COMPSCI4062&5063: Cyber Security Fundamentals

Topic 6: Network Security

Dr. Dongzhu Liu

Email: dongzhu.liu@glasgow.ac.uk
Office: SAWB 510 (b)

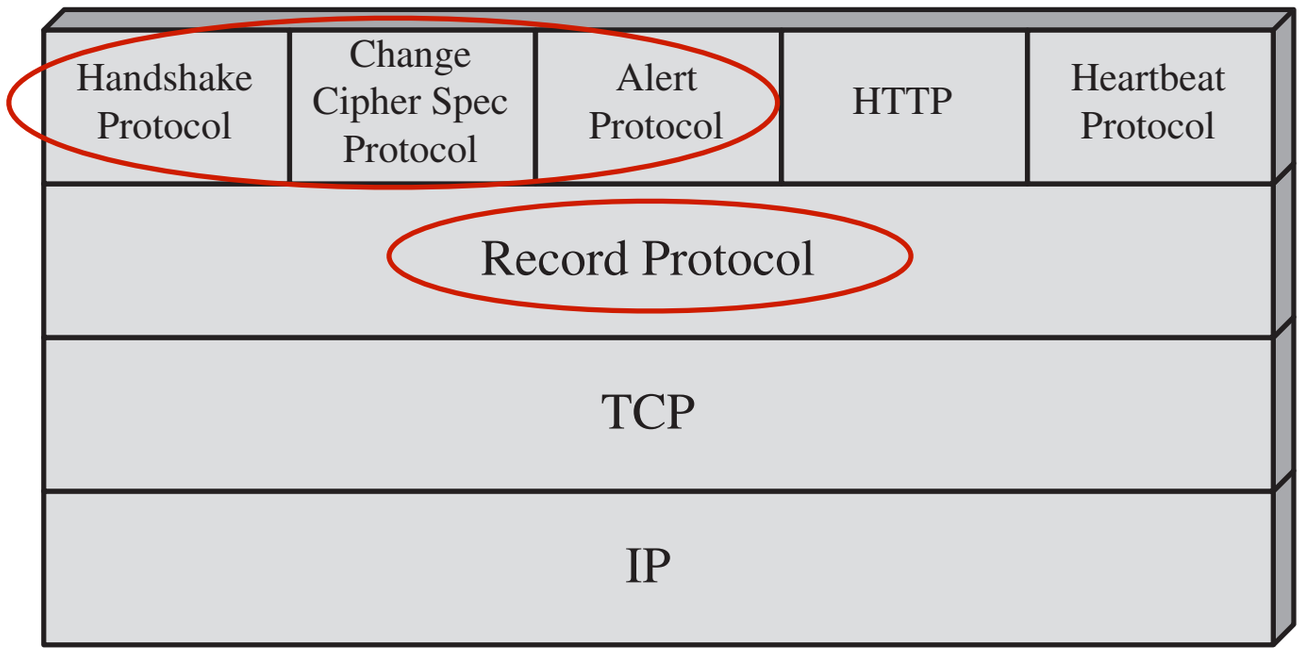
Overview

- Internet Security
  - Secure Sockets Layers (SSL) / Transport Layer Security (TLS)

- Wireless Network Security
  - Wireless Networks Threats
  - Wireless Security Measures
  - IEEE 802.11 Wireless LAN
  - IEEE 802.11i Wireless LAN Security

Transport Layer Security (TLS): Architecture

- TLS is designed to make use of TCP to provide a reliable end-to-end secure service.
- Two layers
  - Record protocol:
  - Handshake, Change Cipher Spec, Alter Protocols:



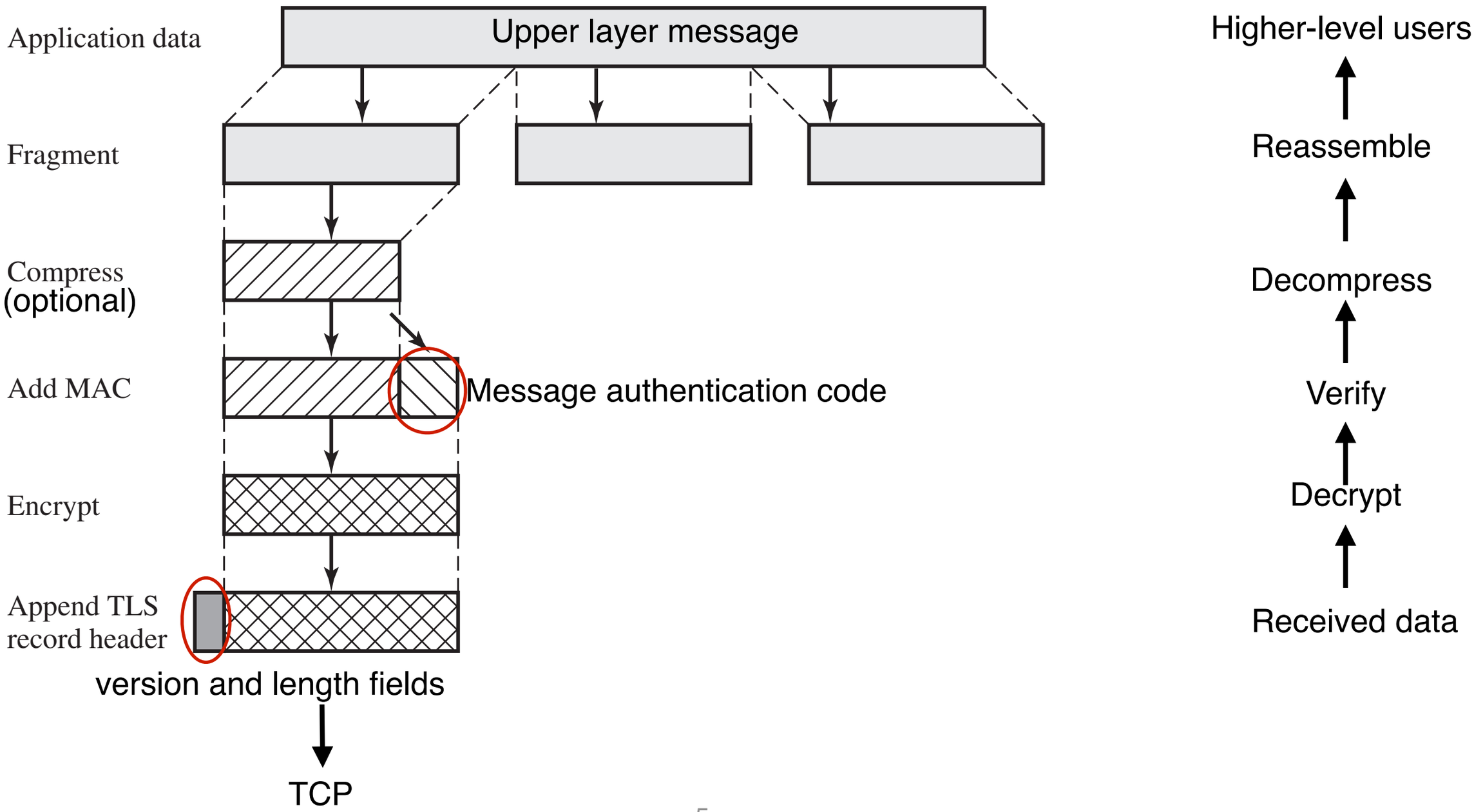
SSL/TLS Protocol Stack

Transport Layer Security (TLS): Two Concepts

- TLS connection
  - A transport that provides a suitable type of service
  - peer-to-peer relationship
  - transient, associated with one session
- TLS session
  - An association between a client and a server
  - Created by the Handshake Protocol
  - Define a set of cryptographic security parameters
  - Security parameters can be shared among multiple connections
  - Avoid negotiation of new security parameters for each connection

Transport Layer Security (TLS): Protocols

- Record Protocol



Transport Layer Security (TLS): Protocols

- Change Cipher Spec Protocol
  - This protocol consists of a single message — a single byte with the value 1.
  - Purpose: cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

Transport Layer Security (TLS): Protocols

- Alert Protocol
  - Purpose: Convey TLS-related alerts to the peer entity
  - Each message in this protocol consists of two byte
  - First byte: severity of the message (“warning” or “fatal”) — if “fatal”, TLS immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established.
  - Second byte: specific alert

Fatal alert example: an incorrect message authentication code

Nonfatal alert example: close_notify message — notifies the recipient that the sender will not send any more messages on this connection.

Transport Layer Security (TLS): Protocols

- Handshake Protocol
  - Allows the server and client to authenticate each other
  - Negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an TLS record
  - This protocol is used before any application data are transmitted

Transport Layer Security (TLS): Protocols

- Handshake Protocol

Phase1

-Initiate a logical connection

-Establish the security capabilities

-Client_hello

Highest TLS version

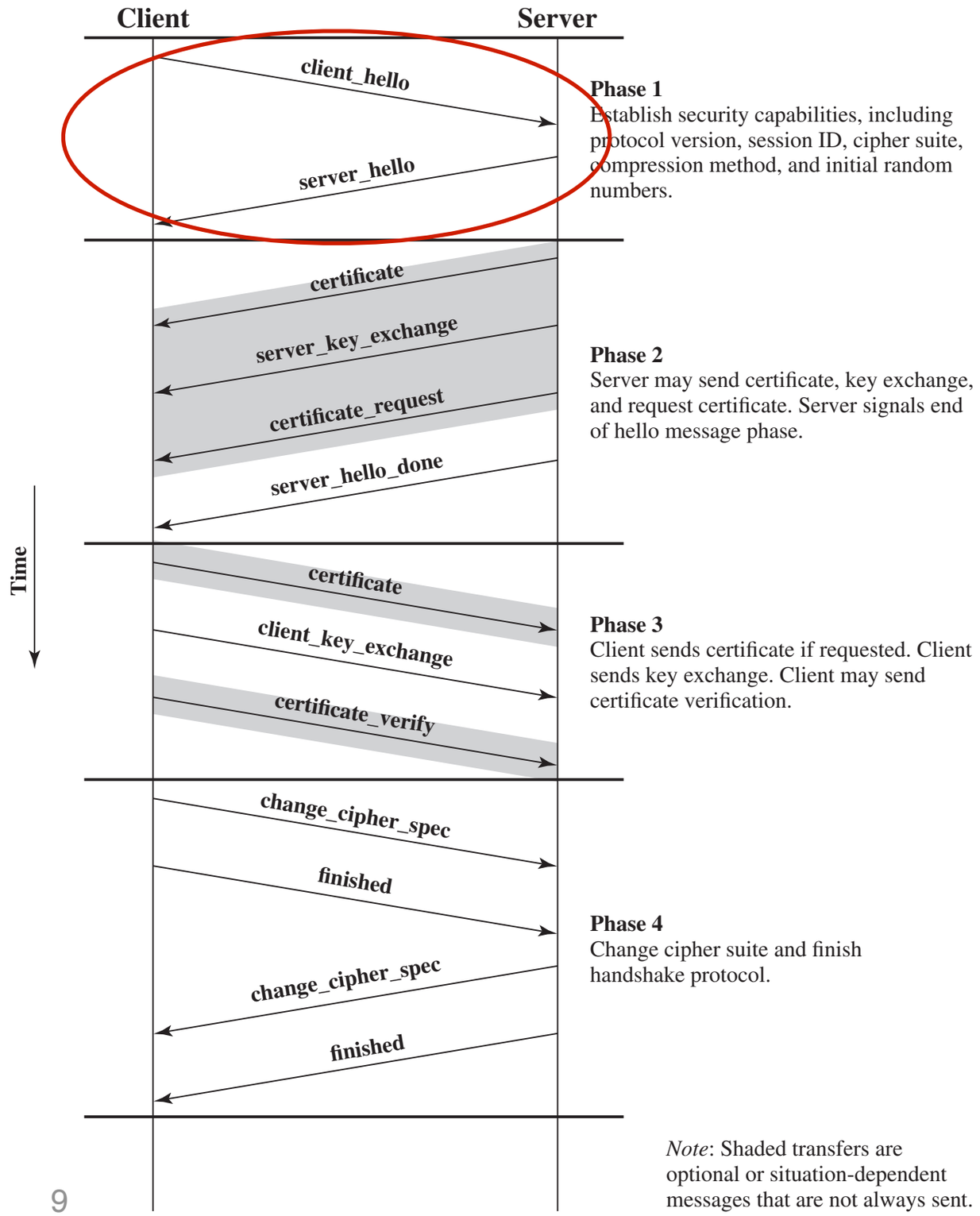
Random structure (for key exchange)

Session ID (nonzero value for updating the parameters of an existing connection or initiating a new connection on this session; zero value for establishing a new connection on a new session)

CipherSuite (cryptographic algorithms)

Compression method

-Server_hello (same parameters as client_hello)



Transport Layer Security (TLS): Protocols

- Handshake Protocol

Phase2

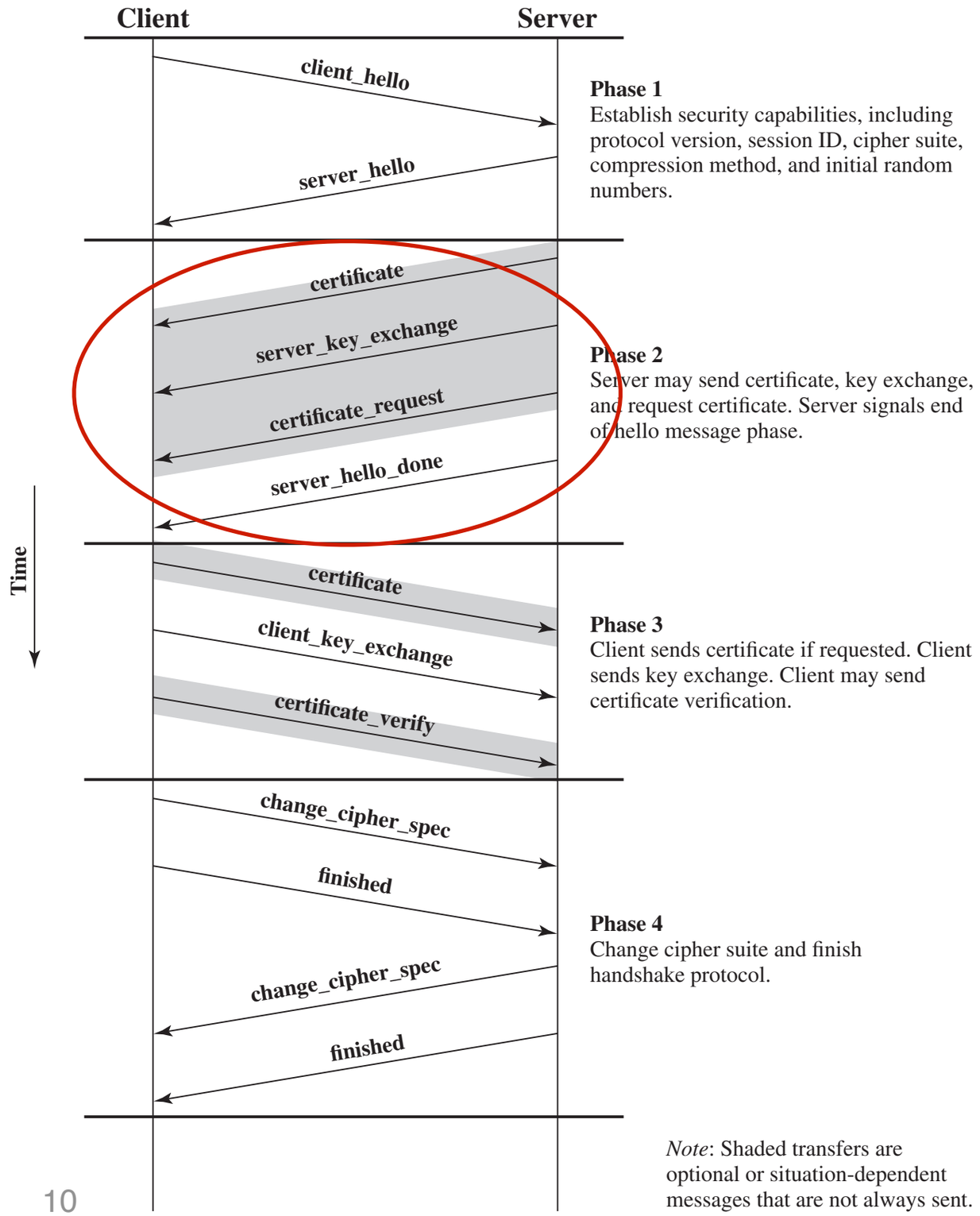
-Passing a certificate to the client

-Additional key information

-Request for certificate from the client

(public-key encryption)

-sever-done message, wait for a client response



Transport Layer Security (TLS): Protocols

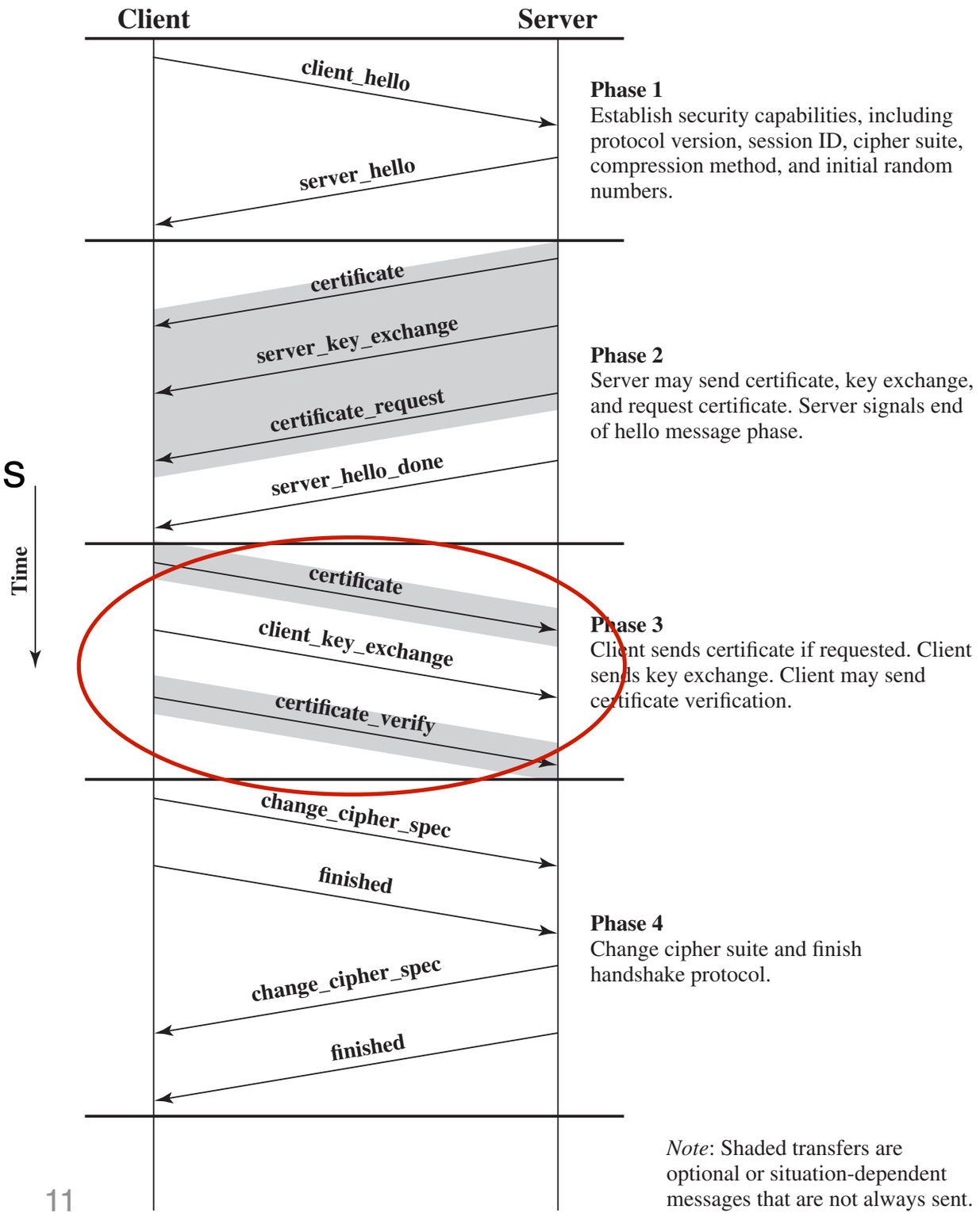
- Handshake Protocol

Phase3

-Verify the certificate

-Check server_hello parameters

if all is satisfactory, the clients sends messages back to the server



Transport Layer Security (TLS): Protocols

- Handshake Protocol

Phase4

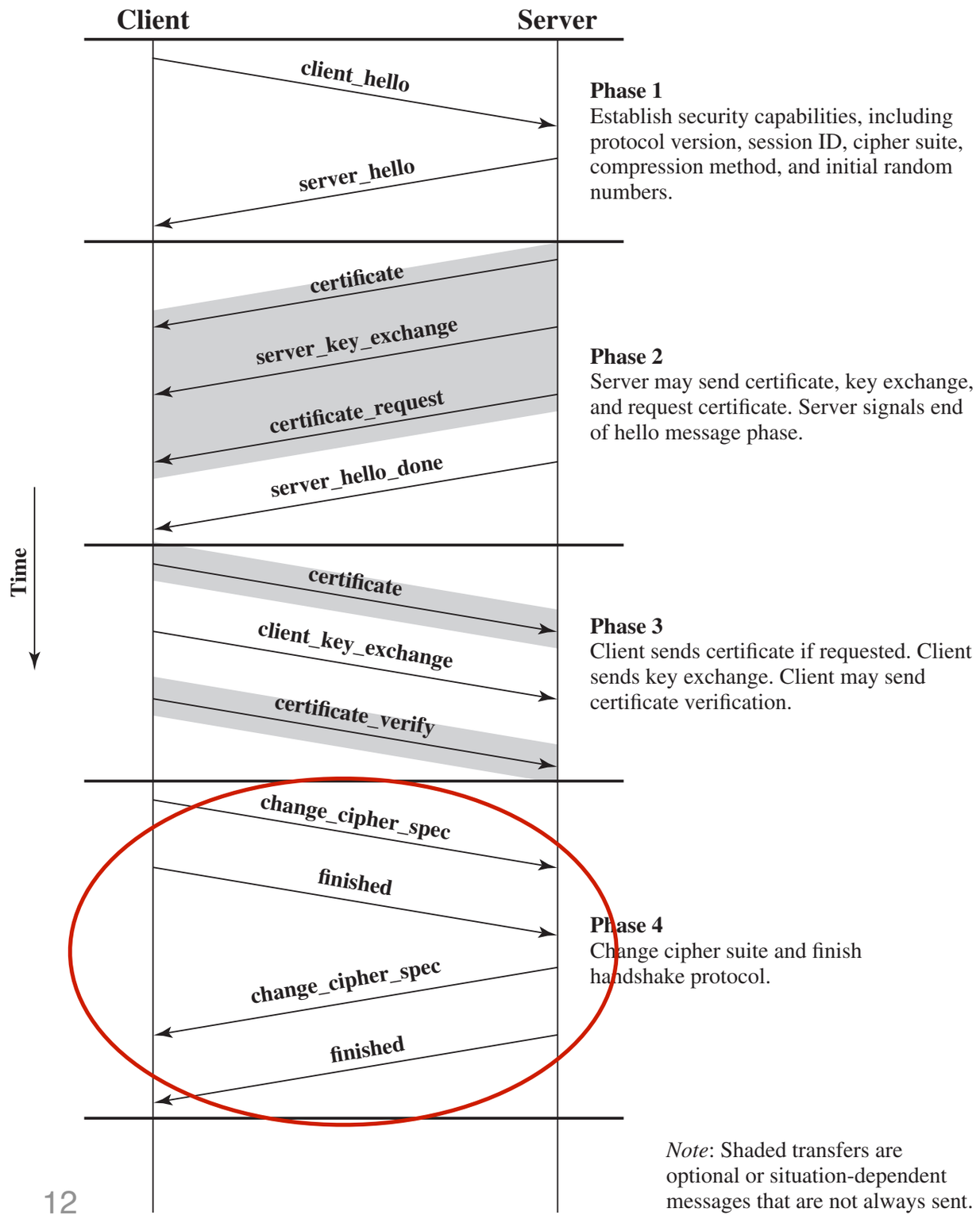
Client

-Sends a change_cipher_spec message and copies the pending CipherSpec into the current CipherSpec (Change Cipher Spec Protocol)

-Sends the finished message under the new algorithms, keys, and secrets — key exchange and authentication processes were successful

Server: change_cipher_spec, sends finished message

Complete Handshake

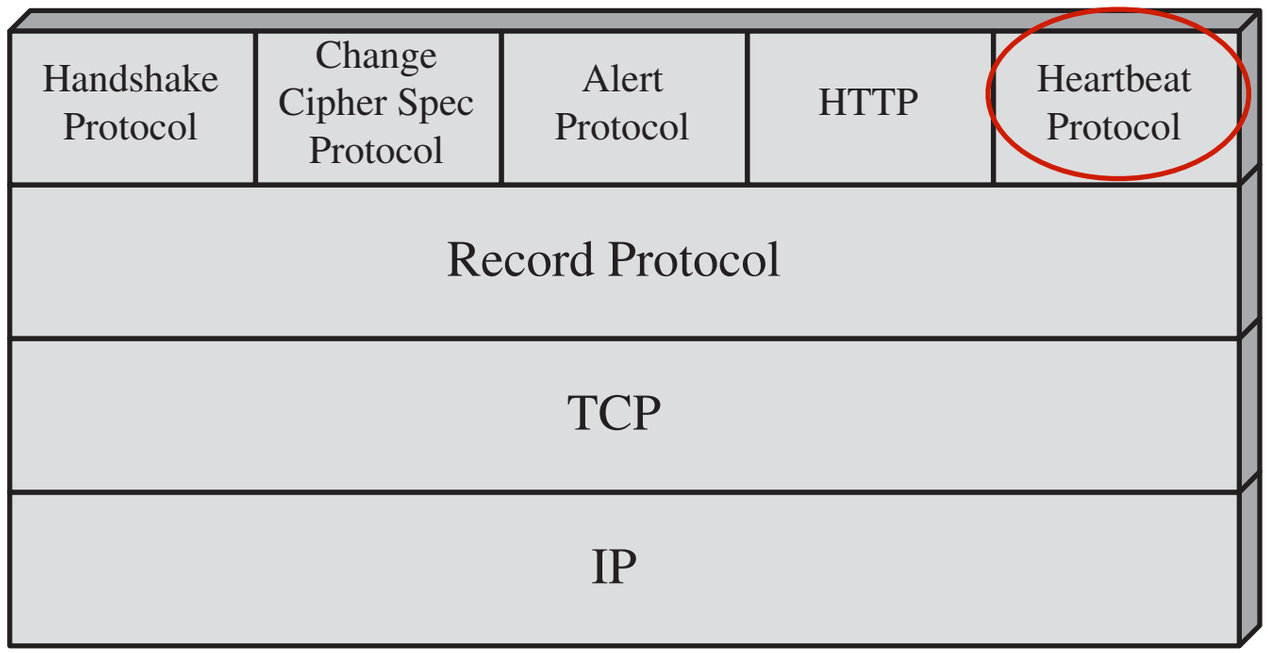


Transport Layer Security (TLS): Protocols

- Heartbeat Protocol

  Heartbeat is a periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system.

  - runs on top of the TLS record protocol
  - message types: heartbeat_request & heartbeat_response
  - established during Handshake Protocol Phase 1
  - Purpose: 1) recipient is still alive 2) avoids closure by a firewall that does not tolerate idle connections



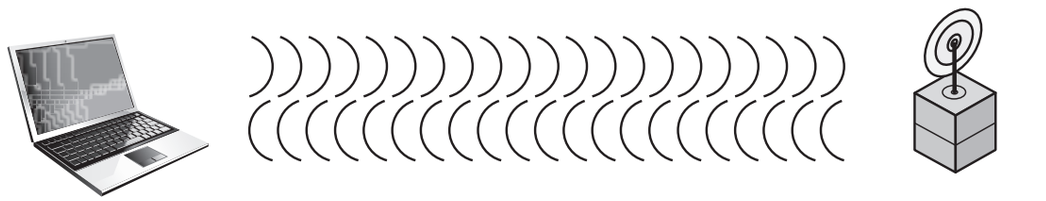
SSL/TLS Protocol Stack

Transport Layer Security (TLS): Attack

- SSL/TLS Exhaustion DDoS Attack
  - Targets the SSL handshake protocol
  - Sends worthless data to a target SSL server
  - Extra workload to process garbage data as a legitimate handshake
  - Firewalls don't help in this case because they are usually not capable of differentiating between valid and invalid SSL handshake packets

Wireless Security

- All security threats and countermeasures discussed in wired networks
- Unique aspects in wireless environment —> higher risk
  - Channel: broadcast communication —> eavesdropping, jamming
  - Resources: smartphones and tablets have sophisticated operating systems but limited memory and processing resources to counter threats —> DoS, malware
  - Accessibility: some wireless devices may be left unattended in remote and/or hostile location (e.g., sensors and robots) —> physical attacks
  - Mobility —> accidental association, malicious association

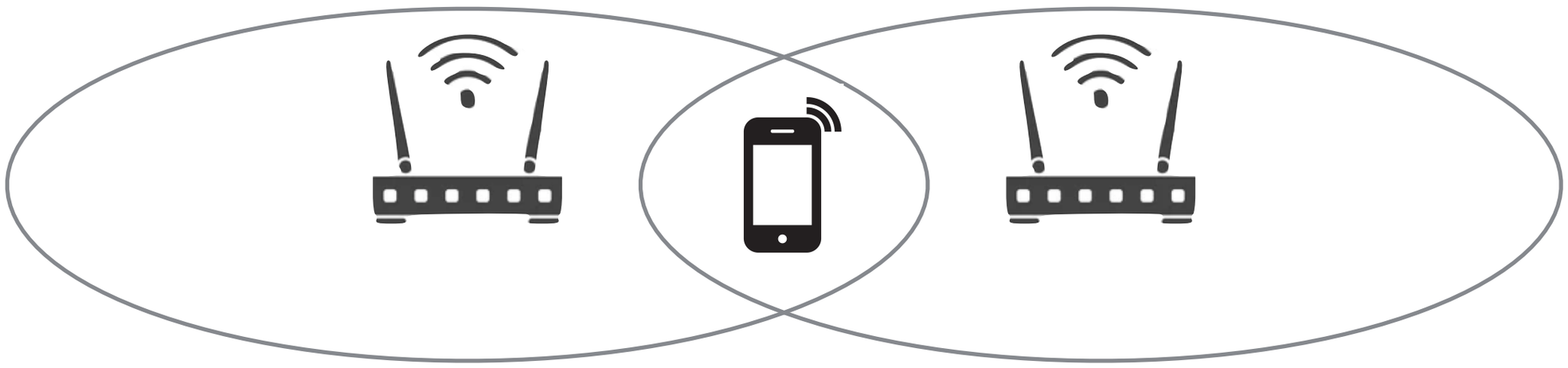


Wireless Network Threats

- Accidental association
- Malicious association
- Ad hoc networks
- Nontraditional networks
- Man-in-the middle attacks
- Denial of service (DoS)
- …

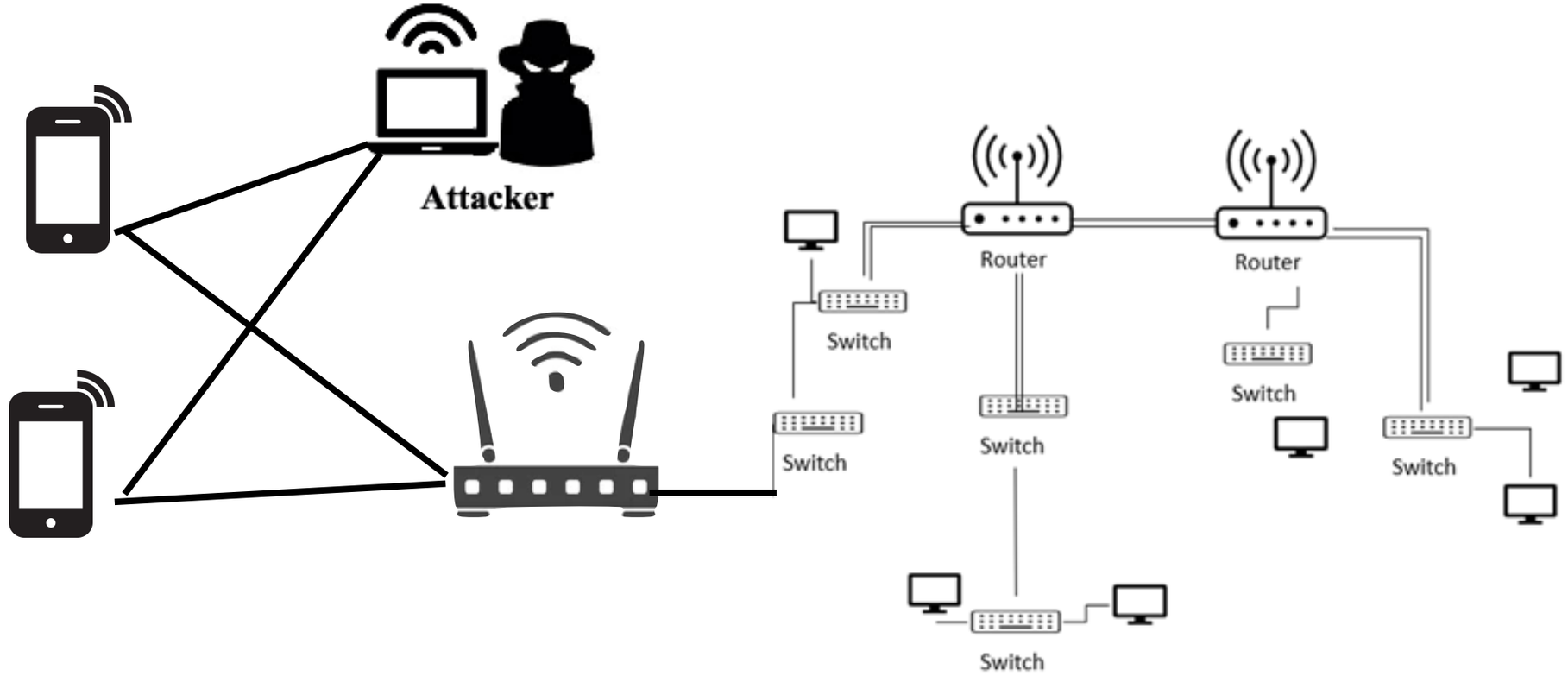
Wireless Network Threats

- Accidental association: A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network — exposes resources of one LAN to the accidental users



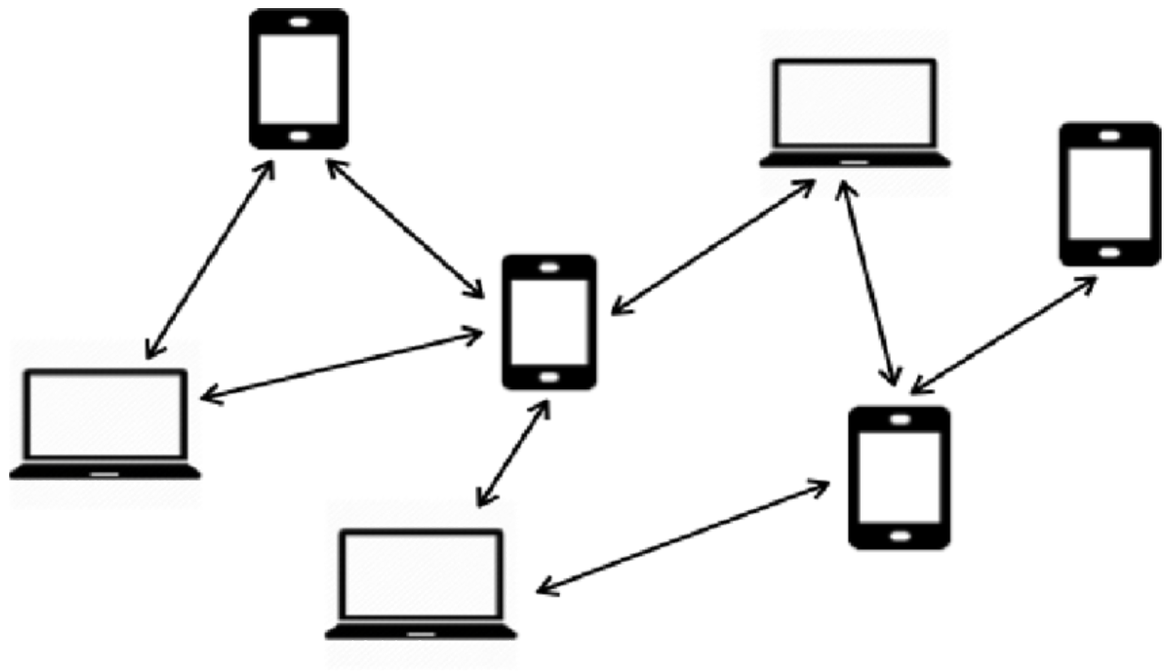
Wireless Network Threats

- Malicious association: a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.



Wireless Network Threats

- Ad hoc networks: peer-to-peer networks between wireless devices with no access point between them. This can pose a security threat due to a lack of a central point of control.

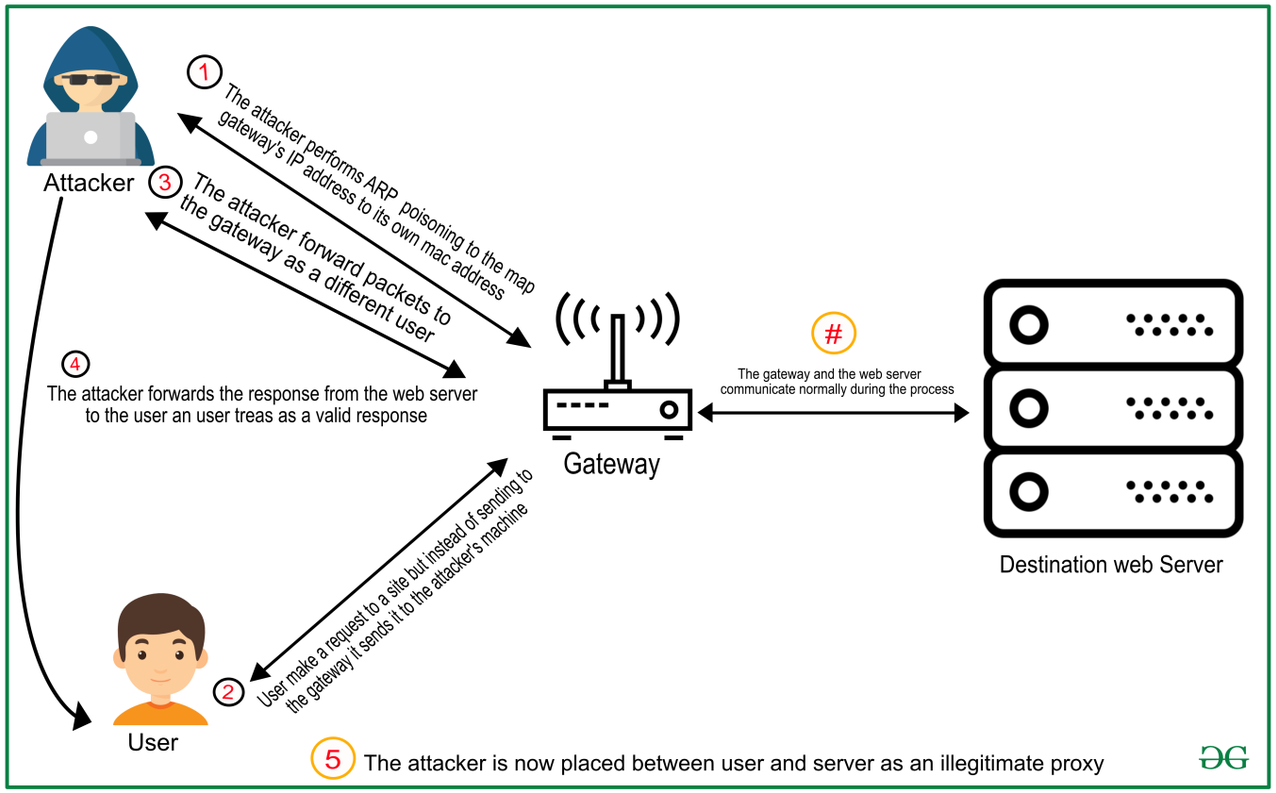


Wireless Network Threats

- Nontraditional networks: personal network Bluetooth devices, barcode readers, and handheld PDAs pose a security risk both in therms of eavesdropping and spoofing.

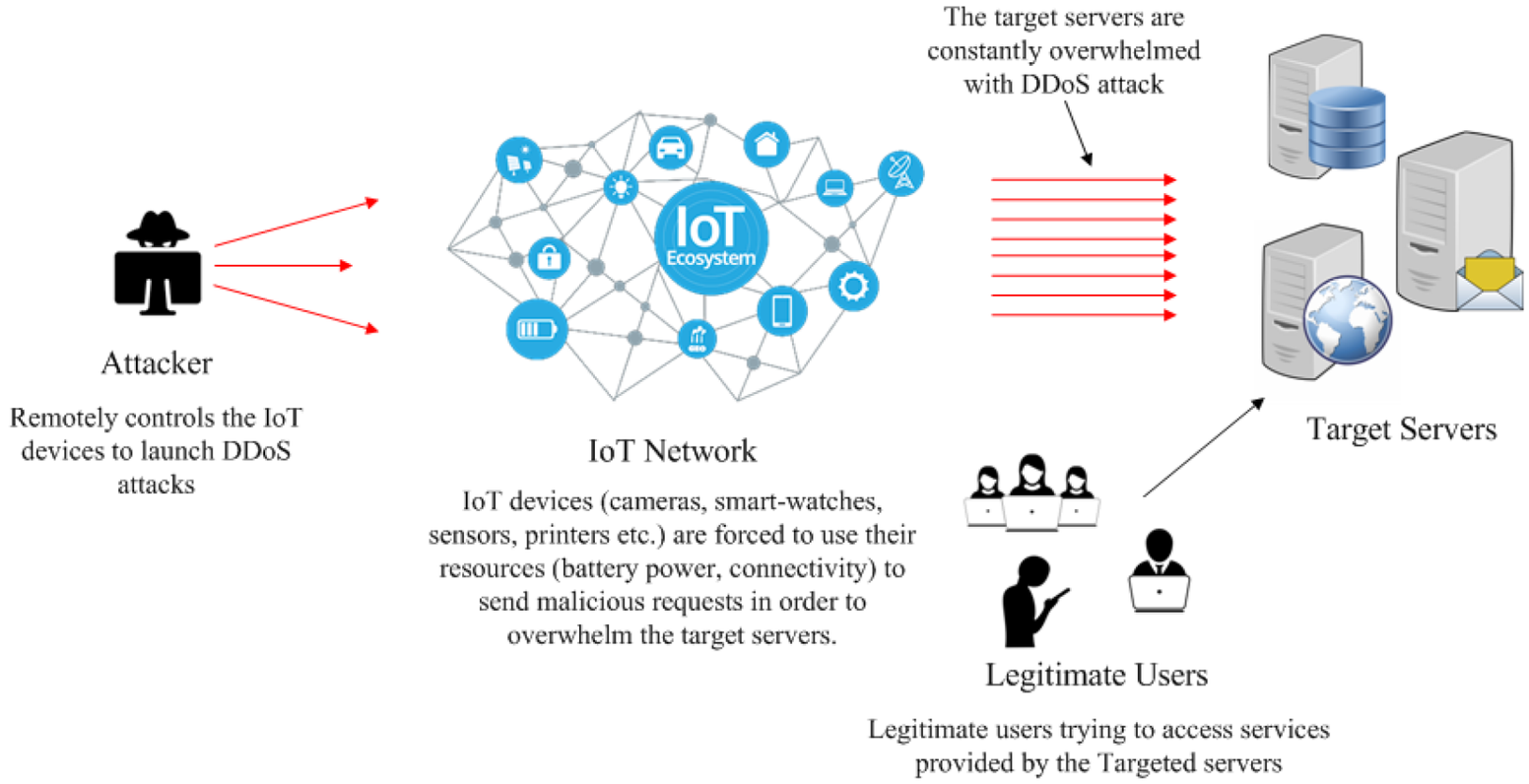
Wireless Network Threats

- Man-in-the middle attacks: In a broader sense, this attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device. Wireless networks are particularly vulnerable to such attacks.



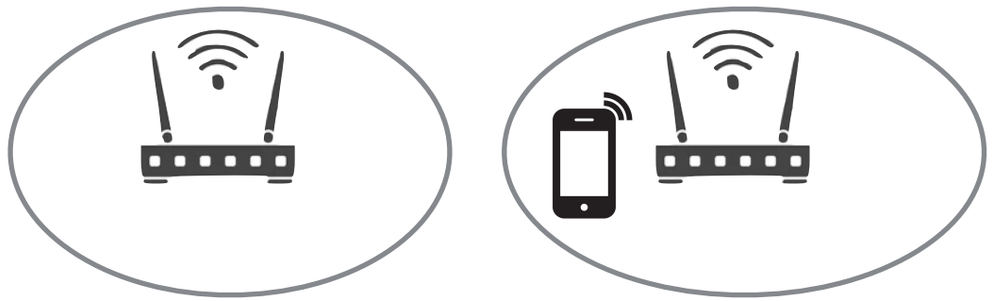
Wireless Network Threats

- Denial of service (DoS): an attacker continually bombards a wireless access point with various protocol messages designed to consume system resources. The wireless environment lends itself to this type of attack, because it is so easy for the attacker to direct multiple wireless messages at the target.



Wireless Security Measures

- Secure wireless transmissions
  - Signal-hiding techniques: make it more difficult for an attacker to locate their wireless access points (e.g., reducing signal strength, directional antennas, signal-shielding …)



  - Encryption

Wireless Security Measures

- Secure wireless networks
  - Use encryption for router-to-router traffic
  - Use anti-virus and anti-spyware software, and a firewall
  - Turn off identifier broadcasting: Wireless routers are typically configured to broadcast an identifying signal so that any device within range can learn of the router's existence. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.
  - Change the identifier on your router from the default
  - Change your router's pre-set password for administration
  - Allow only specific computers to access your wireless network

Wireless Security Measures

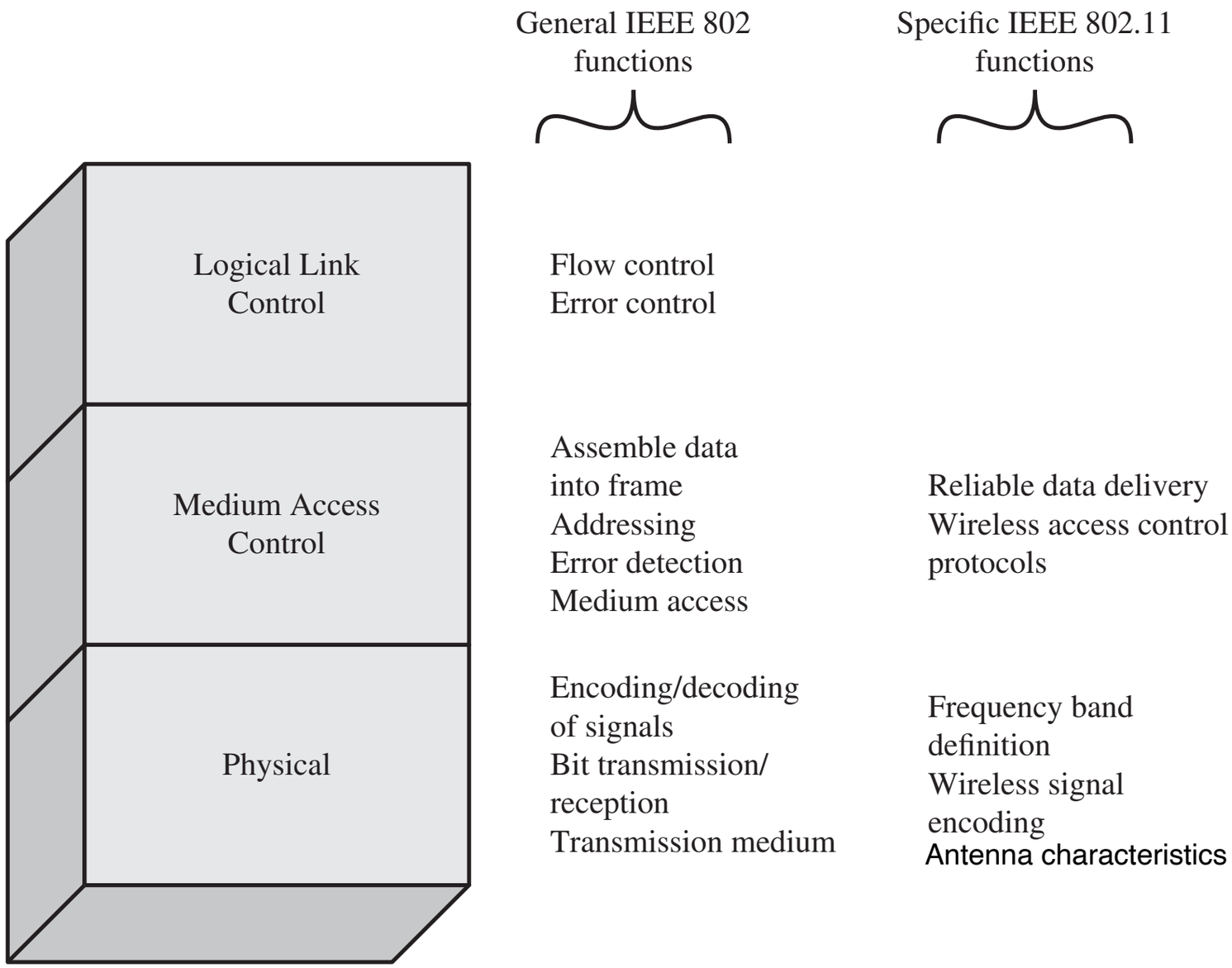
- Secure wireless access points
  - IEEE 802.1X standard for port-based access control
  - Provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
  - The use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

IEEE 802.11 Wireless LAN

- IEEE 802 is a committee that has developed standards for a wide range of local area networks (LANs)
- In 1990, IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs).

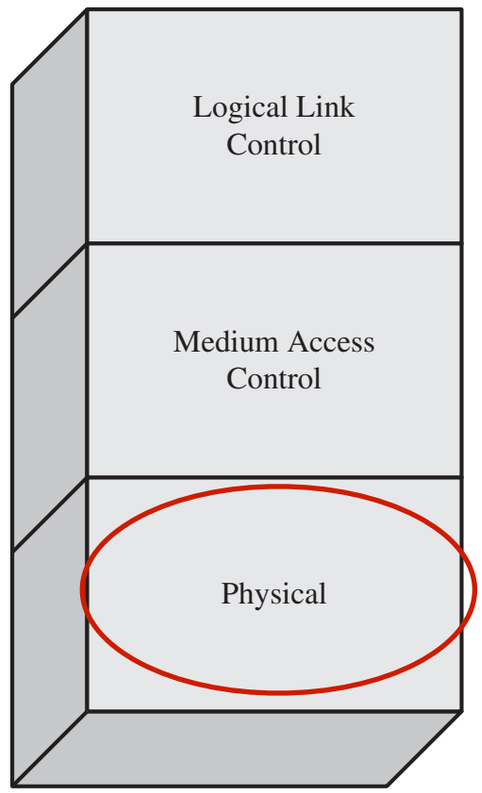
IEEE 802.11 Protocol Architecture

- Layered Protocol Stack



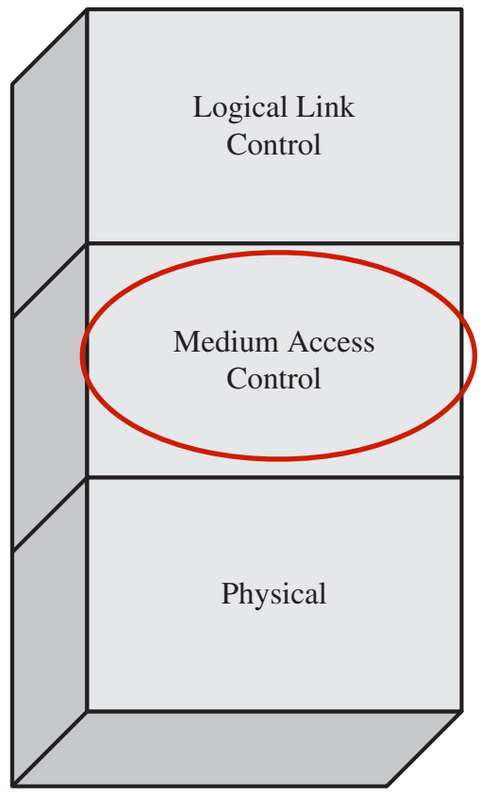
IEEE 802.11 Protocol Architecture

- Physical layer
  - Signal encoding/decoding
  - Bit transmission/reception
  - Specification of the transmission medium
  - For IEEE 802.11: frequency bands and antenna characteristics



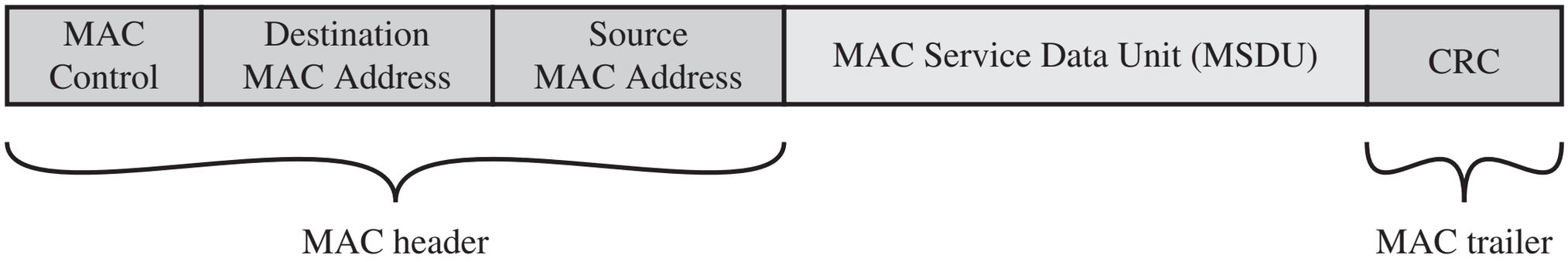
IEEE 802.11 Protocol Architecture

- Medium access control: receives data from a higher-layer protocol, typically the logical link control (LLC) layer, in the form of a block of data — MAC service data unit (MSDU). In general, the MAC layer performs the following functions:
  - On transmission, assemble data into a frame — MAC protocol data unit (MPDU) with address and error-detection fields.
  - On reception, disassemble frame, and perform address recognition and error detection.
  - Govern access to the LAN transmission medium.



IEEE 802.11 Protocol Architecture

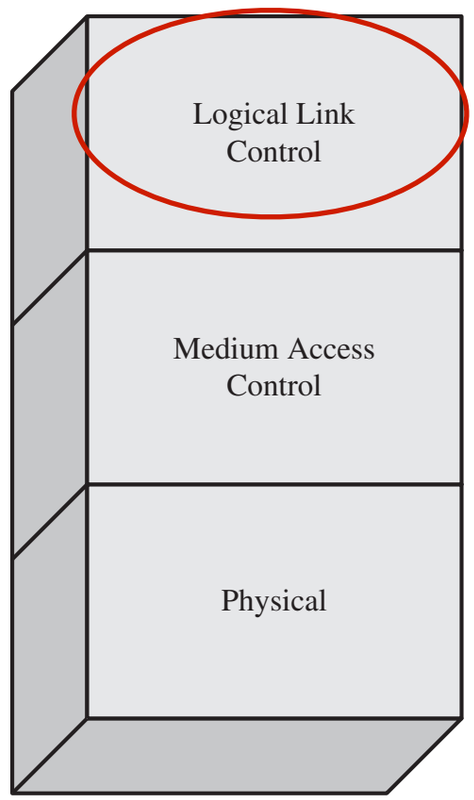
- Medium access control
  - MAC protocol data unit (MPDU)



- MAC control: This field contains any protocol control information needed for the functioning of the MAC protocol. e.g., a priority level could be indicated here.
- MAC service Data Unit: The data from the next higher layer
- CRC: The cyclic redundancy check field.This is an error-detecting code, such as that which is used in other data-link control protocols. The CRC is calculated based on the bits in the entire MPDU.

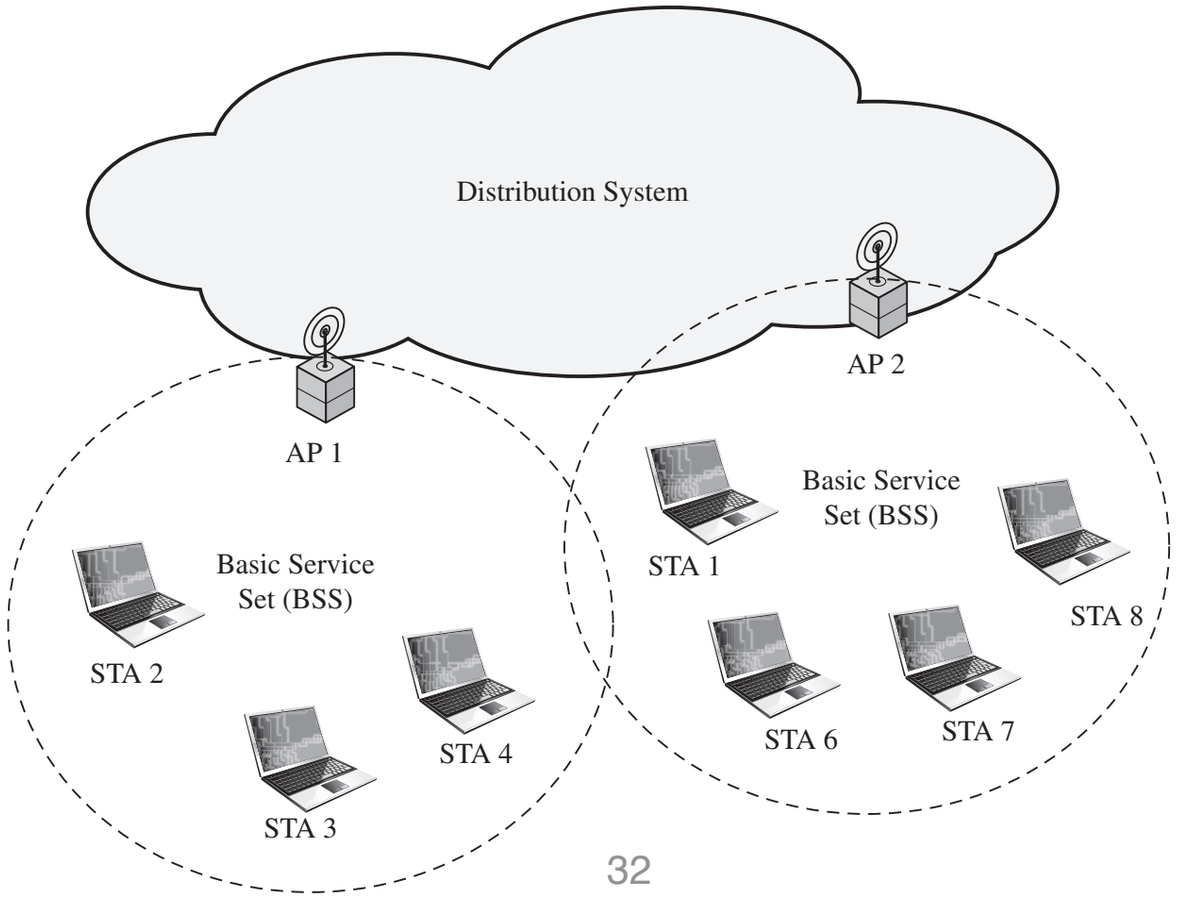
IEEE 802.11 Protocol Architecture

- Logical link control (LLC)
  - MAC layer is responsible for detecting errors and discarding any frames that contain errors.
  - The LLC layer optionally keeps track of which frames have been successfully received and retransmits unsuccessful frames.



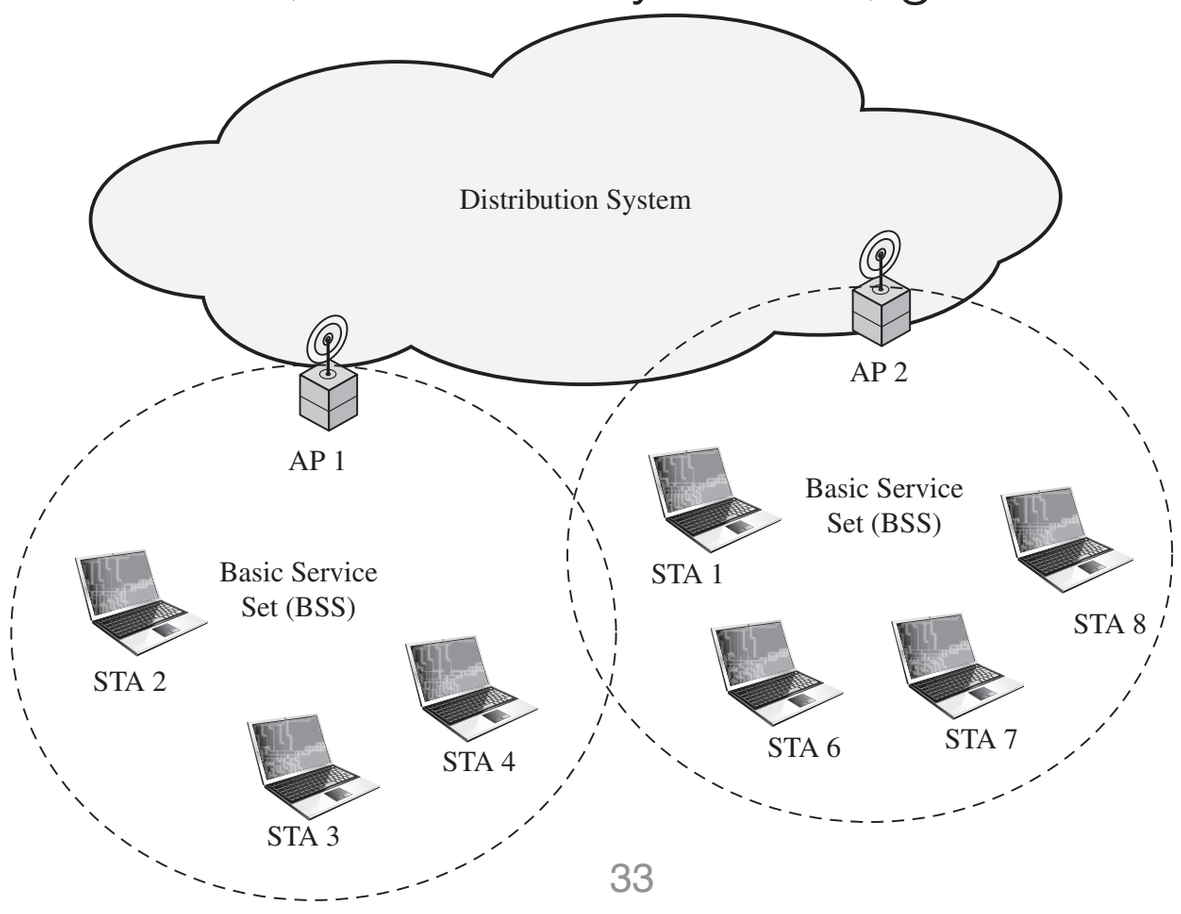
IEEE 802.11 Network Architectural Model

- Smallest building block: basic service set (BSS)
  - BSS may be isolated or connect to a backbone distributed system through an access point (AP)
  - Client stations do not communicate directly, but use AP as a relay: MAC frame is first sent from original station to AP and then from AP to the destination station.



IEEE 802.11 Network Architectural Model

- Smallest building block: basic service set (BSS)
  - BSS = cell; DS can be a switch, a wired network, or a wireless network
  - Independent BSS: ad hoc network, mobile stations communicate directly with one another and no AP is involved.
  - A single station could participate in more than one BSS
  - Dynamic association; stations may turn off, go in/out of range.



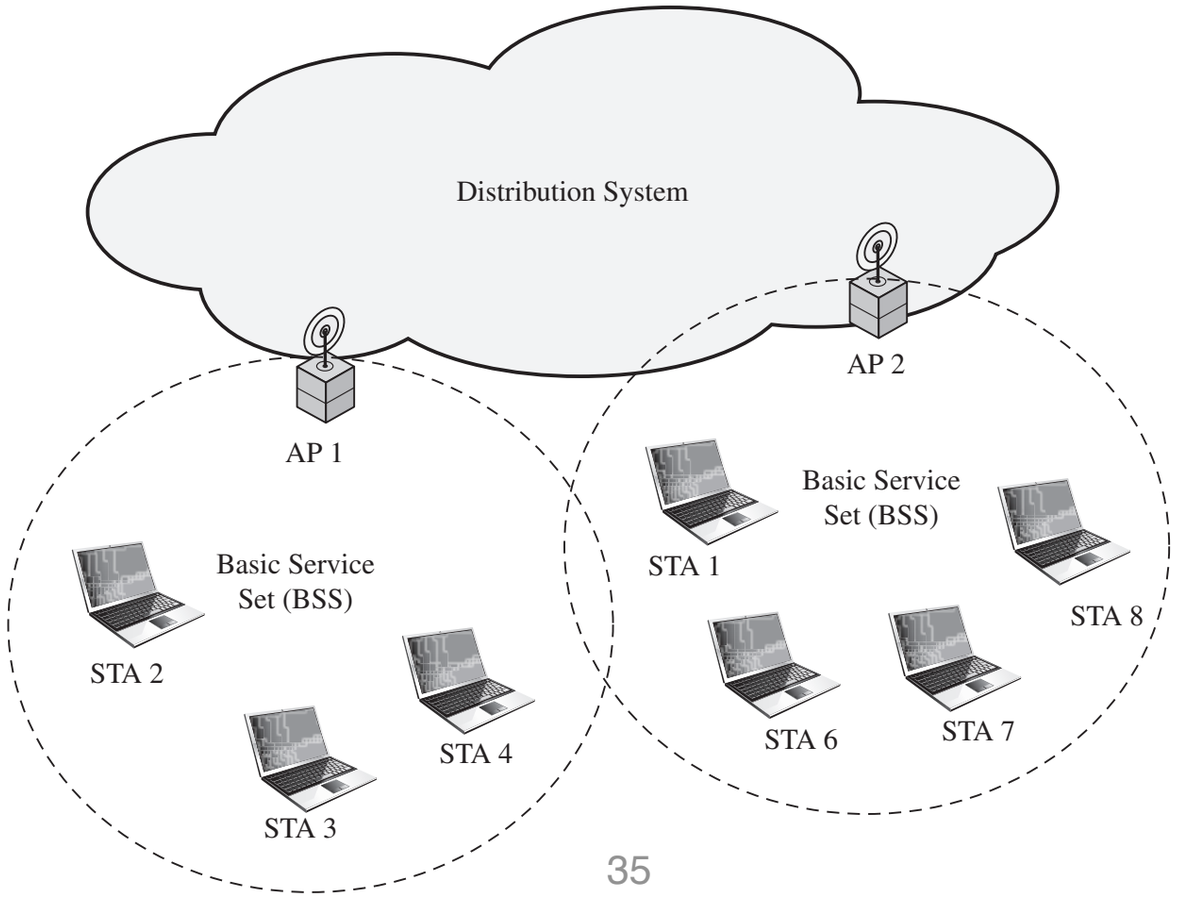
IEEE 802.11 Services

- The service provider can be either the station or the DS.
- (De)authentication, privacy for control access and confidentiality
- Other services for supporting delivery

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

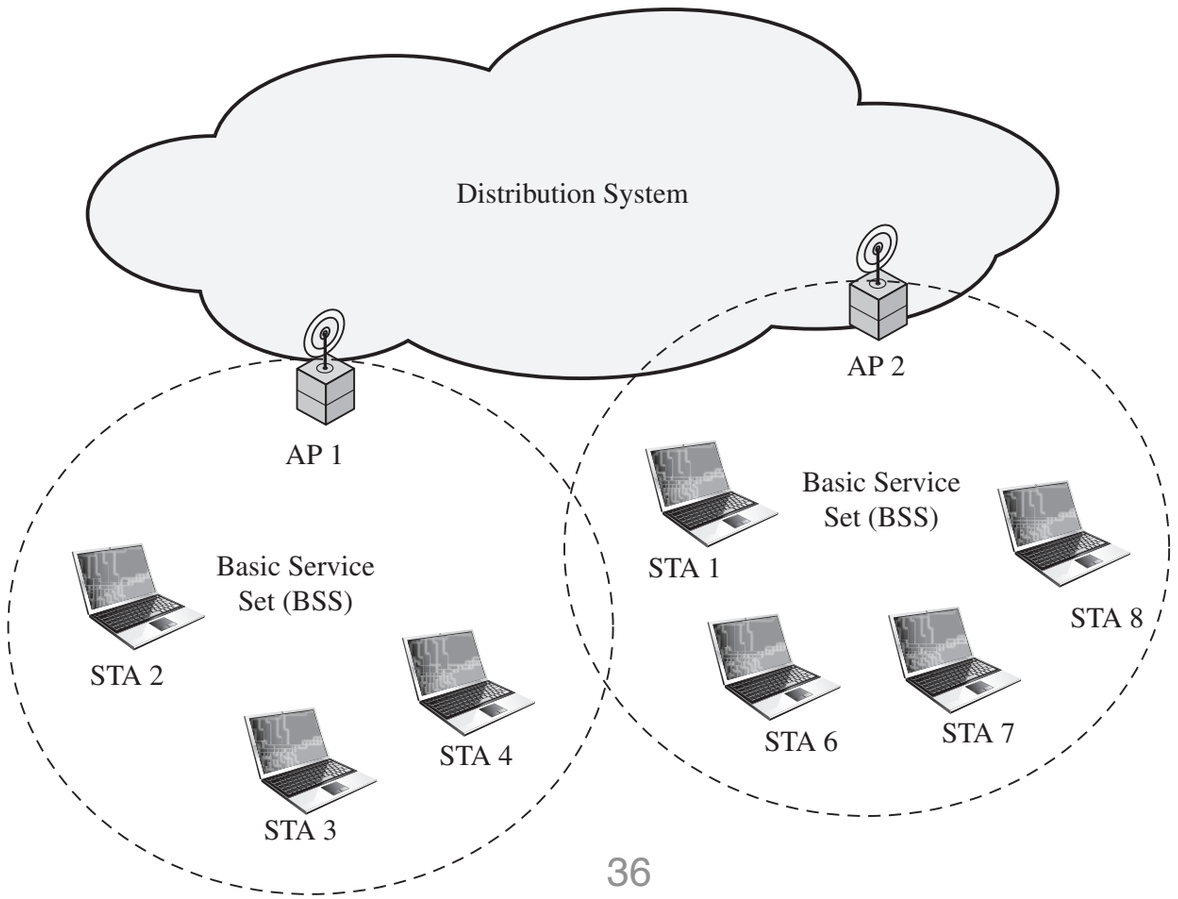
IEEE 802.11 Services

- Distribution and Integration
  - **Distribution** is the primary service used by stations to exchange MAC protocol data units (MPDUs) when the MPDUs must traverse the distributed system (DS) to get from a station in one basic service set (BSS) to a station in another BSS. [e.g., STA 2 —> STA 7]



IEEE 802.11 Services

- Distribution and Integration
  - The **integration** service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN.
  - "Integrated" refers to a wired LAN that is physically connected to the DS and whose stations may be logically connected to an IEEE 802.11 LAN via the integration service.

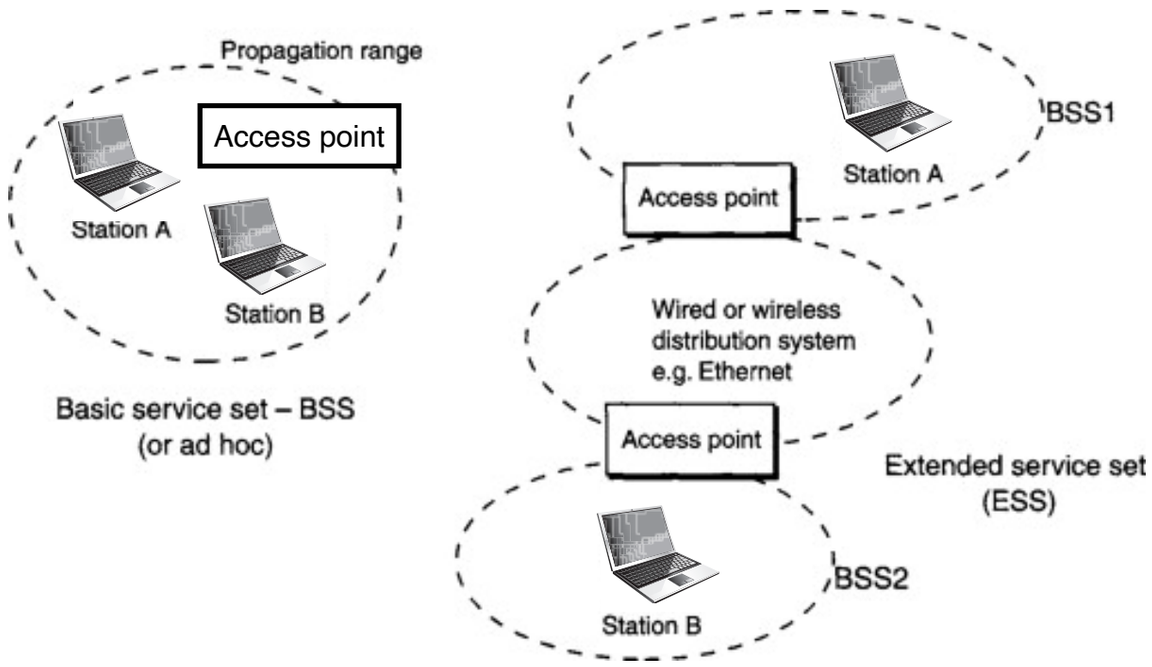


IEEE 802.11 Services

- Association-Related Services

  Before the distribution service can deliver data or accept data from a station, that station must be associated.

  - Transition Types
    - No transition: A station is either stationary or moves within the range of a single BSS
    - BSS transition: A station moves from one BSS to another BSS within the same ESS
    - ESS transition: A station moves from a BSS in one ESS to a BSS within another ESS (802.11 cannot be guaranteed, disruption is likely to occur)



IEEE 802.11 Services

- Association-Related Services

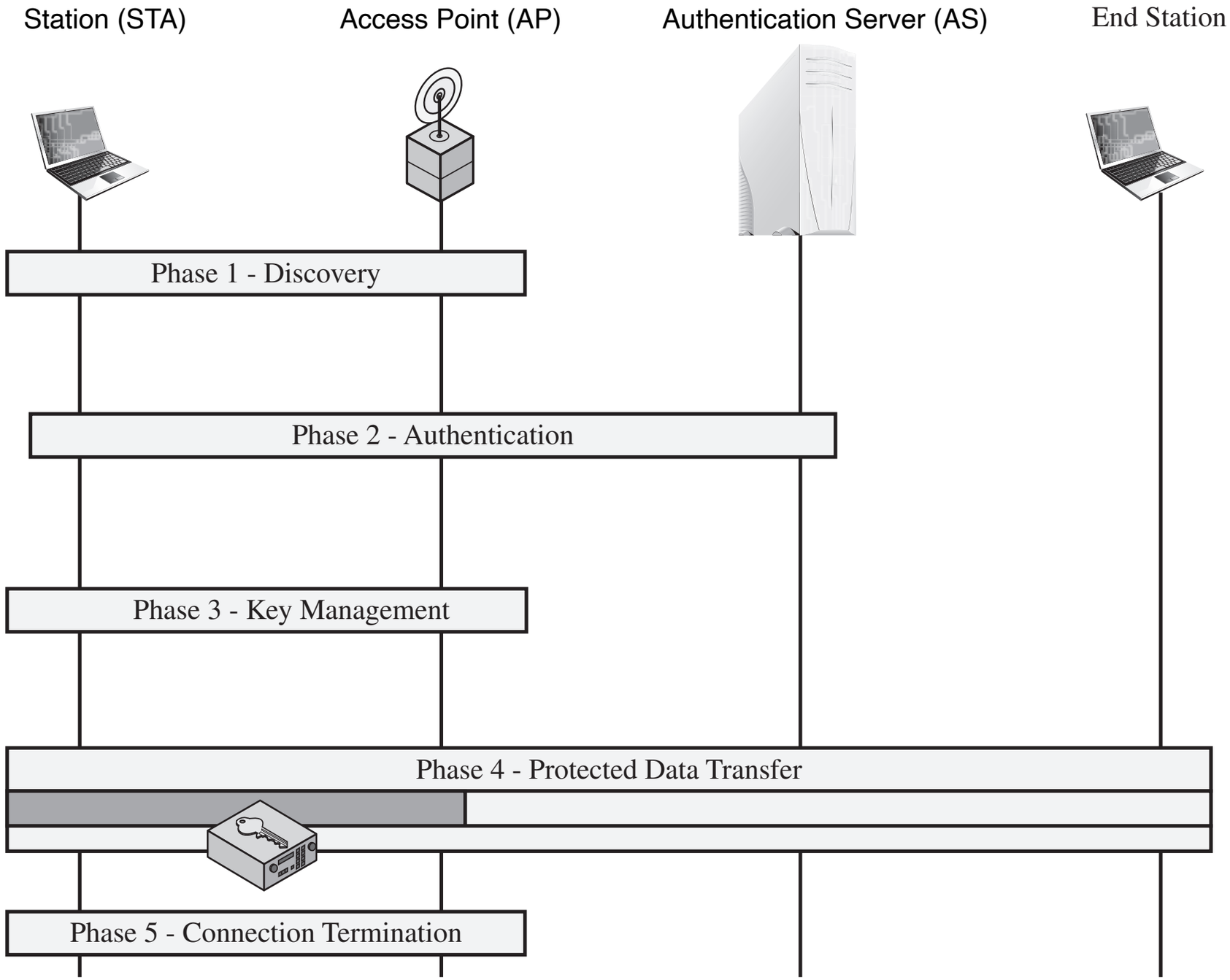
  Distributed system need to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station.
  — A station must maintain an association with the AP within its current BSS.

  - **Association**: Establishes an initial association between a station and an AP. The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.
  - **Reassociation**: Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
  - **Disassociation**: A notification from either a station or an AP that an existing association is terminated. A station should give this notification before leaving an ESS or shutting down.

IEEE 802.11i Wireless LAN Security

- 802.11i standard is referred to as Robust Security Network (RSN)
- IEEE 802.11i security is concerned only with secure communication between **station** and its **access point**, i.e. within each BSS.

IEEE 802.11i Operation



IEEE 802.11i Operation

- Phase 1 Discovery
  - An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy.
  - The STA identifies an AP for a WLAN with which it wishes to communicate.
  - The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.

IEEE 802.11i Operation

- Phase 2 Authentication
  - STA and AS prove their identities to each other.
  - The AP blocks nonauthentication traffic between the STA and AS until the authentication transaction is successful.
  - The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.

IEEE 802.11i Operation

- Phase 3 Key Management
  - The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA.
  - Frames are exchanged between the AP and STA only.

IEEE 802.11i Operation

- Phase 4 Protected data transfer
  - Frames are exchanged between the STA and the end station through the AP.
  - Secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.

IEEE 802.11i Operation

- Phase 5 Connection termination
  - The AP and STA exchange frames.
  - The secure connection is torn down and the connection is restored to the original state.

Summary

- SSL/TLS
  - Protocol Architecture
  - Connection & Session
  - Protocols
  - Attack
- Wireless Network Security
  - Wireless environment —> higher security risk
  - Wireless Security Measures
  - IEEE 802.11 Wireless LAN: protocols, network model, services
  - IEEE 802.11i Wireless LAN Security: operations

Thank You

Quiz Time

- 15 minutes