Computer Networks

Topic 7:

Wireless Network Hardware

V1.0

Computer Networks

Topic 7 – Lecture 1:

Wireless Network Hardware

V1.0

Scope and Coverage

This topic will cover:

- Wireless network hardware
- Wireless hardware selection
- Creating a wireless network

Learning Outcomes

By the end of this topic, students will be able to:

- Select the hardware component of a network
- Configure the hardware components for a wireless network
- Test the connectivity of a network
- Troubleshoot client-side connectivity issues using appropriate tools

Wireless Networks

- Physical cabling replaced with wireless connections
- Still require:
  - ***Workstations***
  - ***Peripherals*** (but may be wireless)
- More flexible in terms of workstation placement
- Requires some hardware that is specific to wireless networks

Wireless Routers

- Support computers configured with ***wireless network adapters*** (see later)
- Contain network switch to allow connection via Ethernet cable
- Allow cable modem and DSL Internet connections to be shared
- May include a built-in firewall

Wireless Access Points

- May join wireless clients to wired Ethernet network
- May connect to another access point, or to a wired Ethernet router
- In home networking, can be used to extend a network based on a wired broadband router
- Clients can join the home network without re-configuring connections

Business WLAN

- Wireless access points are commonly used in large office buildings to create one WLAN.
- Each access point typically supports up to 255 client computers.
- By connecting access points to each other, thousands of access points can be created.
- Client computers may move or "roam" between each of these access points as needed.

Wireless Network Adapters

- Allow a computing device to join a wireless LAN
- Contain a built-in radio transmitter and receiver
- Exist in different forms:
  - ***PCI wireless adapters*** are add-in cards designed for installation inside a desktop computer having a PCI bus
  - ***USB wireless adapters*** connect to the external USB port
  - ***PC Card*** or ***PCMCIA wireless adapters*** insert into a narrow open bay on a notebook computer
  - Most modern computers have inbuilt adapters

Wireless Print Servers

- Allows printers to be conveniently shared across a WiFi network
- Usually connected to printers by a network cable, normally USB
- Can connect to a wireless router over WiFi, or can be joined using an Ethernet cable
- Include a built-in wireless antenna and LED lights to indicate status

Wireless Print Server Advantages

- Allows printers to be located anywhere, tied to the location of computers
- Does not require a computer to manage all print jobs, that can slow down its performance
- Allows administrators to change computer names and other settings without having to re-configure the network printing settings

Wireless Range Extender

- Increases the distance over which a WLAN signal can spread, overcoming obstacles and enhancing overall network signal quality
- Several different forms are available
- Also known as "range expanders" or "signal boosters"

Wireless Peripherals

- A number of peripheral devices are available that can connect to a network using WiFi or Bluetooth technology and these include:
  - Video cameras
  - Game adapters
  - Keyboard
  - Mouse
  - PDA
  - Mobile phone

Bluetooth Hardware

- Many items that can connect to networks:
  - Computer peripherals
  - PDA, smartphone
  - Hands free kits
  - GPS
- USB Bluetooth adapters used for computers that don’t have built in Bluetooth
- Bluetooth access point used for connecting to LAN via Bluetooth

Bluetooth USB Adapter

- ***Dongle*** can plug into a USB port on your PC or laptop
- Comes with software required to get connected
- Allows non-Bluetooth enabled PC to connect to:
  - PDA/Smartphone
  - GPS
  - Peripherals

Bluetooth Access Point

- Can transfer data from a Bluetooth-enabled computer or device to computers connected to the LAN
- Can gain Internet access through the connected LAN

Ad-hoc Wireless Networks

- Bluetooth
- Device connecting directly to each other, peer-to-peer network
- Generally ok for home networks
- In business networks, “infrastructure mode” should be used (access points)

Computer Networks

Topic 7 – Lecture 2:

Wireless Hardware Selection & Creating a Wireless Network

A Small Business Network

- We will assume the network is being built for a small business, but the key points are relevant to any size of business.
- To create a good network the basic plan is:
  1. Decide what kind of WLAN is needed
  2. Purchase the best equipment the budget allows for
  3. Install the equipment
  4. Test the installation

Wireless Router

- Provides both wireless & wired connections
- Acts as bridge between LAN and WAN
- Shares WAN connection between all networked computers
- Acts as a DHCP server allowing each connected device to have a unique IP address
- Generally contains an embedded firewall for security

Choosing a Standard

- All modern WLAN equipment support the IEEE 802.11n standard
  - Maximum transfer rate 540Mbps
  - Real rate less, e.g. interference and overhead
- N standard equipment can usually integrate with older devices connecting at b or g standard, but will slow down entire network
- Buy n standard – it can be worth upgrading old equipment

Choosing Network Adapters

- Every computer connecting to your network must have a wireless adapter.
- Most new computers and other devices now come equipped with built-in wireless adapters.
- Servers and other devices usually make use of built-in network Ethernet ports.
- If your device has neither, purchase a wireless adapter card or USB wireless adapter.

Choosing Access Points

- A router typically has four Ethernet ports for:
  - Storage devices
  - Computers
  - Servers
- If additional ports are required, purchase additional access points.
- Connecting to a router or another access point gives additional ports and enables you to add more nodes to your network.

Know Your Building

- Dense building materials reduce the strength of your wireless signal:
  - Internal brick walls
- Water retaining features limit the range
  - Pipes
  - Bathroom
- May need more access points to ensure a fast, reliable connection

How Many People?

- Number of people using the network is major factor in determining number of access points
- Also need adequate bandwidth
- Network administrator should also be able to manage multiple access points and balance the loads
- Centrally-managed wireless controller appliances can do this dynamically

How Much Power?

- Determine the number of points you need.
- Then determine the power requirements necessary to support these points.
- You should purchase power surge protectors for your equipment
  - the most common cause of equipment failure is a power surge.

Locating Access Points

- Don't settle prematurely on a location
- Install in a central location
- Avoid physical obstructions
- Avoid reflective surfaces
- Avoid other RF transmitters
- Avoid electrical equipment
- Adjust antennae
- Consider repeaters

Don't Settle Prematurely on a Location

- Experiment
- Place the device in several different promising locations.
- Not the most scientific way
- Simple practical method

Install in a Central Location

- For WLANs with multiple wireless clients, find a good compromise position.
- Clients too far away from the base station will manage only 10% - 50% the bandwidth of clients nearby to it
- You might need to sacrifice the network performance of one client for the good of the rest of the network.

Avoid Physical Obstructions

- Barriers along the "line of sight" between client and base station will degrade the signal
- Plaster or brick walls tend to have the most negative impact
- Any obstruction including cabinets or furniture will weaken the signal to some degree
- Obstructions tend to lie close to floor level – can install access point or router near the ceiling

Avoid Reflective Surfaces

- Some Wi-Fi signals literally bounce off:
  - Windows
  - Mirrors
  - Metal filing cabinets
  - Stainless steel counters

- Reduces network range and performance

Avoid Other RF Transmitters

- At least 1m away from other appliances that send wireless signals in the same frequency range, e.g.
  - Microwave ovens
  - Cordless telephones

- Any appliance that transmits in the same general range can generate interference

Avoid Electrical Equipment

- Other electrical equipment may generate interference:
  - Electric fans
  - Motors
  - Flourescent lighting

Adjust Antennae

- Antennas on wireless access points and routers can usually be rotated or re-pointed to fine tune the signal

- Equipment suppliers will normally include instructions on how to do this

Consider Repeaters

- If you cannot find a suitable location for your wireless gear, there are alternatives:
  - Upgrade the base station antenna
  - Install a Wi-Fi repeater
  - Use extra access points

Public or Private?

- Decide what you wish to provide:
  - Mobile and wireless access for you and your employees
  - Or convenient guest access for customers and business associates

- Different types of security and access controls for each

Internal Private Network

- Planning security and the logistics of connecting it to your wired network
- Develop ID and authentication procedures
- Create a well-defined acceptable use policy
- Create a user training program
- Adapting internal firewall for wireless access

Public Network

- Develop a system that automatically takes users to a log-in page
  - Clearly states what can and what cannot be done while using this gateway
  - Enter an email address as an acknowledgement of these public-use policies
- Work with software that can lock users out of specific websites, etc.

Securing Your Network

- Have you ever searched for an unsecured wireless network when away from home or college?
- Keeping the wireless network safe is a top priority
  - Avoid using obsolete protocols for wireless security, like WEP (Wired Equivalent Privacy)
  - WPA (Wi-Fi Protected Access) is better
  - WPA2 is even better and will help safeguard against hackers

Troubleshooting Your Network

- Requires a logical approach as for wired networks
- There are three main areas where problems occur:
  - Workstation issues
  - Access point issues
  - Server/infrastructure issues

The Workstation/AP interface

- If a workstation has a problem, is it that workstation alone?
- If only one workstation has a problem and other workstations function, the problem is with the ***workstation***.
- If the problem is with all workstations, the problem lies with the ***access point***.

The AP/Wired LAN interface

- Use a wired workstation to ping the access point that has a problem.
- If ping is successful, the problem is likely to lie with the wired network
- If ping is unsuccessful, then the AP is not connected and there is a problem with the AP or the wired connection from AP

References

- Lowe, D. (2009). *Networking for Dummies,* 9th edition. John Wiley & Sons.
- Rackley, S. (2007). *Wireless Networking Technology: From Principles to Successful Implementation.* Newnes.

Topic 7 – Wireless Network Hardware

Any Questions?