Wireless Networking

Module : Computer Networks
Lecturer : Lucy White: lbwhite@wit.ie
Office : 324

A Taxonomy of Wireless Networks

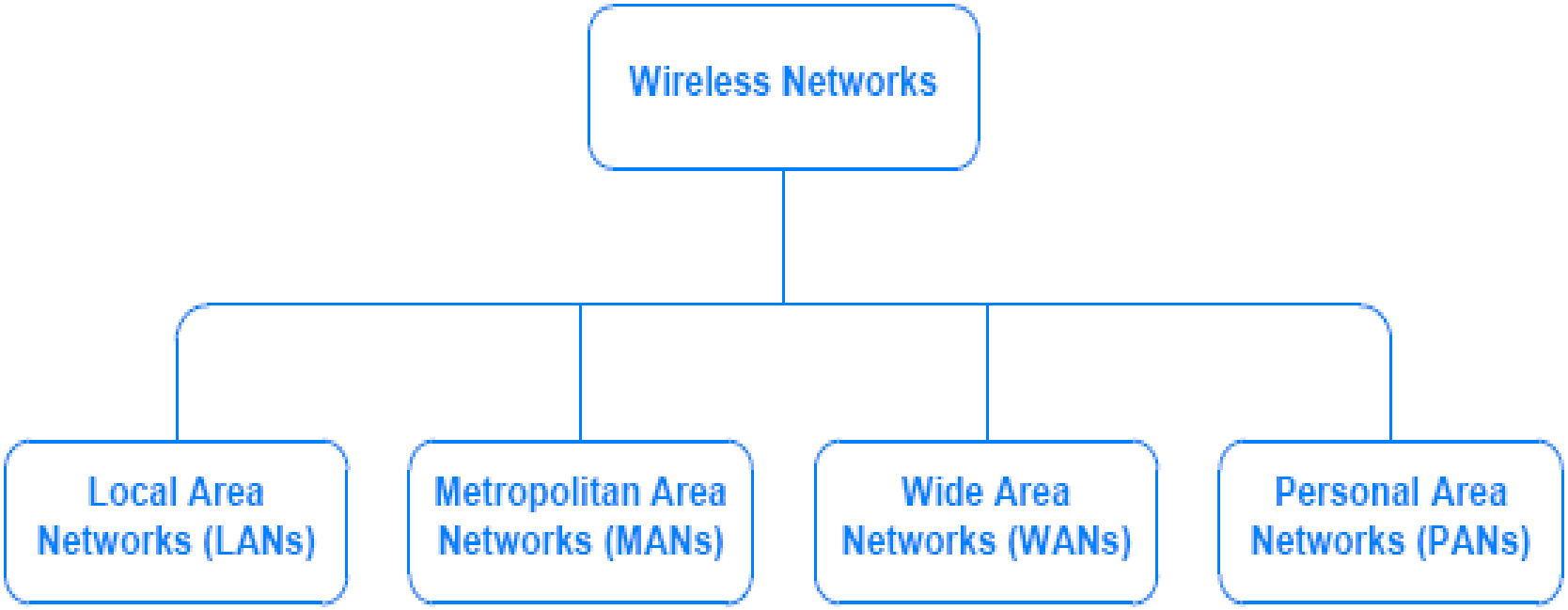
- Wireless communication applies across a wide range of network types and sizes
- Part of the motivation for variety

  government regulations that make specific ranges of the electromagnetic spectrum available for communication
- A license is required to operate transmission equipment in some parts of the spectrum

  and other parts of the spectrum are unlicensed
- Many wireless technologies have been created

  and new variants appear continually
- Wireless technologies can be classified broadly according to network type

A Taxonomy of Wireless Networks



Personal Area Networks (PANs)

- A PAN technology provides communication over a short distance
- It is intended for use with devices that are owned and operated by a single user. For example
  - between a wireless headset and a cell phone
  - between a computer and a nearby wireless mouse or keyboard
- PAN technologies can be grouped into three categories

Type	Purpose
Bluetooth	Communication over a short distance between a small peripheral device such as a headset or mouse and a system such as a cell phone or a computer
InfraRed	Line-of-sight communication between a small device, often a hand-held controller, and a nearby system such as a computer or entertainment center
ISM wireless	Communication using frequencies set aside for Industrial Scientific and Medical devices, an environment where electromagnetic interference may be present

ISM Wireless Bands Used by LANs and PANs

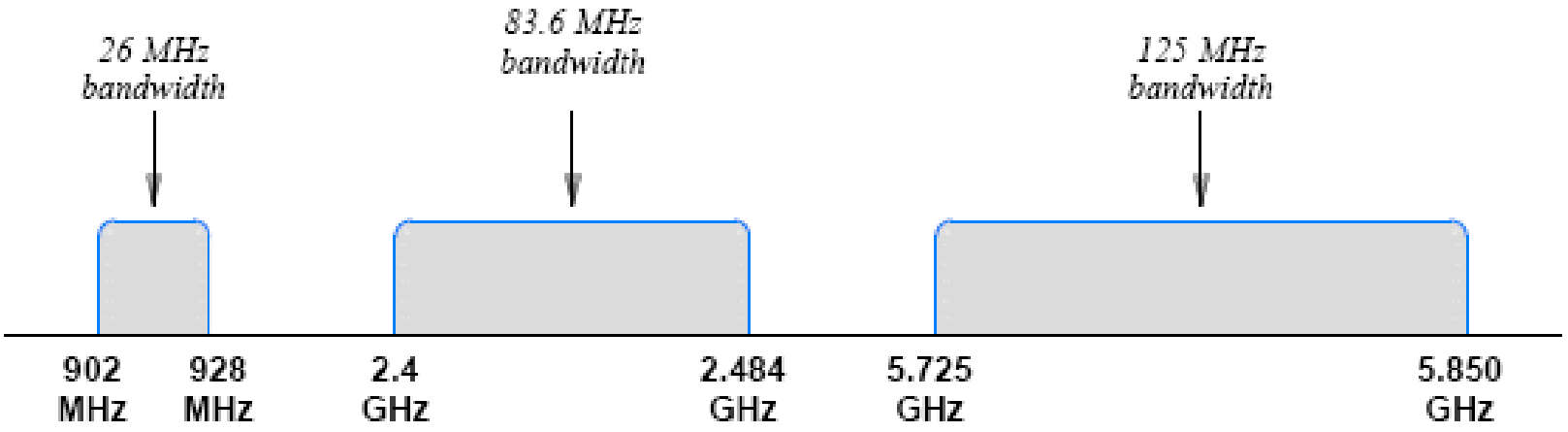
- A region of electromagnetic spectrum is reserved for use by Industrial, Scientific, and Medical (ISM) groups

  Known as ISM wireless

- The frequencies are not licensed to specific carriers

  are broadly available for products, and are used for LANs and PANs

- Figure below illustrates the ISM frequency ranges



Wireless LAN Technologies and Wi-Fi

- A variety of wireless LAN technologies exist that use
  - various frequencies
  - modulation techniques
  - and data rates
- IEEE provides most of the standards
  - which are categorized as IEEE 802.11
- A group of vendors who build wireless equipment formed the Wi-Fi Alliance
  - a non-profit organization that tests and certifies wireless equipment using the 802.11 standards
- Alliance has received extensive marketing, most consumers associate wireless LANs with the term Wi-Fi

Wireless LAN Technologies and Wi-Fi

IEEE Standard	Frequency Band	Data Rate	Modulation Technique	Multiplexing Technique
original 802.11	2.4 GHz	1 or 2 Mbps	FSK	DSSS
	2.4 GHz	1 or 2 Mbps	FSK	FHSS
	InfraRed	1 or 2 Mbps	PPM	–none–
802.11a	5.725 GHz	6 to 54 Mbps	PSK or QAM	OFDM
802.11b	2.4 GHz	5.5 and 11 Mbps	PSK	DSSS
802.11g	2.4 GHz	22 and 54 Mbps	various	OFDM
802.11n	2.4 GHz and 5 GHz	Up to 600 Mbps	various	OFDM, MIMO
802.11ac	2.4 GHz and 5 GHz	Up to 2.6 Gbps	various	OFDM, Spatial Multiplexing and MIMO

Spread Spectrum Techniques

- The term spread spectrum transmission uses multiple frequencies to send data
  - the sender spreads data across multiple frequencies
  - the receiver combines the information obtained from multiple frequencies to reproduce the original data
- Spread spectrum can be used to achieve one of the following two goals:
  - Increase overall performance
  - Make transmission more immune to noise
- The key multiplexing techniques used in Wi-Fi wireless networks are DSSS, FHSS, OFDM and Spatial Multiplexing with MIMO
  - Each technique has advantages
  - Thus, when a wireless technology is defined, the designers choose an appropriate multiplexing technique

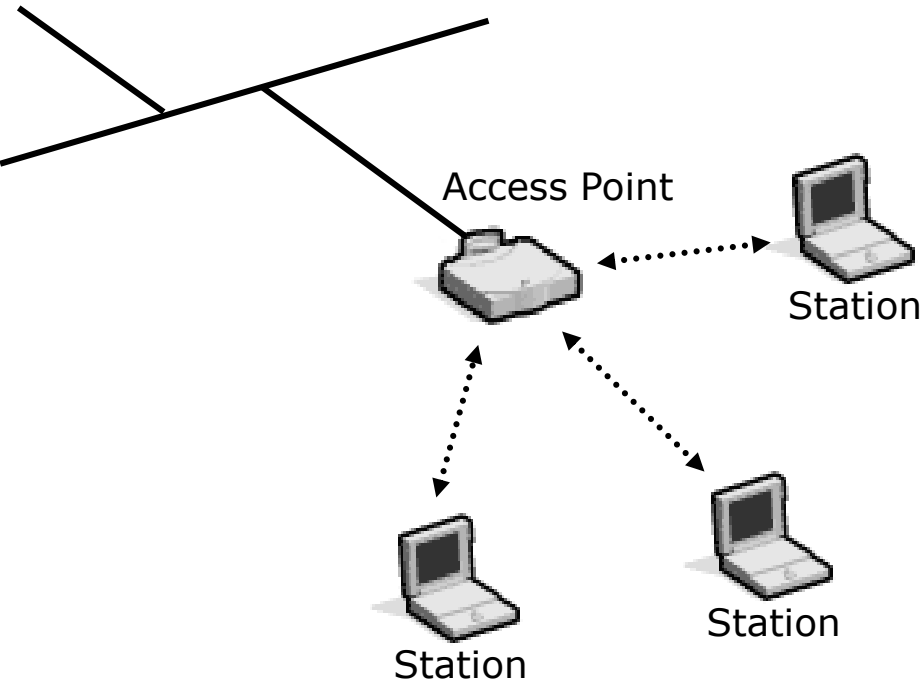
Other 802.11 Wireless LAN Standards...

Standard	Purpose
802.11e	Improved quality of service, such as a guarantee of low jitter
802.11h	Like 802.11a, but adds control of spectrum and power (primarily intended for use in Europe)
802.11i	Enhanced security, including Advanced Encryption Standard; the full version is known as WPA2
802.11k	Will provide radio resource management, including transmission power
802.11n	Data rate over 100 Mbps to handle multimedia (video) applications (may be 500 Mbps)
802.11p	Dedicated Short-Range Communication (DSRC) among vehicles on a highway and vehicle-to-roadside
802.11r	Improved ability to roam among access points without losing connectivity
802.11s	Proposed for a mesh network in which a set of nodes automatically form a network and pass packets

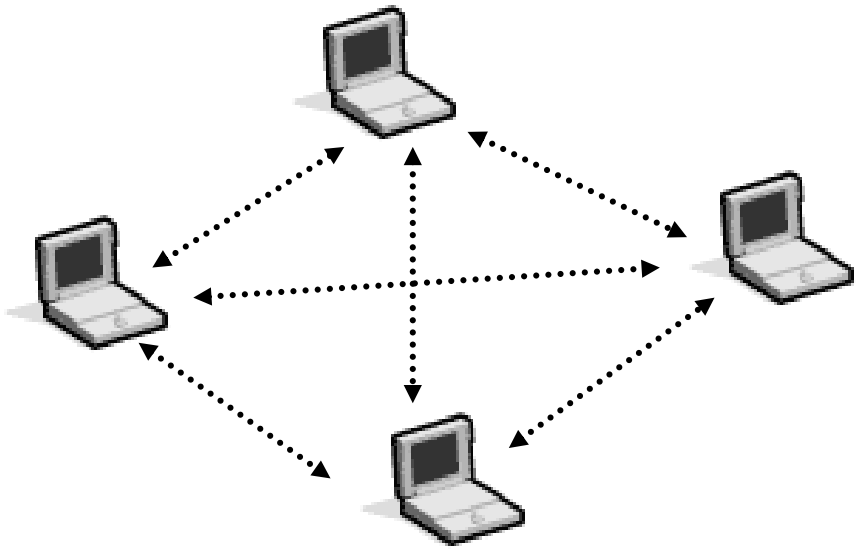
Wireless LAN Architecture

- The three building blocks of a wireless LAN are:
  - Access Points (AP)
  - an interconnection mechanism
    - such as a switch or router used to connect access points
  - a set of wireless hosts
    - also called wireless nodes or wireless stations
- In principle, two types of wireless LANs are possible:
  - Ad hoc
    - wireless hosts communicate amongst themselves without a base station
  - Infrastructure based
    - a wireless host only communicates with an access point, and the access point relays all packets

Modes of Operation



Infrastructure Mode



Ad-hoc Mode

Wireless LAN Architecture

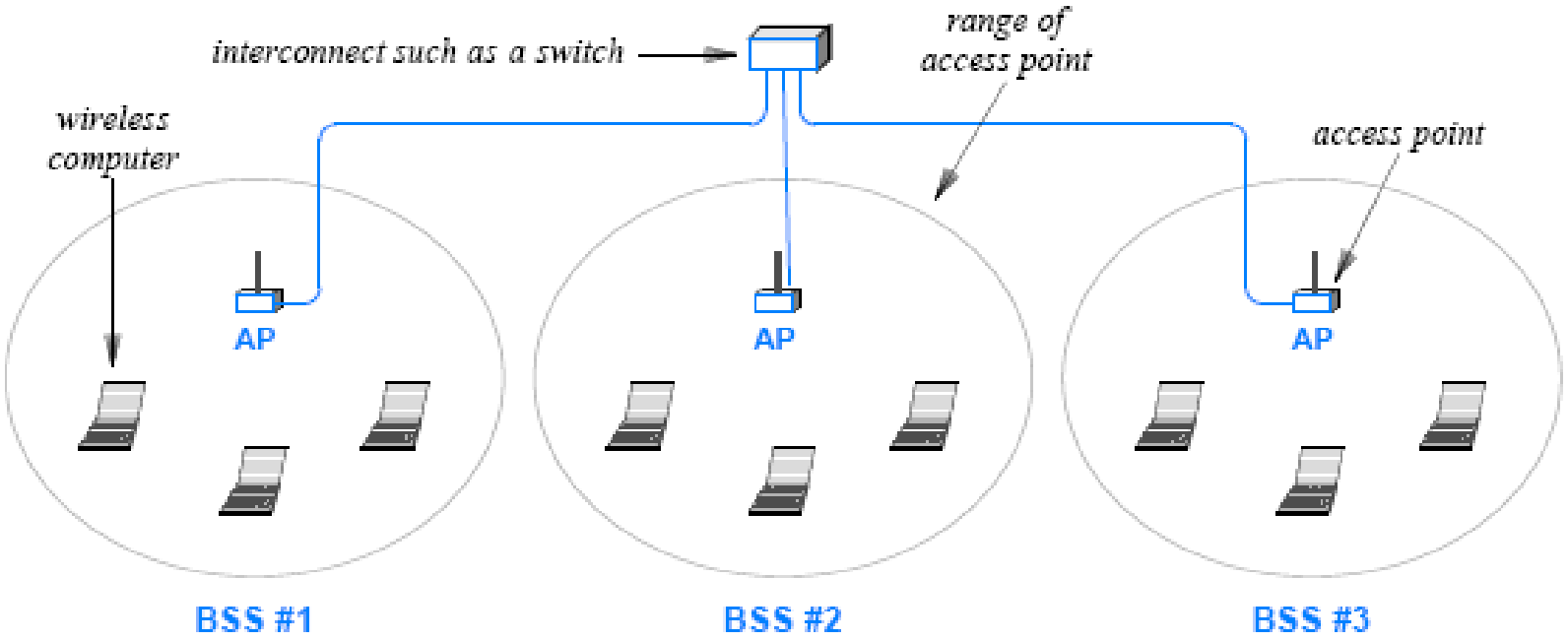


Illustration of an infrastructure architecture for a wireless LAN.

Note: The set of computers within range of a given access point is known as a *Basic Service Set (BSS)*

Connecting to an access point

- Station enters range of one or more access points
  - Access points broadcast periodic signals (beacons)
  - These broadcasts may include SSID (Service Set Identifier)
    - SSID differentiates one access point from another
  - User may choose from among networks that broadcast SSID, or by entering SSID

- Most basic form of security: disable broadcast of SSID
  - Need also to change default SSID from “linksys” or “tsunami” (Cisco default) to something that is less easy to guess
  - Disadvantage: every user needs to know SSID in advance
  - Of limited use anyway, as SSID transmitted in clear by user

SSID (Service Set Identity)

At a minimum a client station and the access point must be configured to be using the same SSID.

- An SSID is:
  - Between 2 and 32 alphanumeric characters
  - Spaces okay
  - Must match EXACTLY, including upper and lower case
  - Beware of typing spaces at the end of your SSIDs in both AP config and client config.

Overlap and Association

- Many details can complicate an infrastructure architecture
  - On one hand, if a pair of APs are too far apart
    - a dead zone will exist between them
    - a physical location with no wireless connectivity
  - On the other hand, if a pair of access points is too close together
    - an overlap will exist in which a wireless host can reach both access points
- Most wireless LANs connect to the Internet
  - Thus, the interconnect mechanism usually has an additional wired connection to an Internet router

Overlap and Association

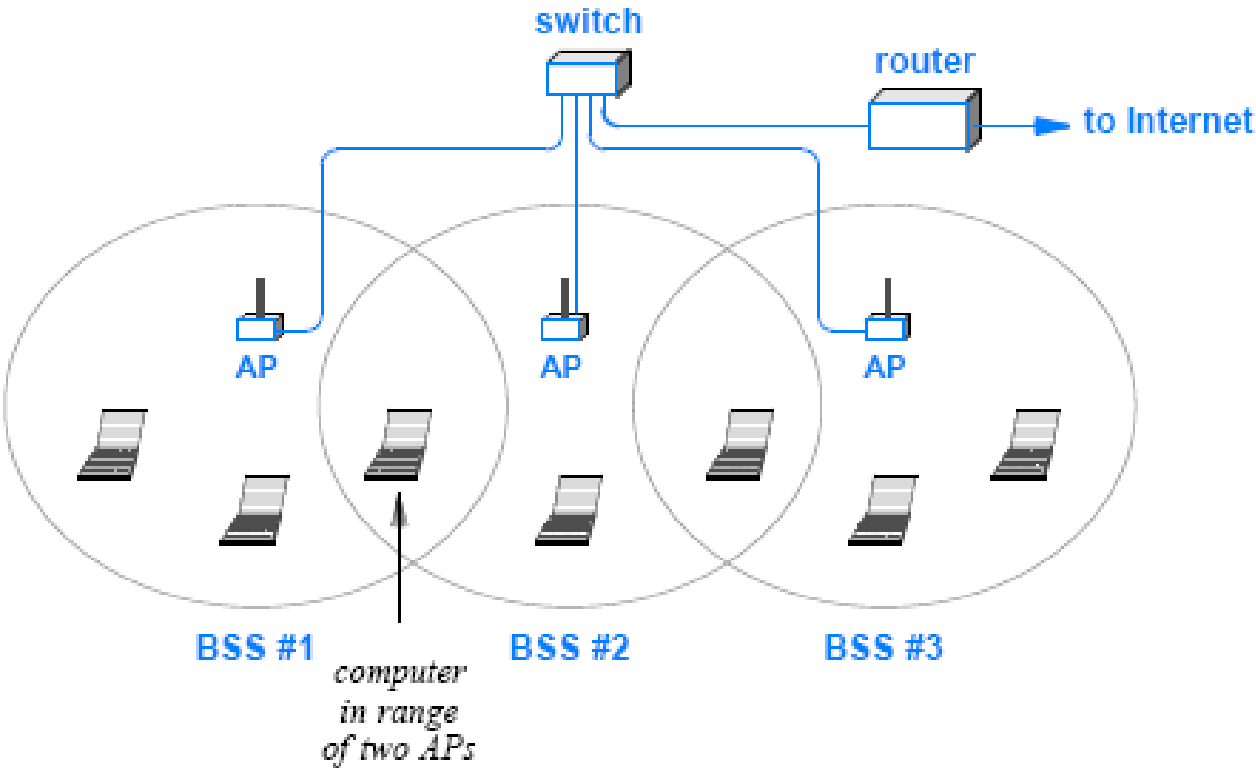


Illustration of an infrastructure with overlapping regions.

Coordination Among Access Points

- To what extent do APs need to coordinate?
- Many early AP designs were complex
- The access points coordinated to provide seamless mobility similar to the cellular phone system

  That is, the APs communicated amongst themselves to insure smooth handoff as a wireless computer moved from the region to another

  Some designs measured signal strength and attempted to move a wireless node to a new AP

    when the signal received at the new AP exceeded the signal strength at the existing AP

Coordination Among Access Points

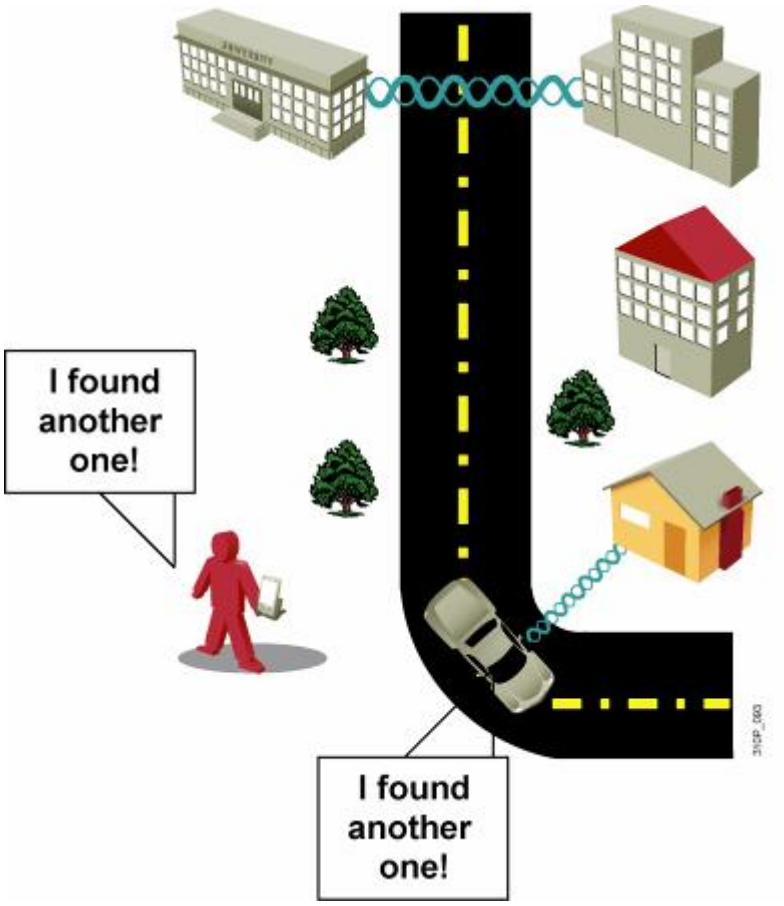
- Some vendors began to offer lower cost, less complex APs that do not coordinate
- The vendors argue that signal strength does not provide a valid measure of mobility
  - a mobile computer can handle changing from one AP to another
  - and that the wired infrastructure connecting APs has sufficient capacity to allow more centralized coordination

Contention and Contention-Free Access

- Physical separation among stations and electrical noise makes it difficult to distinguish between
  - weak signals, interference, and collisions
- Wi-Fi networks do not employ collision detection
  - That is, the hardware does not attempt to sense interference during a transmission
  - Instead, a sender waits for an acknowledgement (ACK) message
  - If no ACK arrives, the sender assumes the transmission was lost
    - and employs a backoff strategy similar to the strategy in wired Ethernet
- In practice, 802.11 networks that have few users and do not experience electrical interference seldom need retransmission
  - However, other 802.11 networks experience frequent packet loss and depend on retransmission

Why WLAN Security?

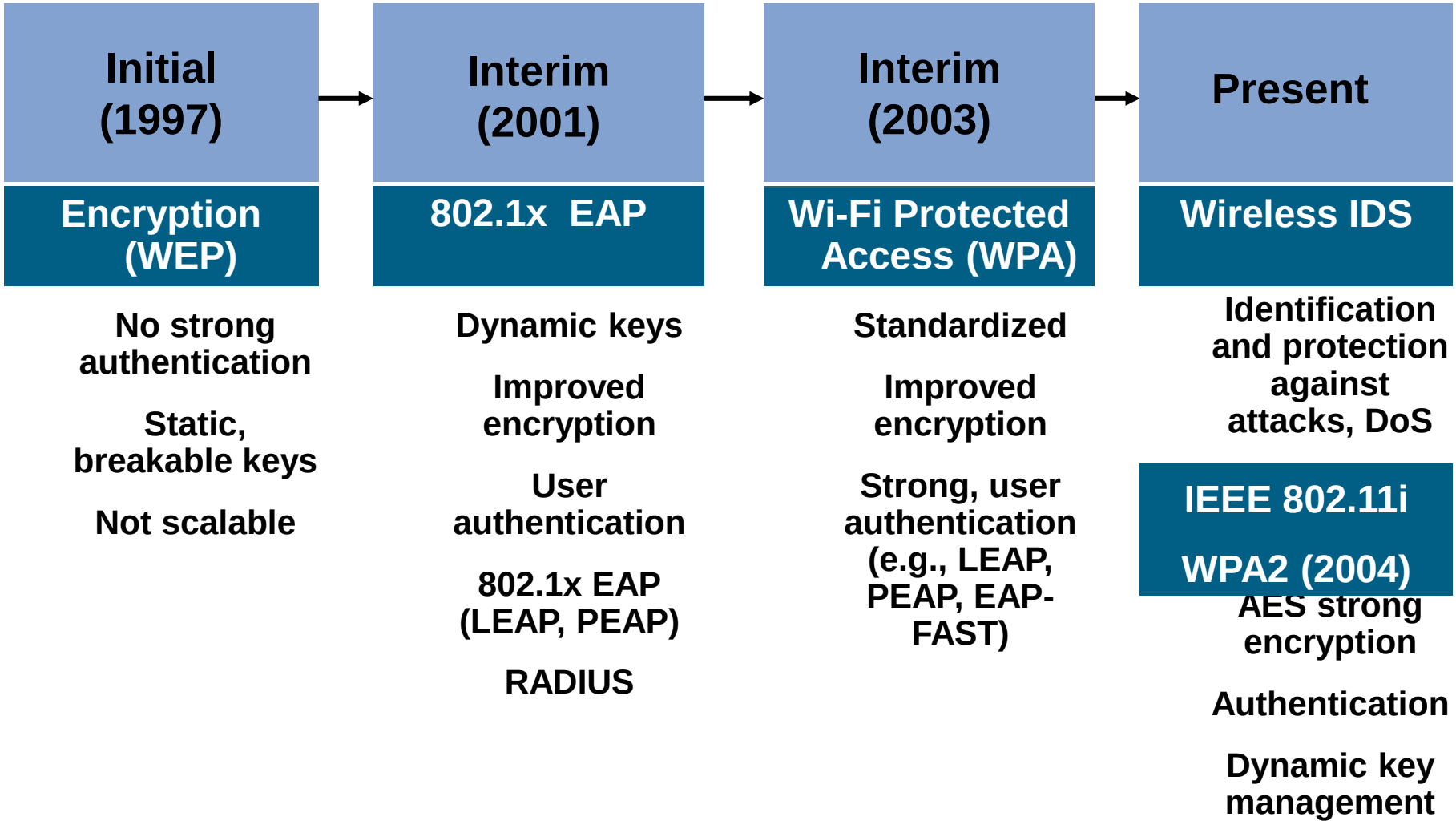
- Wide availability and low cost of IEEE 802.11 wireless equipment
- 802.11 standard ease of use and deployment
- Availability of sniffers
- Statistics on WLAN security
- Media hype about hot spots, WLAN hacking, war driving
- Authentication vulnerability



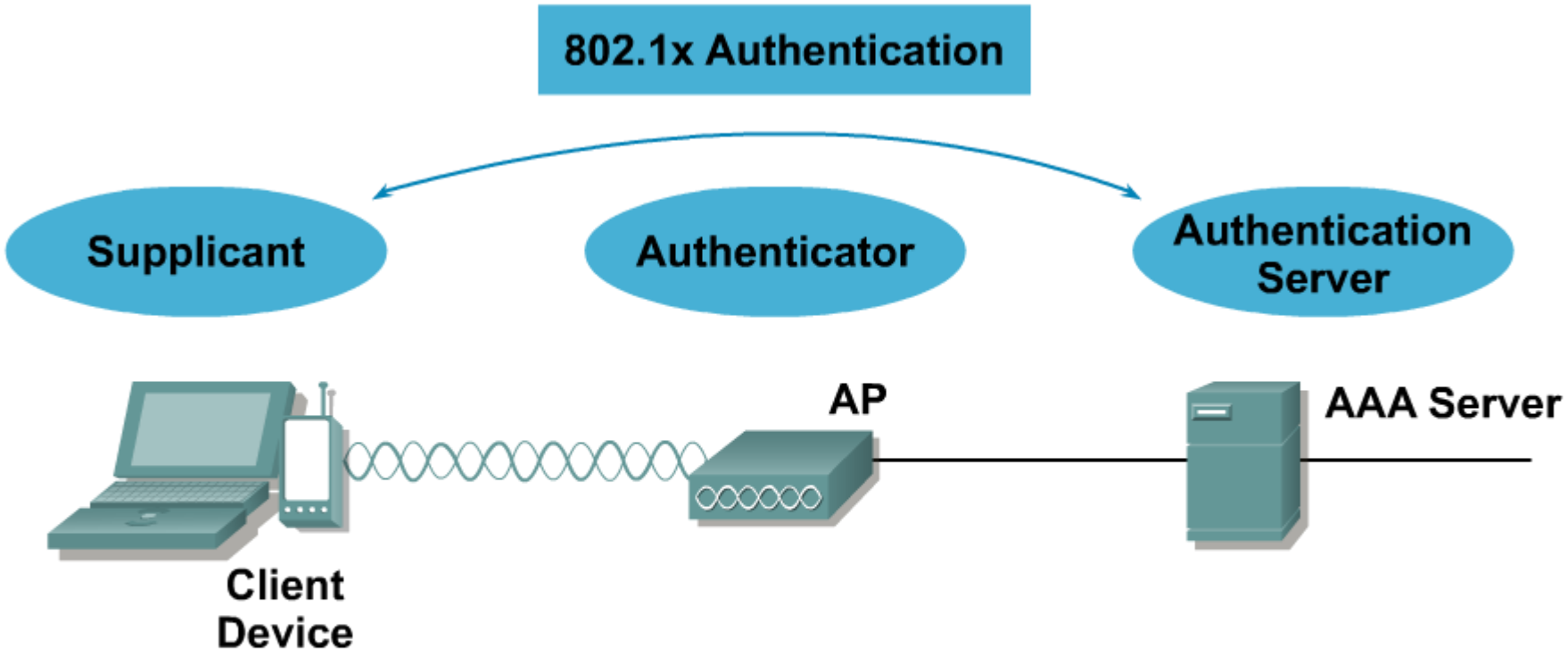
Mitigating the Threats

Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Detection System (IDS)
Ensure that legitimate clients associate with trusted APs.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Evolution of Wireless LAN Security



WPA and WPA2 Authentication



Supplicant for 802.1x Type: LEAP, PEAP, EAP-FAST, etc.

802.1x Support

Server Support for 802.1x Type: LEAP, PEAP, EAP-FAST, etc.

Secure the WLAN

- Modify the default SSID.
- Use strong encryption.
- Deploy mutual authentication between the client and the network.
- Use **WPA2** combined with MAC address control lists to secure business-specific devices.
- Use identity networking in combination with VLANs to restrict access to network resources.
- Ensure management ports are secured.
- Deploy lightweight access points as they do not store security information locally.
- Physically hide or secure access points to prevent tampering.
- Monitor the exterior building and site for suspicious activity.

References

- http://en.wikipedia.org/wiki/IEEE_802.11

- http://en.wikipedia.org/wiki/Wireless_security