives the packet from the web server on its NAT inside interface with source address of the inside local address of the web server and (b) translates the source address to the inside global address.

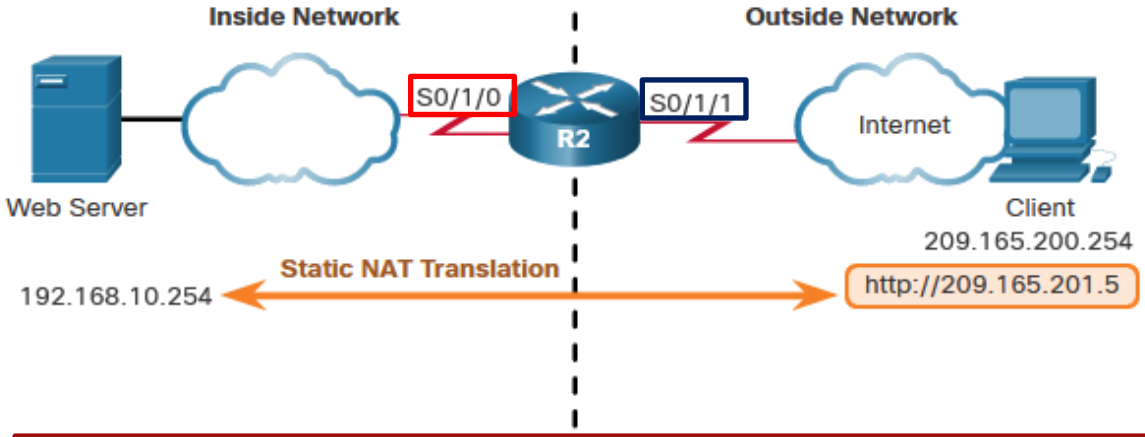


	Inside Local Address	Inside Global Address	Outside Local Address	Outside Global Address
2 5b	192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

Configure Static NAT

To configure static NAT:

- **Step 1** - Create a mapping between the inside local address and the inside global addresses using the **ip nat inside source static** *inside-local inside-global* command.
- **Step 2** – Configure the interfaces participating in the translation as inside or outside relative to NAT with the **ip nat inside** and **ip nat outside** commands.




```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Verify Static NAT

To verify NAT operation, issue the **show ip nat translations** command.

- This command shows active NAT translations.
- For a static NAT configuration, the translation is always present in the NAT table regardless of any active communications.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local      Outside global
---  209.165.201.5       192.168.10.254     ---                ---
Total number of translations: 1
```

- If the command is issued during an active session, the output also indicates the address of the outside device.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local      Outside global
tcp  209.165.201.5       192.168.10.254     209.165.200.254    209.165.200.254
---  209.165.201.5       192.168.10.254       ---                ---
Total number of translations: 2
```

Verify Static NAT (Cont.)

Another useful command is **show ip nat statistics.**

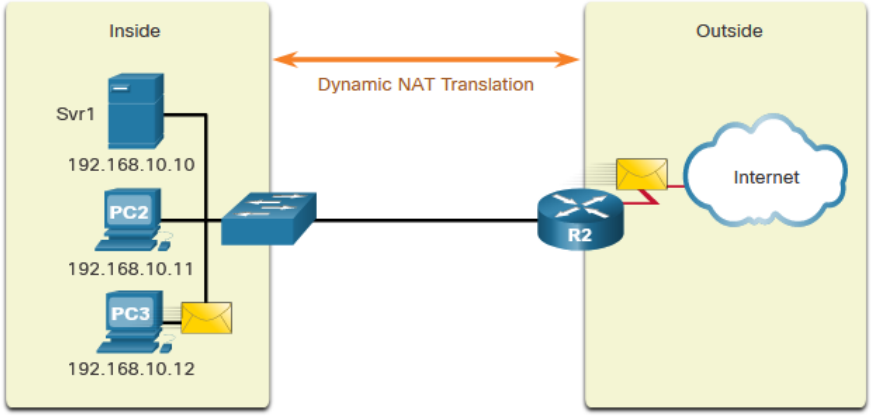
- It displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number of addresses that have been allocated.
- To verify that the NAT translation is working, it is best to clear statistics from any past translations using the **clear ip nat statistics** command before testing.

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 1
(output omitted)
```

5.3 Dynamic NAT

Dynamic NAT Overview

- **Dynamic NAT** uses a pool of public addresses and assigns them on a first-come, first-served basis.
- When an inside device requests access to an outside network, an available address is automatically assigned from the pool.
- Requires that enough public addresses are available to satisfy the expected number of simultaneous user sessions.
- If all addresses in the pool are in use, a device must wait for an available address before it can access the outside network.
- Requires an internal device to initiate outgoing traffic first before it can receive incoming packets



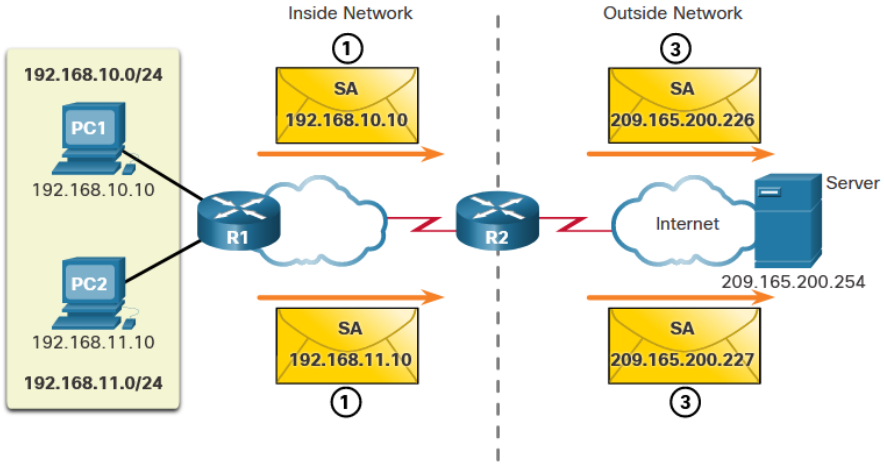
IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool – Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Analyze Dynamic NAT – Inside to Outside

Dynamic NAT translation process:

1. PC1 and PC2 send packets requesting a connection to the server.
2. R2 receives the first packet from PC1, checks if the packet should be translated, selects an available global address from the pool, and creates a translation entry in the NAT table.
3. R2 replaces the inside local source address of PC1 with the translated inside global address and forwards the packet.

   The same process occurs for the packet from PC2 using the a different address from the pool



	IPv4 NAT Pool	
	Inside Local Address Pool	**Inside Global Address**
②	192.168.10.10	209.165.200.226
②	192.168.11.10	209.165.200.227

Analyze Dynamic NAT – Outside to Inside

Dynamic NAT translation process:

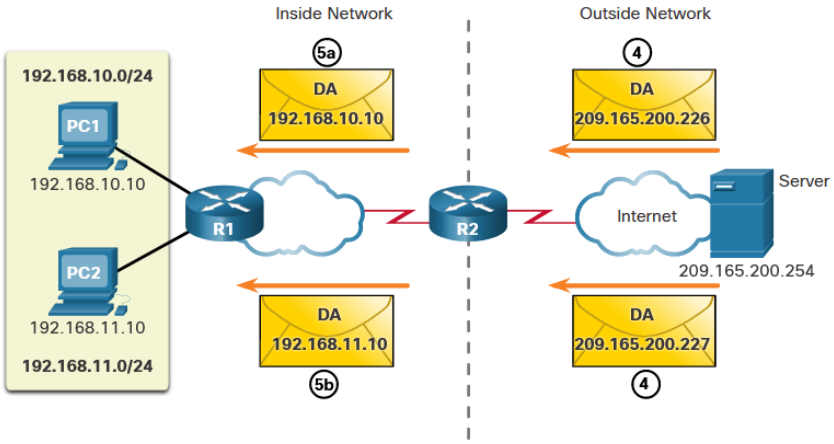
4. The server receives the packet from PC1 and responds using PC1's inside global address (209.165.200.226) as the destination address

   The same process is used when the server receives the packet from PC2. It responds using PC2's inside global address (209.165.200.227) as destination

5. When R2 receives the packet, it performs a NAT table lookup and translates the address back to the inside local address and forwards the packet to the local host

   (a) A packet with destination 209.165.200.226 is translated back to the inside local address of PC1

   (b) A packet with destination 209.165.200.227 is translated back to the inside local address of PC2

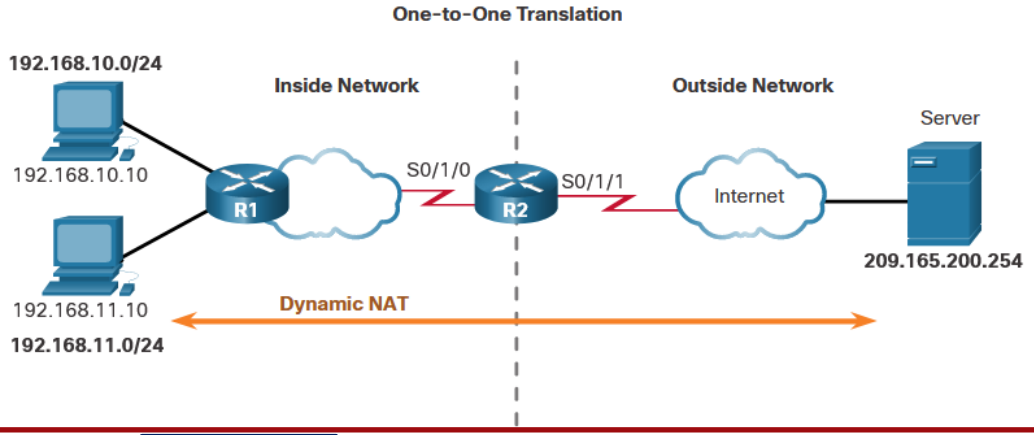


	IPv4 NAT Pool	
	Inside Local Address Pool	**Inside Global Address**
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

Configure Dynamic NAT

To configure dynamic NAT:

- **Step 1** - Define the pool of addresses that will be used for translation using the **ip nat pool** *pool_name start-add end-add* **netmask** *mask* command.
- **Step 2** - Configure a standard ACL to identify (permit) only those addresses that will be translated.
- **Step 3** - Bind the ACL to the pool, using the **ip nat inside source list** *list_id* **pool** *pool_name* command.

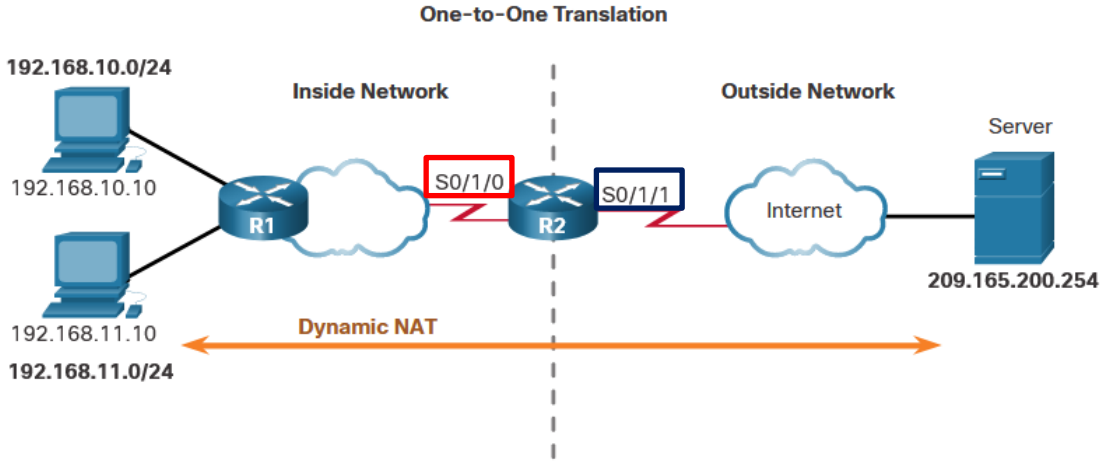



```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Configure Dynamic NAT (Cont.)

To configure dynamic NAT:

- **Step 4** - Identify which interfaces are inside **(ip nat inside).**
- **Step 5** - Identify which interfaces are outside **(ip nat outside)**.




```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

Managing Dynamic NAT

- By default, translation entries time out after **24 hours**
- Timeout duration can been reconfigured with the **ip nat translation timeout** *timeout-seconds* command in global configuration mode.
- To clear dynamic entries before the timeout has expired, use the **clear ip nat translation** privileged EXEC mode command.

Command	Description
clear ip nat translation *	Clears all dynamic address translation entries from the NAT translation table.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation.

```
R2# clear ip nat translation *
R2# show ip nat translation
```

Verify Dynamic NAT

If dynamic NAT is configured, the **show ip nat translations** command displays any dynamic translations that have been created by traffic.

```
R2# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.228    192.168.10.10      ---                ---
--- 209.165.200.229    192.168.11.10      ---                ---
R2#
```

Adding the **verbose** keyword displays additional information about each translation, including how long ago the entry was created and used,.

```
R2# show ip nat translation verbose
Pro Inside global      Inside local       Outside local      Outside global
tcp 209.165.200.228    192.168.10.10      ---                ---
    create 00:02:11, use 00:02:11 timeout:86400000, left 23:57:48, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 10, lc_entries: 0
tcp 209.165.200.229    192.168.11.10      ---                ---
    create 00:02:10, use 00:02:10 timeout:86400000, left 23:57:49, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 12, lc_entries: 0
R2#
```

Verify Dynamic NAT (Cont.)

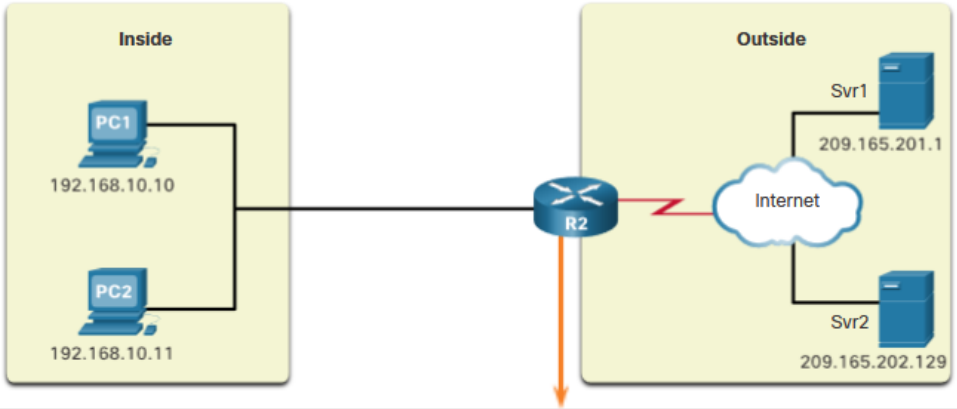
The **show ip nat statistics** command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and how many of the addresses have been allocated.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 0 extended)
Peak translations: 4, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 47  Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 4
 pool NAT-POOL1: netmask 255.255.255.224
      start 209.165.200.226 end 209.165.200.240
      type generic, total addresses 15, allocated 2 (13%), misses 0
(output omitted)
R2#
```

5.4 Port Address Translation

Port Address Translation Overview

- **Port Address Translation (PAT),** also known as **NAT overload**, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
- With PAT, the NAT router uses the source port number of the client to uniquely identify the specific NAT translation and track the session.
- Requires an internal device to initiate an outgoing session first before it can receive incoming packets similar to dynamic NAT



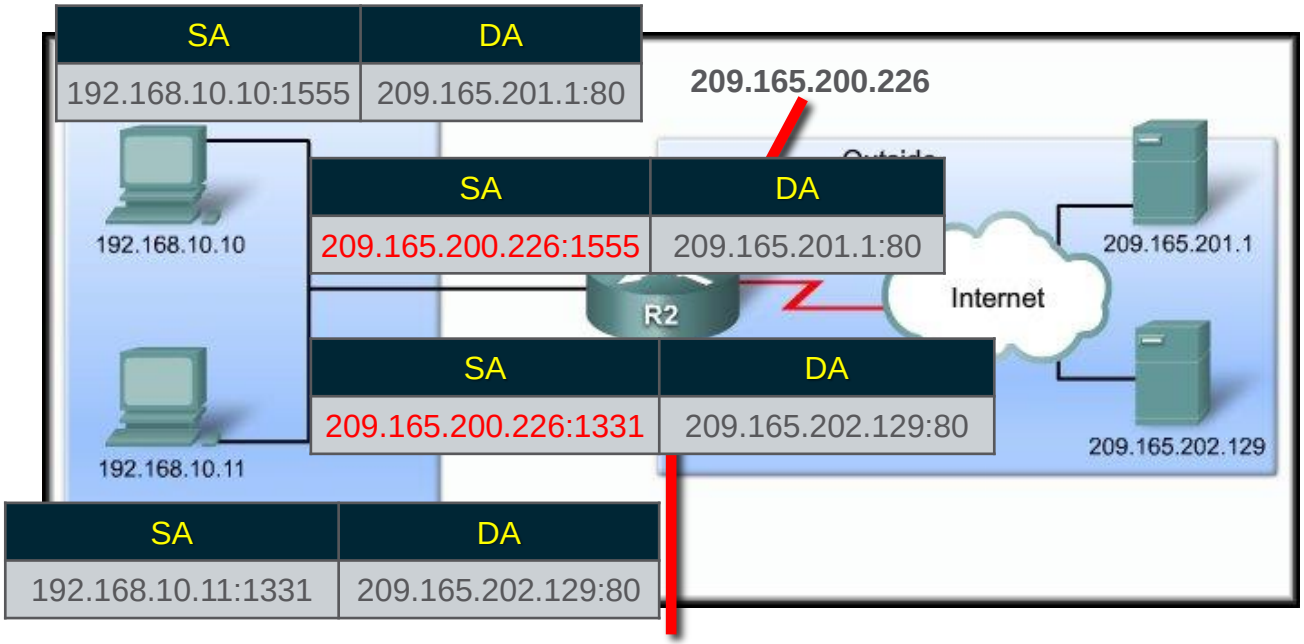
NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Same global address, different port numbers

Analyze PAT – PC to Server

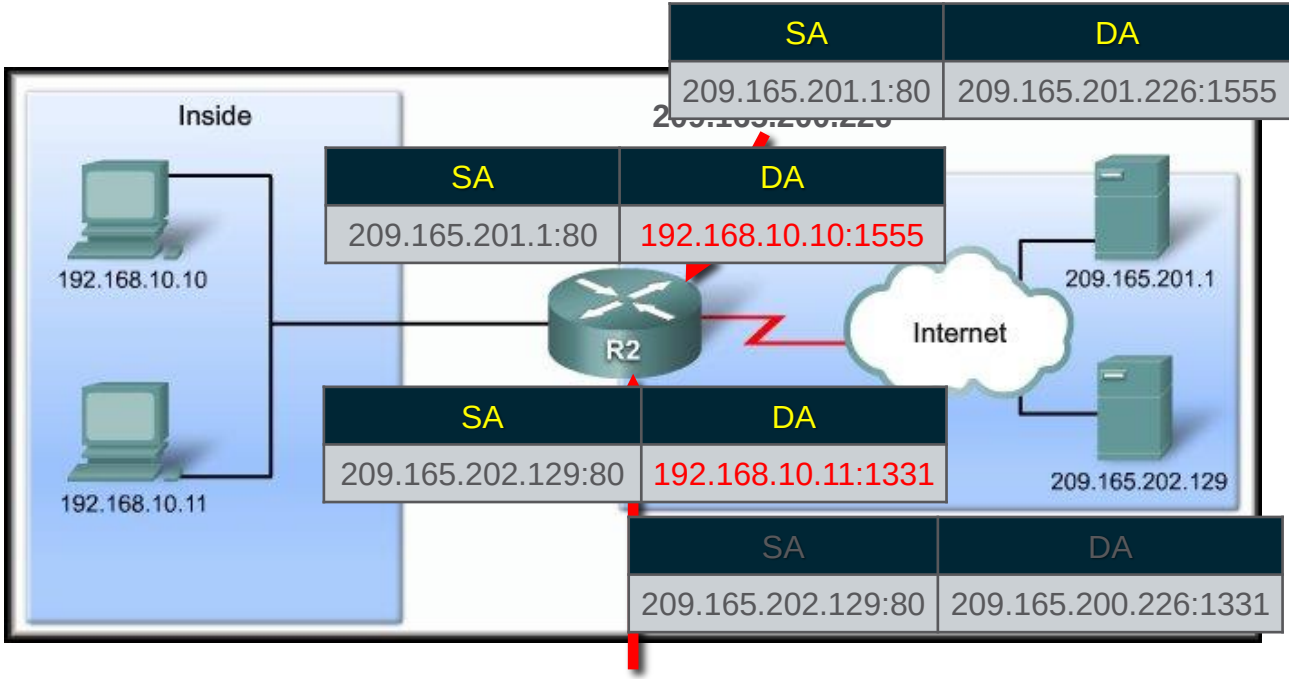
1. PC1 sends a packet to Svr1
2. R2 modifies the source IPv4 address to 209.165.200.226, tracks this with the source port and forwards it towards Svr1.
3. PC2 sends a packet to Svr2
4. R2 modifies the source IPv4 address to 209.165.200.226, tracks this with the source port and forwards it towards Svr2.



Inside Local	Inside Global	Outside Global
192.168.10.10:1555	209.165.201.226:1555	209.165.201.1:80
192.168.10.11:1331	209.165.201.226:1331	209.165.201.129:80

Analyze PAT – Server to PC

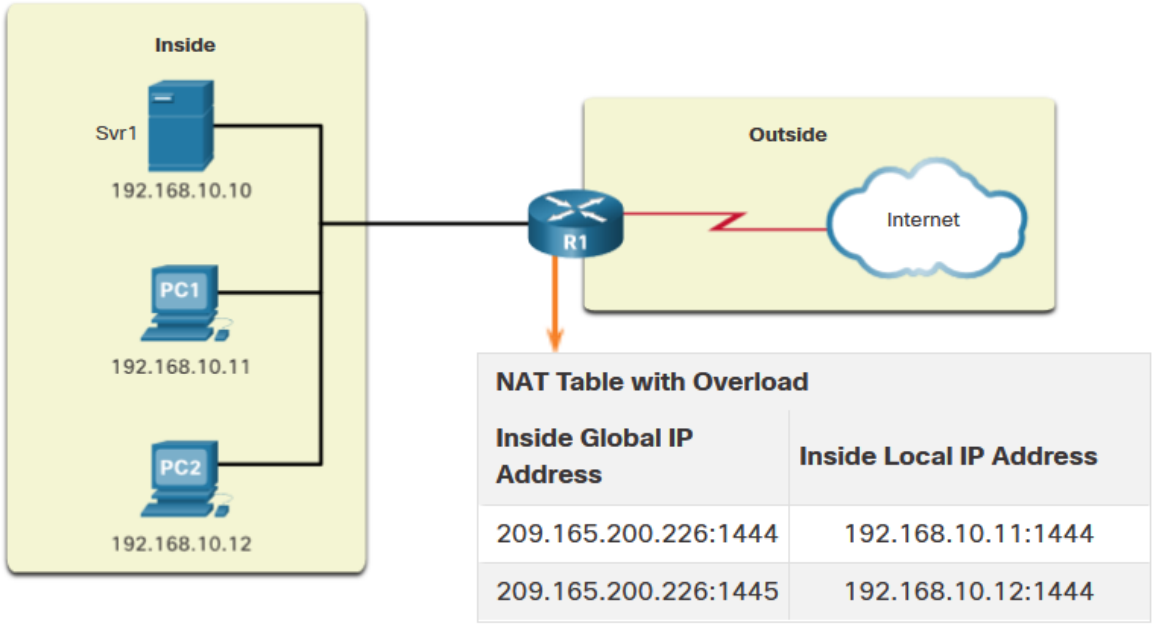
1. The servers use the source port from the received packet as the destination port, and the source address as the destination address for the return traffic.
2. R2 changes the destination address of the packet from Srv1 from 209.165.200.226 to 192.168.10.10 and the packet from Srv2 from 209.165.200.226 to 192.1698.10.11
3. R2 sends the packets to PC1 and PC2 respectively



Inside Local	Inside Global	Outside Global
192.168.10.10:1555	209.165.201.226:1555	209.165.201.1:80
192.168.10.11:1331	209.165.201.226:1331	209.165.201.129:80

Next Available Port

PAT attempts to preserve the original source port. If the original source port is already used, PAT assigns the first available port number



NAT Table with Overload

Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

- When there are no more ports available and there is more than one external address in the address pool, PAT moves to the next address to try to allocate the original source port.
- The process continues until there are no more available ports or external IPv4 addresses in the address pool.

NAT and PAT Comparison

Summary of the differences between NAT and PAT.

NAT - Only modifies the IPv4 addresses

Inside Global Address	Inside Local Address
209.165.200.226	192.168.10.10

PAT - PAT modifies both the IPv4 address and the port number.

Inside Global Address	Inside Local Address
209.165.200.226:2031	192.168.10.10:2031

NAT	PAT
One-to-one mapping between Inside Local and Inside Global addresses.	One Inside Global address can be mapped to many Inside Local addresses.
Uses only IPv4 addresses in translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in translation process.
A unique Inside Global address is required for each inside host accessing the outside network.	A single unique Inside Global address can be shared by many inside hosts accessing the outside network.

Packets without a Layer 4 Segment

- Some packets do not contain a Layer 4 port number, such as ICMPv4 messages. Each of these types of protocols is handled differently by PAT.

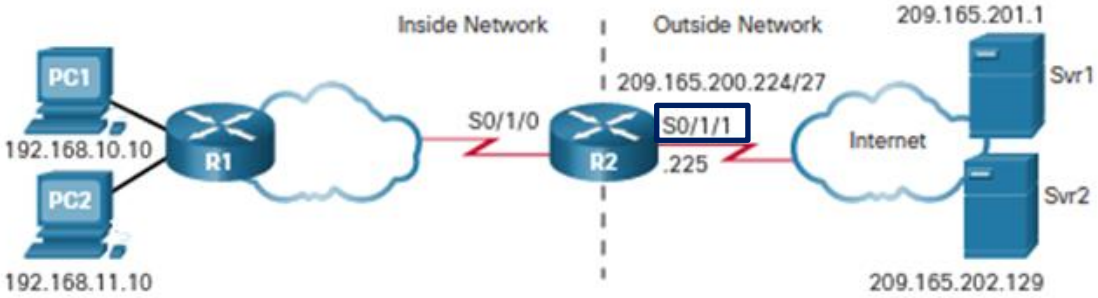
- For example, ICMPv4 query messages, echo requests, and echo replies include a Query ID. ICMPv4 uses the Query ID to identify an echo request with its corresponding echo reply.

Note: Other ICMPv4 messages do not use the Query ID. These messages and other protocols that do not use TCP or UDP port numbers vary and are beyond the scope of this curriculum.

Configure PAT to Use a Single IPv4 Address (Option A)

To configure PAT to use a single IPv4 address configured on the outside interface:

- **Step 1A** - Configure a standard ACL to identify (permit) only those addresses that will be translated.
- **Step 2A** - Bind the ACL to the interface using the **ip nat inside source list** *acl_id* **interface** *int_id* **overload** command.



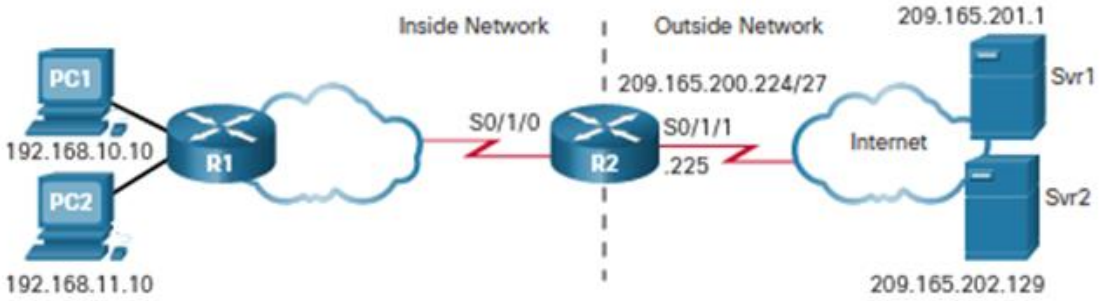

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 interface s0/0/1 overload
```

This approach is commonly used when only the network has only 1 IP address and is especially useful if the public address is assigned dynamically by the ISP

Configure PAT to Use an Address Pool (Option B)

An ISP may allocate more than one public IPv4 address to an organization. In this scenario the organization can configure PAT to use a pool of IPv4 public addresses for translation.

- **Step 1B** - Define the pool of addresses that will be used for translation using the **ip nat pool** *pool_name start-add end-add* **netmask** *mask* command.
- **Step 2B -** Configure a standard ACL to identify (permit) only those addresses that will be translated.
- **Step 3B** - Bind the ACL to the interface using the **ip nat inside source list** *acl_id* **pool** *pool_name* **overload** command.

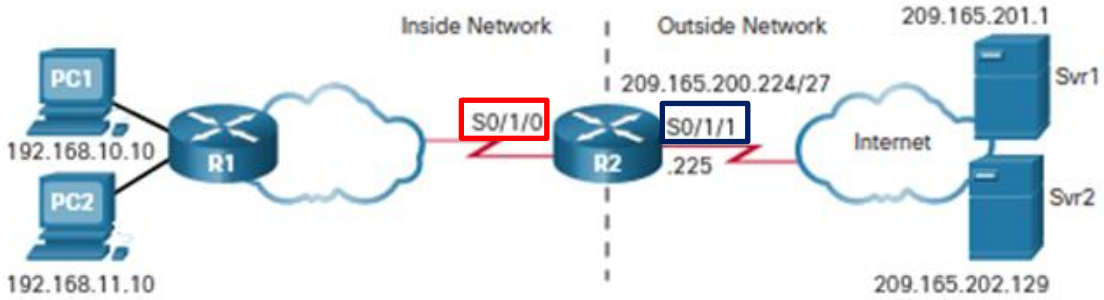



```
R2(config)# ip nat pool PAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool PAT-POOL1 overload
```

Configure PAT (con't)

To configure PAT:

- **Step 4** - Identify which interfaces are inside **(ip nat inside).**
- **Step 5** - Identify which interfaces are outside **(ip nat outside)**.




```
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

Verify PAT

The same commands used to verify static and dynamic NAT are used to verify PAT. The **show ip nat translations** command displays the translations from two different hosts to different web servers.

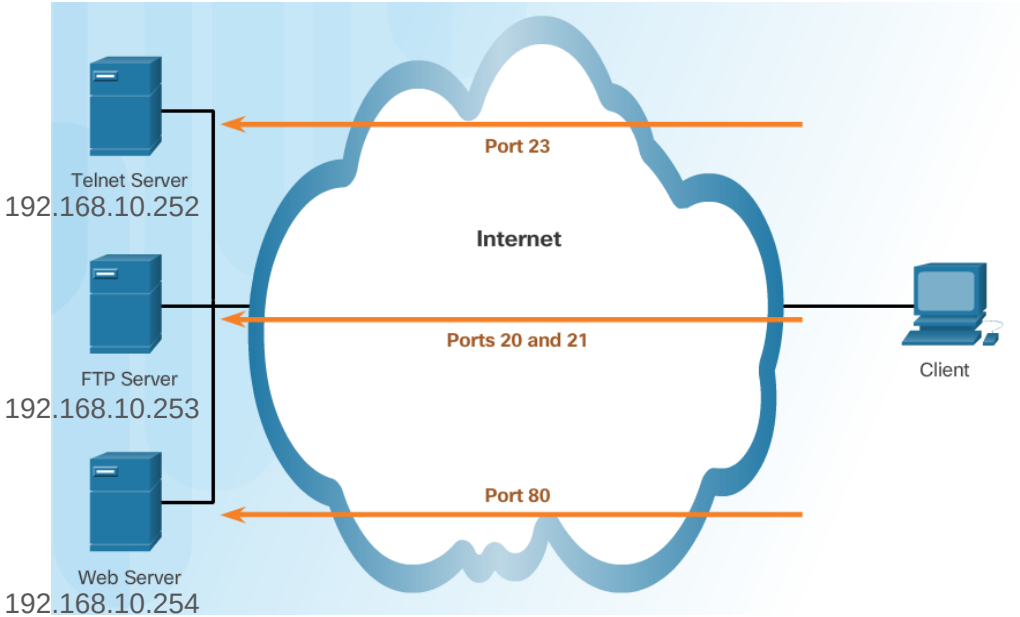
```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local      Outside global
tcp 209.165.200.225:1444  192.168.10.10:1444  209.165.201.1:80   209.165.201.1:80
tcp 209.165.200.225:1445  192.168.11.10:1444  209.165.202.129:80 209.165.202.129:80
R2#
```

When PAT is enabled, multiple inside hosts are allocated the same IPv4 inside global address. The source port numbers in the NAT table differentiate the transactions.

5.5 Port Forwarding

Port Forwarding Overview

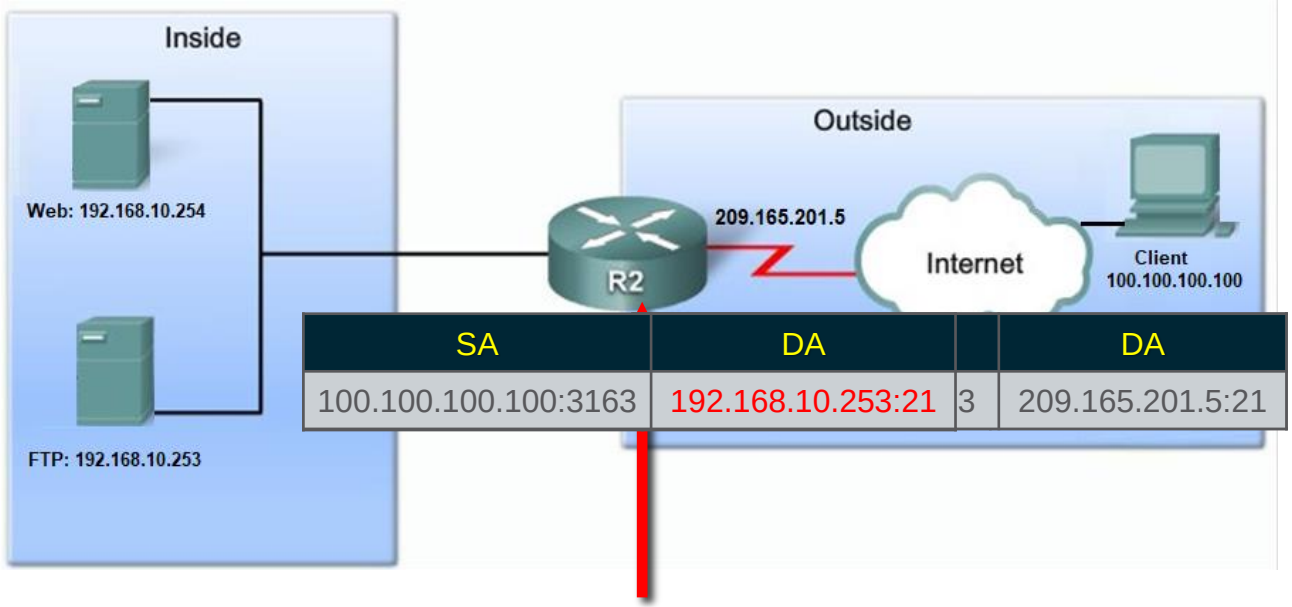
- **Port Forwarding** allows an external device to reach an internal device using static mappings with a specific **port number** for translation
- Solves the problem of PAT only allowing translations for traffic destined for external networks at the request of internal devices.
- Makes it possible to host multiple services on separate servers in the internal network while sharing a single public IP address with other internal hosts



Inside Local	Inside Global	Outside Global
192.168.10.252:23	209.165.201.5:23	100.100.100.100:1555
192.168.10.253:20	209.165.201.5:20	100.100.100.100:1330
192.168.10.253:21	209.165.201.5:21	100.100.100.100:3163
192.168.10.254:80	209.165.201.5:80	100.100.100.100:2481

Analyze Port Forwarding – Client to Internal Server

1. The external client PC access the web service of the inside global address using a destination port 80 (HTTP)
2. R2 translates the destination address to the IP address of the web server (192.168.10.254) and forwards it
3. The external client PC access the file service of the inside global address using a destination port 21 (FTP)
4. R2 translates the destination address to the IP address of the FTP server (192.168.10.253) and forwards it

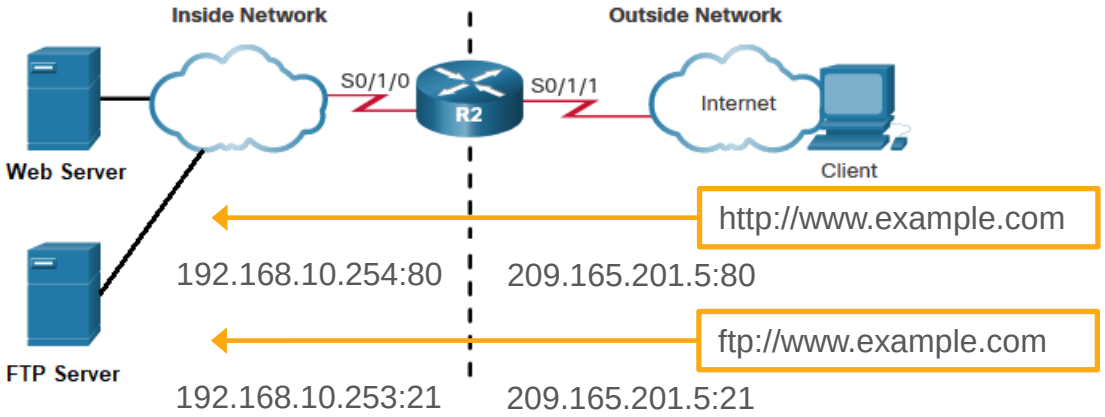


Inside Local	Inside Global	Outside Global
192.168.10.253:21	209.165.201.5:21	100.100.100.100:3163
192.168.10.254:80	209.165.201.5:80	100.100.100.100:2481

Configure Port Forwarding

To configure port forwarding:

- **Step 1** - Create a mapping between the inside local and inside global addresses using the **ip nat inside source static** *l4proto inside-local local-port inside-global global-port* command.
- **Step 2** – Configure the interfaces participating in the translation with the **ip nat inside** and **ip nat outside** commands.




```
R2(config)# ip nat inside source static tcp 192.168.10.254 80 209.165.201.5 80
R2(config)# ip nat inside source static tcp 192.168.10.253 21 209.165.201.5 20
R2(config)# ip nat inside source static tcp 192.168.10.253 21 209.165.201.5 21
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Verify Port Forwarding

The **show ip nat translations** command for port forwarding is similar to static NAT except that the port number mapping are included

- Port forwarding entries remain in the NAT table even when there are no ongoing transactions

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local      Outside global
tcp  209.165.201.5:20    192.168.10.253:20    ---                ---
tcp  209.165.201.5:21    192.168.10.253:21    ---                ---
tcp  209.165.201.5:80    192.168.10.254:80    ---                ---

Total number of translations: 3
```

- During an active session, the output also indicates the address of the outside device.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local          Outside global
tcp  209.165.201.5:20    192.168.10.253:20    ---                    ---
tcp  209.165.201.5:21    192.168.10.253:21    ---                    ---
tcp  209.165.201.5:80    192.168.10.254:80    ---                    ---
tcp  209.165.201.5:80    192.168.10.254:80  100.100.100.100:2481   100.100.100.100:2481
Total number of translations: 4
```

5.6 NAT Caveats

NAT Pros and Cons

NAT provides many benefits:

- Conserves the legally registered addressing scheme by allowing the privatization of intranets and application port-level multiplexing.
- Increases the flexibility of connections to the public network.
- Provides consistency for internal network addressing schemes.
- Allows the existing private IPv4 address scheme to remain while allowing for easy change to a new public addressing scheme.
- Hides the IPv4 addresses of users and other devices.

NAT does have drawbacks:

- Increases forwarding delays.
- End-to-end addressing is lost.
- End-to-end IPv4 traceability is lost.
- Consumes more RAM on the router
- Complicates the use of tunneling protocols, such as IPsec.
- Services that require the initiation of TCP connections from the outside network, or stateless protocols, such as those using UDP, can be disrupted.

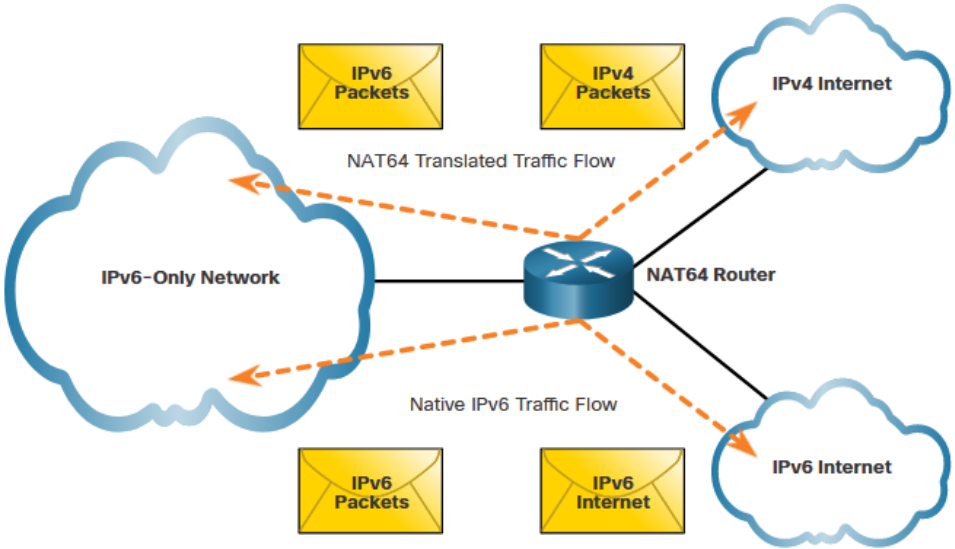
NAT for IPv6?

IPv6 was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary.

- However, IPv6 does include its own IPv6 private address space, unique local addresses (ULAs).
- IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4 but are meant for only local communications within a site.
- ULA addresses are not meant to provide additional IPv6 address space, nor to provide a level of security.
- IPv6 does provide for protocol translation between IPv4 and IPv6 known as NAT64.

NAT64

- NAT for IPv6 is used in a much different context than NAT for IPv4.
- The varieties of NAT for IPv6 are used to transparently provide access between IPv6-only and IPv4-only networks, as shown. It is not used as a form of private IPv6 to global IPv6 translation.
- NAT for IPv6 is intended only as a temporary mechanism to assist in the migration from IPv4 to IPv6.

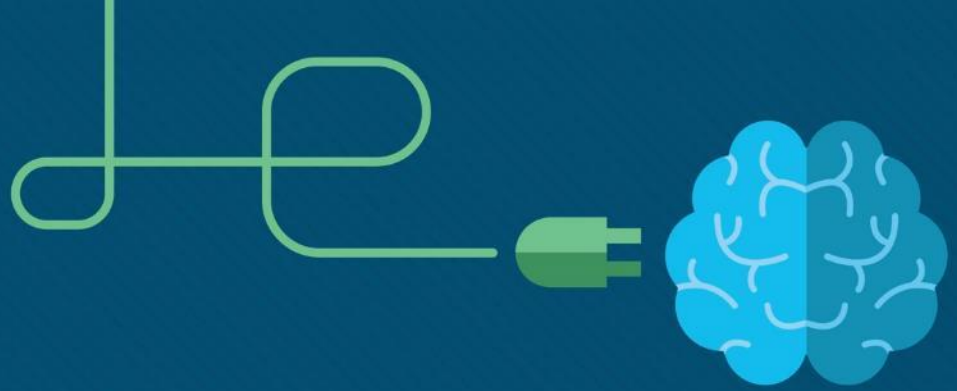


What Did You Learn In This Module?

- There are not enough public IPv4 addresses to assign a unique address to each device connected to the internet.
- Network address translation (NAT) conserves public IPv4 addresses by allowing traffic from hosts assigned with private addresses to be translated into a routable public address
- In NAT terminology, the inside network is the set of local networks that are subject to translation. The outside network refers to all other networks.
  - Inside address are the addresses of the devices which are being translated by NAT.
  - Outside address is the address of the destination device.
  - Local address is any address that appears on the inside portion of the network.
  - Global address is any address that appears on the outside portion of the network.
- Static NAT uses a one-to-one mapping of local and global addresses.
- Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis.

What Did You Learn In This Module?

- Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses by tracking session port numbers.
- Port forwarding maps a permanent private IPv4 addresses and port to a single public IPv4 address and port. It allows multiple static mappings to use the same public address as long as mapped port numbers are different
- Advantages of NAT are: address conservation, flexibility of Internet connection and security through hiding of internal addresses
- Disadvantages of NAT are: Increased forwarding delays, lack of traceability, more RAM utilization, complicates the use of tunneling protocols
- IPv6 was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary.
- IPv6 does provide for protocol translation between IPv4 and IPv6 known as NAT64



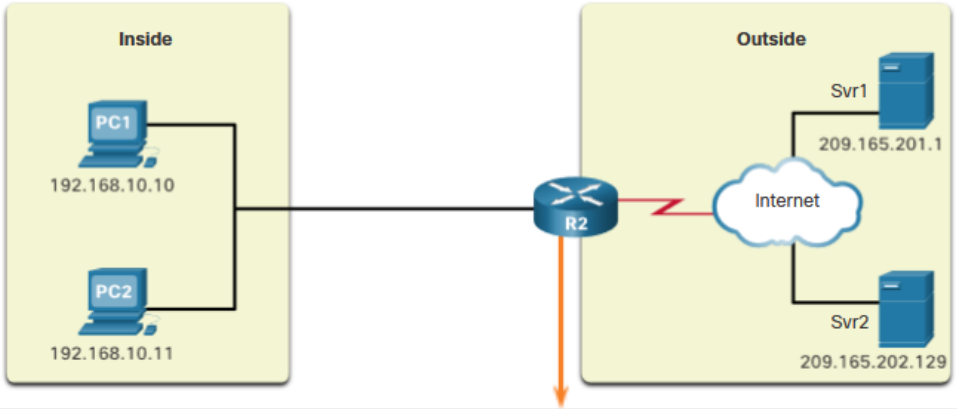
Module 5 Recap
Network Address Translation

ITNET04

WAN Connectivity

Port Address Translation

- **Port Address Translation (PAT),** maps multiple private IPv4 addresses to a single public IPv4 address by using the source port numbers to uniquely identify internal hosts



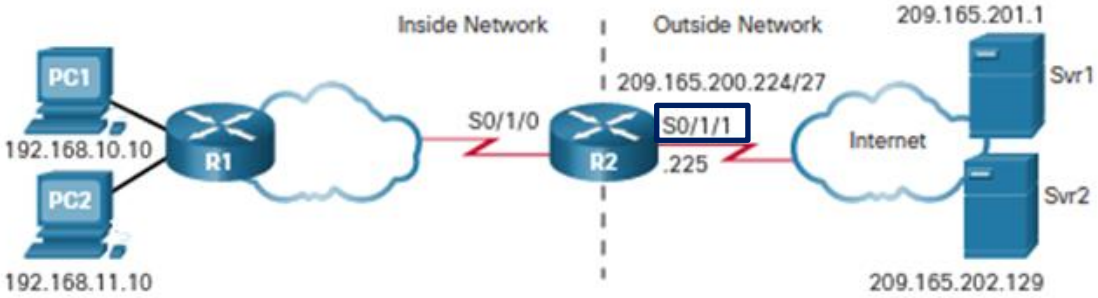
NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Same global address, different port numbers

PAT Configuration – Single Address on External Interface

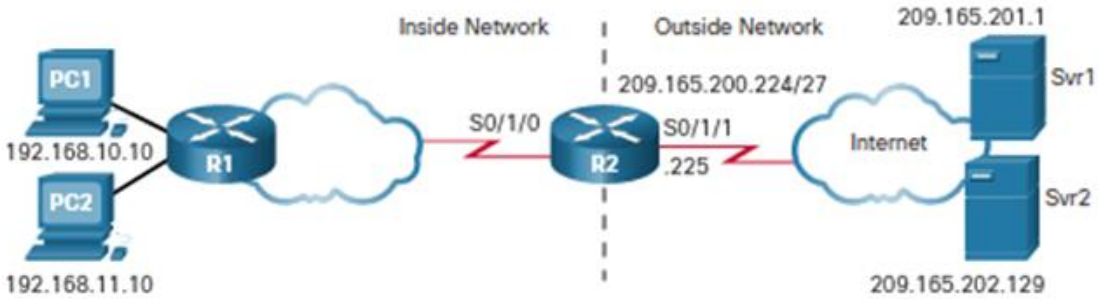
- **Step 1A** - Configure a standard ACL to identify (permit) only those addresses that will be translated.
- **Step 2A** - Bind the ACL to the interface
- **Step 3A** - Identify which interfaces are inside
- **Step 4A** - Identify which interface is outside




```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 interface s0/1/1 overload
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

PAT Configuration – Multiple Overloaded Addresses

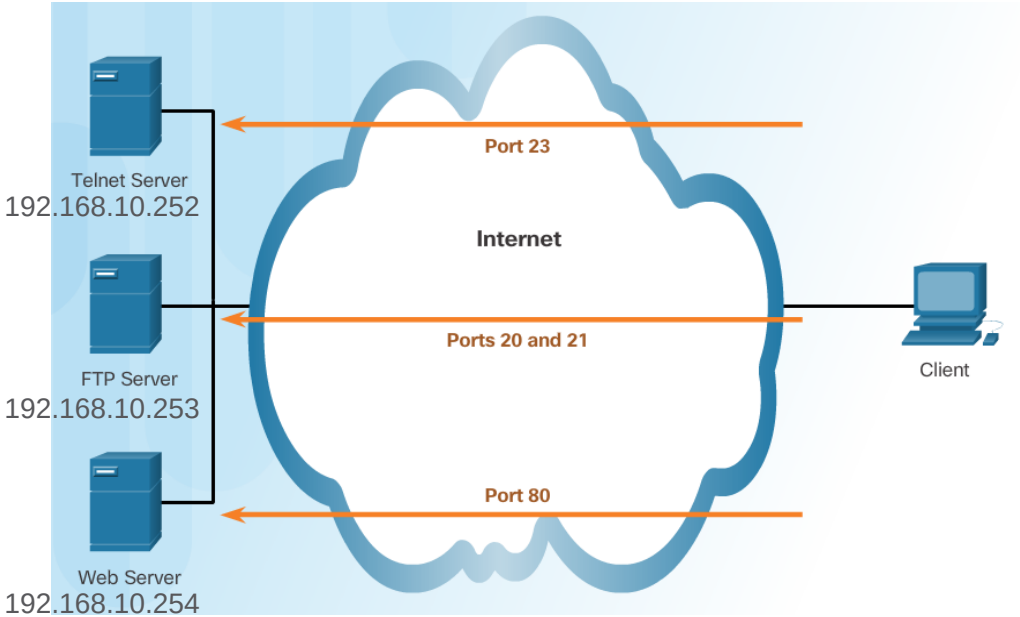
- **Step 1B** - Define the pool of addresses that will be used for translation
- **Step 2B -** Configure a standard ACL to identify (permit) only those addresses that will be translated.
- **Step 3B** - Bind the ACL to the pool
- **Step 4B** - Identify which interfaces are inside
- **Step 5B** - Identify which interface is outside




```
R2(config)# ip nat pool PAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool PAT-POOL1 overload
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

Port Forwarding

- **Port Forwarding** allows an external device to reach an internal device while sharing a public address among multiple internal hosts by using a static mapping with a specific **port number** for translation

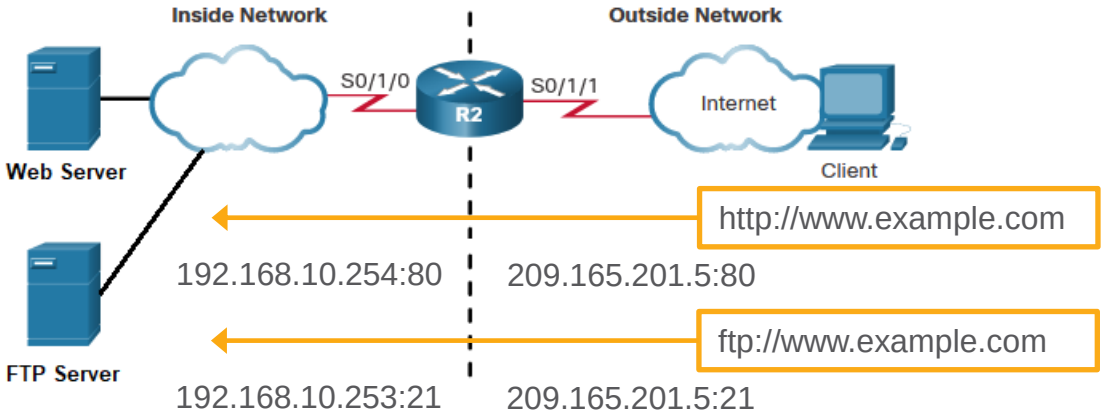


Inside Local	Inside Global	Outside Global
192.168.10.252:23	209.165.201.5:23	100.100.100.100:1555
192.168.10.253:20	209.165.201.5:20	100.100.100.100:1330
192.168.10.253:21	209.165.201.5:21	100.100.100.100:3163
192.168.10.254:80	209.165.201.5:80	100.100.100.100:2481

Port Forwarding Configuration

To configure port forwarding:

- **Step 1** - Create a mapping between the inside local and inside global addresses **and port number**
- **Step 2** - Identify which interfaces are inside
- **Step 3** - Identify which interface is outside




```
R2(config)# ip nat inside source static tcp 192.168.10.254 80 209.165.201.5 80
R2(config)# ip nat inside source static tcp 192.168.10.253 21 209.165.201.5 20
R2(config)# ip nat inside source static tcp 192.168.10.253 21 209.165.201.5 21
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Lab Questions

Q - Will using static NAT result in conservation of public IP Addresses?

A - No – It's a permanent 1-to1 mapping so you still need the same number of public addresses as internal hosts for everyone to get Internet access.

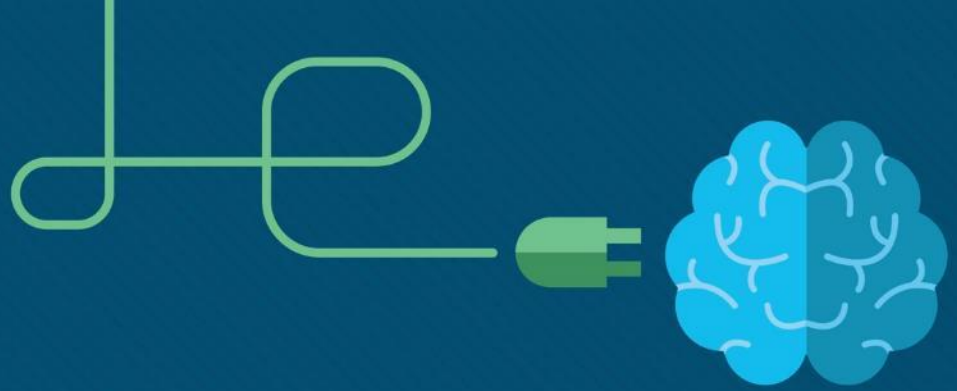
Q - If dynamic NAT is used, will inside hosts be consistently translated to the same global/public IP address? Why or why not?

A – No – You are assigned whichever is the first available address in the pool at the time of connection and this can be returned to the pool after the packet exchange is done

Q - Give at least 1advantage that static NAT has over dynamic NAT, and at least 1 advantage that dynamic NAT has over static NAT

A – Static NAT – can support hosted services accessible to external hosts, external access is assured due to permanent mapping

Dynamic NAT – addresses are conserved due to sharing, less tedious to configure for multiple hosts, more security for internal hosts because external traffic cannot enter unless requested by internal hosts beforehand



Module 6
Virtual Private Networks

ITNET04

WAN Connectivity

Module Objectives

Module Title: Virtual Private Networks

Module Objectives:

- Explain how VPNs secure site-to-site and remote access connectivity.
- Implement a GRE tunnel.
- Implement a secure IPSec tunnel.

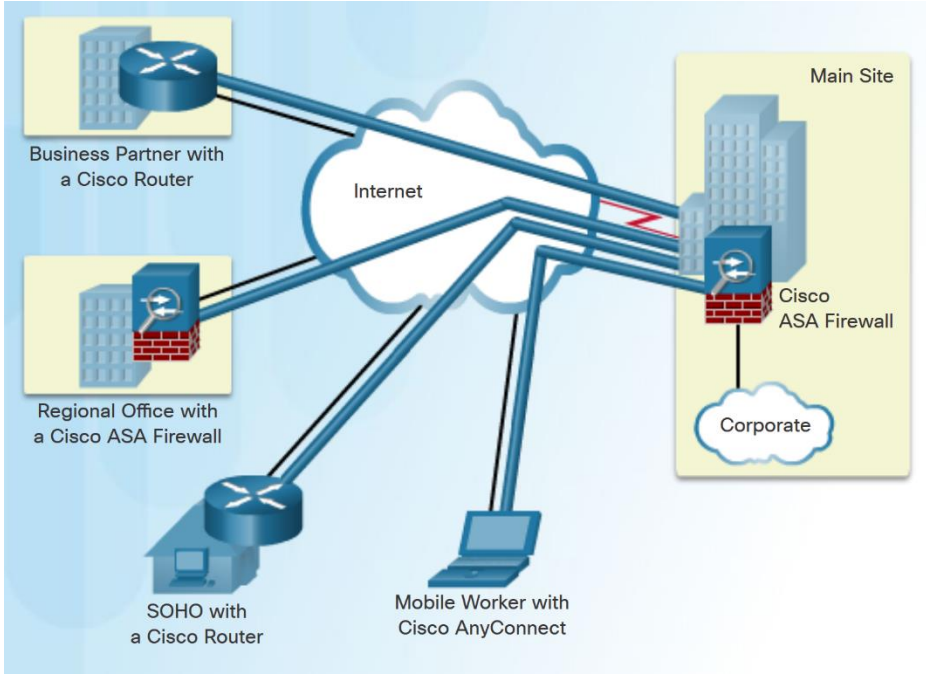
Module References:

- CCNAv7 ENSA– Module 9

6.1 Virtual Private Networks

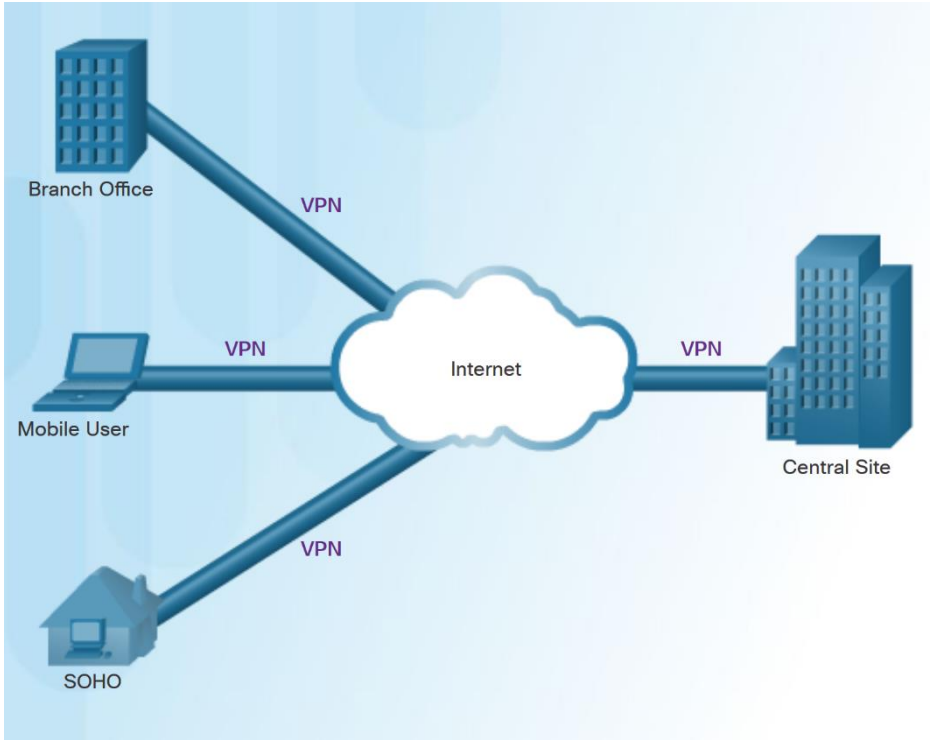
Introducing VPNs

- VPNs are used to create an end-to-end network connection that appears to be private over third-party networks, such as the Internet
- Commonly used to connect private LANs over a public network
- A secure implementation of VPN with encryption, such as IPsec VPNs, is what is usually meant by virtual private networking.
- To implement VPNs, a VPN gateway is necessary - could be a router, a firewall, or a dedicated VPN appliance (e.g. Cisco ASA)



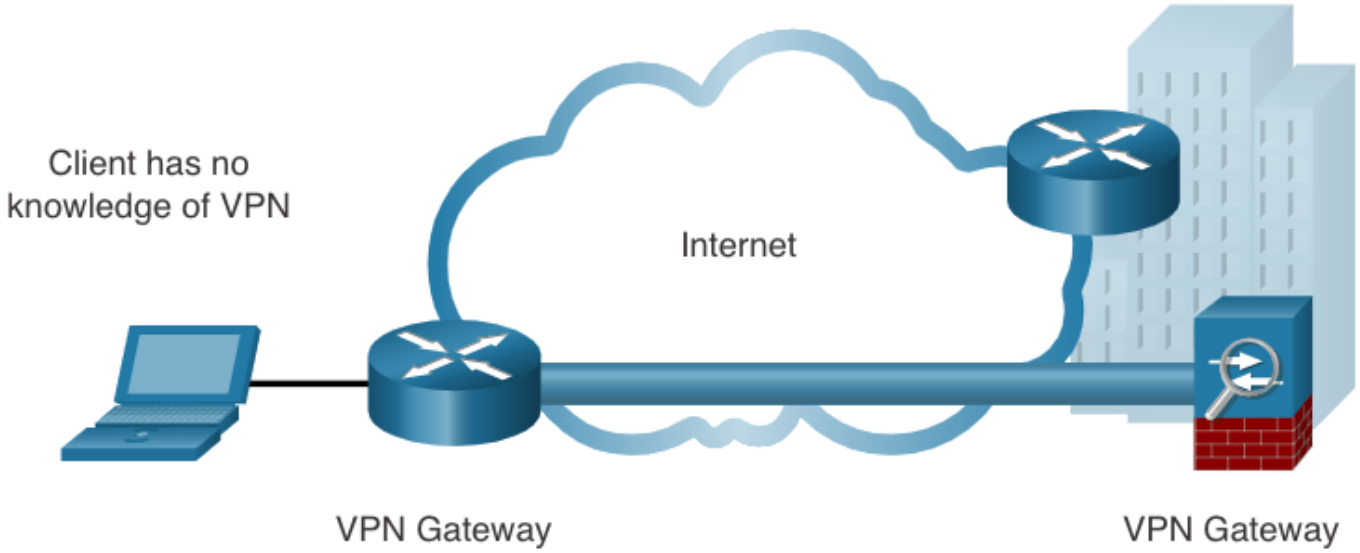
Benefits of VPNs

- The benefits of a VPN include the following:
  - **Cost savings** - VPNs enable organizations to use cost-effective, high-bandwidth technologies, such as DSL to connect remote offices and remote users to the main site.
  - **Scalability** - Organizations are able to add large amounts of capacity without adding significant infrastructure.
  - **Compatibility with broadband technology** - Allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity.
  - **Security** - VPNs can use advanced encryption and authentication protocols.



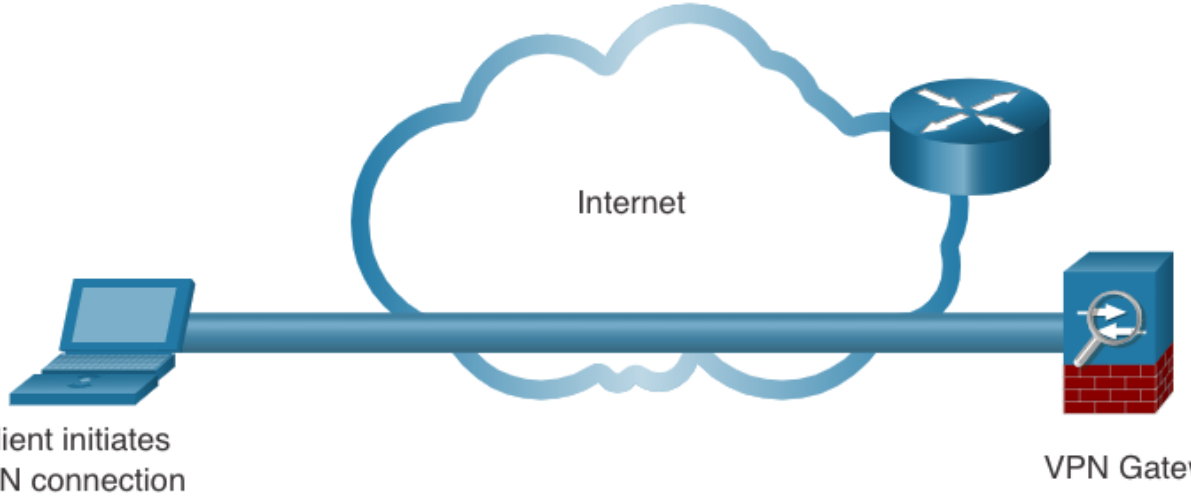
Site-to-Site VPNs

- Site-to-site VPNs connect entire networks in fixed location to each other, for example, connecting a branch office network to a company headquarters network.
- In a site-to-site VPN, end hosts send and receive normal TCP/IP traffic through a VPN “gateway”.
- The VPN gateway is responsible for encapsulating and encrypting outbound traffic.



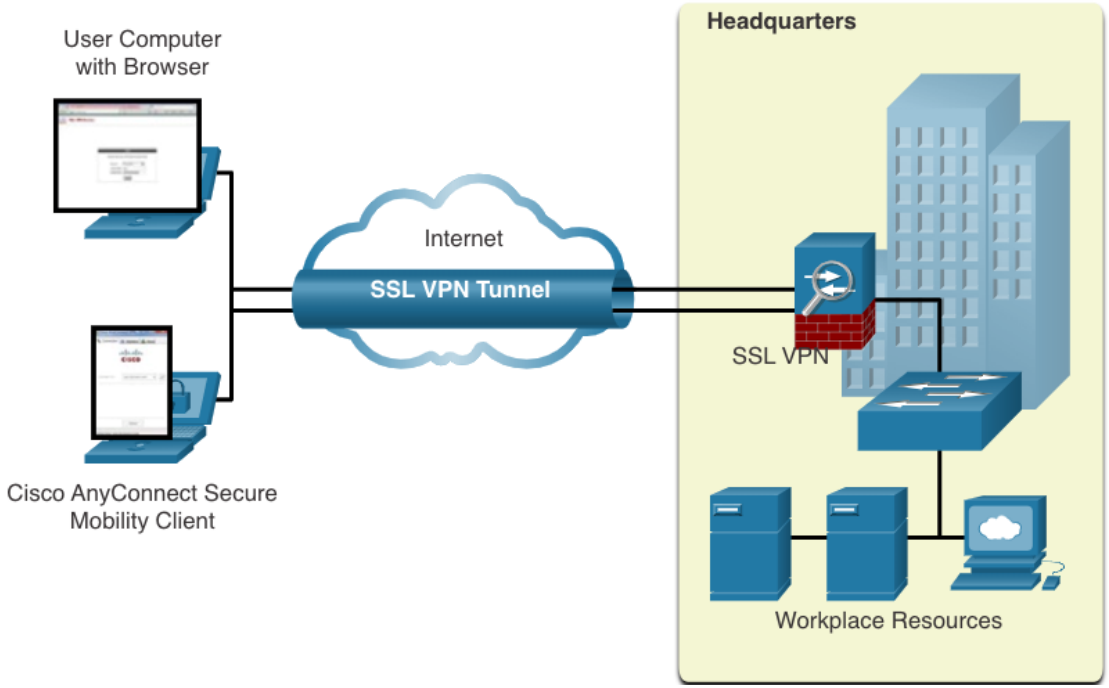
Remote Access VPNs

- Used to connect individual hosts that must access their company network securely over the Internet.
- A remote-access VPN supports the needs of telecommuters, mobile users, and extranet traffic.
- Users can remotely access resources and services on the private network as if they were directly plugged in to the network
- Allows for dynamically changing information, and can be enabled and disabled as needed
- VPN client software may need to be installed on the mobile user's end device.



Remote-Access VPNs

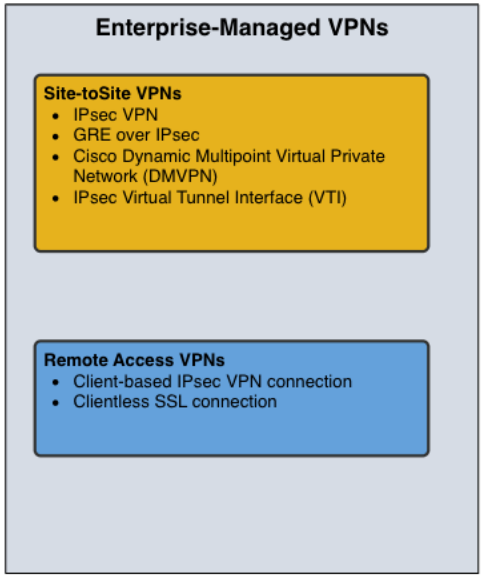
- Remote-access VPNs are typically enabled dynamically by the user when required and can be created using either IPsec or SSL.
  - **Clientless VPN connection** - The connection is secured using a web browser SSL connection.
  - **Client-based VPN connection** - VPN client software must be installed on the remote user's end device.

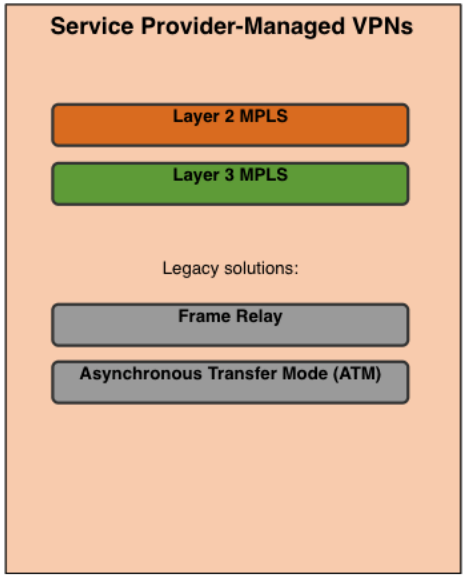


Enterprise and Service Provider VPNs

VPNs can be managed and deployed as:

- **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 the traffic from other customer traffic.





Service Provider MPLS VPNs

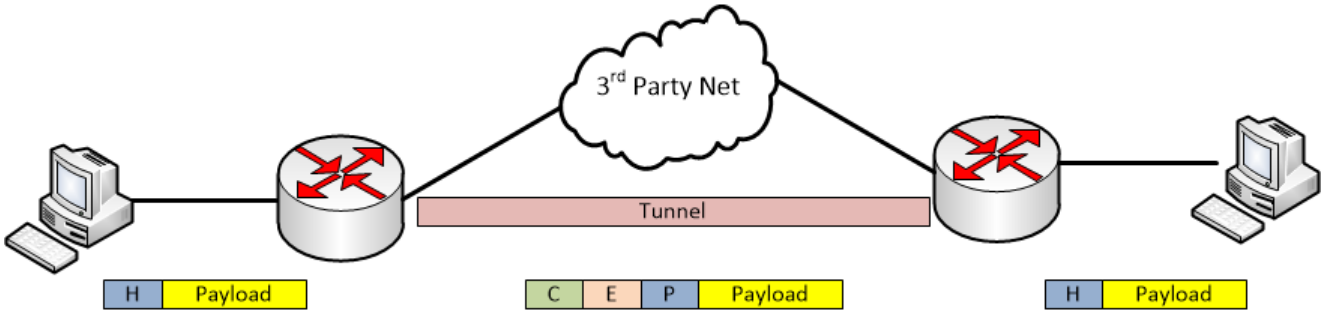
Today, service providers use MPLS in their core network. Traffic is forwarded through the MPLS backbone using labels. Traffic is secure because service provider customers cannot see each other's traffic.

- MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider.
- There are two 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.

6.2 Generic Routing Encapsulation

Tunneling

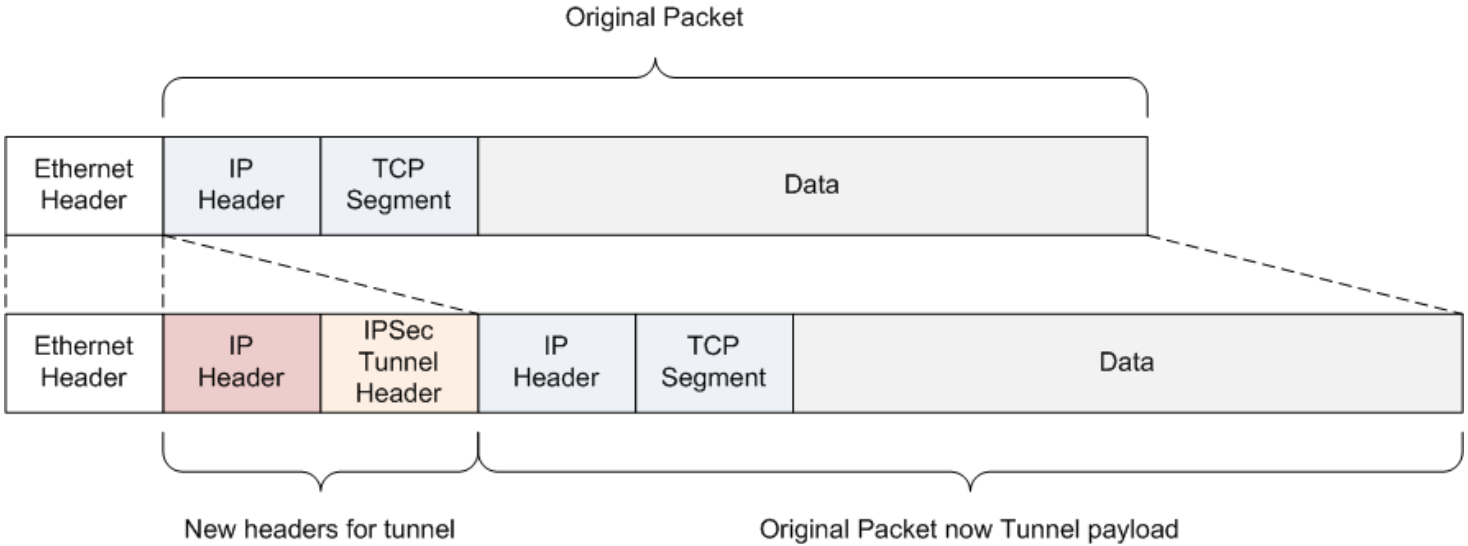
- Tunneling is the process of encapsulating an entire packet within another packet before it's transported over a network
- Involves:
  - Passenger or encapsulated protocol - protocol over which the original data was carried
  - Encapsulating protocol - protocol wrapped around the original data (optional)
  - Carrier or delivery protocol – protocol over which the wrapped data travels



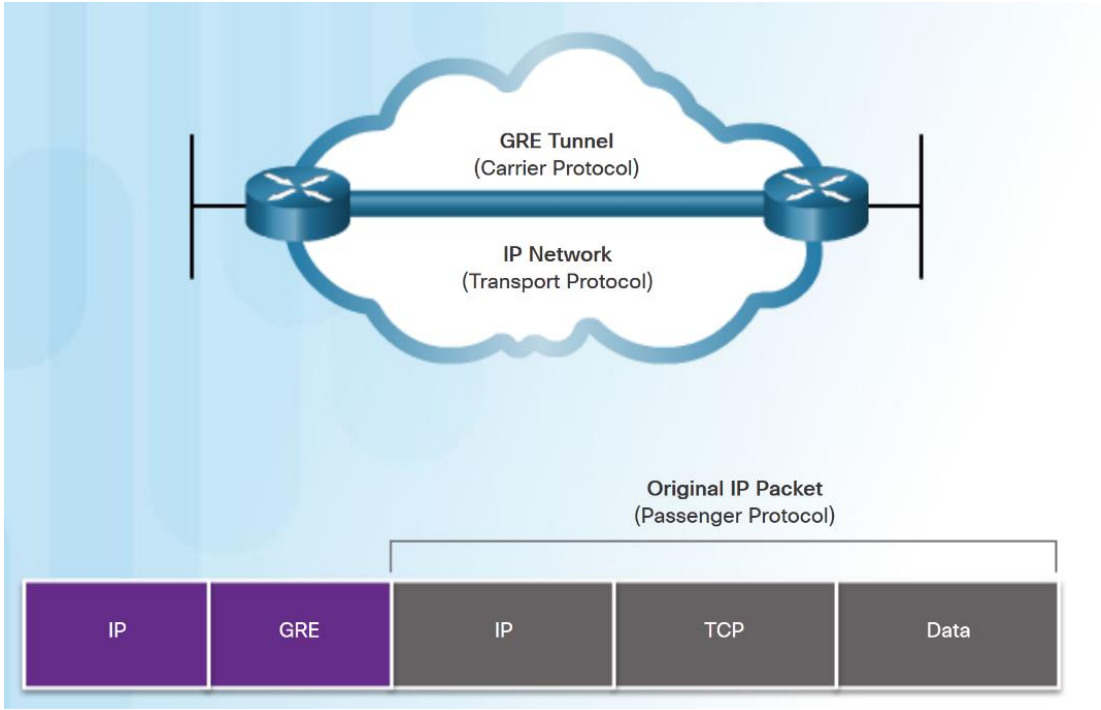
- The encapsulating protocol protects the contents of the passenger protocol

Tunneling in Relation to VPNs

- VPN and tunneling often go hand-in-hand since most VPN technologies use a form of tunneling to accomplish the task of making networks seem like they are directly connected to each other



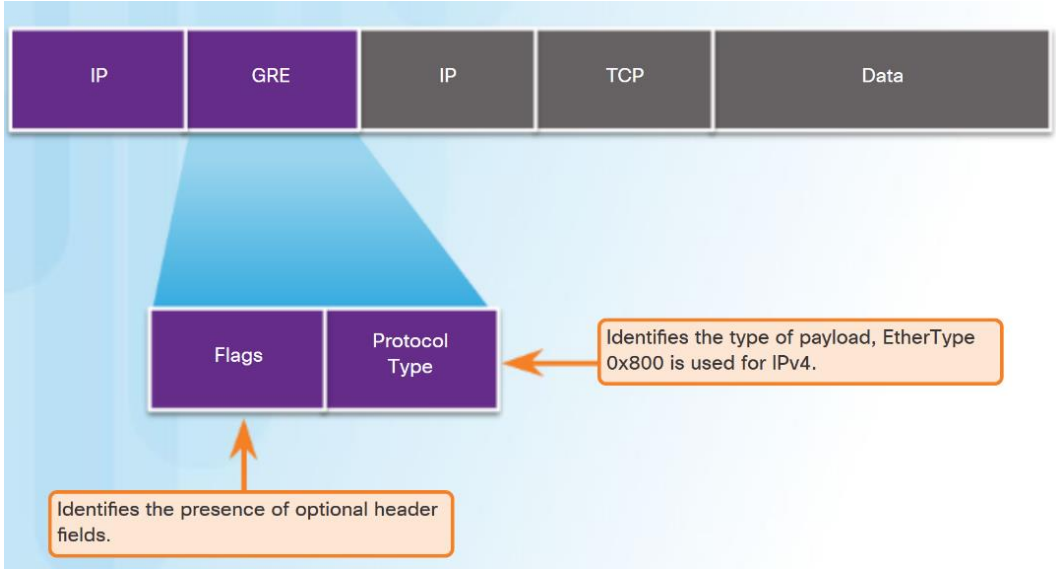
GRE Introduction



- Generic Routing Encapsulation (GRE) is a non-secure, site-to-site VPN tunneling protocol.
  - Developed by Cisco.
  - GRE is stateless.
  - Does not include any mechanisms for data confidentiality and integrity.
  - GRE is defined as an IETF standard (RFC 2784).
- GRE manages the transportation of multiprotocol and IP multicast traffic between two or more sites

GRE Characteristics

- In the outer IP header, 47 is used in the protocol field.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.



Configure GRE

- Before configuring GRE, first ensure the following:

1. The 2 routers that will connected via the tunnel can reach each other's external interface (e.g. To create a tunnel between R1 and R2, ensure that R1 can successfully ping S0/0/0 of R2 and vice versa)
2. ACLs on peer router interfaces allow GRE traffic

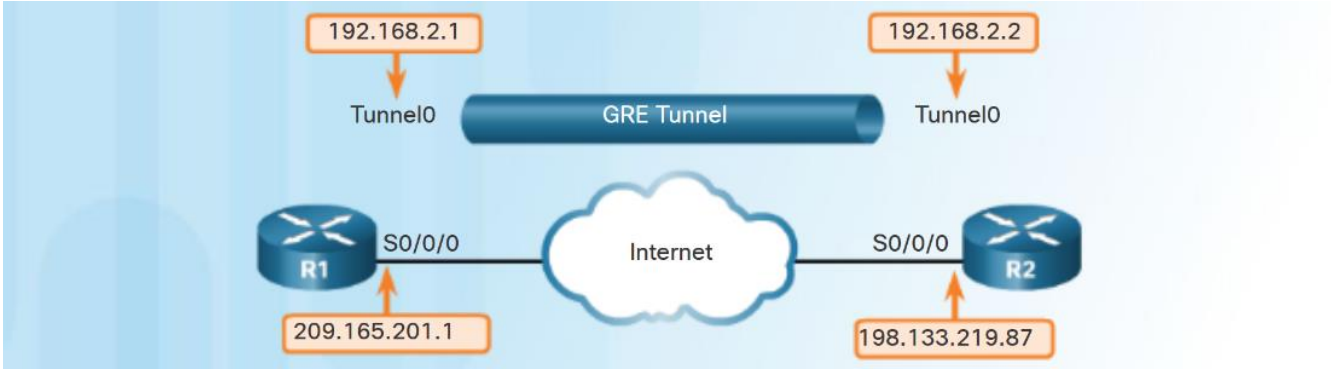
.

```
R1(config)# access-list 100 permit gre host 198.133.219.87 host 209.165.201.1
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 100 in
```

```
R2(config)# access-list 101 permit gre host 209.165.201.1 host 198.133.219.87
R2(config)# interface S0/0/0
R2(config-if)# ip access-group 100 in
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 1. Create a tunnel interface using the **interface tunnel** *number* command.

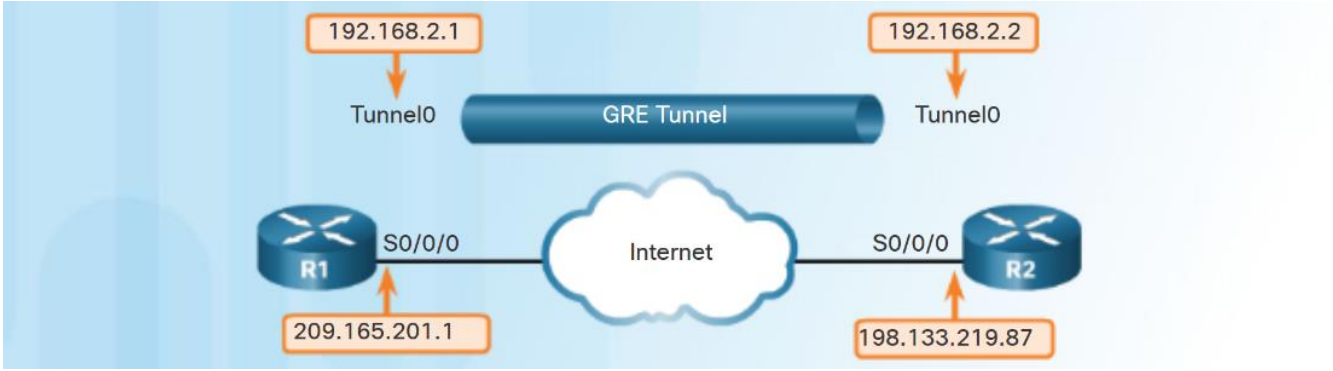



```
R1(config)# interface Tunnel0
```

```
R2(config)# interface Tunnel0
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 2. Specify GRE tunnel mode as the tunnel interface mode (optional)

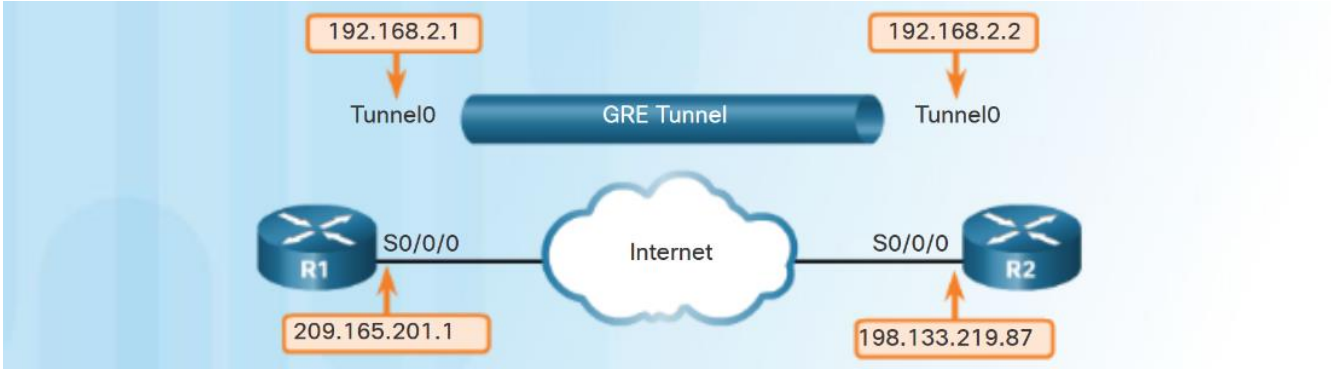



```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 3. Configure an IP address for the tunnel interface. (Usually a private address)

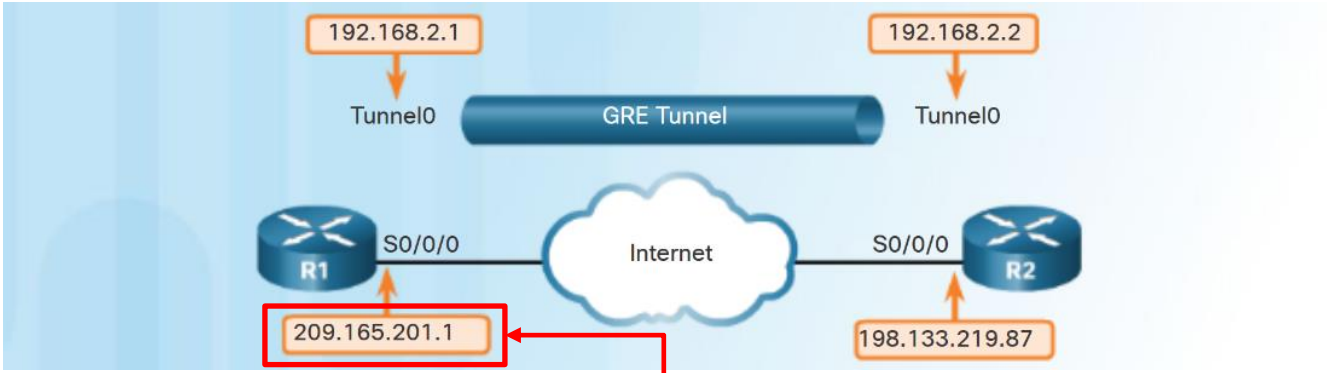



```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 4. Specify the tunnel source interface or IP address. If using IP address, this should match the IP address of the physical interface where the tunneled traffic will exit

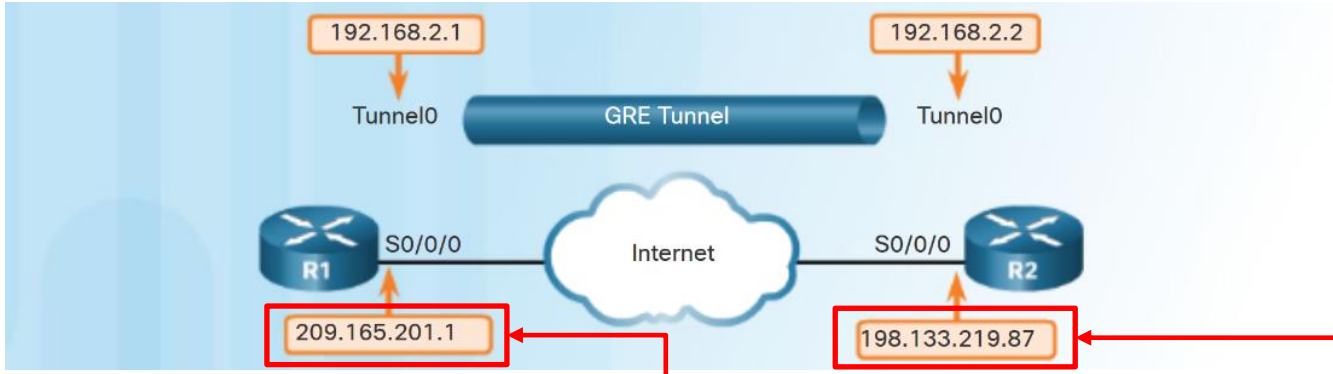



```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
R1(config-if)#tunnel source 209.165.201.1
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
R2(config-if)#
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 4. Specify the tunnel source interface or IP address. If using IP address, this should match the IP address of the physical interface where the tunneled traffic will exit

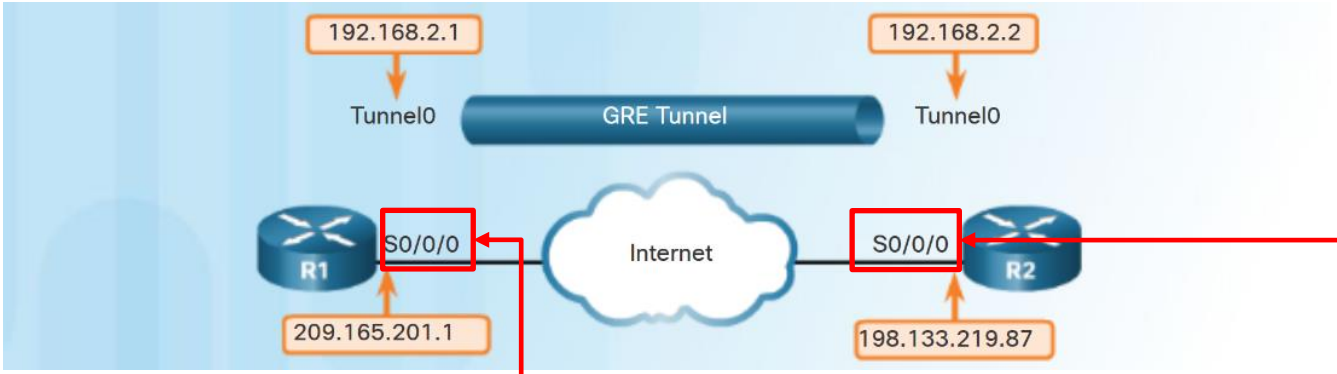



```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
R1(config-if)#tunnel source 209.165.201.1
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
R2(config-if)#tunnel source 198.133.219.87
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 4. Specify the tunnel source interface or IP address. If using IP address, this should match the IP address of the physical interface where the tunneled traffic will exit

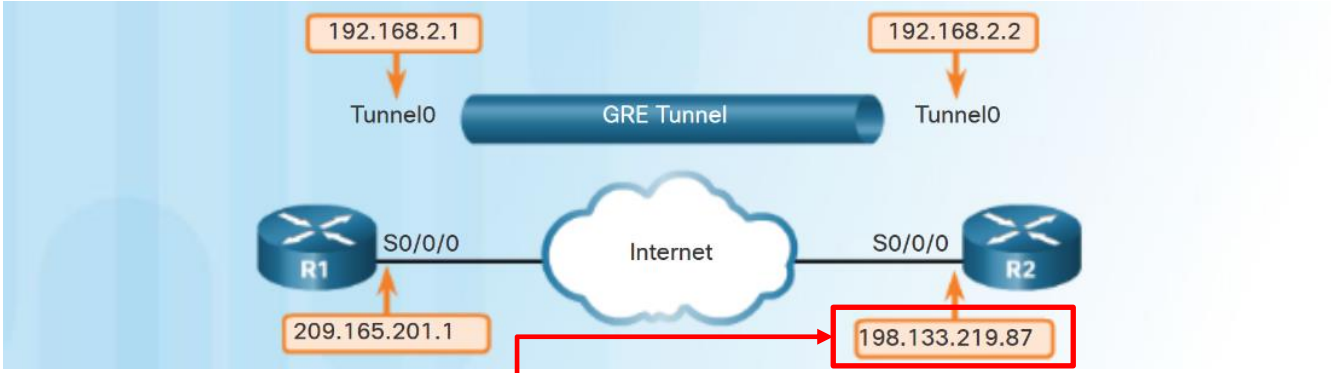



```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
R1(config-if)#tunnel source 209.165.201.1
                or
R1(config-if)#tunnel source S0/0/0
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
R2(config-if)#tunnel source 198.133.219.87
                or
R2(config-if)#tunnel source s0/0/0
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 5. Specify the tunnel destination IP address. This is the IP address of the physical interface of the destination router where the tunneled traffic will be sent to

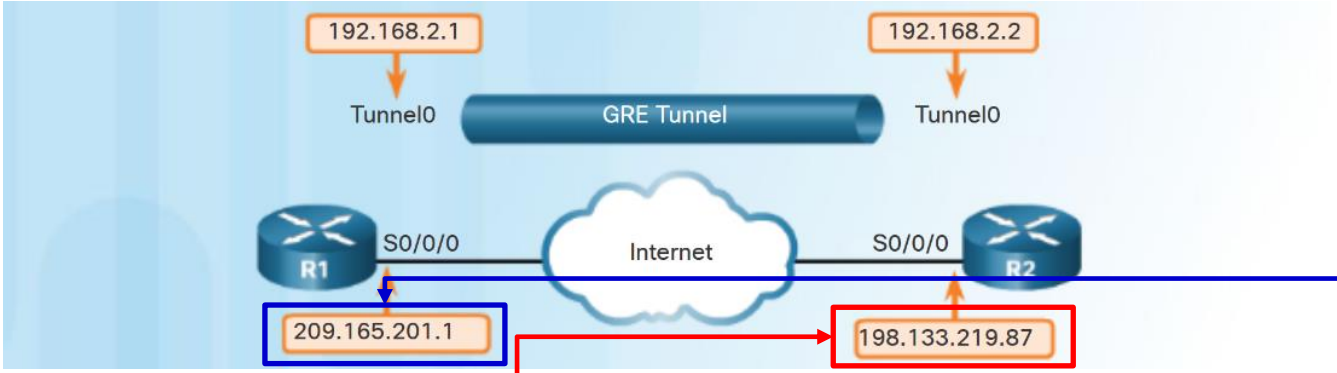



```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
R1(config-if)#tunnel source 209.165.201.1
R1(config-if)#tunnel destination 198.133.219.87
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
R2(config-if)#tunnel source 198.133.219.87
R2(config-if)#
```

Configure GRE

- Five steps to configuring a GRE tunnel:
  - Step 5. Specify the tunnel destination IP address. This is the IP address of the physical interface of the destination router where the tunneled traffic will be sent to




```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
R1(config-if)#tunnel source 209.165.201.1
R1(config-if)#tunnel destination 198.133.219.87
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
R2(config-if)#tunnel source 198.133.219.87
R2(config-if)#tunnel destination 209.165.201.1
```

Verify GRE

- Use the **show ip interface brief** command to verify that the tunnel interface and line protocol are up.

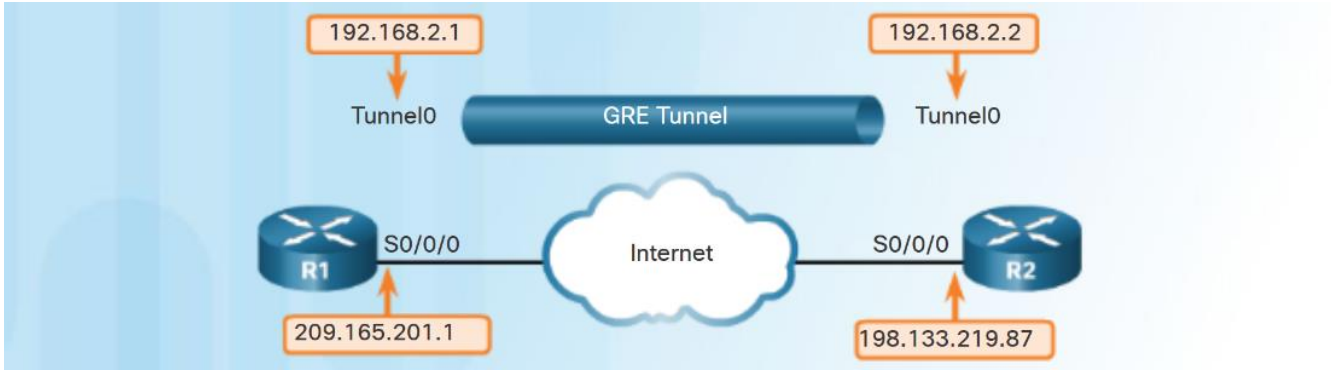
```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            209.165.201.1   YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Tunnel0                192.168.2.1     YES manual up                    up
```

- Use the **show interface tunnel** command to verify the state of the tunnel.

```
R1#show interface Tunnel0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1 (Serial0/0/0), destination 198.133.219.87
  Tunnel protocol/transport GRE/IP
```

Working with GRE Tunnels

- After configuring the tunnel, the 2 routers will appear to have a direct connection between each other; hence static routing or routing protocols can now be configured as if the 2 sites were just a single contiguous LAN
- Example:

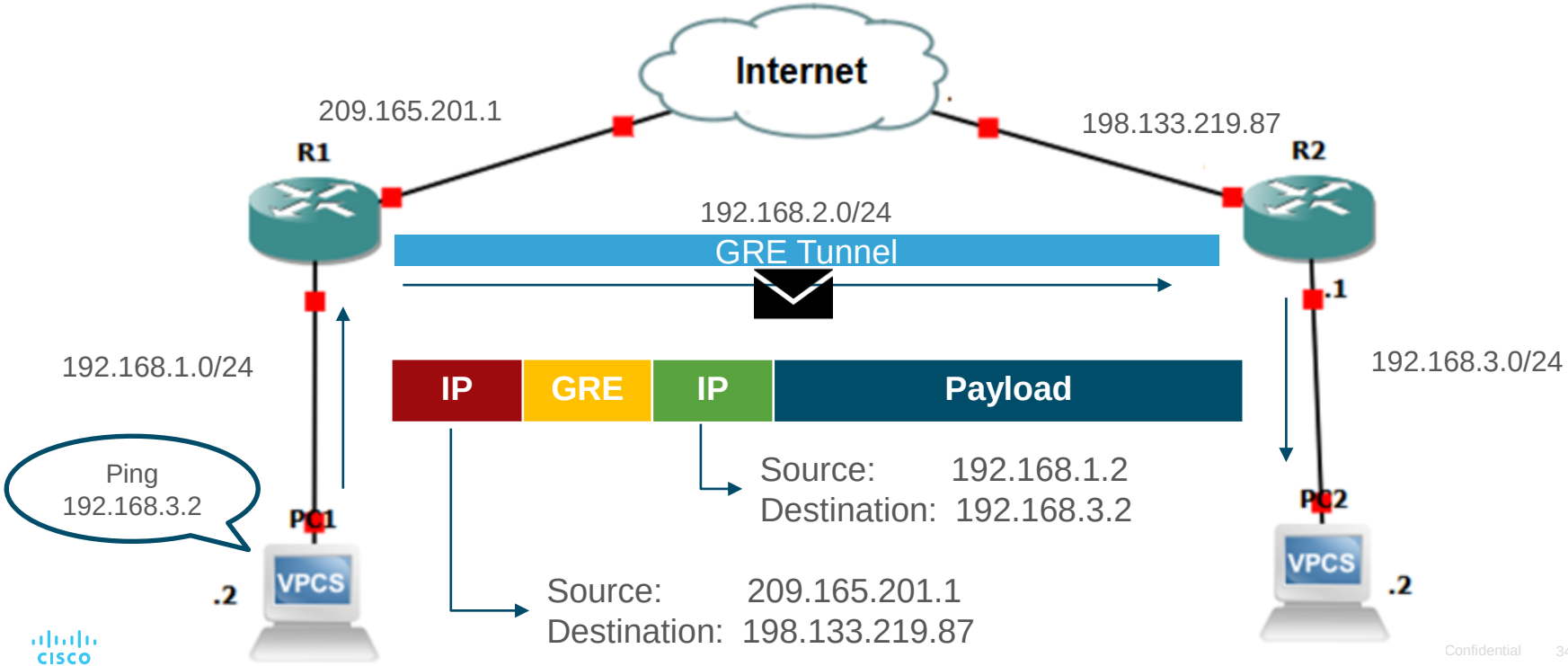



```
R1(config)# router ospf 1
R1(config-router)#network 192.168.2.0
0.0.0.255 area 0
```

```
R2(config)# router ospf 1
R2(config-router)#network 192.168.2.0
0.0.0.255 area 0
```

Working with GRE Tunnels

- Routing between private LANs across the Internet / 3rd party network



Troubleshoot GRE

- Issues with GRE are usually due to one or more of the following:

Cause	To Check
The tunnel interface IP addresses are not on the same network or the subnet masks do not match.	**show ip interface brief**
The interfaces for the tunnel source and/or destination are not configured with the correct IP address or are down.	**show ip interface brief**
The destination address of a tunnel is not reachable from the local router	**show ip route**
Static or dynamic routing is not properly configured	**show ip route** or **show** commands specific to the routing protocol used

What Did You Learn In This Module?

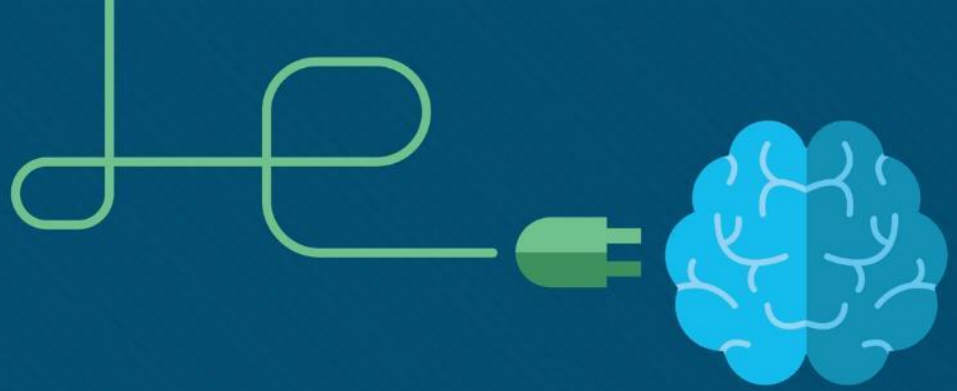
- VPNs are used to create a secure end-to-end private network connection over a third-party network, such as the Internet.
- A site-to-site VPN uses a VPN gateway device at the edge of both sites. The end hosts are unaware of the VPN and have no additional supporting software.
- A remote access VPN requires software to be installed on the individual host device that accesses the network from a remote location.
  - The two types of remote access VPNs are SSL and IPsec.
  - SSL technology can provide remote access using a client's web browser and the browser's native SSL encryption.
- VPNs may be self-deployed by an organization or created by an ISP, usually through MPLS
- GRE is a basic, non-secure site-to-site VPN tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, thus allowing an organization to deliver other protocols through an IP-based WAN.

To Do

- Lab 6.1 Configuring GRE– due Aug 13 (Friday) 9 PM

Next Meeting

- Aug 11 (Wednesday) – Module 6 (Virtual Private Networks) Part 2



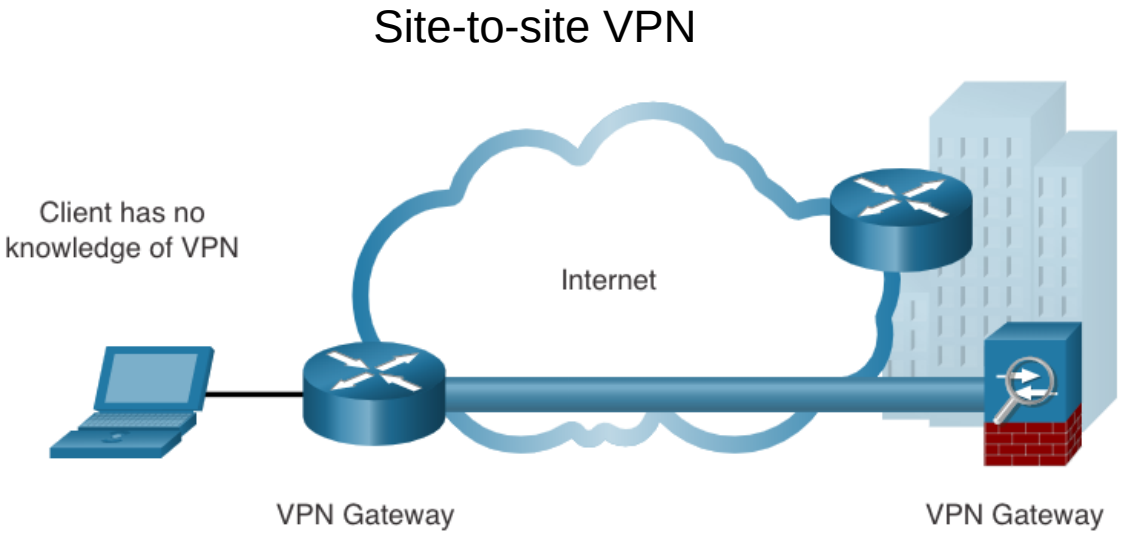
Module 6
Virtual Private Networks (Part 2)

ITNET04

WAN Connectivity

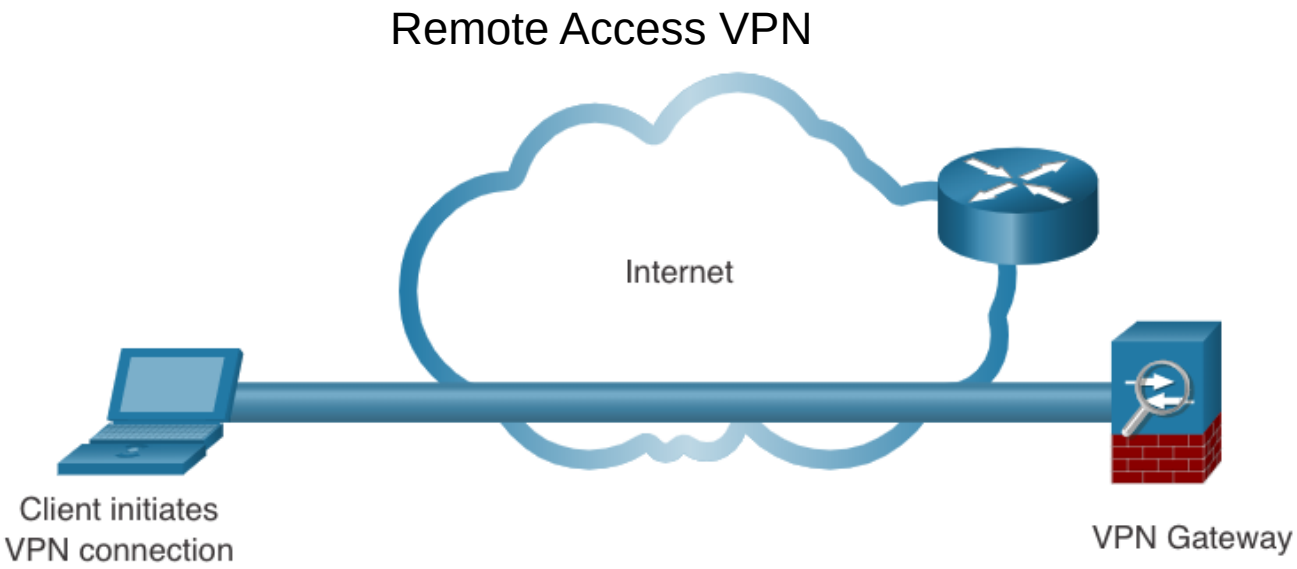
Virtual Private Networks

- VPNs are used to create an end-to-end network connection that appears to be private over third-party networks, such as the Internet



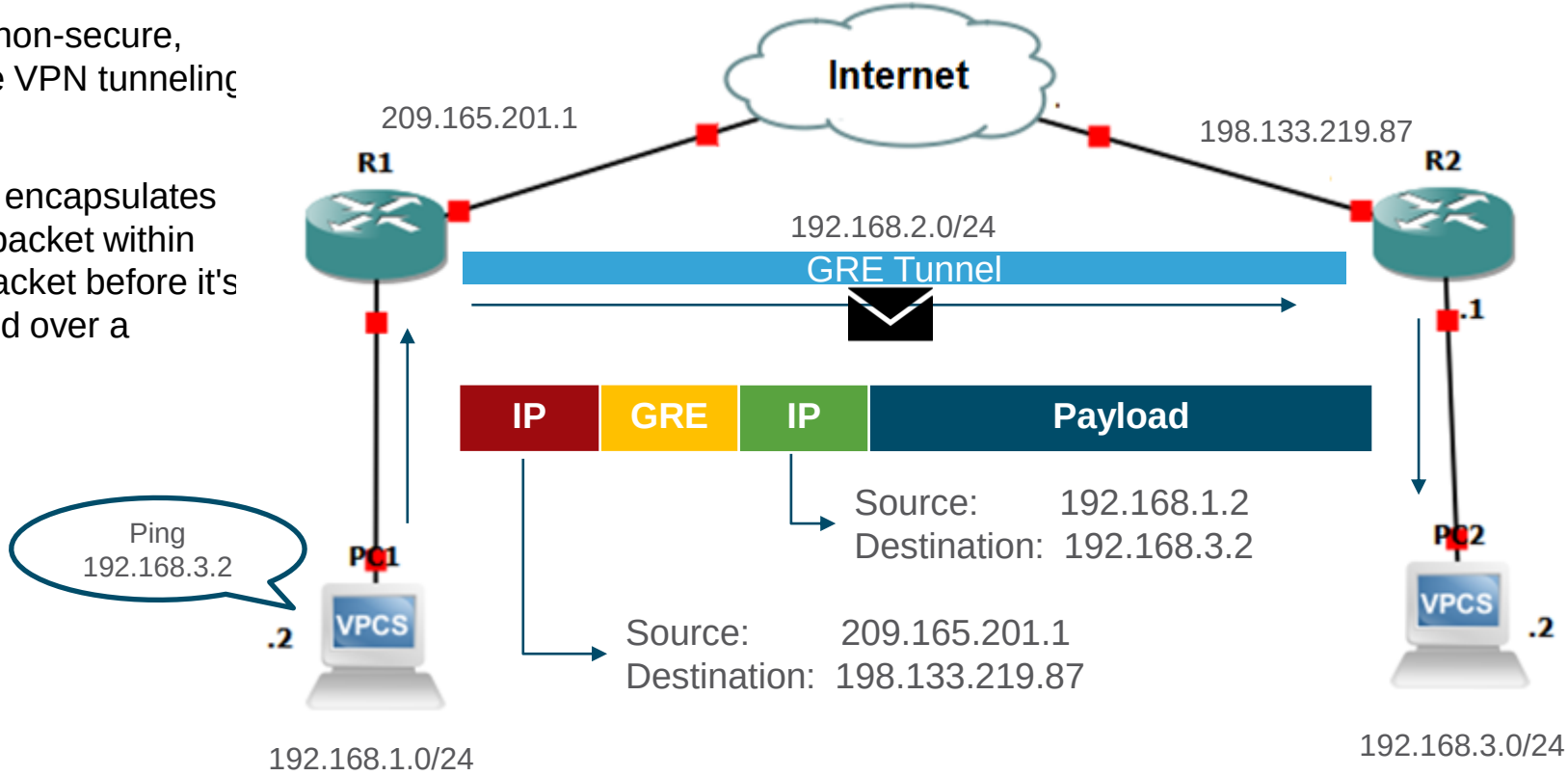
Virtual Private Networks

- VPNs are used to create an end-to-end network connection that appears to be private over third-party networks, such as the Internet



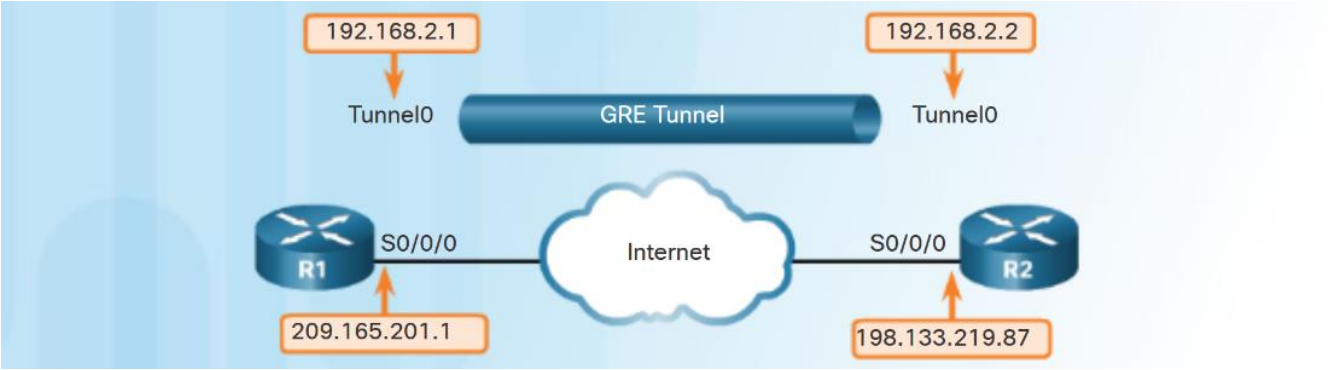
GRE and Tunneling

- GRE is a non-secure, site-to-site VPN tunneling protocol.
- Tunneling encapsulates an entire packet within another packet before it's transported over a network



GRE Configuration

- Step 1: Create the tunnel interface
- Step 2: Set the tunnel source (own external interface)
- Step 3: Set the tunnel destination (external interface of tunnel peer)
- Step 4: Configure the tunnel connection as if it were a direct point-to-point link



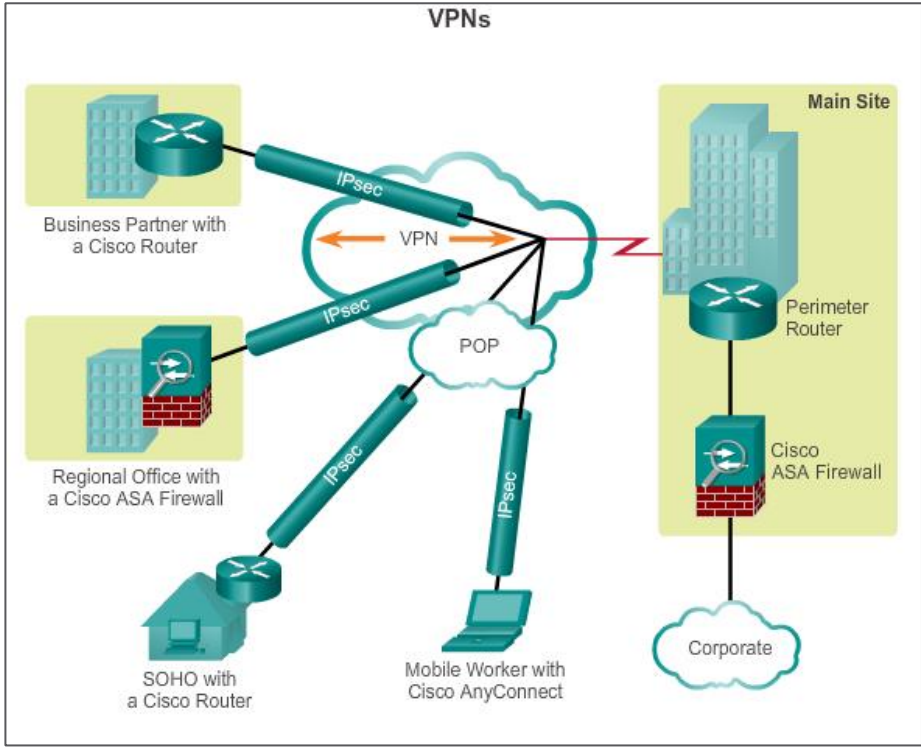

```
R1(config)# interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#tunnel source 209.165.201.1
R1(config-if)#tunnel destination 198.133.219.87
R1(config-if)#ip address 192.168.2.1
       255.255.255.0
```

```
R2(config)# interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#tunnel source 198.133.219.87
R2(config-if)#tunnel destination 209.165.201.1
R2(config-if)#ip address 192.168.2.2
       255.255.255.0
```

3.3 IPSec

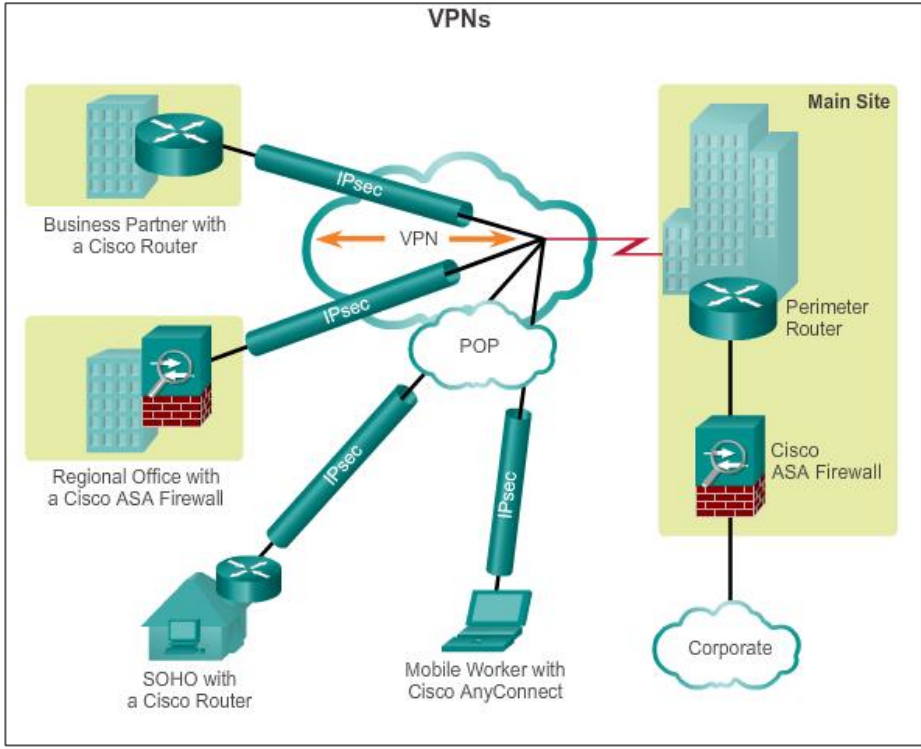
IPsec Technologies

- Secures a path between a pair of gateways, a pair of hosts, or a gateway and host.
- Works at the network layer, protecting and authenticating IP packets between participating IPsec devices.
  - All implementations of IPsec have a plaintext Layer 3 header, so there are no issues with routing.
  - Functions over all Layer 2 protocols, such as Ethernet, ATM, or Frame Relay.



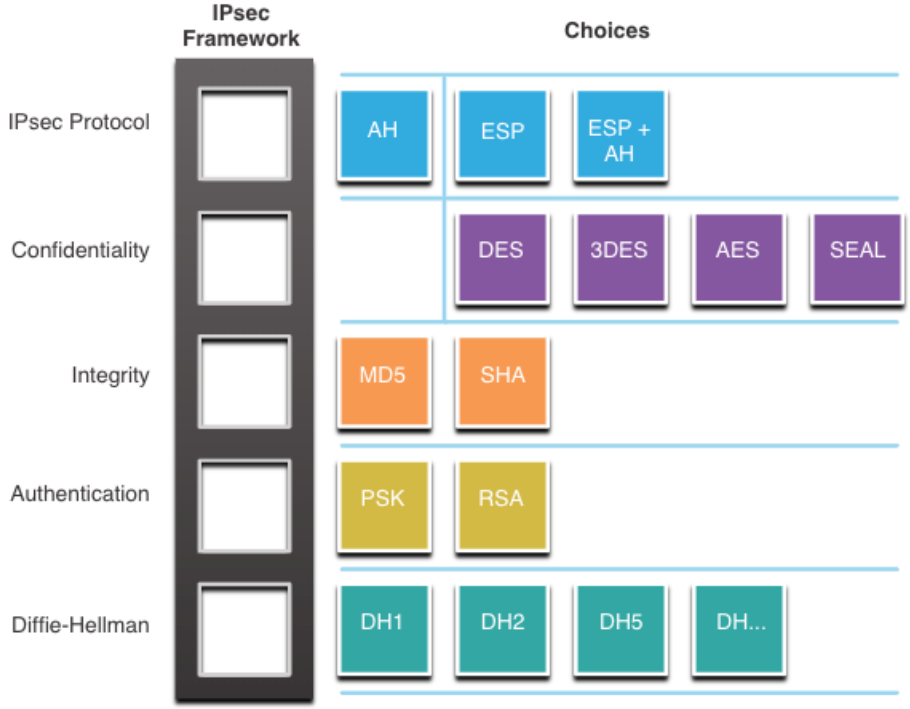
IPsec Technologies

- Information from a private network needs to be securely transported over a public network.
- Internet Protocol Security (IPSec) is a framework of **open standards** that defines how a VPN can configured in a secure manner using IP.
  - Provides the rules for secure communications.
  - Not bound to any specific encryption, authentication, security algorithms, or keying technology.
  - Relies on **existing** algorithms to implement secure communications.



IPsec Framework

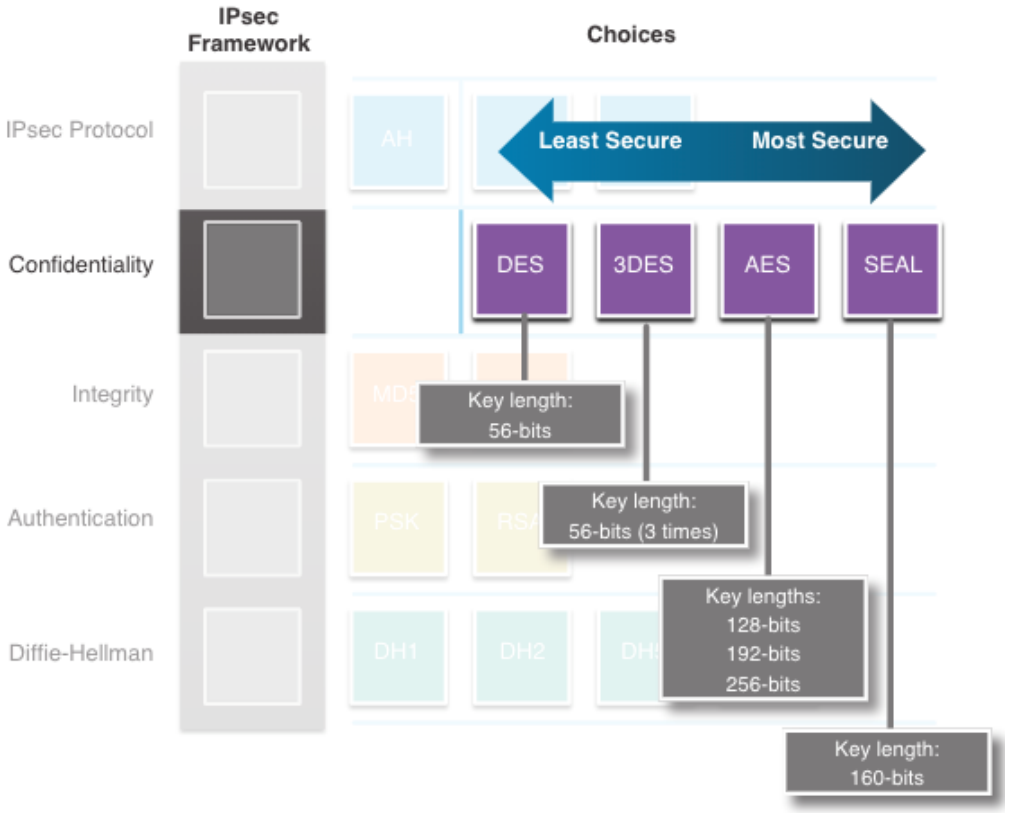
- The IPsec framework consists of five building blocks.
- The administrator selects the algorithms used to implement the security services within that framework.
- The open slots in the IPsec framework shown in the figure can be filled with any of the choices that are available for that IPsec function to create a unique security association (SA).
- New security technologies can be integrated without updating existing IPsec standards.



Confidentiality with Encryption

IPSec uses symmetric key encryption to ensure that only the intended recipient can read the data

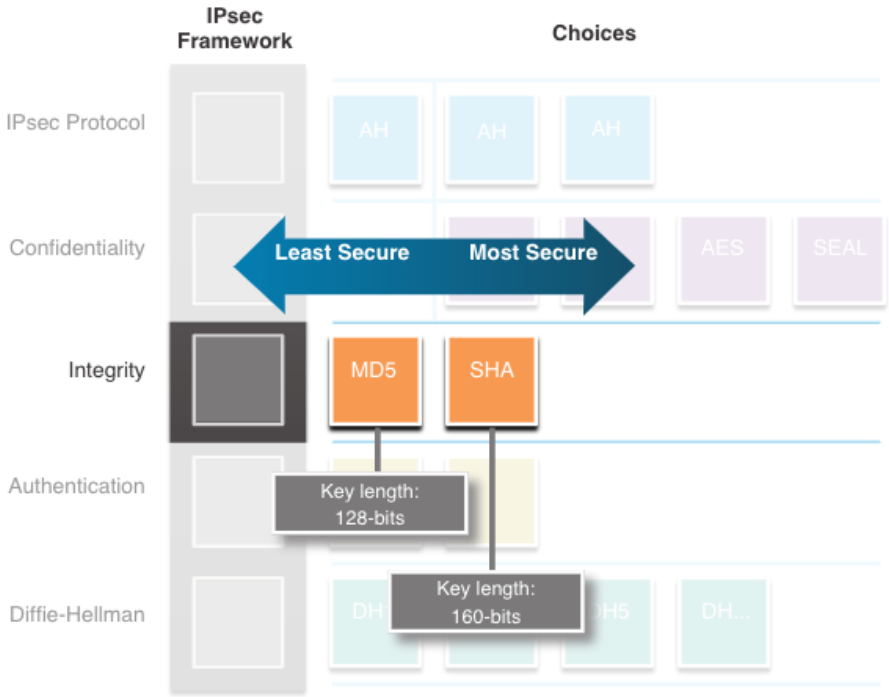
- **DES** uses a 56-bit key.
- **3DES** uses three independent 56-bit encryption keys per 64-bit block.
- **AES** offers three different key lengths: 128 bits, 192 bits, and 256 bits.
- **SEAL** is a stream cipher, which means it encrypts data continuously rather than encrypting blocks of data. SEAL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



Integrity with Hashing

IPSec uses the Hashed Message Authentication Code (HMAC) to guarantee that data has not been changed while in transit. If tampering is detected, the packet is dropped

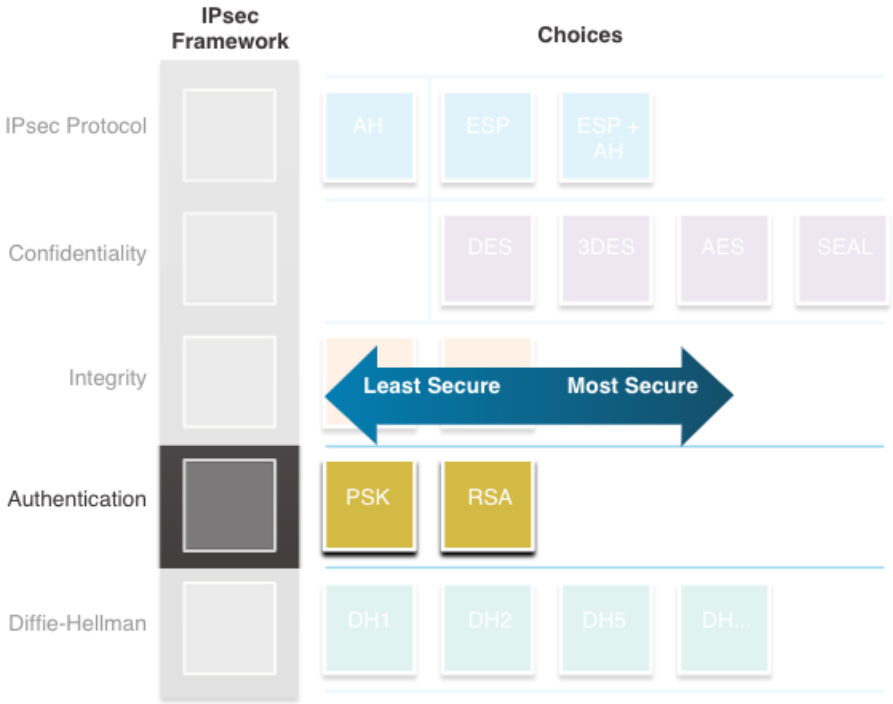
- **Message-Digest 5 (MD5)** uses a 128-bit shared-secret key.
- **The Secure Hash Algorithm (SHA)** uses a 160-bit secret key.



IPSec Authentication

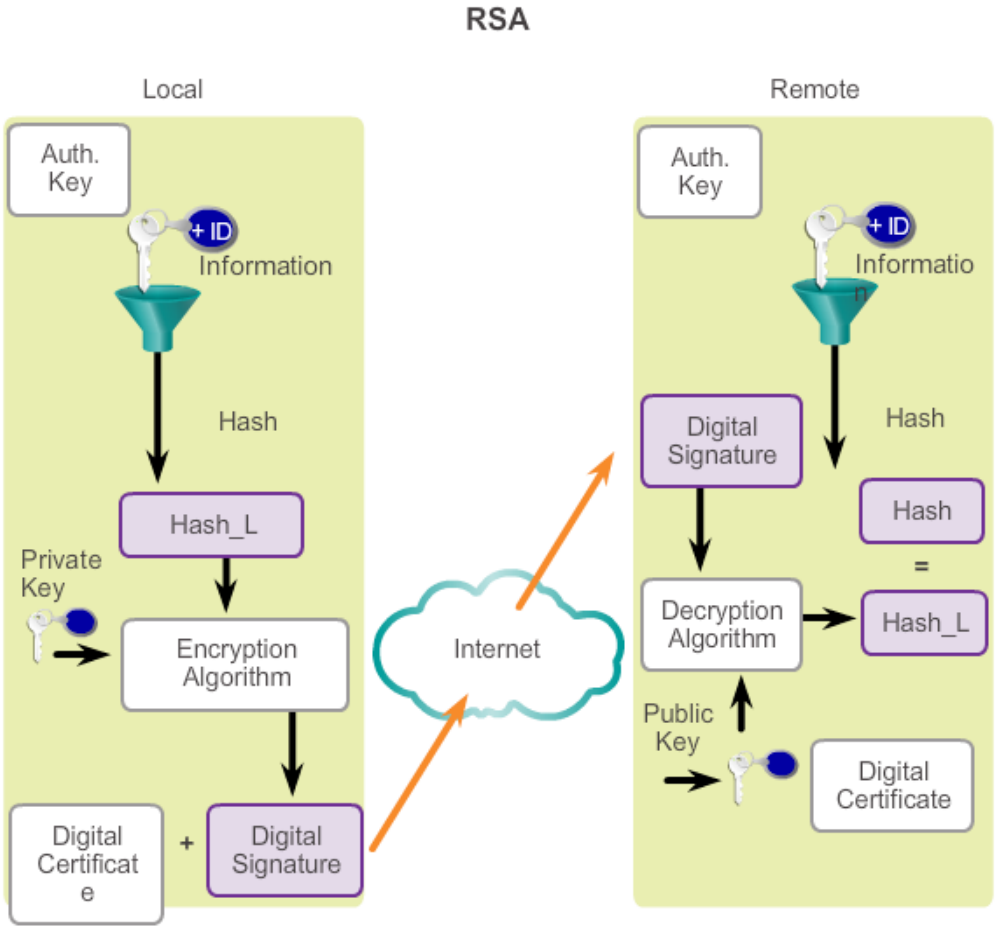
Authentication is used to verify the identity of the data source and ensure that a connection is made with the desired host

1. **Pre-shared key (PSK)** -key value is entered into each peer manually.
   - Easy to configure manually
   - Does not scale well
   - Must be configured on every peer
2. **Rivest, Shamir, and Adleman (RSA)** - authentication uses digital certificates to authenticate the peers.
   - Each peer must authenticate its opposite peer before the tunnel is considered secure.



IPSec Authentication (Digital Certificates)

- Digital certificates use public / private key pairs to authenticate device identity
- Local device derives a hash and encrypts it with its private key to produce a digital signature
- Digital signature will be decrypted by the remote peer using the local device public key

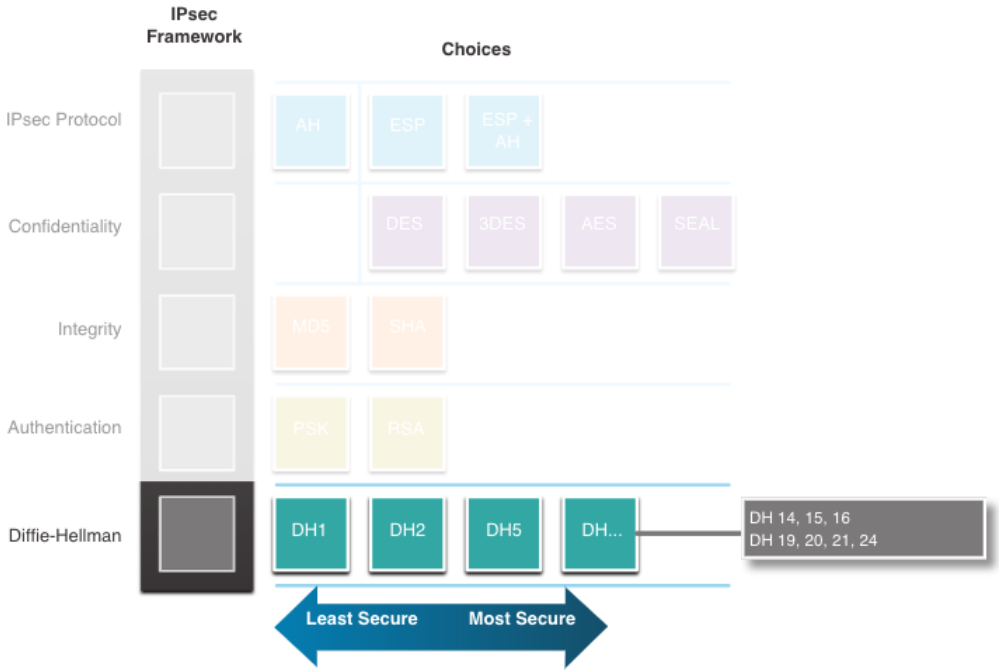


Secure Key Exchange with Diffie - Hellman

DH provides allows two peers to establish a shared secret key over an insecure channel.

Variations of the 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.



IPSec Security Protocol

Choosing the IPsec protocol encapsulation is the first building block of the framework.

- 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.

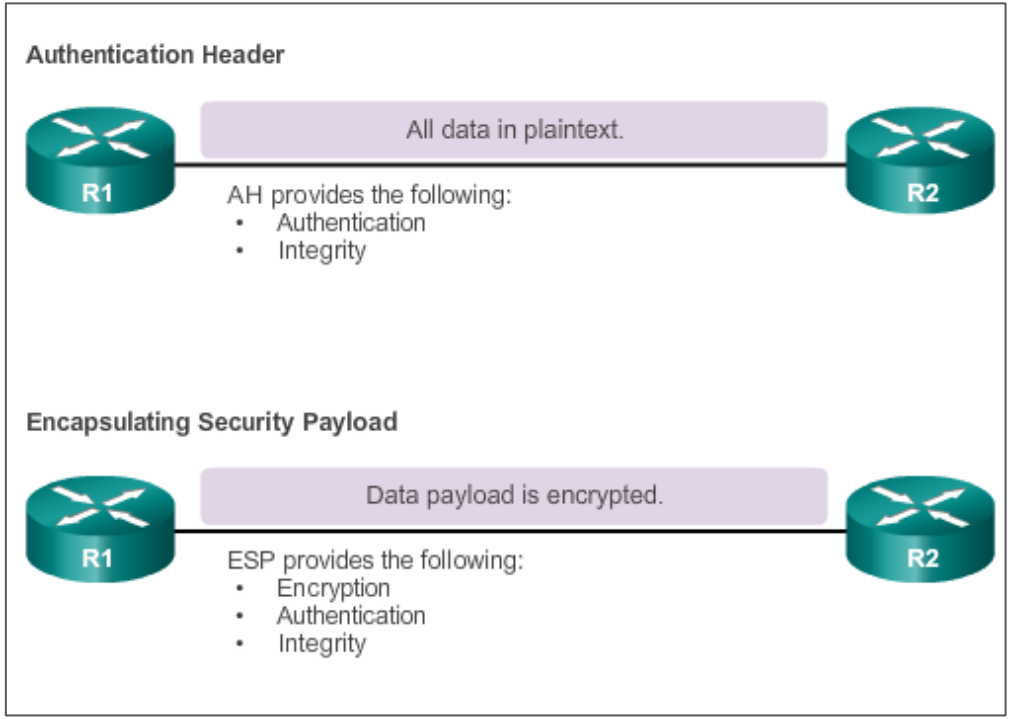
IPSec Security Protocol

Authentication Header (AH)

- Appropriate protocol to use when confidentiality is not required
- Provides data authentication and integrity for IP packets that are passed between two systems.
- Does not provide data confidentiality (encryption) of packets.

Encapsulating Security Payload (ESP)

- A security protocol that provides confidentiality and authentication by encrypting the IP packet.
- Authenticates the inner IP packet and ESP header.



Authentication Header

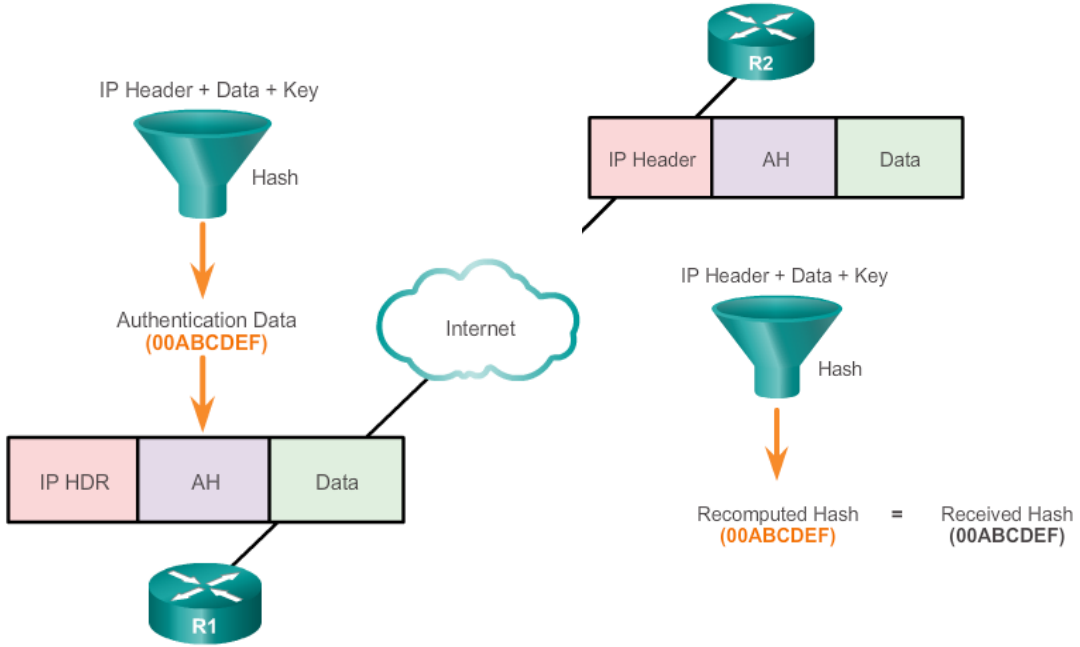
- Appropriate protocol to use when confidentiality is not required
- Provides data authentication and integrity for packets that are passed between two systems.
- Does not provide data confidentiality (encryption) of packets.

1. The IP header and data payload are hashed using the shared secret key.

2. The hash builds a new AH header, which is inserted into the original packet.

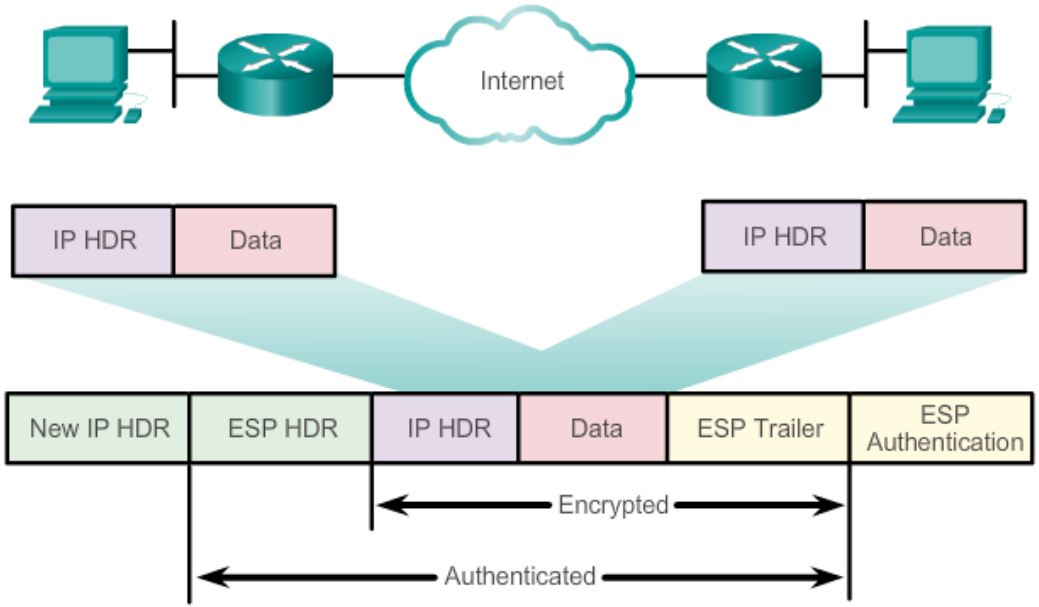
3. The new packet is transmitted to the IPsec peer router.

4. The peer router hashes the IP header and data payload using the shared secret key, extracts the transmitted hash from the AH header, and compares the two hashes.



Encapsulating Security Payload

- ESP provides confidentiality and authentication by encrypting the IP packet.
  - First, the payload is encrypted using DES (default), 3DES, AES, or SEAL.
  - Encrypted payload is hashed to provide authentication and data integrity using HMAC-MD5 or HMAC-SHA-1.
- Authenticates the inner IP packet and ESP header.

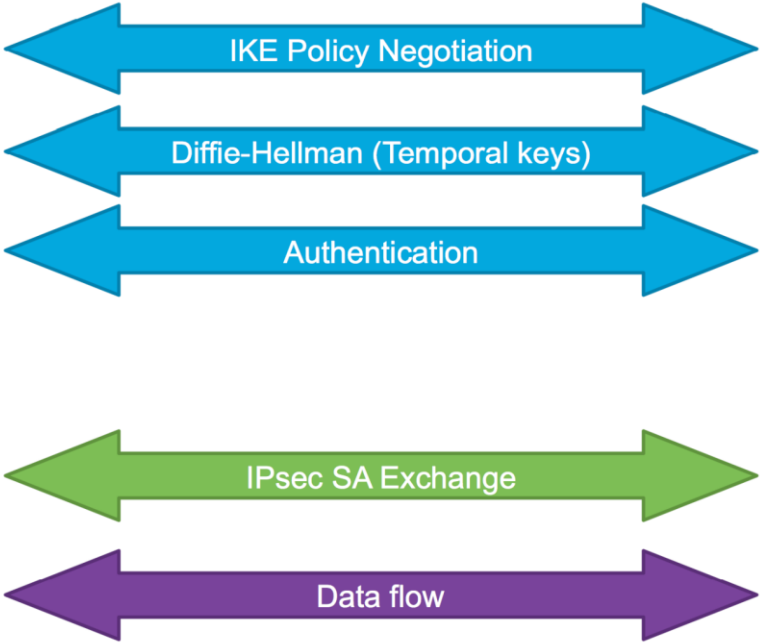


Internet Key Exchange

- Internet Key Exchange (IKE) is the protocol used to help IPSec exchange cryptographic keys and negotiate IPSec parameters (Security Associations)
- Security Association (SAs)
  - The negotiated parameters between two devices.
  - Represent a policy contract between two peers or hosts, and describe how the peers use IPsec security services to protect network traffic.
  - An IPSec VPN has SA entries defining the key exchange parameters as well as SA entries defining the IPsec encryption parameters

IKE Phase 1 and Phase 2

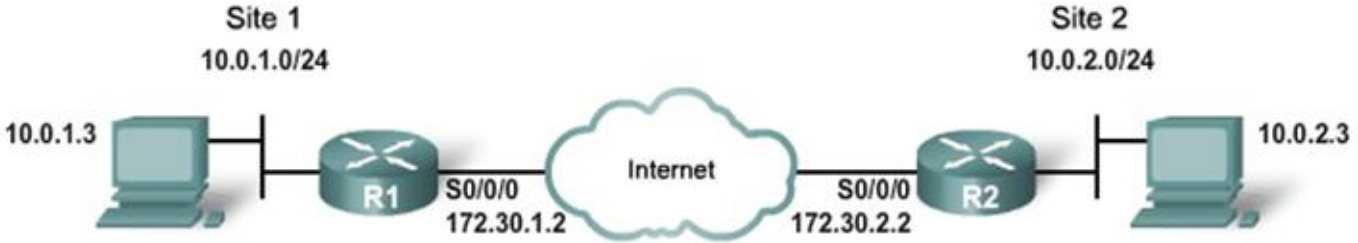
- There are two phases in every IKE negotiation
- IKE Phase One: Authentication
  - Establishes how to protect negotiation of security associations (SA) using ISAKMP
  - Used to exchange identities and authenticate each other
  - Exchange of shared temporal key using Diffie Helman to protect negotiations
  - Establishes the IKE SA and creates the first tunnel, which protects later negotiation messages
- IKE Phase Two: Key Exchange
  - Negotiates IPsec security parameters (IPsec transform sets)
  - Establishes IPsec SAs and creates the tunnel that protects the data



IPsec Configuration Tasks

Some basic tasks must be completed to configure a site-to-site IPsec VPN.

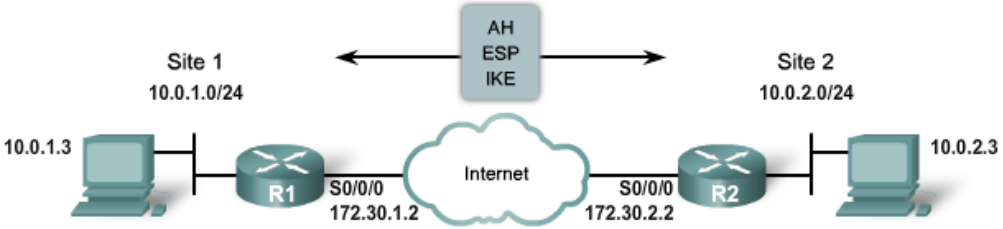
- **Task 1.** Ensure that ACLs configured on interfaces are compatible with the IPsec configuration.
- **Task 2.** Create an ISAKMP (IKE phase 1) policy.
- **Task 3.** Identify peers and configure pre-shared key
- **Task 4.** Configure the IPsec transform set.
- **Task 5.** Create a crypto ACL.
- **Task 6.** Create and apply a crypto map.



Task 1: Configure Compatible ACLs

Ensure that any ACL configured on the external router interfaces do not block ISAKMP (IKE), ESP, and AH traffic

- ESP uses IP protocol number 50.
- AH uses IP protocol number 51.
- ISAKMP (IKE) uses UDP port 500.




```
R1(config)# access-list 100 permit ahp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 100 permit esp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 100 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 100 in
```

```
R2(config)# access-list 101 permit ahp host 172.30.1.2 host 172.30.2.2
R2(config)# access-list 101 permit esp host 172.30.1.2 host 172.30.2.2
R2(config)# access-list 101 permit udp host 172.30.1.2 host 172.30.2.2 eq isakmp
R2(config)# interface S0/0/0
R2(config-if)# ip access-group 101 in
```

Task 2: Create an ISAKMP Policy

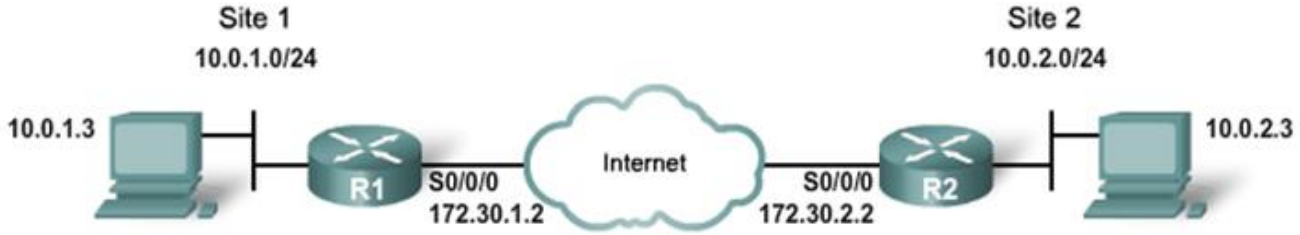
- The second major task is to define the parameters within the ISAKMP policy. Each policy specifies the encryption algorithm, integrity algorithm, key exchange algorithm and peer authentication method

Parameter	Keyword	Accepted Values
encryption	des 3des aes aes 192 aes 256	56-bit Data Encryption Standard Triple DES 128-bit AES 192-bit AES 256-bit AES
hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)
authentication	pre-share rsa-encr rsa-sig	pre-shared keys RSA encrypted nonces RSA signatures
group	1 2 5	768-bit Diffie-Hellman (DH) 1024-bit DH 1536-bit DH

```
Router(config)#crypto isakmp policy pol_num
Router(config-isakmp)#encryption encrypt_option
Router(config-isakmp)#hash hash_option
Router(config-isakmp)#group dh_option
Router(config-isakmp)#authentication auth_method
```

Task 2: Create an ISAKMP (IKE) Policy

- Multiple ISAKMP policies may be configured on each router, but at least 1 policy must have parameters that match exactly between 2 routers before the IKE phase 1 tunnel is successfully established



R1#

```
crypto isakmp policy 100
  hash md5
  authentication pre-share
!
crypto isakmp policy 200
  hash sha
  authentication rsa-sig
!
crypto isakmp policy 300
  hash md5
  authentication pre-share
```

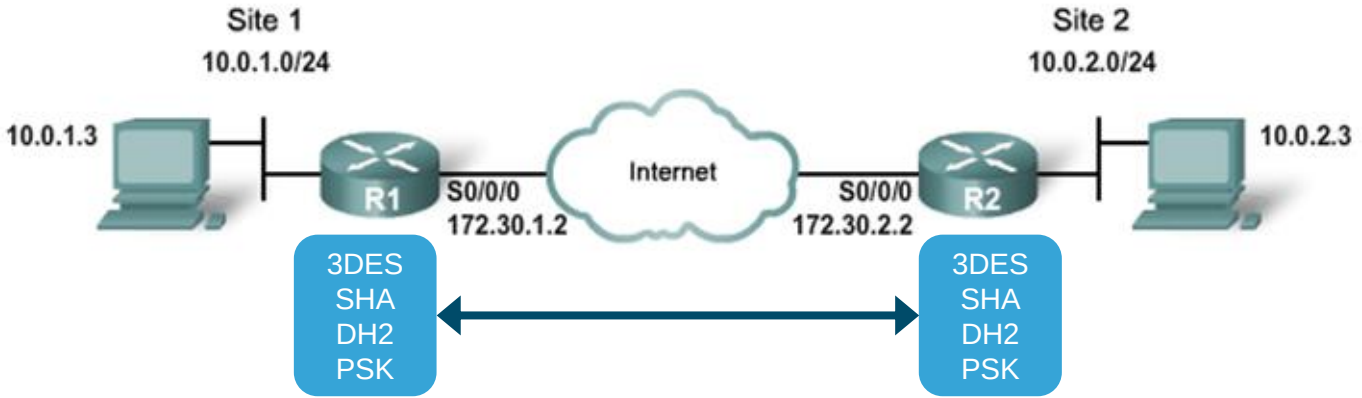
R2#

```
crypto isakmp policy 100
  hash md5
  authentication pre-share
!
crypto isakmp policy 200
  hash sha
  authentication rsa-sig
!
crypto isakmp policy 300
  hash md5
  authentication rsa-sig
```

Task 2: Create an ISAKMP (IKE) Policy

Policy numbers are only locally significant and do not have to match between IPsec peers.

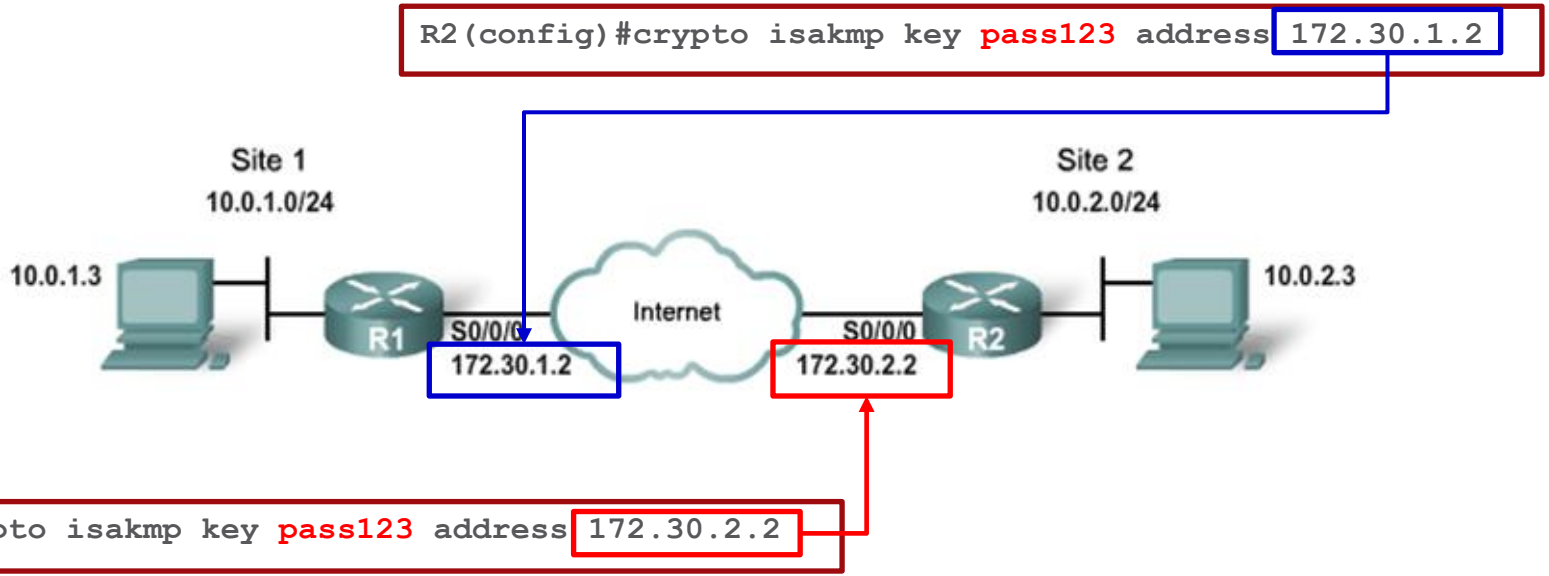
```
R2(config)#crypto isakmp policy 100
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# hash sha
R2(config-isakmp)# group 2
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# exit
```




```
R1(config)#crypto isakmp policy 110
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 2
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# exit
```

Task 3: Identify Peers and Configure PSK

- When using PSK authentication, the peer router and the shared key must be configured using the command **`Router(config)#crypto isakmp key psk_val address peer_rtr`**
- Pre-shared key must match between the peer routers



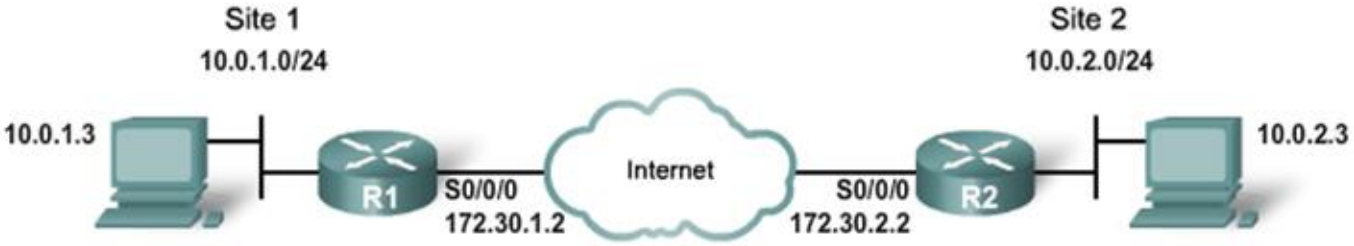
Task 4: Configure IPSec Transform Set

- A transform set is a combination of security protocols and algorithms that define how the router protects data and is negotiated during IKE phase 2 to establish the parameters that will be used the IPSec tunnel
- A transform set defines the IPSec security protocol, encryption algorithm (if using ESP) and the hashing algorithm (both AH and ESP) to be used

```
Router(config)# crypto ipsec transform-set transform-set-name ?
ah-md5-hmac    AH-HMAC-MD5 transform
ah-sha-hmac    AH-HMAC-SHA transform
esp-3des       ESP transform using 3DES(EDE) cipher (168 bits)
esp-des        ESP transform using DES cipher (56 bits)
esp-md5-hmac   ESP transform using HMAC-MD5 auth
esp-sha-hmac   ESP transform using HMAC-SHA auth
esp-null       ESP transform w/o cipher
```

Task 4: Configure IPSec Transform Set

Similar to ISAKMP policies, a router may have multiple transform sets configured; 1 of which must match a transform set on the peer so that the phase 2 tunnel can be established



transform-set ALPHA
esp-3des
tunnel

transform-set BETA
esp-3des, esp-md5-hmac
tunnel

Match ✓ transform-set CHARLIE
esp-3des, esp-sha-hmac
tunnel

transform-set RED
esp-des
tunnel

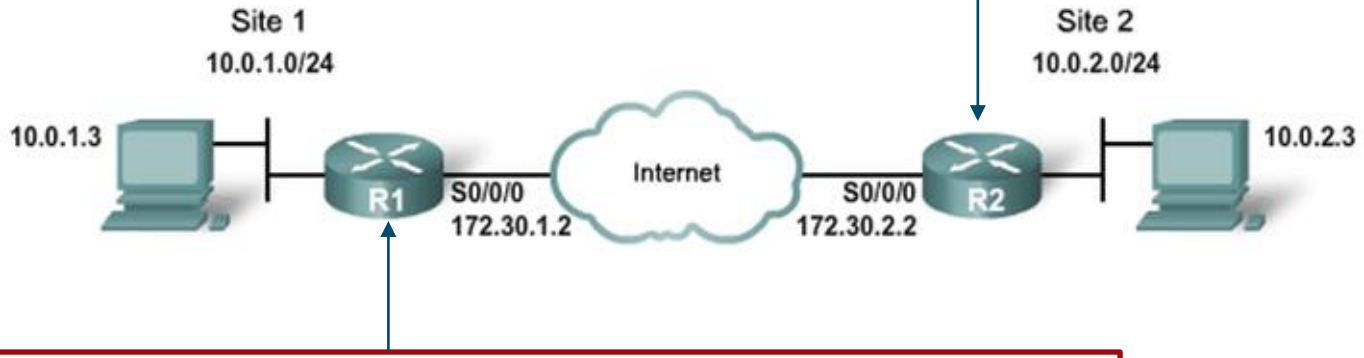
transform-set BLUE
esp-des, ah-sha-hmac
tunnel

transform-set YELLOW
esp-3des, esp-sha-hmac
tunnel
✓ Match

Task 4: Configure IPSec Transform Set

Ex: To create an IPSec transform sets that will result in a security association between R1 and R2 that uses ESP with 3DES encryption and SHA hashing

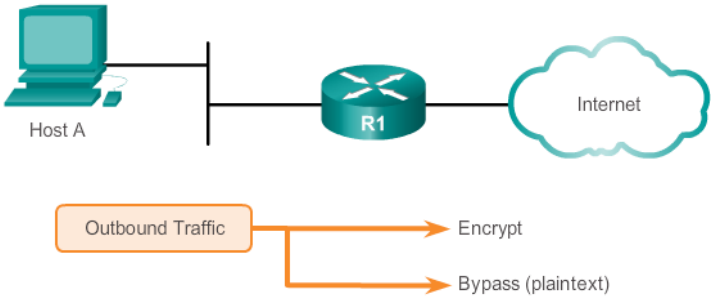
```
R2(config)#crypto ipsec transform set R2SET esp-3des esp-sha-hmac
```

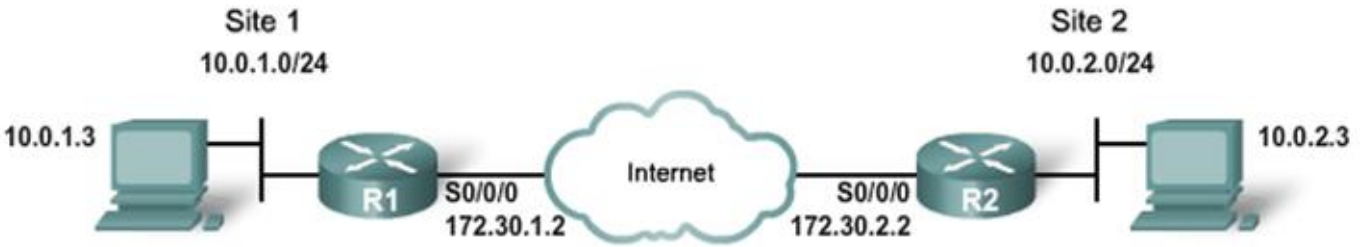



```
R2(config)#crypto ipsec transform set R1SET esp-3des esp-sha-hmac
```

Task 5: Define Crypto ACLs

- Crypto ACLs identify the traffic flows to protected using the IPSec VPN.
- Crypto ACLs define which traffic needs to be encrypted. All other traffic passes as plaintext.
- Example: To specify that all traffic between the Site 1 and Site 2 LAN must pass through the VPN:






```
R1(config)#access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

```
R2(config)#access-list 110 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

Task 6: Create and Apply Crypto Map

- Crypto maps define:
  - Which traffic to protect using a crypto ACL
  - Who the remote IPsec peers are
  - Which type of IPsec security is applied to this traffic (transform sets)
- In global config mode:

```
Router(config)# crypto map map-name seq-num ipsec-isakmp
Router(config-crypto-map)# match address acl_id
Router(config-crypto-map)# set peer peer_address
Router(config-crypto-map)# set transform-set transform_set_name
```

- Apply the crypto map under interface config mode

```
Router(config)# interface int_id
Router(config-if)# crypto map map-name
```

Task 6: Create and Apply Crypto Map


```
R1(config)# crypto map R1MAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2
R1(config-crypto-map)# set transform-set R1SET
R1(config-crypto-map)# exit
R1(config)# interface S0/0/0
R1(config-if) crypto map R1MAP
```

```
R2(config)# crypto map MYMAP 10 ipsec-isakmp
R2(config-crypto-map)# match address 110
R2(config-crypto-map)# set peer 172.30.2.2
R2(config-crypto-map)# set transform-set R2SET
R2(config-crypto-map)# exit
R2(config)# interface S0/0/0
R2(config-if) crypto map MYMAP
```

Verifying IPSec

- The **show crypto map** command verifies crypto map details and shows the SA lifetime.

```
R1# show crypto map
Crypto Map "R1MAP" 10 ipsec-isakmp
            Peer = 172.30.2.2
            Extended IP access list 110
              access-list 110 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
            Current peer: 172.30.2.2
            Security association lifetime: 4608000 kilobytes/3600 seconds
            PFS (Y/N): N
            Transform sets={
                    R1SET,
              }
              Interfaces using crypto map R1MAP:
                    Serial0/0/0
```

Verifying IPSec

- The **show crypto isakmp policy** command displays configured IKE policies

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Verifying IPSec

- The **show crypto isakmp sa** displays currently active IKE Phase 1 security associations

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
172.30.2.2      172.30.1.2      QM_IDLE           1074    0 ACTIVE
```

- The **show crypto ipsec transform-set** command shows all configured transform sets.

```
R1# show crypto ipsec transform-set
Transform set R1SET: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Verifying IPSec

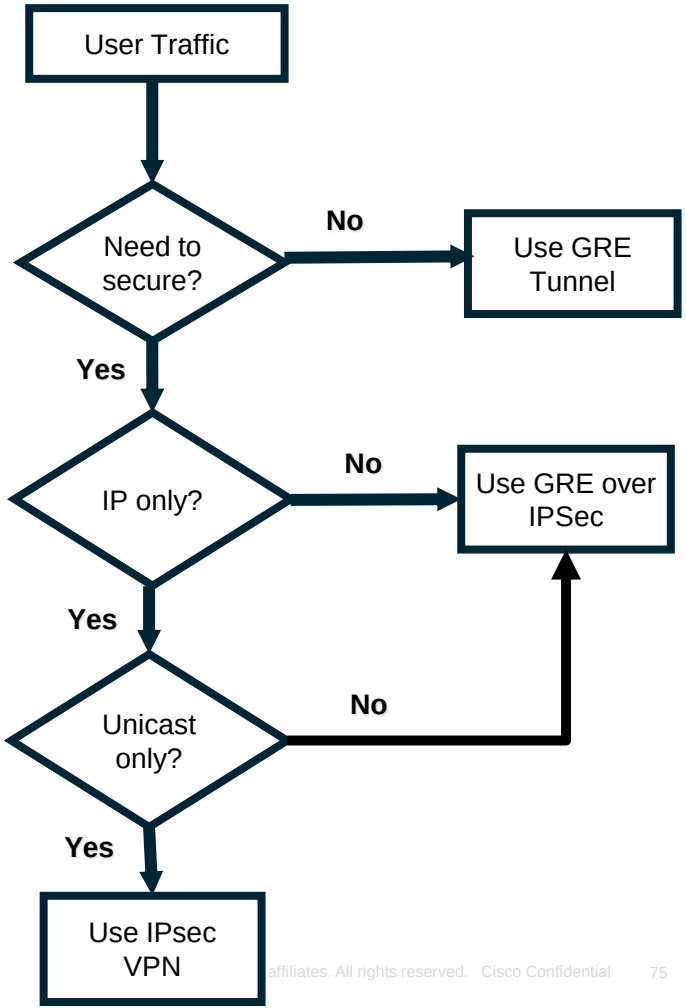
- The **show crypto ipsec sa** displays currently active IKE Phase 2 security associations

```
R1# show crypto ipsec sa
interface: Serial0/0/0
    Crypto map tag: R1MAP, local addr 172.30.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 172.30.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
...
     inbound esp sas:
      spi: 0xE7468816(3880159254)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: R1MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3188)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
...
     outbound esp sas:
      spi: 0xC2F004B4(3270509748)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: R1MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3188)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
...
```

GRE vs IPSec

- GRE
  - Advantage: can tunnel non-IP, multicast and broadcast traffic over an IP network (supports routing protocols).
  - Disadvantage: no security
- IPsec
  - Advantage: traffic is secured
  - Disadvantage: supports unicast IP only
- What to do if we need to secure routing protocol or non-IP traffic over an unsecured connection?
  - Use GRE to tunnel
  - Encrypt the GRE tunnel using IPSec (GRE over IPSec)
  - Crypto ACL must be adjusted to target the GRE traffic between peer routers instead of IP traffic between LAN hosts



What Did You Learn In This Module?

- VPNs are used to create a secure end-to-end private network connection over a third-party network, such as the Internet.
- A site-to-site VPN uses a VPN gateway device at the edge of both sites. The end hosts are unaware of the VPN and have no additional supporting software.
- A remote access VPN requires software to be installed on the individual host device that accesses the network from a remote location.
  - The two types of remote access VPNs are SSL and IPsec.
  - SSL technology can provide remote access using a client's web browser and the browser's native SSL encryption.
- VPNs may be self-deployed by an organization or created by an ISP, usually through MPLS
- GRE is a basic, non-secure site-to-site VPN tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, thus allowing an organization to deliver other protocols through an IP-based WAN.

What Did You Learn In This Module?

- IPsec, an IETF standard, is a framework that defines how to establish a secure tunnel operating at Layer 3 of the OSI model that can protect and authenticate IP packets between IPsec peers.
  - It can provide confidentiality by using encryption, data integrity, authentication, and anti-replay protection.
  - Data integrity is provided by using a hash algorithm, such as MD5 or SHA.
  - Authentication is provided by the PSK or RSA peer authentication method.
- IPsec uses IKE to establish a secure tunnel between peers. The process involves 2 phases:
  - Phase 1 authenticates peers negotiates the parameters of a secure tunnel that will be used to exchange keys
  - Phase 2 exchanges keys in order to establish the secure tunnel that will be used to transport user data