DCF255

Lecture 7 | Ethernet: Wired and Wireless

Agenda

- Wired Ethernet IEEE 802.3
  - Hierarchical Structure
  - Frame Format
- Wired Ethernet Security
  - RSTP
  - 802.1x
- Types of Ethernet Networks and Switches
- Types of Switches
- Wireless Ethernet 802.11
  - Wireless Errors
  - Wireless Frame Format
  - Wireless Security and VPNs

Wired Ethernet

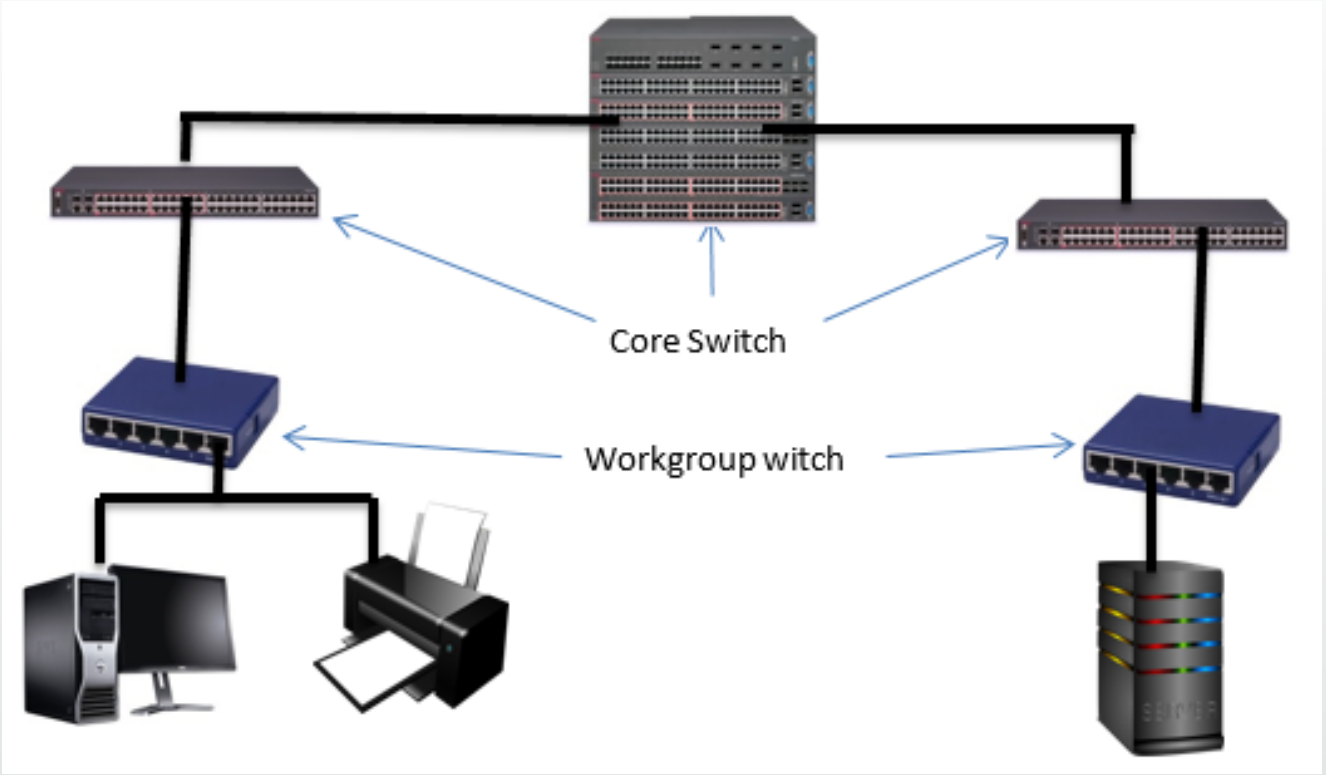
IEEE 802.3

Ethernet

- Wired IEEE 802.3 most popular today
- Great cost to performance ratio.
- Being developed into a MAN and WAN technology:
  - MAN: Metro Ethernet
  - WAN – on hold
- Wireless Ethernet IEEE 802.11
  - Most popular method to access Internet
  - Wired and Wireless work together to provide seamless network communication

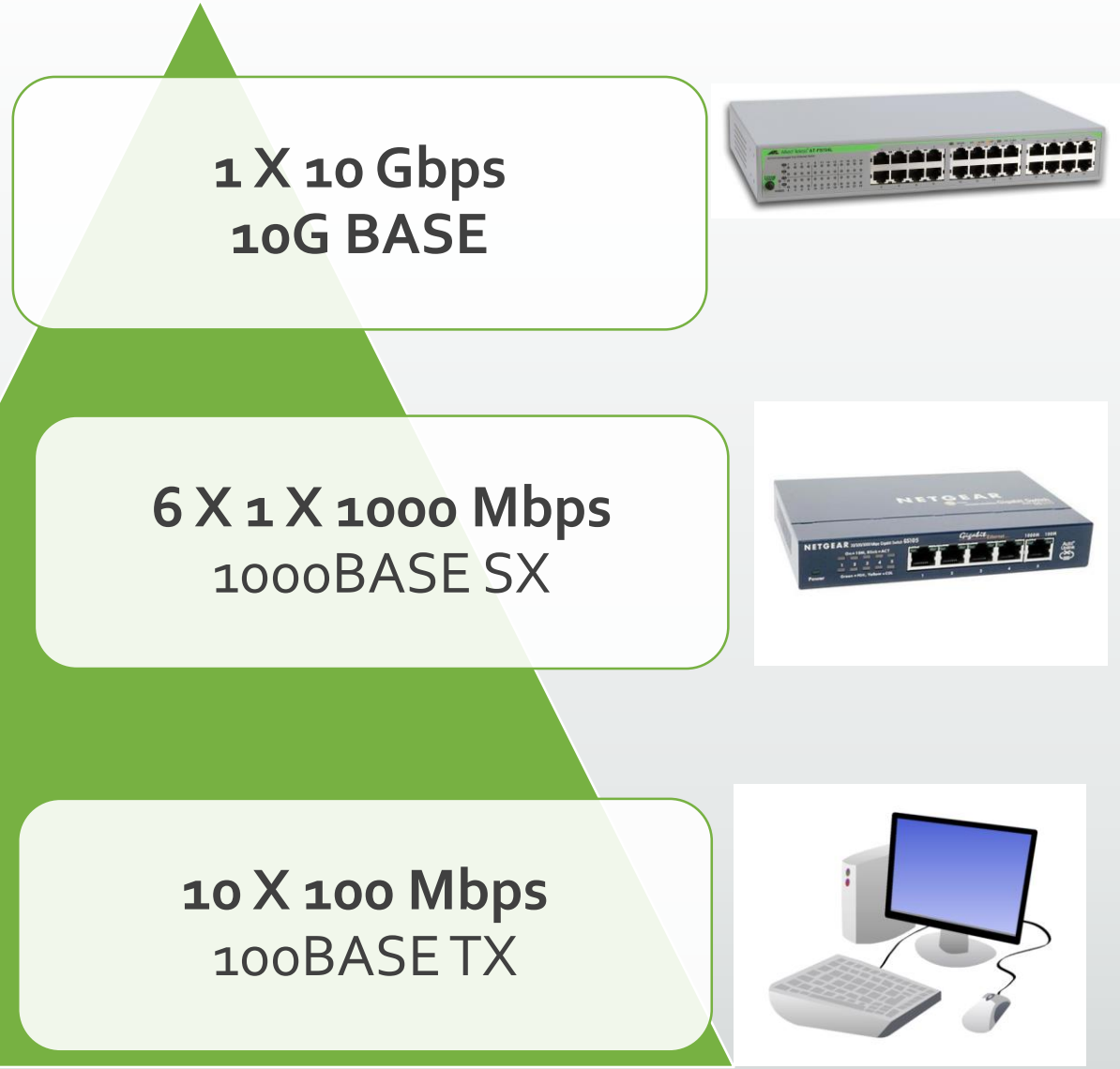
Wired Ethernet 802.3

- Network built in a hierarchical manner using a combination of workgroup and core switches
- Allows combining expensive with cheaper equipment to match performance
- Workgroup switches connect devices to the network
- Core switches connect switches to switches



Aggregate Speed

- Key design principle is that you have enough bandwidth to handle the aggregate speed of all devices on the network
- 10 devices @ 100 Mbps connected to workgroup switch
- Workgroup switch must be able to carry 1000 Mbps total aggregate speed. Most likely cable is 1000 BASE SX
- 6 Workgroup switches @ 1000 Mbps means that the core switch must carry 6 Gbps of total capacity
- Best – 10G core switch allows for future growth and over-provisioning

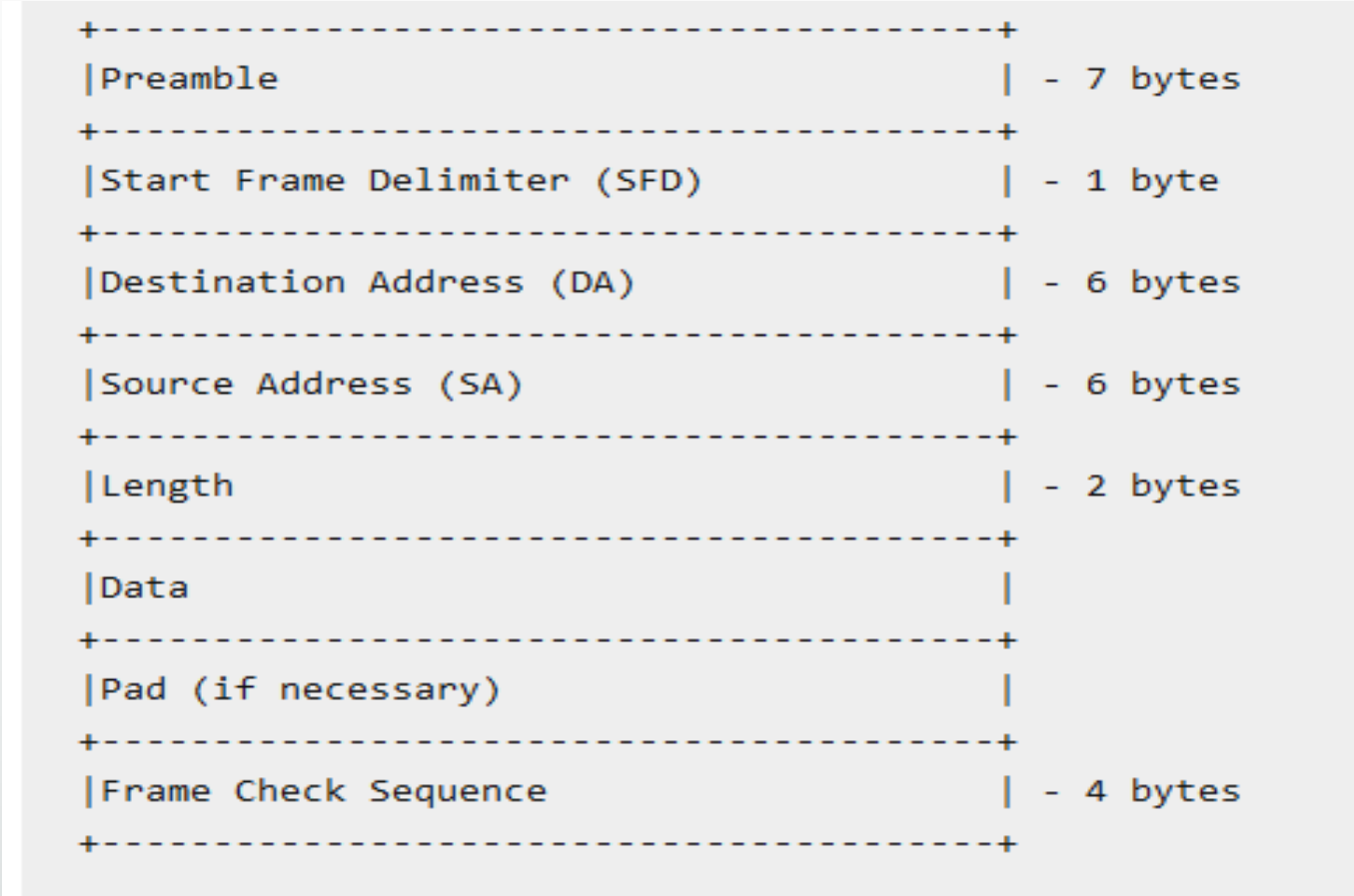


The Evolution of Ethernet Standards to Meet Higher Speeds				
Date	**IEEE Std.**	**Name**	**Data Rate**	**Type of Cabling**
1990	802.3i	10BASE-T	10 Mb/s	Category 3 cabling
1995	802.3u	100BASE-TX	100 Mb/s*	Category 5 cabling
1998	802.3z	1000BASE-SX	1 Gb/s	Multimode fiber
	802.3z	1000BASE-LX/EX		Single mode fiber
1999	802.3ab	1000BASE-T	1 Gb/s*	Category 5e or higher Category
2003	802.3ae	10GBASE-SR	10 Gb/s	Laser-Optimized MMF
	802.3ae	10GBASE-LR/ER		Single mode fiber
2006	802.3an	10GBASE-T	10 Gb/s*	Category 6A cabling
2015	802.3bq	40GBASE-T	40 Gb/s*	Category 8 (Class I & II) Cabling
2010	802.3ba	40GBASE-SR4/LR4	40 Gb/s	Laser-Optimized MMF or SMF
	802.3ba	100GBASE-SR10/LR4/ER4	100 Gb/s	Laser-Optimized MMF or SMF
2015	802.3bm	100GBASE-SR4	100 Gb/s	Laser-Optimized MMF
2016	SG	Under development	400 Gb/s	Laser-Optimized MMF or SMF
Note: *with auto negotiation				

The 40 Gbe is designed for use within the organization between servers and the Ethernet switch, while 100 GbE is geared to long-distance switch-to-switch transmission.

Frame Format

- Preamble – synchronization os and 1s
- SFD – beginning of frame
- Destination MAC address
- Source MAC address
- Length of Header
- Data – Max 1500 bytes (MTU)
- Pad – padding used on frames less than 64 bytes (needed for Collision Detection)
- FCS – 4 bytes
- Total size 1518 bytes

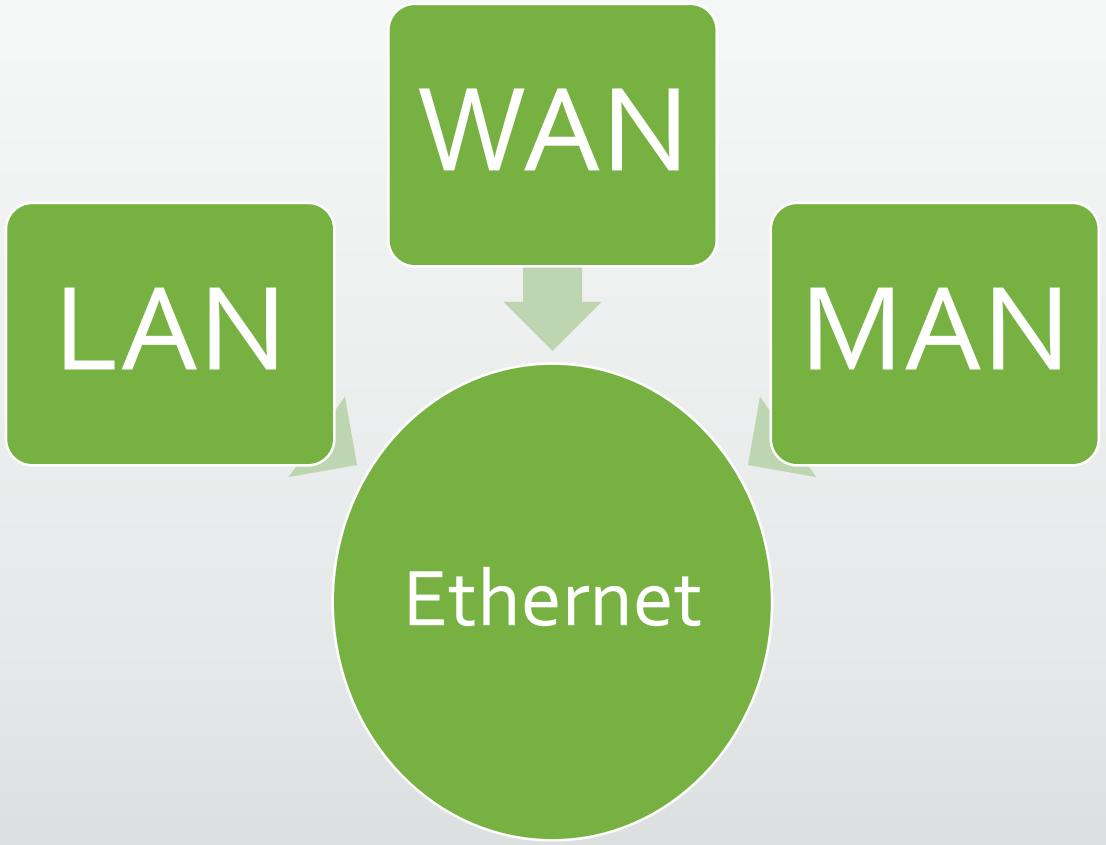


Types Ethernet Networks

And 3 Types of Switches Used

Types of Ethernet Networks

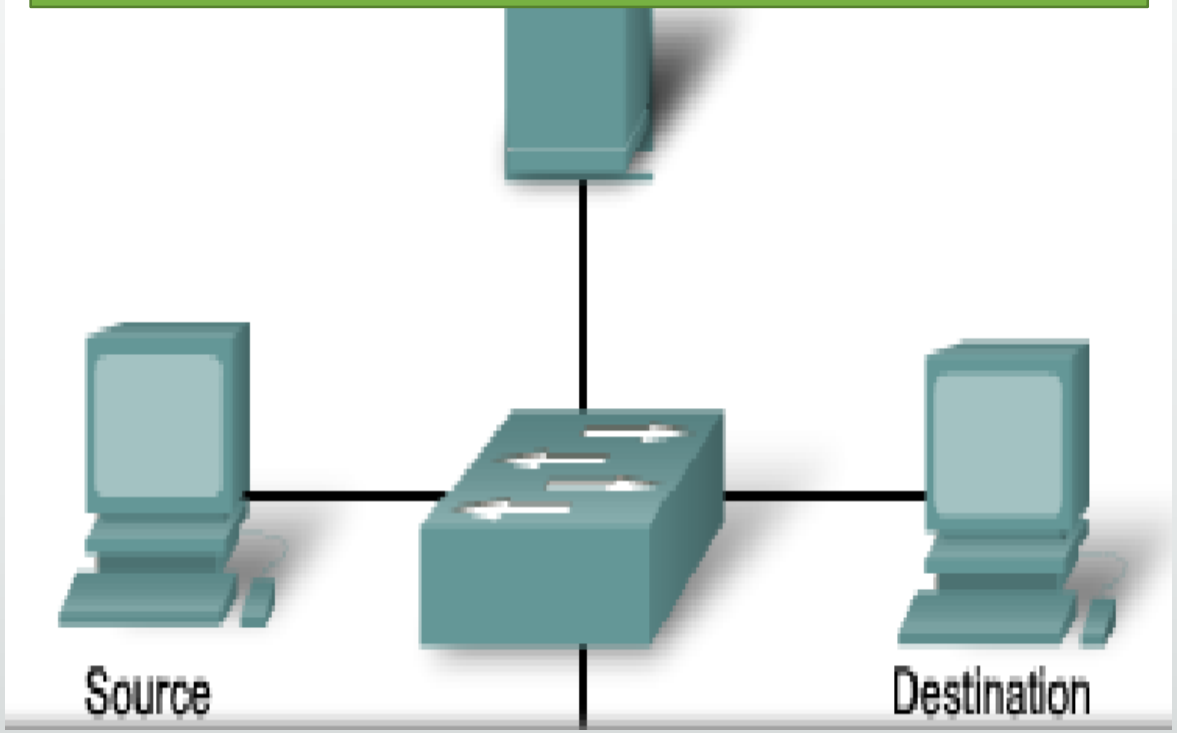
- Gigabit Ethernet: IEEE 802.3z
- 10 Gigabit Ethernet: IEEE 802.3ae
- Power over Ethernet (PoE): IEEE 802.3-2012
- Metro Ethernet



Types of Switches – 3 Types

- **Store and Forward**
  - **Receives the entire frame and stores in memory**
  - **Checks errors by computing the CRC and checking frame length**
  - **If OK then looks at the destination address (if not deletes frame)**
  - **Forwards the frame out the destination port**

Advantage – Uses bandwidth efficiently
Disadvantage – increases latency

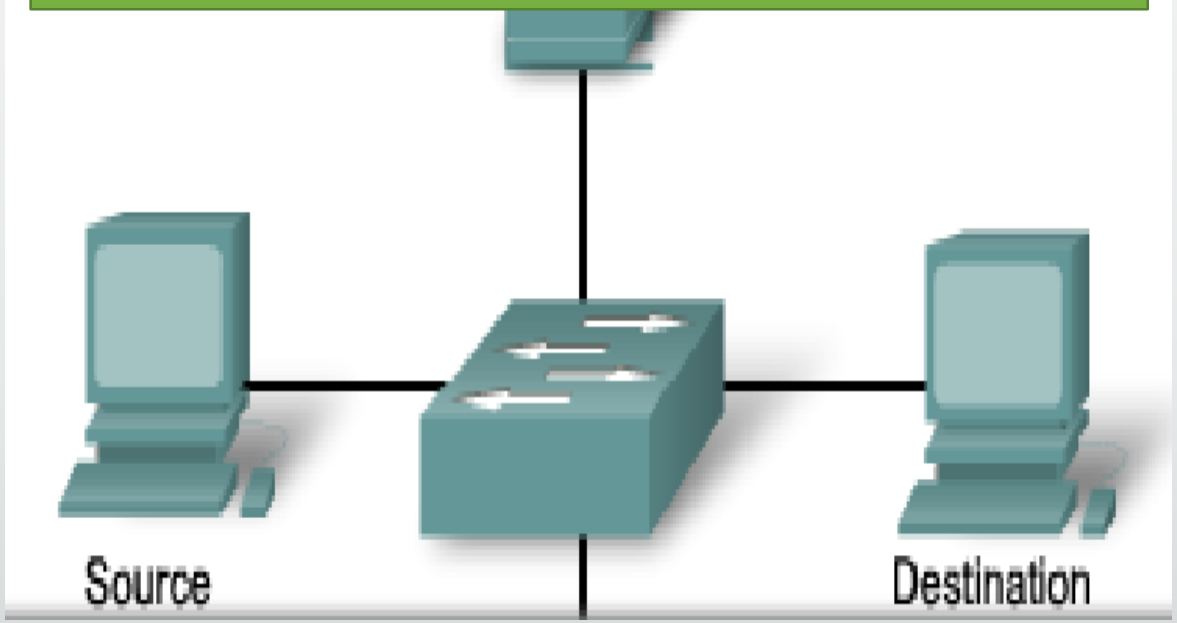


Types of Switches – 3 Types

- **Cut Through**
  - **Starts to forward the frame as soon as it receives the destination address**
  - **Does no error checking**
  - **Advantage – very fast used on high speed backbones**
  - **Disadvantage – may waste bandwidth forwarding frames with errors**

- **fragment-free switching,**
  - lies between the extremes of cut-through switching and store and forward switching.
  - With fragment-free switching,the first 64 bytes of the frame are read and stored. The switch examines the first 64 bytes (which contain all the header information for the frame)
  - if all the header data appears correct, the switch presumes that the rest of the frame is error free and begins transmitting

Note: For a cut through switch to work the speed coming into the switch MUST be the same as the speed leaving the switch

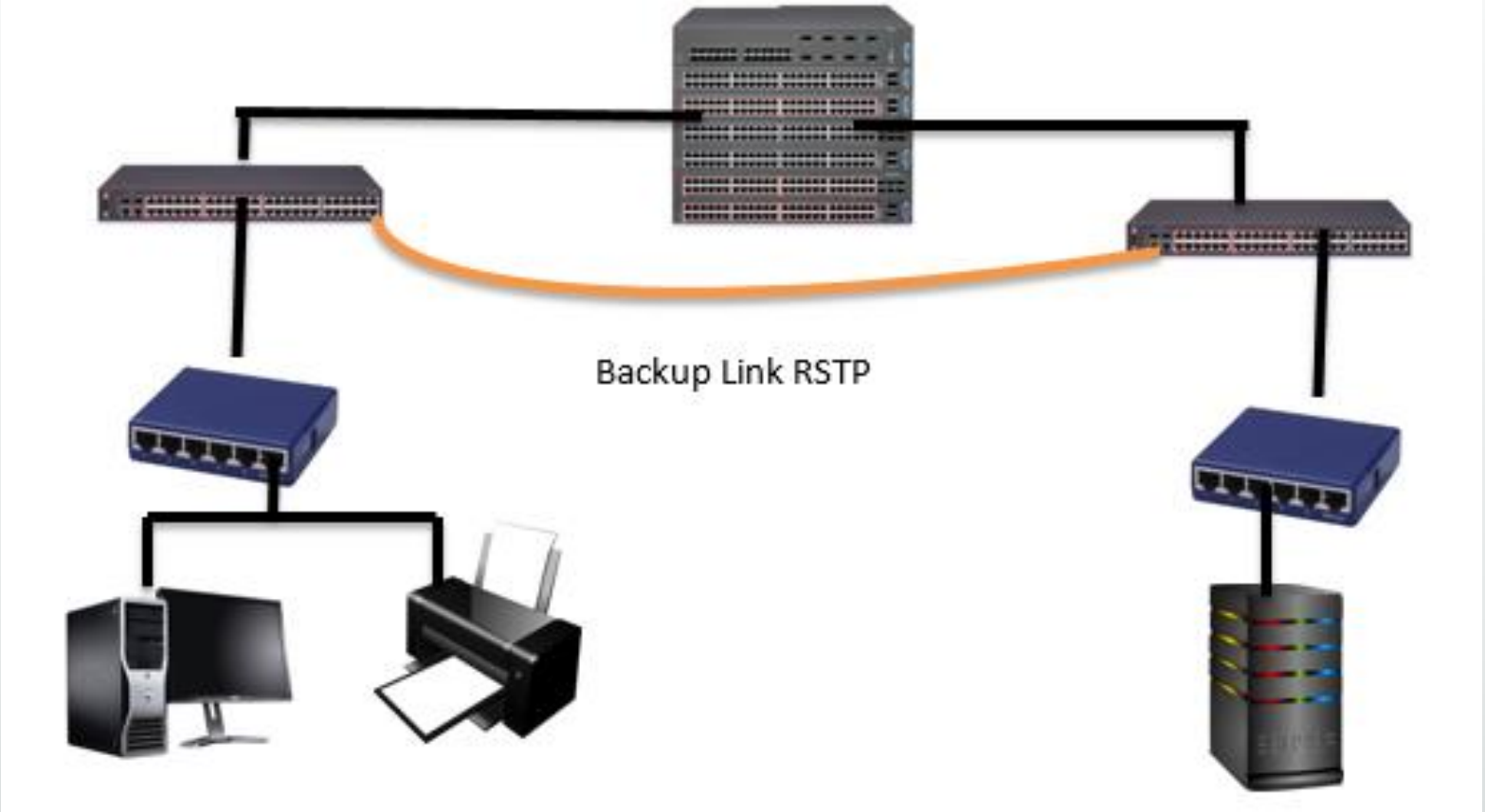


Ethernet Security

RSTP and IEEE 802.1x

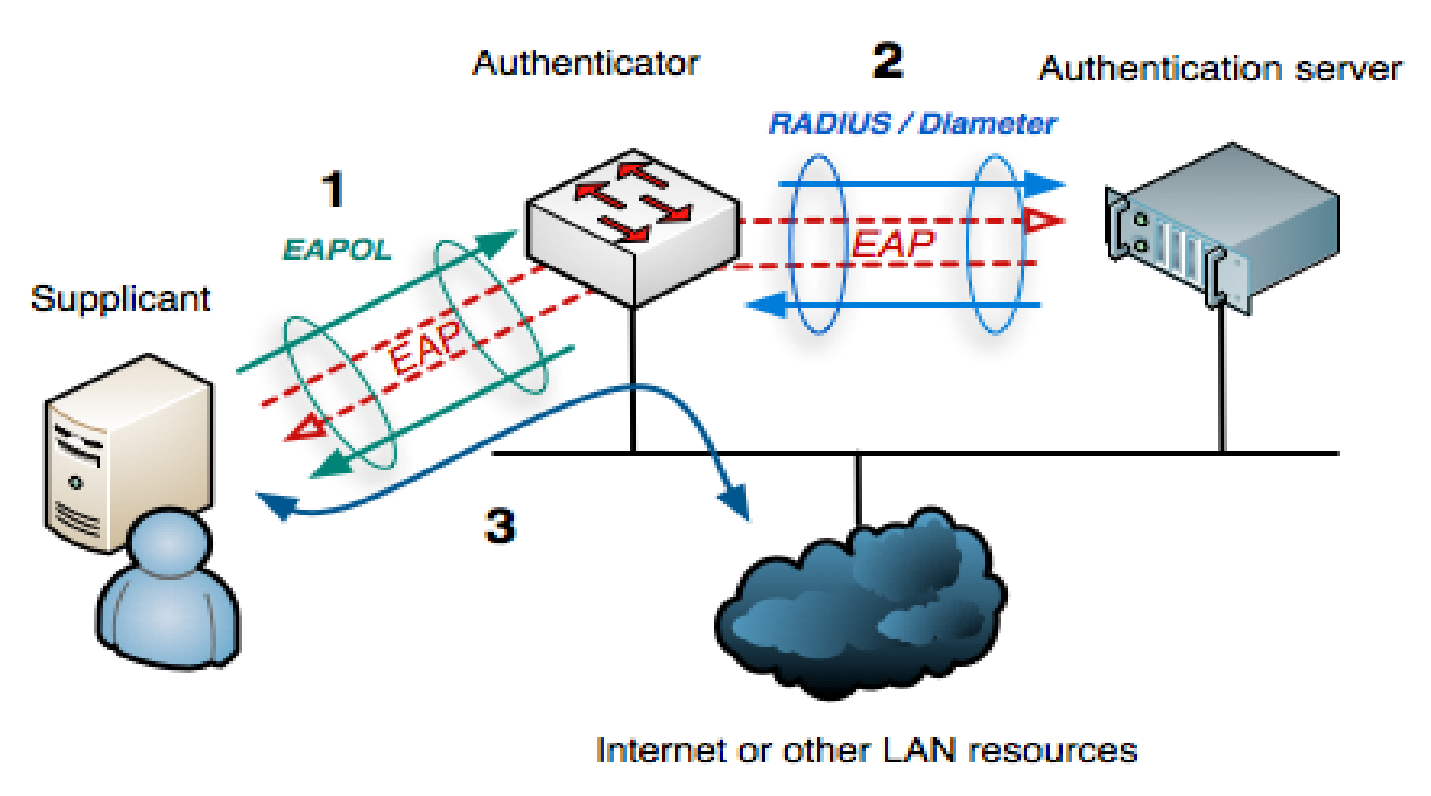
Rapid Spanning Tree Protocol (RSTP)

- A hierarchical network cannot have loops
- Network prone to single points of failure
- RSTP protocol to allow backup links.
- Core switch polls the Main switch to see if alive.
  - If true – ignores backup link
  - If false – uses backup link



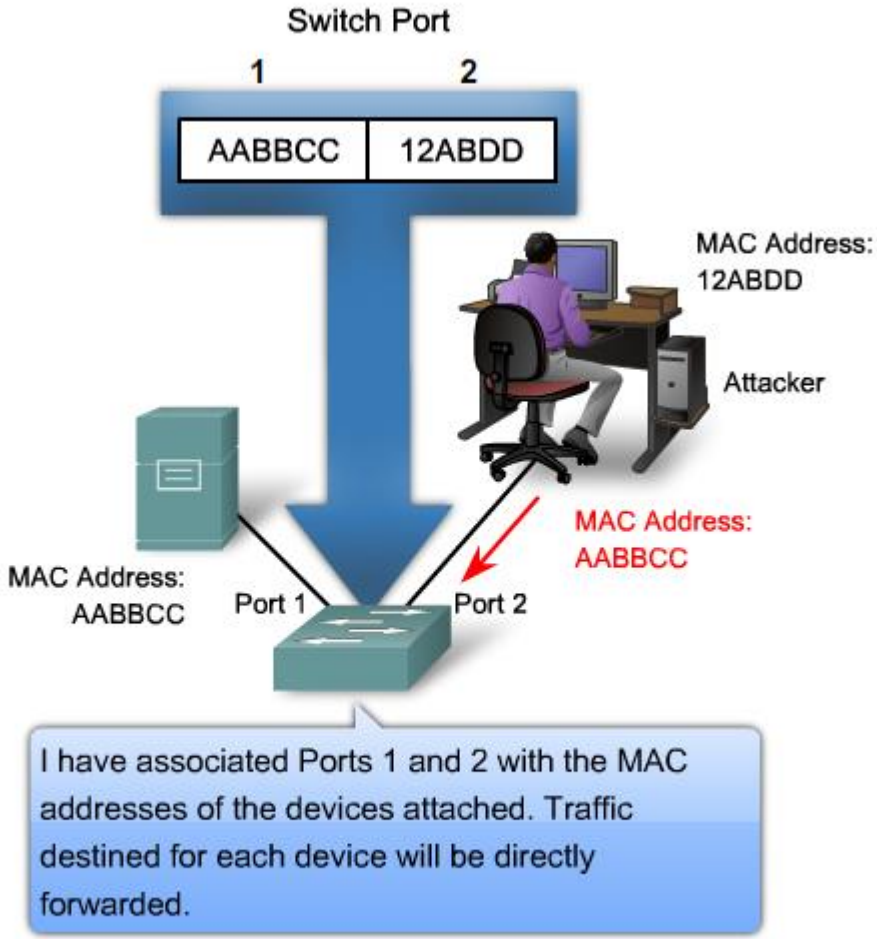
802.1x Port Security

- Designed to protect data ports
- Divides the port into 2 virtual ports
  - Unauthorized port – uses EAP to allow only authentication traffic to RADIUS server
  - RADIUS server sends message to switch if user authorized or not,
  - Authorized user – port changes to authorized mode – full access



MAC Spoofing

- On single switched network devices communicate by MAC address
  - MAC address stored in ARP Cache and must be updated regularly by client
  - Can not prevent someone from client side changing the MAC address
- Spoofing MAC address bases for evil twin and MITM attack
- Switch have built in intelligence to prevent changing port address
  - or recognizing if there are duplicate MAC addresses on the network and alerting administrator



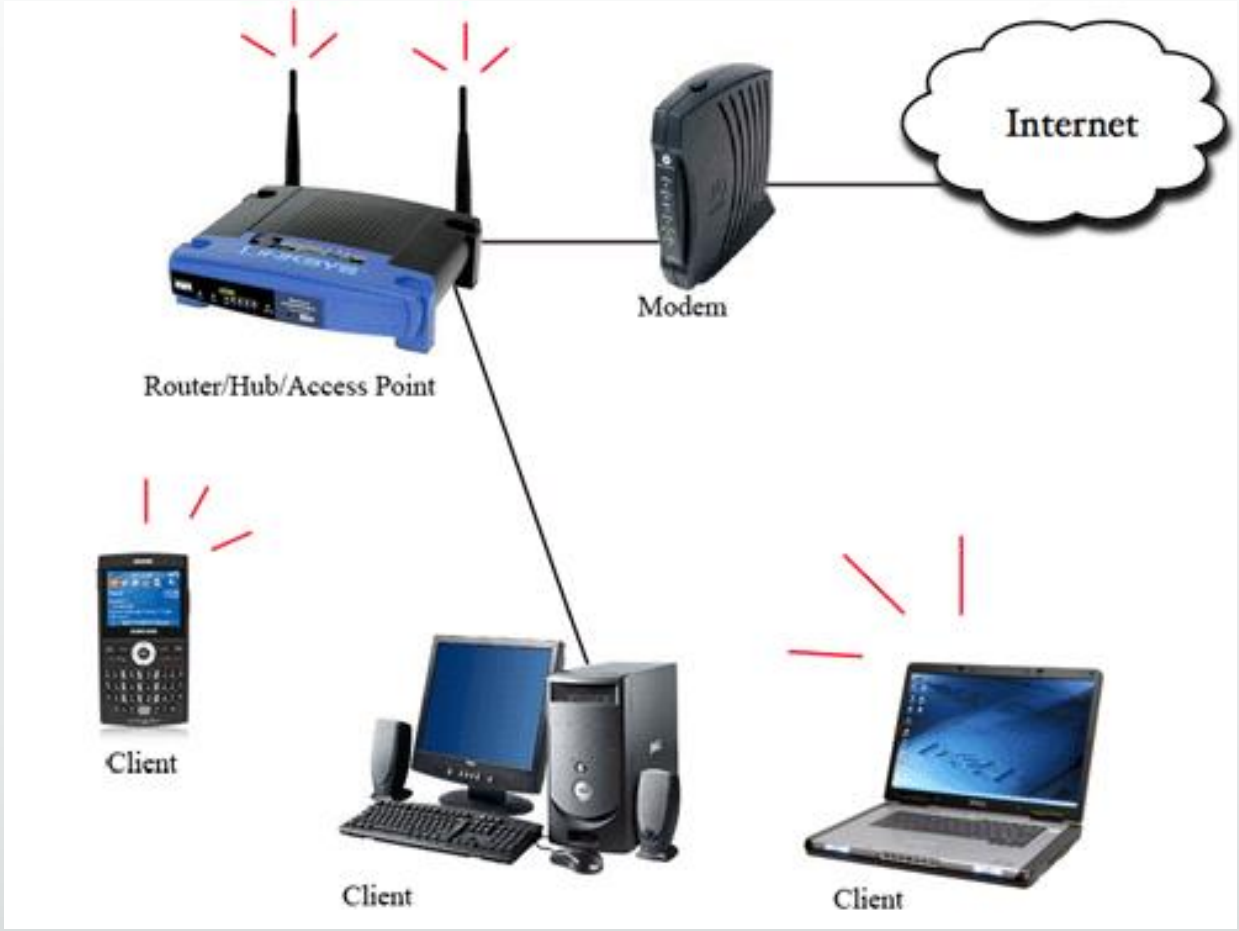
Wireless Ethernet

WLAN – 802.11i

WLANs

- Use radio frequency to transmit and receive data.
- First WLAN specification called WEP (Wired Equivalent Privacy)
- Had security problems and quickly replaced by WPA (Wi-Fi Protected Access)
- WPA backward compatible with WEP
- New standard WPA2 not compatible requires firmware upgrade
- WPA2 works in 2 modes
  - Pre-shared key mode (Personal Mode)
  - Enterprise mode (Infra-structure Mode)

- WPA2 – Enterprise mode works with 802.1x to provide secure authentication and transmi



WLANs

- Problem with WPA2
  - The Wi-Fi networks found in public locations, such as airports, hotels and coffee shops, are open and allow traffic to be sent over them that isn't routinely encrypted
- Solution WPA3
  - WPA3 fixes this by automatically encrypting all traffic between a device and the Wi-Fi access point by using a unique key, without the need for any prior setup by the user (Opportunistic Wireless Encryption (OWE) – RFC 8110)
  - Does not provide the same level of security and assurance as authenticated encryption, but better than having no encryption
- WPA3 works in 2 modes like WPA2 but with increased security
  - Personal Mode: Pre-shared key mode with Simultaneous Authentication of Equals (SAE) algorithm
    - provides more protection to devices that do not have a strong password by preventing it to brute-force and dictionary password attacks
  - Enterprise Mode:offers an 192-bit minimum cryptographic strength with the combination protocols.
    - a set of four cryptographic tools replace Wi-Fi 802.1x for WPA2-Enterprise, and the tools are combined together to provide better protection against attacks, such as password cracking on Wi-Fi networks.
    - Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
    - Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
    - Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
    - Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

Wireless Protocols

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

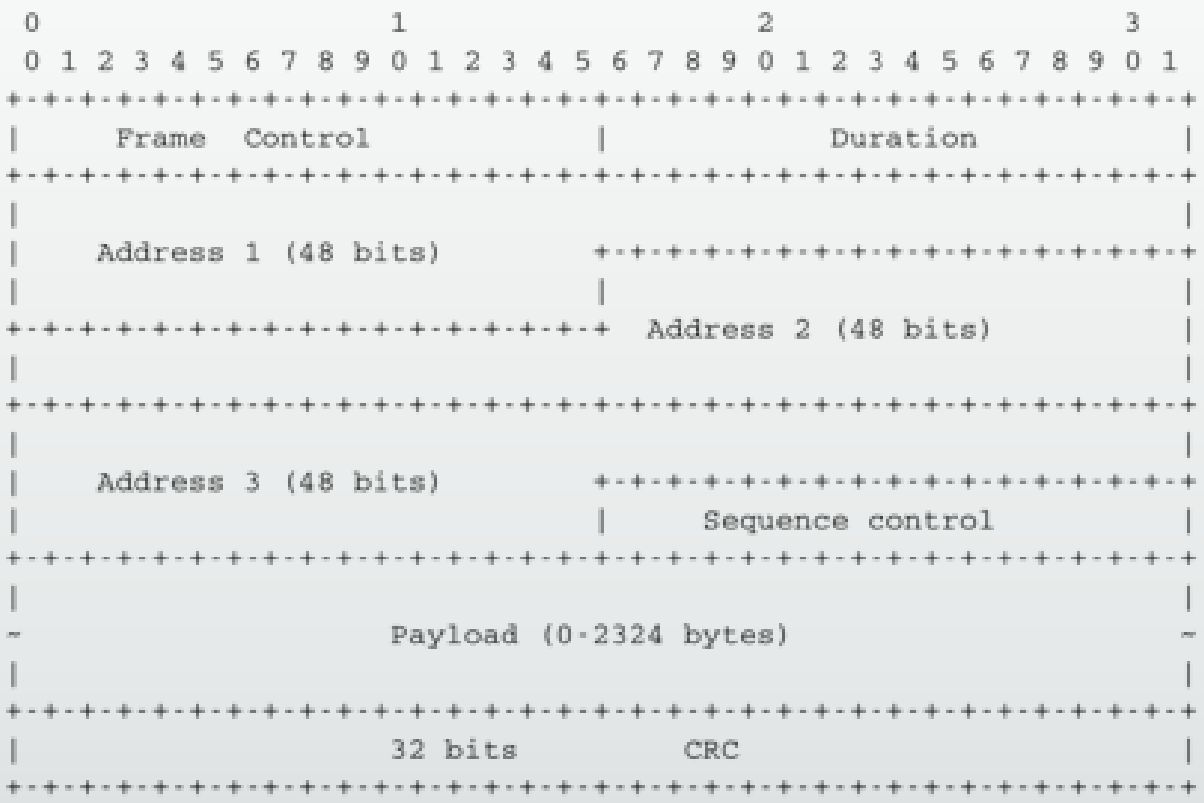
Wireless Errors

- Greater attenuation than copper or fiber optic cable
- "Absorptive attenuation" of plants
- Higher frequencies do not bend around objects can get shadow or dead zones
- Multipath interference main wireless problem requiring retransmission
  - Original signal bounces off ceiling
  - Creates a reflected signal
  - Both signals out of phase with each other and arrive out of time.

Wireless Frame Format

- Frame Control contains flags for type of data frame, acknowledgement, etc.
- Duration 16 bit field reserver transmission channel for the user
- Address 48 bits:
  - MAC of sender
  - MAC of AP
  - MAC of next WiFi device

- Sequence 12 bits number that is incremented for each data frame
- Payload – message
- CRC – 12 bits – error detection



Wireless Security

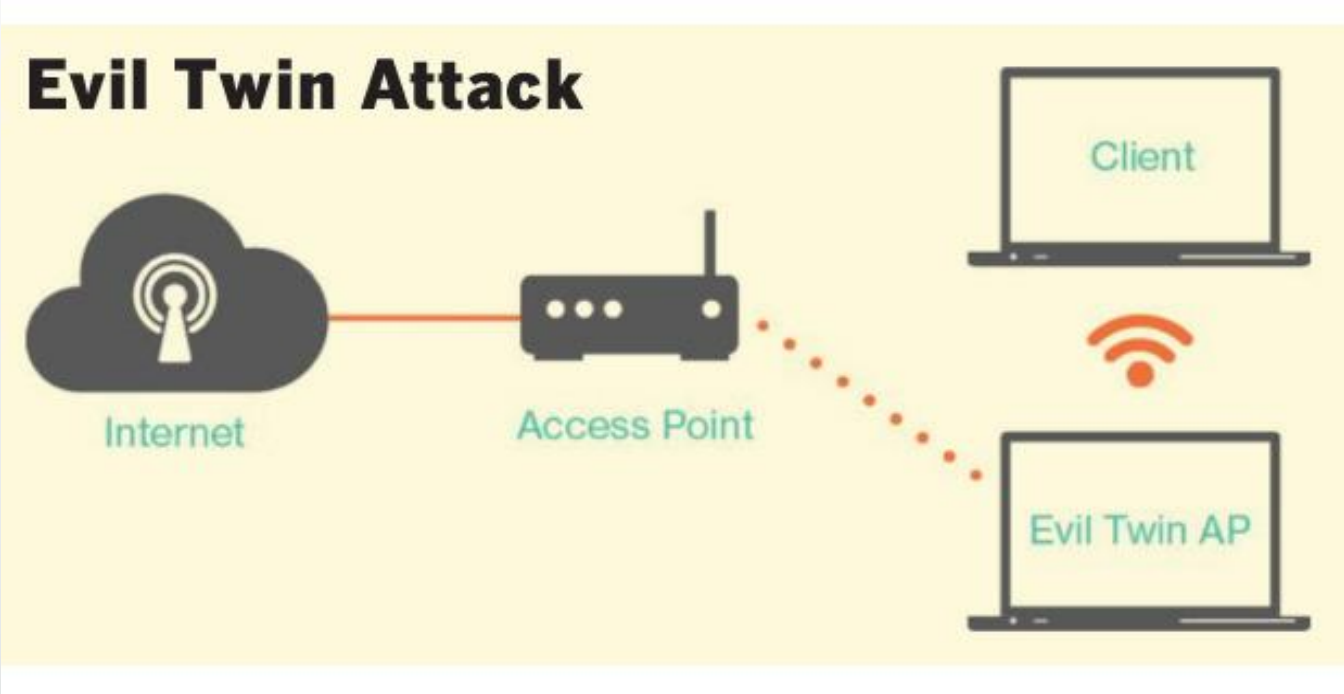
Rouge AP Evil Twin

Rouge Access Point

- Unauthorized access point installed with network SSID
- Created by intruder to steal data or by employee who wants unfettered access.
- Clients connected to Rouge AP must be considered rouge clients because AP bypasses security protocols set by management

Evil Twin

- AP operating at high power with network SSID
- Wireless devices connect to strongest signal – client thinks imposter is the real AP
- Imposter now in the middle (Man in the Middle-MITM) attack.
- Intruder has full access to both sides of the communication and can alter the communication without the other side knowing it
- Used to steal personal information or corporate intellectual property

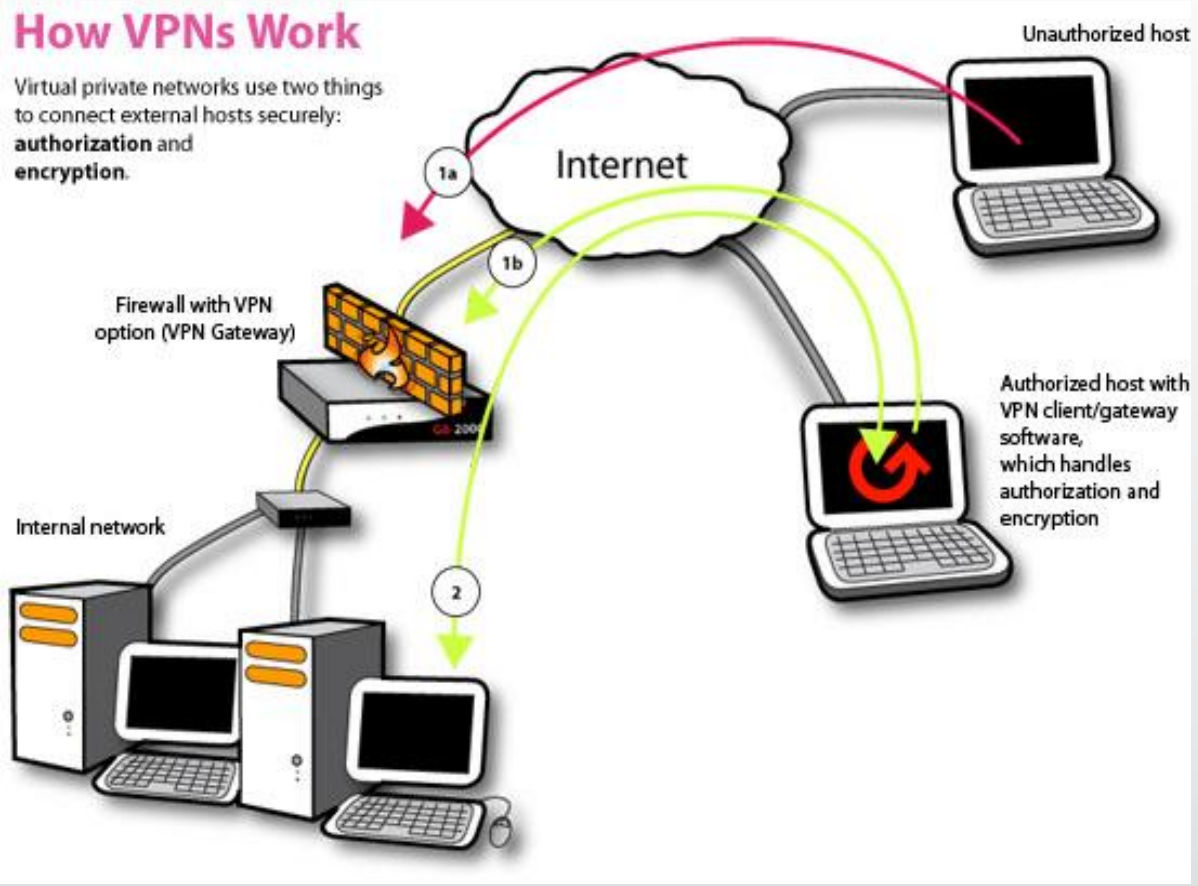


Virtual Private Network

VPN

VPN

- Costly but allows the use of the Internet as extension of private network
- VPN server encrypts outbound traffic, then encapsulates it in an unencrypted IPv4 packet
- Destination VPN, removes IPv4 packet from inbound traffic
- Decryptes the message and forwards to destination host



Summary

1. Wired Ethernet IEEE 802.3 is the most popular LAN architecture today. Its excellent cost to performance ratio has increased the use of Ethernet as a MAN and WAN technology. Switched Ethernet is created using a combination of workgroup and core switches.

2. The network bandwidth must be able to accommodate all of the downstream devices. The most popular cable to connect devices to workgroup switches is 100BASE TX. The workgroup switches are connected to core switches using a fiber optic backbone. The most popular cable to connect core switches is 1000BASE SX. High speed core switches will need 10GBase with provides 10 Gbps. The more popular cable is 10GBASE SW

3. The main security concerns of wireless Ethernet is using RSTP to create backup links and 802.1x to control port access

4. Wireless Ethernet is 802.11. The WLAN standard is WPA2 and 802.11i. These protocols work together to provide excellent security for both small and large networks. Wireless networks have special propagation and security concers.

5. Using VPNs is an excellent choice in providing secure access across the Internet. VPN provides both authentication and encryption services for all connected hosts.