**Lab1 CSCI-5160 Spring 2025**

**Introduction to Enterprise Networks**

Lab 1

Learning about Switches

**Spring 2025**

Lab1 CSCI 5160 Spring 2025

**OBJECTIVES**

1. **Learn how to perform basic switch configuration & troubleshooting including.**
   1. **Review basics for the switch password assignment and IOS navigation**
   2. **How to activate/deactivate a Port**
   3. **How to change the Speed and Duplex Mode on a Switch port**
   4. **How to verify the MAC addresses of computers connected to a specific port**
2. **Learn how to secure a Switch port so that only a specific user/device can connect.**
3. **Learn how to Create VLANs within a single Switch**
4. **Learn how to create VLANs across multiple Switches**
5. **Learn how to achieve Inter-VLAN communication using Trunking Protocols such as 801q and ISL**
6. **Configure VLAN Trunking Protocol (VTP) to manage multiple switches from a single one**
7. **Review the usage of Spanning Tree Protocol and how the switching environment behaves in the event of a network failure**
8. **Learn how Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1W is essential for faster convergence**
9. **Learn to increase the efficiency of a redundant network (PVST)**
10. **Learn about optional STP features like “Portfast” and “Etherchannel”**
11. **Sniff packets from your network.**

A diagram of a network

AI-generated content may be incorrect.

**Scenario:**

A company named **TechCorp** has two departments: **Engineering** and **Accounting**. Both departments need access to a centralized server, which hosts separate directories for each department. The server is located on a separate network (All required routes are configured for this lab), and the two departments are located on different VLANs. Inter-VLAN communication should be restricted except for accessing the server to ensure security and proper isolation.

**Objectives:**

1. **Basic Switch Configuration:**
   * Set up basic switch configurations, setup SSH on the Engineering-Switch and the Accounting-Switch including password protection and IOS navigation.
   * OUTCOME: PCx should be able to SSH to all the switches in the network

Report the commands with screenshots

1. **Default Switch Connectivity Test**
   * Activate and deactivate specific switch ports connected to each client as needed.
   * Assign IP addresses of your choice (/24) and ping from one client to another using the default VLAN.
   * Show the interfaces status on both switches. Use ‘show interface status’ or ‘show ip interface brief’
   * Change port speed to 10Mbps and duplex mode to half for the port connected to Engineering-A.

Turn on debugging and report any changes you see when the port is in half or full duplex mode

* + Verify connected devices using show mac address-table. On both switches.
  + OUTCOME: See how mac addresses are learned by all switches, for all systems connected.

Attach the screenshots

1. **Port Security Configuration:**
   * Configure port security on ethernet0/3 on the Accounting-Switch to ensure that only Accounting-B user can connect to this port.  
     First, add the mac-address of Accounting-B manually and once again configure in such way that the mac-address is read automatically from the switch.
   * Add a new client and test the security policy by swapping cables between devices and verify the console messages when unauthorized devices attempt to connect.

\*\*\*SAVE your config on the switch and clients then shut down the nodes before swapping cables.

Verify that your port security works, and its reversible once approved system is restored.

* OUTCOME: Prove that only a particular mac-address/system can connect to a unique physical port, and if you connect a different computer, port with stop its functionality

Report the commands you used and the screenshots of the debug messages.

Restore network connectivity without reconnecting equipment. (**Adjust security policy only)**

1. **Switch VLAN Configuration:**
   * Create VLANs for each department on each switch:
     + VLAN 10: **Engineering**
     + VLAN 20: **Accounting**
   * Assign the ports connecting to each department’s devices to the appropriate VLAN.
   * Configure the single port between the two switches (e1/2) as a trunk to allow communication with both VLANs.
   * Which trunking encapsulation was supported by both Switches by default? What other options are available? Use all variants and test end-to-end connectivity.
   * Verify that devices within the same VLAN can communicate, but devices from different VLANs cannot.
   * Ping from Engineering to Engineering
   * Ping from Engineering to Accounting. What is the result?
   * OUTCOME: Verify VLAN isolation for each respective department. Users of each department should only be able to ping their members

Report the commands + screenshots

1. **Router-on-a-Stick for Inter-VLAN Communication:**
   * Use the router to enable inter-VLAN communication only for the purpose of accessing the server, and pinging across approved departments
   * Configure sub-interfaces on the Gateway1020 for VLAN 10 and VLAN 20, each with a different IP address in their respective subnets.
   * Use a /24 for Engineering and a /27 for Accounting.
   * Configure one port from the core switch to the Gateway1020 to enable inter-vlan connectivity. (Access or Trunk?)
   * Ensure that the router provides access to both Engineering and Accounting to the Fileserver through their respective default gateway.
   * Do you need to worry about using the same IP addressing on Different VLANs? Why or why not?
   * OUTCOME: Engineering and Accounting departments should be able to reach their respective default gateways and visit the Fileserver.

Report the commands you used on the core switch and the DG for inter-vlan configuration

1. **Multiple Simultaneous Switch VLAN Configuration using VTP (** **):**
   * The core switch provides access to the DG

\*You can add new vlans to the server and propagate them to other switches in the network without having them configured manually on other switches.

* + Configure the core switch as a VTP server, and the Accounting-Switch as a VTP client
  + Leave the Engineering-Switch as transparent.
  + Add a new VLAN (30) on the core switch and make sure that the new VLAN is updated automatically on the other switches.
  + Configure different versions and password protection for the VTP.
  + Configure trunk ports between the switches.
  + Change the name of Accounting VLAN to HumanRes ONLY on the core switch. Verify that the Accounting-Switch adjusts to the new changes automatically as result of VTP.

Report from Switch IOS VLAN name propagation

* + Connect a new Client name it as “Archive” to the Accounting-Switch in VLAN-30
  + Ensure proper reachability to its default gateway Gateway30.

\*\*MAKE SURE TO SAVE YOUR CONFIGS BEFORE ADDING NEW NODES\*\*

Report the commands used for VTP versions, mode, domain, security and pruning + screenshots of the debug messages and the show results.

\* show vtp counters  
\* show vtp status

OUTCOME: Understand the different roles of VTP, understand how changes are propagated automatically by this feature, and what must be manually configured.

6.1 MULTI-HOP Routing

* + Make configuration needed for Archive client to ping all other systems and the FileServer (via its respective default gateway) NOTE that Engineeirng and accounting make use of Gateway1020 for their traffic, while Archive uses Gateway30 for its connectivity. (HINT: use static routes)
  + Add in your report 2 diagrams explaining how packets travel from Engineering to Accounting, and from Archive to Either one of them.
  + OUTCOME: Understand the need for a routing table to reach remote networks beyond default-gateway connectivity.

1. **Spanning Tree Protocol (STP) Configuration:**

Keep “debug spanning-tree bpdu” and “debug spanning-tree switch” ON on the core switch. Explain the messages generated from these commands when the topology changes.

* + Use “show spanning tree” command on each switch and locate any ports that are blocked by STP to prevent loops. Review the packet flow diagrams you created in the last objective and confirm exactly which ports/interfaces are being used by data flows.

  + Identify and document the priority, root bridge, designated, root, forwarding and blocked ports on the three switches, for each respective VLAN.

Include screenshots of the show commands used to document this

* + Change the cost of the path in such way that traffic from Accounting-A follows the following path to reach the Fileserver. Change VLAN configs on the switches whenever needed.   
      
    Accounting-A 🡪 Accounting-Switch 🡪 Engineering-Switch 🡪 Core Switch 🡪 Gateway1020 🡪 Fileserver
  + Change the cost of the path in such way that traffic from Engineering-A follows the following path to reach the Fileserver. Change VLAN configs on the switches whenever needed.   
      
    Engineering-A 🡪 Engineering-Switch 🡪 Accounting-Switch 🡪 Core-Switch 🡪Gateway1020 🡪 Fileserver
  + Use appropriate commands to replace the root bridge for another of your preference, make sure each VLAN has a different root switch.
  + Shut down one of the ports that connects your Root Bridge to another Switch on a particular VLAN (in forwarding state), document how the backup port transitions from Blocking to Forwarding.
  + How long does it take STP to re-converge (Report)?
  + Stop the DEBUG once done. (NOTE if using a virtual lab tool, this might not show intermediate steps)

1. **RSTP**:   
     
   STP has disadvantage that it has low convergence which is important at layer 2 LAN. IEEE with document 802.1W introduced an evolution of spanning tree protocol: Rapid Spanning Tree Protocol (RSTP), which reduces the convergence time after a topology change occurs in the network. STP takes 30 to 50 seconds from transit from blocking state to forwarding state. RSTP usually responds less than 10 seconds of a physical link failure.

* + Enable Rapid Spanning Tree Protocol (RSTP) for faster convergence.
  + Shut down one of the ports that connects your Root Bridge to another Switch, report how long does it take RSTP to re-converge (Report) Stop the debug commands

Turn on debugging for spanning-tree and report the show command results and the differences.

References: [http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree- protocol/24062146.html](http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-%20protocol/24062146.html)

Report the commands you used for configuring and manipulating spanning-tree.

OUTCOME: Learn how STP works by default, how to manipulate root role and path selection. Understand STP auto- convergence.

1. **Enhancing Network Efficiency with EtherChannel by overriding STP blockage between devices:**
   * You are facing congestion problems on your uplinks to the core switch, configure EtherChannel on the uplinks between the two Switches and the core switch to increase network capacity and redundancy. Configure E1 with PAGP and E2 with LACP.
   * Verify that STP treats the EtherChannel as a single logical link. Once you implement Etherchannel correctly you should not see a blocking port between Core switch and its neighbors
   * Assure that data flow for engineering and accounting over the switches still follows the paths defined before. Adjust as necessary to restore it (if needed)

9.1 STP Stability with Etherchannel

* + Test the network by disconnecting one of the EtherChannel member links and observing whether STP reconverges or not.
  + Explain the difference between STP cost, port speed and bandwidth on an ethernet switch. Which of these features was useful to you for this objective? Where are the other ones used?
  + OUTCOME: Etherchannel (EC) configuration via 2 different protocols, and the effects of EC over STP.

Report the results

1. **PortFast**

What are the advantages of portfast?

Enable portfast on one of the ports on which one of the clients is connected

Verify the change in response time. Give a snapshot of the debug command used and explain what you see in it.  
  
\*\* This part might not be doable on the virtual lab. Just report the commands you used for configuring portfast\*\*

1. **Configuring SPAN for Packet Sniffing:**
   * Configure SPAN on Engineering switch, so it can capture the traffic exchanged between all users and send it to the Sniffer System.
   * What does SPAN do? Why is this capability provided?
   * Set up a SPAN session on one of the switches to mirror traffic from a department’s VLAN.
   * Use Wireshark or TCPDump to capture and analyze packets. .
   * Add to your report a snippet of packets captured.

**Report Questions (answer after the questions):**

* + 1. How would you secure a switch to prevent others from accessing the network? (Hint: think layers)
    2. What is the length of the MAC address? How is it divided?
    3. Are sticky ports secure? Why or why not? Is it recommended?
    4. Why are switches faster than routers?
    5. How many MAC addresses does your computer have? How do you find out?
    6. What problem is portfast meant to solve in a network?
    7. Can you change your MAC address? If so, how?

1. Name/explain other applications of SPAN (Why do we need port replication/monitoring services for?)
2. What are the advantages of using VLANs?
3. Tell me any disadvantages of using VLANs
4. Can you do trunking with a PC? Is this a popular practice?
5. Can you telnet into a switch? Can any PC on any VLAN telnet into a switch (assume all PCs are connected to the same switch)?
6. Why do we need a Native VLAN for?
7. Give any important details regarding native VLANs in 802.1Q trunking.
8. Find and explain other trunking services used in industry.
9. What is a multilayer switch?
10. Explain how is RSTP better than STP?
11. What is the advantage of having Per VLAN STP? Explain VTP VLAN pruning.
12. Why do we need a Native VLAN for?
13. Give any important details regarding native VLANs in 802.1Q trunking.
14. Find and explain other trunking services used in industry.
15. What is a multilayer switch? What internal processing has to happen inside the switch (to the packet) in order to be able to do forward data based on layer 3 information?
16. Explain how RSTP is better than STP