Chapter 7
Basic Wireless Concepts and Configuration
Part I

3rd December 2013

Basic Wireless Concepts and Configuration

The Wireless LAN
Why Use Wireless?

- Business networks today are evolving to support people who are on the move.
  - Productivity is **no longer restricted** to a fixed work location or a defined time period.
  - People now expect to be **connected at any time and place**, from the office to the airport or even the home.
  - Now employees can check e-mail, voice mail, and the status of products on personal digital assistants (PDAs) while at many temporary locations.
  - At home, the **method of accessing the Internet** has quickly moved from temporary modem dialup service to dedicated DSL or cable service.
- In addition to the flexibility that WLANs offer, another benefit is reduced **costs**.
  - For example, with a wireless infrastructure already in place, savings are realized when moving a person within a building, reorganizing a lab, or moving to temporary locations or project sites.
  - Another example is when a company moves into a new building that does not have any wired infrastructure. In this case, the savings resulting from using WLANs can be even more noticeable, because the cost of running cables through walls, ceilings, and floors is largely avoided.

### Wireless LANs

- Most current business networks rely on switch-based LANs for day-to-day operation inside the office.
- Workers are becoming more mobile and want to **maintain access to their business LAN resources** from locations other than their desks.
- You can see that the WLAN is an extension of the Ethernet LAN.
Comparing a WLAN to a LAN

- WLANs use radio frequencies (RF) instead of cables at the physical layer and MAC sub-layer of the data link layer.
  - RF does not have boundaries, such as the limits of a wire.
  - RF is unprotected from outside signals.
  - RF transmission is subject to the same challenges inherent in any wave-based technology. For example, as you get further away from the source, eventually you may lose the signal all together.
  - RF bands are regulated differently in various countries.
- WLANs connect clients to the network through a wireless access point (AP) instead of an Ethernet switch.
- WLANs connect mobile devices that are often battery powered.
  - Wireless NICs tend to reduce the battery life of a mobile device.
- WLANs support hosts that contend for access on the RF media (frequency bands).
  - 802.11 prescribes collision-avoidance instead of collision-detection for media access to proactively avoid collisions within the media.
- WLANs use a different frame format than wired Ethernet LANs.
  - WLANs require additional information in the Layer 2 header.
- WLANs raise more privacy issues
  - because radio frequencies can reach outside the facility.

### Table: Network Architecture Standards

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>802.11 Wireless LAN</th>
<th>802.3 Ethernet LANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td>Radio Frequency (RF)</td>
<td>Cable</td>
</tr>
<tr>
<td>Media Access</td>
<td>Collision Avoidance</td>
<td>Collision Detection</td>
</tr>
<tr>
<td>Availability</td>
<td>Anyone with a radio NIC in range of an access point</td>
<td>Cable connection required</td>
</tr>
<tr>
<td>Signal Interference</td>
<td>Yes</td>
<td>Inconsequential</td>
</tr>
<tr>
<td>Regulation</td>
<td>Additional regulation by local authorities</td>
<td>IEEE standard dictates</td>
</tr>
</tbody>
</table>

Physical Media
Comparing a WLAN to a LAN

Wireless Access Points (AP) instead of a switch.

Wireless NICs tend to reduce battery life.

Different Frame Format

Privacy Issues

CSMA/CA (Avoidance) instead of CSMA/CD

Introducing Wireless LANs

• 802.11 wireless LANs extend the 802.3 Ethernet LAN infrastructures to provide additional connectivity options.
• In an 802.3 Ethernet LAN, each client has a cable that connects the client NIC to a switch. The switch is the point where the client gains access to the network.
• In a wireless LAN, each client uses a wireless adapter to gain access to the network through a wireless device such as a wireless router or access point.
  • The wireless adapter in the client communicates with the wireless router or access point using RF signals.
  • Once connected to the network, wireless clients can access network resources just as if they were wired to the network.
Wireless LAN Standards

- **802.11** wireless LAN is an IEEE standard that defines how radio frequency (RF) in the unlicensed industrial, scientific, and medical (ISM) frequency bands is used for the physical layer and the MAC sub-layer of wireless links.

- **Data Rate:**
  - **802.11**: 1 - 2 Mb/s data rates
  - **802.11a and g**: support up to 54 Mb/s
  - **802.11b**: supports up to a maximum of 11 Mb/s
  - **802.11n**: Speculated to be 300 Mb/s.

- **Modulation technique:**
  - Direct Sequence Spread Spectrum (DSSS) 802.11b, 802.11g
  - Orthogonal Frequency Division Multiplexing (OFDM), 802.11a, 802.11g, 802.11n

- **Band:**
  - **2.4 GHz**: 802.11b, 802.11g, 802.11n
  - **5 GHz**: 802.11a, 802.11n
Wireless LAN Standards

• Data Rates are affected by modulation technique:
  • Direct Sequence Spread Spectrum (DSSS):
    • Simpler of the two methods.
    • Less expensive to implement.
    • 802.11b and 802.11g.
  • Orthogonal Frequency Division Multiplexing (OFDM):
    • Faster data rates than DSSS.
    • 802.11a, 802.11g, 802.11n.

• 802.11a
  • OFDM modulation and uses the 5 GHz band.
  • Less likely to experience interference than devices that operate in the 2.4 GHz band
    • Because there are fewer consumer devices that use the 5 GHz band.
  • There are some important disadvantages to using the 5 GHz band.
    • The first is that higher frequency radio waves are more easily absorbed by obstacles such as walls, making 802.11a susceptible to poor performance due to obstructions.
    • The second is that this higher frequency band has slightly poorer range than either 802.11b or g.
    • Also, some countries, including Russia, do not permit the use of the 5 GHz band, which may continue to curtail its deployment.
Wireless LAN Standards

• **802.11b and 802.11g**
  - 802.11b specified data rates of 1, 2, 5.5, and 11 Mb/s in the 2.4 GHz ISM band using DSSS.
  - 802.11g achieves higher data rates in that band by using the OFDM modulation technique.
    - 802.11g also specifies the use of DSSS for backward compatibility with IEEE 802.11b systems.
    - OFDM data rates of 6, 9, 12, 18, 24, 48, and 54 Mb/s.
  - Advantages of using the 2.4 GHz band.
    - Devices in the 2.4 GHz band will have better range than those in the 5GHz band.
    - Transmissions in this band are not as easily obstructed as 802.11a.
  - Disadvantage to using the 2.4 GHz band.
    - Many consumer devices also use the 2.4 GHz band and the devices to be prone to interference. Microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

• **802.11n**
  - The IEEE 802.11n draft standard is intended to improve WLAN data rates and range without requiring additional power or RF band allocation.
  - 802.11n uses multiple radios and antennae at endpoints, each broadcasting on the same frequency to establish multiple streams.
    - The multiple input/multiple output (MIMO) technology splits a high data-rate stream into multiple lower rate streams and broadcasts them simultaneously over the available radios and antennae.
    - This allows for a theoretical maximum data rate of 248 Mb/s using two streams.
  - The standard was ratified in September 2009.
Wi-Fi Certification

- The 3 key organizations influencing WLAN standards are:
  - **ITU-R**
    - ITU-R regulates allocation of RF bands.
    - The ITU-R regulates the allocation of the RF spectrum.
  - **IEEE**
    - IEEE specifies how RF is modulated to carry information.
    - The IEEE developed and maintains the standards for local and metropolitan area networks. The dominant standards in the IEEE 802 are 802.3 Ethernet, and 802.11 Wireless LAN.
  - **Wi-Fi Alliance (www.wi-fi.org)**
    - Ensures that vendors make devices that are interoperable by certifying vendors for conformance to industry norms and adherence to standards.
    - Certification includes all IEEE 802.11 RF technologies and the WPA and WPA2 security standards based on IEEE 802.11i.
    - A global, nonprofit, industry trade association devoted to promoting the growth and acceptance of WLANs.
    - The Wi-Fi Alliance’s testing and certification programs help ensure the interoperability of WLAN products based on the IEEE 802.11 specification.

Wireless LANs

- The Wireless LAN, then, is an extension of the Ethernet LAN.
Wireless LAN Components

- Additional components and protocols are used for 802.11 wireless connections to extend the 802.3 Ethernet LAN.

Wireless NICs

- The device that makes a client station capable of sending and receiving RF signals is the **wireless NIC**.
  - Like an Ethernet NIC, the wireless NIC, using the modulation technique it is configured to use, encodes a data stream onto an RF signal.
  - Wireless NICs are most often associated with mobile devices, such as laptop computers.
  - In the 1990s, wireless NICs for laptops were cards that slipped into the PCMCIA slot.
  - PCMCIA wireless NICs are still common, but many manufacturers have begun building the wireless NIC right into the laptop.
  - Unlike 802.3 Ethernet interfaces built into PCs, the wireless NIC is not visible, because there is no requirement to connect a cable to it.
  - Other options have emerged over the years as well. Desktops located in an existing, non-wired facility can have a wireless PCI NIC installed.
    - To quickly set up a PC, mobile or desktop, with a wireless NIC, there are many USB options available as well.
Wireless Infrastructure Components

- **Wireless Access Points:**
  - An access point is a Layer 2 device that functions like an 802.3 Ethernet hub.
  - Connects wireless clients (or stations) to the wired LAN.
  - Client devices communicate with the AP – not each other.
  - Converts the TCP/IP data packets from their 802.11 frame encapsulation to the 802.3 Ethernet frame format.
  - Clients must **associate** with an access point to obtain network services.
  - **Association:** The process by which a client joins an 802.11 network. It is similar to plugging into a wired LAN.
Wireless Access Points:

Wireless Infrastructure Components

- **CSMA/CA**: Carrier Sense Multiple Access with Collision Avoidance.
  - This simply means that devices on a WLAN must sense the medium for energy (RF stimulation above a certain threshold) and wait until the medium is free before sending.
  - If an access point receives data from a client station, it sends an **acknowledgement** to the client that the data has been received.
  - This acknowledgement keeps the client from assuming that a collision occurred and prevents a data retransmission by the client.
- **RF signals attenuate**.
  - That means that they lose their energy as they move away from their point of origin.
Hidden Node/Station Problem

- Two client stations that both connect to the access point, but are at opposite sides of its reach.
- If they are at the maximum range to reach the access point, they will not be able to reach each other.
- Neither of those stations sense the other on the medium, and they may end up transmitting simultaneously.

One means of resolving the hidden node problem is a feature called request to send/clear to send (RTS/CTS).

- When RTS/CTS is enabled in a network, access points allocate the medium to the requesting station for as long as is required to complete the transmission.
- When the transmission is complete, other stations can request the channel in a similar fashion.

Remember, stations actually communicate through the Access Point. The access point has a single channel for all traffic.
Wireless Infrastructure Components-Router

• Wireless Routers:
  • Wireless routers perform the role of access point, Ethernet switch, and router.
  • For example, the Linksys WRT300N used is really three devices in one box.
    • First, there is the wireless access point, which performs the typical functions of an access point.
    • A built-in four-port, full-duplex, 10/100 switch provides connectivity to wired devices.
    • Finally, the router function provides a gateway for connecting to other network infrastructures.
  • The WRT300N is most commonly used as a small business or residential wireless access device.
  • The expected load on the device is low enough that it should be able to manage the provision of WLAN, 802.3 Ethernet, and connect to an ISP.
Configurable Parameters for Wireless Endpoints

- The figure shows the initial screen for wireless configuration on a Linksys wireless router.

Configurable Parameters: Mode

802.11g is backward compatible with 802.11b. Mixed mode supports both.
Configurable Parameters: SSID

A shared service set identifier (SSID) is a unique identifier that client devices use to distinguish between multiple wireless networks in the same vicinity.

Several access points can share an SSID.

Alphanumeric, case-sensitive, from 2 to 32 characters.

Configurable Parameters: Channel

- **Wireless channel:** The 2.4 GHz band is broken down into 11 channels for North America and 13 channels for Europe.
  - These channels have a center frequency separation of only 5 MHz and an overall channel bandwidth (or frequency occupation) of 22 MHz.
  - The 22 MHz channel bandwidth combined with the 5 MHz separation between center frequencies means there is an overlap between successive channels.
  - Best practices for WLANs that require multiple access points are set to use non-overlapping channels:
    - If there are three adjacent access points, use channels 1, 6, and 11.
    - If there are just two, select any two that are five channels apart, such as channels 5 and 10.
Configurable Parameters: Channel

The IEEE 802.11 standard establishes the channelization scheme for the use of the unlicensed ISM RF bands in WLANs. The 2.4 GHz band is broken down into 11 channels for North America and 13 channels for Europe.

Best practices for WLANs that require multiple access points are set to use non-overlapping channels.

Wireless Topologies

- WLANs can accommodate various network topologies.
- When describing these topologies, the fundamental building block of the IEEE 802.11 WLAN architecture is the basic service set (BSS).
  - BSS: A group of stations that communicate with each other.
- Three Types:
  1. Ad Hoc (Independent Basic Service Set – IBSS)
  2. Basic Service Set (BSS)
  3. Extended Service Set (ESS)
**Wireless Topologies: Ad Hoc**

- Wireless networks can operate without access points.
- Client stations which are configured to operate in ad hoc mode configure the wireless parameters between themselves.
- The IEEE 802.11 standard refers to an ad hoc network as an independent BSS (IBSS).

**Wireless Topologies: BSS**

- **Basic Service Sets (BSS):**
  - Access points provide an infrastructure that adds services and improves the range for clients.
  - A single access point in infrastructure mode manages the wireless parameters and the topology is simply a BSS.
  - The coverage area for both an IBSS or a BSS is the basic service area (BSA).
**Wireless Topologies: Extended Service Sets (ESS)**

- When a single BSS provides insufficient RF coverage, one or more can be joined through a common distribution system into an extended service set (ESS).
- One BSS is differentiated from another by the **BSS identifier (BSSID)**. This is usually the MAC address of the AP
  - The coverage area is the **extended service area (ESA)**.

**Different MAC Addresses = different BSSIDs.**

**Wireless Topologies**

- **Common Distribution System:**
  - Allows *multiple access points* in an ESS to appear to be a *single BSS*.
  - An ESS generally includes a **common SSID** to allow a user to **roam** from access point to access point.
  - **Cells** represent the coverage area provided by a single channel.
    - An ESS should have 10 to 15 percent overlap between cells.
    - Roaming capability created by using **non-overlapping channels** (e.g. one cell on channel 1 and the other on channel 6).

**Summary of WLAN Topologies**

<table>
<thead>
<tr>
<th>Wireless Devices</th>
<th>Topology Mode</th>
<th>Topology Building Block</th>
<th>Coverage Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>No access points</td>
<td>Ad Hoc</td>
<td>Independent Basic Service Set (IBSS)</td>
<td>Basic Service Area (BSA)</td>
</tr>
<tr>
<td>One access point</td>
<td>Infrastructure</td>
<td>Basic Service Set (BSS)</td>
<td>Basic Service Area (BSA)</td>
</tr>
<tr>
<td>More than one access point</td>
<td>Infrastructure</td>
<td>Extended Service Set (ESS)</td>
<td>Extended Service Area (ESA)</td>
</tr>
</tbody>
</table>
Client and Access Point Association

- Key part of the 802.11 process is discovering a WLAN and connecting to it.
- The primary components:
  1. **Beacons**: Frames used by the WLAN network to advertise its presence.
  2. **Probes**: Frames used by WLAN clients to find their networks.
  3. **Authentication**: Left over from the original 802.11 standard, but still required.
  4. **Association**: Establishing the data link between an access point and a WLAN client.

Wireless Association: Beacon

- Frames used by the WLAN network to advertise its presence.
- The primary purpose of the beacon is to allow WLAN clients to learn which networks and access points are available in a given area, thereby allowing them to choose which network and access point to use. Access points may broadcast beacons periodically.

The only part of the process that may be broadcast on a regular basis. Not necessarily enabled.
Wireless Association

Before an 802.11 client can send data over a WLAN network, it goes through the following three-stage process:

- **Step 1**: 802.11 Probing.
- **Step 2**: Authentication.
- **Step 3**: Association.

Wireless Association

**Step 1: 802.11 Probing**
- Clients search for a specific network by:
  - Sending a probe request out on multiple channels.
  - Specifies the network name (SSID) and bit rates.
  - A typical WLAN client is configured with a desired SSID.
  - Client is simply trying to discover any available WLANs:
    - Sends out a probe request with no SSID.
    - All access points that are configured to respond to this type of query respond.
    - WLANs with the broadcast SSID feature disabled do not respond.
Wireless Association

• **Step 2: Authentication**
  802.11 was originally developed with two authentication mechanisms.
  1. **Open Authentication:**
     • A NULL authentication
     • The client says "authenticate me".
     • The access point responds with "yes".
     • This is the mechanism used in almost all 802.11 deployments.
  2. **Shared Key Authentication:**
     • Based on a key that is shared between the client station and the access point called the Wired Equivalency Protection (WEP) key.
     • The idea of the shared WEP key is that it gives a wireless link the equivalent privacy of a wired link, but the original implementation was flawed.
     • WEP needs to be included in client and access point implementations for standards compliance but it is not used or recommended.

Wireless Association

• **Step 3: 802.11 Association**
  • Finalizes the security and bit rate options.
  • Establishes the data link between the WLAN client and the access point.
  • The client learns the BSSID (MAC Address) of the access point.
  • Access point maps a logical port known as the association identifier (AID) to the WLAN client.
  • AID is equivalent to a port on a switch.
  • Association allows the infrastructure switch to keep track of frames destined for the WLAN client so that they can be forwarded.
Planning the Wireless LAN

- There needs to be a well-documented plan before a wireless network can be implemented.

- **Number of Users:**
  - Not a straightforward calculation.
  - Depends on the geographical layout of your facility (how many bodies and devices fit in a space),

- **Data Rates expected:**
  - RF is a shared medium and the more users there are the greater the contention for RF.
  - Use non-overlapping channels in an ESS.
  - You will have sufficient wireless support for your clients if you plan your network for proper RF coverage in an ESS.
Planning the Wireless LAN: Location of Access Points

- When planning the location of access points, it is not as simple as drawing coverage area circles and drop them over a plan.
- Do access points use existing wiring?
- If access points are to use existing wiring.
  - Position access points above obstructions.
  - Position access points vertically near the ceiling in the center of each coverage area, if possible.
  - Position access points in locations where users are expected to be e.g. conference rooms are a better location for AP than a hallway.
- When these points have been addressed, estimate the expected coverage area of an access point. This value varies depending on
  - The WLAN standard or mix of standards that you are deploying,
  - The nature of the facility,
  - The transmit power that the access point.
- Based on your plan, place access points on the floor plan so that coverage circles are overlapping

Planning the Wireless LAN: Example

- An open auditorium (a Warehouse/Manufacturing Building Type) shown in the figure is approximately 20,000 square feet.
- Network requirements specify that there must be a minimum of 6 Mb/s 802.11b throughput in each BSA, because there is a wireless voice over WLAN overlaid on this network.
  - With access points, 6 Mbps can be achieved in open areas like those on the map, with a coverage area of 5,000 square feet in many environments.
  - Note: The 5,000 square foot coverage area is for a square. The BSA takes its radius diagonally from the center of this square.
- Let us determine where to place the access points.
  - The facility is 20,000 square feet, therefore dividing 20,000 square feet by a coverage area of 5,000 square feet per access point results in at least 4 access points required for the auditorium.
  - Next, determine the dimension of the coverage areas and arrange them on the floor plan.
    - Because the coverage area is a square with side "Z", the circle that is tangent to its four corners has a radius of 50 feet, as shown in the calculations.
20,000 Sq. Ft. (1860 Sq. Meters)

Minimum of 6 Mbps 802.11b throughput for each Basic Service Area (BSA)

Can be achieved with a coverage area of 5,000 Sq. Ft. (465 Sq. Meters)

Number of Access Points

Planning the Wireless LAN

Planning the Wireless LAN

Dimension of Coverage Area

Align coverage areas along "Z" to ensure minimum BSA overlap

71 foot (22 Meter) Square
Planning the Wireless LAN

Location of Access Points