Chapter 5: Wireless Design Models, Topologies, and Infrastructure

Overview

Define, describe, and apply the following concepts associated with WLAN service sets

- Stations and BSSs
- Starting and Joining a BSS
- BSSID and SSID
- Ad Hoc Mode and IBSS
- Infrastructure Mode and ESS
- Distribution System (DS) and DS Media
- Layer 2 and Layer 3 Roaming

WLAN design modelsExplain and apply the following power management features of WLANs

- Active Mode, Power Save Mode, and WMM Power Save (U–APSD)
- TIM/DTIM/ATIM

Chapters 2 through 4 primarily focused on WLAN technology and standards from the bottom up. This chapter investigates WLANs from a top down perspective in that it covers the logical entities that exist within WLANs and the different design models that are commonly implemented.

Additionally, power management operations are covered because it is important to understand how a station can exist as part of a WLAN network when the transceiver is not actually powered on at all times.

Service Sets

The concept of a service set, to which previous chapters allude, has not been fully defined up to this point. The service set is the basic logical entity that exists in IEEE 802.11 WLANs. Service sets and stations are both defined and explained in this section.

Additionally, the distribution system is explored in order to understand how a WLAN is spread throughout a service area using both wired and wireless technologies. Finally, this section provides an overview of roaming within IEEE 802.11 WLANs.

Stations, BSSs, and BSAs

The IEEE 802.11 standard defines an entity known as a *station* and uses the term *STA* to refer to this entity. The STA is defined as any device that has an IEEE 802.11 compliant MAC and PHY interface to the WM. This means that the following devices, among others, would all be considered valid STAs, assuming they use IEEE 802.11 compliant radios and drivers:

- Access points (APs)
- Laptops, desktops, and servers with wireless NICs
- PDAs with IEEE 802.11b radios
- Residential gateways (mostly known as wireless routers)
- Wireless print servers
- Wireless presentation gateways
- Wireless bridges
- Wireless gaming adapters (mostly just wireless bridges)
- Wireless VoIP (Voice over IP) phones

This list is just a partial list. Many devices use IEEE 802.11 compliant radios and drivers and are capable of acting as an IEEE 802.11 STA.

However, it is also possible to use IEEE 802.11 devices in ways that are not defined within the IEEE standards and in ways that are not compatible with IEEE based WLANs. These implementations usually have alternate MAC or PHY layers that change the functionality of the IEEE 802.11 compliant device in such a way that it is no longer considered a valid IEEE 802.11 STA.

In other words, the device is capable of operating in an 802.11 compliant manner, but the drivers or software cause it to function in a noncompliant manner. This can be done because an IEEE 802.11 device uses a radio that has the capability of behaving in ways that are not in compliance with the standard.

Keep in mind that the standards are used to ensure interoperability between devices and that nonstandard devices should be avoided in common WLAN implementations.

It might seem odd to you to think of an AP as a station if you are used to wired networks where you use the term client station to mean an end user's computer; however, even in wired networks, any computer or device using the IEEE 802.3 Ethernet standard is technically a *node* on the network, where node is the generic term for any Ethernet device, and station is the generic term for any IEEE 802.11 device.

If the device can communicate on an IEEE 802.11 conformant WLAN, it has a set of STA services and is able to participate in a basic service set (BSS). This brings us to the phrase *basic service set.*

The BSS is defined as a set of stations that have successfully synchronized after one station has executed the START primitive. In the previous chapter, you learned about DCF.

The stations that are all cooperating together in the same DCF group form a BSS. There are more than one type of BSS. There is a BSS that is more dynamic (independent) and another that is more static (infrastructure).

You can also combine more than one BSS together to form a logical group through which a STA may pass without network interruption. The following sections describe the components of a BSS, the BSS types, and the process of starting and joining a BSS.

The BSA is the *basic service area.* This is the conceptual area within which BSS members may communicate. Another way of saying this is to say that the BSA is the physical space within which the STAs that are participating in the BSS may communicate with each other.

In some BSS implementations, the client STAs communicate directly with each other, and in other BSS implementations, the client STAs communicate with each other through the AP STA. In either case, the BSA is the physical space boundary within which these STAs may communicate with each other.

The BSA will vary or change slightly over time in most environments and can vary greatly in some environments. This is due to changes in the physical space such as atmospheric changes, physical item placement, the number of people present, and so forth.

This is why a particular signal strength can be seen at a location at one time and a very different signal strength can be seen at the exact same location at another time. Though the AP has not moved, environmental conditions change, and this results in a varying BSA.

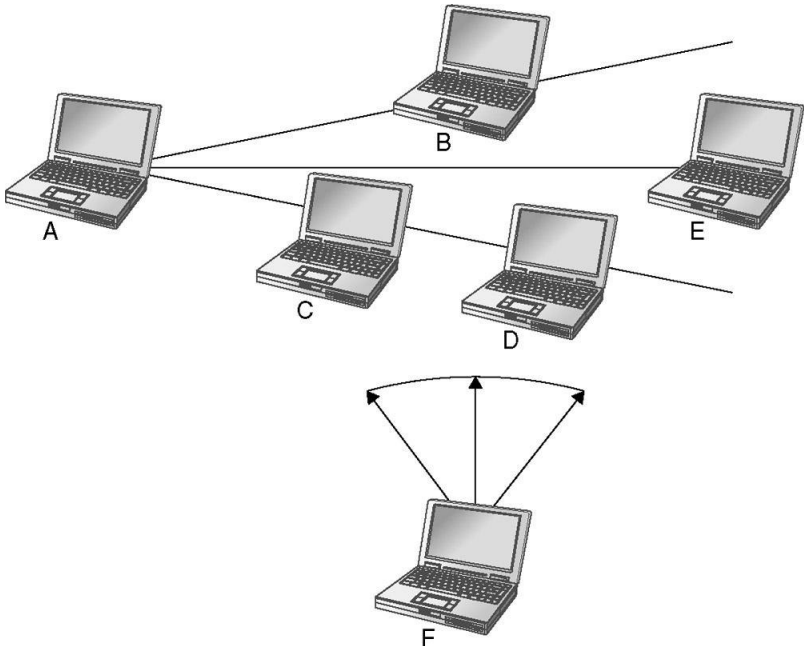
Ad Hoc Mode and IBSS

The dynamic topology offered by the IEEE 802.11 standard is the *independent BSS (IBSS)*. This is sometimes called an *ad hoc* wireless network or wireless gorkgroup. An IBSS is a collection of STAs that are communicating with each other directly without the use of an AP.

In order for a STA to be able to communicate with another STA, they must be within RF range of each other. There is no relaying of signals from one STA to another through the various STAs in the IBSS. For this reason, an IBSS is constrained to a fairly small BSA.

As an example, consider the example below. In this figure, the STAs on the right and the left can communicate with each other at an acceptable rate. All the STAs in between the extreme right and left STAs can also communicate with STAs A through E effectively.

However, signals from STA F, represented in the lower portion of example below, cannot reach the other STAs in the IBSS and the other STAs' signals cannot reach it. STA F is outside the BSA of the IBSS.



Infrastructure Mode and ESS

When a wireless AP station is used, an *infrastructure BSS* (simply called a BSS) is implemented. At the same time, an *extended service set (ESS)* is made possible.

An ESS, as defined in IEEE 802.11–1999 (R2003), is a collection of one or more BSSs sharing the same service set identifier (SSID) (defined in the next section). The following is the definition of an ESS pulled directly from the standard:

> 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 associated with one of those BSSs.

The definition in the standard reveals that a single BSS can indeed form an ESS. The phrase, "A set of one… BSSs," reveals such. This is also seen in the definition of the extended service area (ESA), which is the ESS equivalent of the BSA. The ESA is defined as being larger than or equal to a BSA.

The majority of WLAN literature indicates that you *create* an ESS when you group more than one BSS together using the same SSID. This is an incorrect understanding and it leads to a misunderstanding of what an ESS really is.

An ESS is more like a Windows Workgroup than a Windows Domain, for those familiar with Windows environments. In other words, there is no real "central" controller of the ESS or requirement for more than one BSS to have an ESS.

The ESS exists logically the moment the first AP comes online and forms a BSS just as a Windows Workgroup exists as soon as a computer comes online using the Workgroup name.

The first computer cannot prevent other computers from using the same Workgroup name or control their access to the Workgroup.

An ESS is the same in that the first AP that comes online starts the ESS and additional APs can join the ESS by using the same SSID (they may even become a virtual enlarged ESS even though they have different SSIDs), and this is not controlled by the initial AP.

Though some WLAN switches or controllers may be able to control entry to an ESS, this is not part of the IEEE 802.11 standard.

To get clarity on this subject, you can read the *IEEE 802.11F* recommendation for the management of STA handoff between APs in an ESS. This recommendation states that *the initialization of the first AP via the MLME–START.request(BSSType=Infrastructure) establishes the formation of an ESS.*

It goes on to say that *subsequent APs that are interconnected by a common DS* (distribution system) *and that are started with the same SSID extend the ESS* **created by the first** [emphasis added]. While the IEEE 802.11F recommendation is just that, a recommendation, and it has been withdrawn as of February 3, 2006, it states the reality of ESS creation more clearly than the IEEE 802.11 standard itself.

Another angle of approach would be to say that the SSID is actually the ID of the ESS and not the BSS. In fact, as stated earlier, the BSS has an ID, which is the BSSID. The ESS has an ID too, which is the SSID. This understanding clears up the confusion that results in common questions like:

- What is the difference between the SSID and the BSSID?
- Where is the ESSID set?
- How do you "create" an ESS?

The answer to the first question is that every service set has a machine–friendly name (the BSSID) and a people–friendly name (the SSID). The answer to the second question is nowhere.

There is no such thing as an ESSID and where it is referenced in the IEEE 802.11 Annex, it should read SSID. The answer to the third question is that you create an ESS when the first AP comes online and executes a START primitive as an infrastructure BSS.

The IEEE has not determined how to make multiple ESSs into one ESS but has suggested that this is something that needs to be addressed in the future.

Ultimately, you might consider that there are two perspectives to the creation of an ESS. The first is that the ESS is logically created when the first AP comes online, as it is now available

for other APs to join. By this, I mean that there is only one BSS and most people think of an ESS as "more than one BSS," but the ESS exists the moment the first AP comes online.

The second is that the ESS is created physically or in reality when the second AP is brought online and configured to use the same SSID or when it uses some other method of joining the ESS on the shared distribution system.

Effectively, an ESS exists when the first AP comes online and defines the SSID. As each new A P, which is connected to the same distribution system, comes online with the same SSID as the first, it joins the existing ESS.

This reveals that the ESS is really using the SSID to determine which APs should participate in the ESS. This is the default behavior that is most frequently implemented. The exceptions to this basic functionality would include when roaming specifications are implemented and configured to use RADIUS to control the APs that are allowed in the ESS or when some other proprietary protocol is used to constrain the APs that can participate in the ESS.

BSSID and SSID

The SSID, or service set identifier, is used to indicate the identity of an ESS or IBSS, depending on the implemented topology. The SSID can be from 2 to 32 characters in length and is normally sent in the beacon frames.

A STA seeking to join a WLAN may send probe request frames including the SSID of the desired WLAN. If an AP "hears" the probe request frame and it uses the same SSID, it will respond with a probe response frame.

The STA that transmitted the original probe request frame may now authenticate and, if successful, associate with the BSS. The *basic service set identifier (BSSID)* should not be confused with the SSID.

The BSSID is a 48–bit identifier that is used to uniquely identify each service set. The BSSID is usually the MAC address of the STA within the AP in an infrastructure BSS.

In an IBSS, the BSSID will be an ID generated according to the rules for locally administered addresses specified in Clause 5.2 of the IEEE 802–1990 standard. This means that the first bit (the individual/group bit) will be 0 to indicate an individual and the second bit (the universal/local bit) will be 1 to indicate that the address is a locally administered address.

The remaining 46 bits of the BSSID will be generated using an algorithm that minimizes the likelihood of other STAs generating the same BSSID.

Where the SSID identifies the service set, which may extend across multiple BSSs, the BSSID is unique to each BSS in an ESS or to each independent BSS. In order to help you better understand this, the following sections will provide details of the different types of service sets.

Distribution System (DS)

The *distribution system (DS)* is defined as a system used to interconnect a set of BSSs and an integrated LAN to form an ESS. Additionally, the DS is used for the transfer of communications between the APs in the ESS.

The communication that occurs between APs may be proprietary to the AP vendor, it may be according to a non IEEE specification, or it may be in accordance with the IEEE 802.11F recommendation even though this recommendation was withdrawn.

Every AP has a DS within it, regardless of whether it is connected to other APs across some other shared system such as Ethernet. The DS is composed of two parts: the Distribution System Medium and the Distribution System Services.

Distribution System Medium (DSM)

The *Distribution System Medium (DSM)* is the medium or set of media used for communications among APs in the ESS. The most popular medium in use today is certainly Ethernet, but the IEEE standard allows for the use of other media such as Token Ring or even another form of wireless.

Distribution System Services (DSS)

The *Distribution System Services (DSS)* are composed of the services that provide the delivery of frame payloads between stations that are in communication with each other over a shared instance of WM and in the same infrastructure BSS. In other words, the DSS provide communications between stations in the same BSS. At this point, the IEEE 802.11 standard does not specify the full delivery path from a STA in a BSS to a station in another BSS or from a STA in a BSS to a network node outside the BSS. Usually, each AP drops the frames out the connected portal (usually Ethernet) and hopes the Ethernet infrastructure (routers, switches, etc.) knows how to reach the destination.

Starting and Joining a BSS

The process of starting a BSS differs depending on whether it is an IBSS or an ESS (infrastructure BSS). In the case of an IBSS, the first station coming online starts the IBSS. In the case of an ESS, the AP starts the BSS when it comes online. The following sections provide more details on the start–up of an IBSS or an ESS. Joining a BSS was covered in Chapter 4 in the topics "Active Scanning" and "Passive Scanning."

Starting an IBSS

An IBSS is started when the first station comes online. Specifically, the station processes an MLME–START.request primitive with the parameter BSSType set to independent. This station sets the SSID to use in the IBSS, and all other stations that wish to join the same IBSS must use the same SSID. Additionally, this first station will set the BSSID according to the guidelines specified in the IEEE 802.11 standard. A station may scan before attempting to start the IBSS, or the station may start the IBSS without performing a scan first.

Starting an ESS

An infrastructure BSS (ESS) is started when the AP is started. The AP will process an MLME START.request primitive with the parameter BSSType set to infrastructure. The AP sets the SSID to use in the ESS. The BSSID will likely be the MAC address of the AP. At this starting point, the AP will specify the parameters to be used within the ESS. These parameters are presented below. Other parameters are also configured.

BSS Parameter	Description
SSID	The SSID to use for the ESS.
PHY parameter set	The parameter set used by the PHY that is being implemented. For example, OFDM, DSSS, etc.
Beacon period	The Beacon Period to be used in the ESS.
Data rates	Information such as supported data rates.

Layer 2 and Layer 3 Roaming

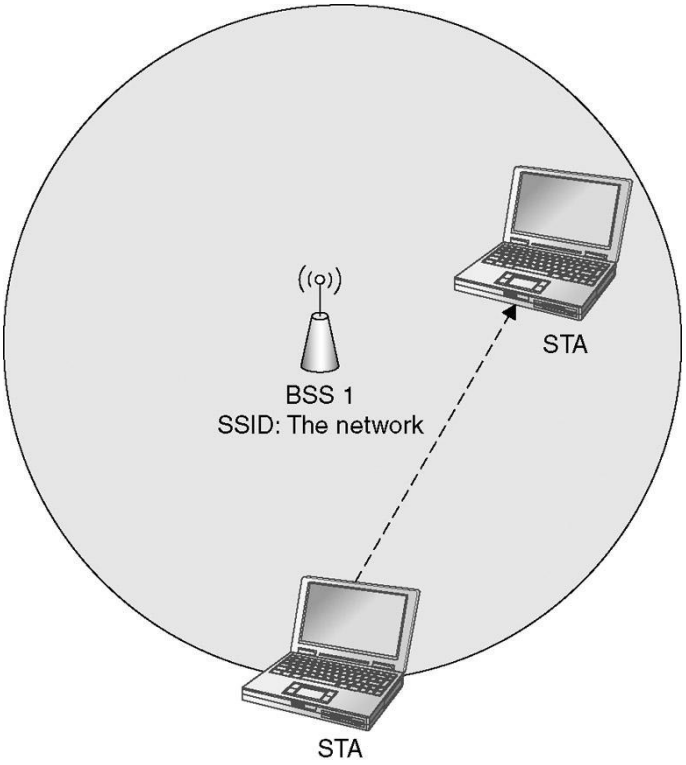
When a station associates with an AP in a BSS, it is joining a potentially larger network (the ESS). If the station moves out of the range of the initial AP, it may disassociate and reassociate with another AP that is participating in the same ESS.

This process of reassociation is known as *roaming.* Roaming provides mobility, but there are different types of mobility. This section will present the different types of mobility and then covers the basics of roaming.

Mobility Types
There are three basic types of mobility that can occur in an IEEE 802.11 WLAN.

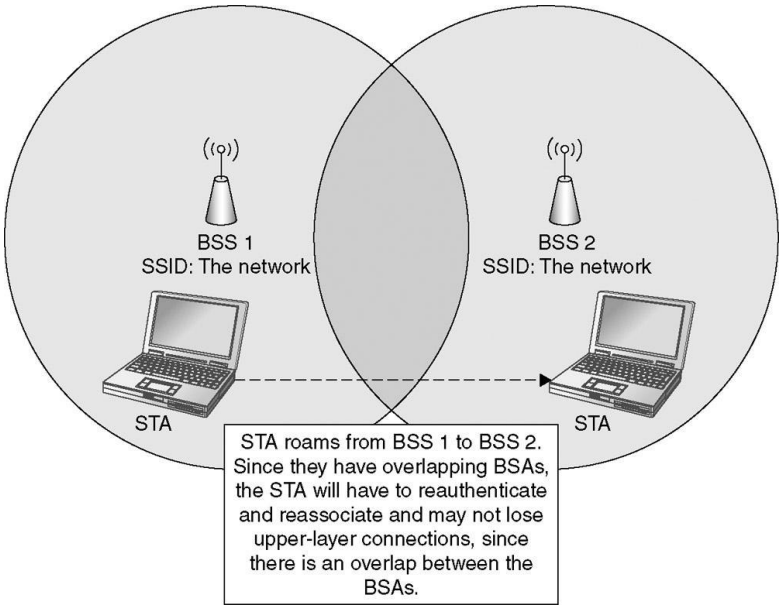
- **No–Transition** Static or local movement.
- **BSS–Transition** Moving around to different BSSs within an ESS.
- **ESS–Transition** Moving from a BSS in one ESS to a BSS in another. The IEEE states that upper–layer connections are not guaranteed and are likely to be lost.

The first, notransition, indicates that the station will not transition from one BSS to another while attempting to maintain upper–layer connections. In other words, it stays in range of its BSS. Picture below illustrates nonoverlapping BSSs and a no transition type of mobility.



STA moves around within range of its BSS. No roaming occurs and the connection is not lost. This is no-transition mobility.

The second type is what is most commonly referenced as roaming. The BSS transition mobility model is one that does allow for the maintenance of upper layer connections while moving from one BSS to another within the same ESS. Also called seamless roaming, this is represented:



The third type occurs when a station moves from a BSS in one ESS to a BSS in a different ESS. Since an ESS can be thought of as a "virtual" LAN even though it may spread across massive areas, it is logical that you can maintain upper layer connections while roaming within an ESS (BSS transition).

However, separate ESSs can be thought of as separate "virtual" LANs and it is also logical that you will lose upper layer connections while roaming from one ESS to another (ESS transition).

There are technologies which allow for roaming between ESSs while still maintaining upper–Layer connections. IEEE 802.11 does not specify such a technology, but proprietary solutions do exist

WLAN Design Models

With an understanding of the basic logical entities that exist in a WLAN and the roles played by various station types, you can begin to explore the different WLAN design models. Many WLAN design models exist; the one you choose to implement will depend on the needs discovered during a site survey and customer interviews. This section provides an overview of these WLAN design models.

Site–to–Site Connections

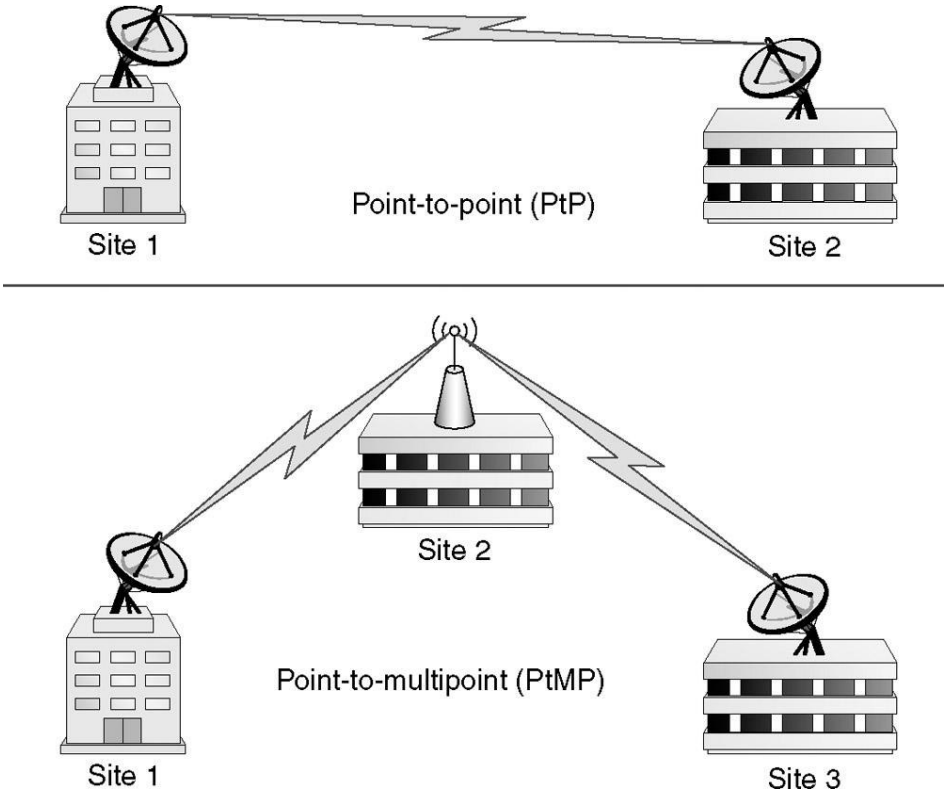
When using WLAN technology to form site to site links, you will either create *point to point (PtP)* or *point to multipoint (PtMP)* links. This section describes both.

Point–to–Point (PtP)

A PtP WLAN connection is a dedicated connection between two wireless devices. These two devices are usually bridges that allow for the bridging of two otherwise disconnected LANs.

These wireless connections allow for the creation of large scale campus networks and may even be used to create metropolitan networks that span cities.

They provide the benefit of connecting disconnected LANs over some distance without the need for leased lines or running cable when the connection is created within a large campus or otherwise owned area. Picture below shows a PtP connection and a PtMP connection.



These PtP connections will use semidirectional or highly directional antennas to form the connection. These antennas, unlike the more common indoor omnidirectional antennas that are seldom aimed at anything but rely on reflections to get the job done, do focus the signal mostly in a desired direction so that more amplitude is available in that desired direction.

Point–to–Multipoint (PtMP)
A PtMP wireless link is created when more than one link is made into a central link location like that represented in above in the lower half of the image. An omni or semidirectional antenna is usually used at the central location, and semidirectional or highly directional antennas are used at the other locations.

When only one connection is needed, you will usually choose the PtP model, and when there is a need for multiple locations to link back to a central location, you will usually choose the PtMP model.

However, there are times when multiple PtP links may be justified instead of using the PtMP model. Specifically, this may be needed when you cannot accept the throughput constraints imposed by having a single antenna positioned centrally that is accessed by all remote locations.

WLAN Models

In the common WLAN PtMP model, there are two primary implementation methodologies: the *single MAC model* and *the split MAC model*. The single MAC model is also known as an *edge* or *intelligent edge* model, and the split MAC model is also known as a *centralized* model.

Single MAC Model (Edge, Autonomous, or Stand−Alone)

When a single MAC model is used, it means that the APs contain all of the logic within them to perform MAC layer operations.

In other words, all IEEE 802.11 services reside within the AP, with the possible exception of security services when IEEE 802.11i is implemented.

The single MAC model is the oldest and is still very popular in small and medium sized WLANs. There are both costs and benefits of the single MAC model.

Single MAC model costs:

- Decentralized administration may require more ongoing support effort.
- APs may be more expensive, since they have more powerful hardware.
- Each AP may be able to handle fewer client stations.

Single MAC model benefits:

- No single point of failure. If one AP goes down, the others continue to function.
- Less wired network traffic is required to manage the wireless stations.
- More features are available within the APs themselves.

Split MAC Model (Centralized)

The split MAC model is called such because portions of the MAC layer operations are offset to centralized controllers and other portions remain in the AP.

These types of APs are often called thin APs because they do not perform as many functions as the traditional APs (fat APs).

The split MAC model is very popular in large networks today and is becoming more popular in smaller networks as well. There are costs and benefits associated with the split MAC model, too. Split MAC model costs:

- A possible single point of failure occurs at the WLAN controller.
- Increased wired network traffic is required to manage the wireless stations.
- There are fewer features within the APs themselves when using truly thin APs.

Split MAC model benefits:

- Centralized administration may reduce ongoing support efforts.
- APs may (or may not) be less expensive, since they can have less memory and processing power.
- Each AP may be able to handle more client stations, since the AP doesn't have to handle management processing overhead.

You may have noticed that, in a large way, the benefits of the split MAC model are the costs of the single MAC model and the benefits of the single MAC model are the costs of the split MAC model.

While there are certainly more details involved than this, it is important to understand that you will be giving up something regardless of the model you choose. The key is to determine what is best for the organizational and technical needs of the organization in which you are

implementing the WLAN. You will learn more about this in Chapter 6 when you learn about site surveys and WLAN network planning.

Wireless Mesh Networks

Another wireless networking model that is now more than a theory is the wireless mesh networking model. Earlier you learned about the PtP and PtMP models. In the database world, you have a one to one relationship model, and this is like the PtP model in WLANs.

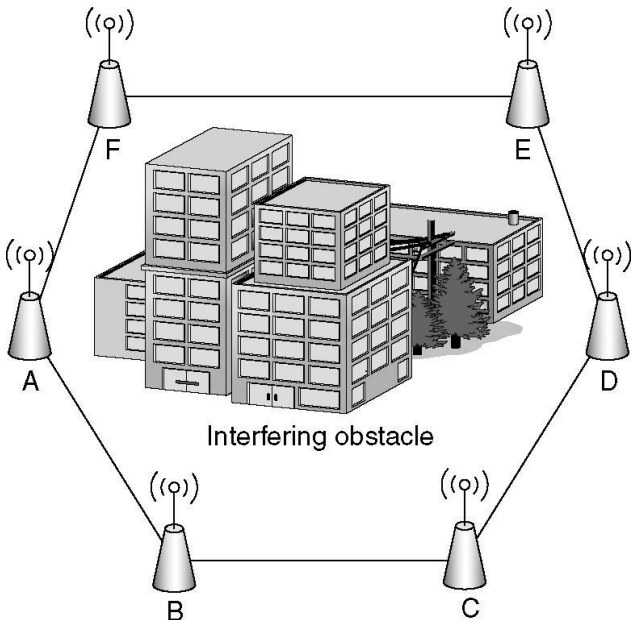
You also have a one to many relationship model, and this is like the PtMP model in WLANs. However, database theory also presents a many to many relationship model, and this is much like the mesh networking model in WLANs.

Therefore, you could say that mesh networking is like a multipoint to multipoint (MPtMP) model. In a mesh network, all APs can connect to all other stations that are turned on and within the range of each other.

Additionally, data travels through each node so that each node is both a router/repeater and an end node at the same time. The benefits of a mesh networking model include:

- Communications within areas that would normally have many LOS obstructions
- Data routing redundancy

The first benefit is seen because mesh nodes are placed close enough to each other that a path will always be available around obstructions that would normally prevent wireless links. Illustrated below. Notice that data can travel from node A to node B and then to node C and finally to node D. If this were not a mesh network, there would be no clear path from node A to node D.



The second benefit is also seen in Figure 5.5. If the route mentioned previously (A to B to C to D) was to become unavailable, there is data routing redundancy in that the route from A to F to E to D could be utilized.

The IEEE 802.11s amendment is currently in development and will specify a standard for wireless mesh networking. Earlier in this chapter, you learned that the normal DS for a WLAN is an Ethernet LAN.

However, the IEEE standard leaves the specification open so that a wireless distribution system (WDS) could also be used.

The IEEE 802.11s amendment is aimed at detailing just such a WDS. This means that our future could see networks that are entirely wireless without a single Ethernet cable (or other wired standard) anywhere.

Right now, it seems that the more wireless we implement, the more wires we install; but this could change with evolving modulation schemes, frequency distribution, and powerful processors at lower prices.

This will be aided by both the IEEE802.11n amendment for a MIMO PHY and the 802.11s amendment for a mesh based WDS, but there is still plenty of work to do and plenty of uses for those wires.

While we are years and more likely decades from an entirely wireless infrastructure, the potential is exciting.

Evolution of WLAN Models

To put the pieces together, this section will present the WLAN models that have evolved over time. We will start with the first model that was implemented using IEEE 802.11 technology and then progress through the evolutionary stages of WLAN design models.

While the models did not necessarily evolve in a precisely sequential order as presented here, the adoption of the differing models does seem to have followed a path much like this.

Intelligent Edge (Distributed)

The first devices to be released to the market were the standard fat APs that are still used heavily today.

This kind of AP contains the entire logic system needed to implement, manage, and secure (according to the original IEEE 802.11 specification) a WLAN. The benefit of this type of WLAN is that implementation is very quick when you are implementing only one AP.

The drawback to this type of WLAN is that implementation is very slow when you are implementing dozens or hundreds of APs. There are many networks around the world that have more than 1000 APs.

You can imagine the time involved if you have to set up each AP individually. At stage one, intelligent edge, this was your only choice. The APs implemented in this model are also known as autonomous APs.

WLAN Network Management Systems (Centralized Management/Distributed Processing)

When we arrive at stage two in the evolution of WLAN management, we encounter centralized configuration management with distributed intelligence. The devices and software that provide this functionality are known as a WLAN Network Management System (WNMS).

This stage provided much faster implementations of traditional fat APs and worked using SNMP or other proprietary communication protocols to configure the APs across the network.

The WNMSs usually supported the rollout of firmware so that the APs could be updated without having to visit each one individually. This model provided scalability, but did not

reduce the cost of the APs and did not offset any processing from the APs so that they could handle more stations at each AP. In this model, autonomous APs are still used.

Centralized WLAN Architecture (Split MAC)

That brings us to stage three: Centralized WLAN Architecture. This networking model utilizes lightweight or thin APs and depends on a wired network connection to the WLAN switches.

The WLAN switch contains all the logic for processing and managing the WLAN. This allows the APs to handle more client stations and provides for simple implementation. For example, most of these systems allow you to simply connect the lightweight AP (sometimes called an access port to differentiate them from an access point) to the switch that is connected to the WLAN controller, and the AP and controller will automatically synchronize without any intervention from the engineer.

Of course, there is still the requirement of initial setup and configuration of the controller, but moving forward, it can be automatic. The things that are automatically configured may include the channel used by the AP, the encryption methods used, the SSID, and more.

Distributed Data Forwarding (DDF) WLAN Architecture

The DDF WLAN architecture uses a WLAN controller like the centralized architecture and represents stage four. The difference is that DDF APs are used instead of lightweight APs. A DDF AP is an AP that can perform some or all of the functions needed within a BSS and can also allow for some or all of these functions to be managed by the central controller.

Unified WLAN Architecture

The stage is now set for another evolutionary move where the wireless controlling functions are simply integrated into the standard wired switches used within our network cores. This would mean that the switches that provide wired network functionality to wired clients will also have the capability to serve the needs of wireless APs so that specialty wireless switches/controllers are no longer needed as separate devices.

Today's centralized and hybrid solutions usually depend on a connection from the wireless controller to a wired switch that actually has connections to the APs. The future may see more development of multiport switches that have wireless controller functionality built in, reducing the need for an extra wired switch.

WLAN Power Management Features

The stations that participate in a WLAN and provide mobility to the end users will likely be battery powered. For this reason, the IEEE has defined a set of power save operations that are implemented in 802.11 WLAN devices in order to provide for longer battery life. These operations are explained in this section.

WiFi devices are very power consuming!

Active Mode

When a station is in *active mode*, it does not utilize any power management features. Instead, the radio is left on at all times and frames that are destined for the station do not have to be cached at the AP.

This mode is usually used by desktop computers that are using wireless connections and may be used by laptop computers as well. It is not uncommon for a laptop user to disable power save features when connected to power so that network communications are more efficient.

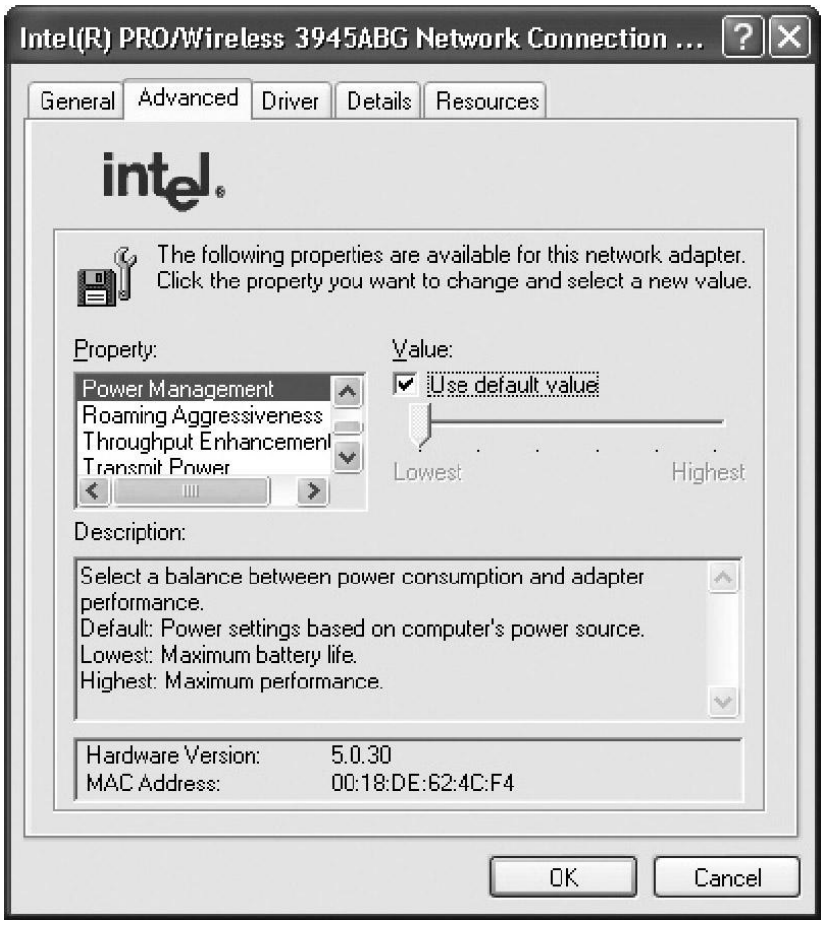
By disabling power save mode on static devices that are always plugged into power outlets, you may also improve the performance of your WLAN overall. This is because the APs will no longer have to cache frames for any stations in the WLAN that have the power save features disabled.

Below shows the device driver interface where power management settings can be configured on a Windows XP client station.

Power Save Mode

When a station is configured to use *power save mode*, it alternates between two states: dozing and awake. In the dozing state, much of the wireless NIC is disabled or powered down in order to save battery life.

The dozing state lasts a specific interval, and then the station switches to awake so that it can check for cached frames at the AP that are intended for it. The actual activity that takes place when a station is configured in power save mode is covered in the section "TIM/DTIM/ATIM" later in this chapter.



WMM Power Save (U–APSD)

The WMM certification includes a power management function known as *unscheduled automatic power–save delivery (U–APSD).* Devices supporting U–APSD will support both legacy power management (as described in the section "TIM/DTIM/ATIM") and triggered U–APSD. In order to implement U–APSD, QAPs (QoS APs) must be used.

These are APs supporting IEEE 802.11e. The intention of the WMM Power Save procedures is to provide longer battery life in QoS–demanding devices such as VoIP phones. Both unscheduled and scheduled APSD are documented in the IEEE802.11e–2005 amendment.

TIM/DTIM/ATIM

When an IEEE 802.11 station uses power management, it uses information known as the Traffic Indication Map, the Delivery Traffic Indication Message or the Ad Hoc Traffic iindication Message window. The following sections describe these concepts.

Traffic Indication Map (TIM)

Every station that is associated with an AP has an association identifier (AID). In infrastructure BSSs, this AID is used in the power management process. Within the beacon frame transmitted by the AP is a *Traffic Indication Map (TIM)* that is really nothing more than the list of AIDs that currently have frames buffered at the AP.

This TIM is used by all stations that are participating in power management and have their power save mode enabled. You'll remember (from the last chapter) that beacon frames are transmitted at regular intervals, and this means that a station can predict when the next and future beacon frames will be transmitted.

The station can go into dozing mode and then wake at a time just before a beacon frame is transmitted so that it can inspect the frame to see if any cached frames are waiting at the AP that are destined for its AID.

The station is not required to wake at every beacon frame interval and, in fact, can balance performance versus power saving by waking at longer intervals (say, every third beacon instead of every second beacon). Usally slider that can be used to balance power management versus performance.

Delivery Traffic Indication Message (DTIM)

Some frames are intended to go to multiple specific stations (multicast) or all stations (broadcast). IEEE 802.11 specified the *DTIM* for managing these frame types. All stations must be awake when the DTIM is transmitted.

The AP indicates the DTIM interval to the stations so that they can be awake for every DTIM. The DTIM includes the same information that the TIM contains and additionally contains information about broadcast or multicast frames.

While every beacon contains a TIM, only every *n*th beacon contains a DTIM. This may be every third or some other interval. If the DTIM interval were every third beacon, then all stations would be required to wake for every third beacon.

Ad Hoc Traffic Indication Message (ATIM)

As you'll remember, ad hoc WLANs or IBSS WLANs do not have APs. Since this is the case, something other than the TIM and DTIM must be used to facilitate power management. The ATIM is used in the IBSS WLAN.

The *ATIM* is a window of time (known also as the ATIM window) when all stations are required to be awake. Any station in the IBSS having frames buffered for any other station sends a unicast ATIM frame to the station for which the frames are destined. The recipient of the

ATIM frame will acknowledge the frame and remain awake so that it can receive the buffered

frames. Stations not receiving an ATIM frame within the ATIM window will go back to dozing after the ATIM window expires. When considering power management within a WLAN, it is important to strike a balance between performance and endurance.

While you may be able to greatly extend battery life by configuring your WLAN stations to wait for longer periods before waking, this will also degrade the performance of the WLAN.

Equally, when you have the stations wake more frequently, you lessen the length of time in which the stations can operate on battery power. The balance is usually found by considering the use of the stations and then setting the power management capabilities accordingly.

For example, if you are using a laptop for VoIP communications, you may want to lean more toward performance and further away from battery conservation. On the other hand, if you are using a laptop strictly for e–mail and web browsing, you will likely lean in the opposite direction.

Summary

This chapter provided you with an overview of the WLAN topologies and architectures that are available to today's WLAN engineer. Additionally, you learned about the power management and roaming capabilities of wireless stations in IEEE 802.11 WLAN. You learned that a BSS is the fundamental building block of a WLAN and that there are two types of BSSs: infrastructure and independent. You also learned that multiple BSSs can be joined together to form an ESS in order to provide coverage to larger or more areas.

Review Questions

1. There are two types of basic service sets specified in the IEEE 802.11 standard. What are these two types?

A. Independent basic service set
B. Extended service set
C. Infrastructure basic service set
D. Integrated basic service set

2. A station roams from BSS A to BSS C. These BSSs are managed by APs from different vendors. Both APs support the IAPP, and the BSSs do overlap their BSAs. Finally, they both share the same SSID and function on the same LAN. Should the client station lose its IP address after roaming from BSS A to BSS B and why?

A. Yes, because the APs do not support IEEE 802.11F
B. Yes, because the DHCP server is on BSS A
C. No, because all conditions are met for seamless roaming
D. No, because any ESS provides seamless roaming regardless of these various specified details

3. You want to implement 34 thin APs with as little time invested as possible. You have also determined that you must support seamless roaming for all wireless stations. Which model are you likely to implement? (Choose one.)

A. Split MAC
B. Single MAC
C. Active mode
D. Power save mode

4. 4. You are operating a station in power save mode. The station is participating in an IBSS. What is the window called within which the station must be awake?

A. DTIM
B. TIM
C. MSDU
D. ATIM

5. What is the ID of an ESS?

A. BSSID
B. SSID
C. ESSID
D. It doesn't exist

6. You are implementing a WLAN based on the intelligent edge architecture. What kind of APs are you installing?

A. Thin APs
B. Hybrid APs
C. Lightweight APs
D. Autonomous APs

7. What kind of APs are used with a centralized architecture?

A. Autonomous
B. Cisco
C. Lightweight
D. None

8. Which part of the beacon frame sent from the AP is the list of STAs that have data buffered at the AP when they awake?

A. Traffic Indication Map
B. Header Frame
C. Footer Frame
D. Contention Window

Answers

1. A, C. The correct answers are infrastructure basic service set and independent basic service set. An extended service set is a collection of one or more basic service sets sharing the same SSID. There is no such thing as an integrated basic service set in the IEEE 802.11 standards.

2. C. The correct answer is no. The station should not lose its IP address since IEEE 802.11F, or IAPP, is in use and a true ESS with overlapping BSAs among the BSSs does exist.

3. A The correct answer is the split MAC model. The split MAC model will allow you to implement a large number of APs with less effort than the single MAC model in most scenarios. The roaming is a factor that is not addressed by any of the models presented and therefore does not factor into the decision

4. D. The correct answer is ATIM. The Ad Hoc Traffic Indication Message window must be acknowledged by all stations participating in the IBSS, in that they must all be awake during this window of time.

5. D. The correct answer is it doesn't exist. Many books reference an ESSID, but this is improper terminology, as no such entity exists in the IEEE 802.11 standards.

6. D. The correct answer is autonomous APs. The autonomous or fat AP is the AP with all the intelligence needed to manage the BSS, with the possible exception of security capabilities when implementing IEEE 802.11i.

7. C. Lightweight APs are used with a centralized architecture.

8. A The Traffice Indication Map (TIM) includes a list of all the STAs with frames waiting in the AP's buffer.