NSR/AS

# Wireless LAN Network Security

Lecture Twenty-five

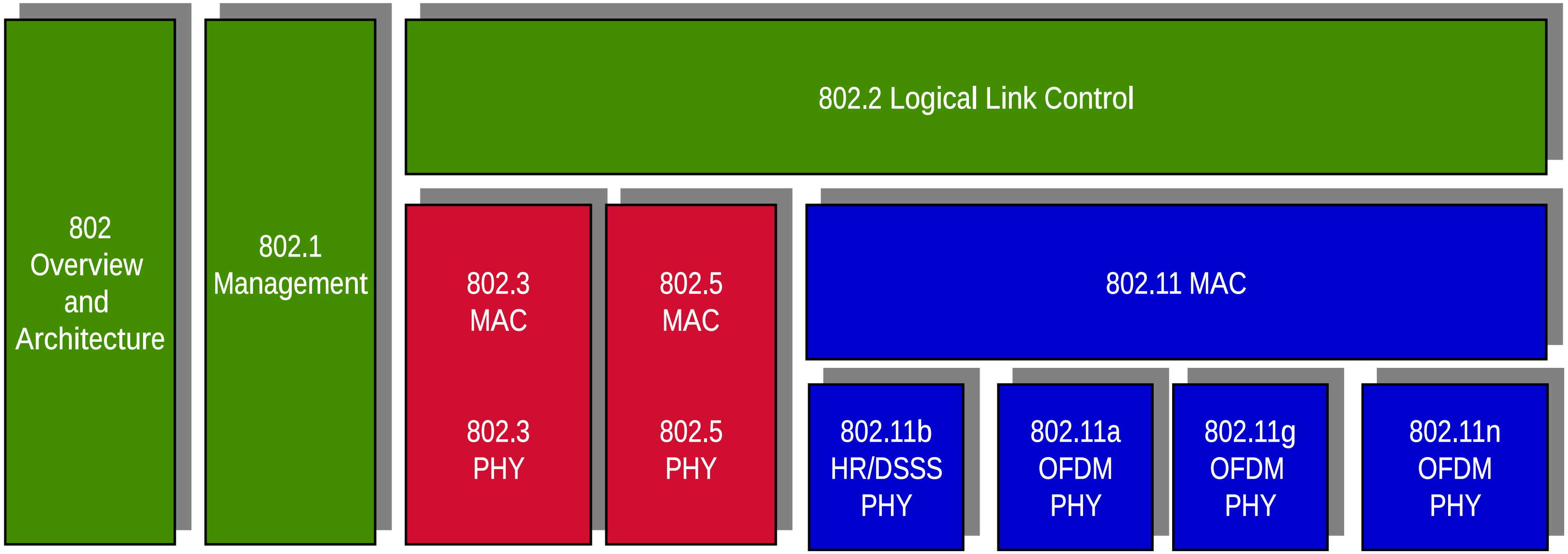
# Outline of Lecture

- Overview of WLAN
- WLAN security

# Wireless LAN

- Wireless Local area network
- Developed by IEEE 802.11 task groups
- A number of sub-groups. Main ones
  - a, b, g, n, ac transmission protocols
  - e Quality of service
  - i enhanced security
  - Many other groups dealing with interworking, network management, mobility etc.
- Uses ISM bands around 2.4 GHz and 5 GHz

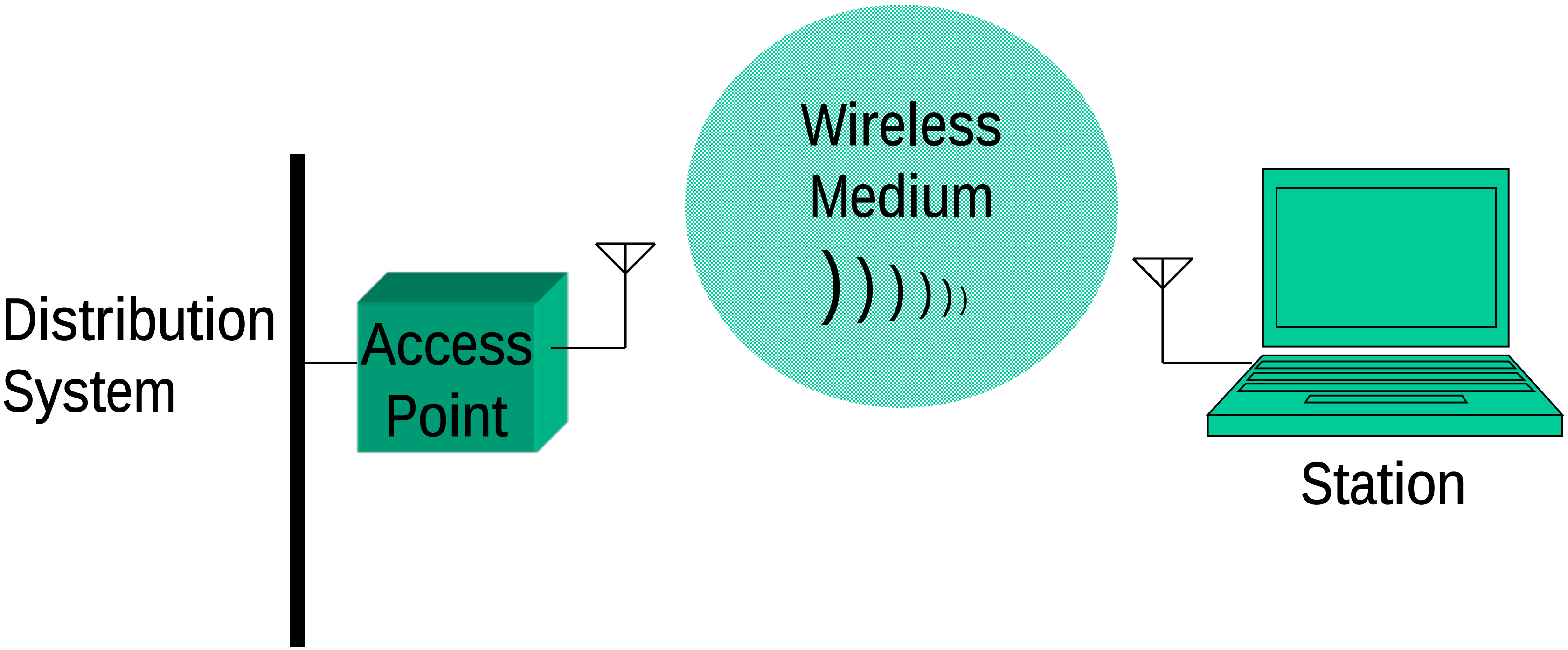
# IEEE 802 Network Protocols



# 802.11 Requirements

- Requirements
  - Purpose is to provide layer 2 connectivity only
  - Carries higher layer traffic (TCP/IP)
  - Single MAC layer for different physical layer technologies
  - Allow multiple overlapping networks (shared band)
  - Handle interference from other ISM band radios and microwave ovens
  - Privacy and access control

# 802.11 Architecture



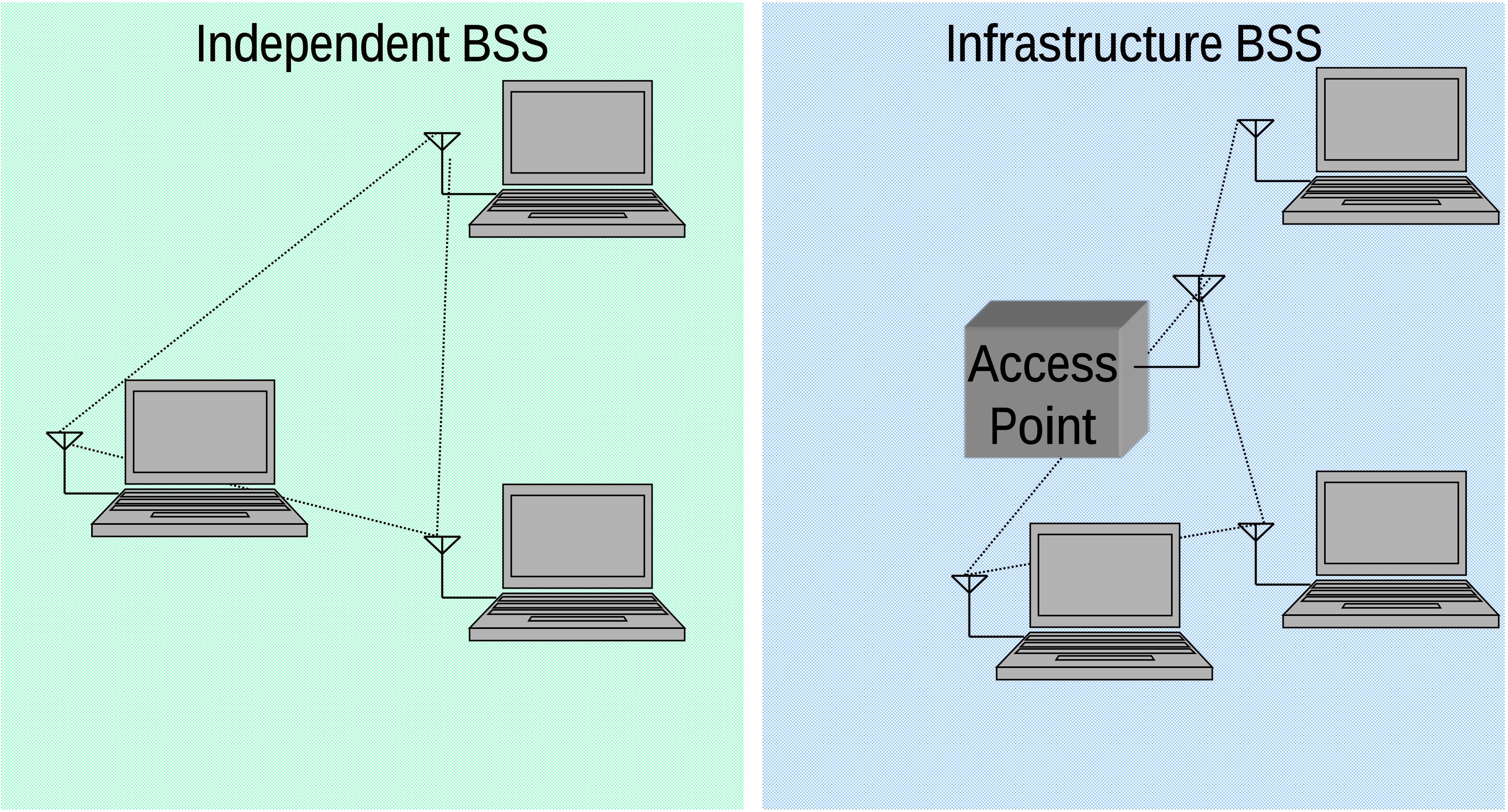
# 802.11 Architecture

- Shared medium
  - Broadcast channel
  - Issue of sharing channel amongst distributed users
- Distribution System
  - Used to connect multiple Access Points to form a coverage area
  - Usually Ethernet
- Access Point
  - Bridge between distribution system and wireless medium
- Wireless Medium
  - RF in the 2.5 and 5.0 GHz ranges
- Station
  - Computing device with wireless network interface cards

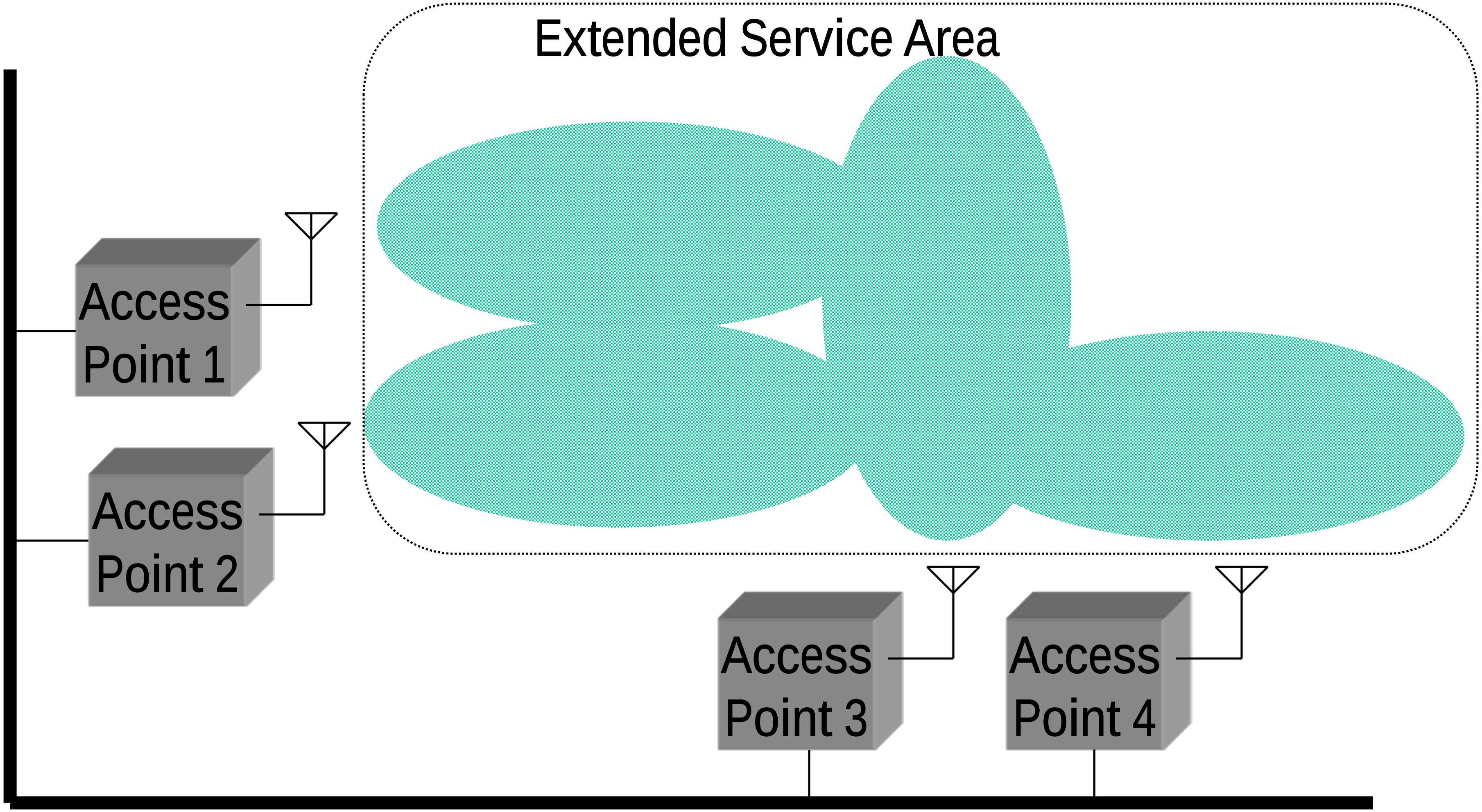
# 802.11 Network Types

- Basic Service Set
  - Group of stations that communicate
- Basic Service Area
  - Coverage of wireless medium
- Two types of networks
  - Independent BSS
    - All stations in Basic Coverage area communicate directly
    - Ad-hoc network
  - Infrastructure BSS
    - Stations communicate via an access point
- Can link multiple infrastructure BSS into Extended Service Sets

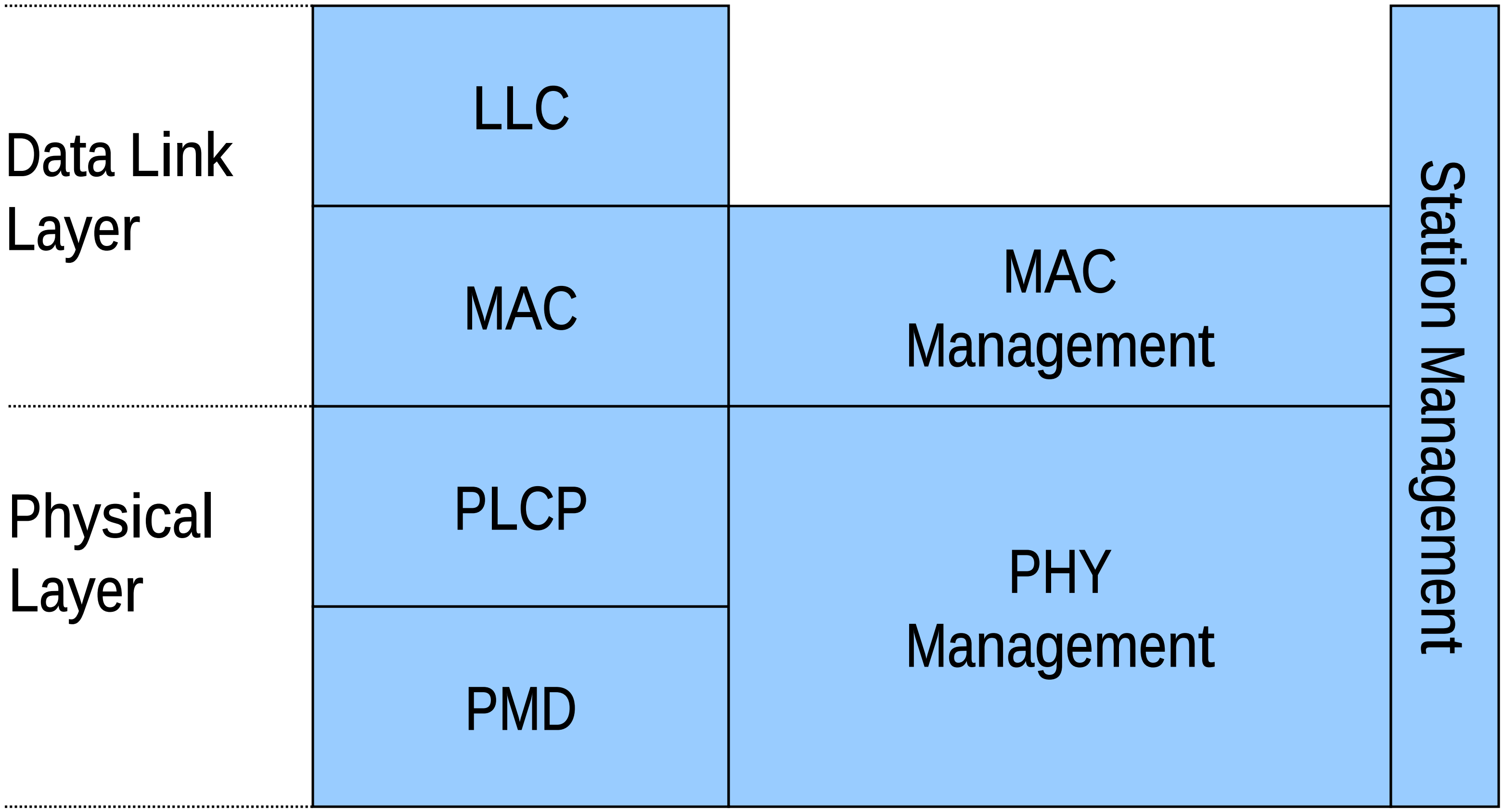
# 802.11 Network Types



# Extended Service Area



# 802.11 Protocol Stack



# MAC Layer

- Familiar problem of sharing a common channel
  - Ethernet uses CSMA/CD
  - Bluetooth uses a Master-slave to specify who can transmitt
  - GSM uses slotted ALOHA in the Random Access Channel
- 802.11 uses CSMA/CA
  - Carrier Sense Multiple Access / Collision Avoidance
  - Station monitors the channel ("Carrier Sensing") before transmitting
  - All transmitted frames are acknowledged
  - Collisions are avoided by a station sending messages to gain the channel before sending frames
    - Optional

# MAC Access Modes

- Two mechanisms for accessing the shared radio medium
- Distributed Coordination Function (DCF)
  - Checks to see if radio link is clear
  - Waits a random backoff time each frame when channel is clear
  - Optionally uses CTS/RTS to avoid collisions
    - CSMA/CA
- Point Coordination Function (PCF)
  - Infrastructure networks only (Access Points)
  - PCF allows stations to transmit frames earlier than DCF

# WLAN Attacks

- WLAN susceptible to the same attacks at the application and transport layer as all IP networks
  - Application layer
    - HTTP drive-by downloads etc
  - Transport layer
    - SYN flooding, Session hijacking, etc
  - IP layer
    - Smurf attacks (ping flooding), IP spoofing etc
- WLAN is also susceptible to new forms of attacks at the Physical and Data link layers

# Physical layer attacks

- 802.11 operate on different frequency bands around 2.4 GHz and (less commonly) 5 GHz
  - Industrial, Scientific, Medical band
  - A lightly regulated, publicly available band
- Plenty of (non malicious) devices create noise in 2.4 GHz range
  - DECT cordless phones, Microwave ovens, Bluetooth
  - Operating these devices in proximity to WLAN will affect capacity
    - Devices that are faulty or malicious may completely disable a WLAN
- Easy to build devices that produce noise around this frequency

# Data link layer attacks

- Much scope for malicious attacks at the WLAN Data link layer
  - Broadcast MAC
  - Weak encryption
  - Weak authentication
  - Distributed control
  - Resource allocation based on interframe spacings
- Easy for a non-conforming station to subvert WLAN MAC layer
  - DOS attacks
  - Man in the middle attacks
  - Illicit use

# DOS Attacks

- Flooding
  - Because of lower bandwidth compared with Ethernet a host attached to a WLAN can easily be overwhelmed by DDoS traffic
- Interframe spacing attacks
  - Priorities in WLAN determined by nature of frame to be transmitted
  - Priority given by different waiting times for access to wireless medium
    - SIFS, PIFS, DIFS
  - A misbehaving workstation can ignore interframe spacing and transmit messages without waiting for appropriate interframe spacing
    - Can be used as a DOS or just to gain unfair access to bandwidth

# Man in the middle attacks

- Eavesdropping
  - Broadcast nature of WLAN means that no special effort is needed to listen in on messages
  - Just have to be in range and listening to appropriate ISM band
- Manipulation
  - Can masquerade as another party
    - Take over sessions already in operation using TCP hijack

# ARP Poisoning

- Can use WLAN to intercept communications between two wired stations
  - ARP poisoning
- ARP Cache
  - contains mapping of MAC to IP address
  - Mapping can be obtained two ways:
    - ARP requests
      - Who has IP address 192.168.0.1?
    - Receipt of packets from hosts on the same LAN
      - Lazy ARP (most common)

# ARP Poisoning

- Attacker can force packets to go through a malicious host by exploiting Lazy ARP
  - Attacker wishes to intercept communications between client (192.168.0.99) and server (192.168.0.1)
  - Attacker on same LAN segment as server and client
  - Attacker sends a message to the client with IP address of server but MAC address of attacker
  - Attacker sends a message to the server with IP address of client but MAC address of attacker
  - All traffic will be sent to the attacker even if the client and server are on a wired, switched network
  - Attacker can watch, drop, forward or manipulate data

# WLAN component security

- Station
  - Mobile station
    - laptop, PDA
- Access point
  - Interface between wired and wireless network
  - Can be layer 2 or 3
- Gateway
  - Wireless capable Firewall

# WLAN Station security

- Secure communication
  - Should use some form of encryption
  - Should be regarded as mandatory for wireless communication
    - Look at options later in the lecture
- Audit logging should be considered
  - Use some exception notification to warn of attempted attacks
- Static ARP should also be considered
  - If always using the same gateway then ARP should be configured with a static ARP entry
  - Will override any dynamic ARP information

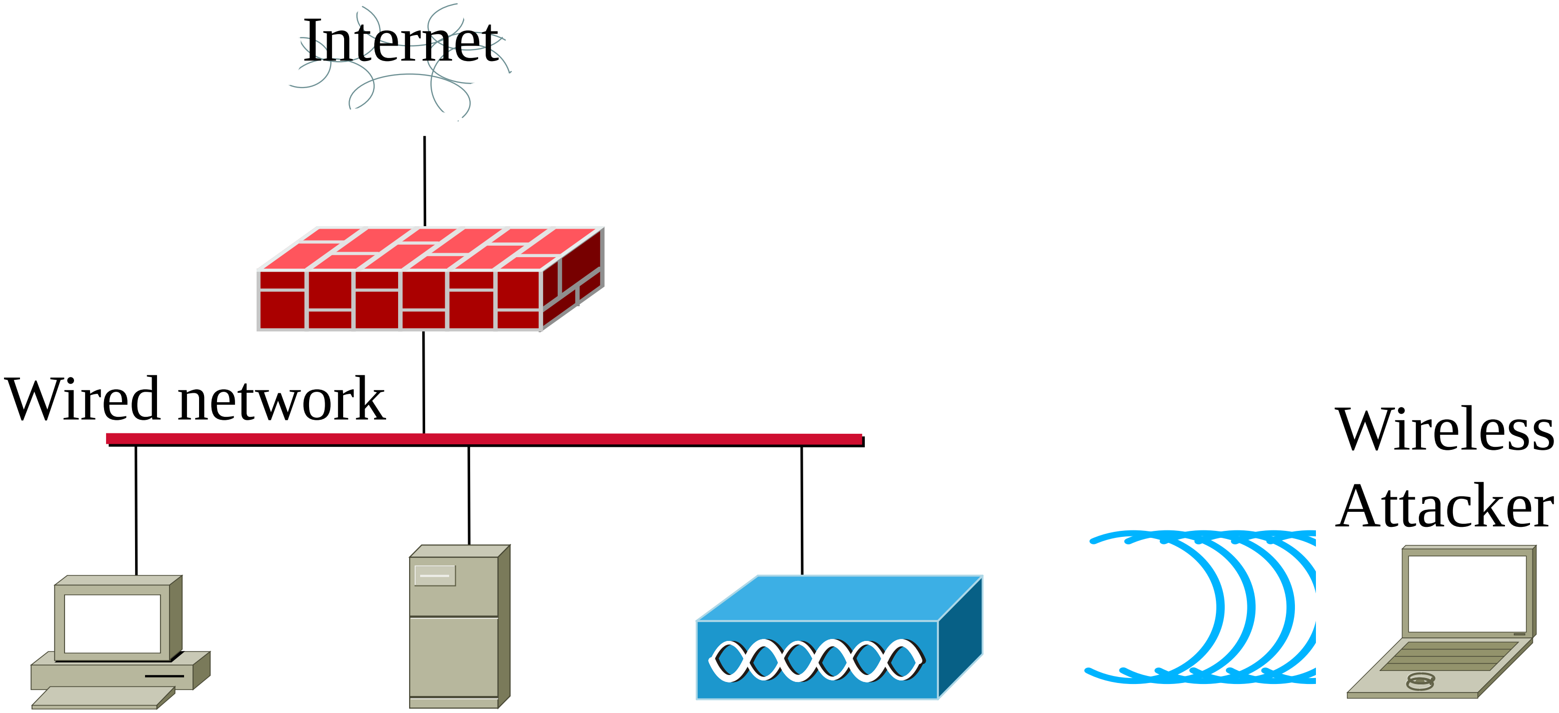
# WLAN Access Point Security

- Should configure and use available encryption
- Should use MAC address filtering where possible
  - Only allow communication to and from specific devices based on MAC address
- Management interfaces need to be well protected and probably disabled
  - Most APs have an administration interface accessed through HTTP, Telnet or USB
    - Telnet should be avoided if possible
    - Administration interfaces should be disabled after configuration

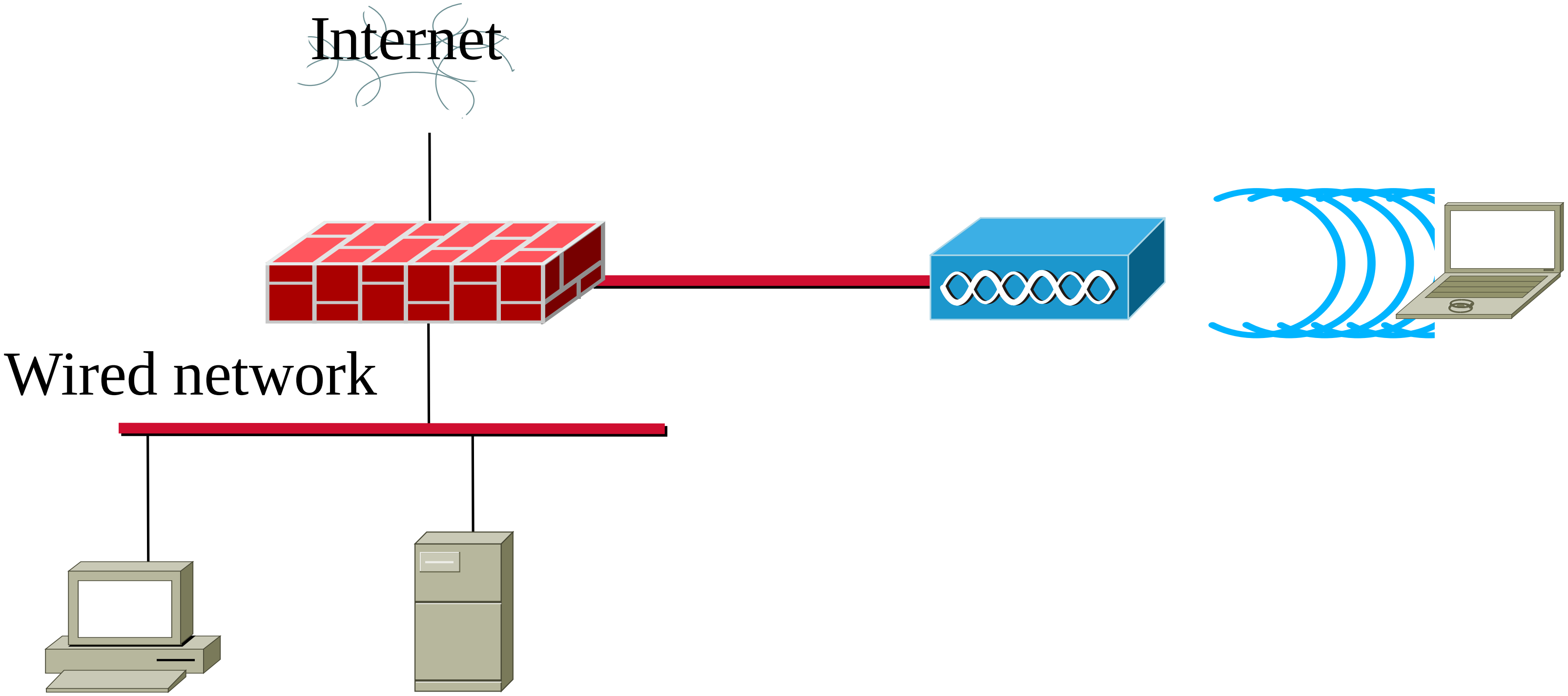
# WLAN Gateway/Firewall Security

- Important to separate wired network from wireless network
  - Prevents ARP poisoning attacks
- Most commonly done with a WLAN Gateway/Firewall
- Multiple Access Points form a single SSID
  - No reason for communication between stations connected to the same SSID
  - Firewall should prohibit direct communications between mobile stations
    - Bridging firewall

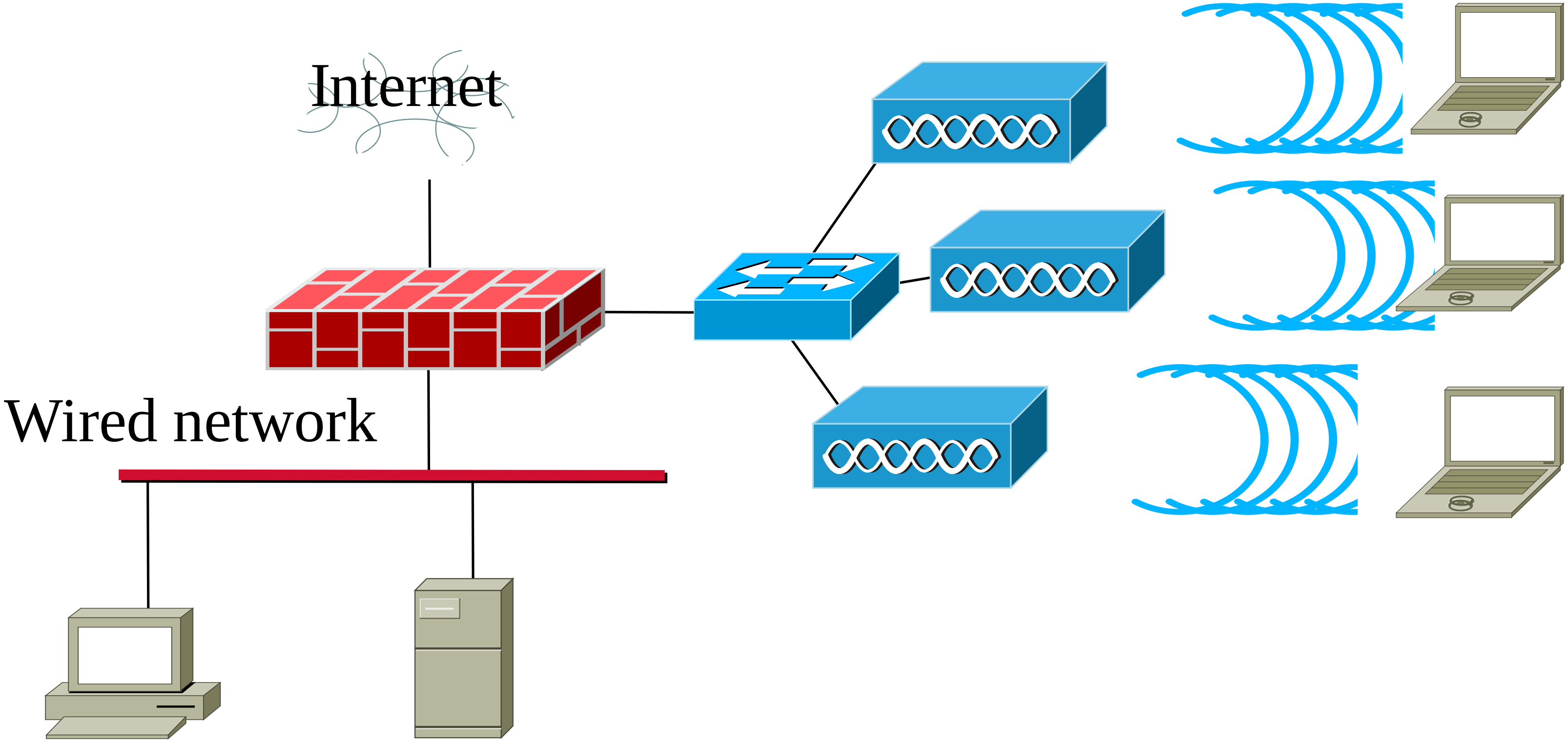
# WLAN Gateway/Firewall Insecure Configuration



# WLAN Gateway/Firewall Secure Configuration



# WLAN Gateway/Firewall Secure Configuration with Bridging Firewall



# Wired Equivalent Privacy (WEP)

- Intended to provide the same level of security as that of wired LAN
- Layer 2 security
  - point to point
- Simple symmetric encryption with a manually exchanged key
- Symmetric encryption used to encrypt messages
- Symmetric encryption used to provide authentication
- Cyclic Redundancy Check used to provide integrity

# WEP Cryptography

- RC4
  - Stream, shared secret key cipher
  - Used to provide authentication, confidentiality and integrity
  - Developed 1987
    - Used in WEP
- Crypto systems based on RC4 should discard the first few bytes generated by RC4
  - First few bytes provide a considerable amount of information about the key
  - Systems that concatenate the initialisation vector with the key (such as WEP) are particularly vulnerable

# Problems with WEP

- A major difficulty with WEP is that it uses the master key rather than a one-off derived key per session
  - The initialisation vector was intended to deal with this, but it is too short (24 bits)
  - On average, the initialisation vector will be repeated after about 5 hours
- Another major difficulty is that WEP has no replay protection
  - An attacker can capture a sequence of messages and just replay them
  - No sequence numbering
- Because of the US ban on export of strong cryptographic protocols WEP originally had a weak key length of 40 bits

# WPA

- WiFi Protected Access
- An interim protocol issued by 802.11i to fill the gap caused by the failure of WEP
- Key size (usually) 128 bits
- Still uses RC4 but incorporates additional techniques to make more secure
  - Frequent change of session key
  - Typically every 10 minutes to an hour (configurable)
- Many WEP devices upgradeable to WPA
- Designed to replace WEP without replacing legacy hardware
  - Need to continue to use RC4

# WPA

- WPA was announced 2002
- User authentication
  - 802.1X
  - Extensible Authentication Protocol (EAP)
- Encryption
  - Temporal Key Integrity Protocol (TKIP)
  - 802.1X for dynamic key distribution
- WPA can include of 802.1X, EAP, TKIP, MIC
- WPA2 uses AES with cipher block chaining

# Temporal Key Integrity Protocol (TKIP)

- TKIP Still uses RC4 but improves on it in the following ways
  - Improved initialisation vector
  - Frequent (every 10000 frames) change of session key
  - Calculation of message integrity code (MIC) to protect contents
  - Per-frame TKIP sequence counter (TSC) for replay protection
  - Different encryption key for each frame
    - Combines a session key, address and TSC to generate a encryption different key
- Frequent change of key most important change

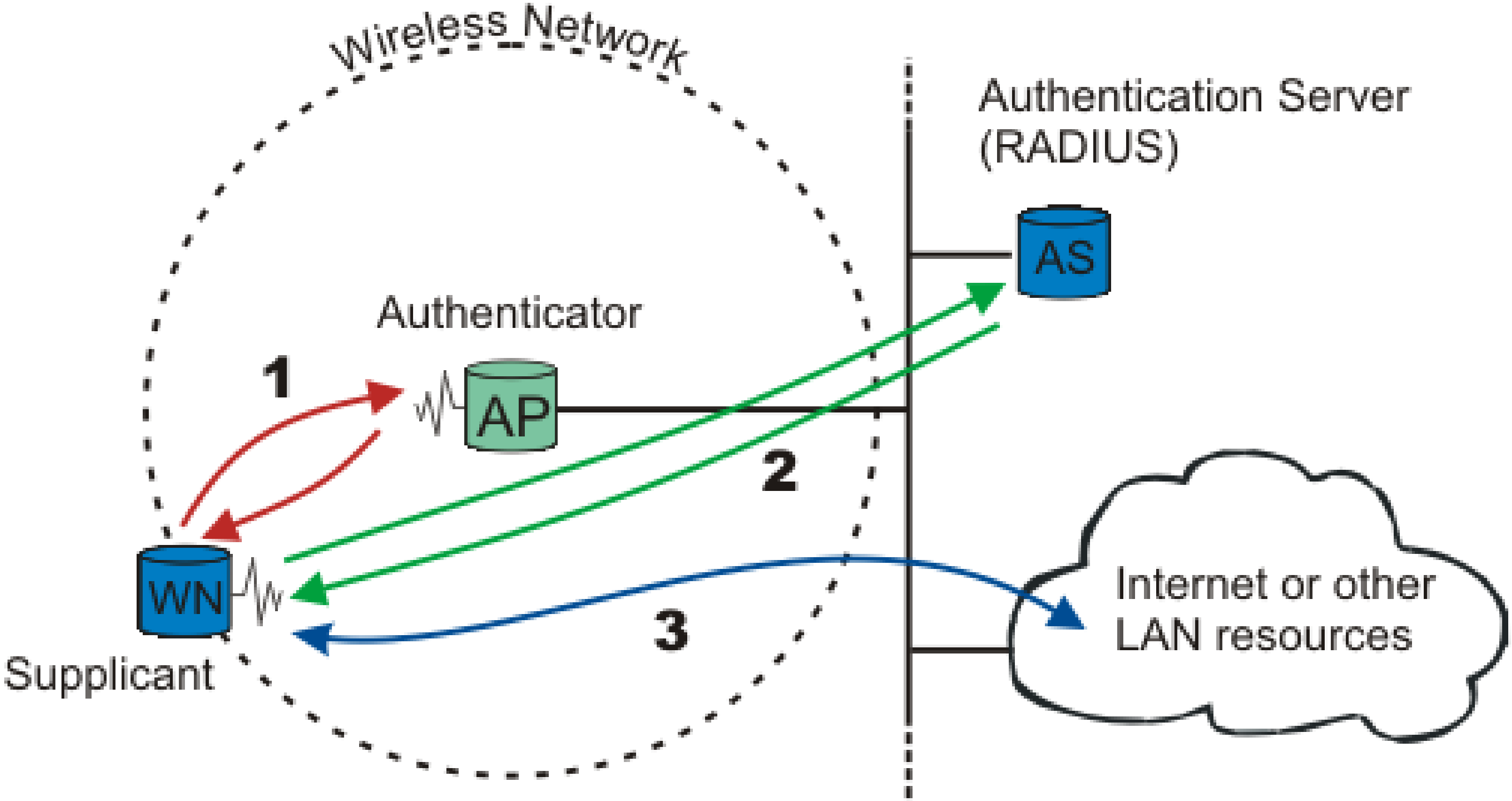
# WPA Modes of Use

- Two modes of use
  - With an 802.1X authentication server
    - Distributes different keys to each user
    - WPA-Enterprise
  - In less secure "pre-shared key" (PSK) mode (every user is given the same passphrase).
    - WPA-Personal
    - Domestic use

# 802.1X

- A framework for authentication and encryption
  - Integrates an authentication server such as RADIUS
  - Not restricted to wireless
  - Makes use of Extensible Authentication Protocol
- Authentication
  - Who can access the network and services?
- Authorization
  - What is the user allowed?
- Access Control
  - Control is based on authentication and authorization

# 802.1X



Ref: Wikipedia

# 802.1X

- Transports authentication information in the form of Extensible Authentication Protocol (EAP) payloads
- Authenticator (Network Access Server) relays EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information
- Three forms of EAP are specified in the standard
  - EAP-MD5 – MD5 Hashed Username/Password
  - EAP-OTP – One-Time Passwords
  - EAP-TLS – Strong PKI Authenticated Transport Layer Security (SSL)

# WPA2 and WPA3

- WPA2
  - Makes use of AES
  - Replaces TKIP with CCMP
    - CCMP uses AES with Cyclic Block Chaining
- WPA3
  - Strengthens authentication using a Diffie-Hellman like authentication mechanism over an Elliptic Curve
  - “Dragonfly Key Exchange”

# Conclusion

- Overview of wireless networking
- Security issues
- Introduction to WLAN
- Some attacks of WLAN
- Security protocols in WLAN