Incident Response Lab Report: Cisco Packet Tracer Network Simulation

By Marcus Dunn

Executive Summary

Here is a record of a network simulation lab built on Cisco Packet Tracer. The objective was to create a network that is segmented with VLANs, with routing, with ACLs, as well as with centralized SYSLOG logging being a key component of enterprise security infrastructures. It reveals how access can be monitored with segmentation in a virtualized SOC (Security Operation Center) environment. This is appropriate for entry-level infosec pros that must understand some of the fundamentals of network security and monitoring.

Lab Overview and Objectives

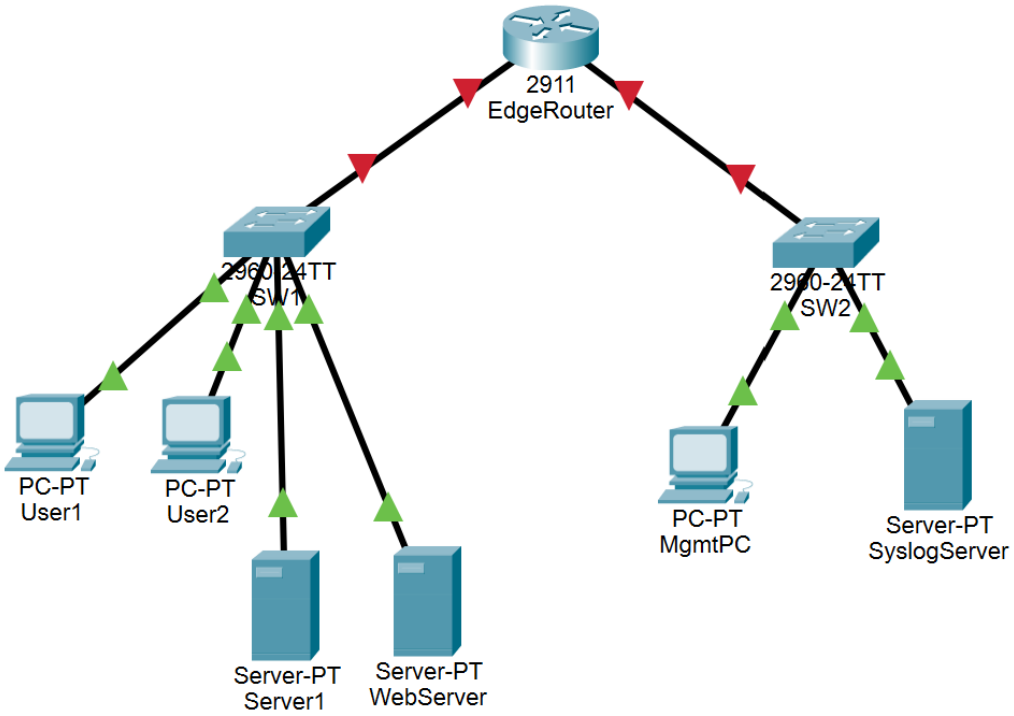
- Form a network topology with router, switches, servers, and user devices
- Create VLANs to divide traffic logically
- Set up static IPs and default gateways for all devices
- Configure router-on-a-stick for inter-VLAN
- Employing ACLs for blocking illegitimate access
- Set up a Syslog server for collecting and processing event logs
- Confirm connectivity and check traffic filtering and logging

Environment Architecture

The simulated environment includes:

- 1 Cisco 2911 Router (EdgeRouter)
- 2 Cisco 2960 Switches (SW1 and SW2)
- 2 User PCs in VLAN 10
- 1 Internal Server in VLAN 20
- 1 Web Server in VLAN 30 (DMZ)
- 1 Admin workstation and 1 Syslog server in VLAN 99 (Management)

Network Topology:



Lab Setup & Configuration

VLAN and Switch Port Configuration:

SW1

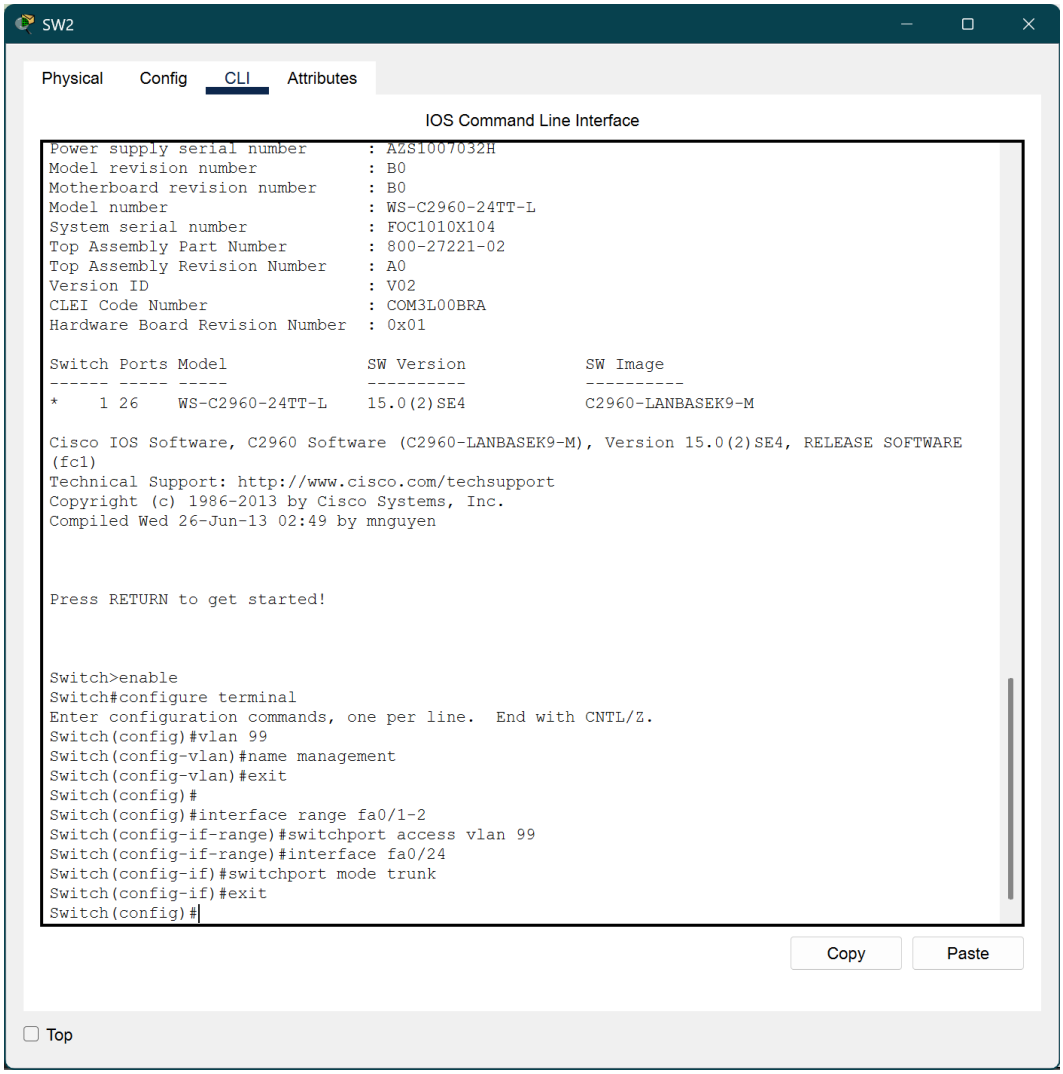
Physical Config CLI Attributes

IOS Command Line Interface

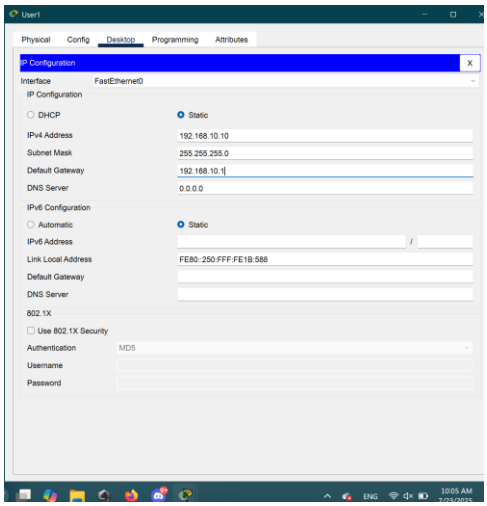
```
CLEI Code Number                 : COM3L00BRA
Hardware Board Revision Number   : 0x01

Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!



Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Users
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Servers
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name DMZ
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface fa0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface fa0/4
Switch(config-if)#switchport access vlan 30
Switch(config-if)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

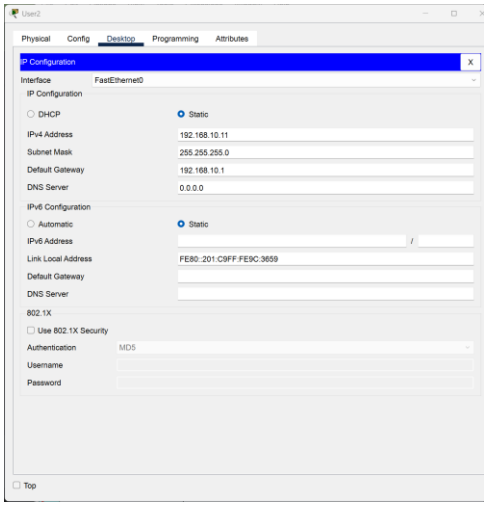
Copy Paste

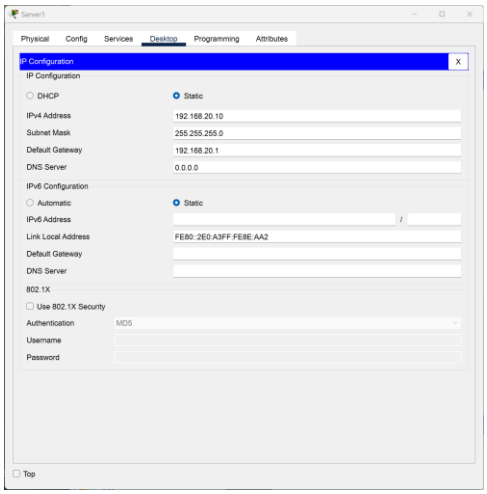
Top

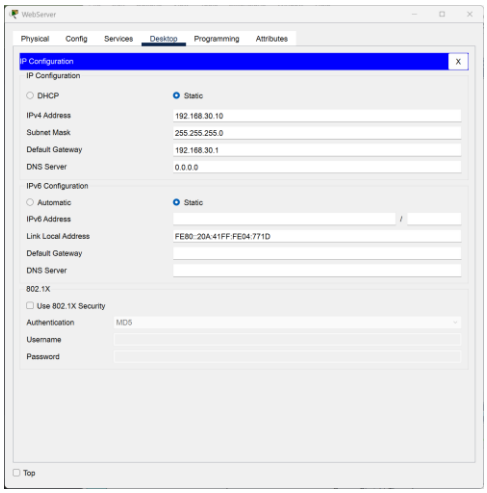


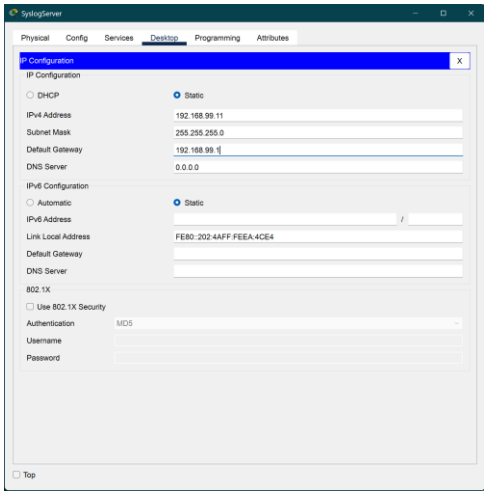
IP Address Assignments:




User2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:C9FF:FE9C:3659
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Server1
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.20.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2E0:A3FF:FE8E:AA2
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


WebServer
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.30.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20A:41FF:FE04:771D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top



Router-on-a-Stick Configuration:

EdgeRouter

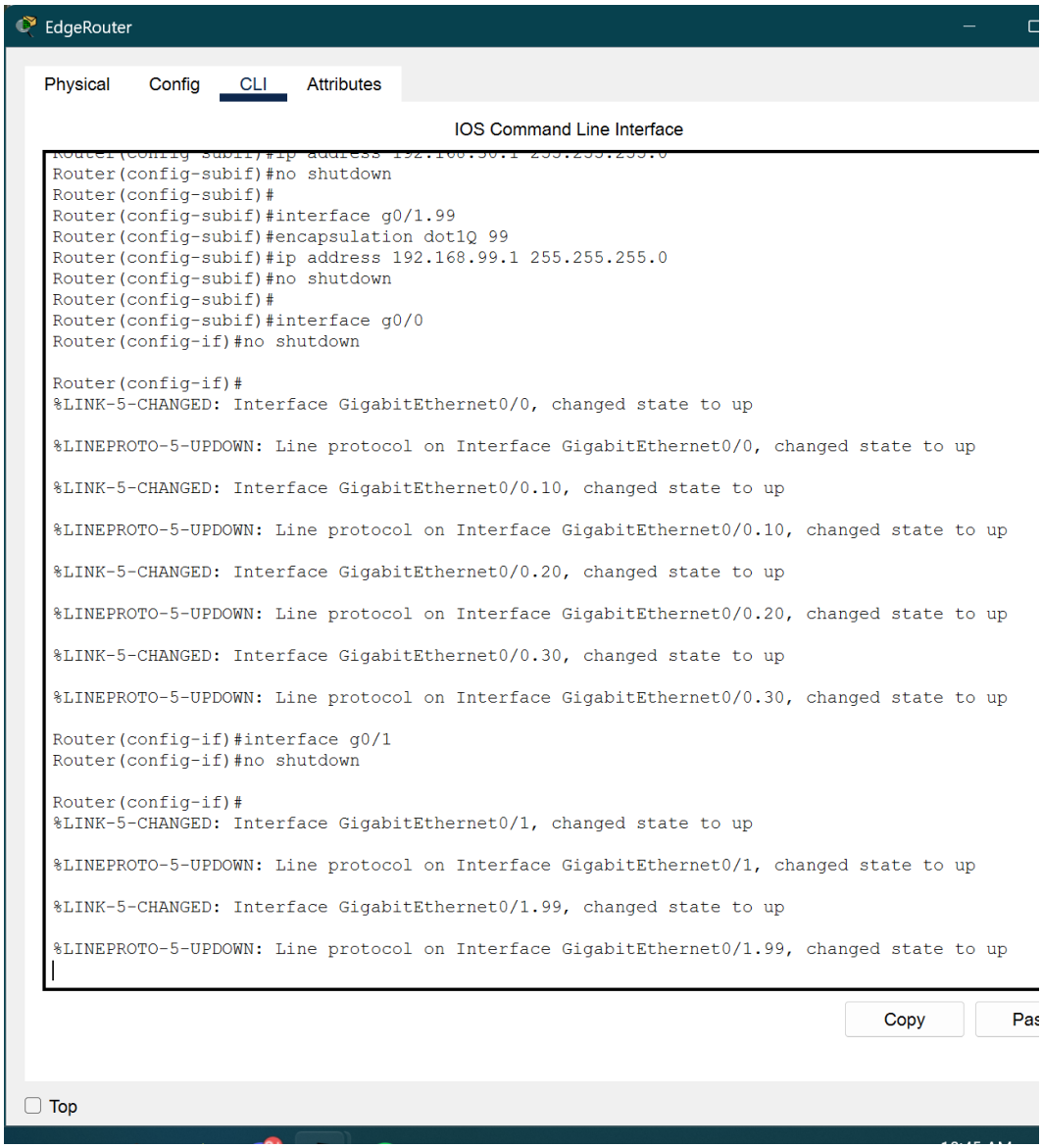
Physical Config CLI Attributes

IOS Command Line Interface

```
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#interface g0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#interface g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#interface g0/1.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip address 192.168.99.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#
Router(config-subif)#
```

Copy Pas

Top



Access Control and Network Segmentation

An extended access control list (ACL 100) was configured on the router to deny access from VLAN 10 (Users) to VLAN 99 (Management). This will prevent any unauthorized user traffic from reaching sensitive administrative systems like the Syslog server.

EdgeRouter

Physical Config CLI Attributes

IOS Command Line Interface

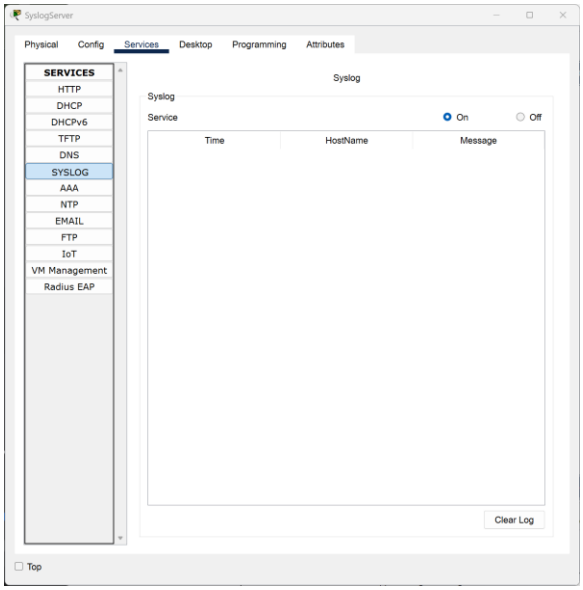
```
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

Router(config-if)#interface g0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.99.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#interface g0/0.10
Router(config-subif)#ip access-group 100 in
Router(config-subif)#exit
Router(config)#
```

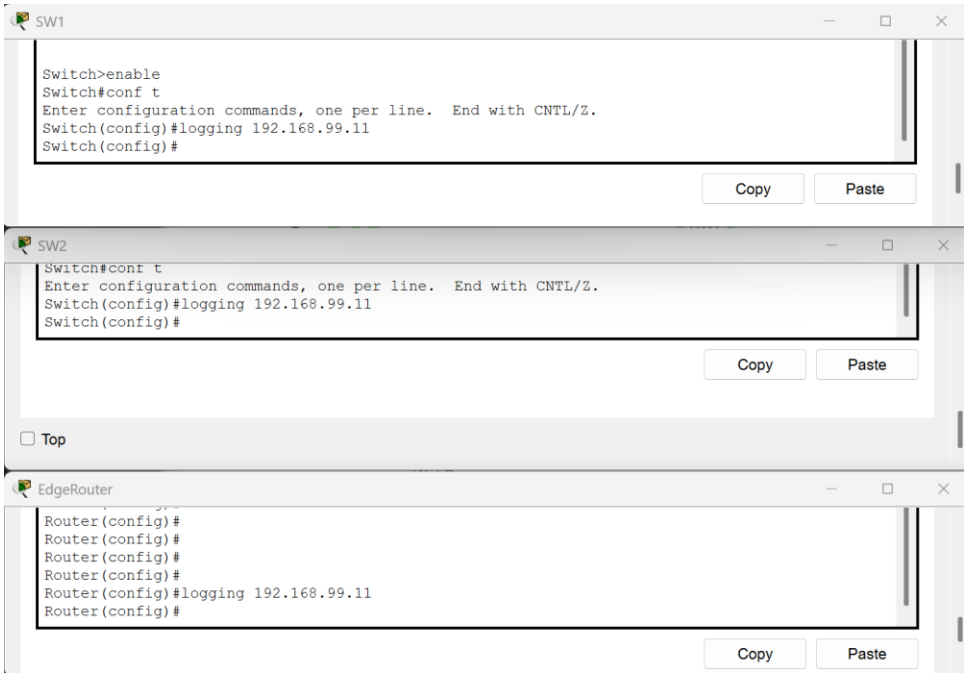
Copy Pas

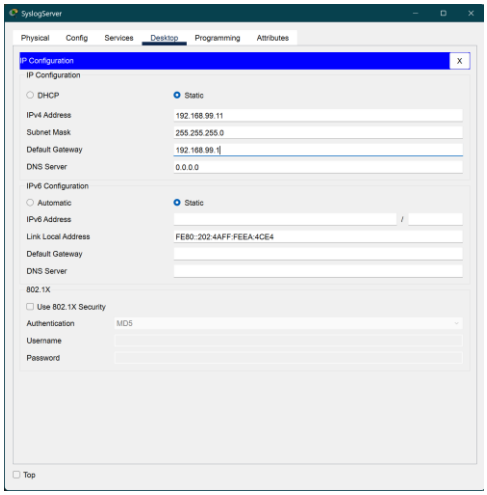
Top

Centralized Syslog Logging

A Syslog server was configured to collect logs from all network devices. The Syslog service was enabled on the server and each switch and router was pointed to it using the `logging` command. Interface state changes and other critical events were successfully logged.

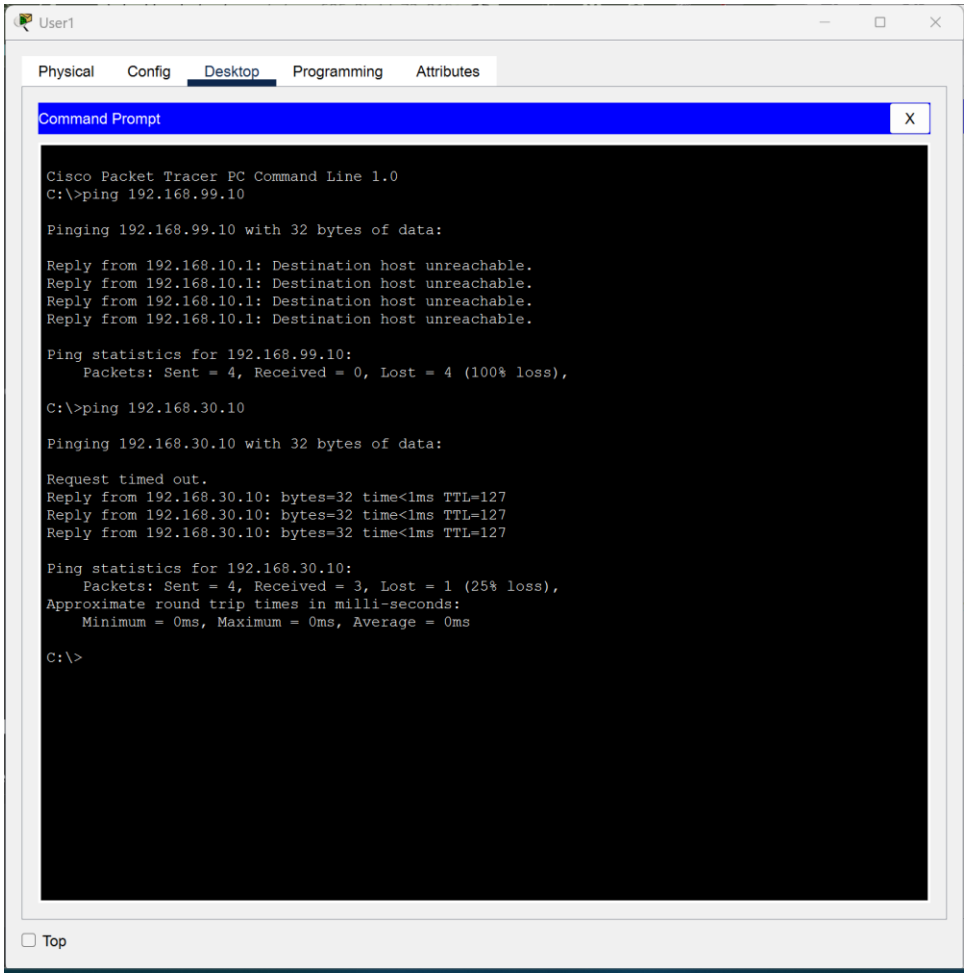

SyslogServer
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
Syslog
Syslog
Service
On
Off
Time
HostName
Message
Clear Log
Top


SW1
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#logging 192.168.99.11
Switch(config)#
Copy
Paste
SW2
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#logging 192.168.99.11
Switch(config)#
Copy
Paste
Top
EdgeRouter
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#logging 192.168.99.11
Router(config)#
Copy
Paste



Testing and Validation

Tests for confirming ACL functionality as well as syslog functionality were conducted. Pings from User1 to MgmtPC were being prevented as intended by ACLs. However, access by User1 to WebServer demonstrated that connectivity to DMZ was fine. A switch port was brought down to raise a log event.



Troubleshooting and Problem Solving

• Syslog server isn't getting logs – corrected by verifying IP address and enabling Syslog service.
• Devices not pinging across VLANs – corrected by confirming router sub-interfaces were established properly and active.
• ACL not functioning – fixed by putting access group on correct sub-interface and verifying syntax.

Lessons Learned

• VLANs and ACLs can be readily utilized to divide and control traffic in enterprise networks.
• Syslog is critical in monitoring device activity for abnormal behavior.
• A router-on-a-stick is a simple way for a single router interface to support multiple VLANs.
• Proper settings for IP address and default gateway are necessary for successful communication.

• Multi-level troubleshooting and validation at each stage must be done in order to detect and correct configuration issues.