Mobile and Wireless Technology

CT090-3-2-MWT Version VD01

WLAN Terminology and Technology

Topic & Structure of The Lesson

Wireless LAN Modes of Operation - Ad-hoc & Infrastructure

Connecting to a Wireless Network – Passive Scanning & Active Scanning

Distribution System (DS)

Data Rates, Throughput, Dynamic Rate Switching

WLAN Roaming

Learning Outcomes

A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

At the end of this topic, You should be able to

- Understand the different operation modes for IEEE 802.11 wireless networks.
- Be familiar with the different service sets used with wireless networking.
- Identify the terminology used with IEEE 802.11 wireless networking. Know the process devices use to join a wireless LAN.
- Understand the differences between distribution systems as well as data transfer.
- Identify the differences as well as the function of a distribution system and wireless distribution system and roaming between each.
- Know the differences between data rate and throughput as well as dynamic rate switching

Key Terms You Must Be Able To Use

If you have mastered this topic, you should be able to use the following terms correctly in your assignments and exams:

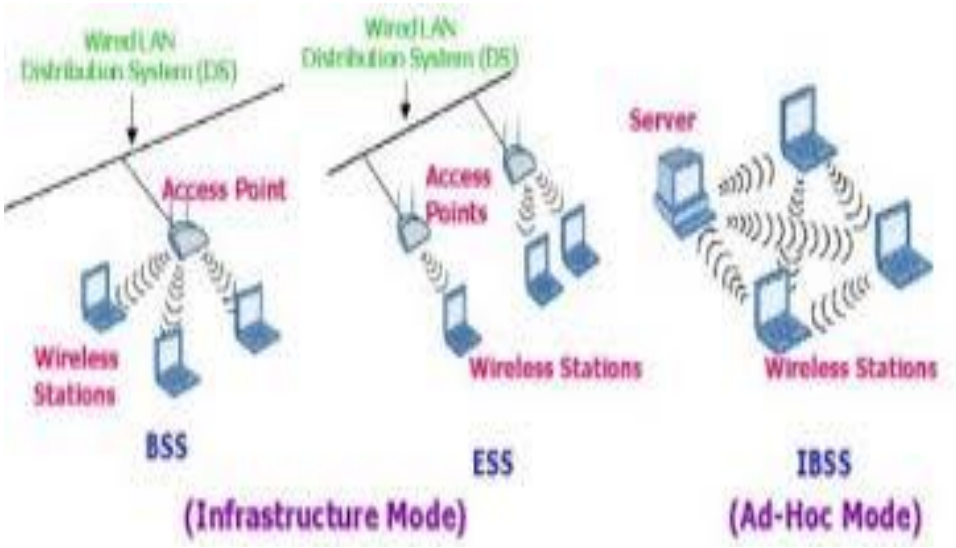
- BSS(Basic Service Set)
- ESS(Extended Service Set)
- IBSS(Independent Basic Service Set)
- SSID(Service Set Identifier)

Wireless LAN Modes of Operation

802.11 wireless LANs may be configured in one of two modes, either ad hoc or infrastructure mode.

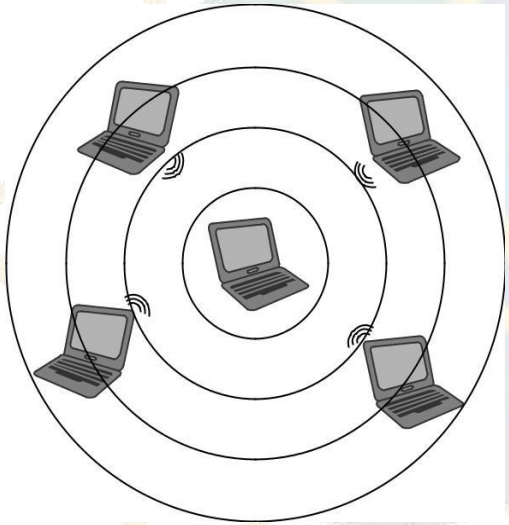
These **two modes** can be **broken down into three different** configurations:

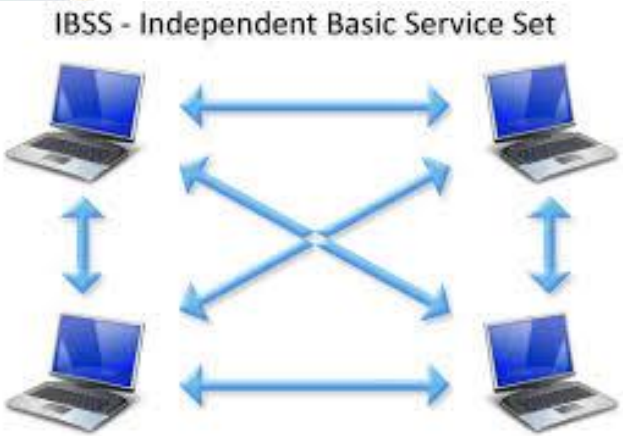
- **Independent basic service set (IBSS)**
- **Basic service set (BSS)**
- **Extended service set (ESS)**

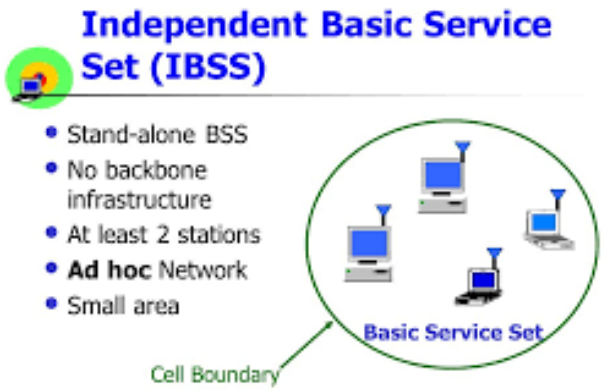


Wireless LAN Modes of Operation - IBSS

This operation mode **uses no access points** and consists of only wireless LAN devices or client computers. Communication occurs only among devices that are part of the same IBSS. Unlike an access point, this mode **has no centralized control** or managed security features.







Wireless LAN Modes of Operation - IBSS

Certain parameters must be set on the devices that **wish to participate in an IBSS.** These parameters must be the same on all the devices in order for them to effectively communicate with one another. Three common parameters set on devices that belong to the same IBSS are:

- **Service set identifier (SSID)**
- **Radio frequency channel**
- **Security configuration**

Wireless LAN Modes of Operation – IBSS

Service set identifier (SSID) - The **SSID is the name of the service set used to identify the wireless network** and for device segmentation. The SSID is used by devices to select a wireless network to join.

Every device that wishes to be part of the same wireless LAN IBSS, BSS, or ESS will use a common SSID. For infrastructure devices such as access points, the SSID parameter is manually set on the access point.

From the client access side, the SSID is a user-configurable parameter that can be set manually in the client software utility or received automatically from networks that broadcast this parameter.

Wireless LAN Modes of Operation - IBSS

Networks that are set to broadcast the SSID—also known as *open networks*—allow other devices to connect and use resources from the network based on the designated permissions or rights of the resource.

The **SSID is case sensitive and has a maximum limit of 32 characters** or, as specified in the IEEE 802.11 standard, 32 octets.

Wireless LAN Modes of Operation - IBSS

Radio frequency channel - The IBSS configuration requires a user to set the specific RF channel that will be used by all devices that are part of the same IBSS network.

This is accomplished in the client utility software for the network adapter. Some client software utilities set this automatically, in which case the IBSS will use the channel automatically specified.

It is important to understand that all devices in any common IBSS must be communicating on the same channel. If the client utility does allow a channel to be set, the channel chosen is up to the user but based upon the regulatory domain in which the network is used.

Wireless LAN Modes of Operation - IBSS

Security

With IBSS networks, there is no centralized control and no security management features.

Security is left up to the individual user or device. If a user inadvertently shares a resource it could expose sensitive information and pose security threats.

This can be a concern for many enterprise installations and therefore the use of an IBSS may be against corporate policy.

Wireless LAN Modes of Operation - BSS

The *basic service set* (BSS) is the foundation of the wireless network. This mode consists of an access point connected to a network infrastructure and associated devices.

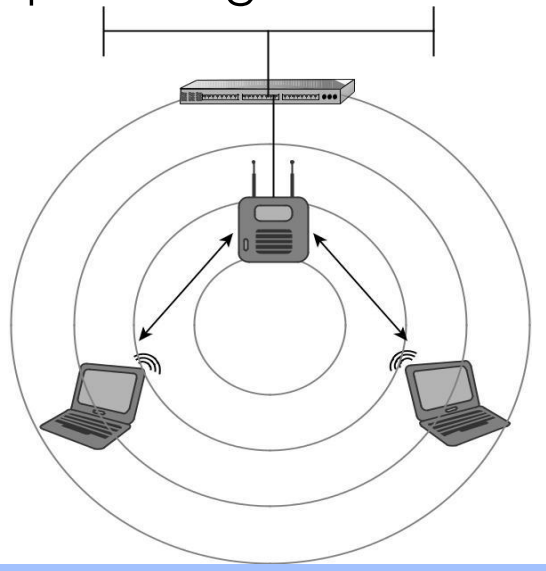
This is considered the foundation because it may be one of many access points that form a wireless network.

With a BSS setup, each access point is connected to a network infrastructure, also known as the distribution system (DS) and allows connected wireless LAN devices to access network resources based on the appropriate permissions the device or user has access to.

Wireless LAN Modes of Operation - BSS

The radio frequency area of coverage depends on several factors such as the antenna gain and output power settings; this area of coverage is known as the *basic service area(BSA)*.

Any wireless device in radio range and part of the BSA with the correct configuration parameters, including SSID and security settings, will be able to successfully connect to the access point. Figure 7.5 shows an example of a BSS.



Wireless LAN Modes of Operation - ESS

***Extended service set* (ESS) is defined as "a set of one or more interconnected basic service sets (BSSs)** that appears as a single BSS to the logical link control (LLC) layer at any station (STA) associated with one of those BSSs."

In basic terms, this can be one or more basic service sets connected to a common distribution system. An ESS is a common configuration in many wireless LAN deployments for small to medium businesses as well as large enterprise organizations.

In most cases, an ESS would be used to provide consistent and complete coverage across an entire organization.

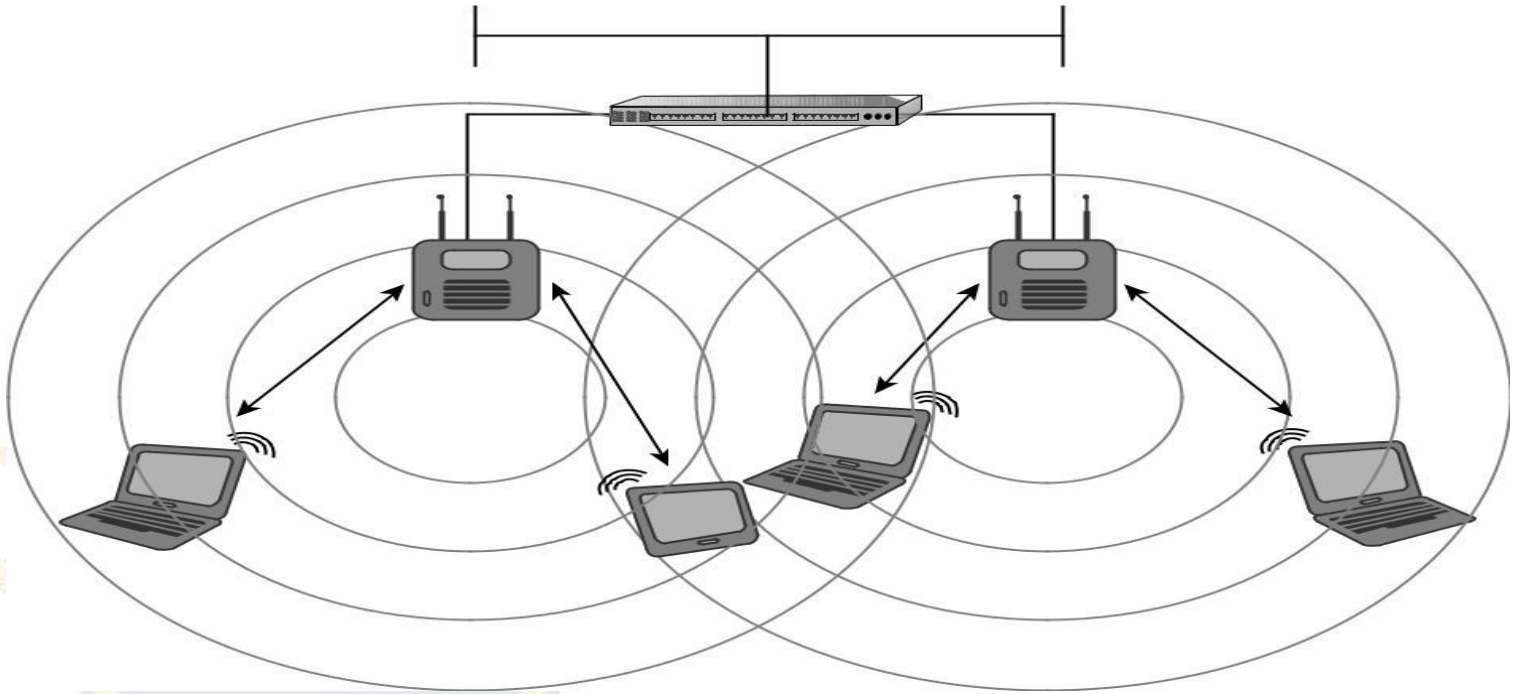
Wireless LAN Modes of Operation - ESS

An ESS can be thought of as several basic service sets (BSSs) that have matching parameters such as SSID and security settings.

It is the distribution system connecting these together that makes up the ESS. In most cases, the basic service area for each BSS will overlap to allow roaming from one BSS to another.

Wireless LAN Modes of Operation - ESS

ESS - Extended Service Set



Connecting to a Wireless Network – Passive Scanning

The first part of the discovery phase in IEEE 802.11 of wireless networking is known as *passive scanning*. This process allows wireless LAN devices to "listen" for information about wireless networks in the radio receiving area of the wireless network or the BSA.

During the passive scanning process, wireless LAN devices will listen for specific information to make them aware of networks in the area. An analogy to this process would be using an FM radio tuner to scan through the entire band listening for a station to tune in.

Connecting to a Wireless Network – Active Scanning

Active scanning is another part of the wireless LAN discovery phase. In active scanning, wireless LAN devices wishing to connect to a network send out a frame known as a probe request.

The function of this management frame is to find a specific wireless access point to connect with. Depending on the client software used, if an SSID is specified in the client utility software active profile, the device will join only a network with the matching SSID.

Access points constantly listen for probe request frames. Any access point within hearing range of the wireless device and having a matching SSID sends out a probe response frame to the wireless device.

Connecting to a Wireless Network – Authentication

Authentication in general is defined as verifying or confirming an identity.

- We use a variety of authentication mechanisms in our daily lives, such as logging onto a computer or network at home or at the office, accessing secure sites on the Internet, using an ATM machine, or showing an identification badge to get access to a building.

IEEE 802.11 devices must use an authentication process in order to access network resources. **This authentication process differs from conventional authentication methods such as providing a username and password to gain access to a network.**

Connecting to a Wireless Network – Authentication

The *authentication* discussed here is device authentication, required in order for the device to become part of the wireless network and participate in exchanging data frames.

The IEEE 802.11 standard addresses two types of authentication methods: open system and shared key.

Connecting to a Wireless Network – Association

Association takes place after a device has been successfully authenticated either by open system or by shared key authentication.

In the association state, the authenticated device can pass traffic across the access point to the network infrastructure or other associated wireless devices, allowing access to resources that the device or user has permissions to access.

After a device is authenticated and associated, it is considered to be part of the basic service set. A device *must* be authenticated before it can be associated.

Distribution System

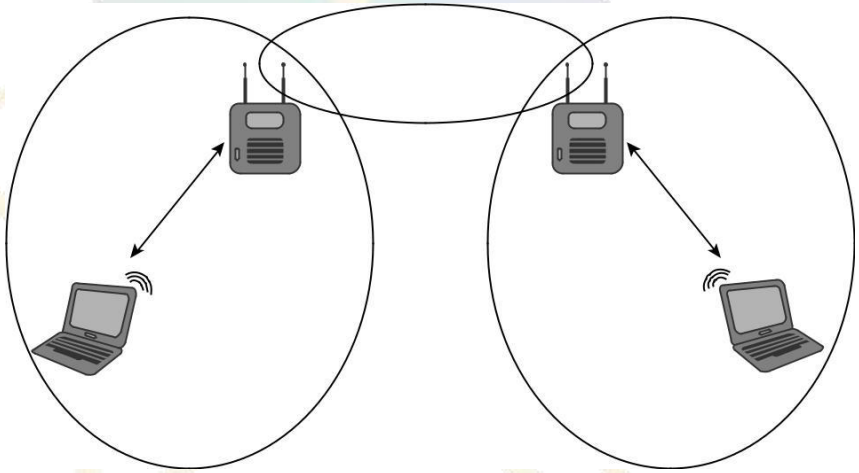
In wireless LAN technology, the *distribution system (DS)* is the common infrastructure to which access points are connected and can be wired or wireless. In most cases this would be Ethernet.

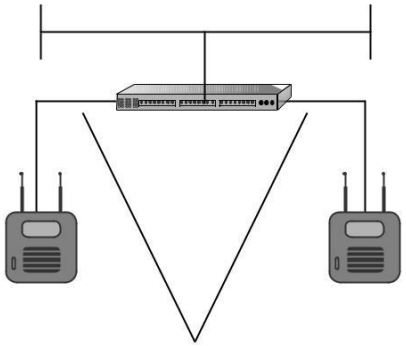
In this capacity, the access point acts like a Layer 2 translational bridge. A *translational bridge* is defined as a device used to connect two or more dissimilar types of LANs together, such as wireless (802.11) and Ethernet (802.3).

From a receiver's perspective, this allows an access point to take information from the air (the communication medium in wireless networking) and make a decision either to send it back out to the wireless radio or to forward it across to the distribution system.

Distribution System

An access point can do this because it has enough intelligence to determine if a data frame is destined to be sent to the distribution system or if it should stay on the wireless side of the network. This is possible because the access point knows whether a device is part of the wireless LAN side through the authentication and association methods mentioned earlier.





Distribution System

The distribution system is a network segment that consists of one or more connected basic service sets. As mentioned earlier, according to the original IEEE 802.11 standard, one or more interconnected basic service sets make up an extended service set.

The distribution system allows wireless LAN devices to communicate with resources on a wired network infrastructure or to communicate with each other through the wireless medium.

Either way, all wireless frame transmissions will traverse through an access point. In some cases it may be feasible and justified to use a *wireless distribution system*

Data Rates & Throughput

The **speed in which wireless devices are designed to exchange information** is known as the ***data rate***. Data rates do not accurately represent the amount of information that is actually being transferred between devices and a wireless network. This is done by throughput.

Throughput is the **amount of information** actually being transmitted or received.

Many variables affect the actual throughput of information being sent. Some of these include:

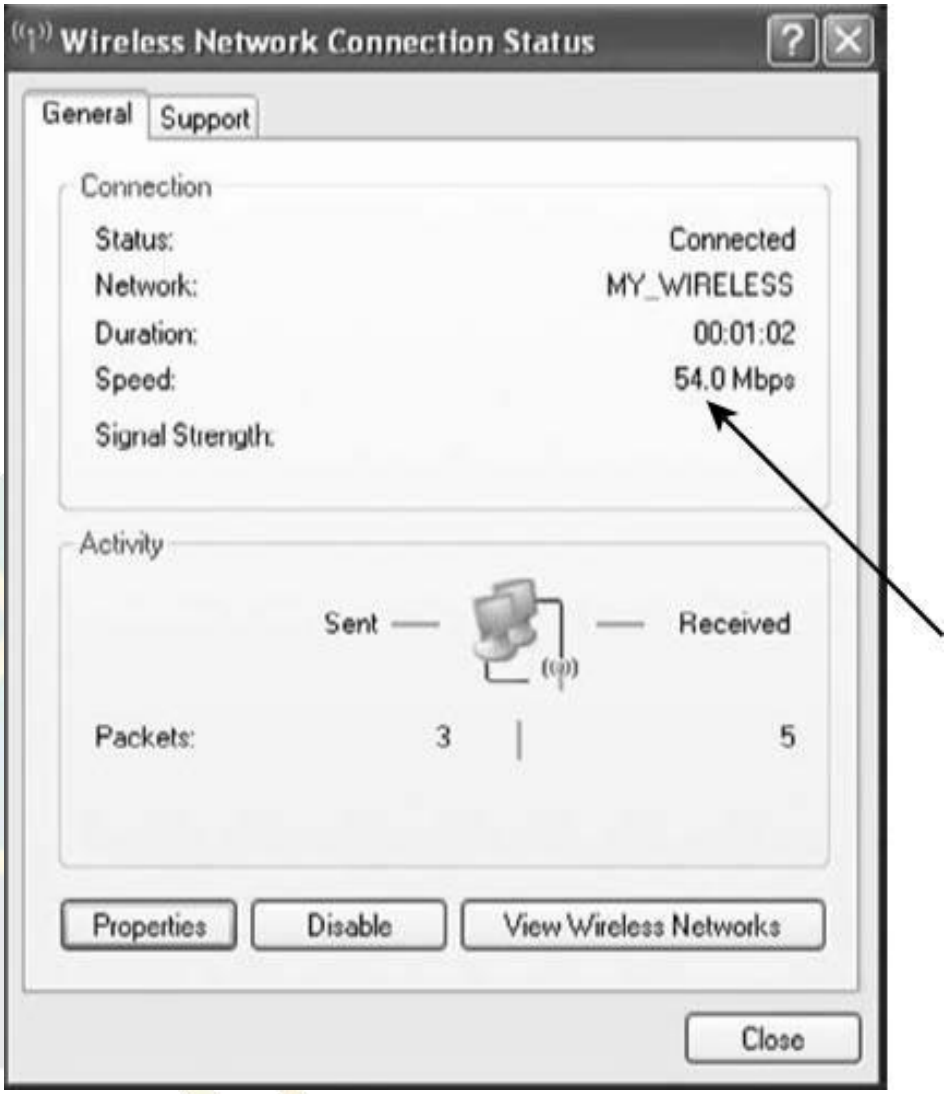
- Spread spectrum or technology type in use
- RF interference
- Number of users connected to an access point

Data Rates & Throughput

Table 7.1 Data Rates Based on Spread Spectrum Type

Standard/Amendment	Technology	Data Rates
802.11	FHSS 1	2 Mbps
802.11	DSSS	1 and 2 Mbps
802.11b	HR/DSSS	5.5 and 11 Mbps; 1 and 2 Mbps from DSSS
802.11a	OFDM	6, 9, 12, 18, 24, 36 and 48 Mbps
802.11g	ERP-OFDM	6, 9, 12, 18, 24, 36 and 48 Mbps
802.11n	HT-OFDM	Up to 300 Mbps

Data Rates & Throughput



Data Rates & Throughput

For example, an 802.11b wireless access point has a maximum data rate of 11 Mbps. With one user connected to this access point, chances are the best throughput that could be expected is about 50 percent of the maximum, or 5.5 Mbps.

If more users connect to the same access point, the throughput for each user would be even less, because of the contention between users sharing the same wireless medium.

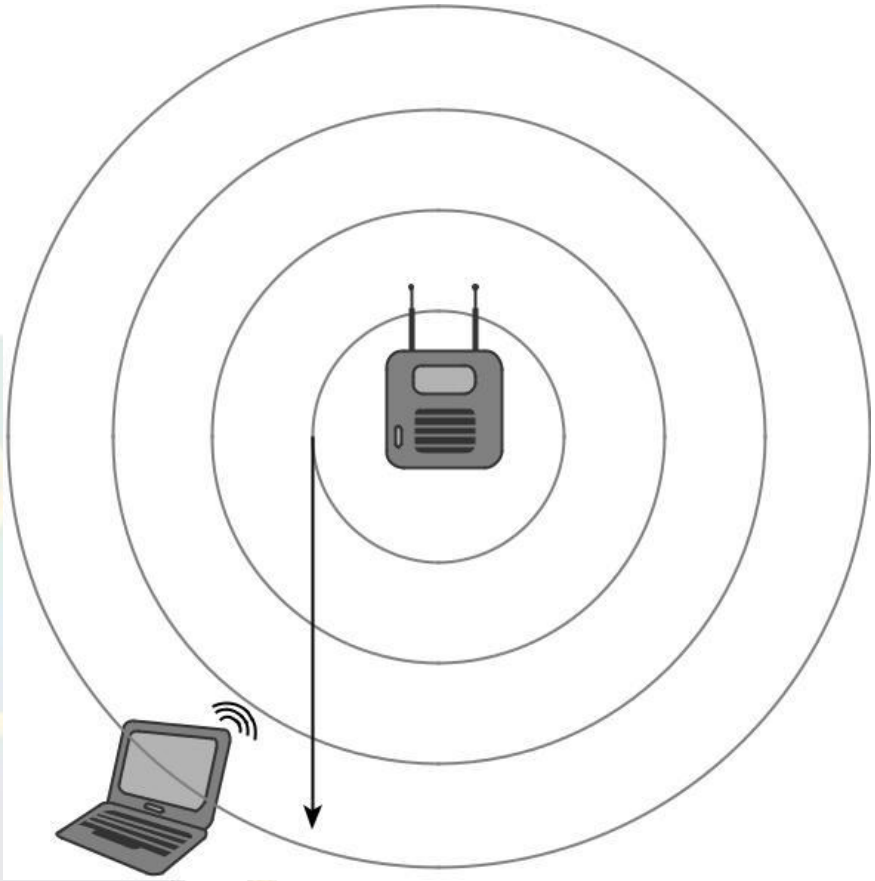
Dynamic Rate Switching

When a wireless device moves through the BSA or as the distance from the access point increases, the data rate will decrease.

This is called *dynamic rate switching (DRS)*, also known as dynamic rate selection. This process allows a device to adapt to the RF in a particular location of the BSA.

DRS is typically accomplished through proprietary mechanisms set by the manufacturer of the wireless devices. The main goal of dynamic rate switching is to improve performance for the wireless device connected to an access point.

Dynamic Rate Switching



Roaming

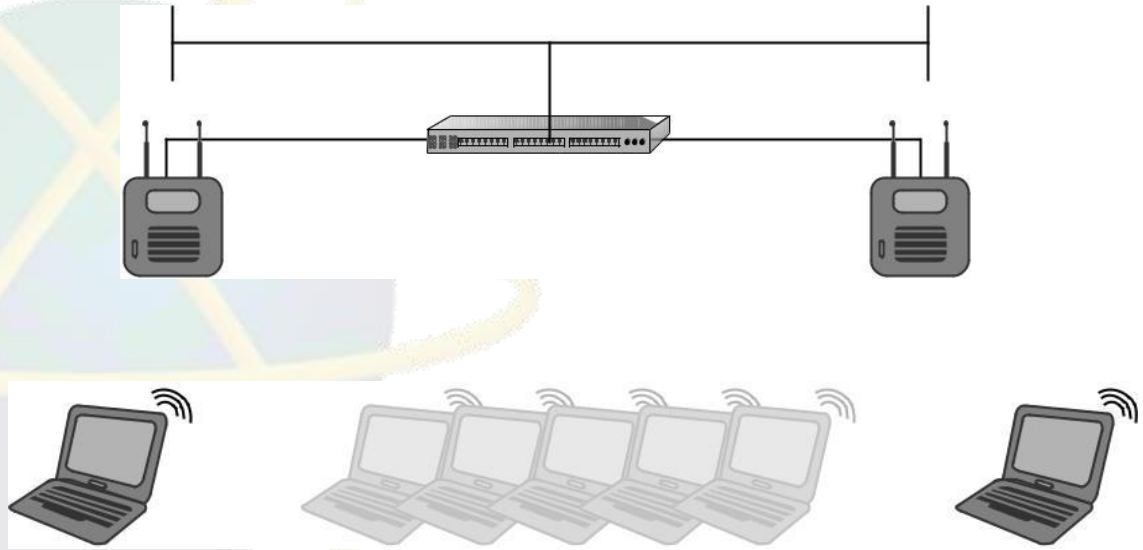
In wireless LAN technology,

Roaming is the term for what happens when a device moves from one basic service set to another. Roaming is not addressed in the original IEEE 802.11 standard.

This process is typically accomplished in a proprietary manner based on how the manufacturer chooses to implement it. Manufacturers use different criteria to initiate roaming from one access point to another.

Roaming

When a wireless LAN device moves through a BSA and receives a signal from a second access point, it needs to make a decision whether to stay associated to the current access point or to re associate to the new access point.



Roaming

This decision when to roam is proprietary and based on specific manufacturer criteria.

Some of these criteria are:

- **Signal strength**
- **Signal to noise ratio**
- **Error rate**
- **Number of currently associated devices**

Roaming

When a wireless LAN device chooses to re associate to the new access point, the **original access point will hand off the association to the new access point as requested from the new access point.** This is done over the wired network or distribution system based on how the manufacturer implemented the roaming criteria.

Quick Review Question

- What is Dynamic rate switching?
- What is active and passive scanning?
- Define IBSS,BSS and ESS.
- What is roaming?

Summary of Main Teaching Points

WLAN Mode of Operation

– Ad-Hoc and Infrastructure

- three configurations IBSS,BSS & ESS

Connecting to a wireless Network –

-Passive Scanning, Active Scanning, Authentication, Association,

Distribution System

Data Rate and Throughput

Dynamic Rate Switching

Roaming

Question and Answer Session

A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Q & A

What we will cover next

Wireless LAN Threats and Intrusion

- IEEE 802.11 Standards Security
- Open System Authentication
- Shared Key Authentication

Early WLAN Security Mechanisms

- Service Set Identifier (SSID)
- SSID Hiding
- Media Access Control (MAC) Address

Overview of other WLAN Security Standards and Technology