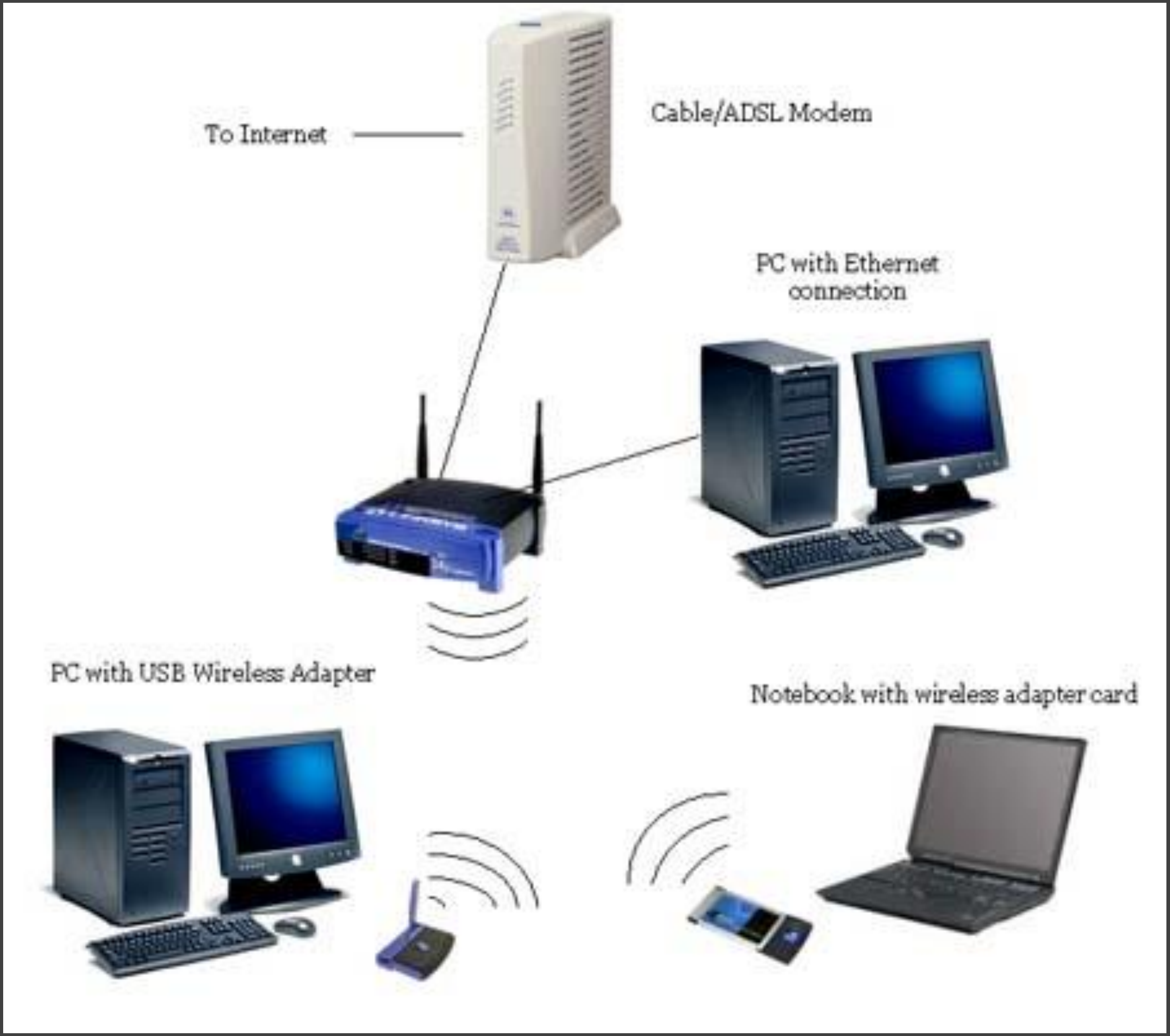
Wireless Networking

Outline

- Introduction
- Wireless Network Architecture
- Types of Wireless Networks
- Spread Spectrum
- Wireless Network Security

Introduction

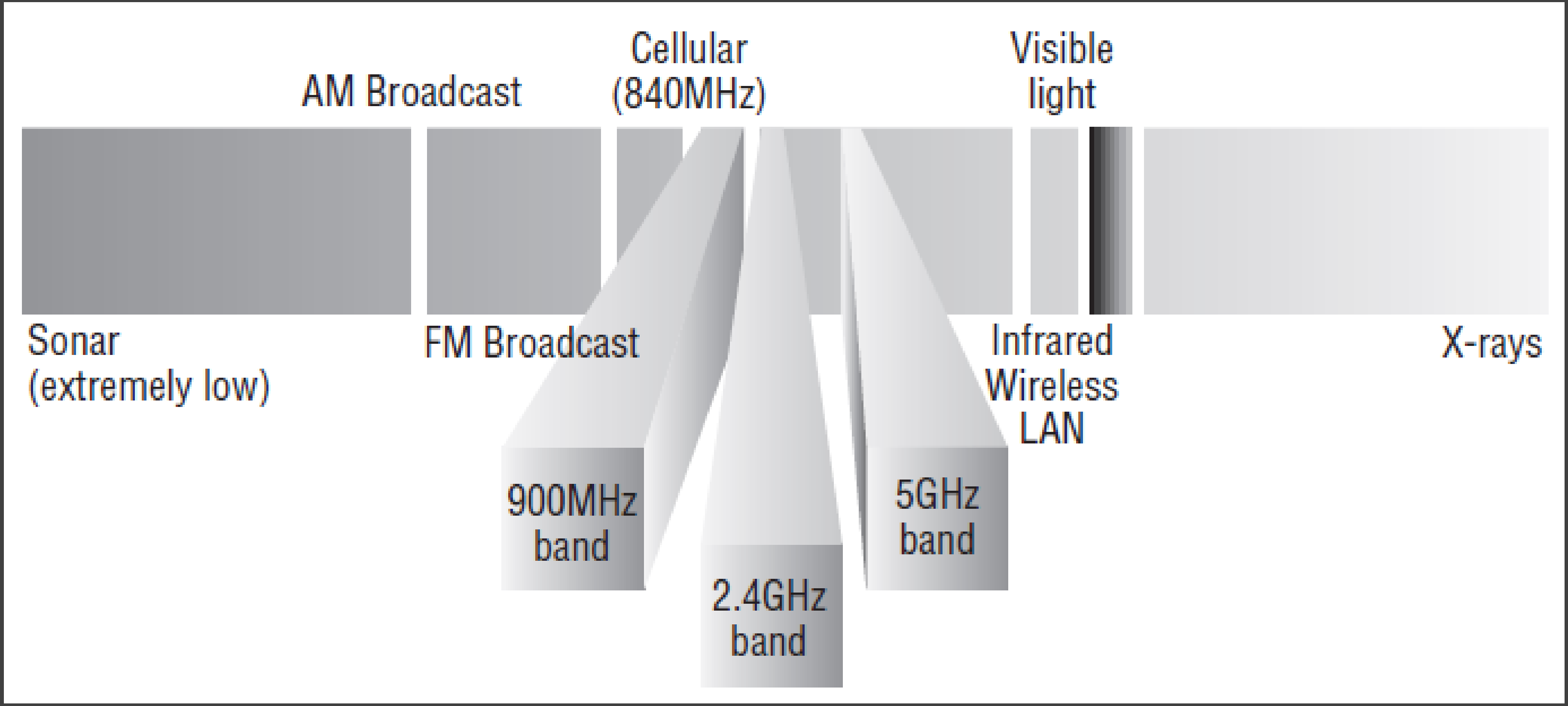
- Wireless Network
  - Type of computer network that uses high frequency radio waves rather than wires to connect devices such as laptops and any other network-enabled devices


To Internet
Cable/ADSL Modem
PC with Ethernet connection
PC with USB Wireless Adapter
Notebook with wireless adapter card

Typical wireless network

ISM Wireless Bands

- Industrial Scientific and Medical – ISM



Unlicensed frequencies

Introduction (cont’d)

- Advantages
  - Convenience
  - Mobility
  - Productivity
  - Deployment (Easy Setup)
  - Expandability
  - Cost

Introduction (cont’d)

- Disadvantages
  - Security
  - Range
  - Reliability
  - Speed

Components

Wireless Network Interface Card

Components (cont’d)

Wireless Access Point

Terms

Is a trademark term meaning IEEE 802.11x

A global non-profit industry organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any “wireless local area network products that are based on the IEEE 802.11 standards”

Terms (cont'd)

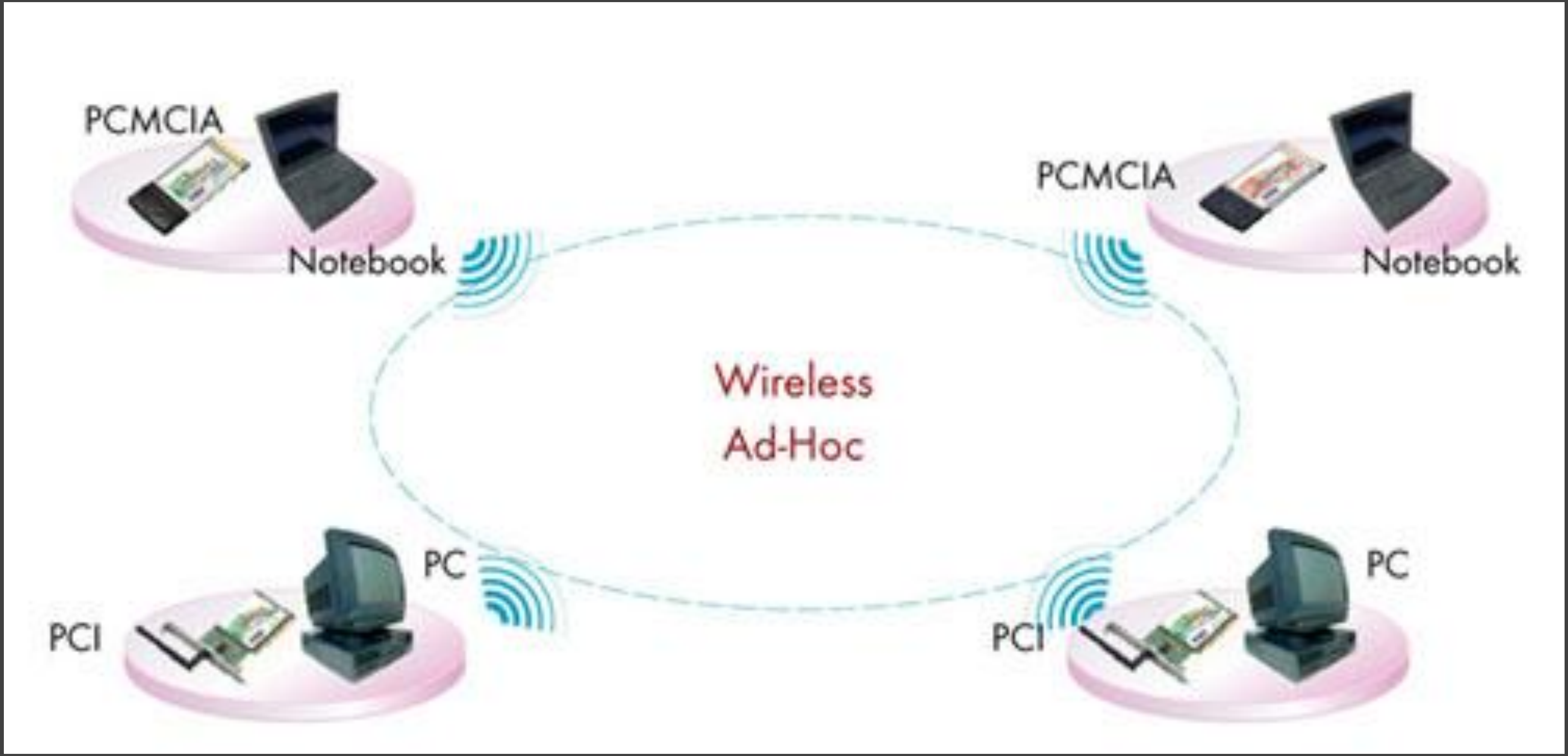
A site that offers internet access over a wireless local area network through the use of a router connected to a link to an internet service provider.

Hotspots typically use Wi-Fi technology.

Wireless Network Architecture

- Ad Hoc (IBSS)
  - Consists of at least two wireless stations where no access point is involved in their communication
  - Ad Hoc mode WLANs are normally less expensive to run, as no APs are needed
  - Cannot scale for larger networks and lack of some security features like MAC filtering and access control

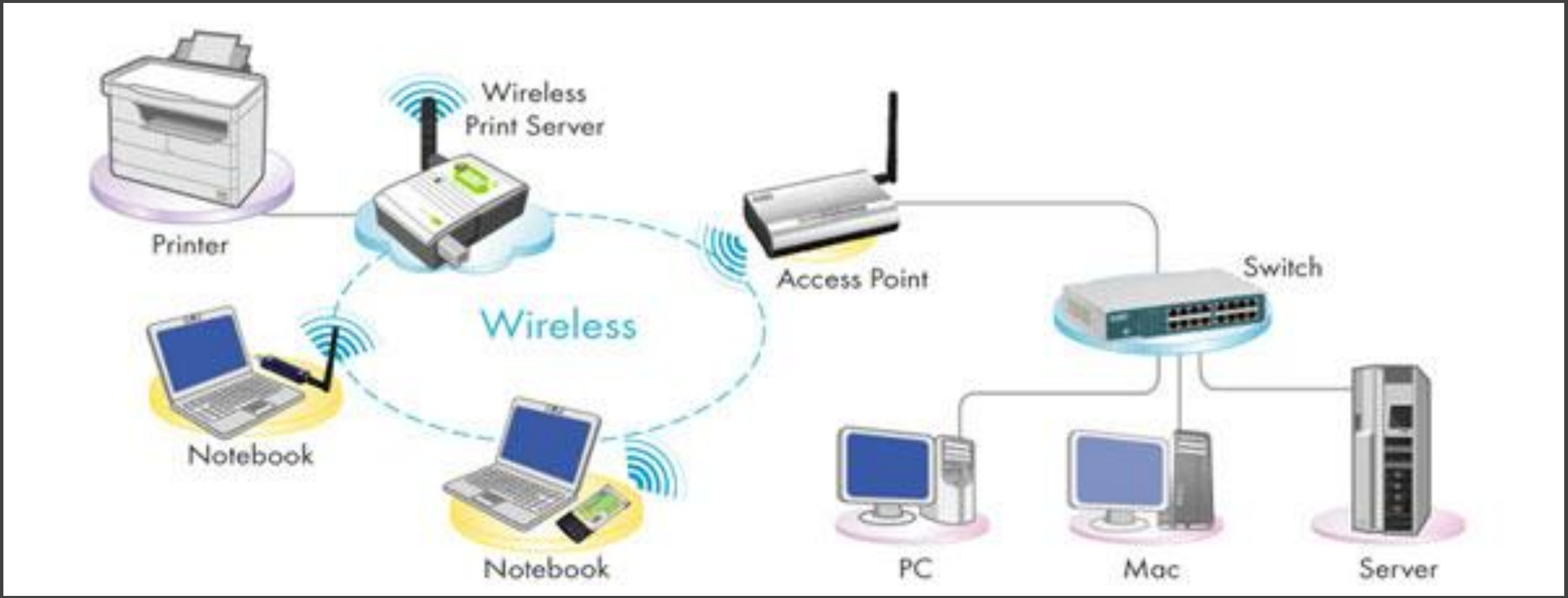
Wireless Network Architecture (cont’d)



Wireless Network Architecture (cont’d)

- Infrastructure (BSS)
  - Consists of a number of wireless stations and access points
  - The access points usually connect to a larger wired network
  - Can scale to large-scale networks with arbitrary coverage and complexity

Wireless Network Architecture (cont'd)



Types of Wireless Networks

- Wireless Personal Area Networks (WPAN)
  - 802.15.1 → Bluetooth
- Wireless Local Area Networks (WLAN)
  - 802.11a/b/g/n
- Wireless Metropolitan Area Networks (WMAN)
  - 802.16a → WiMAX

Wireless Personal Area Network

- Provides communication over a short distance, and is intended for use with devices that are owned and operated by a single user

- Example:

  Communication between a wireless headset and a cell phone

WPAN – Bluetooth

- Low cost and short-range radio communication standard for exchanging data over short distances (using short-wavelength radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices.
- Bluetooth Special Interest Group (BSIG)
- IEEE 802.15.1

WPAN – Bluetooth (cont’d)

Version	Data Rate
1.2	1 Mbps
2.0 + EDR	3 Mbps
3.0 + HS	24 Mbps
4.0	24 Mbps

Wireless Local Area Network

- Link two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access.

WLAN Standards

- 802.11a

Release time	: October 1999
Transfer rate	: 54 Mbps
Frequency	: 5 GHz
Range	: Indoor 15m, Outdoor 30m

WLAN Standards (cont’d)

- 802.11b

Release time	: Early 2000
Transfer rate	: 5.5 Mbps – 11 Mbps
Frequency	: 2.4 GHz
Range	: Indoor 45m, Outdoor 90m

WLAN Standards (cont'd)

- 802.11g

  Release time : June 2003

  Transfer rate : 54 Mbps

  Frequency : 2.4 GHz

  Range : Indoor 45m, Outdoor 90m

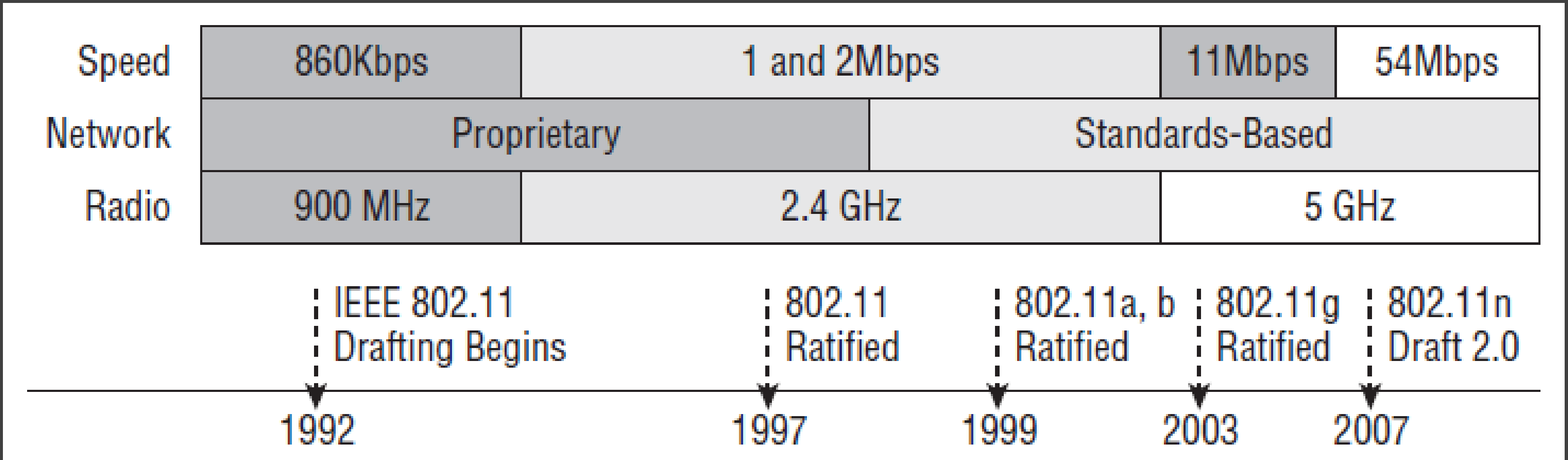
WLAN Standards (cont’d)

- 802.11n

Release time	: 11 September 2009
Transfer rate	: 600 Mbps
Frequency	: 2.4 GHz / 5 GHz
Range	: Indoor 70m, Outdoor 250m

Comparison of WLAN Standards

	802.11a	802.11b	802.11g		802.11n
Ratified	1999	1999	2003		Not Ratified
Frequency Band	5 GHz	2.4 GHz	2.4 GHz		2.4 GHz, 5 GHz
No. of Channels	Up to 23	3	3		Varies
Transmission	OFDM	DSSS	DSSS	OFDM	DSSS, CCK, OFDM
Data Rates (Mbps)	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	100+, up to 500



WLAN history

WMAN – WiMAX

- Worldwide Interoperability for Microwave Access

- Wireless communications standard designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbps for fixed stations.

- WiMAX Forum

  Formed in June 2001 to promote conformity and interoperability of the standard.

- IEEE 802.16

WMAN – WiMAX (cont’d)

- Uses
  - Providing portable mobile broadband connectivity across cities and countries through a variety of devices
  - Providing a wireless alternative to cable and digital subscriber line (DSL) for last mile broadband access
  - Providing data, telecommunications (VoIP) and IPTV services (triple play)
  - Providing a source of internet connectivity as part of a business continuity plan

Spread Spectrum Technique

- Spread Spectrum
  - The bandwidth of the transmitted signal is much greater than the bandwidth of the original message
  - The bandwidth of the transmitted signal is determined by the message to be transmitted and by an additional signal known as the Spreading Code

Spread Spectrum Technique (cont’d)

- Advantages
  - Redundancy

    The message is (or may be) present on different frequencies from where it may be recovered in case of errors. The effect is that Spread Spectrum systems present high resistance to noises and interference, being able to recover their messages even if noises are present on the medium.

Spread Spectrum Technique (cont'd)

- Advantages
  - Low power density

    The transmitted energy is spread over a wide band, and therefore, the amount of energy per specific frequency is very low. The effect is that such a signal will not disturb (interfere with) the activity of other system's receivers in the same area that such a signal can not be detected by intruders, providing a high level of intrinsic security.

Spread Spectrum Technique

- Techniques
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Orthogonal Frequency Division Multiplexing (OFDM)

Spread Spectrum Technique (cont’d)

- Direct Sequence Spread Spectrum – DSSS
  - Creates a redundant bit pattern for each bit that’s transmitted, increasing DSSS’s resistance to interference.
  - The benefit of this is that if any bits in the bit pattern are damaged in transmission, you’ve got a chance at recovering the original data from the redundant bits.

Spread Spectrum Technique (cont’d)

- Frequency Hopping Spread Spectrum – FHSS
  - Modulates the data signal with a carrier signal that changes (hops) in a random but, over time, predictable sequence of frequencies.
  - Changes also occur over a wide frequency band, with a spreading, or hopping, code establishing transmission frequencies used.
  - Isn’t the technique of choice.

Spread Spectrum Technique (cont’d)

- Orthogonal Frequency Division Multiplexing – OFDM
  - Distributes the data over 52 carriers, which are spaced apart at precise frequencies.
  - Help prevent demodulators from seeing frequencies other than their own.
  - Resistant to RF interference, and it present lower multipath distortion—big reasons why it’s been used in high-speed wireless networks.

Wireless Network Security

- Open Access
- Service Set Identifiers (SSID), Wired Equivalent Privacy (WEP), Media Access Control (MAC) Address Authentication
- Remote Authentication Dial In User Service (RADIUS)
- Temporal Key Integrity Protocol (TKIP) – WPA
- WPA2 Pre-Shared Key

Wireless Network Security (cont’d)

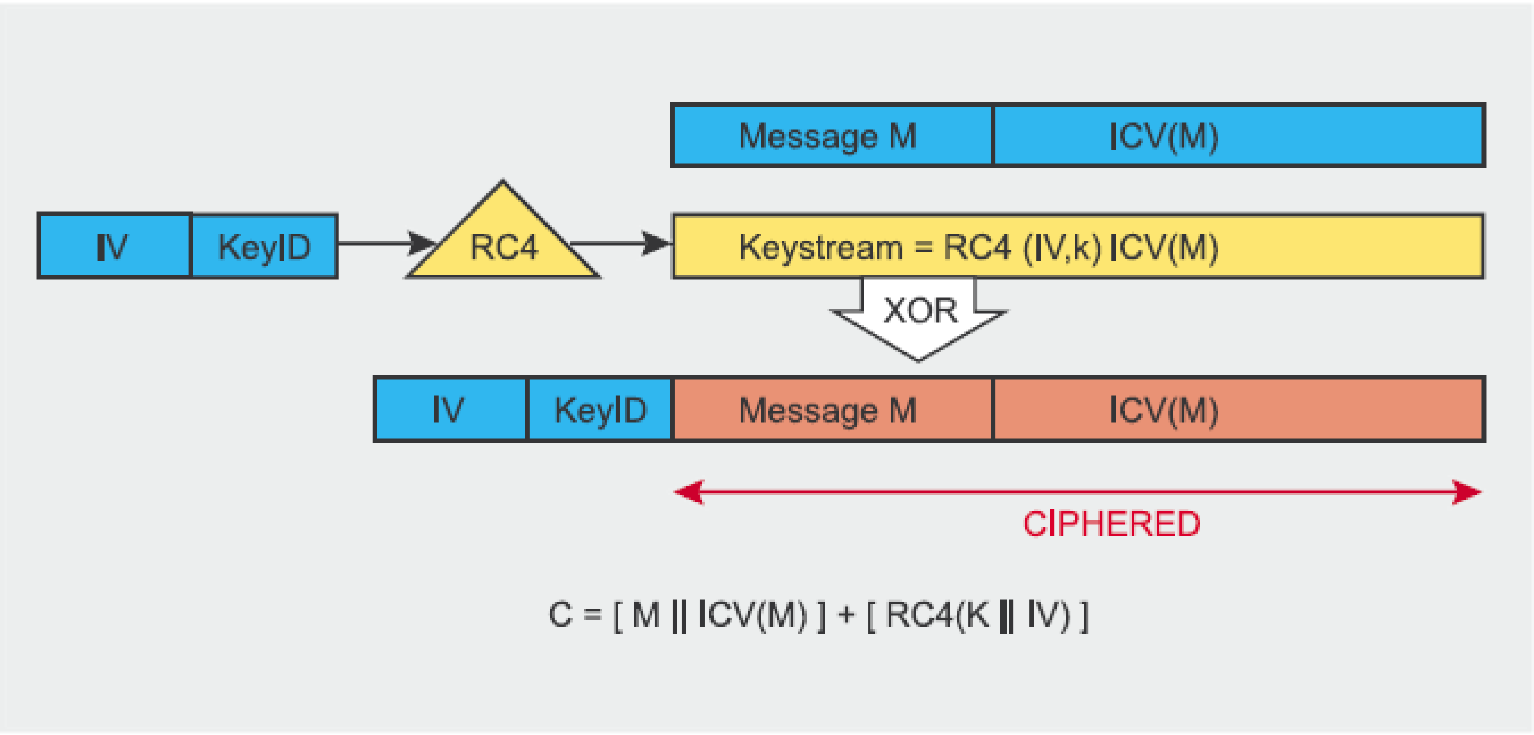
- Open Access
  - – Shipped with all Wi-Fi certified products
    - So that any person who knows absolutely nothing about computers can just buy an access point, plug it into their cable or DSL modem, and they’re up and running.
    - It’s marketing, plain and simple, and simplicity sells.
  - – Not an option for an enterprise organization or private home network

Wireless Network Security (cont’d)

- SSIDs, WEP, MAC Address Authentication
  - Basic security features
  - Sound like a lot, but none of these really offer any type of serious security solution
  - SSID, network name that broadcast many times in a second
  - MAC Address Authentication
    - MAC address can be statically typed and changed.
    - Anyone equipped with a free wireless sniffer can just read the client packets sent to the AP and spoof their MAC address.

Wireless Network Security (cont'd)

- SSIDs, WEP, MAC Address Authentication
  - Wired Equivalent Privacy (WEP)
    - Based on RC4 algorithm to encrypt the plaintext


Message M
ICV(M)
IV
KeyID
RC4
Keystream = RC4 (IV,k) ICV(M)
XOR
IV
KeyID
Message M
ICV(M)
CIPHERED
C = [M || ICV(M)] + [RC4(K || IV)]

Wireless Network Security (cont'd)

- SSIDs, WEP, MAC Address Authentication
  - WEP Authentication
    - Open System Authentication
      - No authentication occurs
    - Shared Key Authentication
      - Client sends an authentication request to the AP
      - AP replies with a clear-text challenge
      - Client encrypts the challenge-text using the configured WEP key, sends it back in another authentication request
      - AP decrypts the response. If it matches the challenge-text the AP sends back a positive reply

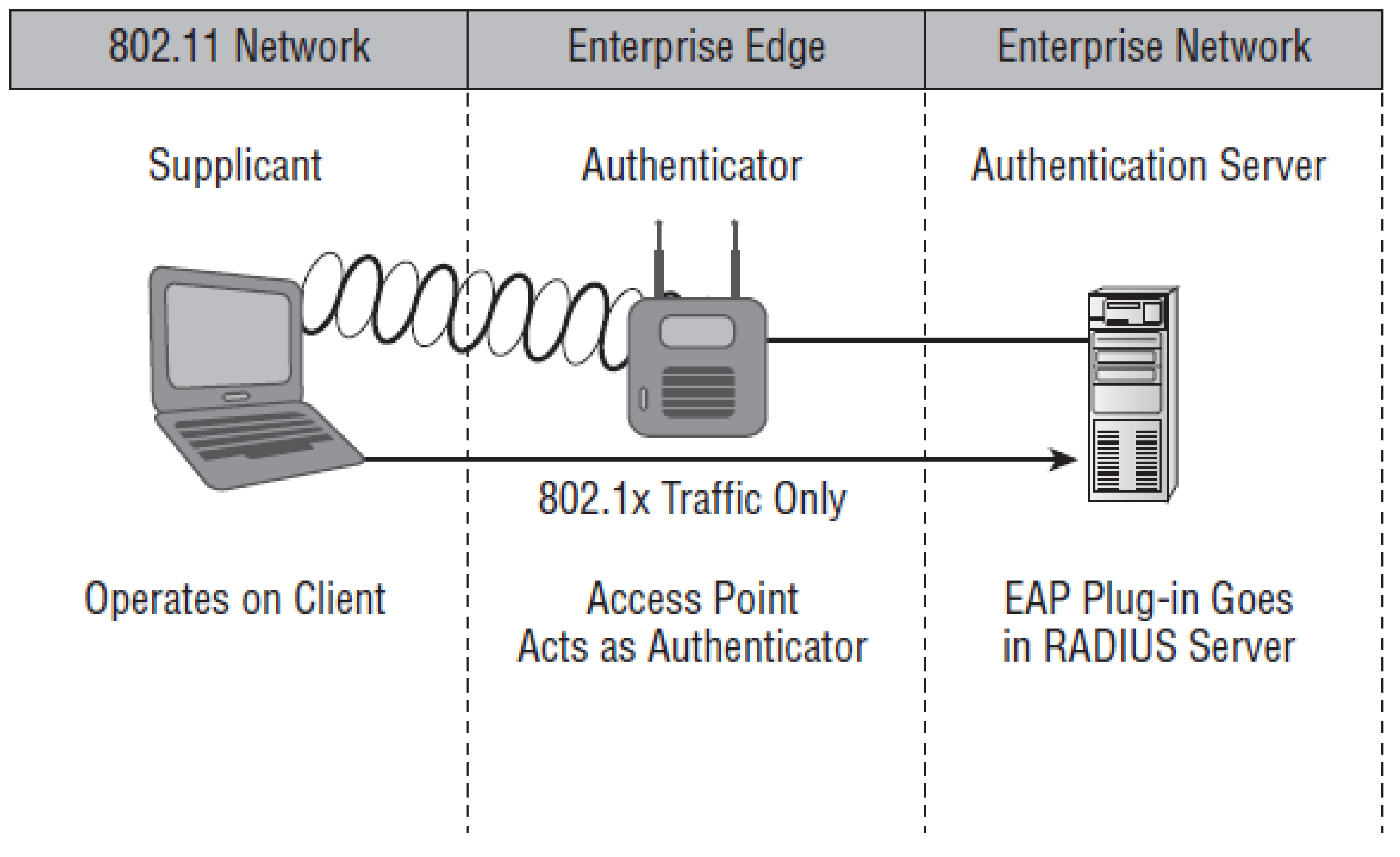
Wireless Network Security (cont’d)

- Remote Authentication Dial In User Service (RADIUS)
  - Networking protocols that offers several security benefits
    - Authorization
    - Centralized access
    - Accounting supervision regarding the users and/or computers that connect to and access the network’s services

Wireless Network Security (cont'd)

- Remote Authentication Dial In User Service (RADIUS)
  - Once RADIUS authenticated, it allows us to specify the type of rights a user or workstation has, plus control what it, or they, can do within the network.
  - It also creates a record of all access attempts and actions.
  - Critically important in large corporate environments.

Wireless Network Security (cont’d)



802.11 Network	Enterprise Edge	Enterprise Network
Supplicant	Authenticator	Authentication Server
Operates on Client	Access Point Acts as Authenticator	EAP Plug-in Goes in RADIUS Server

Radius Authentication Server

Wireless Network Security (cont’d)

- Temporal Key Integrity Protocol (TKIP)
  - Unveiled in late 2002 by the Wi-Fi Alliance and introduced it as Wi-Fi Protected Access (WPA).
  - Final version approved on summer 2004 by IEEE and added 802.1X and AES-CCMP (AES – Counter Mode CBC-MAC Protocol).
    - Named WPA2 by the Wi-Fi Alliance for marketing purpose.

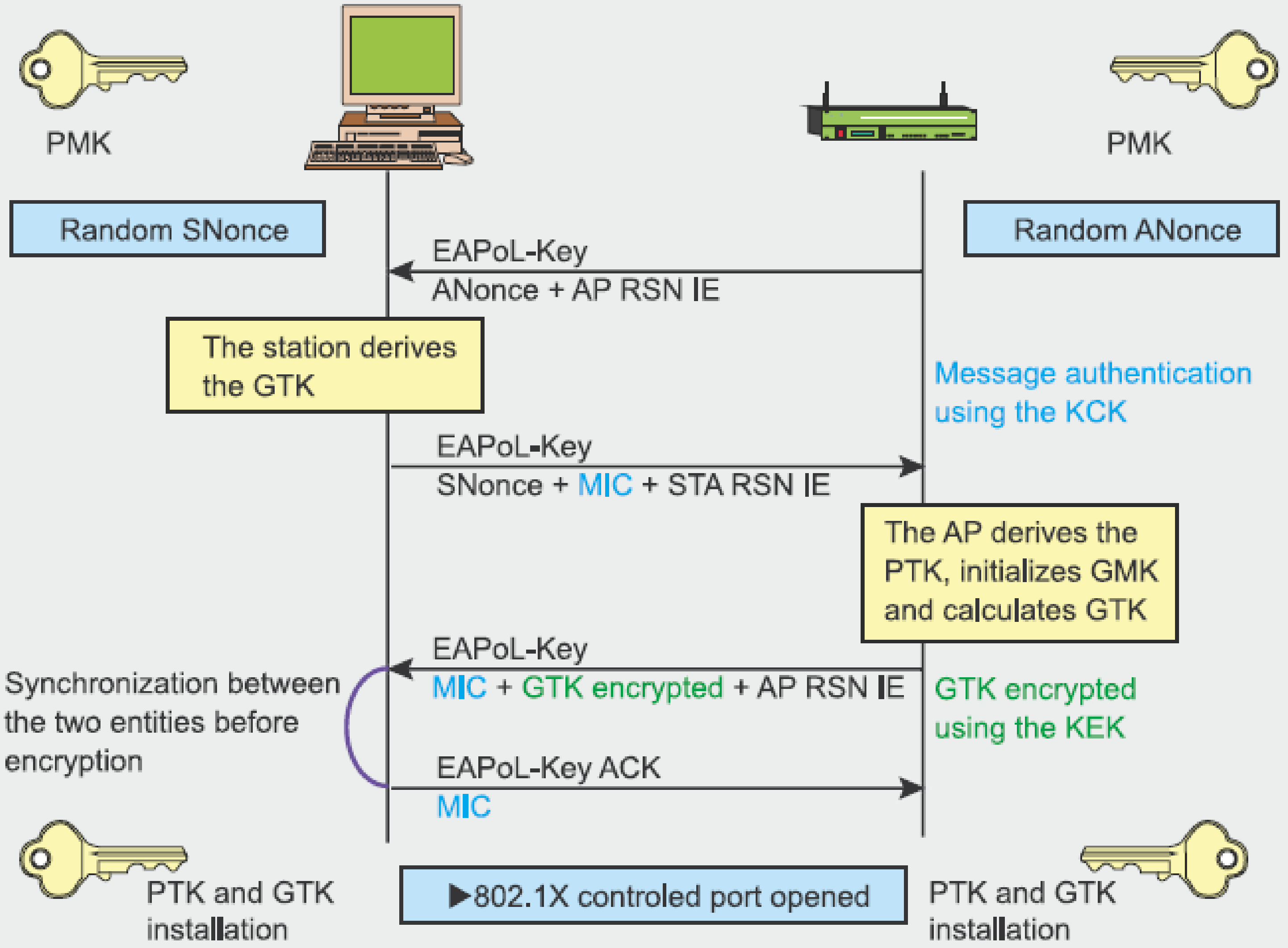
Wireless Network Security (cont’d)

- Temporal Key Integrity Protocol (TKIP)
  - No need hardware upgrade in order to use it.
    - It just kind of a wraps around the pre-existing WEP encryption key (which was way too short) and upgrades it a whole lot to a much more impenetrable 128-bit encryption.
    - Its encryption mechanism and the RC4 algorithm used to power and define WEP, respectively, remained the same.

Wireless Network Security (cont’d)

- WPA2 Pre-Shared Key (PSK)
  - A better form of wireless security than any other basic wireless security method
  - PSK verifies users via a password or identifying code (passphrase) on both the client machine and the AP.
  - A client gains access to the network only if its password matches the APs password.

Wireless Network Security (cont'd)



PMK

PMK

Random SNonce

Random ANonce

EAPoL-Key
ANonce + AP RSN IE

The station derives the GTK

Message authentication using the KCK

EAPoL-Key
SNonce + MIC + STA RSN IE

The AP derives the PTK, initializes GMK and calculates GTK

EAPoL-Key
MIC + GTK encrypted + AP RSN IE

GTK encrypted using the KEK

Synchronization between the two entities before encryption

EAPoL-Key ACK
MIC

PTK and GTK installation

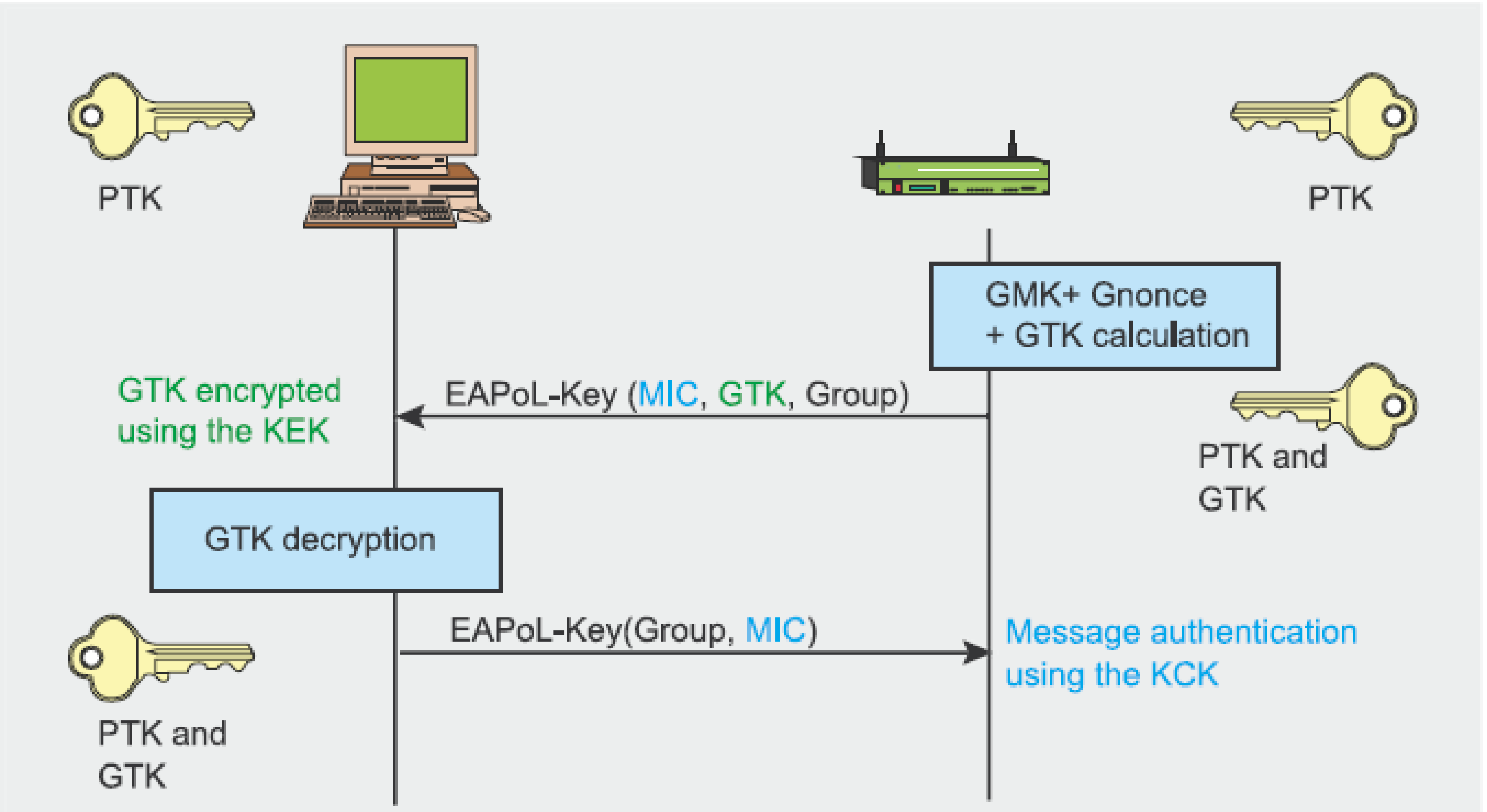
▶802.1X controled port opened

PTK and GTK installation

```
PTK = PRF-X(PMK, « Pairwise key expansion »,
Min(AP_Mac, STA_Mac) || Max(AP_Mac, STA_Mac) ||
Min(ANonce, SNonce) || Max(ANonce, SNonce))
```

four-way handshake

Wireless Network Security (cont'd)



```
GTK = PRF-256(GMK, Group Key Expansion,
 AP_Mac || GNonce))
```

Group Key Handshake

Wireless Network Security (cont’d)

- WPA2 Pre-Shared Key (PSK)
  - PSK is stored on the client station and can be compromised if the client station is lost or stolen.
  - Use a strong PSK passphrase that includes a mixture of letters, numbers, and non-alphanumeric characters.
  - WPA2 can change dynamically while the system is used.
  - The highest level is WPA2-AES

```
> end;
```