Switch Configuration

- **Virtual LANs**
- **Configuring Switches**
- **Spanning-Tree Protocol**
- ***Network Management*** (*see textbook*)
- ***Power over Ethernet*** (*see textbook*)

Virtual LANs

- Recall our discussion of **physical** versus **logical** entities:
  - "Physical" tends to indicate the *actual or literal* entity
  - "Logical" refers to something more *abstract*. It can...
    - Stand in for
    - Emulate
    - Serve as a proxy for
  - ...its physical counterpart. In the case of emulating, we might call such a thing virtual.

Virtual LANs

- A **virtual LAN (VLAN)** is a group of networked hosts (e.g., servers and computers) that are
  - Configured ***as if*** they were on a LAN …
  - …even though they may be separated by routers, in actuality.
- This is useful because the network administrator can group the hosts based on factors other than physical location, such as the department within an organization.
- There are three main types of VLANs…

Virtual LANs

- **Port-based** :
  - Here, a specific VLAN is associated with a particular set of ports on a switch.
  - For example, if a single switch were to have 16 ports, you might have...
    - VLAN 1: Ports 1-4
    - VLAN 2: Ports 5-10
    - VLAN 3: Ports 11-13
  - While switches normally form a single broadcast domain, these VLANs would in fact belong to separate domains.

Virtual LANs

- **Tagged-based** :
  - This uses Ethernet frames, along with the IEEE 802.1Q standard
  - Here, the Ethernet frame will include a VLAN id
  - This way, you could actually have more than one VLAN on a switch port
- **Protocol-based** :
  - Data traffic connects on different ports based on protocol
  - Separates data traffic for different networks

Virtual LANs

- Assignment of VLAN membership can be of two types:
  - **Static assignment** : Port-based. Membership happens at time of port assignment to a VLAN.
  - **Dynamic assignment** :
    - Port assignment is based on other factors, like MAC address or username.
    - This way, location can change, while maintaining VLAN membership.

Configuring Switches

- With regards to using a switch in GNS3, much will be similar.
- Many of the modes and commands you used to interact with your Cisco router will also apply to your Cisco switch -- though there will also be some differences because the switch is a different type of device.
- Most notably, you will be configuring a VLAN, which will have an IP address.
  - On a router, the IP address exists so that it can serve as a gateway for the LAN

Configuring Switches

- On a switch, the VLAN IP address is so that the switch can communicate with other VLAN devices.
  - This is useful if you need to remotely connect to the switch to manage it.
  - The switch is still functioning at *Layer 2*. It is **not** performing any routing.
- Some command examples will follow, with two caveats:
  - What we are describing here is in the context of *GNS3* and our labs in this class. However, much will still be relevant in *real-life* situations dealing with physical networks and hardware.
  - In GNS3, we are ***not*** using a proper managed switch. Instead, we are using an **`EtherSwitch router`** that is configured to *behave* like one.
  - As such, *some* of the commands that you use will be different than what is presented in the textbook.

Configuring Switches

- In *configuration mode*, "VLAN" is like a type of interface that you can configure.

```
ESW1(config)#interface VLAN 1
```

- In *interface configuration mode*, you will use similar commands as you used on a router

```
ESW1(config-if)#ip address 192.168.2x.10 255.255.255.0
ESW1(config-if)#no shutdown
```

- Your switch will also need a *default gateway*, which will be your router's local NIC:

```
ESW1(config)#ip default-gateway 192.168.2x.1
```

Configuring Switches

- Finally, you will also be able to view configuration information for VLAN 1:

```
ESW1#show interface VLAN 1
```

- In *Homework #10*, you will start by configuring the first VLAN, which will be the default for administrative purposes.
- At first, all Ethernet ports will be associated with that one. You can verify this by running the command **`show vlan`** (On your EtherSwitch router in GNS3: **`show vlan-switch`**)
- Moving forward, *you can establish other VLANs*.

Configuring Switches

- On your EtherSwitch router in GNS3...
  - you would enter the correct mode with the command **`vlan database`**, which gives you the prompt **`ESW1(vlan)#`**
  - There, you can create new VLANs, specified by number and name: **`vlan`** `[number]` **`name`** `[VLAN's name]`. For example:

    ```
    vlan 2 name Sales

    vlan 3 name Engineering
    ```

  - (*Contrast* this to the textbook example.)
- You can associate different Ethernet ports with one VLAN or another...

Configuring Switches

- To do this:
  - Enter *configuration mode*.
  - Enter *interface configuration mode*, for the port in question.
  - Enter the command **`switchport mode access`**
  - Enter the command
  - **`switchport access vlan`** `[number]`
  - The **`end`** command

Configuring Switches

- Example:

```
ESW1#configure terminal
ESW1(config)#int fa 1/1
ESW1(config-if)#switchport mode access
ESW1(config-if)#switchport access vlan 3
ESW1(config-if)#end
```

- You can run **show vlan** (On your EtherSwitch router in GNS3: **show vlan-switch**) in order to see the updated state of Ethernet ports with respect to VLANs.

Spanning-Tree Protocol

- In many cases, it is good to have some level of ***redundancy*** in your network setup. For example…
  - A host device may have **both** an Ethernet card **and** a wireless card, enabling it to gain network access in a wider variety of environments.
  - A wireless access point might function on both the **2.4 GHz** and **5 GHz** bands, allowing more connection options.
  - If there are *multiple* Layer 3 routes between two endpoints, then one route can be used in the event that the default route fails.

Spanning-Tree Protocol

- As such, you might have Layer 2 redundancy in a LAN.
  - That is, there might be *more than one* Layer 2 path between two devices, on account of *multiple* switches being interconnected. We might say that *the switches themselves* are in a "mesh" topology.
  - On *one* hand, this can be beneficial for maintaining network connectivity, in the event that one switch fails.
  - On the *other* hand, if not properly managed, you can end up with a **switching loop**.
  - Example: **https://www.youtube.com/watch?v=P04gaoq53FU** (0:10 - 3:10)

Spanning-Tree Protocol

- A **switching loop** occurs when a data packet, that has passed out of a switch, ends up passing back into it.
  - This can happen in scenarios where the switch does not have one unique destination for a packet -- such as *broadcasting* or *flooding*.
  - It begins when the switch receives a data packet on a port....
  - For whatever reason -- such as a broadcast packet or an unknown destination MAC address -- the switch forwards (i.e., *floods*) the packet to all ports (except for the entry port).
  - Other switches, on receiving the packet, do the same.
  - Because of *path redundancy*, the packet ends up coming back.

Spanning-Tree Protocol

- Two main types of problems can arise:
  1. ***Broadcast storms*:**
     - A **broadcast packet** is addressed to `ff:ff:ff:ff:ff:ff`
     - If a switch receives one, then it transmits that packet to *every* other port currently in use.
     - In other words, one packet in = ***Multiple*** packets out!
     - If one of those packets happens to arrive again, then it is once again broadcast out
     - This *exponential* proliferation of packets can quickly overtake the network's capacity

Spanning-Tree Protocol

2. ***MAC flapping*:**
   - When a host sends a packet into a switch, the *source MAC* is examined to establish an *association* (between the host and the port) in the switching table.
   - If the switch does not have the *destination MAC* in its table, then it ***floods*** to all other ports, except the source port.
   - If the same packet enters *another* port -- on the same switch -- via a loop, then the source MAC can become associated with that other port.
   - This creates *instability* in the Layer 2 links.

Spanning-Tree Protocol

- On *managed* switches, we can use **Spanning Tree Protocol** (STP) to prevent loops and keep data flowing along the right paths.
- To understand the notion of a "spanning tree", consider a collection of interconnected nodes.
  - Between any two nodes, there are multiple paths.
  - You can eliminate (or "disable") some of those connections, such that, between any two nodes, there is only one possible path because redundant paths have been removed.
  - If you make one node the "root", then you can think of it as a tree

Spanning-Tree Protocol

- When you have *multiple switches with redundant paths*, the purpose of STP is to prevent looping by:
  - Making one of those switches the **root**
  - For any other switch, allowing **only one port** to lead to the root
- Switches accomplish this by exchanging **Bridge Protocol Data Units (BPDUs)** in order to:
  - Choose a **root** switch
  - For other switches:
    - Determine the *shortest* path to root
    - Choose the switch port providing that best path
    - Decide which switch ports participate in STP

Spanning-Tree Protocol

- In addition, there are also packets for *communicating topology changes* and *acknowledging* those notifications.
- There are *five* STP states:
  - **Blocking** : Not sending data but still keeping track of BPDUs
  - **Listening** : Processing BPDUs
  - **Learning** : Using packets to learn MAC addresses
  - **Forwarding** : Switch is currently sending and receiving
  - **Disabled** : Not actually part of STP, but the network administrator can choose to disable a port