LAB 2
Documentation

Team: ByteBunch5

Arijana Määttä
Adrian Garcia Castro
Mohamed el Allati
Sofia Ojala
Metehan Çakal

Table of Contents

PROJECT SUMMARY

A structured network with specific layouts, VLANs, switched connections, routing setups, and enabled remote access, all with dynamic IP addressing through DHCPv4 was created in a previous Lab 1 exercise.

For this, Lab 2, we focused on enhancing security. We allocated all unused switch ports to a new VLAN. We turned off automatic trunking for ports and added PortSecurity to the switch ports connecting to specific PCs, controlling the number of devices that could connect, and setting up alerts or shutdowns for any excess. Additionally, we configured PortFast and BPDU guard on certain ports and ensured everything was working as expected.

NETWORK CONFIGURATION DETAILS – TABLES

Addressing table

Note VLANS and corresponding IP subnets

Device	Interface	IP Address	Default Gateway
SW1_broom	VLAN 10	192.168.10.2 /24	192.168.10.1
SW2	VLAN 10	192.168.10.3 /24	192.168.10.1
Router_on_a_stick	F0/1.10 F0/1.20 F0/1.30 F0/1.40	192.168.10.1 /24 N/A 192.168.30.1 /24 192.168.40.1 /24	N/A
Saana-PC	NIC	DHCP Assigned	DHCP Assigned
Student-PC	NIC	DHCP Assigned	DHCP Assigned

VLAN Table

VLAN	Name	Interface Assigned	Trunking Ports - DTP Disabled on all
10	Remote_Management	SW1_broom: VLAN 10 SW2: VLAN 10 Router_on_a_stick: F0/1.10	SW1_broom :G0/1-2(, F0/1 SW2 : G0/1-2 Router_on_a_stick: F0/1
20	Native_Replacement		SW1_broom :G0/1-2, F0/1 SW2 : G0/1-2 Router_on_a_stick: F0/1.20
30	Smart_IoT_Students	SW2: F0/1 (access port) Router_on_a_stick: F0/1.30	SW1_broom :G0/1-2, F0/1 SW2 : G0/1-2 Router_on_a_stick: F0/1
40	Saana_LabRats	SW1_broom: F0/2 (access port) Router_on_a_stick: F0/1.40	SW1_broom :G0/1-2 , F0/1 SW2 : G0/1-2 Router_on_a_stick: F0/1
999	UNUSED_PORTS	SW1_broom: F0/3-24 SW2: F0/2-24	

PortFast and BPDU Guart

Switch	Interface	PortFast	BPDU Guard
SW1_broom	F0/2	Enabled	Enabled
SW1_broom	F0/3 - 24	Enabled	Enabled
SW2	F0/1	Enabled	Enabled
SW2	F0/2 - 24	Enabled	Enabled

EtherChannel Table

Channel Group	Port-Channel	Ports	Protocol
1	Po1	SW1_broom - G0/1-2 SW2 - G0/1-2	PAgP

Subnets and DHCP settings

VLAN	Subnet	Gateway	Pool Name	DHCP server	Excluded/reserved addresses
10	192.168.10.0/24	192.168.10.1			
20	192.168.20.0/24				
30	192.168.30.0/24	192.168.30.1	Students	192.168.30.254	192.168.30.1 – 192.168.30.10, 192.168.30.254
40	192.168.40.0/24	192.168.40.1	Saana	192.168.40.254	192.168.40.1 – 192.168.40.10, 192.168.40.254

Physical Cable Table

From - interface	To - interface
SW1_broom - G0/1-2	SW2 – G0/1-2
SW1_broom – F0/1	Router_on_a_stick – F0/1
SW1_broom – F0/2	Saana-PC – NIC (PortSecurity: Max MAC 4, Shutdown on Exceed, Secure MAC: [Saana's MAC], Sticky MAC)
SW2 – F0/1	Student-PC – NIC (PortSecurity: Max MAC 10, Syslog on Exceed, Dynamic MAC, Age-out 60 min)

Remote access

Username: ByteBunch5
Password: cisco

TROUBLESHOOTING

Problem: After restarting the switches, the trunking ports reset to VLAN1 (Default) instead of retaining their pre-assigned VLANs.

Steps we took:

- Verified current VLAN assignments on trunk ports
- Checked for saved configurations post-VLAN assignments
- Ensured consistent native VLAN on both trunk sides
- Allowed VLAN 20 on the trunk ports
- Saved and verified updated configuration

Result: After permitting VLAN 20 and saving the configuration, trunk ports correctly retained their designated VLANs post-restart.

QUESTIONS

Question 1: Should you modify your trunk settings to allow it to carry the data for the new VLAN you created in Part 1 of this lab? Why?

No, we should not modify trunking settings to allow the new VLAN to carry data across the trunk. The purpose of creating this VLAN was to isolate unused ports for security reasons. The primary reason for such VLAN is to separate and secure unused ports.

Question 2: Imagine the lab network you created was a real network that exists in our real classroom. Identify and name at least 3 existing (physical) security measures that are in use to prevent unauthorized access to our equipment or protect the lab and equipment or people working in the lab in case something goes wrong.

1. Restricted Access to the classroom with Card Scanner : only staff members and students with appropriate clearance can enter classroom.
2. Surveillance Cameras : Surveillance cameras on the corridors that monitor the classroom. If needed they are able to provide a record of individuals entering the lab.
3. Security guard: there is a security guard at the reception of the building
4. Fire detecting alarms: in a case of fire, the alarms will go off and possibly prevent any further damages to the equipment

Question 3: Can you think of any other security configurations on the networking devices that you could still implement to further fortify your network? You do not have to implement them.

1. Access Control Lists (ACLs): Utilize ACLs to define permissions based on source/destination IP addresses, port numbers, and protocol types, enhancing network security by controlling traffic flow.

2. Console Line Passwords: Secure console access with strong, regularly updated passwords to prevent unauthorized access to network devices.

3. IEEE 802.1X Authentication: Enhance network security by implementing IEEE 802.1X authentication, ensuring that only authorized users or devices with valid credentials can access the network.

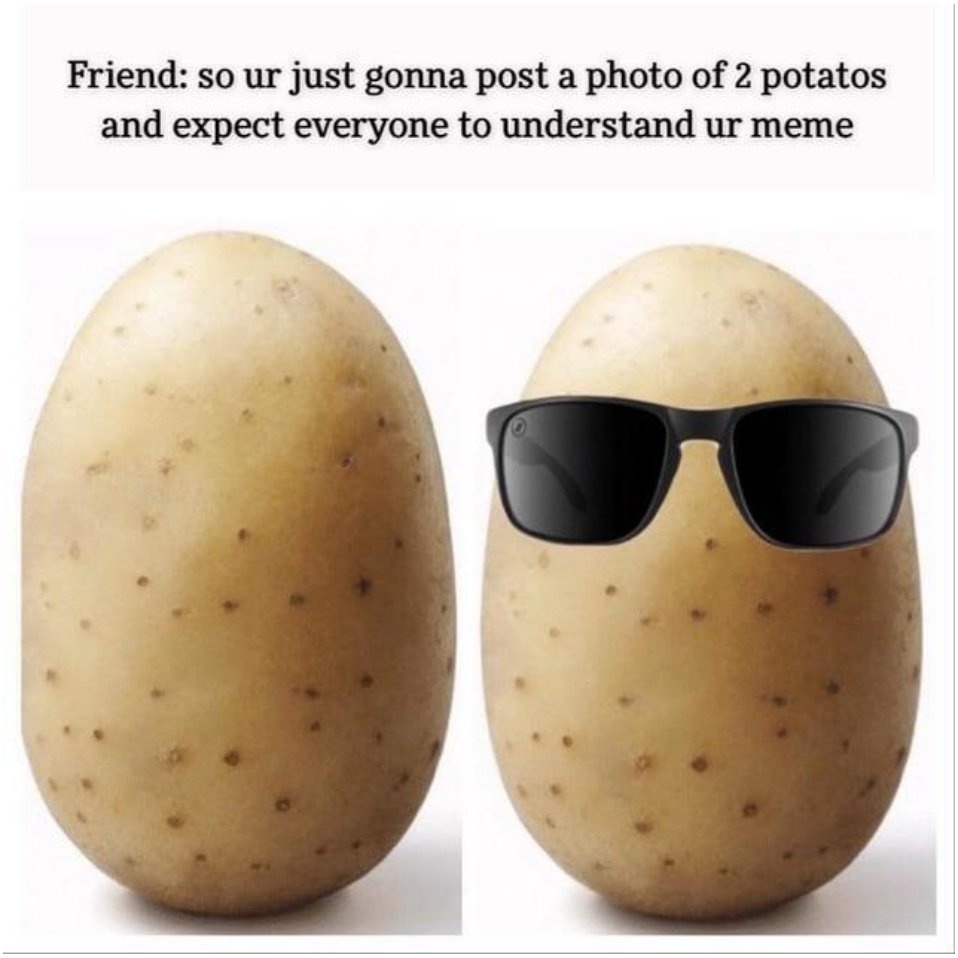
4. Host-Based Intrusion Prevention Systems (HIPS): Strengthen network security by deploying HIPS solutions on individual devices, actively monitoring and blocking potential threats at the device level.

5. Advanced Malware Protection (AMP): Detect and mitigate malware and other malicious threats across the network using AMP, bolstering overall network security.

6. DHCP Snooping: Enabling DHCP snooping prevents rogue DHCP servers on the network. DHCP snooping can ensure that only authorized DHCP servers are providing IP addresses to clients.

7. Dynamic ARP Inspection (DAI): Validates ARP packets in the network to prevent ARP spoofing attacks. It ensures that only valid ARP packets are allowed, protecting against man-in-the-middle attacks.

MEME


Friend: so ur just gonna post a photo of 2 potatos
and expect everyone to understand ur meme