

Module 07

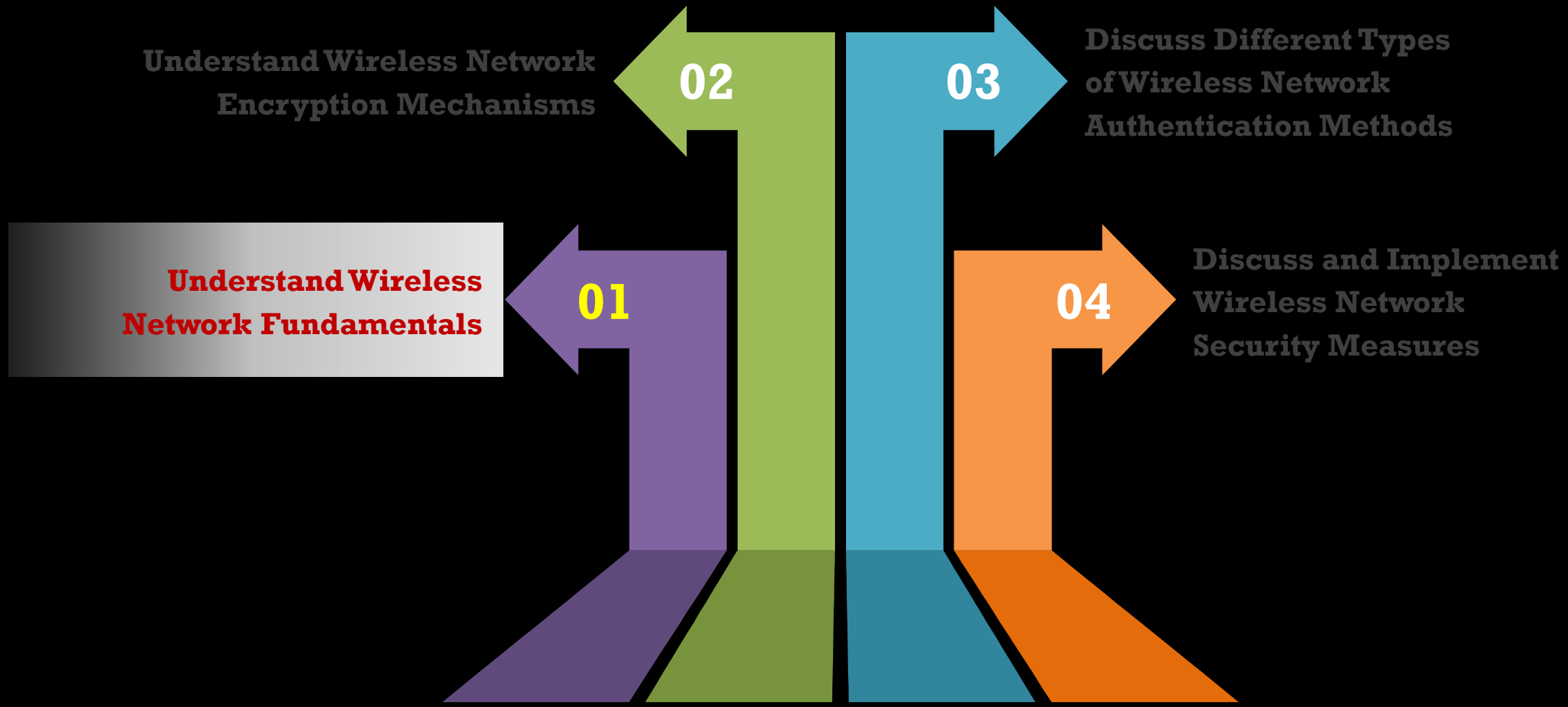
Wireless Network Security



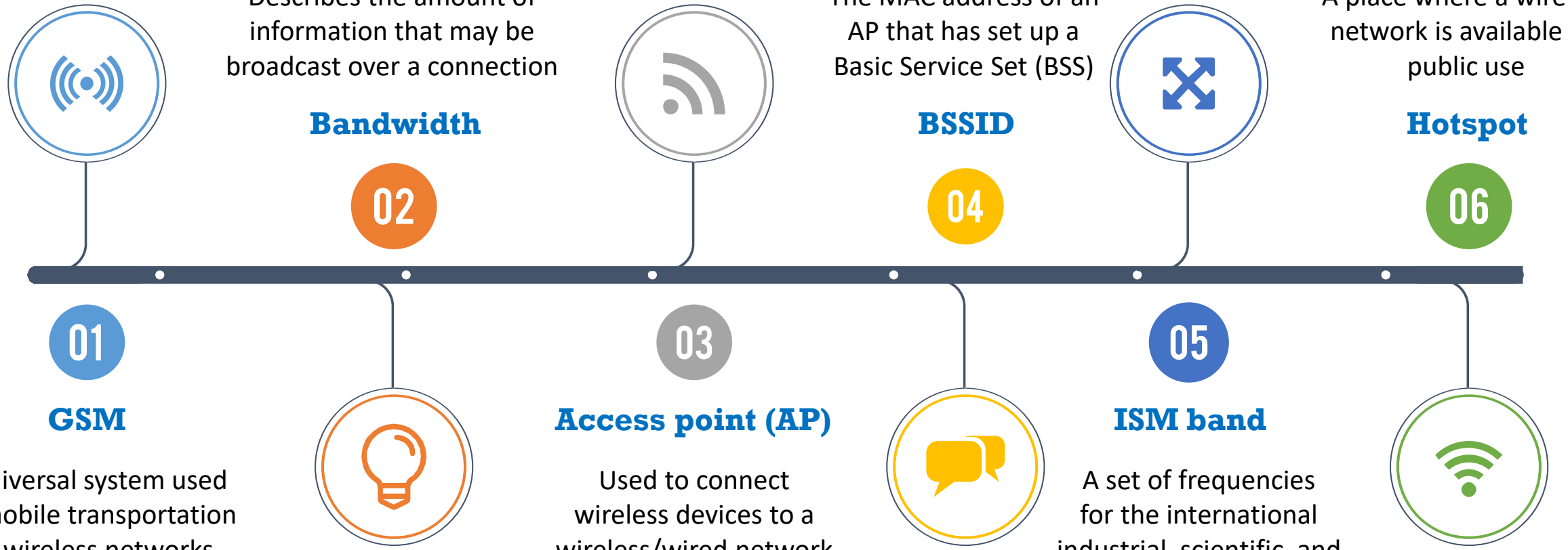
Module Objectives

1. Understanding the Wireless Terminology, Wireless Networks, and Wireless Standards
2. Understanding the Wireless Network Topologies and Classification of Wireless Networks
3. Understanding the Components of a Wireless Network
4. Overview of Wireless Network Encryption Mechanisms
5. Understanding the Different Types of Wireless Network Authentication Methods
6. Understanding Wireless Network Security Measures and Wireless Security Tools

Module Flow


Understand Wireless Network Encryption Mechanisms
02
03
Discuss Different Types of Wireless Network Authentication Methods
Understand Wireless Network Fundamentals
01
04
Discuss and Implement Wireless Network Security Measures

Wireless Terminologies



01

GSM

A universal system used for mobile transportation for wireless networks worldwide

02

Bandwidth

Describes the amount of information that may be broadcast over a connection

03

Access point (AP)

Used to connect wireless devices to a wireless/wired network

04

BSSID

The MAC address of an AP that has set up a Basic Service Set (BSS)

05

ISM band

A set of frequencies for the international industrial, scientific, and medical communities

06

Hotspot

A place where a wireless network is available for public use

Wireless Terminologies (Cont'd)

Association

The process of connecting a wireless device to an AP

Service Set Identifier (SSID)

A unique identifier of 32 alphanumeric characters given to a wireless local area network (WLAN)

Orthogonal Frequency-division Multiplexing (OFDM)

Method of encoding digital data on multiple carrier frequencies

Multiple input, multiple output orthogonal frequency-division multiplexing (MIMO-OFDM)

An air interface for 4G and 5G broadband wireless communications

Direct-sequence Spread Spectrum (DSSS)

An original data signal multiplied with a pseudo-random noise spreading the code

Frequency-hopping Spread Spectrum (FHSS)

A method of transmitting radio signals by rapidly switching a carrier among many frequency channels

Wireless Networks

- Wireless networks use **radio frequency (RF) signals** to connect wireless-enabled devices in a network
- The wireless fidelity (Wi-Fi) technology uses the Institute of Electrical and Electronics Engineers (IEEE) standard of 802.11 and uses radio waves for communication

Advantages

- Installation is easy and **eliminates wiring**
- Access to the network can be from **anywhere** within the range of an access point (AP)
- Public places such as airports, schools, etc., can offer a **constant internet connection** using WLAN



Wireless Technologies

In a wireless network, data transmission occurs by means of **electromagnetic waves** that carry signals over the communication path

Types of Wireless Technologies

Wi-Fi

- It uses **radio waves** or **microwaves** to allow electronic devices to exchange data or connect to the Internet

Bluetooth

- Using Bluetooth technology, data is transmitted between cell phones, computers, and other networking devices over **short distances**

RFID

- It uses **radio frequency** (RF) electromagnetic waves to transfer data for automatic identification and for **tracking tags** attached to objects

WiMAX

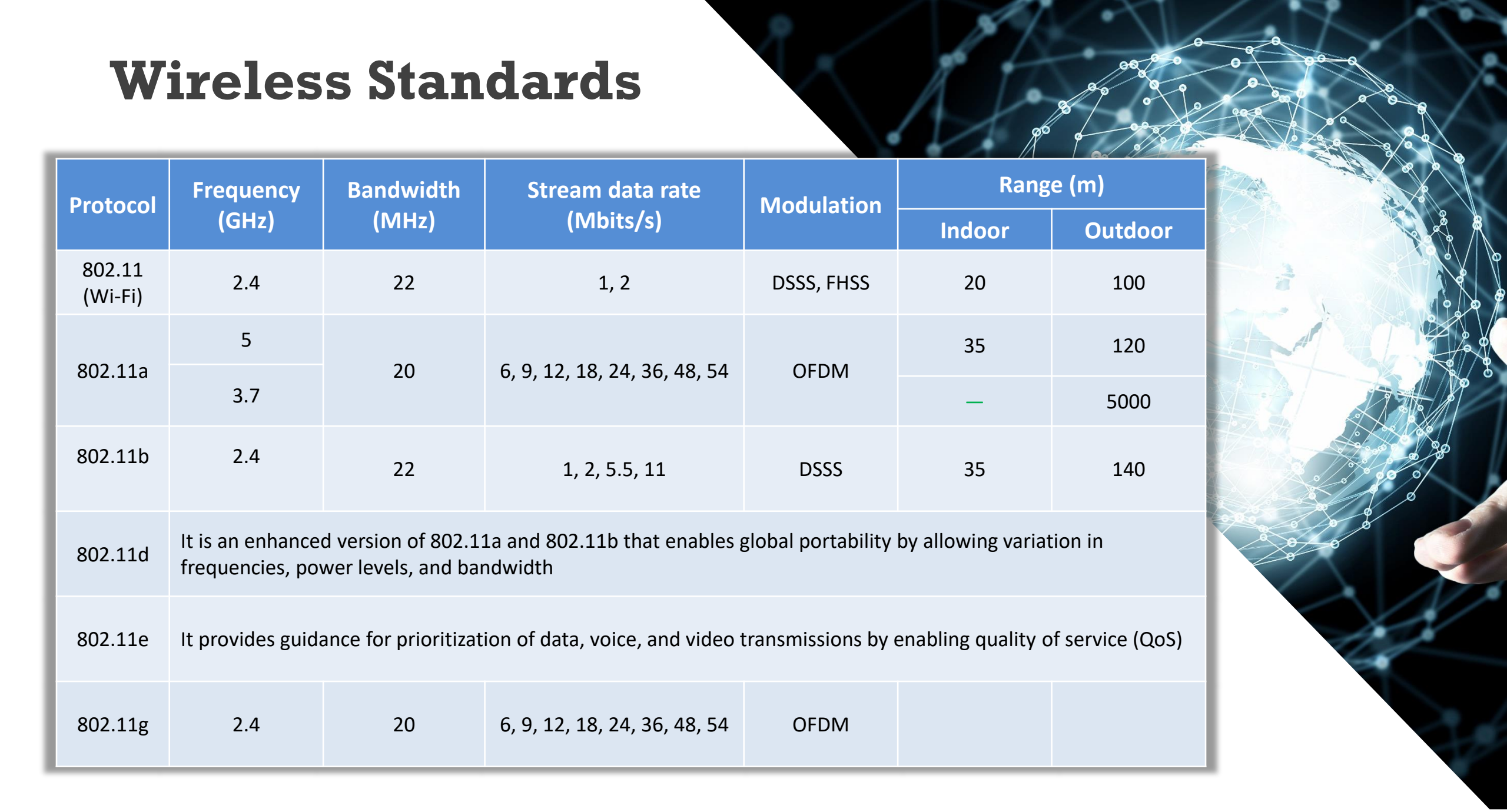
- It uses **long distance** wireless networking and **high-speed Internet** and belongs to the IEEE 802.16 family of wireless networking standards

Wired vs. Wireless Networks

Wired Networks	Wireless Networks
High bandwidth	Low bandwidth
Low bandwidth variation	High bandwidth variation
Low error rates	High error rates
More secure	Less secure
Less equipment dependent	More equipment dependent
Symmetric connectivity	Possible asymmetric connectivity
High-power machines	Low-power machines
High-resource machines	Low-resource machines
Low delay	High delay
Connected operation	Disconnected operation



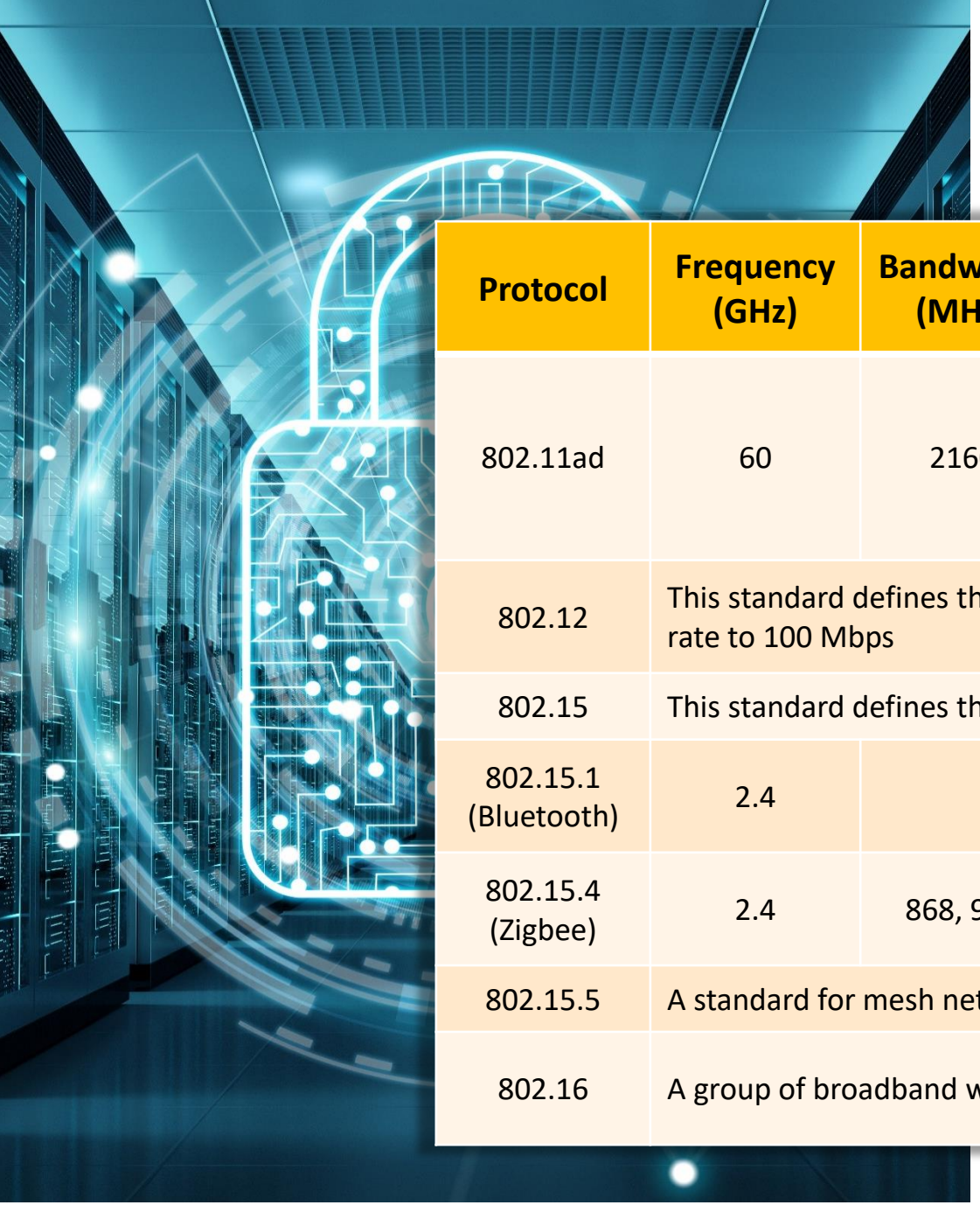
Wireless Standards



Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbits/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11 (Wi-Fi)	2.4	22	1, 2	DSSS, FHSS	20	100
802.11a	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
	3.7				—	5000
802.11b	2.4	22	1, 2, 5.5, 11	DSSS	35	140
802.11d	It is an enhanced version of 802.11a and 802.11b that enables global portability by allowing variation in frequencies, power levels, and bandwidth					
802.11e	It provides guidance for prioritization of data, voice, and video transmissions by enabling quality of service (QoS)					
802.11g	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM		

Wireless Standards (Cont'd)

Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbits/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11i	This is a standard for WLANs that provides **improved encryption** for networks that use the 802.11a, 802.11b, and 802.11g standards					
802.11n	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	MIMO-OFDM	70	150
	2.4	40	15, 30, 45, 60, 90, 120, 135, 150		70	150
802.11ac	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3	MIMO-OFDM	35	
		40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200		35	
		80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3		35	
		160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7		35	
802.11ax	2.4/5/6	40	Up to 2294[F]	MIMO-OFDM	30	120
		80	Up to 4803[F]			
		80+80	Up to 10530			



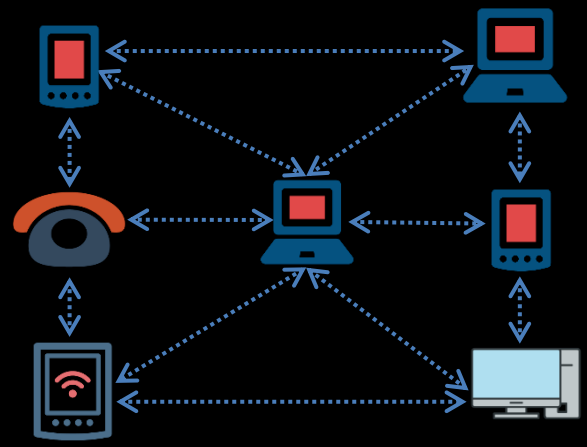
Wireless Standards (Cont'd)

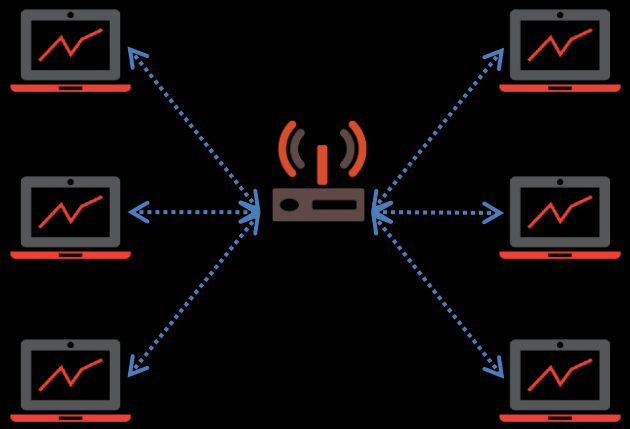
Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbits/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11ad	60	2160	6.75 Gbit/s	OFDM, single carrier, low-power single carrier	60	100
802.12	This standard defines the demand priority and media access control protocol for increasing the Ethernet data rate to 100 Mbps					
802.15	This standard defines the communication specifications for wireless personal area networks (WPANs)					
802.15.1 (Bluetooth)	2.4		1-3 Mbps		10	
802.15.4 (Zigbee)	2.4	868, 900				
802.15.5	A standard for mesh networks with enhanced reliability via route redundancy					
802.16	A group of broadband wireless communication standards for **metropolitan area networks (MANs)**					

Wireless Network Topologies

Ad-hoc Standalone Network Architecture (Independent Basic Service Set (IBSS))

- Devices exchange information with each other similar to that in a **peer-to-peer** communication mode without the need of an AP for communication
- To setup this mode properly, first configure the wireless adapter for all the devices. They should all have the **same channel name** and SSID in order to activate the connections





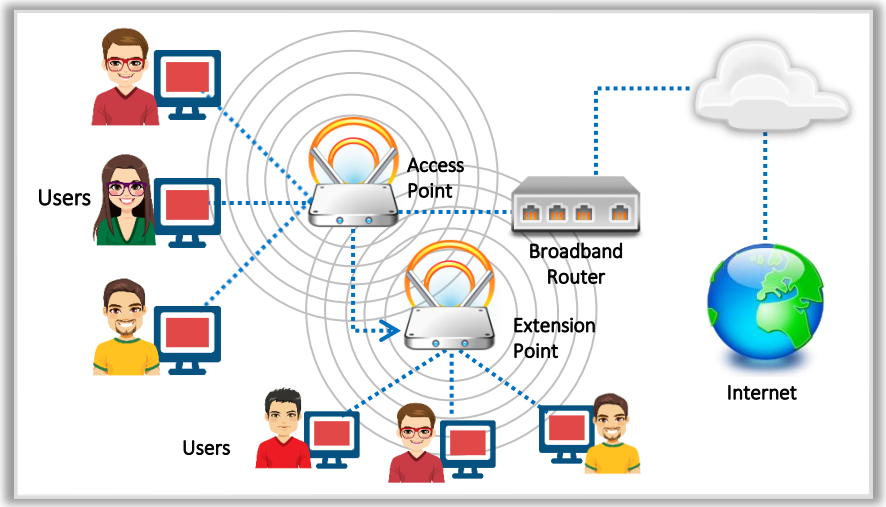
- Devices in the wireless network are connected through an **AP**
- An AP connects to the internet via a modem
- Installed in large organizations

Infrastructure Network Topology (Centrally Coordinated Architecture/ Basic Service Set (BSS))

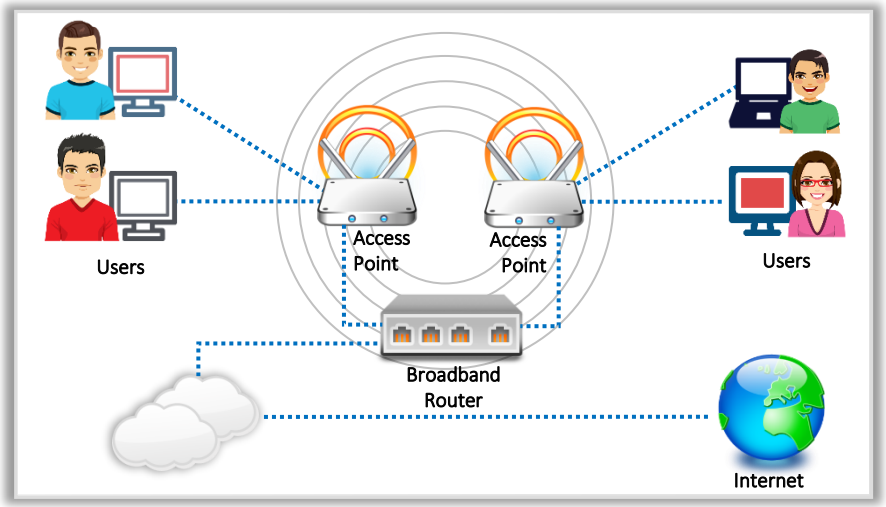
Classification of Wireless Networks

Wireless Networks Based on the Connection

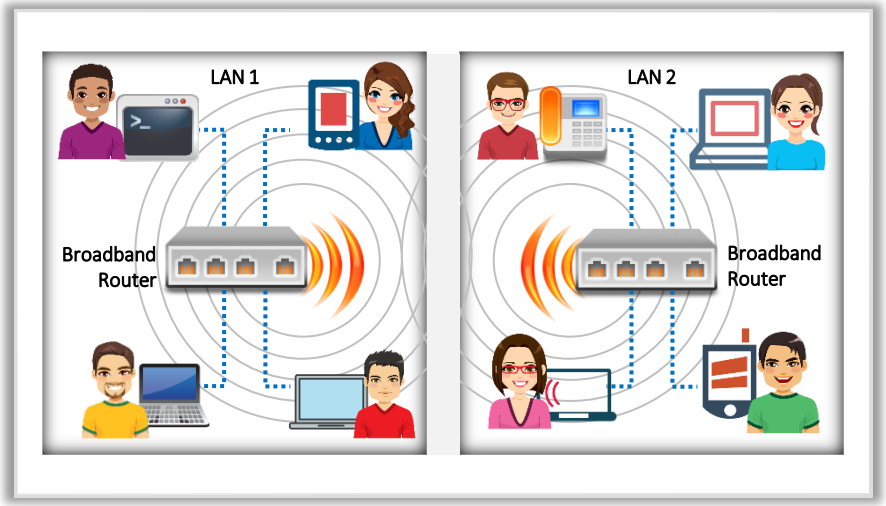
Extension to a Wired Network



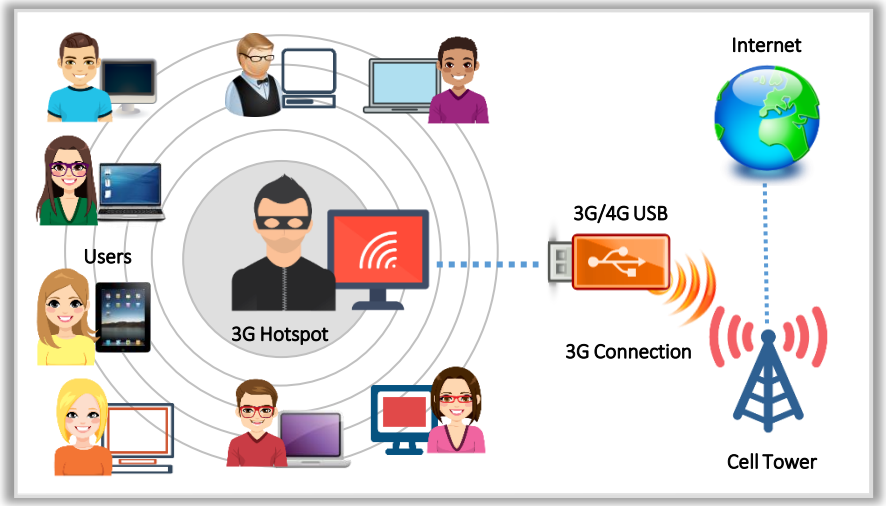
Multiple Access Points



LAN-to-LAN Wireless Network



4G Hotspot



Classification of Wireless Networks (Cont'd)

Wireless Network Based on the Geographic Area Coverage

WLAN

It connects users in a local area with a network. The area may range from a **single room** to an **entire campus**

WWAN

WWAN covers an area **larger than the WLAN**. It can cover a particular region, nation, or even the entire globe



WPAN

It interconnects devices positioned **around an individual**, in which the connections are wireless. It has a very short range

WMAN

It accesses **broadband area networks** by using an exterior antenna. It is a good alternative for a fixed-line network

Components of a Wireless Network



Access Point (AP)

- It is a **hardware device** that allows wireless communication devices to connect to a wireless network via wireless standards such as Bluetooth, Wi-Fi, etc.

Wireless Cards (NIC)

- Systems connected to the wireless network require a network interface cards (NIC) to establish a standard **Ethernet connection**

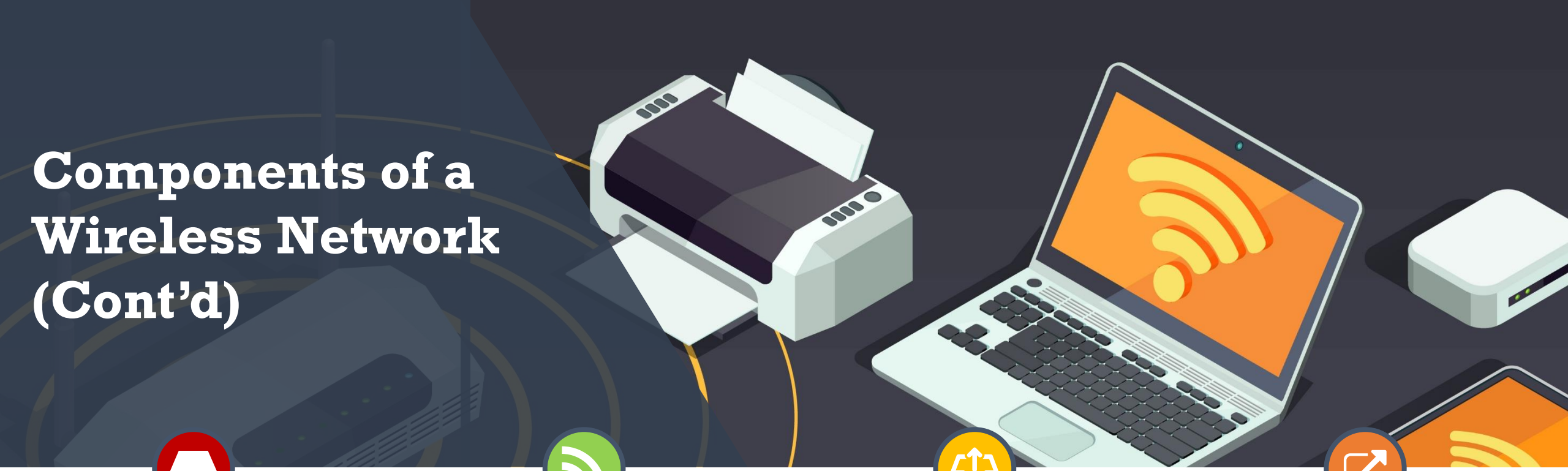
Wireless Modem

- It is a device that receives and transmits **network signals** to other units without requiring physical cabling

Wireless Bridge

- It connects multiple LANs at the medium access control (MAC) layer and is separated either logically or physically. It is used for increasing the **coverage area of the wireless network**

Components of a Wireless Network (Cont'd)



Wireless Repeater

- **Retransmits** the existing signal captured from a wireless router or AP to create a new network

Wireless Router

- Performs the **functions of a router** as well as a wireless AP and provides Internet access to various devices

Wireless Gateways

- **Routes data packets** and functions as a wireless AP. An Internet connection can be shared between multiple stations

Wireless USB Adapter

- **Connects** different devices to a wireless network in order to access the Internet without a computer, router, or any other network device

Components of a Wireless Network (Cont'd)

Antenna

- Converts electrical impulses into **radio waves** and vice versa

Types of Antenna



Directional Antenna

a single direction



Parabolic Grid Antenna

satellite dish



Dipole Antenna

client connections



Omnidirectional Antenna

360° horizontal radiation



Yagi Antenna

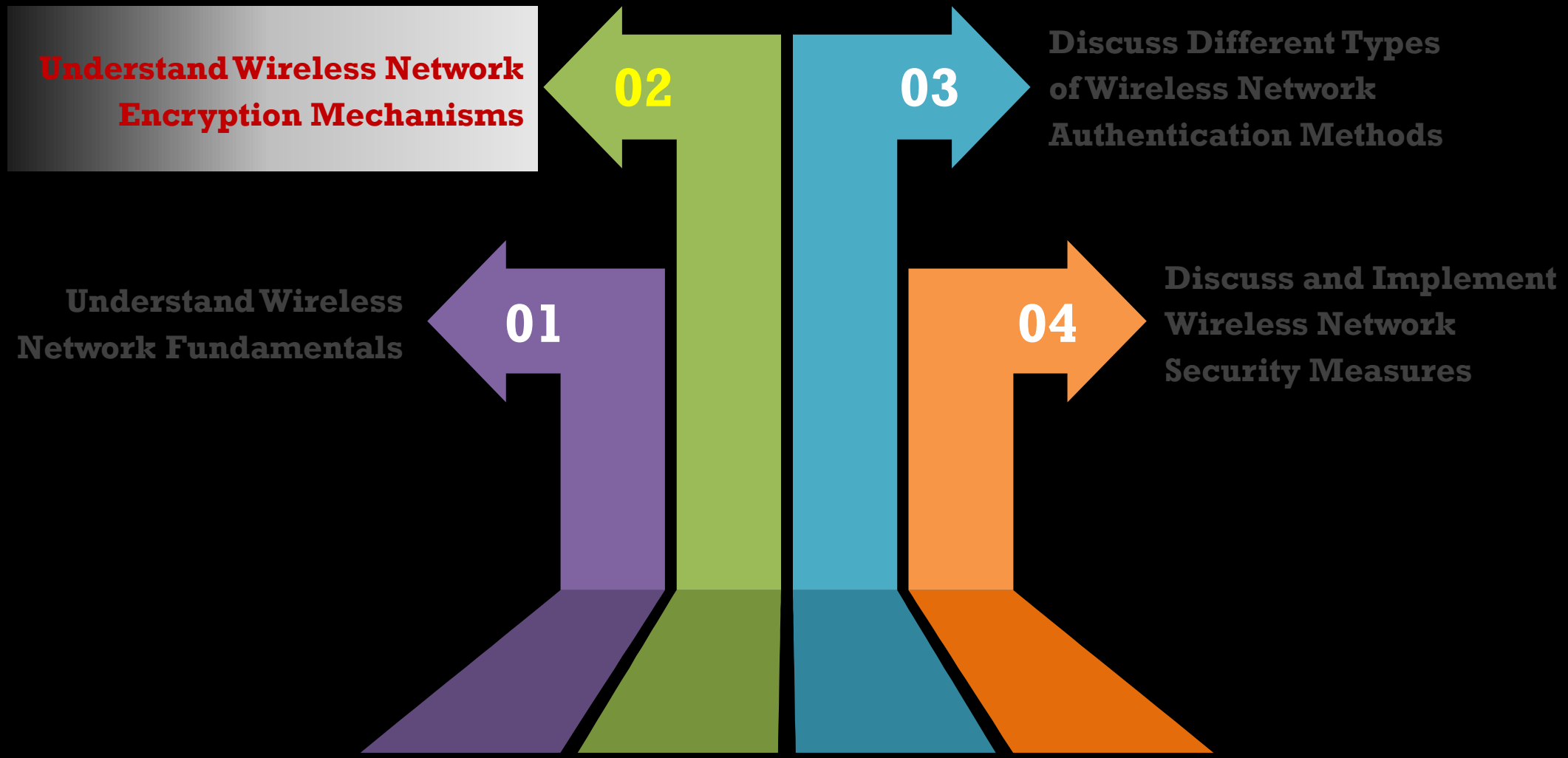
unidirectional antenna



Reflector Antennas

concentrating electromagnetic energy

Module Flow


Understand Wireless Network Encryption Mechanisms
02
03
Discuss Different Types of Wireless Network Authentication Methods
Understand Wireless Network Fundamentals
01
04
Discuss and Implement Wireless Network Security Measures

Types of Wireless Encryption



802.11i — An IEEE amendment that specifies security mechanisms for **802.11** wireless networks

WEP — An **encryption** algorithm for IEEE 802.11 wireless networks

EAP — Supports multiple authentication methods, such as **token cards**, **Kerberos**, and certificates

LEAP — A proprietary version of **EAP** developed by Cisco

WPA — An advanced wireless encryption protocol using **TKIP** and **MIC** to provide stronger encryption and authentication

TKIP — A security protocol used in **WPA** as a replacement for WEP

Types of Wireless Encryption (Cont'd)



WPA2	An upgrade to WPA using **AES** and **CCMP** for wireless data encryption
AES	A symmetric-key encryption, used in **WPA2** as a replacement for TKIP
CCMP	An encryption protocol used in WPA2 for stronger encryption and authentication
WPA2 Enterprise	Integrates **EAP** standards with WPA2 encryption
RADIUS	A centralized **authentication** and **authorization** management system
PEAP	A protocol that **encapsulates** the **EAP** within an encrypted and authenticated transport layer security (TLS) tunnel
WPA3	A third-generation Wi-Fi security protocol that uses **GCMP-256** for encryption and HMAC-SHA-384 for authentication

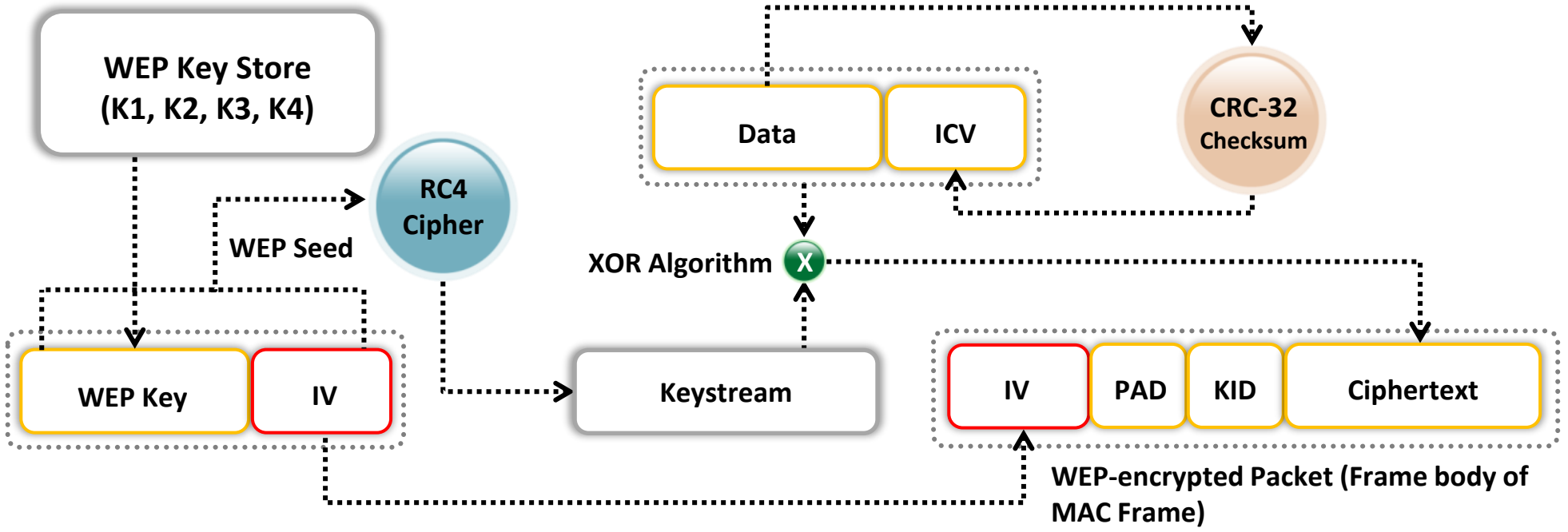
Wired Equivalent Privacy (WEP) Encryption

WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to that of a wired LAN

WEP **uses a 24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmissions

It has significant vulnerabilities and design flaws and **can therefore be easily cracked**

How WEP Works

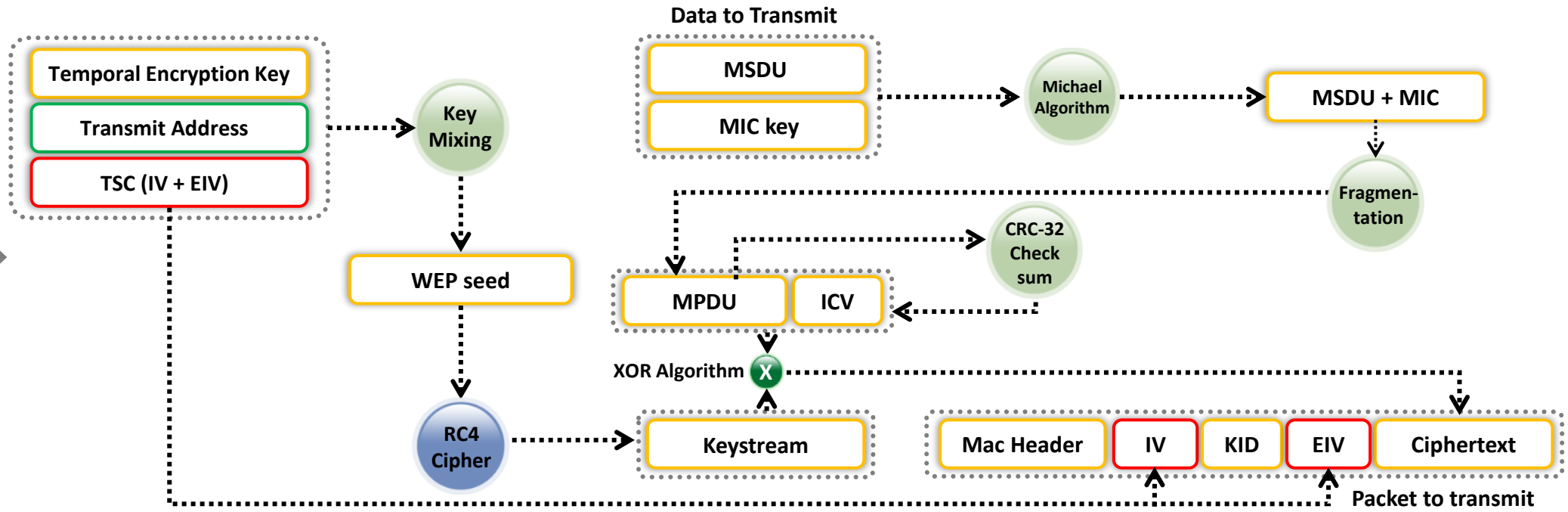


Wi-Fi Protected Access (WPA) Encryption

- WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication

- WPA uses TKIP to eliminate the weaknesses of WEP by including **per-packet mixing functions**, **message integrity checks**, **extended initialization vectors**, and **re-keying mechanisms**

How WPA Works



WPA2 Encryption

upgrade to WPA

CCMP

an AES-based encryption mode

Modes of Operation

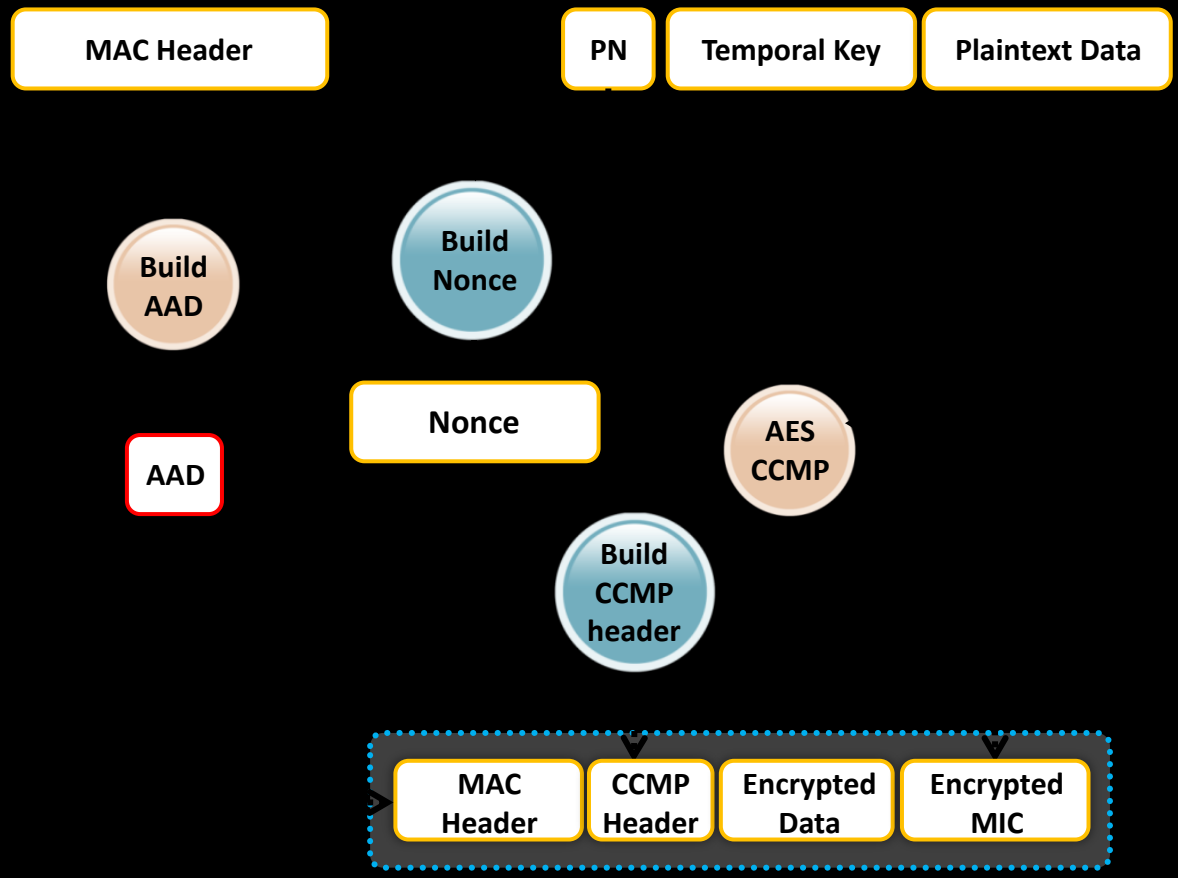
WPA2-Personal

- ✓ It uses a set-up password (**pre-shared Key**, PSK) to protect unauthorized network accesses
- ✓ In PSK mode, each wireless network device encrypts the network traffic using a 128-bit key, which is derived from a passphrase of 8 to 63 ASCII characters

WPA2-Enterprise

- ✓ It includes **EAP** or **RADIUS** for centralized client authentication using multiple authentication methods, such as token cards, and Kerberos
- ✓ Users are assigned **login credentials** by a centralized server, which they must present when connecting to the network

How WPA2 Works



WPA3 Encryption

WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the **AES-GCMP 256** encryption algorithm



Modes of Operation

WPA3 - Personal

- It is mainly used to deliver **password-based authentication** using the SAE protocol, also known as Dragonfly Key Exchange
- It is resistant to offline dictionary attacks and key recovery attacks

WPA3 - Enterprise

- It **protects sensitive data** using many cryptographic algorithms
- It provides authenticated encryption using GCMP-256
- It uses HMAC-SHA-384 to generate cryptographic keys
- It uses ECDSA-384 for exchanging keys

Comparison of WEP, WPA, WPA2, and WPA3

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256



WEP, WPA	Should be replaced with more secure WPA and WPA2
WPA2	Incorporates protection against forgery and replay attacks
WPA3	Provides enhanced password protection and secured IoT connections; encompasses stronger encryption techniques

Issues in WEP, WPA, and WPA2



Issues in WEP

- CRC-32 does not ensure complete cryptographic integrity
- IVs are 24 bits and sent in cleartext
- Vulnerable to **known plaintext attacks**
- Prone to **password cracking attacks**
- Lack of centralized key management



Issues in WPA

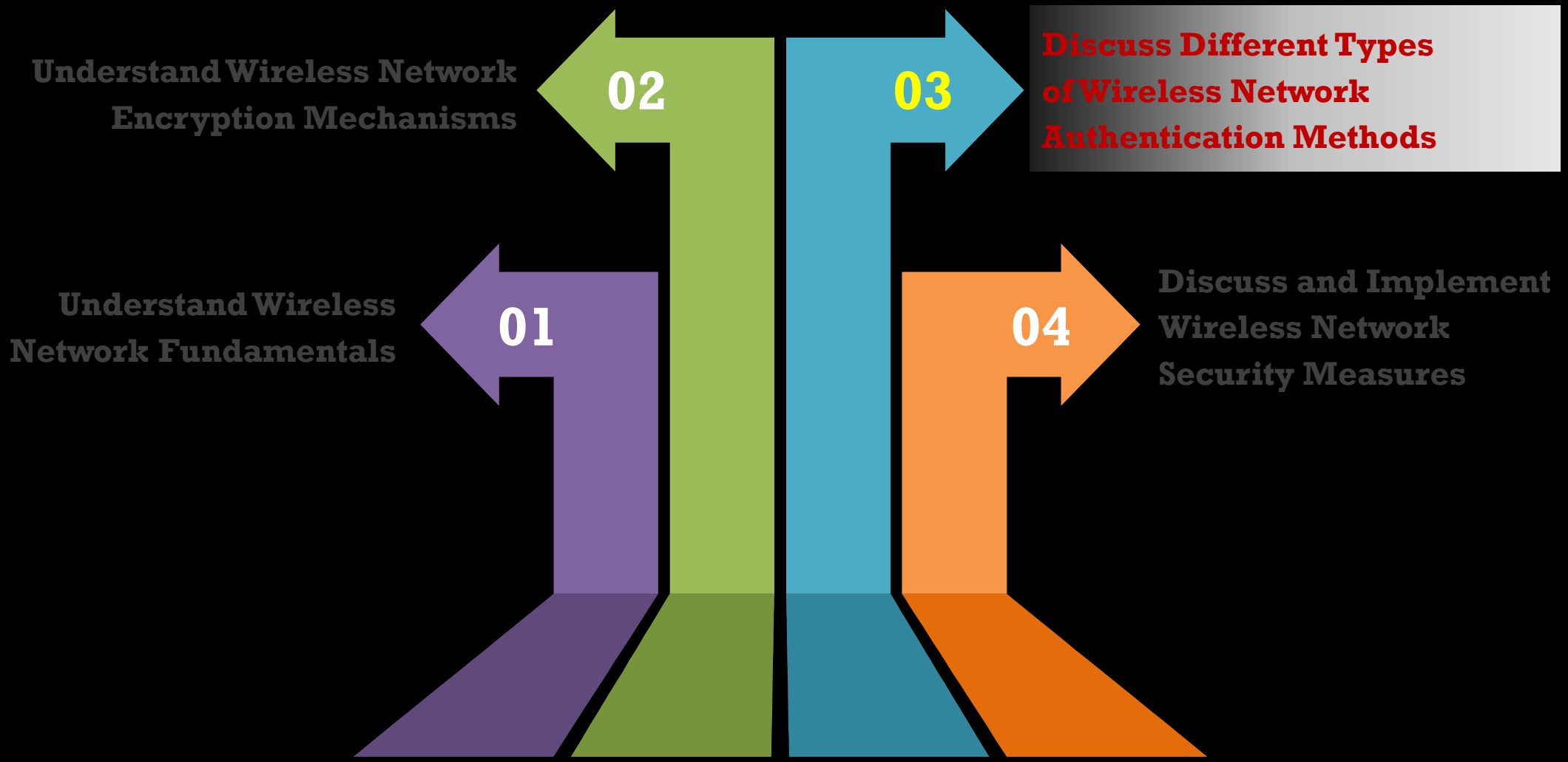
- Pre-shared key is vulnerable to **eavesdropping** and dictionary attacks
- Lack of forward secrecy
- WPA-TKIP is vulnerable to **packet spoofing** and decryption attacks
- Insecure random number generator (RNG) in WPA allows the **discover of GTK** generated by AP
- Vulnerabilities in TKIP allow attackers to guess the IP address of the subnet



Issues in WPA2

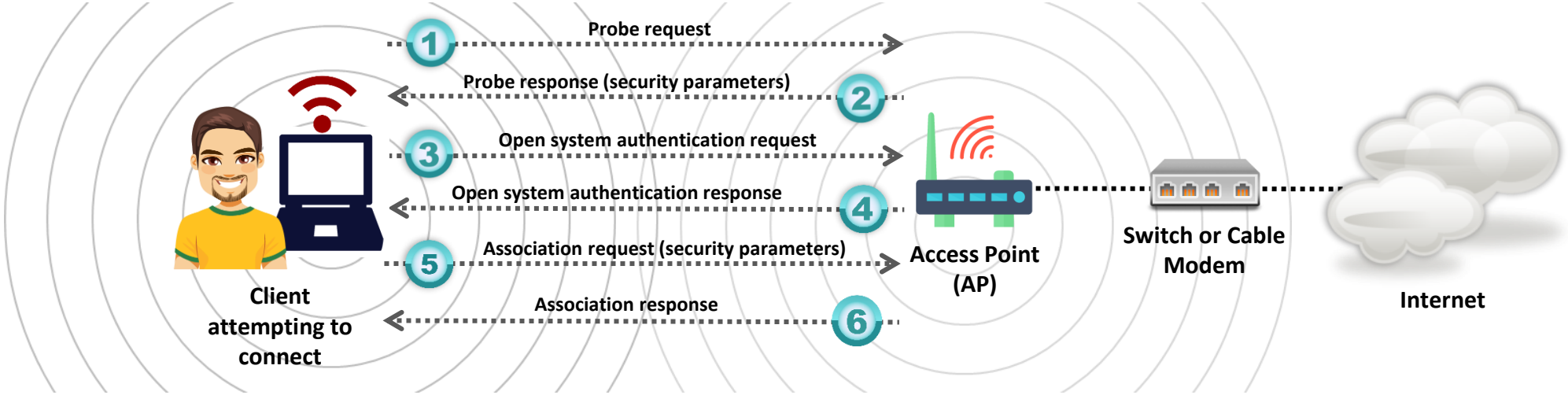
- Pre-shared key is vulnerable to eavesdropping and **dictionary attacks**
- Lack of forward secrecy
- Hole96 vulnerability makes WPA2 vulnerable to **MITM and DoS attacks**
- Insecure random number generator (RNG) in WPA2 allow attackers to **discover GTK** generated by AP
- **KRACK vulnerabilities** make WPA2 vulnerable to packet sniffing, connection hijacking, malware injection, and decryption attacks

Module Flow


Understand Wireless Network Encryption Mechanisms
02
03
Discuss Different Types of Wireless Network Authentication Methods
Understand Wireless Network Fundamentals
01
04
Discuss and Implement Wireless Network Security Measures

Wi-Fi Authentication Methods: Open System Authentication

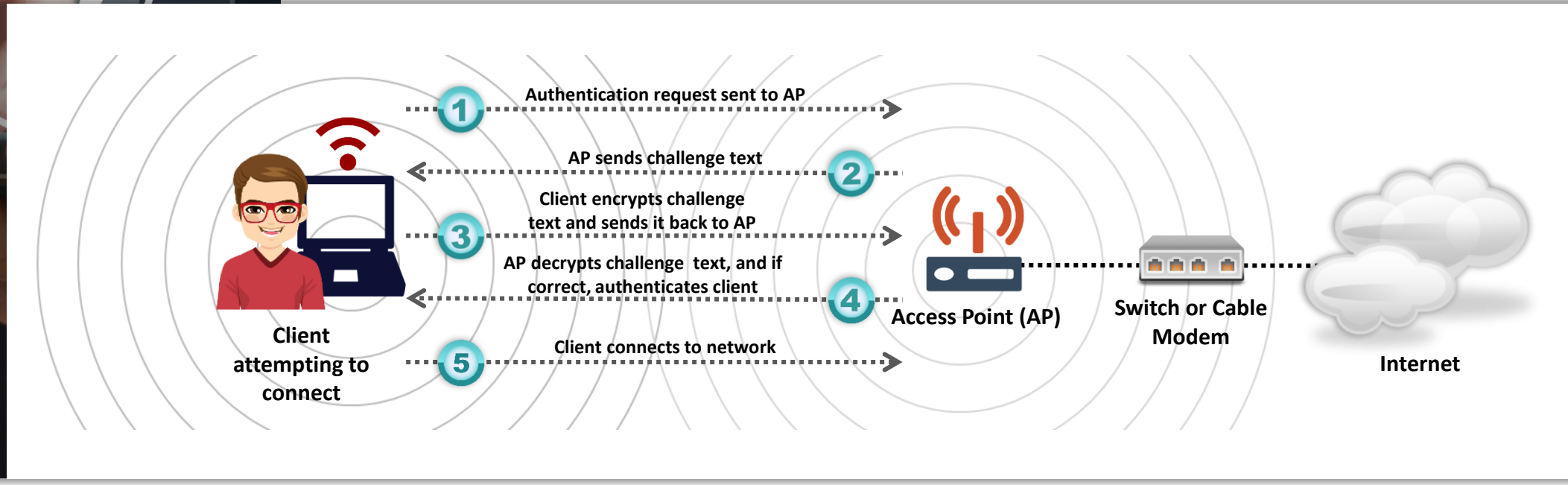
Any wireless device can be **authenticated** with the AP, thus allowing the device to transmit data only when its WEP key **matches** to that of the AP



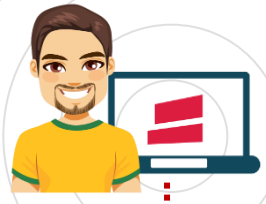


Wi-Fi Authentication Methods: Shared Key Authentication

- The station and AP use the **same WEP key** to provide authentication, which means that this key should be **enabled** and configured manually on both the **AP** and **client**



Wi-Fi Authentication Process Using a Centralized Authentication Server



Client



Access Point



RADIUS Server

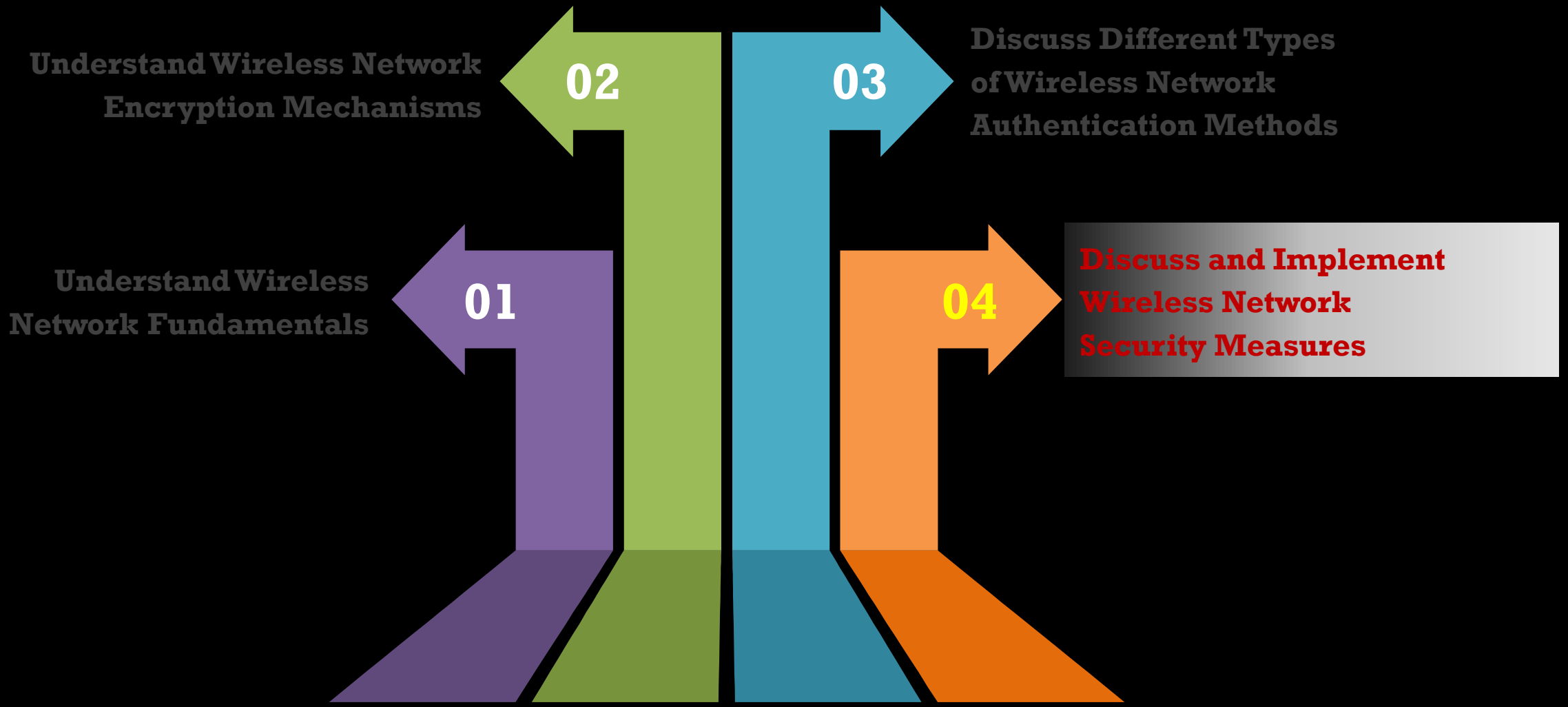
1. Client requests connection
2. AP sends an EAP-Request to determine identity
3. EAP-Response with identity
4. Forwards the identity to the RADIUS server using the uncontrolled port
5. Sends a request to the wireless client via the AP specifying the authentication mechanism to be used
6. The wireless client responds to the RADIUS server with its credentials via the AP
7. Sends an encrypted authentication key to the AP if the credentials are acceptable
8. Sends a multicast/global authentication key encrypted with a per-station unicast session key







Module Flow


Understand Wireless Network Encryption Mechanisms
02
03
Discuss Different Types of Wireless Network Authentication Methods
Understand Wireless Network Fundamentals
01
04
Discuss and Implement Wireless Network Security Measures

Wireless Network Security Measures

Wireless Network Security Techniques

01 Create an inventory of wireless devices

02 Placement of the wireless AP and antenna

03 Disable SSID broadcasting

04 Select a strong wireless encryption mode



05 Defend against WPA cracking

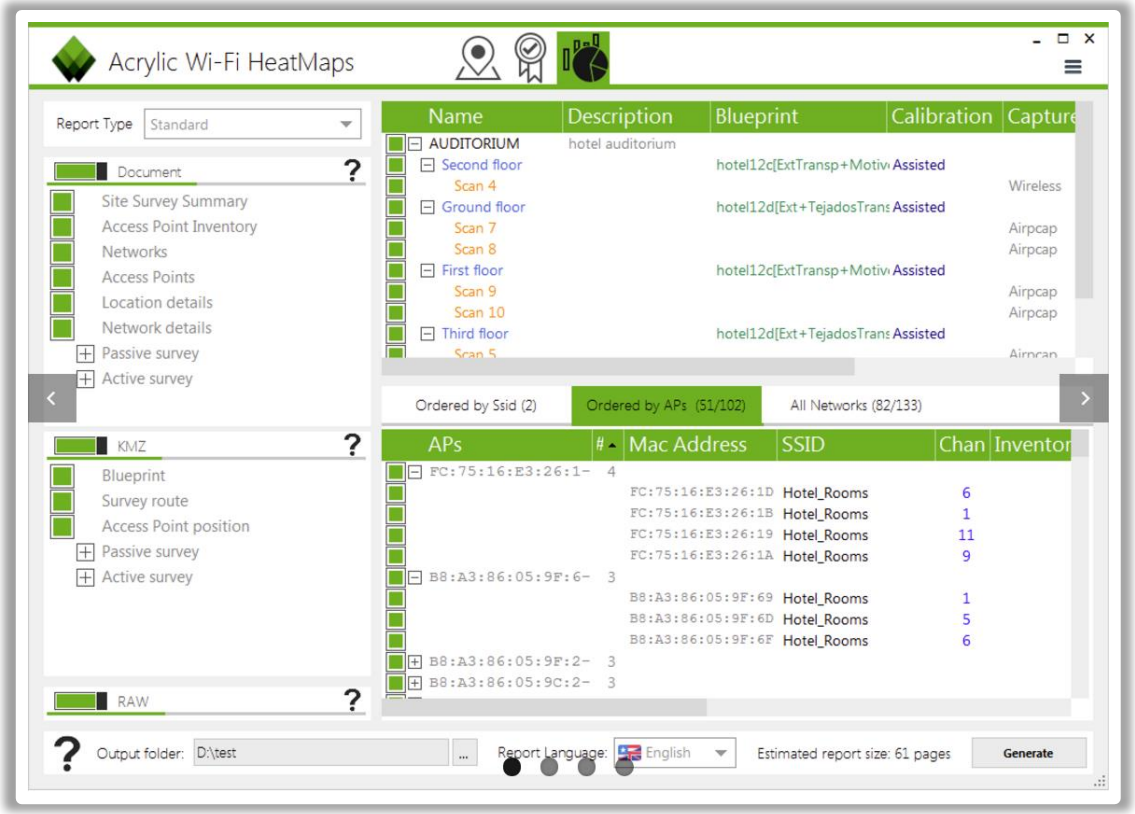
06 Detect rogue APs

07 Locate rogue APs

08 Configure the security on wireless routers

Creating an Inventory of Wireless Devices

- Identify and document all the client devices according to the make/models/applications, encryption, firmware, wireless channel, etc.
- This helps the network defenders to **manage and monitor** the wireless devices in the network



#	Make	Model	Operating System	Strongest Authentication Mode	Best Firmware Level	802.11 Radio Type	Maximum Output Power
A	Intermec	CK31	Win CE .NET	WPA2/802.1x	4.20	b/g	17 dBm
B	Symbol	9090G	Windows Mobile	WPA2/802.1x	5.1.70	a/b/g	20 dBm
C	Vocollect	Talkman T5	Proprietary Voice	WPA-PSK	4.20	b only	12 dBm
D	Symbol	6846	MS-DOS	WEP	-	b only	20 dBm
E	Xybernaut Atigo	S310LX	Windows XP	WPA2/802.1x	5.0	a/b/g	20 dBm

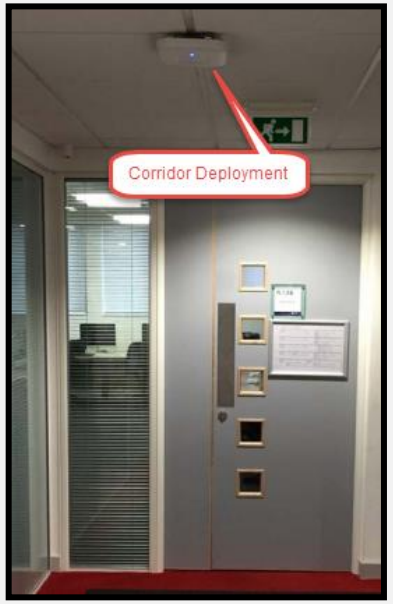
https://www.acrylicwifi.com

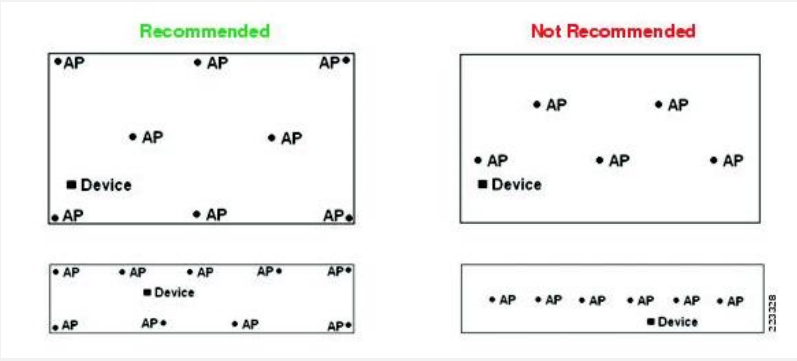
Placement of a Wireless AP

- Guidelines for AP mounting:
  - ✓ Place APs in central locations
  - ✓ Install an AP on the ceiling
  - ✓ Avoid placing APs too high on ceilings
  - ✓ Avoid mounting an AP on a wall as it may restricts its **360° coverage**
  - ✓ Avoid installing APs in corridors
  - ✓ Avoid installing APs above suspended ceilings
  - ✓ Use locks and a plastic sarel enclosure to secure the AP from theft
  - ✓ Avoid enclosing the AP in a metal cage
  - ✓ Keep the AP away from metal objects

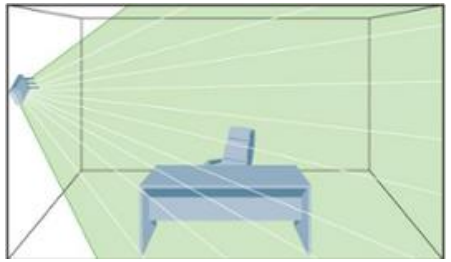


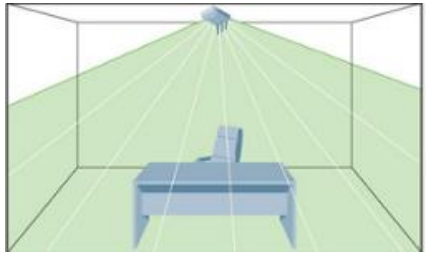




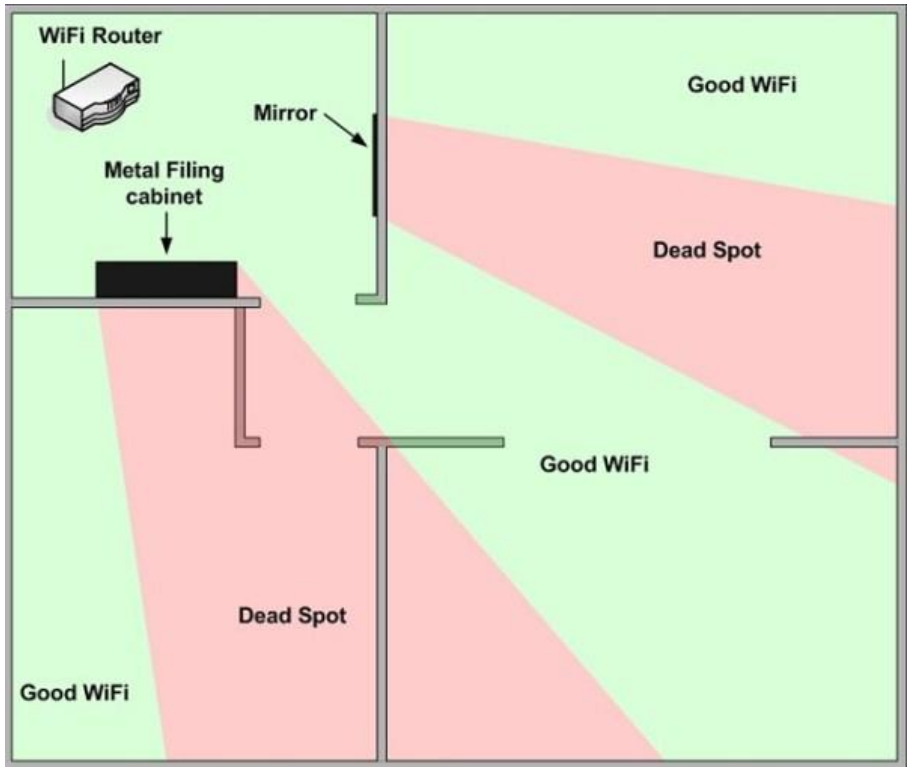


Placement of a Wireless Antenna





- Guidelines for antenna placement:
  - ✓ Use the trial-and-error method to select an appropriate location and direction
  - ✓ Place the AP antenna in a **perpendicular direction**
  - ✓ Avoid keeping the antenna at an angle of 45°
  - ✓ Point the antenna gain towards users
  - ✓ Know the antenna radiation patterns
  - ✓ Do not place obstructions or objects that interfere with the function of the antenna
  - ✓ The use of external antennas as integrated antennas has a limitation

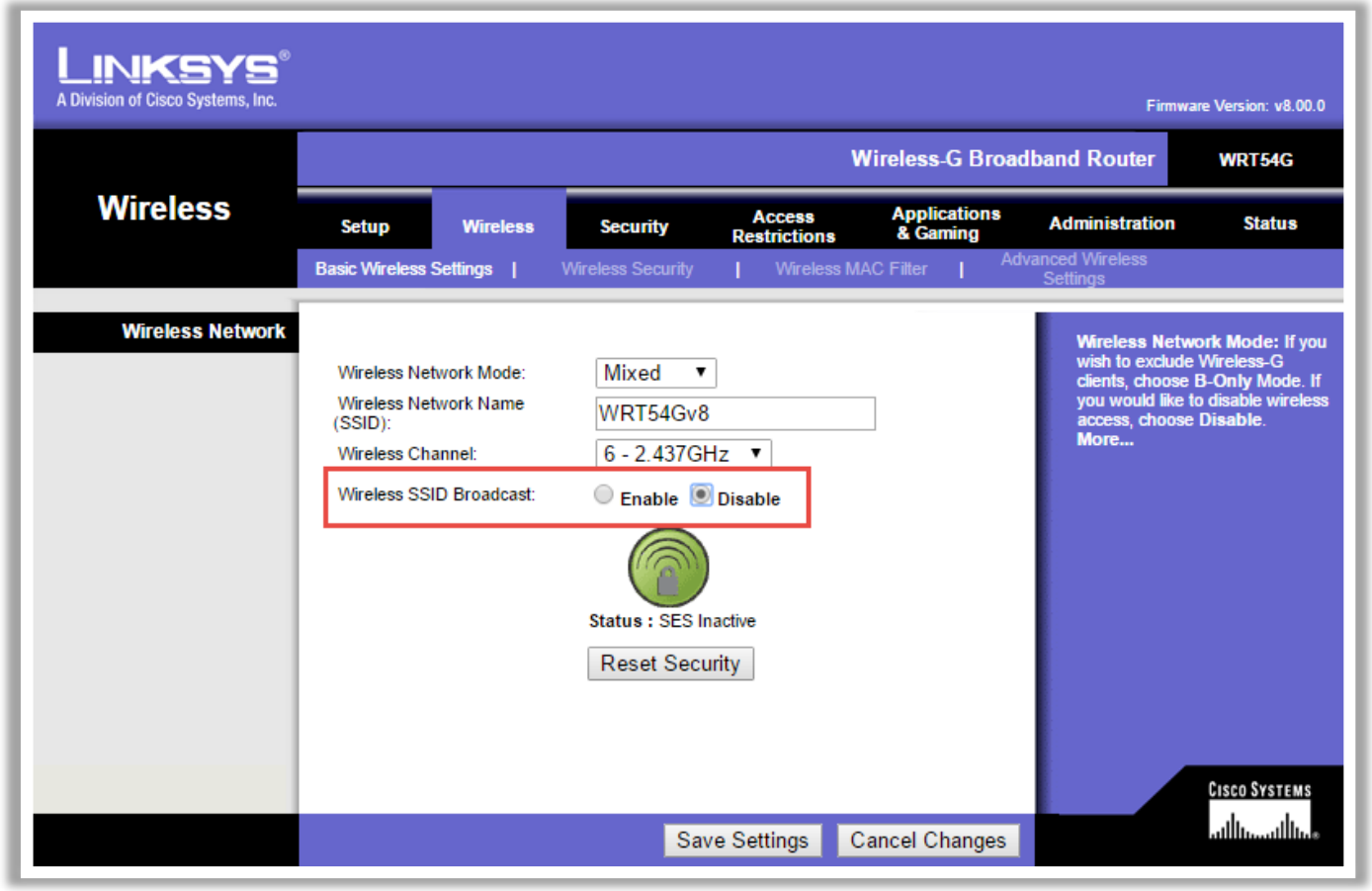


Disable SSID Broadcasting

If the SSID is broadcast, the AP will announce its presence and name, allowing everyone to attempt to authenticate and connect to the wireless network

The SSID broadcast should be **disabled**. In this scenario, an AP will only broadcast its presence, but not its name.

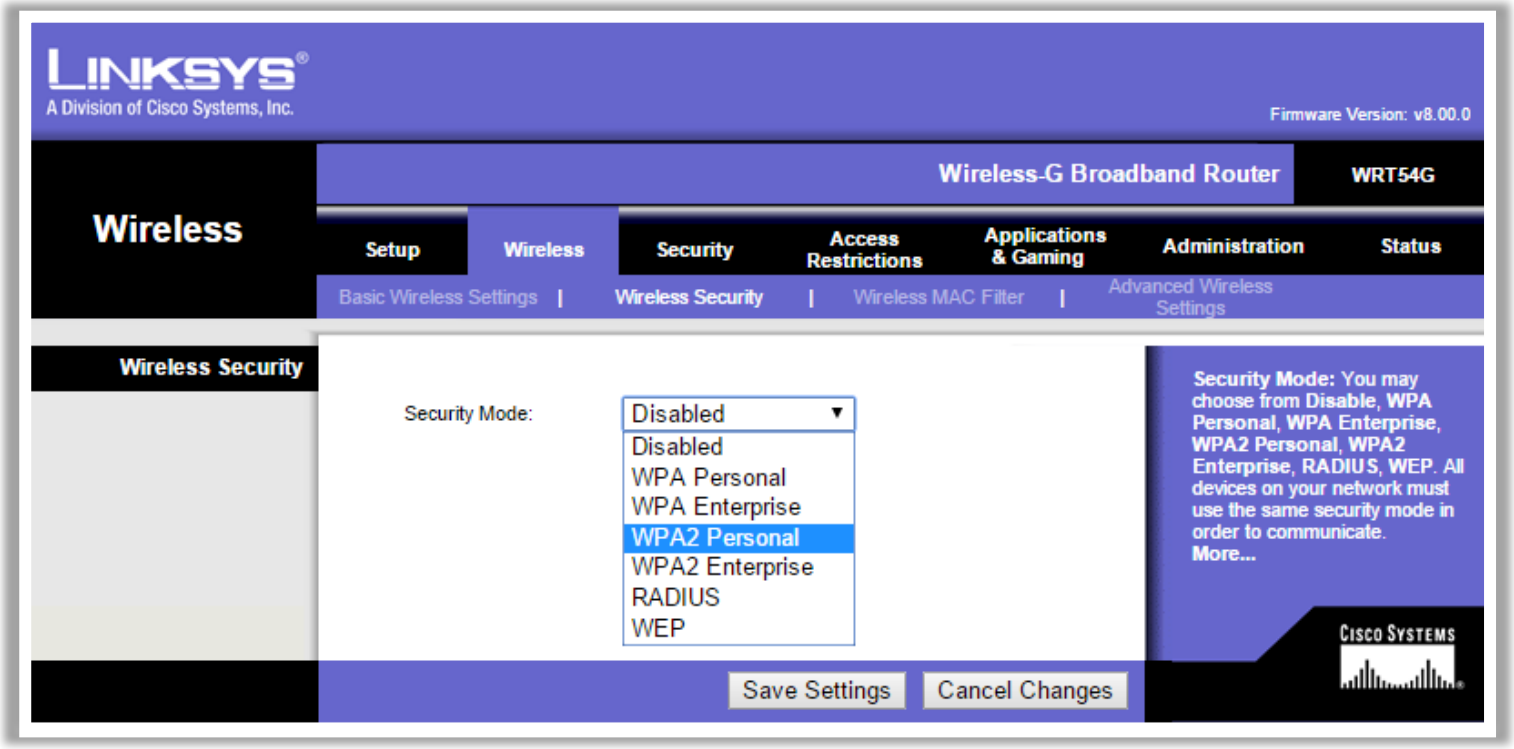
This **discourages unauthorized association** requests to the network and permits connections from legitimate users to the wireless network who have the correct SSID



Selecting a Strong Wireless Encryption Mode

- A strong **wireless encryption mode** should be selected for the wireless network





Order of preference for choosing an encryption mode:

01 WPA3

02 WPA2 Enterprise with RADIUS

03 WPA2 Enterprise

04 WPA2 PSK

05 WPA Enterprise

06 WPA

07 WEP

Defending Against WPA Cracking

- Select a **random passphrase** that is not made up of dictionary words
- Select a complex passphrase which contains a minimum of **20 characters** and change the passphrase at regular intervals
- Use WPA3 /WAP2 **encryption** only
- Set the client settings properly (e.g., validate the server, specify the server address, do not prompt for new servers, etc.)
- Use a **virtual private network (VPN)** such as a remote access VPN, Extranet VPN, Intranet VPN, etc.
- Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity



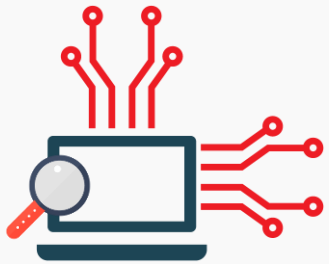
Detecting Rogue Access Points

Wireless Scanning

- Performs a wireless network scanning to detect the presence of **wireless APs** in the vicinity
- Discovery of an AP not listed in the wireless device inventory indicates the presence of a rogue AP
- Use **wireless discovery tools** such as inSSIDer, NetSurveyor, NetStumbler, Vistumbler, Kismet, etc., to detect wireless networks

Wired Network Scanning

- Use network scanners such as **Nmap** to identify APs on the network. This will help in locating rogue devices on the wired network



Simple Network Management Protocol (SNMP) Polling

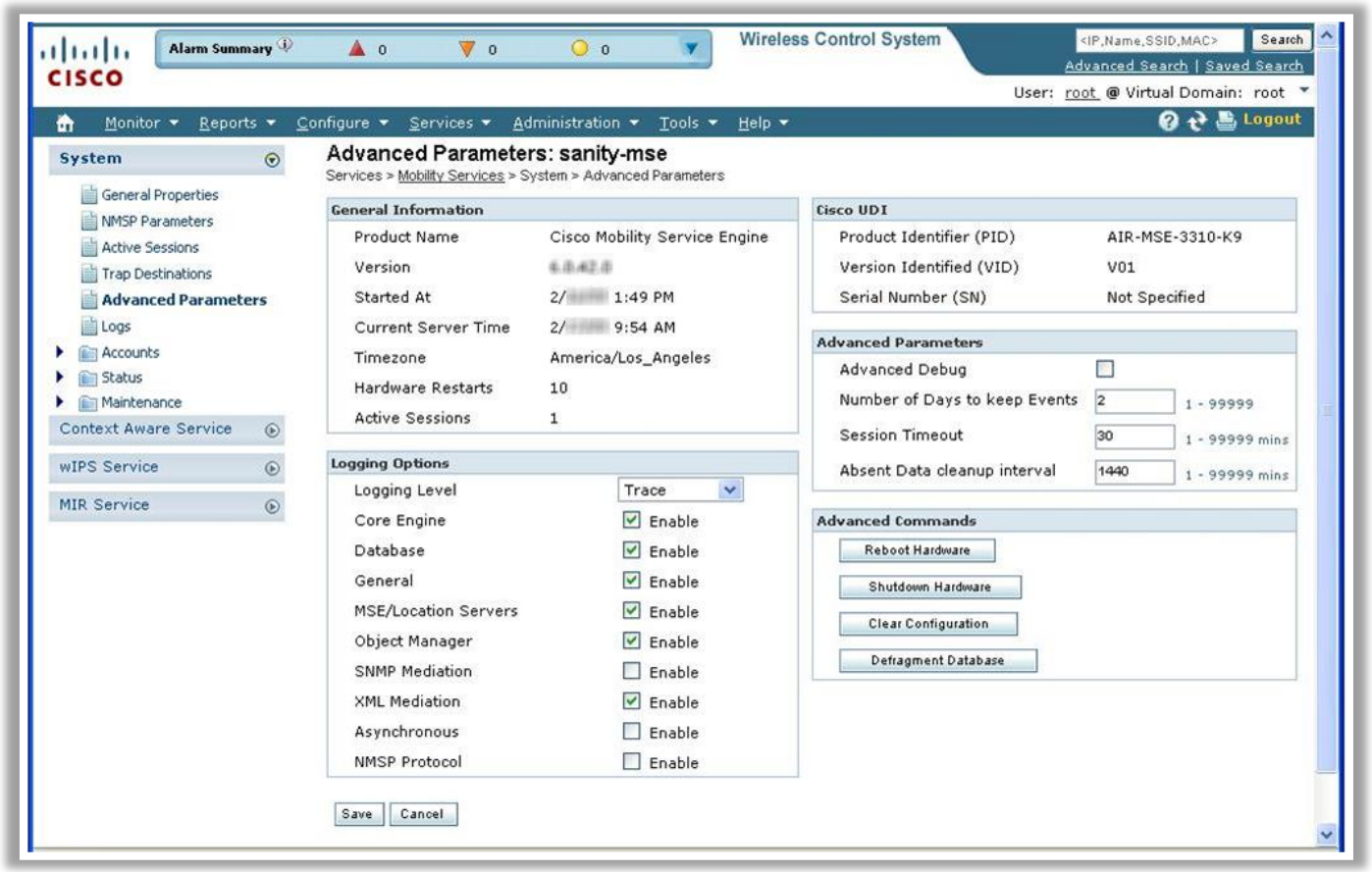
- Use the **SNMP** to identify the IP devices attached to the wired network
- Use the SNMP detection utilities such as SolarWinds SNMP scanner, Lansweeper SNMP scanner, etc., to identify the SNMP-enabled devices on the network

Note: To use SNMP polling, the SNMP service on all IP devices in the network should be enabled.

Wireless Security Tools

Cisco Adaptive Wireless IPS

- It provides wireless-network **threat detection and mitigation** against malicious attacks and security vulnerabilities



https://www.cisco.com

AirMagnet WiFi Analyzer PRO
https://www.netally.com

RFProtect
https://www.arubanetworks.com

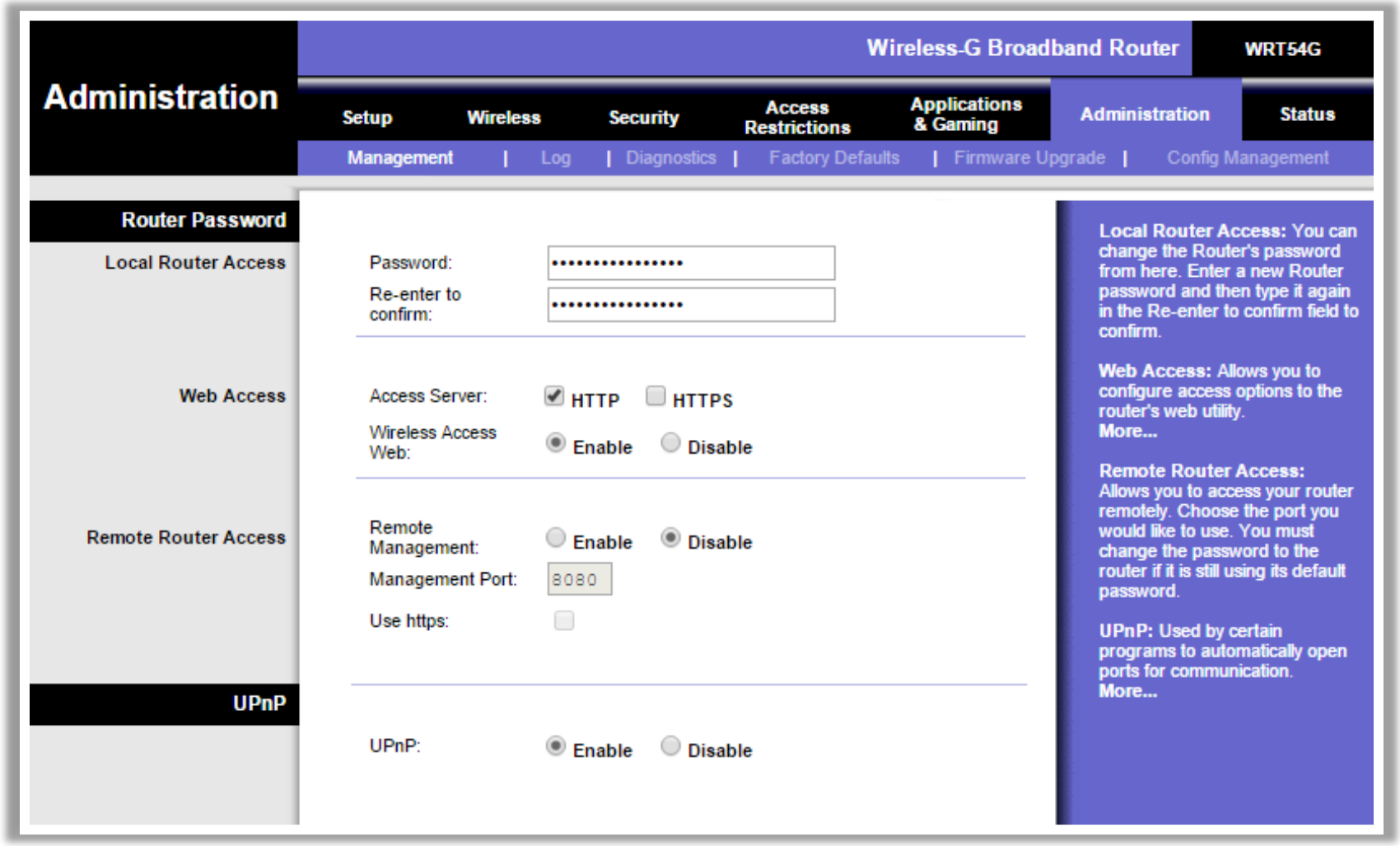
Fern Wifi Cracker
https://github.com

OSWA-Assistant
http://securitystartshere.org

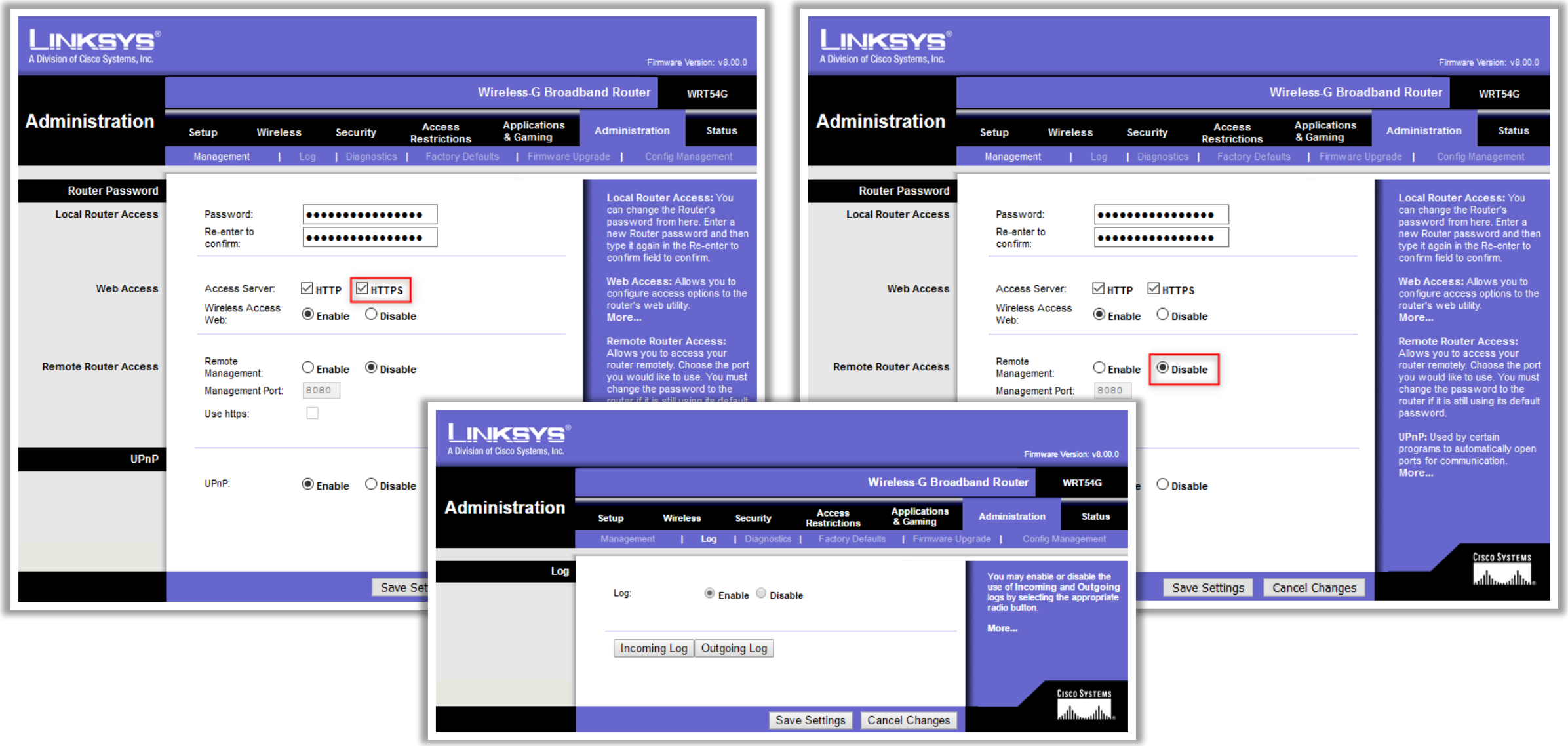
BoopSuite
https://github.com

Configuring the Administrative Security on Wireless Routers

- Change the **default password** on the wireless router
- Assign **a strong and complex password** to the router
- Choose the **HTTPS** for secure communication
- Disable remote router access
- Enable logging



Configuring the Administrative Security on Wireless Routers (Cont'd)





Module Summary

1

2

3

4

5

6