
NETWORKS

Network Basics

Network: devices that are connected together to share data & resources

Network Adapter / Interface Card: card that enables devices to connect to a network adapting the signal from one side to the other. Motherboard uses parallel transmission using voltages, networks serial using voltages, light or radio waves.

Local Area Network (LAN): a network over a small geographical distance – usually on one site & typically used by one organisation

Wide Area Network (WAN): a network spread over a large geographical distance

Network topology

Network topology: the layout of a network usually in terms of its conceptual layout rather than physical layout

Physical Topology: the way in which devices in a network are physically connected

Logical Topology: the conceptual way in which data is transmitted around a network

A network physically wired in star topology can behave logically as a bus network by using a bus protocol and appropriate physical switching.

Bus topology

A way of connecting devices (nodes) in a network where each node connects to a main data cable as a backbone to transmit data. Cheaper and easier to install, but less secure and slow.

Protocol CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

1. If the bus is busy; monitor until the bus is idle
2. When the *bus is idle*; transmit a frame
3. While transmitting; monitor the bus for a collision
4. If a collision is detected
 - a. Send a *jamming signal*
 - b. All hosts realise there has been a collision and stop transmitting
5. Hosts wait for a *random timeout period*
6. Start the process again from step 1

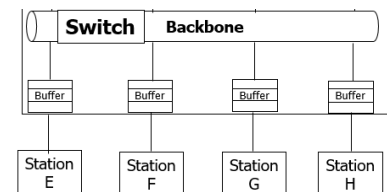
Star topology

A way of connecting devices (nodes) in a network where each workstation has a dedicated cable to a central computer or switch.

Switched Ethernet: Star topologies connected together with high speed buses.

Switch

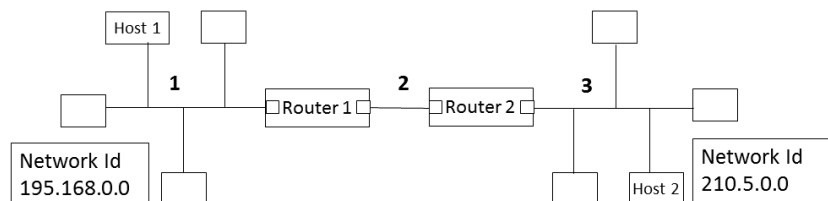
Backbone is an internal bus. The switch builds a *lookup table* mapping MAC address to *line cards* → reduce unnecessary traffic



MAC address

The MAC (Media Access Control) address is a unique code that identifies a particular device on a network, assigned by NIC manufacturer. Six groups of 2 Hex digits (3 for Manufacturer, 3 for NIC).

Routing Messages USING IP & MAC Addresses



Hop	Source IP	Destination IP	Source MAC	Destination MAC
1	195.168.0.37	210.5.0.67	00-03-47-C9-69-52 (Host 1)	00-02-22-C9-54-13 (R. 1)
2	195.168.0.37	210.5.0.67	00-02-22-C9-54-14 (R. 1)	00-62-77-C9-A1-88 (R. 2)
3	195.168.0.37	210.5.0.67	00-62-77-A1-12-40 (R. 2)	01-32-07-D6-55-46 (Host 2)

Client-server networks

Client-server is a network methodology where one computer has the main processing power and storage and the other computers act as clients requesting services from the server. Possible client requests: access to a printer, an email, an application, a file or providing a secure connection to the internet.

Peer-to-peer network

A network methodology where all devices in a network share resources between them rather than having a server. In peer-to-peer networks:

- each computer has equal status, so can act as both client and server;
- computers communicate directly with each other, there is no dependence on a server;
- management of security / administration could be more difficult;

Wireless networks

Wireless Wide Area Network (WWAN): a WAN that does not use cables but sends data via radio waves.

Wireless Local Area Network (WLAN): a LAN that does not use cables but connects using radio waves. MAC addresses are used to identify devices.

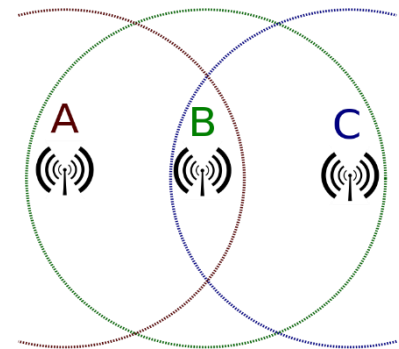
WiFi: an international standard method for connecting devices wirelessly to a network and to the internet (through a WLAN network)

- Note: the speed is shared between all the connected devices, more nodes → slower speed

CSMA / CA: Collision Avoidance Protocol

On Wireless Networks, CSMA / CD cannot be used due to the *Hidden Node problem*: if B is the AP then

- C can see the AP but not see A, it is out of range
- A can see the AP but not see C, it is out of range
- → A & C cannot detect collisions with traffic emanating from each other



A different protocol is used *CSMA /CA* : collision avoidance (not detection)

1. Sending Node determines if the medium is idle
 - a. Sends entire message if idle, without listening
 - b. Otherwise waits random timeout interval and tries again
2. Receiving Node sends an *acknowledgment* back
3. If sending node does not receive an ACK within a specified time it will try and send again

Request to Send / Clear to Send (RTS / CTS) is an extension to CSMA / CA: sending Node listens to see if the medium is idle, if idle sends a RTS to the AP, if the AP is aware of no other transmissions it will reply with a CTS → AP only allows one Node to transmit at a time. RTS / CTS not commonly used due to overhead on small transmissions.


Wireless Access Point

Messages between wireless nodes go via the Access Point AP: Node sends to the AP, then AP to the Receiving Node. This duplication of messages effectively halves the speed of the Wireless network.


- On a Home LAN: the Router is
 - A Wireless Access Point for the wireless network
 - A Switch for the wired network
- On a Commercial LAN: there are 1+ Wireless Access Points connected to the wired network. Roaming between APs is only possible with intelligent equipment

Wireless Network Security

Wireless nodes need to be able to specify the Wireless network they want to connect to via the SSID or Network Name

-  Service Set Identifier (SSID) is a locally unique 32 character code that identifies a device on a wireless network. The SSID is inserted into every message.

Nodes usually need to provide a Wireless Key to access the Wireless Network

-  WiFi Protected Access (WPA / WPA2) is a protocol for encrypting data and ensuring security on WiFi Networks.

Wireless Access Point will retain lists of the MAC addresses (of each Node's Network Interface Card)

Improving security:

- Hide the SSID in outward transmissions from the AP (Network Cloaking), users can no longer click on a list of Wireless Network Names to connect and need to be informed of the SSID to connect
- Use WiFi Protected Access (WPA or WPA2) with a strong Wireless Key
- Create a "White List" of MAC addresses: a list of all the MAC addresses that are allowed to connect to the network