Module Three

CSG1105 Applied Communications

The Network Access Layer

- The Network Access Layer (AKA the link or data link layer) provides local delivery of frames if the destination is on the same subnet or if the destination is on a different subnet, forwards frames to a routing device for processing
- It also converts frames to bits for transmission and vice-versa
- If the technology has shared access to the medium (WiFi, Ethernet), a local addressing scheme is necessary as is a mechanism to share access to the medium.
- During a HTTP session, an IP packet may traverse **multiple** subnets, each of which may have a different Network Access Layer Technology
- There are **many** technologies (Ethernet, WiFi, ATM, Frame Relay, MPLS, FDDI)
- In LANs (local area networks), the most common technology is **Ethernet**

Ethernet

- Originally developed in the late 1970's, Ethernet was release as an IEEE standard (802.3) in 1983
- This version, known as 10Base5 (10 Mb/s (megabits per second), baseband signalling, 500 meters) over thick-wire coaxial cable.
- A protocol known as CSMA/CD (Carrier Sense, Multiple Access, Collision Detection) was utilized to share access to the medium
- It used a 48 bit addressing scheme known as MAC (Medium Access Control) addresses
- A later version 10Base2 (200 meters), used cheap RG-58 coaxial cable
- Most coax was eventually replaced with Category 5 UTP (unshielded twisted pair) and 10BaseT was released. This had a maximum cable length of 100 meters

The Ethernet Frame

Destination MAC	Source MAC	802.1q Tag*	Ether Type	Payload	FCS
6 Bytes	6 Bytes	4 Bytes	2 Bytes	46-1500 Bytes	4

*Optional

Figure 1: Ethernet Frame

- The 802.1q Tag field is required for VLANs (to be covered later)
- The Ether Type field used to be the length in 802.3 frames, in Ethernet II frames it identifies the payload type
- The FCS (Frame Check Sequence) is a transmitted checksum that is re-calculated at the receiving station. If the transmitted FCS and the calculated FCS differ, a transmission error has occurred and the frame is discarded.
- The maximum payload length is 1500 bytes. The upper layers must be aware of the Link layers MTU (Maximum Transmission Unit) and fragment messages appropriately

MAC Addresses

- MAC addresses are 48 bits (six bytes) in length and consist of two sections:
  - The OUI (Organisation Unique Identifier) 24 bits
  - A unique sequence number from the OUI owner 24 bits
- Each manufacturer has one or more OUIs assigned to it
- the address are normally expressed as six hexadecimal numbers separated by colons

00:0A:12:43:99:DB

- An all-stations broadcast address is all bits of the MAC set to one FF:FF:FF:FF:FF:FF
- The address is normally in ROM on a NIC (Network Interface Controller), although many contemporary NICs permit the MAC to be altered.
- While useful, this may also be used to perform man in the middle eavesdropping

MAC Processing

- On a broadcast medium (WiFi, non-switched Ethernet), all stations (NICs) receive all transmissions. On switched ethernet, all stations still receive broadcasts.
- The FCS is checked to confirm a valid frame
- The NIC compares the received destination MAC with it's own
  1. If the MAC does not match, the frame is discarded
  2. If the MAC matches, the payload is passed up to the internetwork layer for processing
  3. If the MAC is a broadcast address, the payload is passed up to the internetwork layer for processing

CSMA/CD 1

- Carrier Sense, Multiple Access/Collision Detection
- The original ethernet networks were **half-duplex**, meaning stations could send or receive, but not at the same time (think walkie/talkies)
- These networks used a physical bus topology, with all stations connected to the same cable
- Stations listened while sending; if they saw other than their own message, a collision has occurred
- Each added station reduces the average available bandwidth
- Repeaters (simple amplifiers) were needed to increase transmission distance

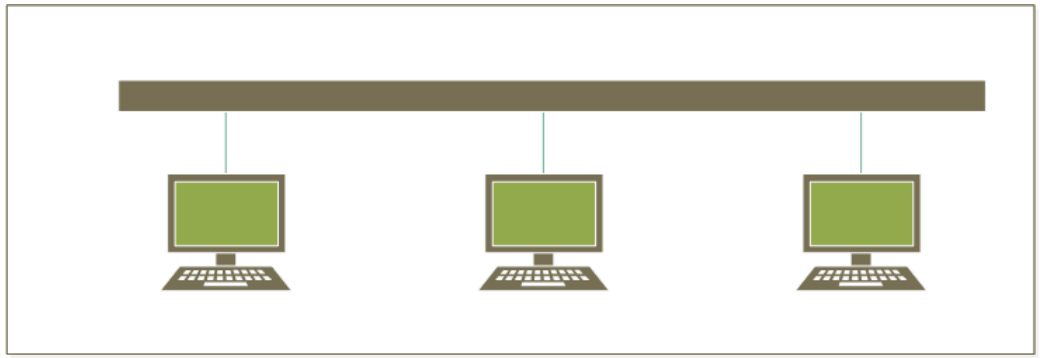


Figure 2: 10Base2

CSMA/CD 2

- Later networks replaced coaxial cables with UTP
- Stations were connected using multi-port repeaters called **hubs**
- A hub took a signal in on one port, and repeated it out all other ports
- There is no interpretation of the contents of the frame, just each bit amplified
- The physical topology was now a star, but the logical topology was still a bus and CSMA/CD was still required
- As the number of workstations grew, bandwidth per station decreased and collisions became more frequent

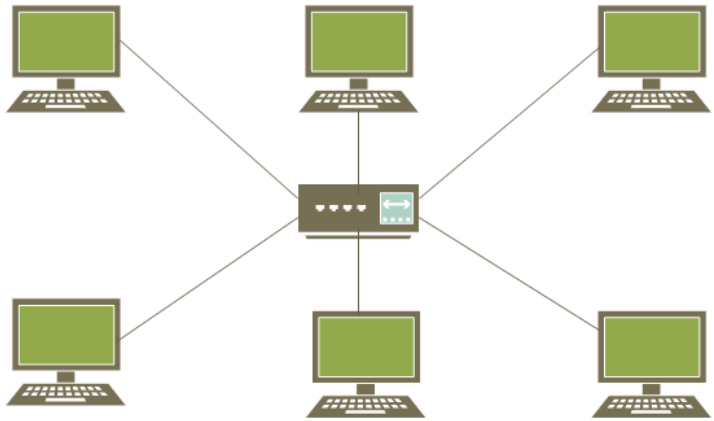


Figure 3: 10BaseT

Bridges 1

- An early solution to busy networks was a device called a **bridge**
- A bridge had two ports, one for each network
- Each time a frame was received on the bridge port, it would add the **source** MAC address to a table associated with that port
- If it saw a subsequent frame with the **destination** MAC address in it's table, it would **not** forward that frame across the bridge
- Unknown MAC addresses and broadcasts were forwarded across the bridge
- This allowed the localisation of ethernet frames
- Collisions are not propagated across bridges

Bridges 2

- This diagram uses abbreviated MAC addresses of two hex characters

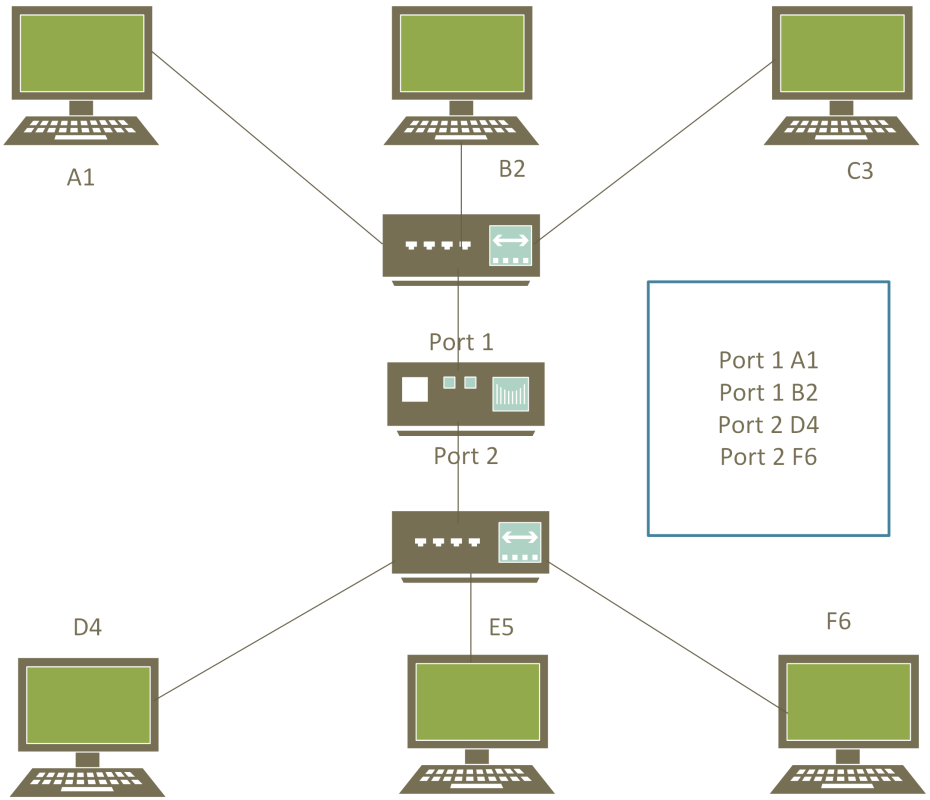
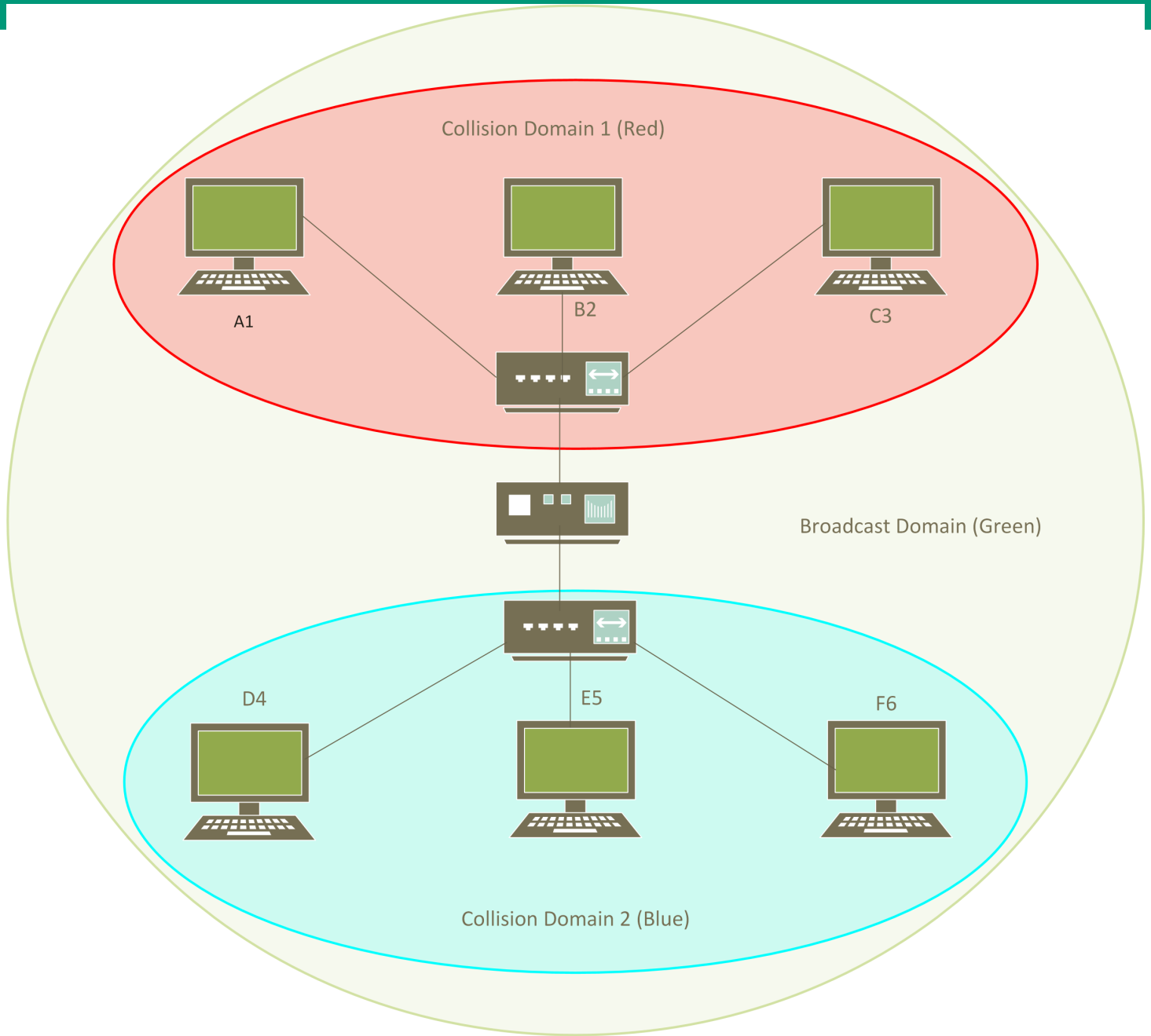


Figure 4: Bridge

Bridges 3

- Previous transmissions have populated the table of each port of the bridge
- If **A1** transmits a frame destined for **B2** the bridge checks the table and does not forward it as it on this side of the bridge
- If **A1** transmits a frame for **F6** as it is not in the table for port 1 so it will be forwarded out port 2
- If **A1** transmits a frame for **C3** it will be forwarded as it is not yet in the bridge table for port 1
- Over time, all active stations have their MAC address recorded in the table and local traffic will remain on each side of the bridge
- Broadcast frames will still traverse the bridge

Collision and Broadcast Domains 1



Collision and Broadcast Domains 2

- A **Collision Domain** exists where CSMA/CD is in operation
- Bridges and later Switches, divide collision domains as they don't propagate collisions
- Broadcasts pass through Bridges (and switches), so all devices connected via either of these devices are members of the same **Broadcast Domain**
- The concept of a Broadcast domain becomes important when we need to start managing the bandwidth on a LAN.

Switches

- In 1990, a company called Kalpana (acquired by CISCO in 1994) introduced a product called an **Etherswitch**
- The initial product, a seven port device, was priced around $US5000
- An **Ethernet Switch** is essentially a **multiport network bridge**
- All ports on the switch share a MAC/CAM (Content Addressable Memory) table that maintains a list of MAC addresses seen as source addresses in frames entering a port
- The MAC table may have multiple MAC addresses associated with a single physical port. This is needed for tiered networks of switches, where a departmental switch connects to a core switch.
- On receiving a frame the switch updates the MAC table and performs one of three actions
  1. If the destination MAC is in the table, forward it to that port only
  2. If the destination MAC is not in the table, flood the frame to all ports, except the ingress port
  3. If the destination MAC is a broadcast MAC (all bits set), flood the frame to all ports, except the ingress port

Switches - MAC Table

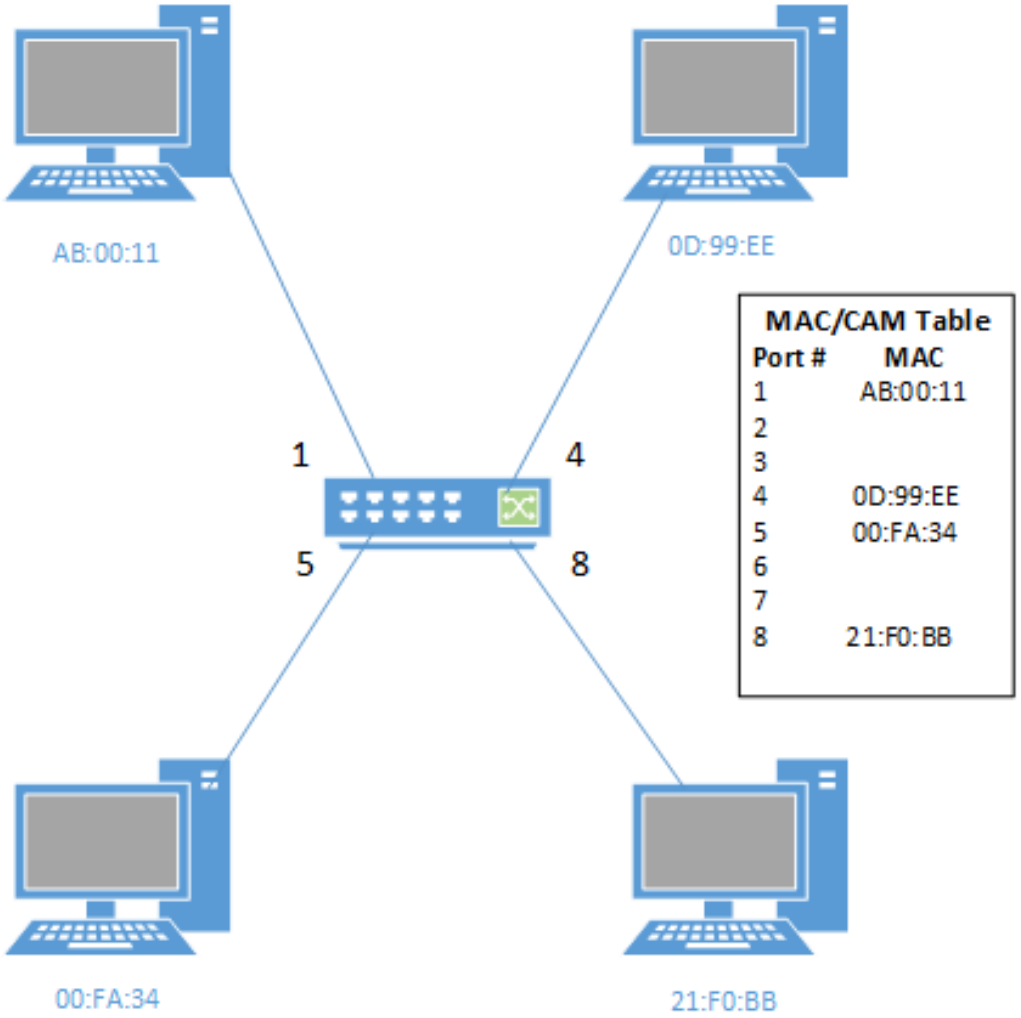
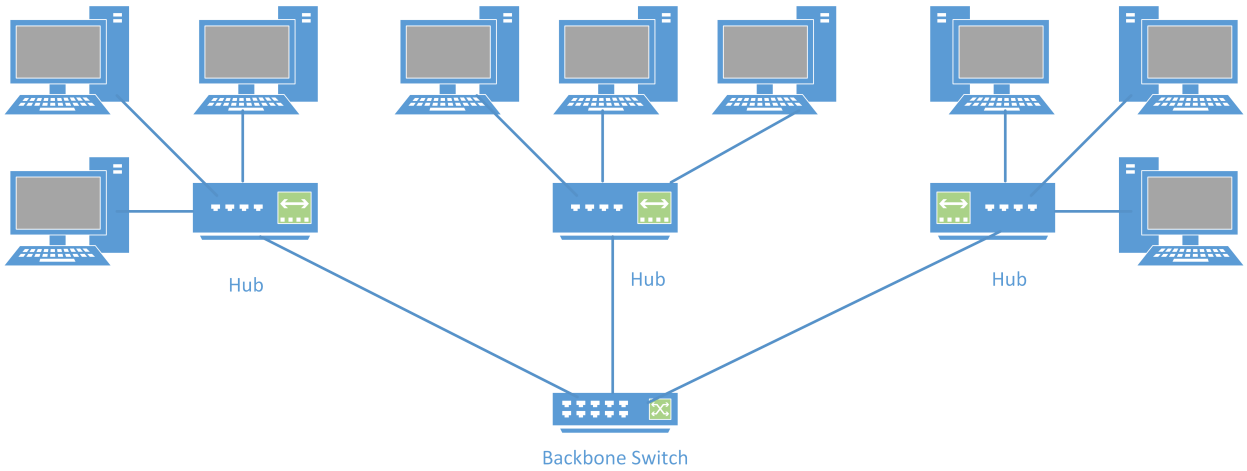


Figure 6: MAC/CAM Table

Switches -

- The initial expense of switches limited their use to Backbones of



networks

- Development over time reduced the cost of switches to eliminate the need for hubs as a network device.
- All devices are linked using switched ports, reducing the size of a collision domain is reduced to a single port
- Connections are **Full Duplex** permitting simultaneous transmission and reception of data on the same port.
- Each port on a switch may operate independently of all others, allowing multiple devices to communicate simultaneously

Switches 4

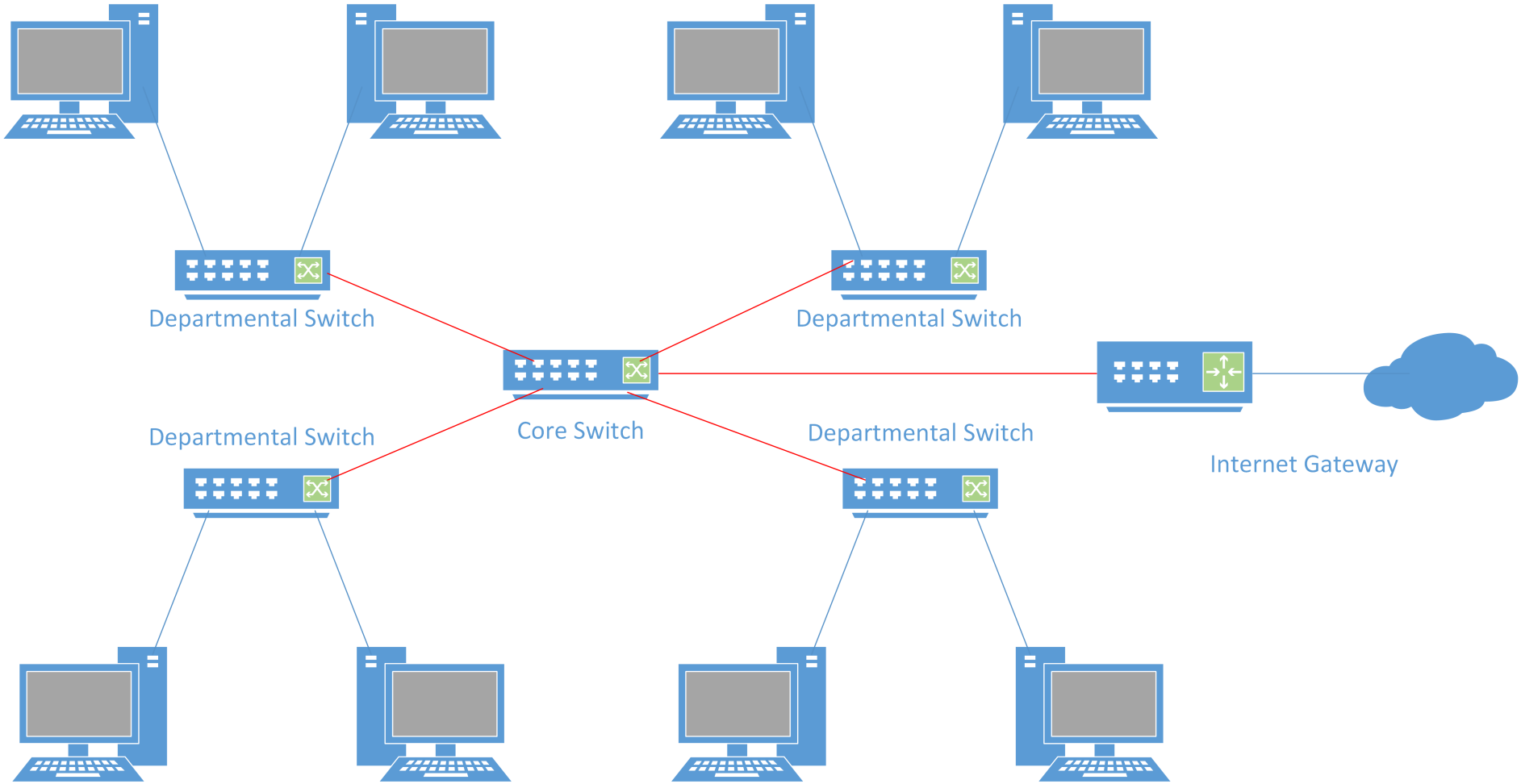


Figure 7: Fully Switched LAN

Switches 5

- Consumer grade switches are **unmanaged** switches
- Unmanaged switches
  - don't require any configuration
  - have MAC tables are built automatically from received frames after the device is powered on.
  - have contents of the MAC tables lost when the switch is powered down
  - don't have remote management of the switch
  - may not implement the STP (Spanning Tree Protocol)
  - are generally inexpensive

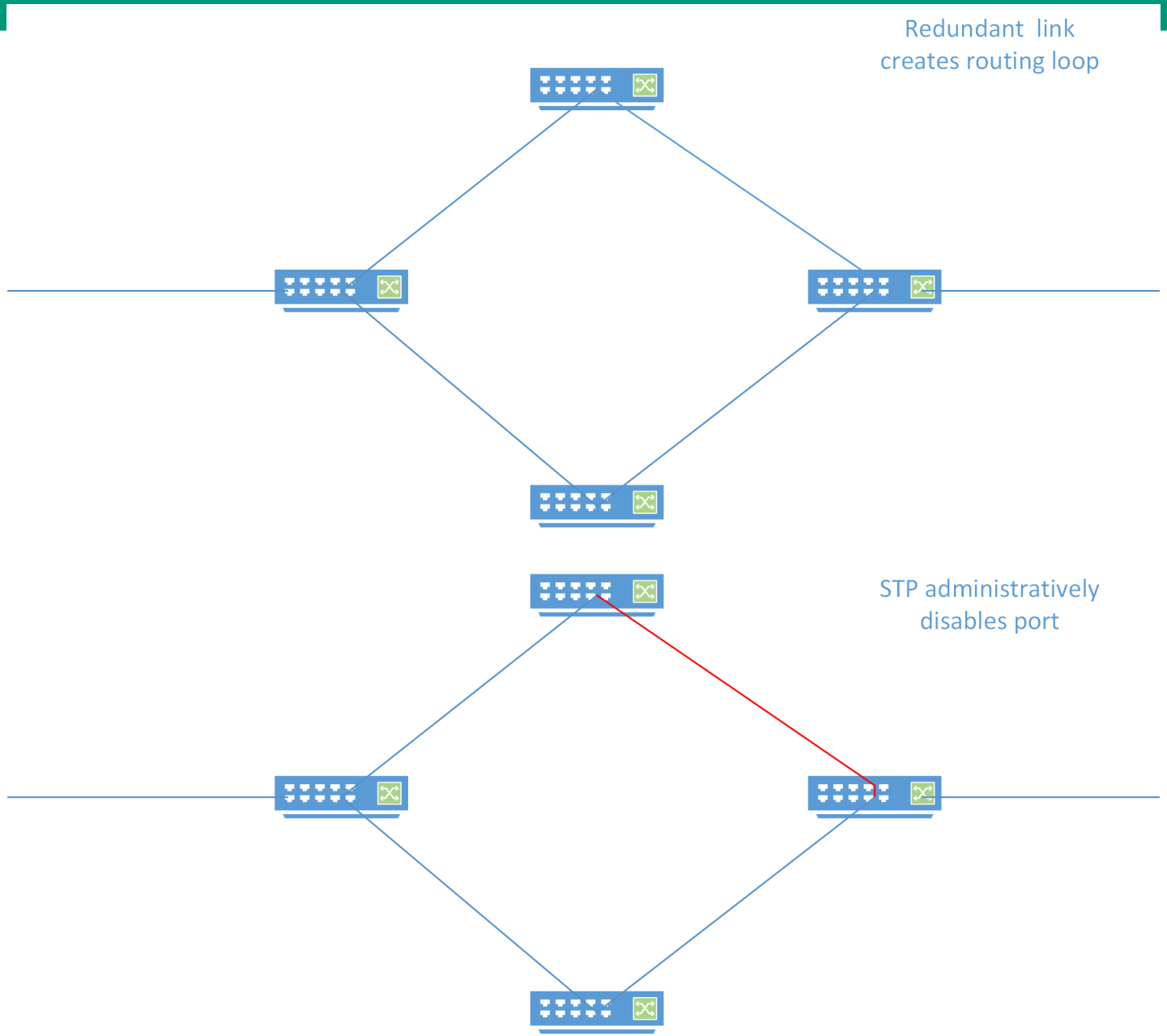
Managed Switches

- **Managed switches:**
  - require a skilled administrator to configure the device
  - have MAC tables are built automatically from received frames after the device is powered on.
  - permit the administrator to manually add entries to the MAC table
  -
  - are commercial grade devices that have the capacity to be centrally managed
  - have features to manage traffic on a per-port basis
  - provide processing of 802.1q tags to implement VLANs (covered later)
  - implement STP
  - provide a command interface for local or remote configuration
  - maintain their configuration (but not the dynamic MAC table entries) when powered down
  - are much more expensive than unmanaged switches

Spanning Tree Protocol (STP)

- Bridges and switches may be physically configured to provide redundant links
- This allows network to continue to function if a link fails
- The problem is that it may create "routing loops" where MAC tables will forward frames endlessly
- Bridges and switches exchange information that identifies potential loops
- STP will administratively disable a link to prevent a loop
- If primary link becomes unavailable, STP will re-enable the redundant link

STP


Redundant link
creates routing loop
STP administratively
disables port

Media conversion

- Ethernet may run over several different media types (COAX,UTP,Fibre)
- COAX is generally now obsolete
- For a period, some devices supported both COAX and UTP
- This was possible because the frame format was identical
- Some current switches support UTP and Fibre
- Fibre is often used to link departmental switches to core switches because
  1. It supports higher bandwidth(speed)
  2. It can span longer distances
  3. It is less effected by interference

Transmission Speeds

- The original Ethernet transmission speed was 10Mb/s
- In the mid 1990's 100Mb/s on both UTP and Fibre was introduced (100BaseT2,100BaseTX)
- Late 1990's introduced Gigabit Ethernet (1000BaseT and 1000BaseX)
- Higher grades of UTP (Cat 6) are recommended for higher speeds
- There are 10Gb and higher speeds available, mostly for data centre use. Some of the higher speeds run on fibre only
- Equipment supporting the higher speeds is generally considerably more expensive

MAC meets IP!

- We've seen that a MAC address is used to deliver a **frame** to the intended host
- MAC addresses only have **local LAN** significance
- End to end delivery requires an IP address
- Enter ARP - Address Resolution Protocol
- ARP is used to discover the MAC address of an IP

Address Resolution Protocol

- How do you find the MAC address of an IP?
- The station requiring the MAC address sends a broadcast asking "Who has 192.168.0.3?"
- The broadcast frame will include the IP and MAC of the sending station
- All stations in the **broadcast domain** will receive the request frame
- The station that has the address 192.168.0.3 will reply to the MAC of the sending station with its MAC address

ARP cache

- Sending an ARP every time we want to establish a connection will cause considerable broadcast traffic
- To counter this issue, devices connected to LANs generally maintain an **ARP cache**
- This is a simple table containing IP/MAC pairs that the Internetwork layer checks before sending an ARP request
- The table is built from received ARP responses
- Powering down a station generally clears the ARP cache

```
Interface: 192.168.0.3 --- 0x13
  Internet Address      Physical Address      Type
  192.168.0.1           bc-30-d9-e7-e2-8b     dynamic
  192.168.0.2           08-3e-5d-06-b8-c7     dynamic
  192.168.0.4           58-cb-52-48-57-08     dynamic
  192.168.0.5           30-05-5c-b6-26-82     dynamic
  192.168.0.6           24-5e-be-11-44-94     dynamic
```

Figure 9: ARP Cache