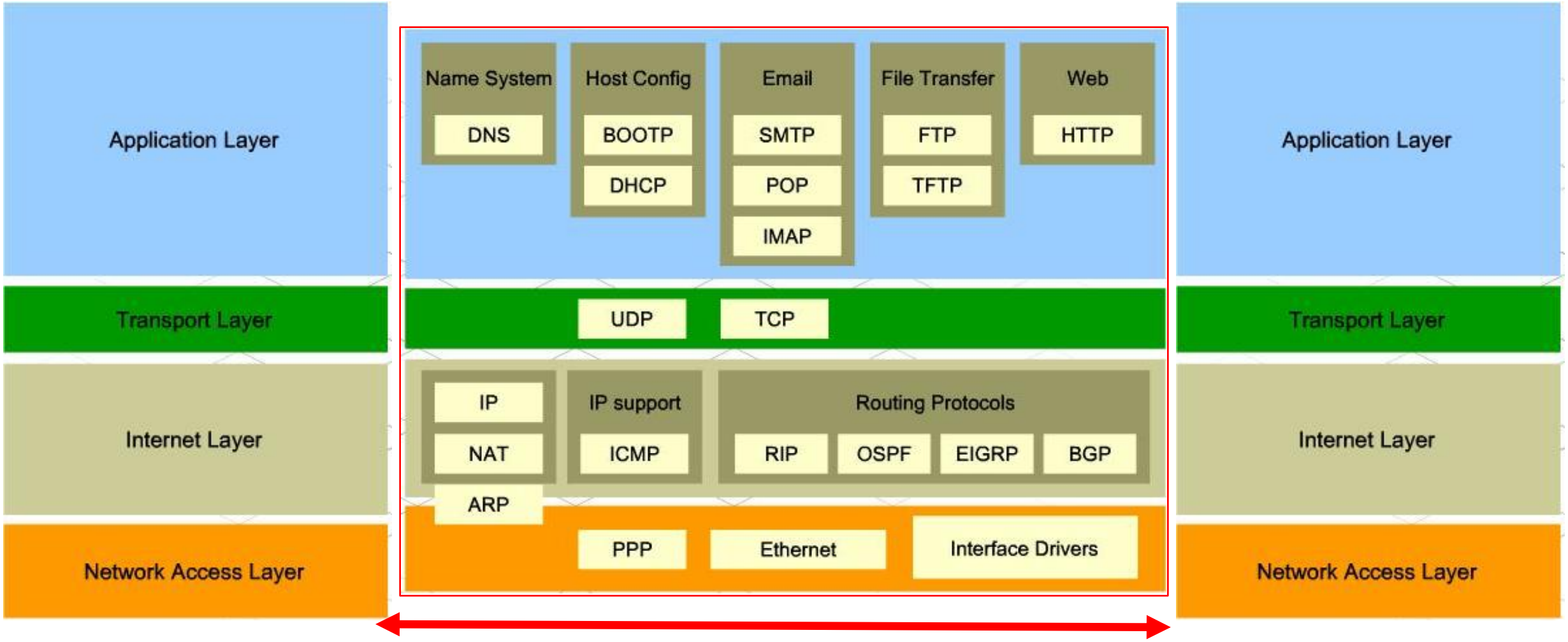
Link-Layer Security

Wired Protocols

Wired Protocols: Overview (1/3)



Wired Protocols: Overview (2/3)

The top three types of link-layer protocols for wired communications

- Data Link Control and Framing Protocols: These are foundational to wired communication, as they define how data is packaged, addressed, and transmitted across a physical link to another device.
- Physical Addressing and Mapping Protocols: Protocols like ARP (Address Resolution Protocol) are crucial for linking network-layer IP addresses to MAC addresses within a local network.
- Error Detection and Correction Protocols: These protocols play an important role in ensuring the reliability of data transmission.

Wired Protocols: Overview (3/3)

- Ethernet Protocol: Ethernet is the fundamental protocol for wired local area networks (LANs). It defines how data is framed, addressed, and transmitted over physical connections, using MAC addresses to deliver packets to the correct devices within a network.

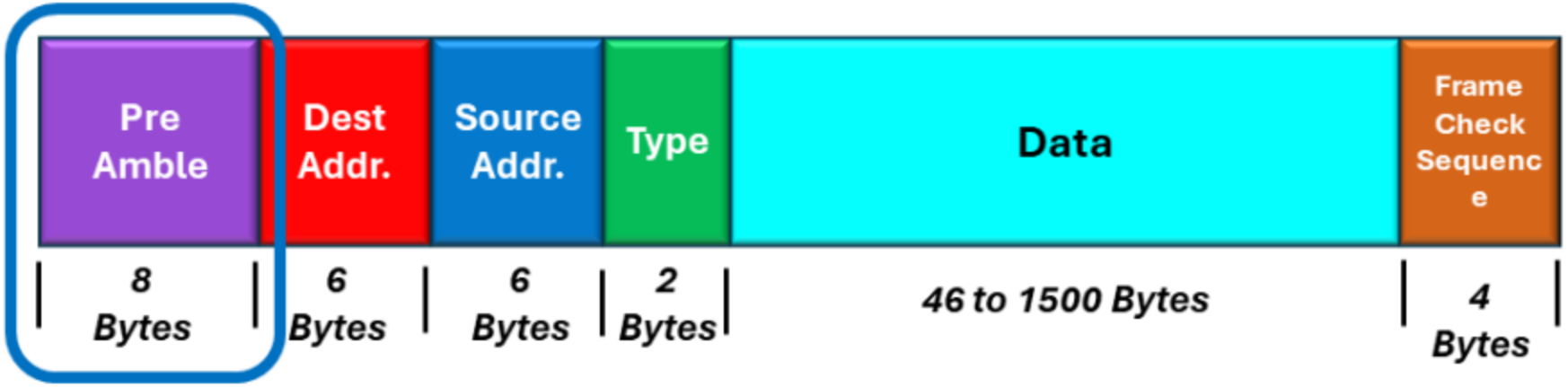
- ARP (Address Resolution Protocol): ARP is responsible for mapping IP addresses to MAC addresses on a local network. When a device needs to communicate with another device within the same network, it uses ARP to find the corresponding MAC address for a known IP address.

- LLDP (Link Layer Discovery Protocol): LLDP is a network daiscovery protocol that enables devices to share information about themselves and their neighbors. It allows devices, like switches and routers, to advertise their identity, capabilities, and connection details.

Wired Protocols: Ethernet (1/4)

- Ethernet is the fundamental protocol for wired local area networks (LANs). It defines how data is framed, addressed, and transmitted over physical connections, using MAC addresses to deliver packets to the correct devices within a network.

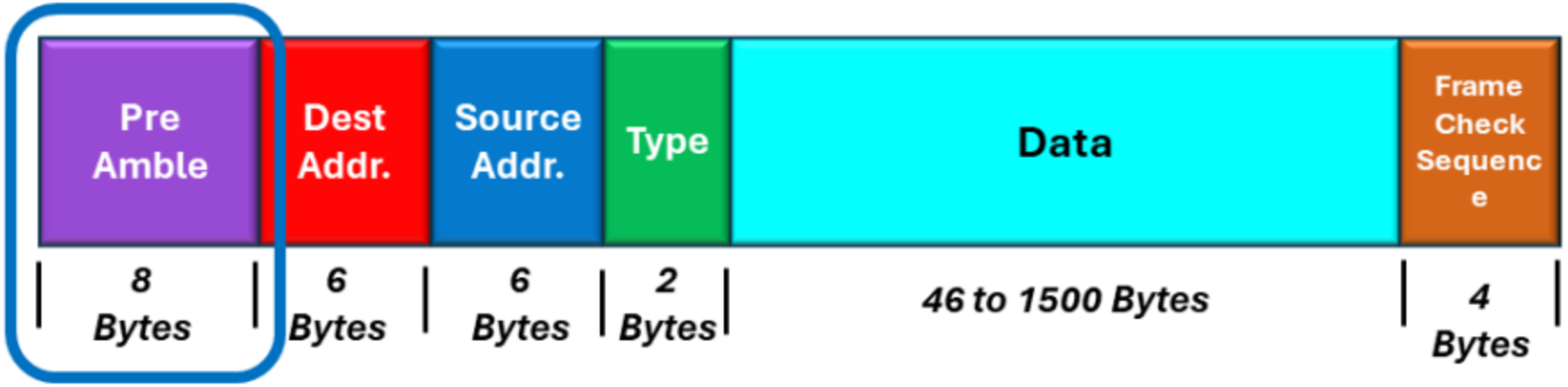
Wired Protocols: Ethernet (2/4)



IEEE 802.3: Standardized in 1983, establishing rules for Ethernet's physical and data link layers.

- Preamble： Signs for sunchronizing receiver clocks to make sure it can receive the frame. All values in preamble field of all frames are identical.
- Dest Address: Receiver's MAC address (48 bits, 12 hexadecimal digits)
- Source Address: Sender's MAC address (such as 00:1A:2B:3C:4D:5E)
  - First 24 bits: Device Manufacturers (Cisco Systems, Inc)
  - Last 24 bits: Device Identifier

Wired Protocols: Ethernet (3/4)



- Type: Indicates payload type (which protocol from network layer)
- Data: Contains the actual data (with optional padding)
- Check Sequence: Error-checking using CRC. If incorrect, delete the frame. Will not send it to above layer.

Wired Protocols: Ethernet (4/4)

The MAC address in Ethernet frames is forgeable due to the lack of authentication. For instance, if device A is using MAC address X to communicate with router R, an adversary could forge their device's MAC address to match X when connecting to router R. This situation presents two potential issues:

- Router Accepts Identical MAC Addresses: If the router allows two devices to have the same MAC address, any data sent to device A will also be forwarded to the adversary. This could lead to the interception of sensitive information.

- Router Rejects Identical MAC Addresses: If the router detects a conflict and rejects the connection of devices with identical MAC addresses, device A will also be disconnected from the router. This results in a loss of connectivity for device A (DOS attack).

Wired Protocols: ARP (1/5)

- The Address Resolution Protocol (ARP) is a fundamental network protocol used to map IP addresses to MAC (Media Access Control) addresses within a local area network (LAN).

- When a device wants to communicate with another device using an IP address, it must first determine the corresponding MAC address of that device.

Wired Protocols: ARP (2/5)

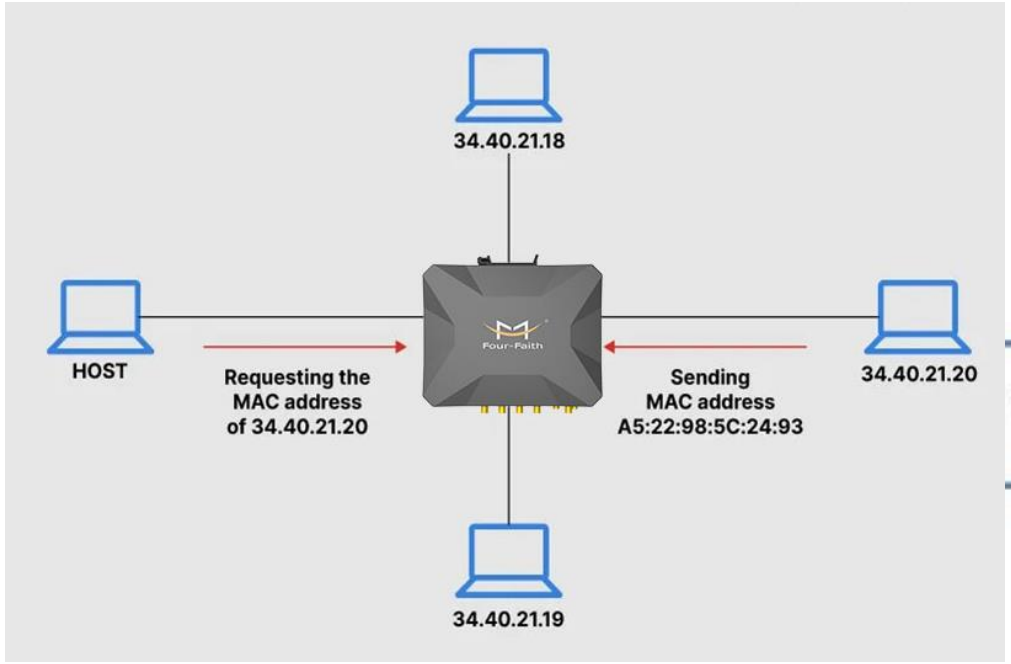
How ARP Works (High-Level):

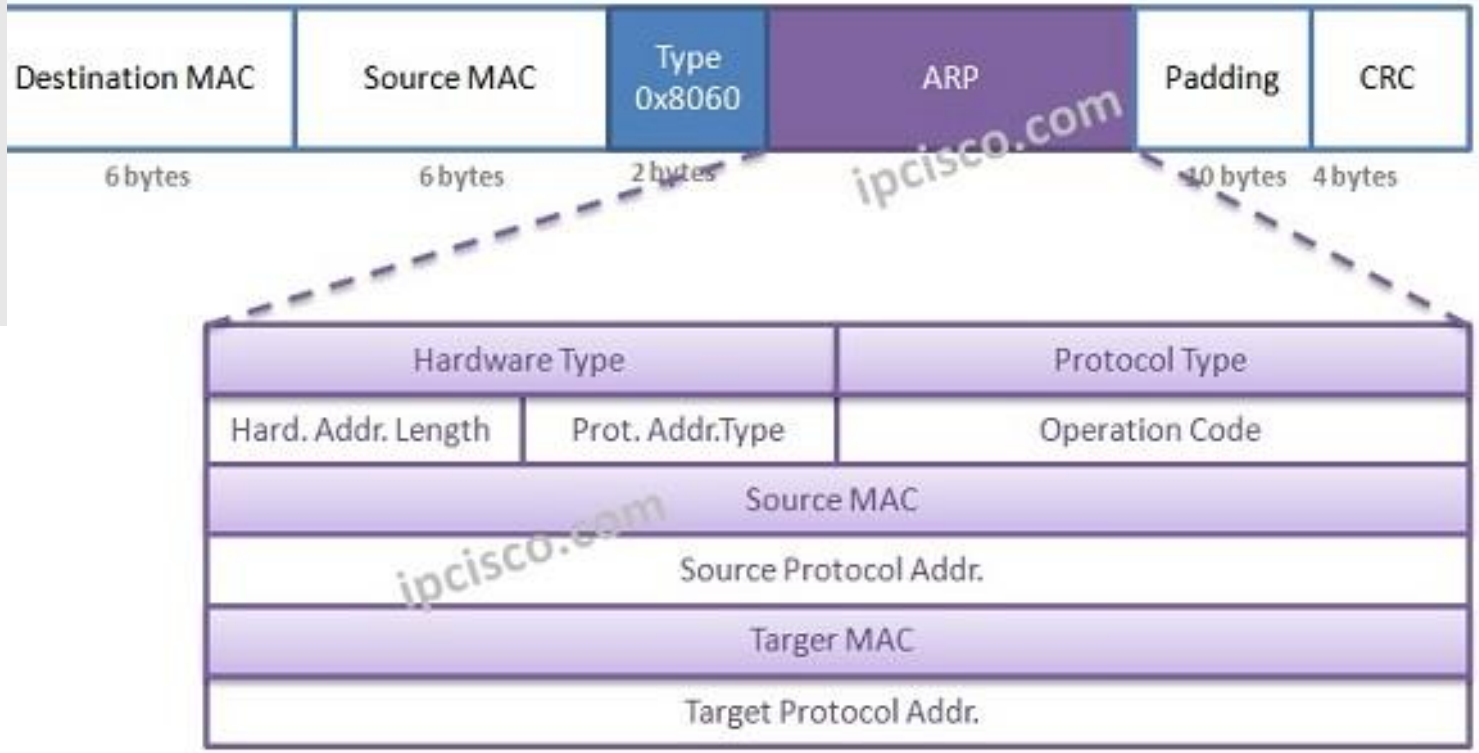
- ARP Request: When a device (let's call it Device A) wants to send a packet to another device (Device B) on the same local network, Device A will check its ARP cache (a table that stores IP-to-MAC address mappings) to see if it already knows the MAC address of Device B. If it doesn't, Device A sends an ARP request broadcast to all devices on the LAN. The request contains Device B's IP address and asks:

  "Who has this IP address? Please send me your MAC address."

- ARP Response: All devices on the network receive the ARP request, but only Device B, which recognizes its own IP address, will respond. Device B sends back an ARP reply directly to Device A, containing its MAC address.
- Updating ARP Cache: Upon receiving the ARP reply, Device A updates its ARP cache with the new mapping of Device B's IP address to its MAC address. Now, Device A can send frames directly to Device B using its MAC address.

Wired Protocols: ARP (3/5)





Wired Protocols: ARP (4/5)

- When a device (let's call it Device A) wants to communicate with an IP address that is outside its LAN, it must send the data through a default gateway.

- ARP protocol uses broadcast MAC address. It is a special address used in Ethernet networks to send a packet to all devices on a local network segment simultaneously. It allows for communication with all devices without needing to specify each device's MAC address individually. The broadcast MAC address is represented as FF:FF:FF:FF:FF.

- Broadcast MAC address plays a crucial role in processes like ARP and service discovery while also presenting challenges related to network performance and security.

Wired Protocols: ARP (5/5)

ARP Spoofing/Poisoning:

- When device A asks the MAC address of a specific IP addree and an adversary sends falsified ARP messages claiming that their MAC address corresponds to the IP address of a legitimate device, then the legitimate device A's traffic will be redirected to the attacker.

- Impact 1: This enables the attacker to intercept and manipulate the data, leading to potential data breaches or unauthorized access.
- Impact 2: Legitimate device A's traffic will be sent to the attacker instead of the intended recipient, leading to potential data loss and service disruption.

Wired Protocols: LLDP (1/5)

- The Link Layer Discovery Protocol (LLDP) is a standardized network protocol used for discovering and advertising information about directly connected devices on a local area network (LAN).

- LLDP is primarily used to facilitate network management and monitoring by allowing devices to advertise their identity, capabilities, and neighbors. This helps network administrators understand the topology of their network.

Wired Protocols: LLDP (2/5)

How It Works (High-Level):

- Each LLDP-enabled device periodically sends out (advertise) LLDP Data Units (LLDPDU) as multicast packets. These packets contain various information, including the device's MAC address, system name, port identifier, and the type of device (e.g., switch, router).

- When a device receives an LLDPDU from another device, it updates its LLDP database with the information received, allowing it to learn (discovery) about its neighboring devices.

Wired Protocols: LLDP (3/5)

LLDP Spoofing:

- How it Works: An adversary can configure their device to send false LLDP Data Units (LLDPDUs) claiming to be another legitimate device on the network. By broadcasting a forged identity, they can mislead network devices into believing they are interacting with a trusted device.

- Implications: This can result in the adversary gaining unauthorized access to sensitive data, altering traffic flows, or even launching man-in-the-middle attacks by positioning themselves between legitimate communication channels.

Wired Protocols: LLDP (4/5)

Denial of Service (DoS):

- How it Works: An adversary could flood the network with excessive LLDP traffic by sending numerous LLDPDUs. This could overwhelm the processing capacity of legitimate devices, causing them to become slow or unresponsive.

- Implications: Such a denial of service can disrupt network operations and make it difficult for legitimate devices to communicate with each other, thereby affecting productivity and service availability.

Wireless Protocols

Wireless communication involves the transfer of information between two or more devices through electromagnetic waves, eliminating the need for physical connections like wires or cables.

Wireless Protocols: Background (1/6)

- Wired Communication Protocol (1983): The wired communication protocol was standardized in 1983. This foundational protocol established a framework for reliable data transmission over wired networks and set the stage for further advancements in network technology.

- Wireless Communication Protocol (1997): The wireless communication protocol, known as IEEE 802.11, was standardized in 1997. This groundbreaking development marked the beginning of wireless networking, enabling devices to communicate without physical connections. The standard has evolved significantly ensuring it meets the growing demands of users and applications in an increasingly connected world.

Wireless Protocols: Background (2/6)

- In Wireless network, each mobile device client sends all of its communications to a network device called an access point (AP).

- The AP acts as an Ethernet bridge and forwards the communications to the appropriate network, such as a wired LAN or another Wireless Network.

Wireless Protocols: Background (3/6)

Security requirements are more critical in wireless communications for several reasons:

- Inherent Vulnerability: Wireless communications transmit data over radio waves, making signals accessible to anyone within range. This open medium exposes data to eavesdropping and unauthorized interception, increasing the need for robust security measures to protect sensitive information.

- Lack of Physical Barriers: Unlike wired networks, where physical access to cables is required to intercept data, wireless networks do not have the same physical limitations. This ease of access means that malicious actors can exploit vulnerabilities from a distance, requiring stronger security protocols to mitigate risks.

Wireless Protocols: Background (4/6)

1. Eavesdropping

Description: Eavesdropping involves intercepting data packets transmitted over the wireless medium. Since wireless signals travel through the air, attackers can use simple tools to capture these signals without needing physical access to the network.

Impact: Attackers can gain access to sensitive information such as passwords, personal data, and confidential communications.

2. Man-in-the-Middle (MitM) Attacks

Description: In MitM attacks, an attacker secretly intercepts and relays messages between two parties who believe they are directly communicating with each other. This is easier in wireless settings because attackers can position themselves between devices without needing physical access.

Impact: Attackers can modify the communication, steal credentials, or inject malicious content into the data stream.

Wireless Protocols: Background (5/6)

3. Rogue Access Points

Description: Attackers can set up rogue access points that appear legitimate but are actually controlled by the attacker. Unsuspecting users may connect to these rogue points, thinking they are connecting to a trusted network.

Impact: This allows attackers to capture credentials and sensitive information from connected devices.

4. Denial of Service (DoS) Attacks

Description: In wireless networks, attackers can easily disrupt service by flooding the network with traffic or sending de-authentication packets to disconnect legitimate users. This can be done from a distance, making it easier than in wired networks.

Impact: Users may be unable to access the network, leading to service interruptions.

Wireless Protocols: Background (6/6)

5. Session Hijacking

Description: Attackers can take control of a user's session by stealing session tokens or cookies over the air. This is more feasible in wireless environments due to the ease of intercepting data packets.

Impact: Attackers can impersonate users and gain unauthorized access to accounts or services.

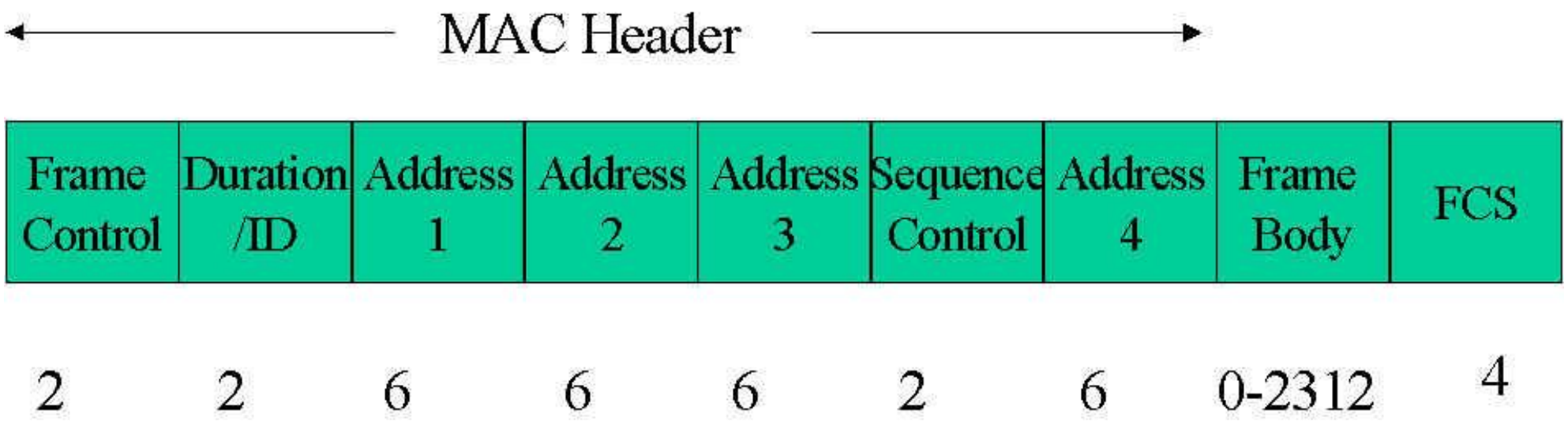
6. Jamming

Description: Jamming involves broadcasting signals that disrupt the communication channels of a wireless network. This can effectively block legitimate communication.

Impact: Users cannot connect to the network, resulting in denial of service.

Wireless Protocols: Frame (1/5)

A Wi-Fi frame, also known as an 802.11 frame, is the unit of communication in Wi-Fi networks. It contains all the data needed to transfer information between devices over a wireless network, including addressing, control information, and the payload. Wi-Fi frames are more complex than Ethernet frames because they support wireless-specific functions like security.



Wireless Protocols: Frame (2/5)

1. Frame Control (2 bytes): This field contains subfields that specify the frame type (management, control, or data) . To make sure the receiver know the purpose of this frame. ACK is applied here to gurantee that the transmission is reliable similar to TCP protocol.

2.Duration/ID (2 bytes): This field indicates how long the frame will occupy the wireless medium, which allows other devices to know when to wait before transmitting.

Wireless Protocols: Frame (3/5)

3. Addresses (6 bytes each)

Address 1 (Receiver Address): Specifies the MAC address of the destination device.
Address 2 (Transmitter Address): Specifies the MAC address of the device sending the frame.
Address 3 (BSSID): Represents the MAC address of the wireless access point (router) or base station, used to identify the specific network.

Address 4 (Optional): This is present only in certain frame types, like frames in wireless distribution systems (WDS). It is used when packets travel between access points.

Wireless Protocols: Frame (4/5)

4. Sequence Control (2 bytes): This field is used to reassemble fragmented frames by providing a sequence number, which helps the receiver reassemble frames in the correct order.

- Sequence Number: This part remains the same for all fragments of a single packet. Each packet (before fragmentation) is assigned a unique sequence number.
- Fragment Number: Each fragment within a sequence has a different fragment number, starting from 0 and increasing by 1 for each subsequent fragment of the same packet. This lets the receiver reassemble the fragments correctly in sequence

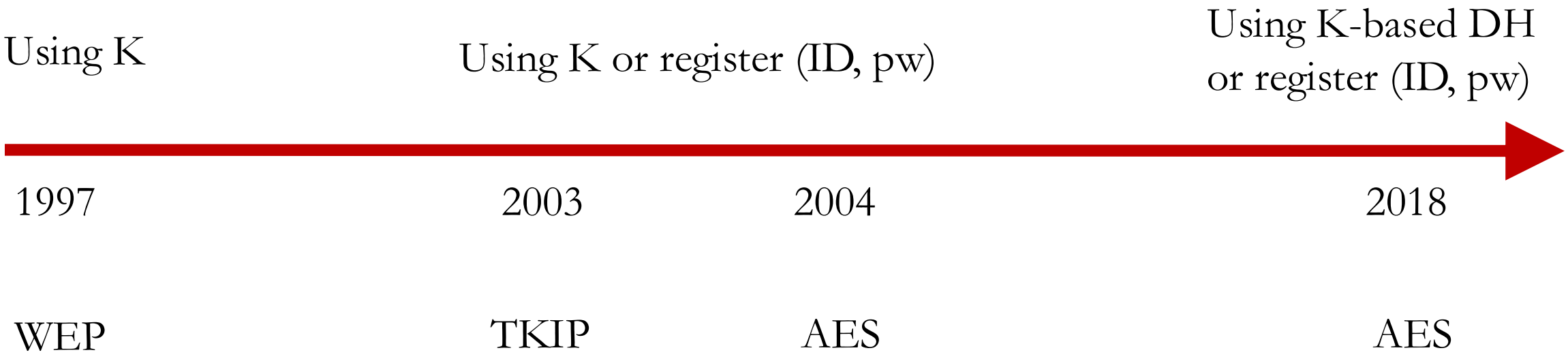
Wireless Protocols: Frame (5/5)

5. Frame Body (0-2312 bytes)
Contains the actual data payload for data frames or information specific to management or control frames. This section may be encrypted data if security is enabled.

6. FCS (Frame Check Sequence) (4 bytes)
This field holds a CRC (Cyclic Redundancy Check) value to ensure data integrity. The receiver checks this value to verify that the frame wasn't corrupted during transmission. If the FCS doesn't match the calculated value, the frame is discarded.

Wireless Protocols: Thinking

Who can connect to AP?



How to secure communications?

Wireless Protocols: WEP (1/6)

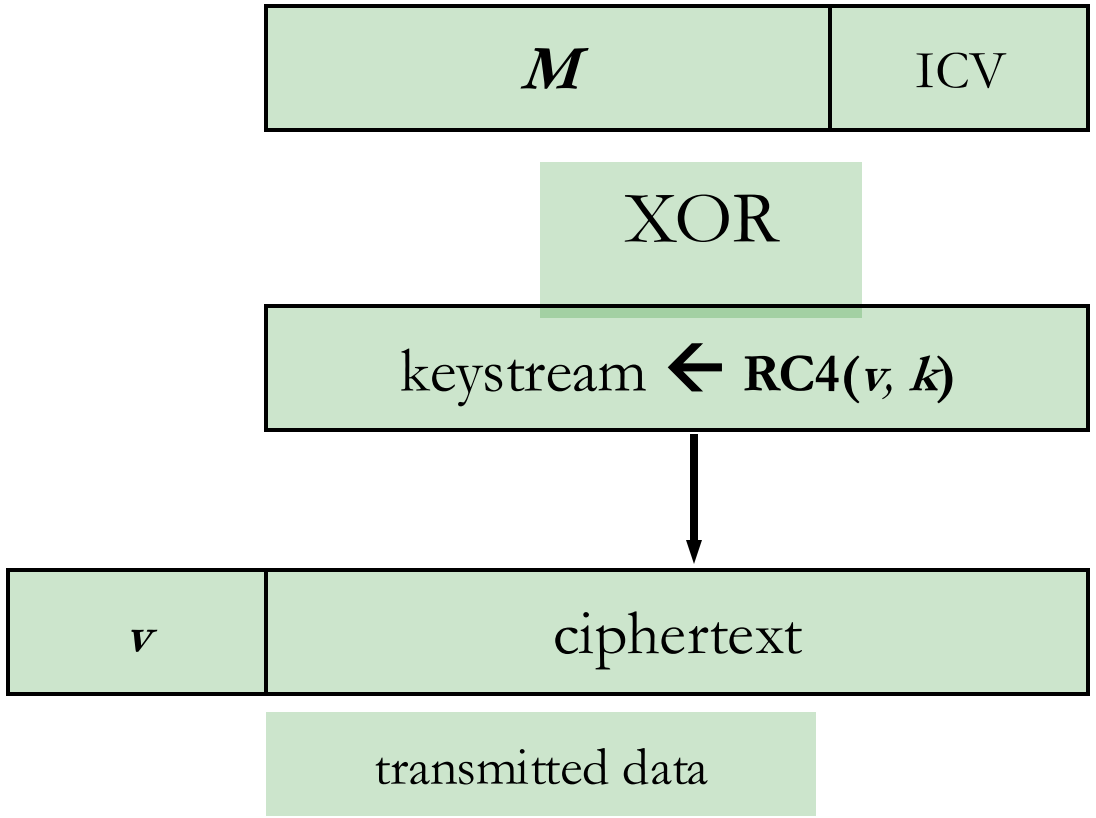
- Wired Equivalent Privacy (WEP) is an early security protocol (1997) designed to protect wireless networks by encrypting data transmitted over Wi-Fi.

- It provides authentication and a level of security (confidentiality & integrity) comparable to wired networks by encrypting data with the RC4 stream cipher and using a shared key for all devices on the network.

- However, WEP has significant weaknesses, particularly in how it manages encryption keys and its use of a short initialization vector (IV), making it vulnerable to attacks. These vulnerabilities allow attackers to crack the encryption within minutes, exposing data to interception and manipulation.

Wireless Protocols: WEP (2/6)

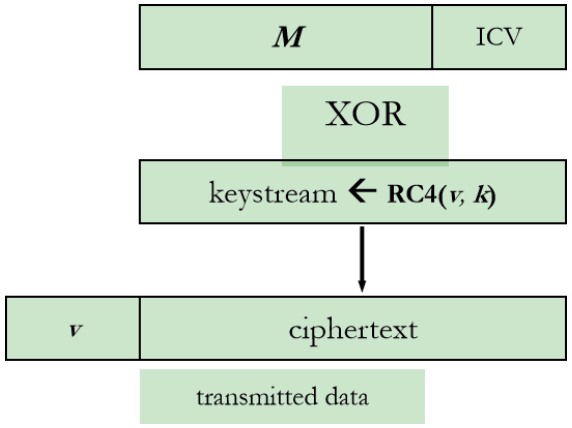
Let ***M*** be the message, ***v*** the current IV and ***k*** the secret shared key:



To protect against unauthorised data, an integrity algorithm CRC-32 operates on the plaintext to produce the ICV. This is a (**non-cryptographic**) 32-bit checksum, or integrity check value (ICV).

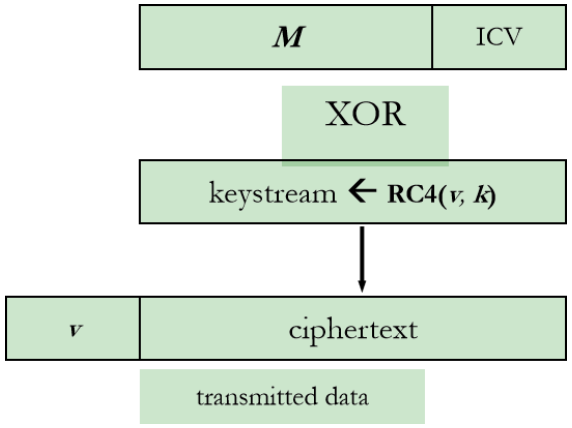
RC4 algorithm will generate a long-enough keystream to XOR bitstrings ***M||ICV***

Wireless Protocols: WEP (3/6)



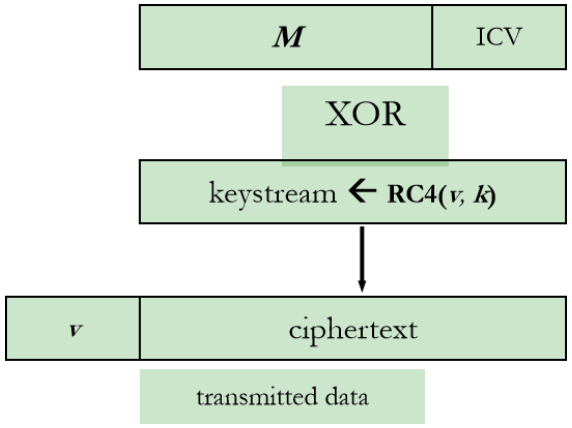
1. The 40-bit secret key is concatenated with an 24-bit initialisation vector (IV), resulting in a key with an overall length of 64-bits.
2. The resulting key is put into the pseudo-random number generator (PRNG), i.e., the stream cipher RC4.
3. The PRNG (RC4) outputs a pseudo-random key sequence based on the input key.
4. The resulting sequence is used to encrypt the data (M and ICV) by doing a bitwise XOR.

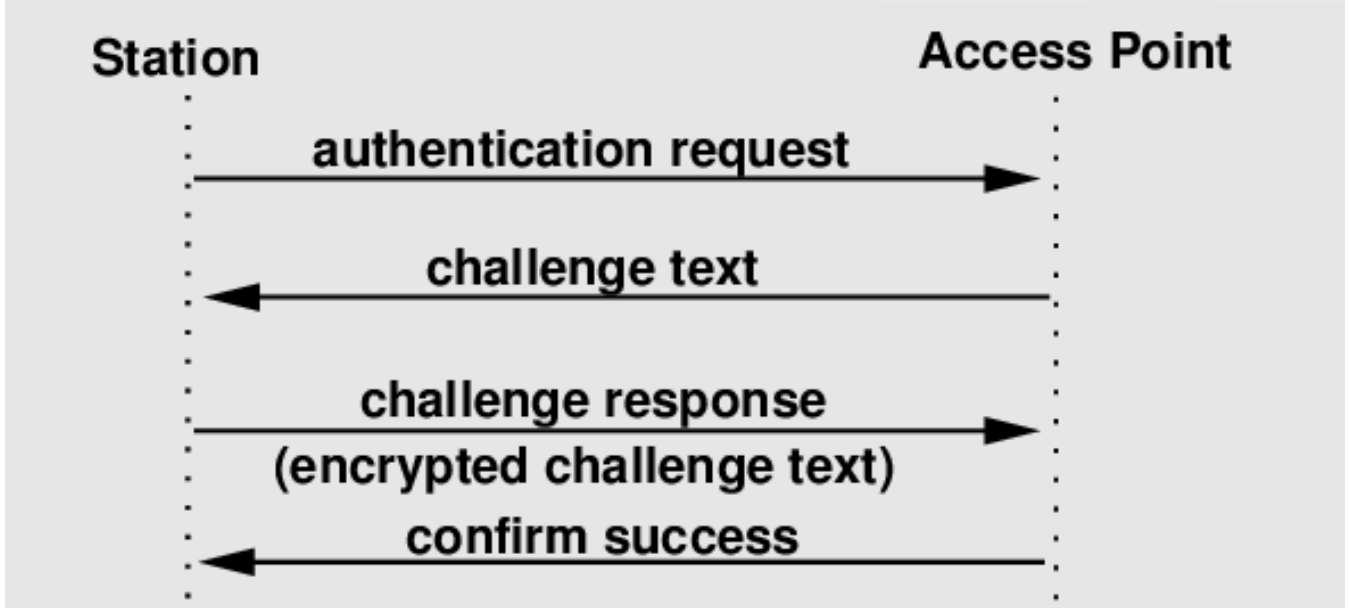
Wireless Protocols: WEP (4/6)



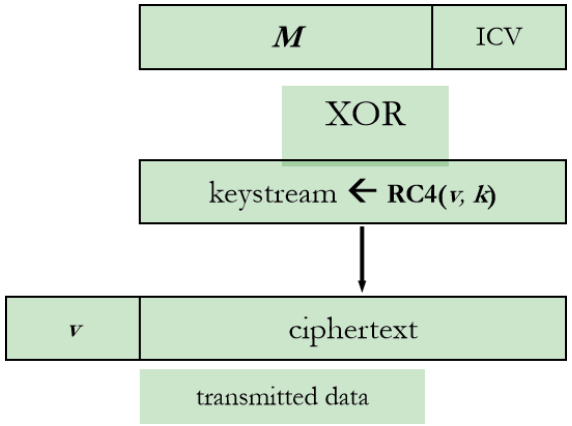
1. The IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message.
2. The ciphertext, combined with the proper key sequence, yields the original plaintext and ICV.
3. The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV to the ICV transmitted with the message.
4. If the ICV is not equal to the ICV received, the message has an error and returns the error.

Wireless Protocols: WEP (5/6)





Wireless Protocols: WEP (6/6)



- **Key management:** the same shared secret key is used for both authentication and encryption.
- **Integrity:** It is possible to modify some bits in a message so that the resulting message still passes the ICV test.
- **Confidentiality:** key size is too short, Key stream reuse (IV is too short).

Wireless Protocols: TKIP

- Temporal Key Integrity Protocol (TKIP) is a security protocol introduced to enhance the security of wireless networks, primarily as part of the WPA (Wi-Fi Protected Access) standard (new standard compared to WEP). TKIP was developed as a temporary solution to address the vulnerabilities of WEP (Wired Equivalent Privacy) while maintaining compatibility with existing hardware.

- TKIP allows to be implemented on older wireless devices without requiring significant hardware upgrades or replacements. This approach enabled users to enhance their network security while continuing to use their current equipment.

Wireless Protocols: Authentication in WEP

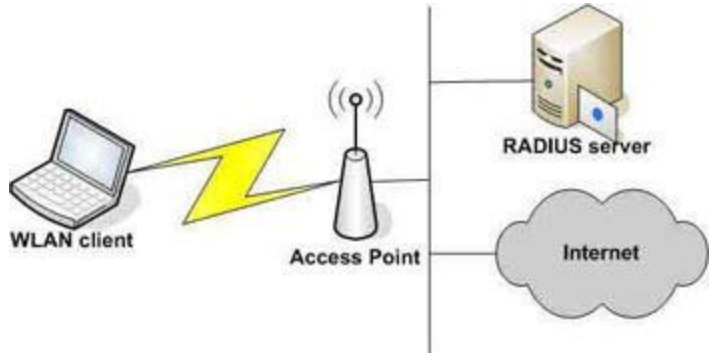
- In WEP, authentication is achieved through a shared secret key, which is the same for all devices connected to the access point (AP). When a device wants to join the network, it must present the shared key to authenticate itself, allowing it to encrypt and decrypt the data transmitted over the network.

- However, Because all devices use the same key, managing that key becomes problematic. If the key needs to be changed (for instance, if a device is compromised), it must be updated on all devices connected to the network, which can be cumbersome and prone to error.

Wireless Protocols: IEEE 802.1X (1/9)

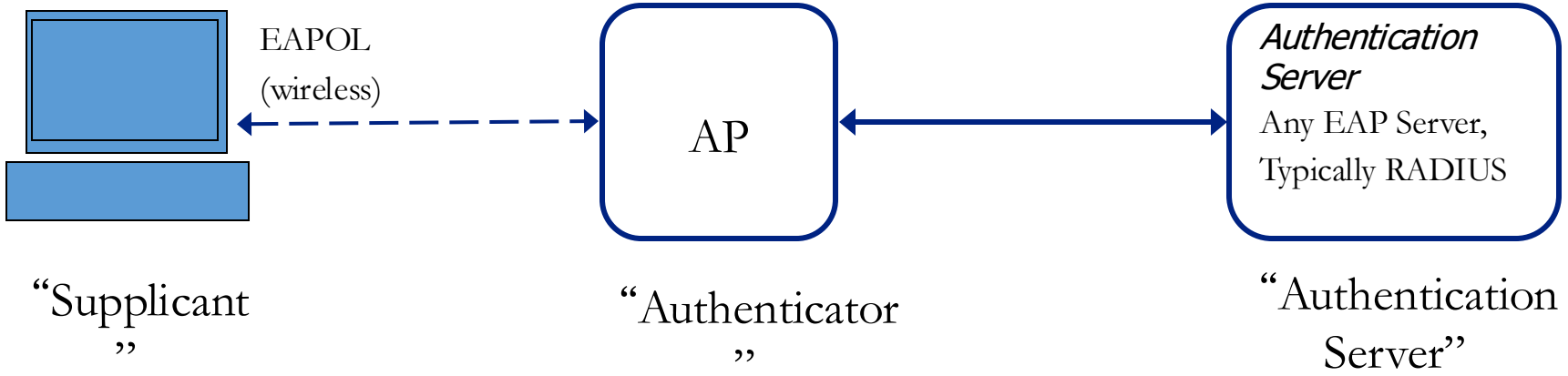
- IEEE 802.1X (2003) is a network access control standard that provides a framework for authenticating devices connecting to a network, typically over Wi-Fi.

- It uses a protocol framwork called EAP (Extensible Authentication Protocol) to perform secure authentication among
  - a client (known as a "supplicant"),
  - an authenticator (such as access point), and
  - an authentication server (usually a RADIUS server).



Wireless Protocols: IEEE 802.1X (2/9)

- IEEE 802.1X setup:
  - Supplicant authenticates via Authenticator to central Authentication Server.
  - Authentication Server confirms Supplicants credentials.
  - Authentication Server directs Authenticator to allow the Supplicant access to services after the successful authentication.

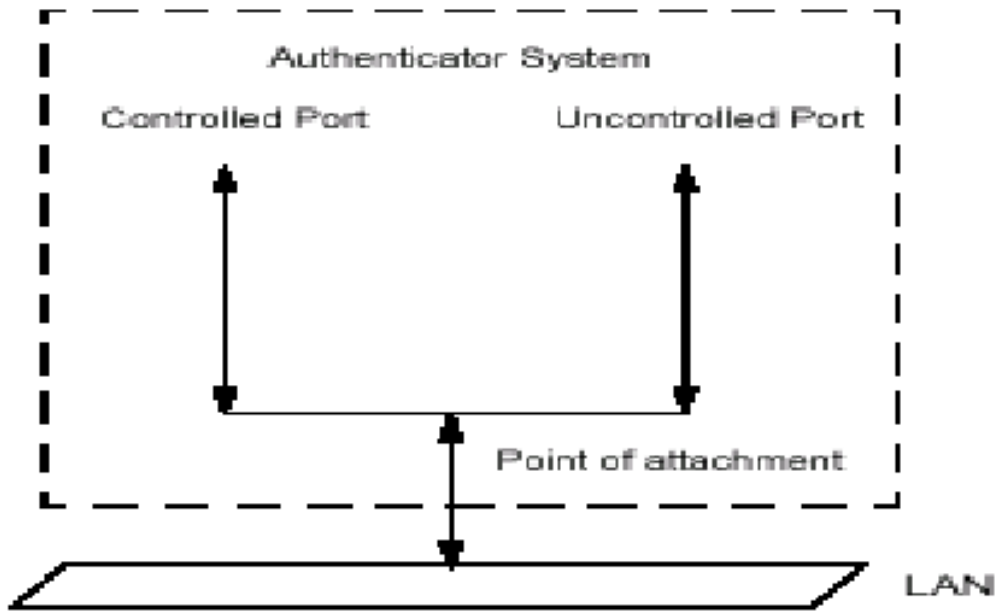


Wireless Protocols: IEEE 802.1X (3/9)

- Port-based access control is a network security mechanism that restricts network access at the point of physical or logical connection, such as an Ethernet or Wi-Fi access port.

- Defined in the IEEE 802.1X standard, it primarily uses the concepts of "ports" to control which devices are allowed access to the network.
  - **Controlled Port** :
  accepts packets from authenticated devices.

  - **Uncontrolled Port** :
  only passes 802.1X packets.



Wireless Protocols: IEEE 802.1X (4/9)

EAP (Extensible Authentication Protocol), as used in 802.1X, is a authentication framework and provides several advantages over WEP's simple shared-key authentication, particularly in areas like user management and key management:

- Individual User Authentication: EAP allows each user to authenticate individually, often with unique credentials (passwords), rather than relying on a single, static network key shared by all devices as in WEP. This approach improves user management, making it easier to track and control access on a per-user basis, which is essential for auditing and accountability.
- Dynamic Key Management: EAP supports the dynamic generation and distribution of session keys. After successful authentication, unique encryption keys are generated for each session, providing stronger security than WEP's fixed shared key. This dynamic keying mechanism means that each user has their own encryption key, reducing the risk of a compromised key affecting the entire network.

Wireless Protocols: IEEE 802.1X (5/9)

PEAP: Password-Based Authentication (via TLS tunnel)

- Process: Client and Authentication Server first establish a secure TLS tunnel. Inside the tunnel, the client sends username/password (using a challenge-response method) for authentication.
- Security: Encrypts the entire authentication process using TLS to protect passwords from exposure.

EAP-TLS: Mutual Certificate-Based Authentication

- Process: Client and Server both use X.509 certificates for mutual authentication. TLS handshake establishes a secure communication channel.
- Security: High security, as it requires certificates on both the client and server sides.

Wireless Protocols: IEEE 802.1X (6/9)

How it (PEAP) works:

- On detection of a new supplicant, the port on the authenticator is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic is dropped.

- Through 802.1X traffic, the client (supplicant) and the Authentication Server (AS) establish a secure TLS tunnel via running TLS protocols. In this step, the server is authenticated by the client using the server's certificate (issued by a trusted Certificate Authority). The TLS tunnel is established to encrypt all further communication between the client and the server. In this step, both know a shared key.

Wireless Protocols: IEEE 802.1X (7/9)

How it (PEAP) works:

- To initiate authentication on client, the authenticator (AP) will periodically transmit EAP-Request Identity frames to a special Layer 2 address on the local network segment. The supplicant listens on this address, and on receipt of the EAP-Request Identity frame it responds with an EAP-Response Identity frame containing an identifier for the supplicant such as a User ID.

- The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the authentication server.

Wireless Protocols: IEEE 802.1X (8/9)

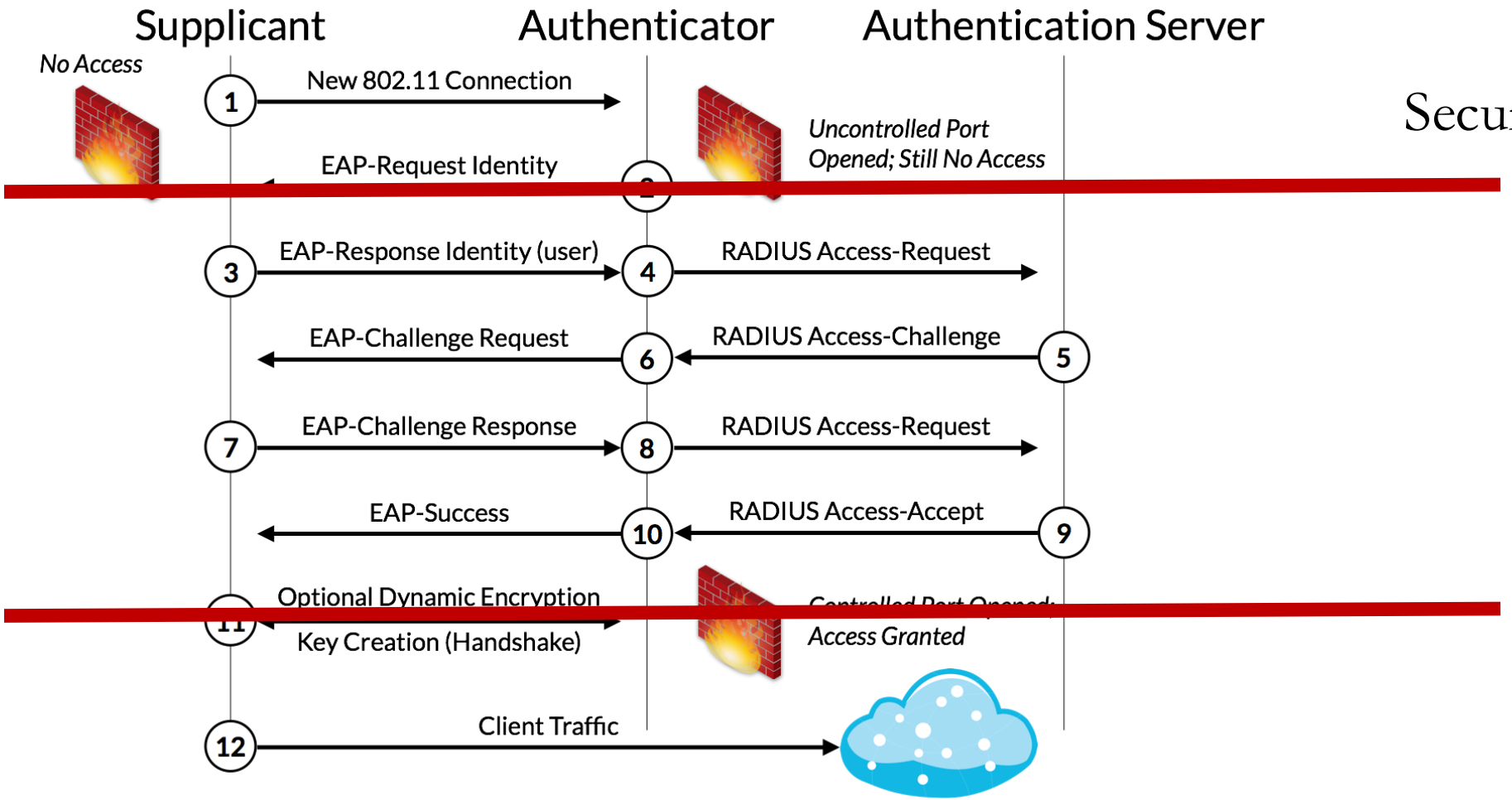
- The authentication server sends a reply (encapsulated in a RADIUS Access-Challenge packet) to the authenticator, containing an EAP Request specifying the EAP authentication Method. The authenticator encapsulates the EAP Request in an EAPOL frame and transmits it to the supplicant.

- If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server (translated by the authenticator) until the authentication server responds with either an EAP-Success message, or an EAP-Failure message.

- If authentication is successful, the authenticator sets the port to the "authorized" state and normal traffic is allowed, if it is unsuccessful the port remains in the "unauthorized" state.

Wireless Protocols: IEEE 802.1X (9/9)

EAP and RADIUS messages in 802.1X authentication session.



Secure Channel with AS

AS verify supplicant

Wireless Protocols: PSK (1/2)

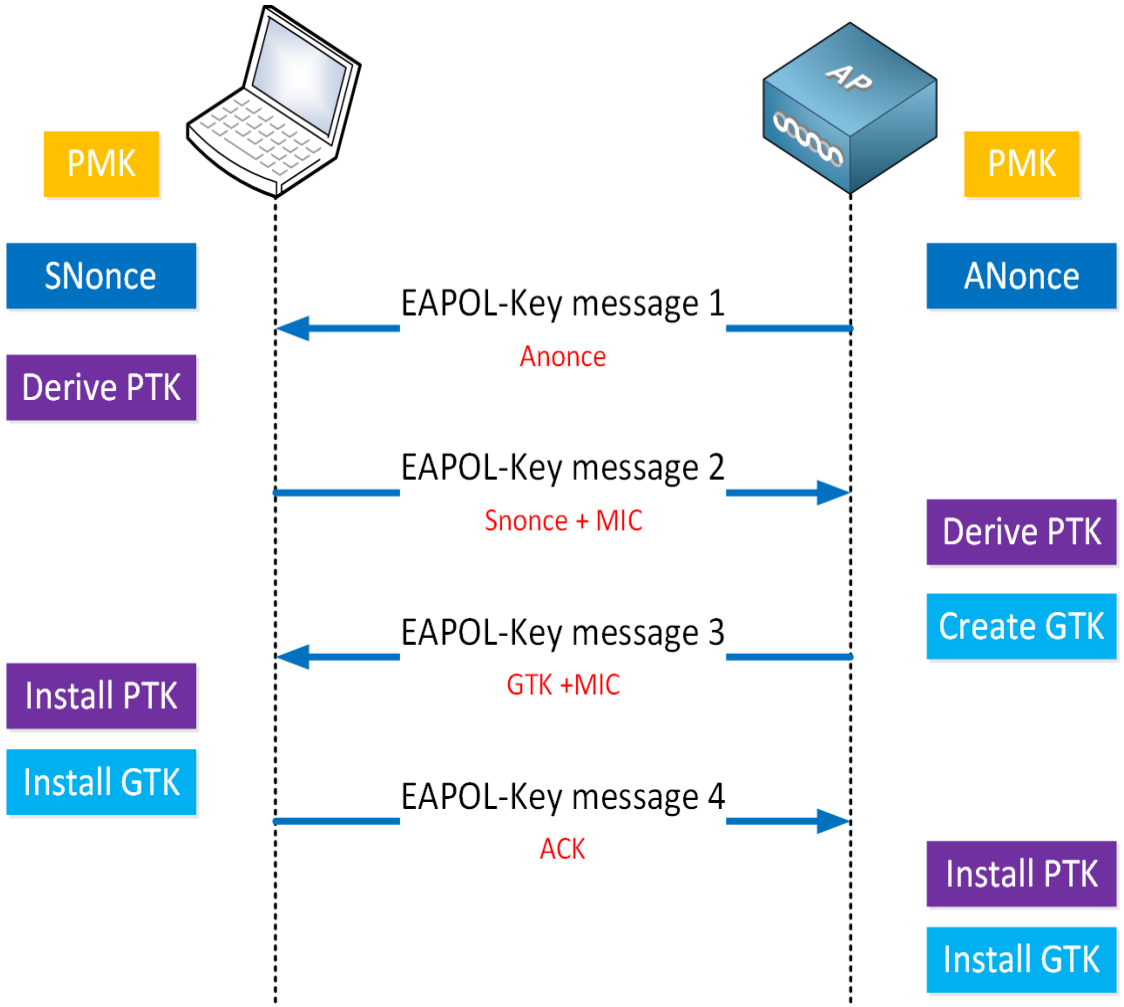
PSK (pre-shared key) mechanism is a simpler authentication method than EAP.

- Shared Key: A common secret key (password) is shared between the user and the network (e.g., a Wi-Fi password).
- Key Derivation: The PSK and nonces are used to derive session keys that are used for encrypting communication between the device and the access point.
- No Server Authentication: PSK does not require a dedicated authentication server and is typically used in home or small office networks.

How Does PSK Work?

1. The user enters a shared password to authenticate with the access point.
2. Both the client and the access point generate a session key from the password (PSK).
3. This session key is used to encrypt all subsequent communication between the client and the access point.

Wireless Protocols: PSK (2/2)



MIC = Message Integrity Check)

PMK = shared secret key

PTK = H(PMK, Snonce, Anonce, MAC1, MAC2)

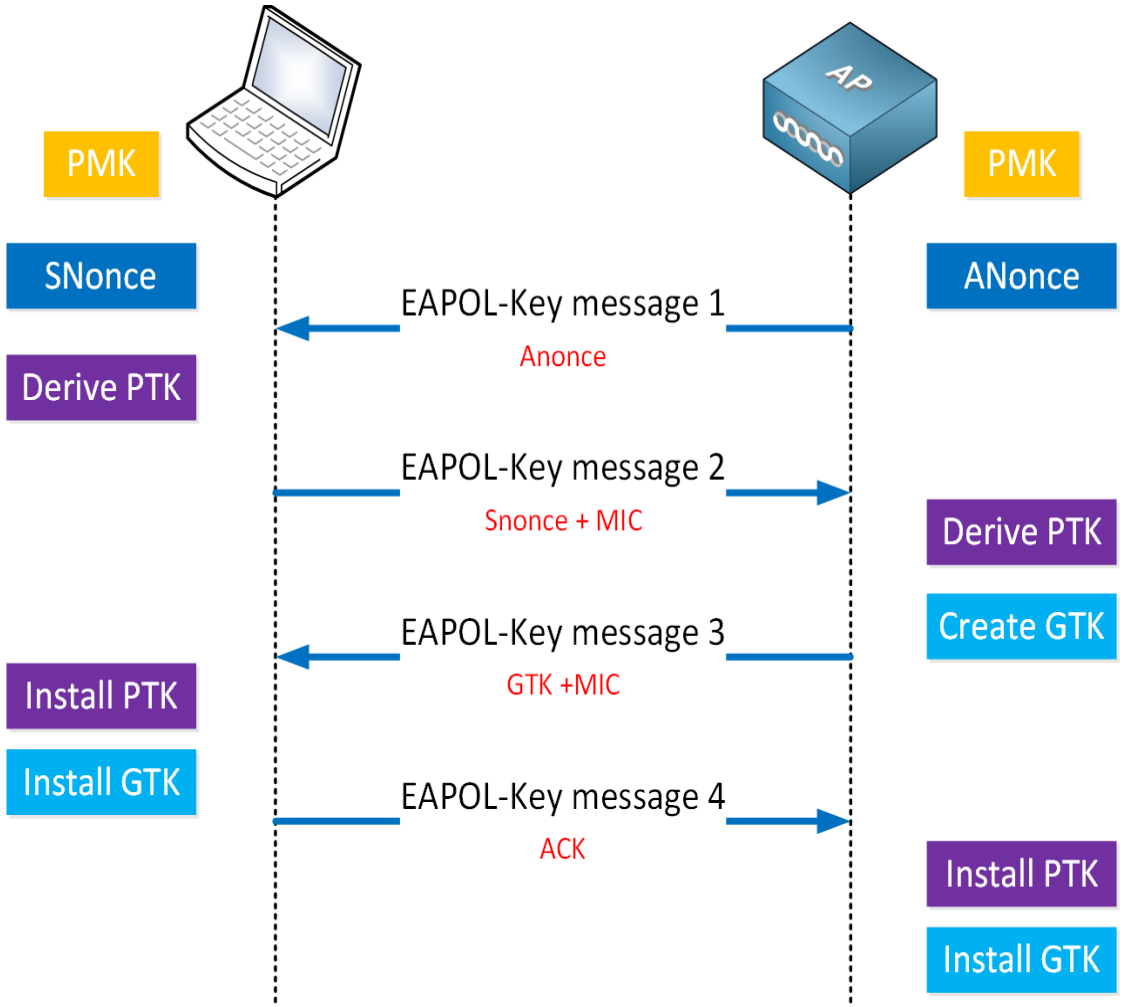
GTK = Generated by the AP, then encrypted with the KEK from the PTK and sent to the client

Wireless Protocols: Comparisons

Feature	WEP	WPA	WPA2
Encryption Algorithm	RC4	RC4-based TKIP	AES
Key	Static shared key	Dynamic key	Dynamic key
Authentication Method	PSK	EAP or PSK	EAP or PSK
Security	Insecure	Better than insecure	Strong

Dynamic = computed from static shared key + nonce

Wireless Protocols: WPA3 (1/3)



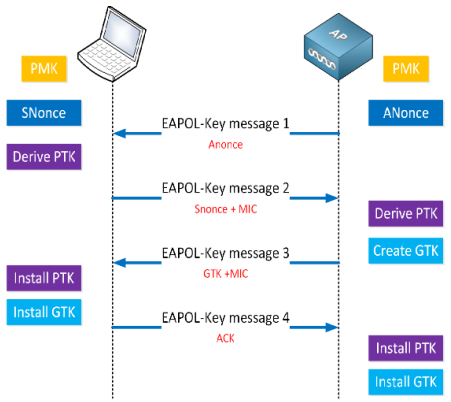
MIC = Message Integrity Check)

PMK = from Diffie-Hellman Key Exchange protocol

PTK = H(PMK, PW, Snonce, Anonce, MAC1, MAC2)

GTK = Generated by the AP, then encrypted with the KEK from the PTK and sent to the client

Wireless Protocols: WPA3 (2/3)



MIC = Message Integrity Check)

PMK = from Diffie-Hellman Key Exchange protocol

PTK = H(PMK, PW, Snonce, Anonce, MAC1, MAC2)

GTK = Generated by the AP, then encrypted with the KEK from the PTK and sent to the client

- Forward security (or forward secrecy) is a security property that ensures that even if long-term keys (such as a pre-shared key) are compromised in the future, past session keys and communications (recorded by the adversary) remain secure.
- Even if an adversary obtains the pre-shared key on Day 2, they would still be unable to decrypt the recorded communications from Day 1. This is because each session's encryption relies on a unique, temporary session key that is separate from the long-term pre-shared key

Wireless Protocols: WPA3 (3/3)

Feature	WEP	WPA	WPA2	WPA3
Encryption Algorithm	RC4	RC4-based TKIP	AES	AES
Key	Static shared key	Dynamic key	Dynamic key	Dynamic key
Authentication Method	PSK	EAP or PSK	EAP or PSK	EAP or PSK
Security	Insecure	Better than insecure	Strong	Stronger

Note: the authentication methods are slightly different.