1.Components of wireless Networks

Wireless LANs consist of components similar to traditional Ethernet-wired LANs. In fact, wireless LAN protocols are similar to Ethernet and comply with the same form factors. The big difference, however, is that wireless LANs don't require wires.

➢ User Devices :

- Users of wireless LANs operate a multitude of devices, such as PCs, laptops.
- The use of wireless LANs to network stationary PCs is beneficial because of limited needs for wiring.
- Laptops and PDAs, however, are commonly equipped with wireless LAN connectivity because of their portable nature.
- User devices might consist of specialized hardware as well. For example, bar code scanners and patient monitoring devices often have wireless LAN connectivity.

➢ Radio NICs :

- A major part of a wireless LAN includes a radio NIC that operates within the computer device and provides wireless connectivity.
- A wireless LAN radio NIC, sometimes referred to as a radio card, often implements the 802.11 standard.
- The cards generally implement one particular physical layer, such as 802.11a or 802.11b/g.
- As a result, the radio card must utilize a version of the standard that is compatible with the wireless LAN.
- Radio cards come in a variety of form factors, including: ISA, PCI, PC card, mini-PCI, and CF.
- PCs generally utilize ISA and PCI cards; but PDAs and laptops use PC cards, mini-PCI, and CF adapters.

➢ Access Points :

- An access point contains a radio card that communicates with individual user devices on the wireless LAN, as well as a wired NIC that interfaces to a distribution system, such as Ethernet.
- System software within the access point bridges together the wireless LAN and distribution sides of the access point.
- The system software differentiates access points by providing varying degrees of management, installation, and security functions.
- Figure shows an example of access-point hardware.

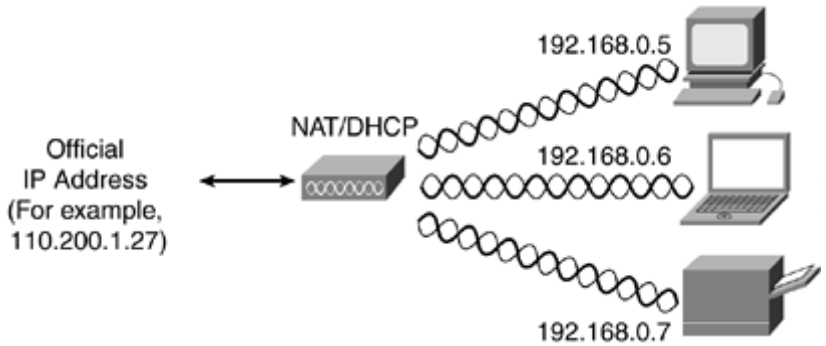
Figure . Wireless LAN Access Points Connect Wireless LANs to Wired Networks (Photo Courtesy of Linksys)

- In most cases, the access point provides an http interface that enables configuration changes to the access point through an end-user device that is equipped with a network interface and a web browser.
- Some access points also have a serial RS-232 interface for configuring the access point through a serial cable as well as a user device running terminal emulation and Telnet software, such as hyper terminal.

➢ Routers :

- By definition, a router transfers packets between networks.
- The router chooses the next best link to send packets on to get closer to the destination.
- Routers use Internet Protocol (IP) packet headers and routing tables, as well as internal protocols, to determine the best path for each packet.
- A wireless LAN router adds a built-in access point function to a multiport Ethernet router.
- This combines multiple Ethernet networks with wireless connections.
- A typical wireless LAN router includes four Ethernet ports, an 802.11 access point, and sometimes a parallel port so it can be a print server.
- This gives wireless users the same ability as wired users to send and receive packets over multiple networks.
- Routers implement the Network Address Translation (NAT) protocol that enables multiple network devices to share a single IP address provided by an Internet service provider (ISP).

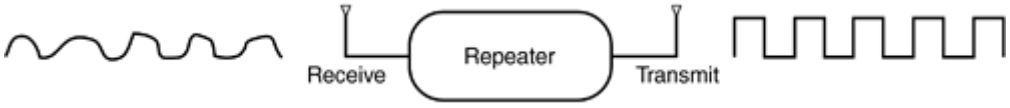
Figure 5.1 illustrates this concept. Routers also implement Dynamic Host Configuration Protocol (DHCP) services for all devices. DHCP assigns private IP addresses to devices. Together, NAT and DHCP make it possible for several network devices, such as PCs, laptops, and printers to share a common Internet IP address.



➢ Repeaters :

- Access points, which require interconnecting cabling, generally play a dominant role for providing coverage in most wireless LAN deployments.
- Wireless repeaters, however, are a way to extend the range of an existing wireless LAN instead of adding more access points.
- There are few standalone wireless LAN repeaters on the market, but some access points have a built-in repeater mode.
- A repeater simply regenerates a network signal to extend the range of the existing network infrastructure.
- (See Figure 5-3.) A wireless LAN repeater does not physically connect by wire to any part of the network.
- Instead, it receives radio signals from an access point, end-user device, or another repeater; it retransmits the frames. This makes it possible for a repeater located between an access point and distant user to act as a relay for frames traveling back and forth between the user and the access point.

Figure 5-3. Wireless LAN Repeaters Are Simple Devices That Require No Cabling



➢ Antennae :

- Most antennae for wireless LANs are omnidirectional and have low gain.
- Nearly all access points, routers, and repeaters come standard with omnidirectional antennae.
- Omnidirectional antennae satisfy most coverage requirements; however, consider the use of optional directive antennae to cover a long, narrow area.

.

2.Security issues in wireless networks

- **Wireless local area networks (WLANs)** transmit and receive data using radio waves rather than wires. This lack of a physical barrier makes WLANs vulnerable to unlawful interception, eavesdropping, hacking and a range of other cyber security issues.

Three most common WLAN security threats include:

- **denial of service attacks** - where the intruder floods the network with messages affecting the availability of the network resources
- **spoofing and session hijacking** - where the attacker gains access to network data and resources by assuming the identity of a valid user
- **eavesdropping** - where unauthorised third-parties intercept the data being transmitted over the secure network

To counter these threats, you should make every effort to configure your WLAN correctly. You should also enable a range of security features, such as standard authentication and encryption, alongside other access control mechanisms.

Basic WLAN security features

Early WLAN hardware used a number of basic security methods, including:

- **Service Set Identifiers (SSIDs)** - these prevent connection to access points unless a device uses a given identifier correctly
- **Media Access Control (MAC)** - this involves using addresses attached to each device to limit connection to access points
- **Wired Equivalent Privacy (WEP)** - WEP uses encryption keys so that only devices with the correct key can communicate with access points.

3.Risk of using unsecured wifi

➢ Unsecured Wi-Fi :

- An unsecured Wi-Fi connection is one that utilizes no security encryption whatsoever.
- Encrypted Wi-Fi channels secure the data from interception, as no one can access any of the connected computers or the connection itself.
- Identifying an unsecured network is easy, as any secured network would ask for a valid password.

➢ Login Information Interception

- A major risk of connecting to an unsecured Wi-Fi connection comes from using services that require login information.
- Data transmitted over unsecured Wi-Fi can be intercepted by third parties.
- These third parties can extract your login information and passwords from this intercepted data and use it to fraudulently access your services.
- This can include online banking, email and other services that can be used to facilitate identity theft.

➢ Sensitive Information Interception

- The same interception risk for login info also applies to other data transmitted over an unsecured Wi-Fi connection.
- Information sent in instant messages, emails and other data-transmission tools can also be intercepted and put to illicit use.
- When transmitting sensitive corporate information, this can be an especially dangerous security risk.

➢ Bandwidth Theft

- If your company is operating an unsecured Wi-Fi, you also risk bandwidth theft.

- When others sign onto your network, the tasks they perform will consume a portion of the available bandwidth.
- Depending on how many people are already using your network legitimately and how many unauthorized users are connected, your users may experience lag.
- This can hurt productivity and create a serious inconvenience for your employees.

➢ Illegal Usage

- If you host unsecured Wi-Fi, an unauthorized user can put your network to illicit use.
- Illegal file transfers and downloads, the use of your network to disseminate viruses, and even using the network to procure child pornography or other illegal materials are all serious crimes.
- Since the perpetrator would be using your network, any investigation will lead back to your network. As such, your company may be liable for any penalties these crimes may incur, even when none of your legitimate users did the crimes.

➢ Network Data Theft

- Hosting unsecured Wi-Fi also endangers the data stored on your company's computers.
- Any unauthorized users will be able to access unsecured resources on your computer network, including the data on any connected computers.
- Without proper intrusion safeguards, sensitive corporate information can be stolen.
- Viruses and other malicious software can also be introduced to the network.