VLANs and Port Security

Gary Lee
Nelson Lee
Kelly Lum
CS 996
10/23/2003
Switched Networked

- Classical logical network topology
  - Switches and hubs connect to end-nodes
  - Routers connect switched, providing backbone

- Separates multicast and collision domain into two segments
  - But routers add latency! Noticeable as networks become larger
Adding Latency

- **Switches are Layer 2 network devices**
  - Forward information based on layer 2, MAC addresses
- **Routers are Layer 3 network devices**
  - Forward information based on layer 3, IP addresses
- **Switches can better allocate bandwidth**
  - Unlike hubs, they do not broadcast traffic to all ports, but keeps track of which computer is connected to which port
Classical Corporate Network
Classical Corporate Network Limitations

- End-nodes are connected to switches
  - Large number of switches connected to routers
  - Routers need to route large amount of packets
- End-nodes need to be physically connected to switches
  - End-nodes need to be 100m or closer to switch
- Cannot further segment switches to limit broadcast or collision domains
  - If you have research lab and public relations on same switch
- You cannot spread a department’s computers over a wide area, such as a scientific research computer laboratory across campus!!
Ideal Switched Network

- Switches are interconnected by a circuit-switched ATM backbone
- But now there is one huge collision domain!!
What is a Virtual LAN?

- A physically switched network that is logically segmented
  - A new set of broadcast domain are created within the switches
- Allows machines on physically different LAN segments to behave as if they were part of the same segment
Sample LAN

- There is a three-story building that is furnished with three computers per floor
- The three departments are oddly partitioned such that one computer from each floor constitutes 1/3 of the department
- We now have to move computers from each floor to its proper location so we can use hubs
- A very tedious and ridiculous job for network admin! (Let an intern do it…)
Sample LAN into a VLAN

- By using switches, we can assign computer on different floors to VLAN1, VLAN2, and VLAN3
- Now, logically, a department is spread across 3 floors even though they are physically located on different floors
Ideal Network Revisited
Why use VLANs?

- Provides limited amount of assurance that only computers part of the VLAN can communicate on it
  - (Higher assurance can be obtained by following Cisco’s Best Practices implementation)
- Improves general network performance by not slowing down other users sharing the network
  - Limits recipients of broadcast traffic
  - Less congestion
- Allows easier network management
VLAN Tagging

- To establish a packet’s association with a particular VLAN, a tag is added.
- **802.1q** – Specifies appending 32-bit VLAN tag (field) into Ethernet Frame after Ethernet header
  - 12 bits are assigned to VLAN ID
- **Usual Scenario**
  - Packet enters switch from source host
  - Tag appended while in switch fabric (even if there is no trunking)
  - Gets routed to specific port
  - Tag is stripped off
  - Original packet passed to destination host
How do packets move in a VLAN?

- Three basic models for controlling how a packet get routed inside a VLAN switch
  - **Port based**
    - Network administrator assigns a port on a switch to a VLAN ID
    - Need to manually enter it into the switch, so if a computer moves, then you have to manually update the changes
    - If a repeater is attached to a port, all of the users on the repeater must be on the same VLAN
  - **MAC Address based**
    - Switch maintains a table of addresses and their corresponding VLAN memberships
    - Easy to keep track of computers that moved
    - Can be, but not easily, part of multiple VLANs
How do packets move in a VLAN?

- Layer 3 based
  - Membership is based on protocols and Layer 3 addresses
  - Ex.: an IP subnet can be a VLAN or an IPX network
  - Can use non-routable protocols like NetBIOS instead of IP or IPX
How is VLAN membership indicated?

- Tagging packets internally and between trunks
  - Tag is appended when packet arrives at switch
  - Tag is stripped when packet reaches destination on same switch

- On a trunk: implicit and explicit
  - Implicit - membership indicated by MAC address
    - All switches supporting a VLAN must share a table of addresses
  - Explicit – tag added to the packet to indicate VLAN membership
    - Used by Cisco ISL and 802.1Q
VTP – VLAN Trunking Protocol

- ISL – Pre-802.1q: Cisco proprietary Inter-switch Link protocol
- VTP – Management protocol that spans the trunks lines (ISL, 802.1q port, LANE, etc)
  - Creates a new domain of switches for VLAN management
  - Make one change, let VTP worry about propagating settings across inter-connected switches
Port Security

- Enables blocking of unauthorized MAC addresses access to ports
- Switches can then monitor the security of those ports
- Alerts may be sent to a network manager where appropriate action should be taken
Port Security for Cisco Catalyst

- Blocks input into a port if the MAC address is different from the set of MAC addresses assigned to the port
- Allows a maximum of 1024 MAC addresses plus one default MAC address for each port
- Manual or Automatic configuration
- Configuration stored in non-volatile RAM
Port Security for Cisco Catalyst (continued)

- Able to set an age time during which the port is secure. After the time has expired, the port becomes insecure. (WHY?)
- Default setting: Ports are secured permanently
- An attempting MAC address that is different from the secure MAC addresses on the port constitutes as a security violation
- After a security violation, ports are defaulted to shutdown permanently
- Port security not supported for trunk ports
Port Security for Cisco Catalyst (continued)

Actions taken by the port:

- Shut down permanently
- Shut down for a period of time
  (If shut down, an link-down trap is sent to SNMP)
- Enabled, but drops packets from insecure hosts
Port Security for HP Procurve 4000M

- For any port, one or both of the following can be configured
  - Authorized Addresses – specify up to 8 MAC addresses allowed for inbound traffic
    - Closes the port to any unauthorized device
  - Prevent Eavesdropping – blocks outbound traffic to unknown destination addresses

- When a security violation is detected
  - An alert flag is set for that port
  - Sends an SNMP trap to network management system
Port Security for HP Procurve 4000M

- Port Security is defaulted to off.
- Configuration parameters
  - Port – port to enable port security
  - Learn mode
    - Continuous (default) – port learns about MAC addresses from inbound traffic, and addresses are Aged out.
    - Static – Manually enter up to 8 MAC addresses
  - Address Limit – the number of addresses to allow
    - 1 is default, 8 is the maximum
Port Security for HP Procurve 4000M

- **Eavesdrop Prevention**
  - Disabled (default) – allows all outbound traffic
  - Enabled – allows outbound traffic with known destination MAC addresses

- **Action**
  - None (default) – no trap is sent
  - Send Alarm – SNMP trap sent to network management system.

- **Authorized Addresses**
  - List of MAC addresses allowed
Resources

- Types of VLAN - http://www.vlan-analyser.co.uk/content/semitechnical.htm