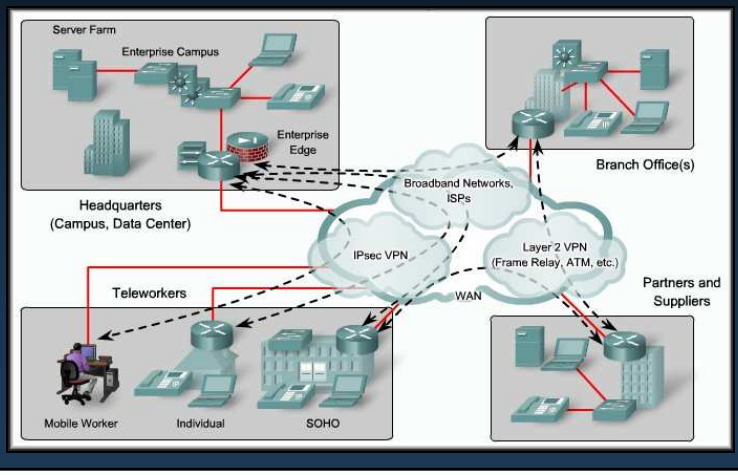
Chapter 6

Teleworker Services

Teleworker Services

Business Requirements for Teleworkers

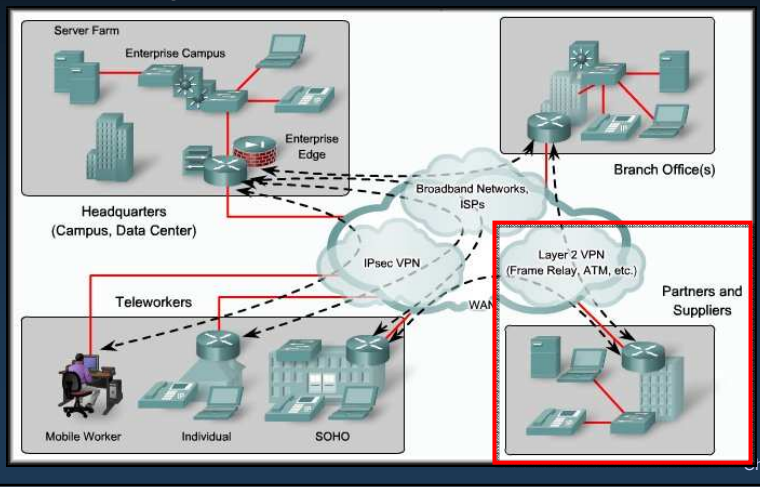


Business Requirements for Teleworkers

- Organizational Benefits:
  - Continuity of operations.
  - Increased responsiveness.
  - Secure, reliable and manageable access to information.
  - Cost-effective integration of voice, video and data.
  - Increased employee productivity, satisfaction and retention.
- Social:
  - Increased employment opportunities.
  - Less travel and commuter related stress.
- Environmental:
  - Smaller carbon footprint.

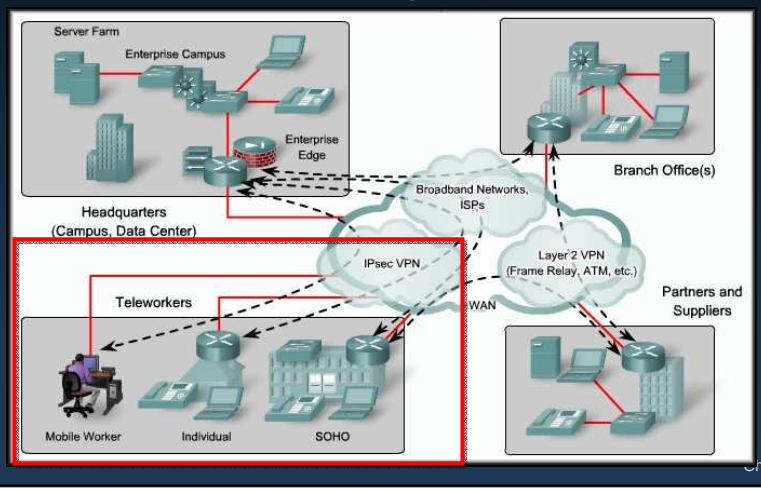
The Teleworker Solution

- Traditional, private WAN technologies:
  - Frame Relay, ATM, Leased Lines



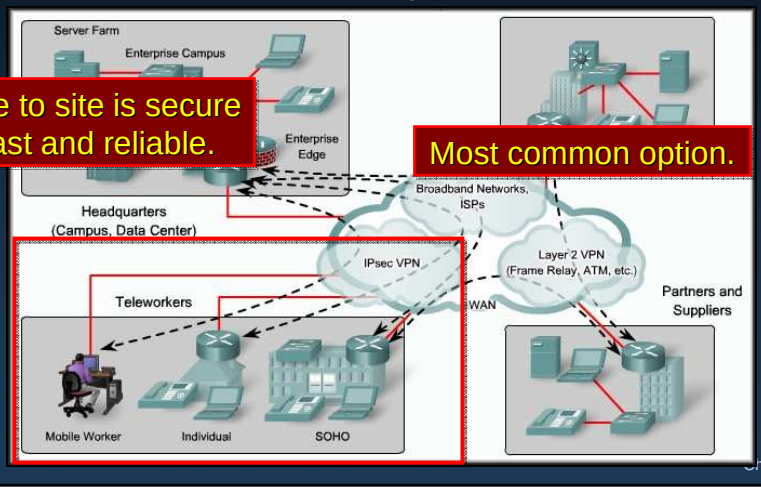
The Teleworker Solution

- IPsec Virtual Private Networks (VPN):
  - Flexible, scalable connectivity.



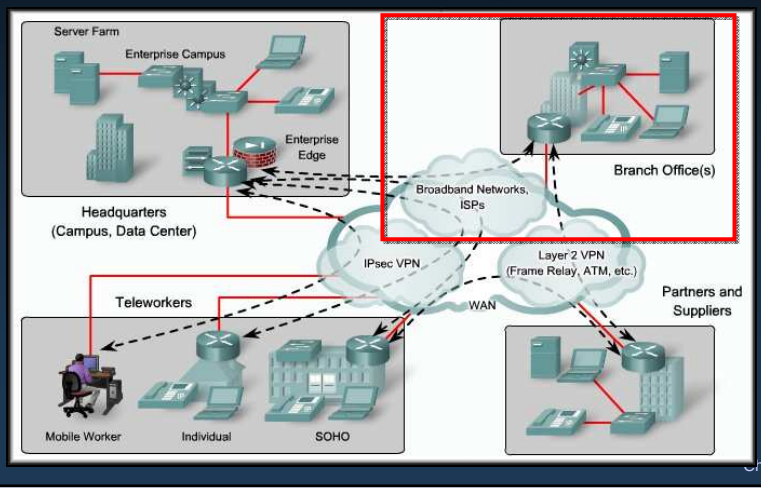
The Teleworker Solution

- IPsec Virtual Private Networks (VPN):
  - Flexible, scalable connectivity.



The Teleworker Solution

- Broadband Connections:
  - DSL, Cable, Wireless, Satellite.



The Teleworker Solution

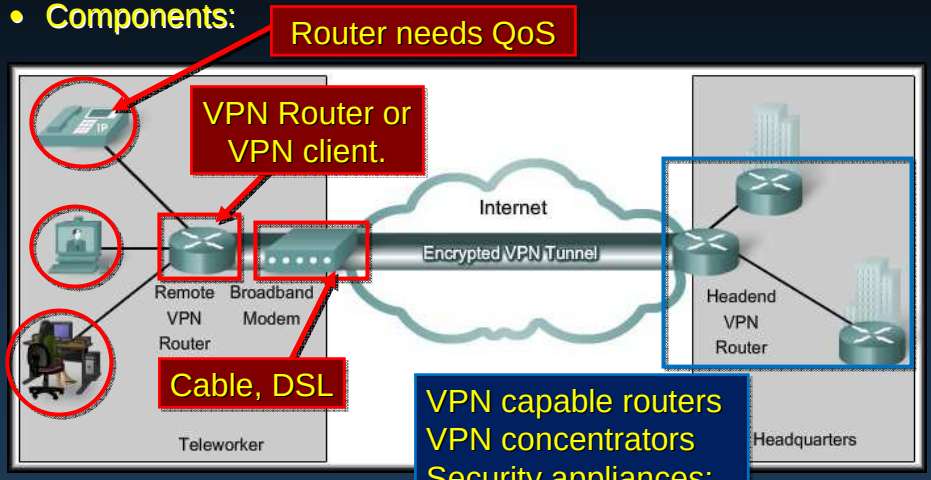
- Broadband Connections:
  - DSL, Cable, Wireless, Satellite.
    - Broadband refers to advanced communications systems capable of providing high-speed transmission of services over the Internet and other networks.
  - Transmission speeds typically exceed 200,000 bits per second in at least one direction:
    - Downstream:
      - From the Internet to the user's computer.
    - Upstream:
      - From the user's computer to the Internet.

The Teleworker Solution

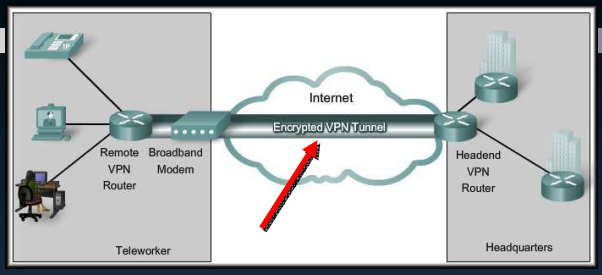
- Broadband vs. Baseband:
  - Baseband:
    - Only one signal on the wire at once.
    - May use Time Division Multiplexing (TDM)
      - Ethernet networks.
  - Broadband:
    - Multiple signals on the same line.
    - Frequency Division Multiplexing.

The Teleworker Solution

- Components:



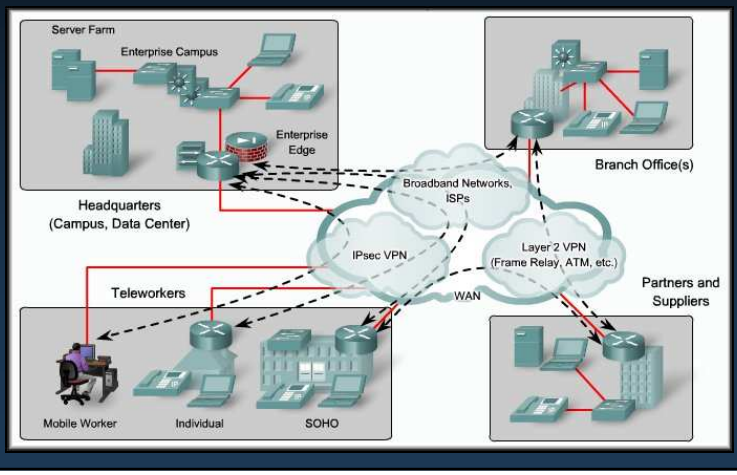
The Teleworker Solution



- Components:
  - The encrypted VPN tunnel is the heart of secure and reliable teleworker connections.
  - Virtual Private Network (VPN):
    - A private data network that uses the public telecommunication infrastructure. VPN security maintains privacy using a tunneling protocol and security procedures.
  - The IPsec (IP Security) tunneling protocol is the favored approach to building secure VPN tunnels.

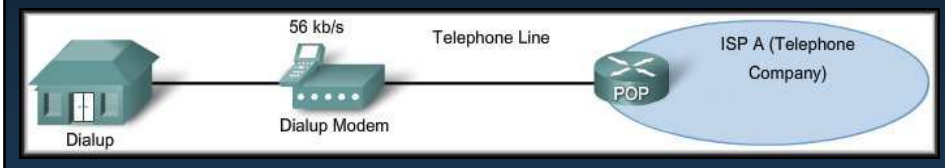
Teleworker Services

Broadband Services



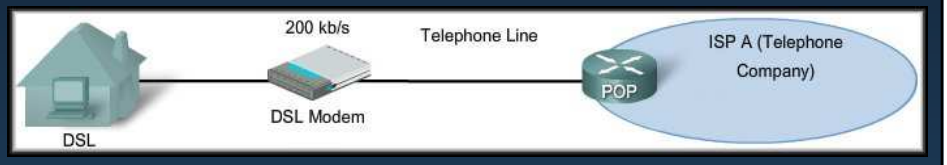
Connecting Teleworkers to the WAN

- Dialup Access:
  - Inexpensive using existing telephone lines.
  - The slowest option, it is typically used by mobile workers in areas where high speed connection are not available.



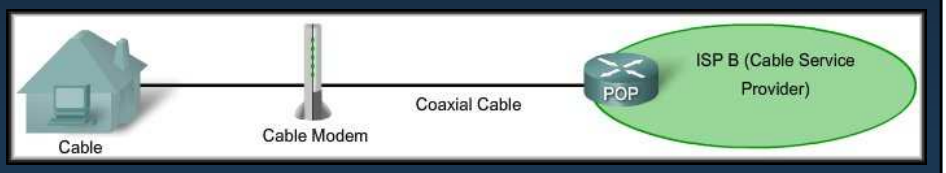
Connecting Teleworkers to the WAN

- DSL Access:
  - DSL also uses telephone lines.
  - A DSL modem separates the DSL signal from the telephone signal.
  - Provides an Ethernet connection to a host computer or LAN.



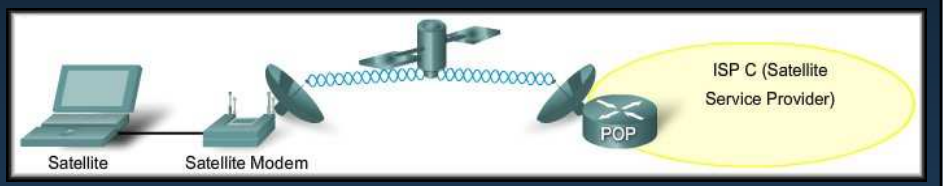
Connecting Teleworkers to the WAN

- Cable Access:
  - The Internet signal is carried on the same coaxial cable that delivers cable TV.
  - The cable modem separates the Internet signal from the other signals.
  - Provides an Ethernet connection to a host computer or LAN.



Connecting Teleworkers to the WAN

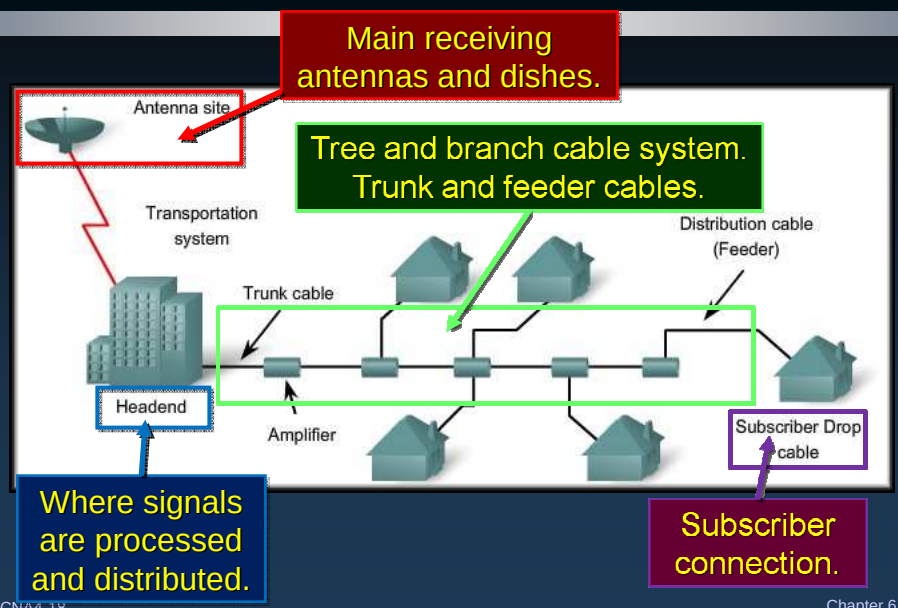
- Satellite Access:
  - The computer connects to a satellite modem that transmits radio signals to the nearest point of presence within the satellite network.
  - Provides an Ethernet connection to a host computer.



Cable

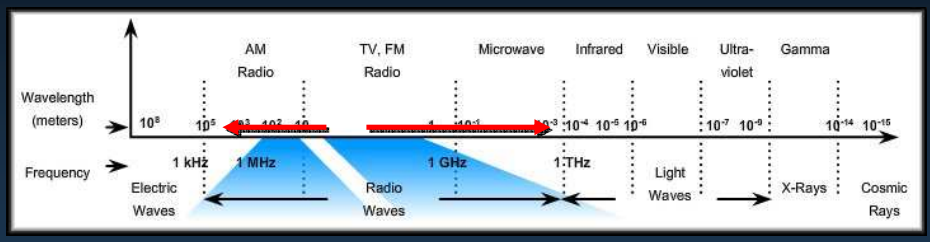
- The “cable” in cable system refers to the coaxial cable that carries radio frequency (RF) signals across the network.
- A typical cable operator now uses a satellite dish or microwave system to gather TV signals.
- Early systems were one-way with cascading amplifiers placed in series along the network to compensate for signal loss.
- Modern cable systems provide two-way communication between subscribers and the cable operator.
  - Cable operators now offer customers high-speed Internet access, digital cable television, and residential telephone service.

Cable



Cable

- Electromagnetic Spectrum:
  - The cable TV industry uses a portion of the RF electromagnetic spectrum.



- Signals are transmitted simultaneously in either direction.
- Divided into two paths:
  - Downstream: Headend to Subscriber (810 MHz).
  - Upstream: Subscriber to Headend (37 MHz).

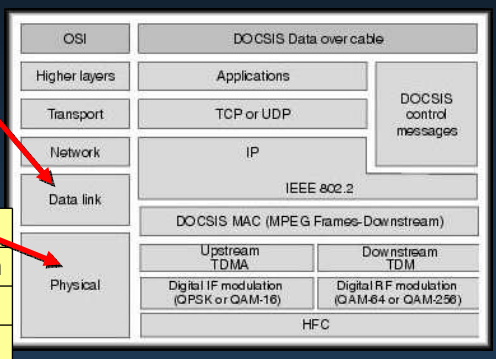
Cable

- DOCSIS:
  - The Data-over-Cable Service Interface Specification (DOCSIS) is an international standard developed by CableLabs.
    - A non-profit research and development consortium for cable-related technologies.
  - CableLabs tests and certifies cable equipment vendor devices:
    - Cable modems.
    - Cable modem termination systems.
    - Grants DOCSIS-certified or qualified status.
  - Euro-DOCSIS: Adapted for use in Europe with different standards.

Cable

- DOCSIS:
  - DOCSIS specifies the Open Systems Interconnection (OSI) Layers 1 and 2 requirements.

Access method regarding the multiplexing of signals.



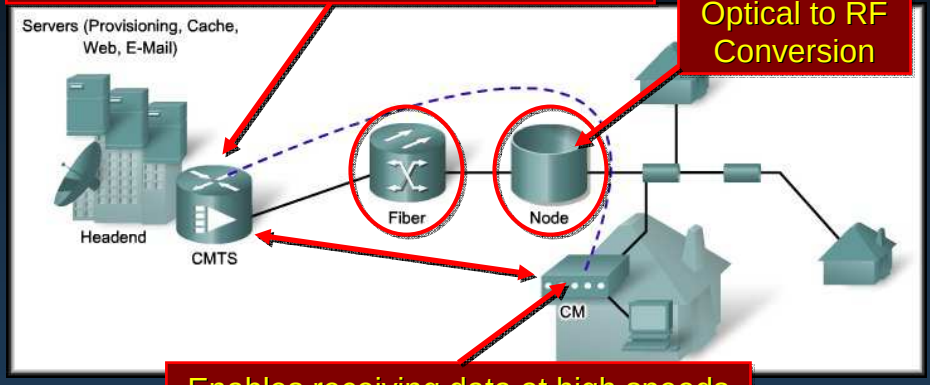
Channel Bandwidths – Mbits/s		
Release	Upstream	Downstream
DOCSIS 1.0	38	10
DOCSIS 2.0	40	30
DOCSIS 3.0	160	120

Cable

- Delivering Services Over Cable:

Cable Modem Termination System (CMTS)

Optical to RF Conversion

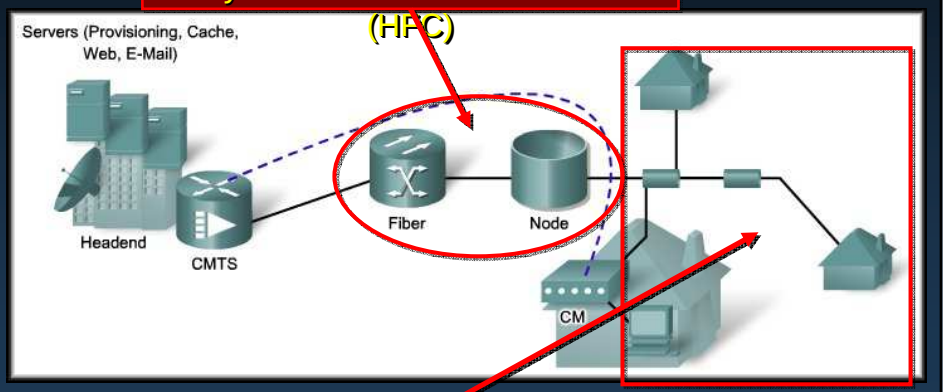


Enables receiving data at high speeds and provides a LAN attachment

Cable

- Delivering Services Over Cable:

Hybrid Fiber-Coaxial Network (HFC)

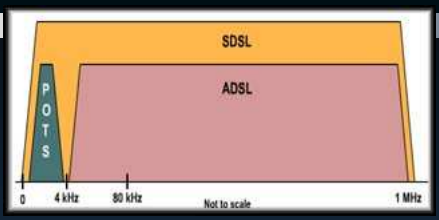


Shared bandwidth can be adjusted for congestion.

Digital Subscriber Line (DSL)

- DSL is a means of providing high-speed connections over installed copper wires.
  - A typical phone line can handle signals up to 1 MHz.
  - A typical phone conversation uses from 300 Hz to 3 kHz.
  - The additional bandwidth is used for DSL.

Digital Subscriber Line (DSL)



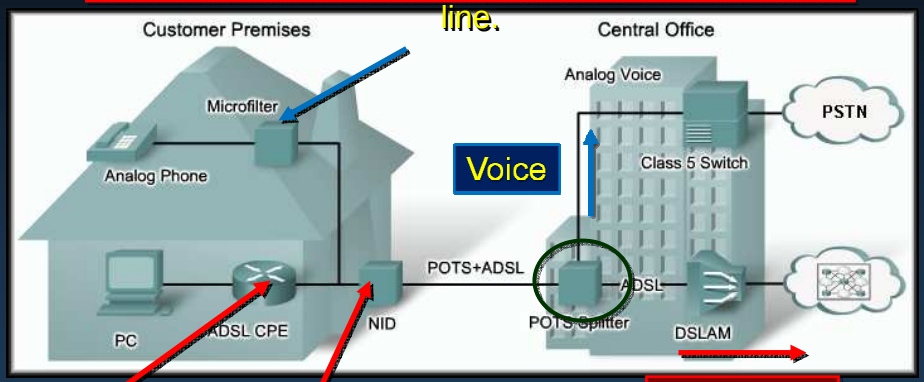
- The two basic types of DSL technologies are asymmetric (ADSL) and symmetric (SDSL).
  - All forms of DSL service are categorized as ADSL or SDSL, and there are several varieties of each type.
  - ADSL provides higher downstream bandwidth to the user than upload bandwidth.
  - SDSL provides the same capacity in both directions.

Service	Download	Upload
ADSL	64 kbps - 8.192 Mbps	16 kbps - 640 kbps
SDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
HDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
IDSL	144 kbps	144 kbps
CDSL	1 Mbps	16 kbps - 160 kbps

Digital Subscriber Line (DSL) - Connections

DSL is not a shared medium.

Voice and data over the same copper telephone line.



DSL modem, router.

Demarc: Network Interface Device.

DSL Access Multiplexer

Broadband Wireless

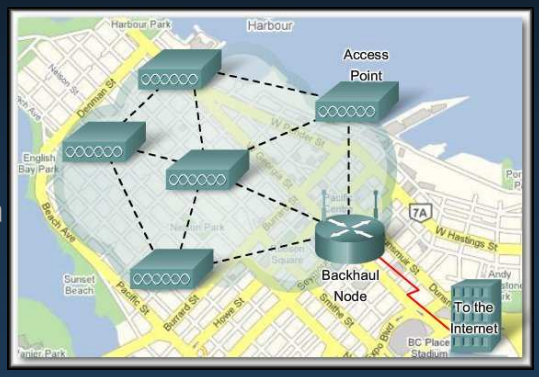
- Wireless networking, or Wi-Fi, has improved the connectivity situation, not only in the SOHO, but also on enterprise campuses.
- Using 802.11 networking standards, data travels using the unlicensed radio spectrum.
- Most radio and TV transmissions are government regulated and require a license to use.

Broadband Wireless

- Until recently, a significant limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or wireless access point that has a wired connection to the Internet.
- Once a worker left the office or home, wireless access was not readily available.
- New developments in broadband wireless technology are increasing wireless availability.
  - Municipal Wi-Fi
  - WiMAX
  - Satellite Internet

Broadband Wireless

- **Municipal Wi-Fi:**
  - Most municipal wireless networks use a **mesh topology** rather than a hub-and-spoke model.
  - The mesh blankets its area with radio signals.
  - Signals travel from access point to access point through this cloud.
  - Installation easier.
  - Faster deployment.
  - More reliable.

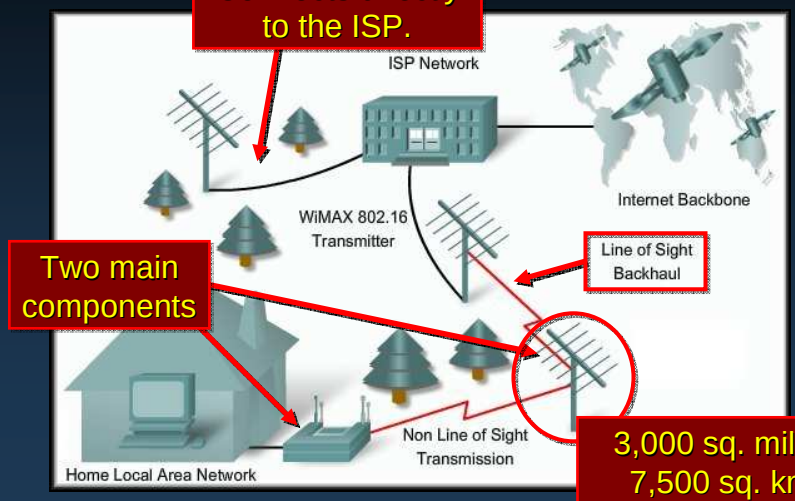


Broadband Wireless

- **WiMAX:**
  - WiMAX **(Worldwide Interoperability for Microwave Access)** is telecommunications technology aimed at providing wireless data over long distances in a variety of ways.
  - WiMAX operates at **higher speeds, over greater distances**, and for a **greater number of users** than Wi-Fi.
  - Because of its higher speed (bandwidth) and falling component prices, the WiMAX will soon supplant municipal mesh networks for wireless deployments.

Broadband Wireless

- **WiMAX:**



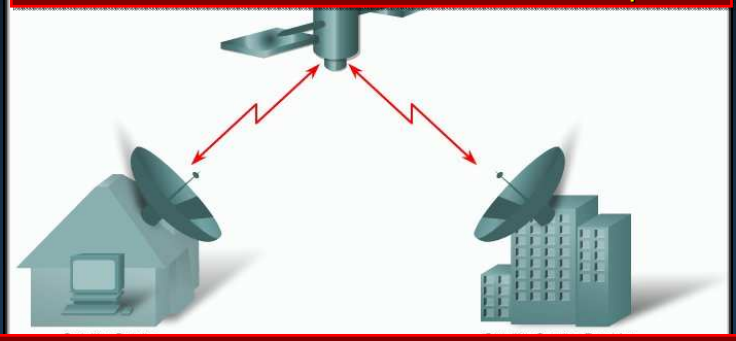
Broadband Wireless

- **Satellite Internet:**
  - Satellite Internet services are used in locations where land-based Internet access is not available, or for temporary installations that are continually on the move.
  - There are 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.

Broadband Wireless

- Two-way Satellite Internet:

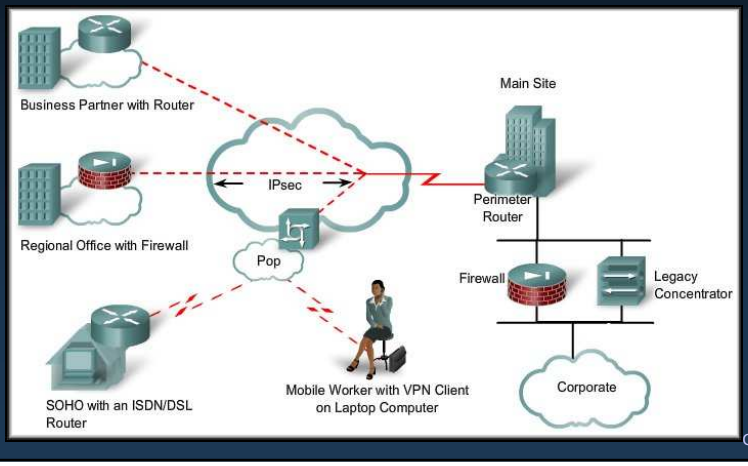
The key installation requirement is for the antenna to have a clear view toward the equator.



Two-way satellite Internet uses IP multicasting technology. Allows one satellite to serve up to 5,000 channels.

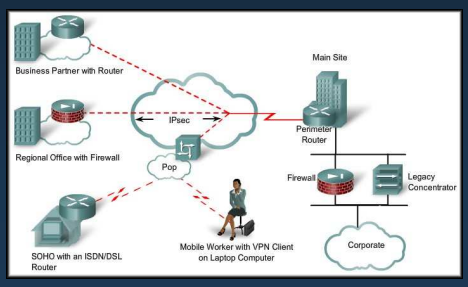
Teleworker Services

Virtual Private Network (VPN) Technology



VPNs and Their Benefits

- What is a VPN?
  - *A VPN creates a private network over a public network infrastructure while maintaining confidentiality and security.*
  - VPNs use cryptographic tunneling protocols to provide protection against packet sniffing, sender authentication, and message integrity.
  - Organizations use VPNs to provide a virtual WAN that connects branch or home offices, business partner sites, and remote telecommuters.

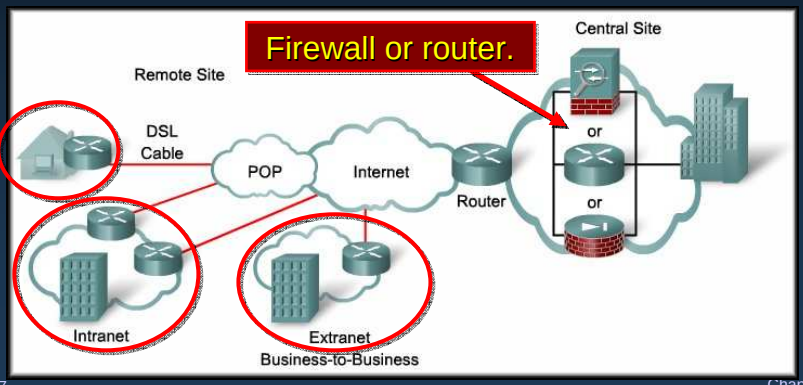


VPNs and Their Benefits

- Benefits:
  - Cost Savings:
    - Organizations can use cost-effective, third-party Internet transport to connect remote offices and users to the main corporate site. This eliminates expensive dedicated WAN links and modem banks.
  - Security:
    - Advanced encryption and authentication protocols protect data from unauthorized access.
  - Scalability:
    - Organizations, big and small, are able to add large amounts of capacity without adding significant infrastructure.

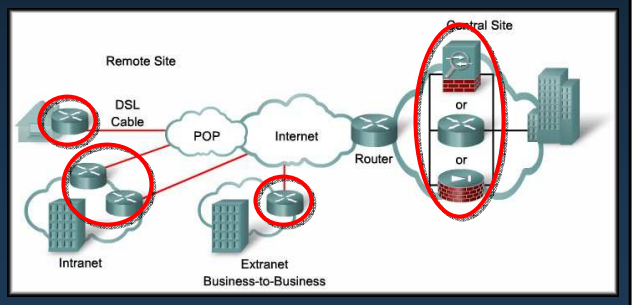
Types of VPNs

- Site-to-site VPN:
  - A site-to-site VPN is an extension of classic WAN networking.
  - Site-to-site VPNs connect entire networks to each other.



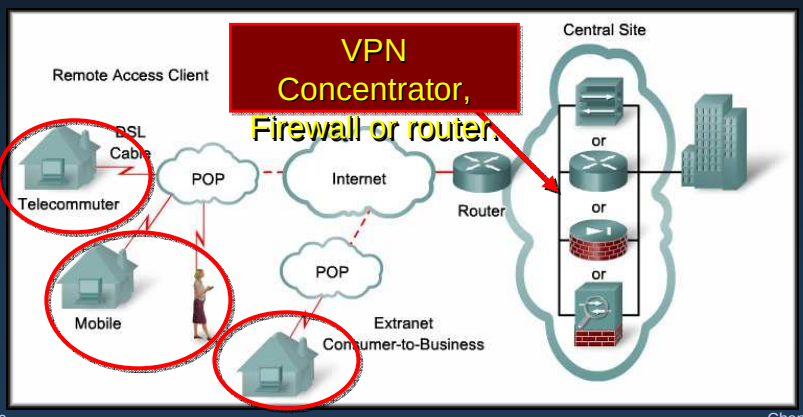
Types of VPNs

- Site-to-site VPN:
  - In a site-to-site VPN, hosts send and receive TCP/IP traffic through a VPN gateway.
  - The VPN gateway encapsulates and encrypts outbound traffic and sends it through a VPN tunnel.
  - On receipt, the peer VPN gateway strips the headers, decrypts the content and relays the packet.



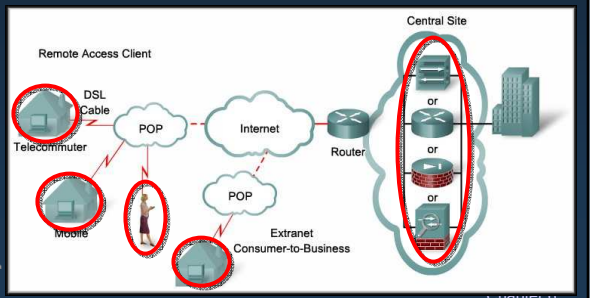
Types of VPNs

- Remote Access VPN:
  - Support the needs of telecommuters, mobile users, as well as extranet consumer-to-business.

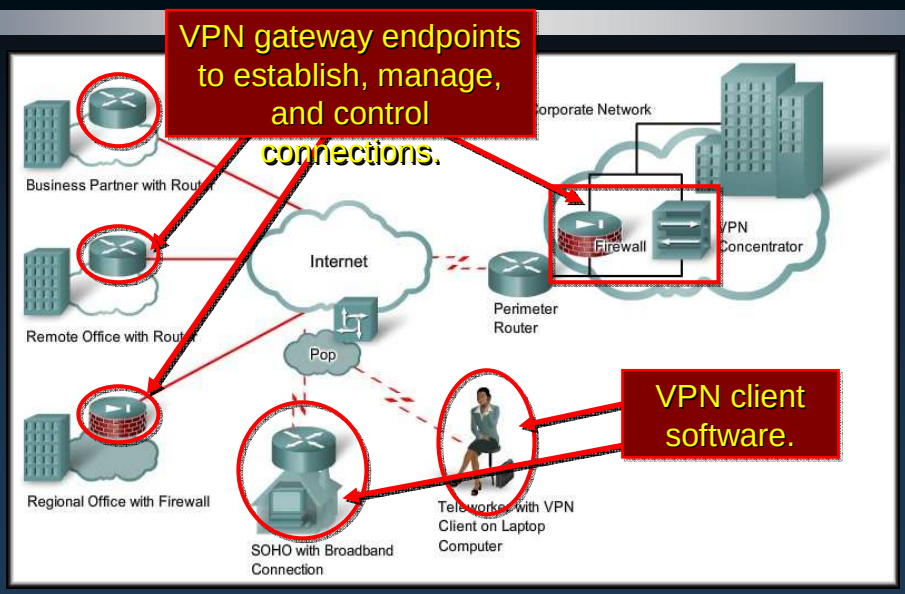


Types of VPNs

- Remote Access VPN:
  - Support the needs of telecommuters, mobile users, as well as extranet consumer-to-business.
  - Each host typically has VPN client software.
  - The software encapsulates and encrypts that traffic before sending it over the Internet.
  - On receipt, the VPN gateway handles the data in the same way as it would handle data from a site-to-site VPN.



VPN Components



VPN Components

- *The key to VPN effectiveness is security.*
  - VPNs secure data by encapsulating and encrypting the data.
  - **Encapsulation is referred to as tunneling**, because encapsulation transmits data transparently from network to network through a shared infrastructure.
    - As if an individual tunnel existed between the endpoints.
  - **Encryption** codes data into a different format using a key.
  - **Decryption** decodes encrypted data into the original unencrypted format.

Characteristics of Secure VPNs

- The foundation of a secure VPN are the following:
  - Data Confidentiality:
    - A common security concern is protecting data from eavesdroppers or unauthorized sources (Encapsulation and Encryption).
  - Data integrity:
    - Data integrity guarantees that no tampering or alterations occur to data while it travels between the source and destination (Hashing).
  - Authentication:
    - Authentication ensures that a message comes from an authentic source and goes to an authentic destination (Passwords, Certificates, Biometrics).

VPN Tunneling

- Tunneling allows the use of public networks like the Internet to carry data for users as though the users had access to a private network.
  - Tunneling encapsulates an entire packet within another packet and sends the new, composite packet over a network.

Tunneling Protocols

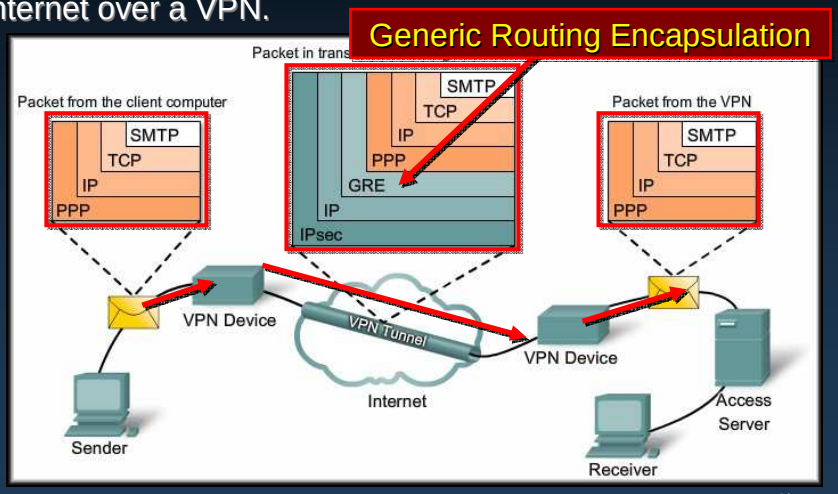
Carrier protocol:
- The protocol over which the information is traveling (Frame Relay, ATM, MPLS).

Encapsulating protocol:
- The protocol that is wrapped around the original data (GRE, IPSec, L2F, PPTP, L2TP).

Passenger protocol:
- The protocol over which the original data was being carried (IPX, AppleTalk, IPv4, IPv6).

VPN Tunneling

- For example, an e-mail message traveling through the Internet over a VPN.

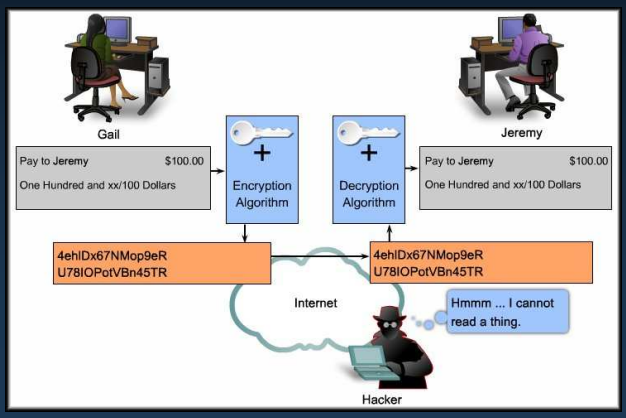


VPN Tunneling

- In the example, PPP carries the message to the VPN device, where the message is encapsulated within a Generic Route Encapsulation (GRE) packet.
  - GRE is a tunneling protocol developed by Cisco.
    - The outer packet source and destination addressing (Internet IP Addresses) is assigned to "tunnel interfaces" and is made routable across the network.
    - Once a composite packet reaches the destination tunnel interface, the inside packet is extracted.

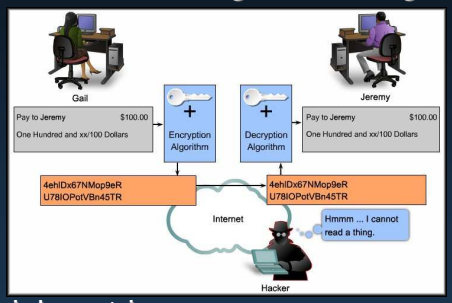
VPN Data Confidentiality and Integrity

- If plain text data is transported over the public Internet, it can be intercepted and read.
  - To keep the data private, it needs to be encrypted.
  - Encryption of the data renders it unreadable to unauthorized receivers.



VPN Data Confidentiality and Integrity

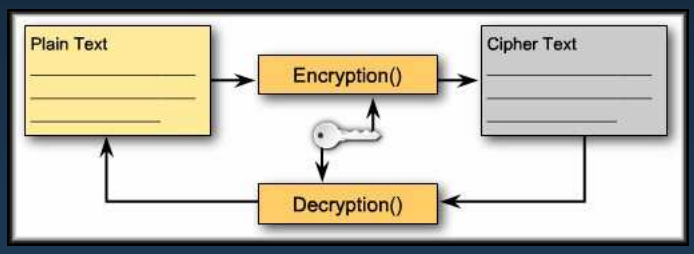
- For encryption to work, both the sender and the receiver must know the rules used to transform the original message into its coded form.
- VPN encryption rules include an algorithm and a key.
- An algorithm is a mathematical function that combines a message, text, digits or all three with a key.



- The output is an unreadable cipher string.
  - Decryption is extremely difficult without the correct key.

VPN Data Confidentiality and Integrity

- The degree of security provided by any encryption algorithm **depends on the length of the key**.
  - The shorter the key, the easier it is to break,
  - However, the shorter the key, the easier it is to pass the message.



VPN Data Confidentiality and Integrity

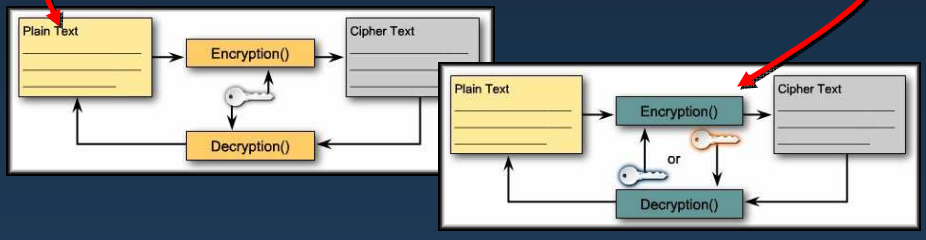
- More common encryption algorithms and key lengths:
  - **Data Encryption Standard (DES)**:
    - Developed by IBM.
    - High performance.
    - 56 bit.
  - **Triple DES (3DES)**:
    - A variant of DES that encrypts with one key, decrypts with another different key, and then encrypts one final time with another key.
    - 192 bit.

VPN Data Confidentiality and Integrity

- More common encryption algorithms and key lengths:
  - Advanced Encryption Standard (AES):
    - Replaced DES encryption.
    - More secure.
    - Computationally more efficient.
    - 128, 192, and 256 bit.
  - Rivest, Shamir, and Adleman (RSA):
    - 512, 768, 1024 bit and larger.

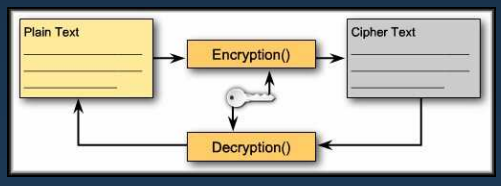
VPN Data Confidentiality and Integrity

- Not only does the degree of security depend on the length of the key but also on the way the key is shared by the end users.
  - Symmetric Encryption (Secret Key):
    - Encryption and decryption keys are the same.
  - Asymmetric Encryption (Public Key):
    - Encryption and decryption keys are different.



VPN Data Confidentiality and Integrity

- Symmetric Encryption (Secret Key):
  - Encryption and decryption keys are the same.
    - How do the encrypting and decrypting devices both have the shared secret key?
      - You could use e-mail, courier, or overnight express to send the shared secret keys to the administrator of the device.
      - A more secure method is asymmetric encryption.



VPN Data Confidentiality and Integrity

- Asymmetric Encryption (Public Key):
  - Encryption and decryption keys are different.
  - One key encrypts the message, while a second key decrypts the message.
    - Each user has two different keys that act as a key pair - public and private.
    - Public keys are exchanged with other users.
    - Messages sent are encrypted with the sender's private key and the recipient's public key.
    - Messages received are decrypted with the sender's public key and the recipient's private key.

VPN Data Confidentiality and Integrity

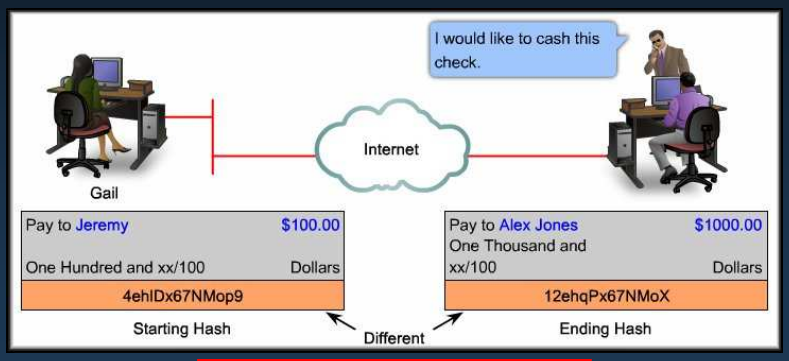
Symmetric Encryption	Asymmetric Encryption
Secret Key cryptography	Public Key cryptography
Encrypt and decrypt with the same key	Encrypt and decrypt with a different key
Typically used for message content	Typically used for digital certificates and key management
DES, 3DES, ADES	RSA

VPN Data Confidentiality and Integrity

- VPN Data Integrity:
  - Hashes contribute to data integrity and authentication by ensuring that unauthorized persons do not tamper with transmitted messages.
    - A hash, also called a message digest, is a value (authentication code) generated from a string of text.
    - It is generated using a formula and a shared key and included as part of the encrypted message.
    - The recipient uses the same formula and key to generate the authentication code.
    - If the values match, the recipient can be sure that the message has not been changed in transit.

VPN Data Confidentiality and Integrity

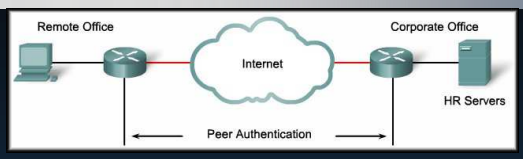
- VPN Data Integrity:
  - Message Digest 5 (MD5): 128 bit key.
  - Secure Hash Algorithm 1 (SHA-1): 160-bit key.



Something was changed!

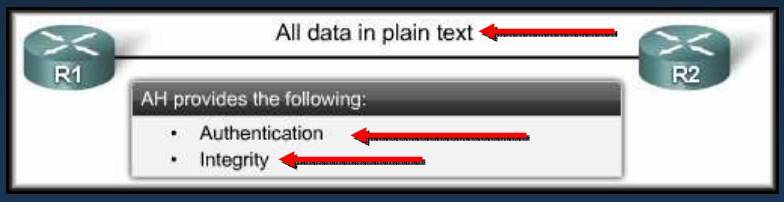
VPN Data Confidentiality and Integrity

- VPN Authentication:
  - The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure.
    - There are two peer authentication methods:
      - Pre-shared key (PSK):
        - A secret key that is shared between the two parties using a secure channel before it needs to be used.
      - RSA signature:
        - Uses the exchange of digital certificates to authenticate the peers.



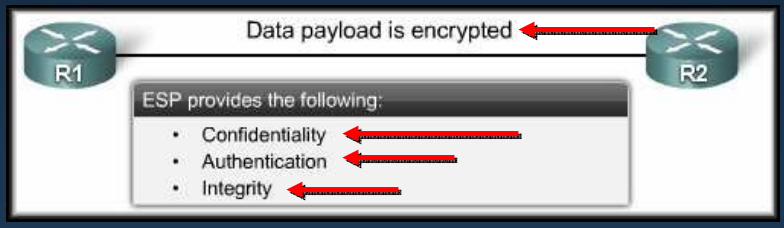
IPsec Security Protocols

- IPsec is a protocol suite for securing IP communications with encryption, integrity, and authentication.
  - There are two main IPsec framework protocols:
    - Authentication Header (AH):
      - Use when confidentiality is not required or permitted.



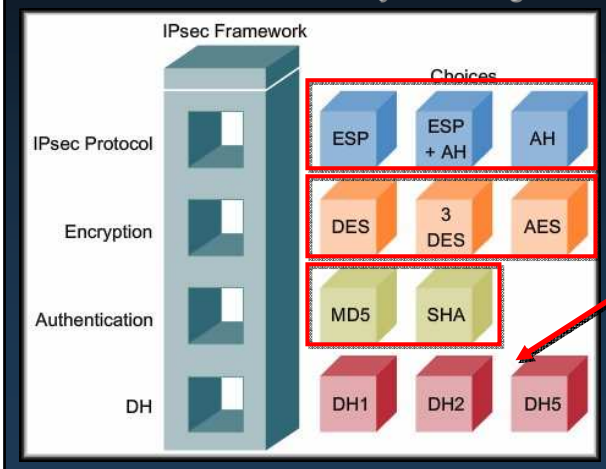
IPsec Security Protocols

- IPsec is a protocol suite for securing IP communications with encryption, integrity, and authentication.
  - There are two main IPsec framework protocols:
    - Encapsulating Security Payload (ESP):
      - Provides confidentiality and authentication by encrypting the packet.



IPsec Security Protocols

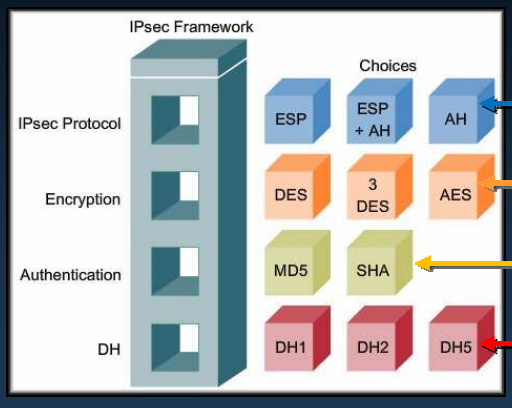
- IPsec relies on existing algorithms to implement encryption, authentication, and key exchange.



Diffe-Hellman: Allows two parties to establish a shared secret key used by encryption and hash algorithms over an unsecure line.

IPsec Security Protocols

- When configuring Ipsec, there are four choices to be made:



Which IPsec Protocol?

Which Encryption?

Which hash method?

How to share keys.