LAN Switching & Wireless

CONFIGURE A SWITCH

Mark Cummins – Institute of Technology Blanchardstown

Objectives

- Summarize the operation of Ethernet as defined for 100/1000 Mbps LANs in the IEEE 802.3 standard.
- Explain the functions that enable a switch to forward Ethernet frames in a LAN.
- Configure a switch for operation in a network designed to support voice, video, and data transmissions.
- Configure basic security on a switch that will operate in a network designed to support voice, video, and data transmissions.

Ethernet Operation

- You should understand how CSMS/CD works.
  - Listening before transmit mode
  - Collision detection
  - Jamming signal
  - Backoff Algorithm

- CSMA/CD only operates in half duplex environment.

Half Duplex and Full Duplex

- Half Duplex:
  - data sent in only one direction at a time, either sending or receiving.
  - Typically uses CSMA/CD because collisions occur.
  - Hubs operate using half duplex.

- Full Duplex:
  - Data sent in both directions at same time.
  - No collisions occur.
  - Switches prefer to operate in full duplex mode.

Switchport Settings

- Cisco switches support three modes of operation:
  - **Auto:** Sets auto negotiation of duplex mode.
  - **Full:** Sets full duplex mode.
  - **Half:** Sets half duplex mode.
- Auto negotiation can cause unpredictable results.
- Ensure same mode at either end to avoid errors.
- Can also use **auto-MDIX** feature on newer switches (enables auto sensing of cable types)

LAN Design

- Proper LAN design uses segmentation to reduce LAN performance problems such as:
  - Collisions
  - Latency
  - Congestion

- Smaller collision domains and broadcast domains = better network performance.

- Switches introduce less latency than routers are the main device used to create smaller collision domains.

LAN Design

- Routers and VLANs can help reduce size of broadcast domains.
- You should understand broadcast and collision domains.

Switch Forwarding

- Switches use MAC addresses to direct Frames.
- Source MAC address of incoming frame is added to MAC address table (or CAM table).
- Destination MAC address of incoming frame compared to CAM table to decide which port to forward frame out.
- Addresses not found in CAM table are forwarded out all other ports (switch acts like a hub).

Switch Forwarding Methods

- Switches use one of two methods for switching data.
  - Store-and-forward:
    - Only method currently used by Cisco switches
    - Complete frame is stored in buffer
    - Performs error checking on CRC
    - Frames with errors are dropped
    - Traffic prioritisation (Converged networks)
    - Quality of service (Converged networks)

Switch Forwarding Methods

Cut-through: (Two variations)

- Fast-forward switching:
  - Fastest forwarding method
  - Reads just the destination before forwarding
  - No error checking, corrupt frames forwarded

- Fragment-free switching:
  - First 64 bytes stored
  - Partial error check
  - Compromise between previous two methods

Symmetric and Asymmetric Switching

LAN switching can be classified as:

- Symmetric:
  - All ports use the same bandwidth.
- Asymmetric:
  - Ports can be different bandwidths.
  - Applies to most Cisco switches.
  - Memory buffering is required.

Memory Buffering

There are two methods of memory buffering:

- Port-based:
  - Frames stored in queues based on incoming port.
  - Frame only sent if all frames before it have been transmitted.
- Shared memory:
  - All frames stored in common memory area
  - Less frames trapped behind a large frame

Layer 2 and Layer 3 switching

- Switches can be layer 2 or layer 3 switches.
- Layer 3 switches can perform layer 3 tasks like IP filtering and access control.
- Layer 3 switches can remove the need for a router in the LAN.
- There are some tasks that layer 3 switches cannot do, for which a router is still required.
- Layer 3 devices, higher latency than layer 2 devices

Switch Management Configuration

You should be familiar with all the basic CLI commands:

- User & Privileged (enable) mode
- Command syntax help
- Passwords
- Hostnames
- Descriptions
- Boot sequence and file locations

All of these are similar for both switches and routers

Management Interface

To manage a switch remotely using TCP/IP you need to set up the management interface on the switch.

To set up the management interface, you need to:

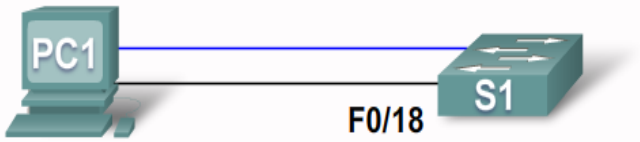
- Create a management VLAN
- Assign management VLAN to a port
- Set the IP address

Other options that you should also set include:

- Default Gateway address
- Duplex and speed of interfaces
- HTTP access

Management Interface

Configure IP Connectivity



PC1:

- IP address - 172.17.99.12
- Connected to Console port
- Connected to port F0/18 on S1

S1:

- VLAN 99
- the management VLAN
- IP address -172.17.99.11
- Port F0/18 assigned to VLAN 99

- For TCP/IP management a Layer 3 address must be assigned to the switch.
- VLAN 1 is the default management interface for all switches
- There are security risks associated with using VLAN 1
- Create another VLAN, for example VLAN 99 or VLAN 150
- Assign that VLAN to an appropriate port, for example F0/18

Management Interface

All of the basic commands covering how to set up the management interface and managing the switch will be covered in the labs and are not covered by these notes

Configuring Switch Security

Telnet is the original remote terminal access program

- All messages are sent in plain text
- It is the default vty supported protocol on Cisco
- Default access is unsecured
- Set vty password to set telnet password

itb

Configuring Switch Security

SSH is a secure alternative to telnet

- All messages are encrypted
- SSHv1 and SSHv2 are supported (use v2 where possible)
- Need to generate RSA keys