Ethernet –Wired and Wireless

Ethernet standards are controlled by the Institute for Electrical and Electronic Engineers (IEEE) and ISO. They are name IEEE 802.3 which is the most common local area network today with speeds of 100 Mbps speeds. Ethernet's popularity continues to grow because of its exceptional performance to cost ratio. It now being used as a MAN technology (Metropolitan Area Network) called Metro Ethernet. The IEEE also had a study group researching making Ethernet a WAN technology, but that group is now on hold.

Wireless Ethernet is controlled by the IEEE 802.11 standard. Many people think that wired and wireless standards are competitors, but they are used in a complimentary fashion to provide cost effective network performance. This lecture will focus only on Ethernet LAN technology: types of networks, the cabling and devices used and the standards that tie the network together.

Wired Ethernet: IEEE 802.3

An Ethernet network is built in a hierarchical manner using Core and Workgroup switches. Core switches are used to connect switches to switches. Workgroup switches join devices to the network such as printers, workstations and servers. This Switched Ethernet diagram below, is effectively upside down; assume this network represents a LAN which occupies a multi-storey building. There would be a workgroup switch on every floor connecting to a central core switch in the basement of the building.

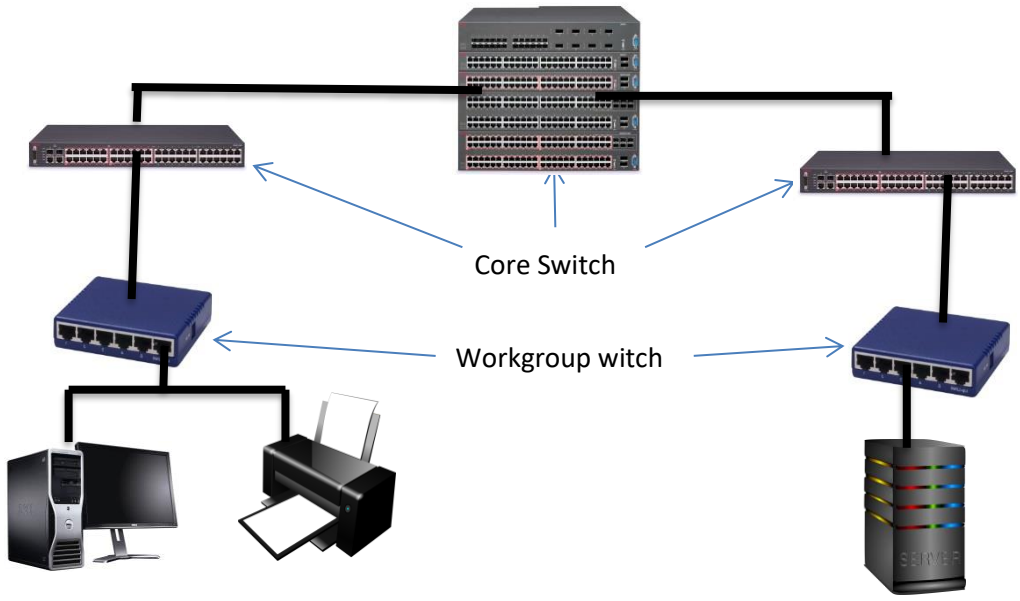


Figure 1: Switched Ethernet

Creating a hierarchical switched network provides the optimal balance between cost and performance. It allows combining less expensive cabling and switches with expensive switches and cabling and using

them only were higher performance is required. On any network, however, there are only a few users who place high loads on the network; these users will be given a dedicated port. Less demanding users, can be grouped into a shared subnet, using wireless Ethernet, and the access point is connected to a port.

A key design principle of a hierarchical network is that the cabling and switches must be able to accommodate the aggregate of the workgroup switches. An excellent analogy for this situation is to look at the 401 highway between Highway 400 and Don Valley Pkwy at 4:00 a.m. there is usually very little traffic, and you can reach your destination quickly and unimpeded. However, at 4:00 p.m.,during rush hour, there are more cars than the road can handle resulting in congestion. Traffic slows to a crawl, and a trip that would take ten minutes at 4:00 a.m. now takes over an hour to complete. To solve the congestion problem, we could built a dedicated road from each person's driveway directly to his or her destination. Then the rush hour congestion problem would go away. A switch' s port provides a "dedicated road" between individual users (or small groups of users) and their destination (usually a file or web server). Workgroup switches run at 100 Mbps interconnected through a high-speed fiber-optic backbone. Each frame has a destination address; the switch examines this field and forwards it **only** to the port attached to the destination device. The most common cabling scheme today for wired Ethernet is 100BASE-TX, which is unshielded twisted pair, transmitting a 100 Mbps for up to 100 meters (IEEE 802.3u); it is used to connect devices such as workstations and printers to the network workgroup switches. This cabling is inexpensive, durable and combined with the RJ-45 connector, expansion of the network is easy, provided the workgroup switch has an available port.

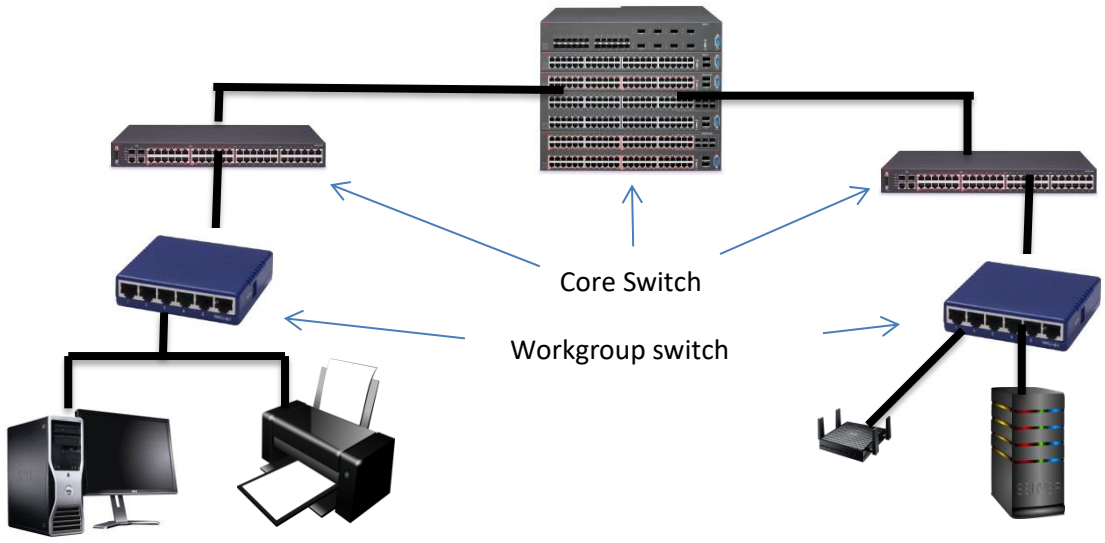


Figure 2: Switched Ethernet with Shared Access Point

Building a dedicated highway for each person is impracticable in real life. It is also impracticable in a network because most users do not need a dedicated port. To allocate a dedicated port would be an inefficient use of resources, when performance does not require it. Most users want to send information to print or browse the Internet. A group of these less demanding users can be placed in a

wireless Ethernet subnet with the access point connected to a wired port. This results in shared bandwidth with a group users whose combined throughput is 100 Mbps, the maximum for the port. [1]

As you move up from the workgroup switches, the core switches must be designed to accommodate the aggregate bandwidth of all downstream devices. For example, if you have 10 users connected to a workgroup switch and each user transmits at 100 Mbps, then the cabling from the workgroup switch to the core switch must be handle 10 X 100 Mbps, or 1000BASE-SX. Six core switches sending data at 1 Gbps requires a centre core switch of 10GBASE transmitting at 10 Gbps (Ethernet speeds increase by a factor of 10). This allows for "over-provision" where networks are designed to handle loads surpassing the maximum for short periods of time and future growth.

Multi-port core 10GBASE switches are very expensive. The hierarchical design properly balances demand with performance to limit the cost of expensive cabling and switches to areas where performance justifies the cost. The most common backbone today is 1000BASE-SX which is a fiber optic cable and can transmit up to a 1Gbps up to 550 meters. Fiber-optic cable is more expensive, but it is invaluable in situations where electronic emissions and environmental hazards are a concern. It is often used in inter-building applications to insulate networking equipment from electrical damage caused by lightning or electromagnetic interference, such as on a factory floor. The Ethernet standard allows for fiber-optic cable segments up to two kilometers long, making fiber-optic Ethernet perfect for connecting nodes and buildings that are otherwise not reachable with copper media.

Types of Ethernet LAN Technology

Gigabit Ethernet: IEEE 802.3z

Gigabit Ethernet was developed to meet the needs of multimedia applications and Voice over IP (VoIP) where real time transmission is required. Commonly called GigE, the latter runs over copper or fiber-optic at speeds 10 times faster than 100Base-T . GigE is currently used for Ethernet backbones to interconnect high performance switches and servers. From the data link layer, GigE is identical to that of Ethernet, except that GigE is optimized for full duplex operation.

[1] In earlier days of networking devices where joined to the network with hubs, which broadcast all traffic to devices. A special protocol CSMA/CD, Carrier Sense Multiple Access with Collision Detection was used at the Data Link layer to control the shared medium and avoid packet collisions. Today, however, Ethernet is exclusively a switched network. With a direct cable connecting each device. CSMA/CD is not needed because the cable is no longer shared. Ethernet designed as a LAN technology is being developed as a MAN and WAN technology because of its excellent balance between cost, speed and reliability.

10 Gigabit Ethernet: IEEE 802.3ae

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards with a transmission rate 10 X GigE. Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. Presently, it is used as a high-speed backbone for high volume transmissions.

Power over Ethernet (PoE): IEEE 802.3-2012

PoE provides both power and data transmission over a single cable. This solution is ideal for surveillance equipment, access points and IP telephones where running power would be difficult or expensive. PoE supports fast data rates up to 100 meters in cable length while delivering 25.5 Watts of power. This is enough power to run cameras, IP telephones and access points, but not workstations.

LAN Technology Specifications

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				

Name	**IEEE Standard**	**Data Rate**	**Media Type**	**Maximum Distance**
Ethernet	802.3	10 Mbps	10Base-T	100 meters

Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Metro Ethernet

Metro Ethernet is a Metropolitan area network (MAN) technology based on Ethernet standards. It is commonly used to connect subscribers to a larger service network or the Internet. Larger businesses can also use metropolitan-area Ethernet to connect their own offices to each other and greatly extend the concept of a LAN.

An Ethernet interface is much cheaper than any current MAN technology such as SONET (Synchronous Optical Network) or FDDI (Fiber Distributed Digital Interface) while providing similar bandwidth and speeds. Another distinct advantage of an Ethernet-based access network is that it can also be easily connected to the customer's network and is well known to network administrators; this means that special training is not necessary and LAN personnel can troubleshoot network problems. Often metro Ethernet is combined with a IP/MPLS backbone which is used to connect to the service provider's switches and routers; these MPLS-based deployments are costly, but highly reliable, very scalable and are typically used by large service providers, such as TELCOs, who service a large number of businesses.

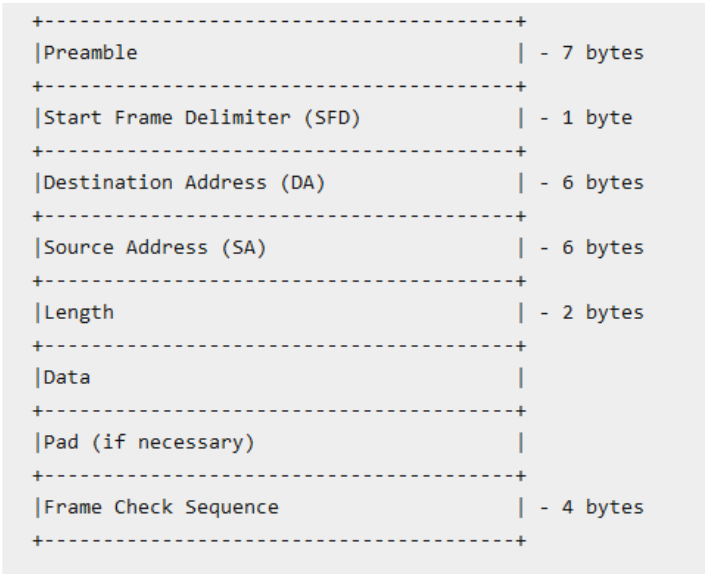
Types of Switches

There are two basic types of switches used on an Ethernet network: store and forward and cut through. A store and forward switch stores each incoming frame and checks for errors. When a frame arrives, the switch stores the entire frame in memory. It then checks the CRC and the frame length, if both are valid, the switch then looks at the destination MAC address and forwards the frame to the destination port. If the frame has errors, the switch deletes it. With a store and forward switch bandwidth is not wasted on invalid or damaged frames. The disadvantage is that it increases the latency of the switch slightly. Store and forward switches are commonly workgroup switches. A Cut Through switch, on the other hand, does not error check and begins forwarding the frame immediately upon receiving the destination Address. This results in lower latency, but can propagate errors from one subnetwork to another, wasting bandwidth on invalid or damaged frames. For a Cut Through switch to work, the speed of the transmission coming into the switch must be the same speed leaving the switch. If you have a

workgroup switch connected to a high-speed backbone, as is usually the case, then the switch must operate in store and forward mode. There is also a hybrid switch combining the two types. This switch monitors the frame error rate, and if it is below a level set by the administrator, the switch will function in Cut Through mode, otherwise it uses Store and Forward mode.

Ethernet 802.3 Frame Format

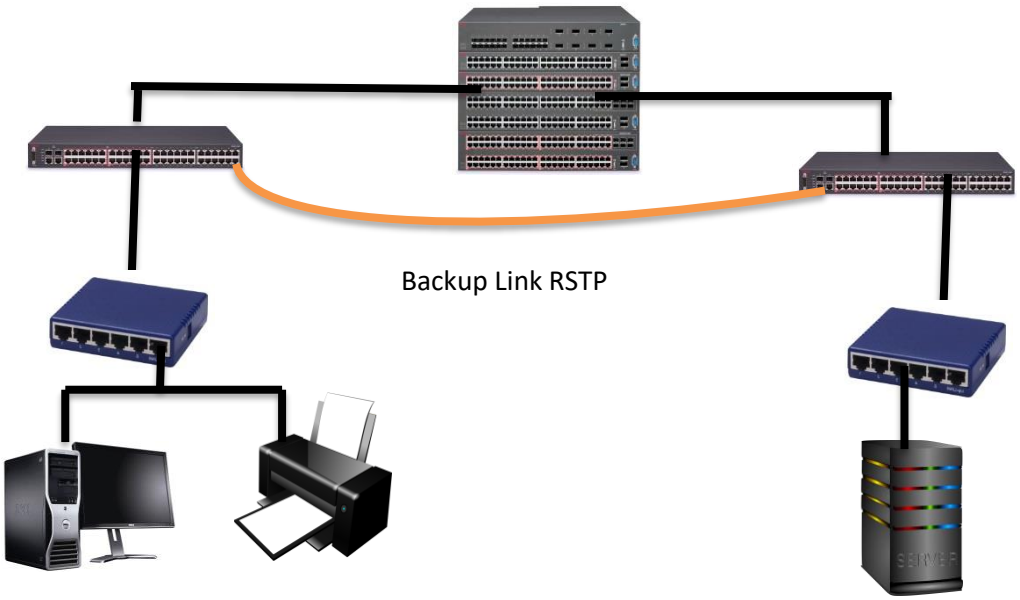
The preamble is 7 byes of "0s" and "1s" where the data link layers synchronize their clocks. The frame begins with the start frame delimiter with indicates the beginning of a transmission. The destination and source address are the layer 2, MAC addresses for communication to occur across a link. The length field is used by router's data link layer when headers have to be removed. The router needs this information to calculate where the payload, contained in the data section, begins. Padding with "0s" is used to prevent very small frames; the smallest frame allowed on Ethernet networks is 64 bytes. The reason for the minimum frame size is for collision detection. If a device sent a very short frame, it may think it had sent it successfully because it did not have heard a collision, before it sent the next frame. Keeping a minimum frame size ensures that each device will hear a collision if they transmit at the same time.



The Maximum Transmission Unit (MTU) size specifies the maximum payload that can be encapsulated in the data portion of the frame which is 1500 bytes. With a header length of 18 bytes, the maximum frame size of a standard Ethernet frame is 1518 bytes. This includes the Ethernet header (14 bytes), the payload (IP packet, usually 1500 bytes), and the Frame Check Sequence (FCS) field (4 bytes). However, GigE allows a very large default size of 9000 bytes called a "jumbo" frame. These larger frames reduce the number of frames created by the data link layer which greatly reduces the processing power and improves network performance.

Ethernet Security

The creation of a hierarchical switched network is best for combining performance with cost. It also ensures a single path between any two devices which provides a single lookup table for each switch – providing fast performance. However, a single path between any two devices makes Ethernet vulnerable to single points of failure, in which the failure of a single component (switch or backbone) can cause network failure. For example, in the diagram below if the central core switch stops functioning, the network goes down. Or, if one of the core switches goes down half the network cannot communicate with the other half.



To avoid single point failures, the IEEE 802.1 Working Group on Ethernet have provided a way to create backup links using the Rapid Spanning Tree Protocol (RSTP). On a hierarchical network, there can only be one path to each device, loops are prohibited. To avoid single points of failure, the RSTP protocol can be used to create backup links. The core switch on the left, before it forwards a packet, is constantly polling if the central core switch is alive. If the central core switch is alive and working the backup RSTP link is NOT used. On the other hand, if the cores switch determines that the central core switch is down, then the RSTP backup link is used to send the frame. For simplicity, the above diagram only shows one backup link. An Ethernet administrator would create backup links between each workgroup and core switch to provide multiple pathways to different parts of the network.

802.1x Port Security

A major security concern with switched Ethernet is the unauthorized use of a data port. Anybody can walk into a conference room, and plug into an empty data jack and get access to all internal network resources using DHCP. The 802.1x specification is designed to prevent unauthorized access to a data port.

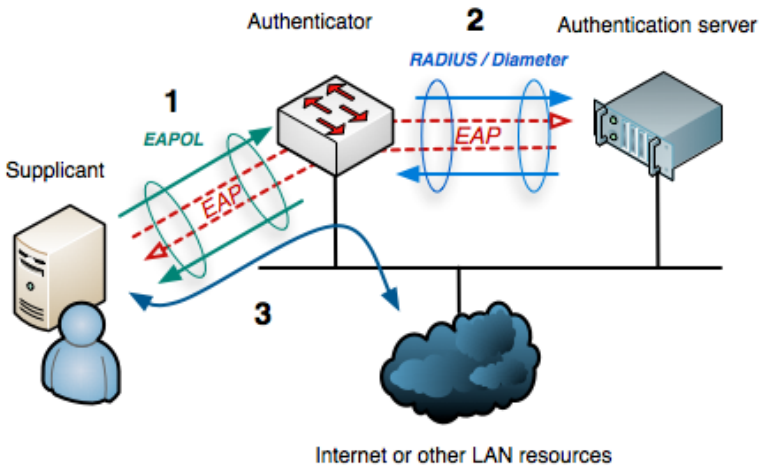


Figure 4: Ethernet IEEE 801x Port Security

The 802.1x security protocol uses the Extensible Authentication Protocol (EAP) combined with a RADIUS (Remote Access Dial In User Service) server which stores user accounts and passwords. It divides each data port into 2 virtual switch ports; one for unauthenticated traffic and one for authenticated traffic. Until the user is authenticated all traffic passes through the unauthenticated port, and the only traffic allowed is EAP authentication traffic; all other traffic is dropped. In this sense the authenticator, the switch, acts like a security guard protecting the switch port from unauthorized use.

To initiate authentication the authenticator periodically transmits an EAP-Request Identity frame to a special data link address. The supplicant, the client software, listens on this address, and when it receives an EAP-Request Identity frame, it responds with an EAP-Response Identity frame containing an identifier for the supplicant such as username and password. The supplicant can also initiate authentication by sending an EAPOL-Start frame (EAP over LAN) to the authenticator, which immediately sends an EAP-Request Identity frame.

The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the RADIUS server for authentication. An analogy to this is providing a valid driver's license when entering a nightclub for proof of age. The RADIUS server then checks for matching credentials. If a match is found the server sends and EAP Success message to the switch. If no credentials are found, then an EAP Failure message is sent to the switch. Upon receiving an EAP Success message the switch opens the authorized port and the user has full access to the network. An EAP Failure message keeps the switch in authentication mode.

Another security concern with switched Ethernet is the ability of a malicious person to "spoof" a MAC address. When two devices are communicating, such as when you PING someone, the devices exchange MAC addresses and store this information is memory called the ARP Cache. On a single network the MAC address is used not the IP address to forward frames and there is no way to prevent MAC address spoofing on the client, since the ARP cache must be regularly updated. Thus, it is possible for someone to change the MAC address of a device and replace it with his/her device's MAC address. This is the essence of a very dangerous attack called the Man in the Middle Attack (MITM). If the attacker can exchange MAC addresses, prior to the beginning of an encrypted transmission, then the attacker would be able to talk to both parties. Each party talking to each other, not knowing that the attacker is seeing all traffic and can modify the frame and send it to the other party.

Since MAC address spoofing cannot be prevented on the client, it can be prevented or monitored at the switch level. Most enterprise switches have built-in intelligence to alert if someone is trying to spoof a MAC address. The switch will not allow the MAC address of the switch port to be changed with proper administrative authentication, or the switch may take proactive action and the block the switch port alert the administrator that some is tried to change an address, or there is a duplicate MAC address on the network.

Wireless Local Area Networks (WLANs) - 802.11

Wireless LANs, or WLANs, use radio frequency technology to transmit and receive data over the air. This minimizes the need for wired connections within the network area. Wireless connections are the most common method today to access the Internet because of the increased mobility.

The first WLAN specification was called WEP, (Wired Equivalent Privacy) this technology had some security problems and was quickly replaced by WPA (Wi-Fi Protected Access). It is backward compatible with WEP products, and uses the temporal key integrity protocol (TKIP) to ensure that keys have not been tampered with and scrambles the keys used for encrypted transmission during the session. WPA also provides user authentication with the extensible authentication protocol (EAP).

The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. WPA2 was designed by the Wi-Fi Alliance standard organization and is basically the same as the IEEE 802.11i standard, with one exception. The WPA2 standard allows the sharing of keys when the network is formed. For example, when setting up your wireless network, you were probably asked to create a Pre-Shared key which wis used to join the network. This Pre-Shared Key (PSK) mode is ideal for small or temporary networks. The key is only used for initial authentication; after initial authentication, the wireless access point gives each user a new key to access the Internet and randomly changes the key during the session. This prevents attackers, who may be listening to the traffic from cracking the key which was a major problem with WEP.

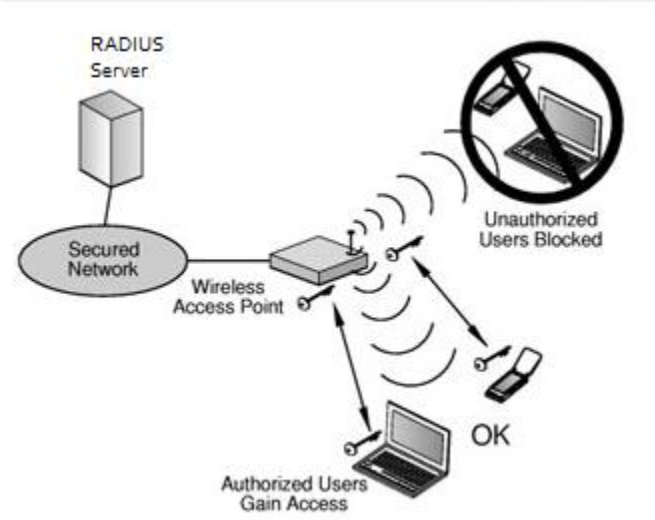


Figure 5: WLAN Security 802.11i

IEEE 802.11i is designed to work with enterprise switches using IEEE 802.1x. This provides better security than the shared key approach but requires an enterprise switch and a RADIUS authentication server.

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, and the traffic can sniffed or hacked during transmission

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), so even if someone sniffed the traffic but difficult decrypt it.

WPA3 works in 2 modes like WPA2 but with increased security

1. Personal Mode: Pre-shared key mode with Simultaneous Authentication of Equals (SAE) algorithm, that provides more protection to devices that do not have a strong password by preventing it to brute-force and dictionary password attacks
2. 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.

a. Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)

b. Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)

c. Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve

d. Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

Wireless Protocol

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

Wireless transmission is good because it allows mobile users to use the network without cables. On the negative side, wireless transmission as security and propagation problems. Setting up a wireless network is difficult and expensive. In addition, to the errors of crosstalk, EMI, jitter and noise, wireless transmissions have special problems. As Signal strength attenuates as it travels down a medium. In copper and fiber optic cable, this attenuation is confined to a fixed path. With radio waves the attenuation is much greater because the signal travels in all directions at the same time. In addition, plants are the "natural enemy" of radio waves and cause "absorptive attenuation" which greatly limits signal travel. Radio waves in the high frequency range cannot reflect around objects, resulting in "shadow or dead" zones. The main problem with wireless communication, however, is "multipath interference". Radio waves can bounce off walls and ceiling, and other objects which creates two signals, the original signal and a reflected signal. Often the two signals arrive at the access point out of phase; one signal may arrive at its highest amplitude, and the reflected signal, with a slight delay, arrives at its lowest amplitude, this causes the signal to be unreadable and will require a retransmission.

Wireless Frame Format: 802.11

The first part of the header is the 16-bit Frame Control field. This field contains flags that indicate the type of data frame, acknowledgement, etc. The Duration is a 16-bit field that is used to reserve the transmission channel to the sender. The Sequence control field contains a 12 bits' sequence number that is incremented for each data frame so the access point can tell the frames that go together or if there is a duplicate frame. Notice that a wireless frame has three 48-bits address fields. This is surprising compared to other protocols in the network and datalink layers whose headers only contain a source and a destination address. The need for a third address in the 802.11 header comes from the infrastructure networks. When a frame is sent from a WiFi device to a server attached to the same LAN as the access point, the first address of the frame is set to the MAC address of the access point, the second address is set to the MAC address of the source WiFi device and the third address is the address of the destination on the LAN. When the server replies, it sends an Ethernet frame whose source address is its MAC address and the destination address is the MAC address of the WiFi device. This frame is captured by the access point that converts the Ethernet header into an 802.11 frame header. The 802.11 frame sent by the access point contains three addresses : the first address is the MAC address of the destination WiFi device, the second address is the MAC address of the access point and the third address the MAC address of the server that sent the frame. Every access point acts like a "bridge" joining to different networks: 802.3 wired Ethernet network to an 802.11 wireless Ethernet network.

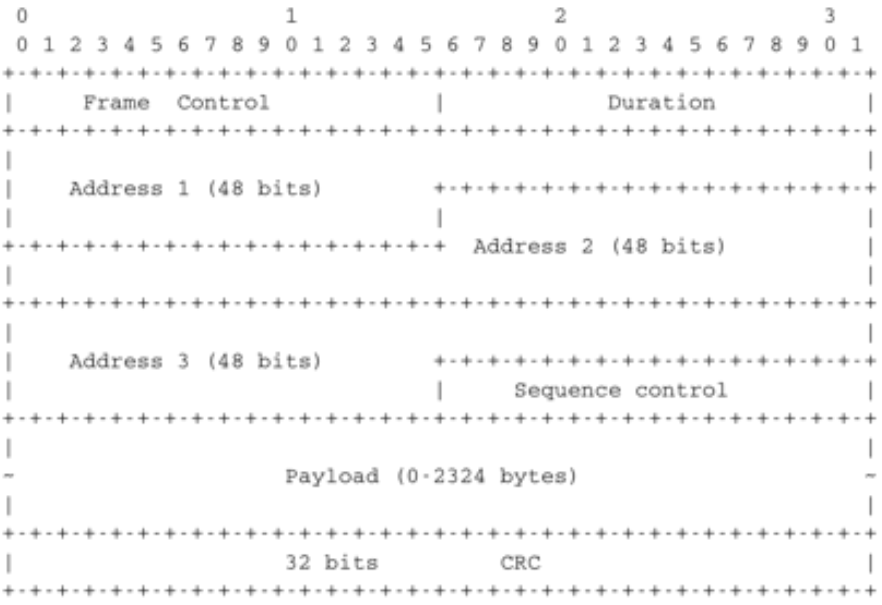


Figure 6: Wireless Frame Format

Wireless Security

Wireless networks by nature are not as secure as wired networks. The two main threats from hackers are route access points and evil twin.

Rogue Access Points

A Rouge AP is a Wi-Fi access point that is installed on a network with the SSID as the network ID, but is not authorized by management. This could be an access point set up by either an employee who wants unfettered access, or by an intruder. Rogue access points can be used to steal data or create a Denial of Service (DoS) attack. Any client who connects to a rogue access point must be considered a rogue client because it is bypassing the authorized security protocols set by management.

Evil Twin

An evil twin is an access point that is operating at high power, usually in a public area, with the same SSID as the real access point. Wireless devices will connect automatically to the strongest signal; thus the wireless client is associated with an imposter network that is operated by a hacker. The evil twin will establish a secure encrypted connection to the wireless client. The hacker now has access to all communication between the client and the access point. In a public area, this technique can be used to steal personal information. In a corporate environment, it is used to steal encrypted keys, trade secrets, or launch DoS attacks**.**

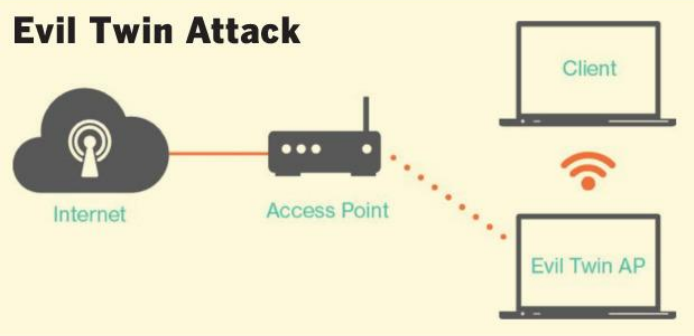


Figure 7: Evil Twin Attack

VPN (virtual Private Network (VPNs)

A VPN network can be used to defeat the evil twin and MITM attacks. A ritual private network (VPN) is a cryptographic connection between the client and a server. VPNs provide end-to-end protection, including authentication. If the PVN authentication is based on a secret shared password, the evil twin would not be able to launch an attack because the shared password is never transmitted. The evil twin would not be able to decrypt the messages passing between the client and server and it would not be able to send authenticated attack messages to create a DoS attack. Using a VPN is a way of using the public Internet as a private network. The network VPN server encrypts outbound network traffic, then wraps the encrypted message in an unencrypted IPv4 packet so it can be routed. If a hacker captures the packet he/she will be unable to read it. The destination VPN server unwraps the message to forward onto the destination host.

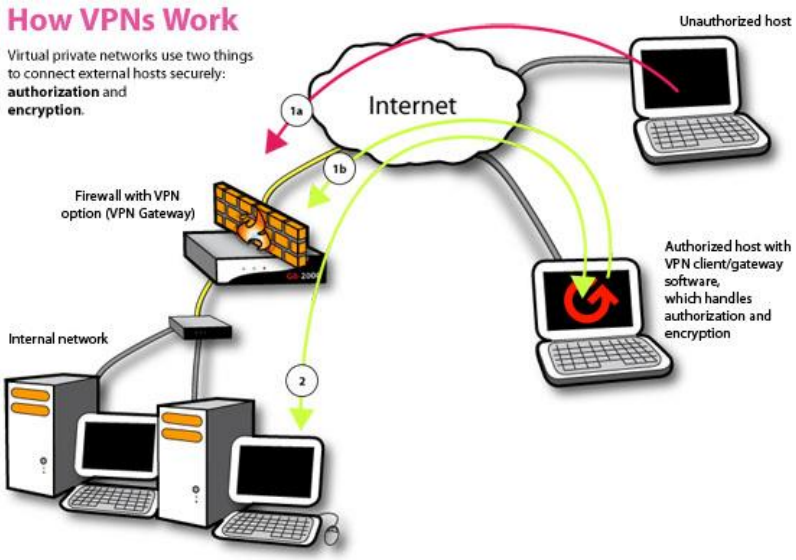


Figure 8: How a VPN Protects a Network