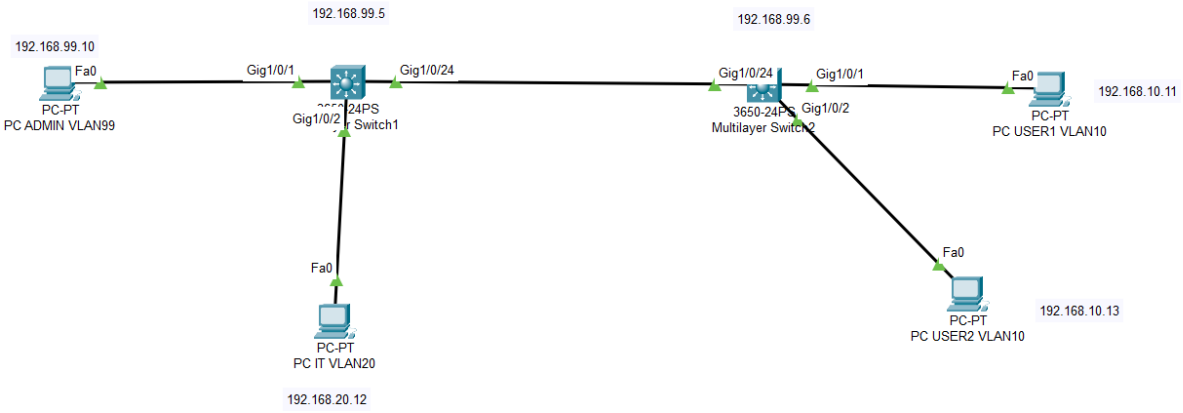
CCNA Lab: VLAN Configuration with SSH/Telnet Remote Management

A comprehensive hands-on laboratory for CCNA students covering VLAN implementation, trunk configuration, and secure remote management.

Network Topology



VLAN Scheme & IP Addressing

Device	Interface	IP Address	Subnet Mask	VLAN	Description
PC_Admin	NIC	192.168.99.10	/24	99	Management
PC_IT	NIC	192.168.20.12	/24	20	IT Department
PC_User1	NIC	192.168.10.11	/24	10	Users
PC_User2	NIC	192.168.10.13	/24	10	Users
SW1	VLAN99	192.168.99.5	/24	99	Management SVI
SW2	VLAN99	192.168.99.6	/24	99	Management SVI

Port Assignments

SW1 Port Configuration:

- **Fa0/1: PC_Admin (VLAN 99 - Management)**
- **Fa0/2: PC_IT (VLAN 20 - IT Department)**
- **Fa0/24: Trunk to SW2**

SW2 Port Configuration:

- **Fa0/5: PC_User1 (VLAN 10 - Users)**
- **Fa0/6: PC_User2 (VLAN 10 - Users)**

- **Fa0/24: Trunk to SW1**

🚀 **Lab Instructions**

Part 1: Basic Switch Configuration

Task 1.1: Configure SW1 Basic Settings

enable

configure terminal

hostname SW1

no ip domain-lookup

enable secret cisco123

line console 0

password console123

login

logging synchronous

exec-timeout 5 0

line vty 0 4

password vty123

login

end

copy running-config startup-config

Task 1.2: Configure SW2 Basic Settings

Repeat the configuration for SW2 (change hostname to SW2 and IP to 192.168.99.6)

Verification:

show running-config | include hostname

Part 2: VLAN Configuration

Task 2.1: Create VLANs on SW1

configure terminal

vlan 10

name Users

vlan 20

name IT_Department

vlan 99

name Management

vlan 999

name BlackHole

exit

Task 2.2: Assign Ports to VLANs (SW1)

interface fa0/1

switchport mode access

switchport access vlan 99

description "PC_Admin - Management"

interface fa0/2

switchport mode access

switchport access vlan 20

description "PC_IT - IT Department"

interface range fa0/3-23

switchport mode access

switchport access vlan 999

description "Unused - BlackHole"

shutdown

exit

Task 2.3: Configure Trunk Port (SW1)

interface fa0/24

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,99

description "Trunk to SW2"

exit

Task 2.4: Repeat Configuration on SW2

- **Create the same VLANs**
- **Assign ports fa0/5 and fa0/6 to VLAN 10**
- **Configure trunk on fa0/24**

Verification Commands:

show vlan brief

show interface trunk

show interface status

Part 3: Management VLAN & SVI Configuration

Task 3.1: Configure SVI on SW1

interface vlan 99

ip address 192.168.99.5 255.255.255.0

no shutdown

description "Management Interface"

exit

Task 3.2: Configure SVI on SW2

interface vlan 99

ip address 192.168.99.6 255.255.255.0

no shutdown

description "Management Interface"

exit

Task 3.3: Configure Default Gateway (Both Switches)

ip default-gateway 192.168.99.1

Verification:

show ip interface brief

ping 192.168.99.6 # From SW1

ping 192.168.99.5 # From SW2

Part 4: Telnet Configuration

Task 4.1: Basic Telnet Setup

line vty 0 4

password telnet123

login

transport input telnet

exec-timeout 10 0

exit

Task 4.2: Test Telnet Connection

From PC_Admin:

telnet 192.168.99.5

telnet 192.168.99.6

Verification:

show users

Part 5: SSH Configuration

Task 5.1: Prepare for SSH

configure terminal

ip domain-name lab.local

username admin privilege 15 secret admin123

username user privilege 1 secret user123

Task 5.2: Generate RSA Keys

crypto key generate rsa

 # Choose 2048 bits when prompted

Task 5.3: Configure SSH

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 3

line vty 0 4

login local

transport input ssh

exec-timeout 15 0

exit

Task 5.4: Test SSH Connection

From PC_Admin:

ssh -l admin 192.168.99.5

ssh -l user 192.168.99.5

Verification Commands:

show ssh

show ip ssh

show users

show crypto key mypubkey rsa

Part 7: Troubleshooting & Diagnostics

Task 7.1: Functionality Tests

Test 1: Intra-VLAN Communication

- **PC_User1 → PC_User2 (ping should work)**
- **PC_Admin → SW1 Management (ping should work)**

Test 2: VLAN Separation

- **PC_User1 → PC_IT (ping should fail)**
- **PC_IT → PC_Admin (ping should fail)**

Test 3: Remote Management

- **Telnet from PC_Admin → SW1 (should be blocked)**
- **SSH from PC_Admin → SW1 (should work)**
- **SSH from PC_User1 → SW1 (should be blocked)**

Task 7.2: Introduce and Fix Common Issues

Error 1: Native VLAN Mismatch

 # On SW2:

interface fa0/24

switchport trunk native vlan 10

Observe: show logging | include CDP Fix: Restore native vlan 99

Error 2: Delete VLAN

 # On SW2:

no vlan 10

Check: show vlan brief, show interface status Fix: Recreate VLAN 10

Error 3: Trunk Allowed VLAN List

 # On SW1:

interface fa0/24

switchport trunk allowed vlan 99

Check: Communication between PC_User1 and PC_User2 Fix: Add VLAN 10 to allowed list

---

Part 8: Verification & Documentation

Task 8.1: Verification Commands

Execute and document results:

show vlan brief

show interface trunk

show ip interface brief

show users

show ssh

show access-lists

show mac address-table

show interface status

Task 8.2: Security Testing

1. **Password Strength Testing:**
    - **Test various password combinations**
2. **Access Restriction Testing:**
    - **Attempt SSH from different VLANs**
3. **Timeout Testing:**
    - **Leave session inactive and verify auto-disconnect**

Task 8.3: Configuration Backup

copy running-config tftp

 # or

copy running-config startup-config

show startup-config

📊 Grading Rubric

Area	Points	Requirements
Basic Configuration	15	Hostname, passwords, descriptions
VLAN Implementation	25	All VLANs working correctly
Trunk Configuration	20	Inter-switch communication
SSH/Telnet Setup	20	Remote management functional
Troubleshooting	5	Correct error resolution

Total: 100 Points

⏱️ Estimated Completion Time

3-4 hours (including testing and documentation)

🛠️ Equipment Requirements

- **Software: Cisco Packet Tracer 8.0+ or GNS3**
- **Hardware Alternative: 2x Cisco 2960 Switches + 4x PCs**
- **Cables: Ethernet straight-through and crossover cables**

📚 Learning Outcomes

After completing this lab, students will be able to:

✅ **Configure and manage VLANs on Cisco switches**
✅ **Implement trunk links with 802.1Q tagging**
✅ **Set up secure remote management (SSH)**
✅ **Apply basic security configurations**
✅ **Troubleshoot common VLAN issues**
✅ **Verify network functionality using show commands**

🤝 Contributing

Found an issue or have suggestions for improvement?

1. **Fork this repository**
2. **Create a feature branch (git checkout -b feature/improvement)**
3. **Commit your changes (git commit -am 'Add improvement')**

4. **Push to the branch (git push origin feature/improvement)**
5. **Create a Pull Request**

📄 License

This lab exercise is provided under the MIT License. Feel free to use and modify for educational purposes.

🏷️ Tags

#CCNA #Cisco #VLAN #SSH #Networking #Lab #PacketTracer #Network-Security

---

Happy Learning! 🎓

If you found this lab helpful, please ⭐ star this repository and share it with other networking students!