Lecture 9: Switched Ethernet Features: STP and VLANs

Prof. Mohammed Hawa
Electrical Engineering Department
University of Jordan

Ethernet Switch Features

- The following features in modern Ethernet switches are quite useful to the network administrator:

1. Self-learning (backwards-learning)
2. Spanning Tree Protocol (STP)
   – IEEE 802.1D
3. Virtual LAN (VLAN)
   – IEEE 802.1Q

Ethernet Switch is Transparent

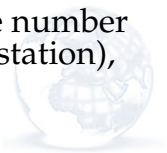
- Switches were designed to mimic hubs, so they are transparent to the Ethernet machines attached to them.
- In other words, a switch acts like a shared medium, but without the possibility of collisions.
- When a frame arrives at one port of a switch, the switch forwards that frame to *all* ports *except* the one that the frame arrived on.
- This behavior is known as flooding. It makes the switch look like a shared medium.

Ethernet Switch is Transparent

- *Remember*: Ports on the switch do NOT have MAC addresses (nor IP addresses). A switch is not like a router. Each interface on a router has its own MAC address and IP address (see *later*).
- An exception is if the switch has a controller inside it to allow the administrator to control the switch.
- In such case, only the controller (which shows a Web page sometimes) has a MAC address, not the switch ports themselves.

Advanced Switch: Forwarding

- *Flooding* makes sure that each frame is seen by *all* machines on the Ethernet LAN, but wastes resources since most communications are unicast (intended to one destination).
- *Forwarding* was introduced in newer switches. The switch forwards the frame to only one port where the destination machine is connected (not to all ports).
- The switch (Layer 2 device) can read the unicast destination address (DA) in the frame and decide where to send the frame based on this DA.
- Forwarding (rather than flooding) reduces the number of frames processed by each switch port (and station), and enhances privacy.



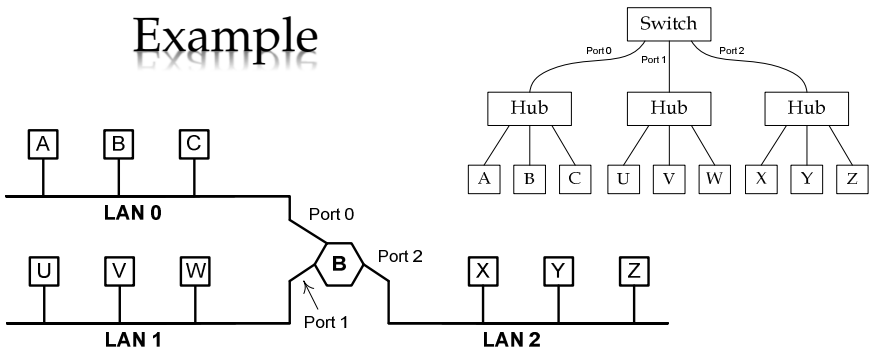
Self-Learning (or Backward-Learning) Switches

- Problem: How can the switch know the MAC address (global or local) of each machine the administrator connects to its ports?
- Table lookup of MAC addresses connected to each of the switch ports.
- Configuring an Ethernet switch with a static table by the administrator is:
  - Time consuming.
  - Error prone.
  - Moving a station from one LAN to another LAN requires maintenance of the tables.

Self-Learning Algorithm

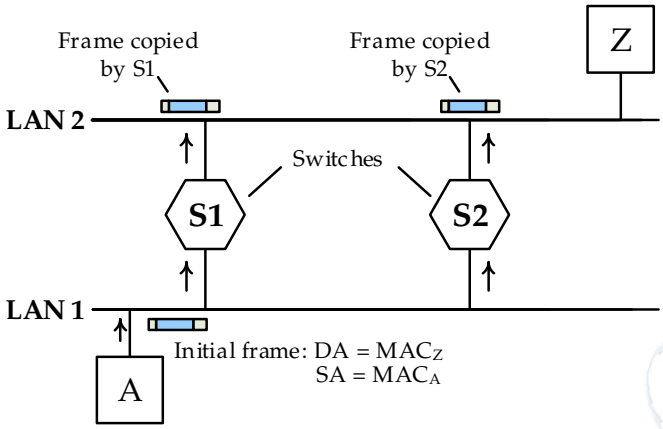
- When the switch boots, its self-learning hash table is *empty*.
- When the switch receives a frame to forward, the switch inspects the DA and SA of the frame:
  - DA: If the switch knows the port belonging to the DA the switch forwards *only* to that port; otherwise the switch *floods* (i.e., forwards to all ports *except* the one that the frame arrived on).
  - SA: The hash table is updated by the SA information.
- Hash tables are treated as cache entries:
  - *New* information overrides *old* information
  - Each entry is assigned a timeout, after which it is erased.

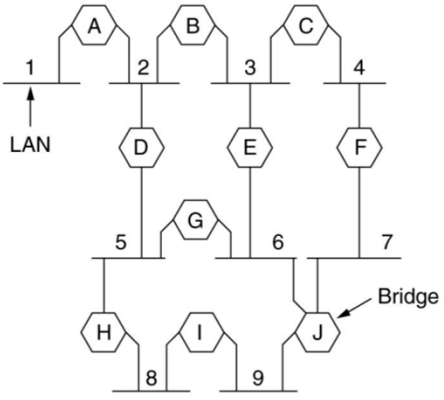
Example

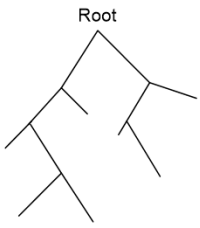


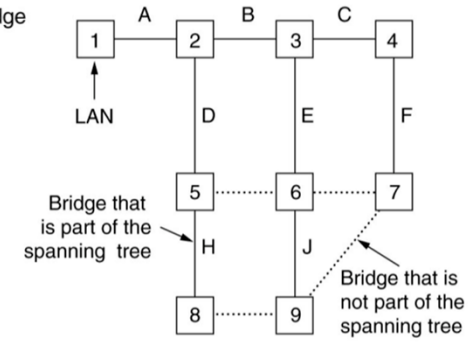
Event	Port 0 List	Port 1 List	Port 2 List	Bridge Action
Bridge boots	-	-	-	Empty Tables
U sends to V	-	U	-	Flood (to Ports 0 and 2)
V sends to U	-	U, V	-	Discard
Z broadcasts	-	U, V	Z	Flood (to Ports 0 and 1)
Y sends to V	-	U, V	Z, Y	Forward to Port 1
Y sends to X	-	U, V	Z, Y	Flood (to Ports 0 and 1)
X sends to W	-	U, V	Z, Y, X	Flood (to Ports 0 and 1)
W sends to Z	-	U, V, W	Z, Y, X	Forward to Port 2

Spanning Tree Protocol (STP) – Avoids Loops









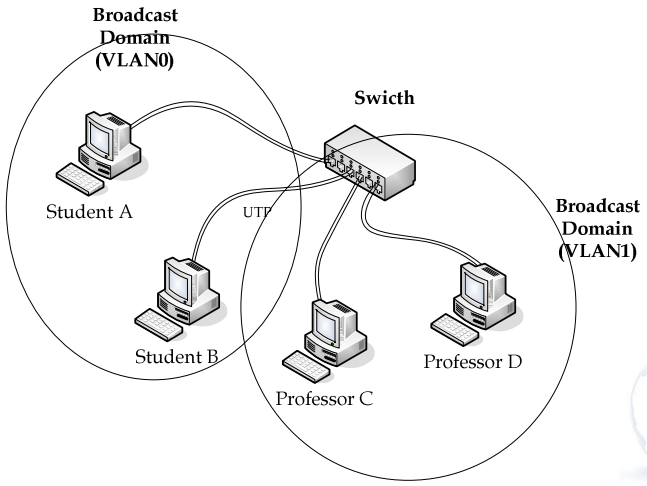
Rapid Spanning Tree Protocol

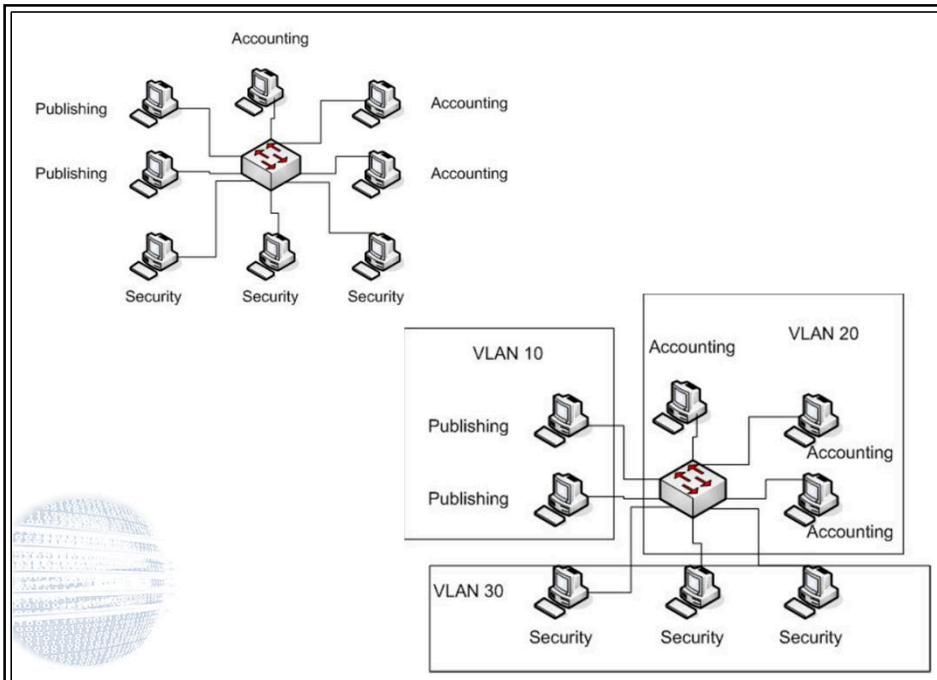
- IEEE introduced RSTP (Rapid Spanning Tree Protocol) in 2001 as IEEE 802.1w.
- RSTP is now part of IEEE 802.1D-2004.
- Original STP is now obsolete, but RSTP is backward-compatible with standard STP.
- RSTP provides faster spanning tree convergence after a topology change (within 3 HELLO times, default: 3 × 2 seconds) or within few milliseconds of physical link failure.
- STP can take 30 to 50 seconds to respond to a topology change.

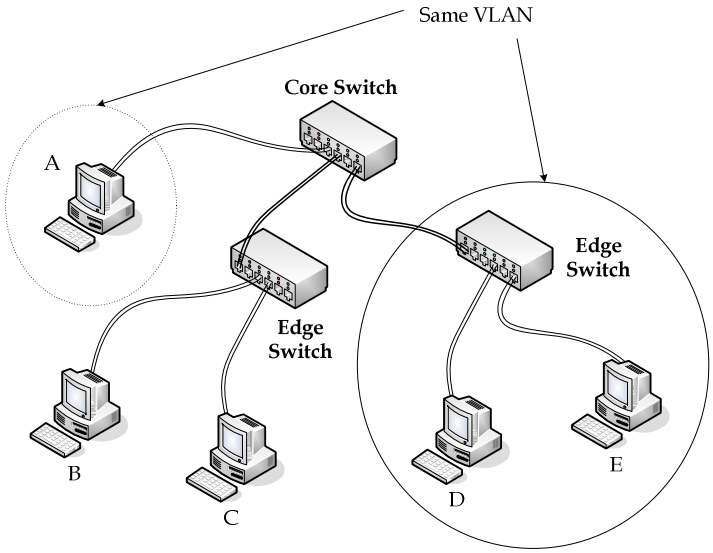
Virtual LANs (VLANs)

- All hosts connected to an Ethernet LAN (consisting of one or more switches) are in the same **broadcast domain**. If one host connected to the LAN sends a broadcast, all of the other hosts receive the broadcast, wasting bandwidth.
- For some protocols, a broadcast received by a host results in that same host transmitting a broadcast of its own. Then when all the hosts receive the first broadcast, they all end up transmitting even more broadcasts. All these broadcasts snowball into a **broadcast storm**.
- Typically few hosts on each LAN really need to broadcast to each other. VLANs *isolate broadcast domains* by splitting an Ethernet switch into multiple virtual switches.
- This reduces overall traffic, avoids broadcast storms, improves security by isolating traffic, and improves privacy.
- All is done by software.

Virtual LANs (VLANs)







VLAN: Administrator Power

- Most switches require assigning a number to a VLAN when it is created, such as VLAN 10, VLAN 20, etc.
- No traffic is able to go from one VLAN to another. By default, there will be no inter-VLAN traffic on the switch, unless a router (Layer 3 device) is involved (probably along with a firewall for security).
- When using VLANs, Ethernet frames contain the optional IEEE 802.1Q tag to identify to which VLAN it belongs.
- Common approaches to assigning VLAN membership:
- **Static VLANs** (port-based VLANs): assigns ports on a switch to a VLAN. The device automatically assumes the VLAN of the port.
- **Dynamic VLANs**: created through a software package (VLAN Management Policy Server), where an administrator assigns VLANs dynamically based on information such as the source MAC address of the device connected to the port or the username used to log onto that device, etc.

