

Network Security & Information Assurance(CY-331)

Project Report

Enterprise Level Architecture Using CISCO Packet Tracer



Group Members

1. Shameer Awais (2022428)
2. Rooshan Riaz (2022506)
3. Umar Maqsood (2022447)
4. Haroon Sheikh (2022381)

Submission Date: 11/12/2024

Ghulam Ishaq Khan Institute of Engineering Sciences and Technology

Contents

1	Introduction	2
2	Network Topology	2
2.1	Components	3
2.1.1	Network Controller (PT-Controller)	3
2.1.2	Switches	3
2.1.3	Routers	3
2.2	Connections	3
2.2.1	Local Area Networks (LANs)	3
2.2.2	Backbone Network	4
2.2.3	Interconnectivity	4
2.3	Login Credentials for Devices	4
2.4	Network Design Goals	4
2.5	Diagram of the Network Topology	4
2.6	Summary	5
3	Device Configuration and Management	5
3.1	Router Configuration	5
3.1.1	Assigning IP Addresses to Interfaces:	5
3.1.2	Enabling OSPF Routing Protocol:	6
3.1.3	Verifying OSPF Configuration:	6
3.2	Switch Configuration	7
3.2.1	Assigning Management IP Addresses:	7
3.2.2	Configuring VLANs:	7
3.3	Device Management	8
3.3.1	Accessing Devices:	8
3.3.2	SDN Controller:	8
3.3.3	Network Monitoring and Logging	8
4	Command Line Interface Operations	9
4.1	Device Access and Authentication	9
4.2	Verification Commands	10
4.3	Debug Commands	11
5	Features of SDN Controller	12
6	Comparative Analysis	13
6.1	Configuration and Management	13
6.2	Network Monitoring	14
6.3	Troubleshooting and Debugging	14
6.4	Security and Access Control	15
6.5	Scalability	15

1 Introduction

Network management is a very significant aspect to assess the efficiency, reliability and security of today's computer networks. No doubt, the CLI is always considered the best way that network administrators have been using in the past to configure and manage devices. But the emergence of SDN has opened new opportunities for applications, which are centralized, automated and scalable in the network field.

This project explores and compares two approaches to network management: Command Line Interface based version configuration and Software Defined Networking Controller based management. The project uses Cisco's Packet Tracer simulator to show how both methods can be applied practically across a simulated network. Some of the basic things to do are focusing on CLI of routers and switches, creating an SDN controller and then mapping the network with the help of the controller, setting up configurations to the switch/router using the controller.

In more details, the aim of this study is to describe and compare the relative merits of using CLI and SDN based management practices in the current network architecture as well as elaborate on the benefits of embracing SDN for contemporary network platforms. The comparison made in this paper will assist in evaluating how network programmability can make tasks easier and enrich the management process. In greater detail, this study seeks to:

- Summarize the CLI approach concentrating on its benefits and drawbacks in The division entails the administrative tasks such as management of the network setting and the problems that come with it.
- Emphasize the element of excellence of SDN such as, centralised control, automation and others. temporary, as well as the other aspects that are valuable for modern networks such as real-time monitoring.
- Establishment of relative effectiveness, and scalability of CLI and SDN. and security.
- Identify real life scenarios where both approaches have been applied using Cisco Packet Tracer to give a practical approach.

2 Network Topology

The topology consists of a structured network environment designed for a comparative study of CLI-based and SDN controller-based management. At the core, three ISR4331 Routers (R1, R2, and R3) are used for interconnection among various subnetworks to ensure efficient routing. To simplify the network management and to host network related services a network controller and server are connected to SWL1. There are PCs (PC1-PC4 and Admin PC) in two LANs (10.0.1.0/24 and 10.0.2.0/24) over SWR switches for end user operation. The switches are arranged in a more mesh like manner to provide redundancy and also load balancing. Each device assigns its own subnet IP addressing in order of arbitration, security and scalable networking. There is also wise use of a single set of login credentials for the management of devices in the design.

2.1 Components

The primary components of the network topology are described below:

2.1.1 Network Controller (PT-Controller)

The PT-Controller therefore functions as the managing focal point of the Software-Defined Network (SDN). It is meant to command and schedule network devices through a programmable interface.

- **IP Address:** 192.168.101.254
- **Function:** Manages the various networks that occur in the SDN environment through offering them configuration as well as monitoring.

2.1.2 Switches

Switches serve as key components in both local and backbone networks.

- **Local Area Network (LAN) Switches:**
 - SWL1: Connects the local devices, including the server and end-user systems.
 - SWL2: Provides additional LAN connectivity for client devices.
- **Backbone Switches:**
 - SWR1, SWR2, SWR3, SWR4: Configured in a mesh topology to ensure load balancing and fault tolerance.

2.1.3 Routers

Switches are used to connect local area networks and use routing to interconnect different subsets of the various LANs.

- **Routers:** R1, R2, R3
- **Purpose:** Enable interconnectivity between LANs and provide routing for different IP ranges.
- **Subnet Masks:** All IP addresses use a /24 subnet mask.

2.2 Connections

The network topology is organized into two primary sections: Local Area Networks (LANs) and the backbone network.

2.2.1 Local Area Networks (LANs)

- **LAN 1:** Includes SWL1, Server-PT, and associated end devices.
- **LAN 2:** Includes SWL2 and associated end devices.
- LAN switches are connected to routers R1, R2, R3, which facilitate inter-LAN communication.

2.2.2 Backbone Network

- The backbone network consists of SWR1, SWR2, SWR3, SWR4, configured in a mesh topology.
- This configuration ensures fault tolerance and load balancing.

2.2.3 Interconnectivity

- Local switches are connected to routers R1, R2, R3, which provide interconnectivity between local networks.
- Routing between different IP ranges is achieved using static or dynamic routing protocols.

2.3 Login Credentials for Devices

It is noted that all devices in the network should be configured with the following detail for administrator access Beitrag melden:

- **Username:** cisco
- **Password:** cisco123!

2.4 Network Design Goals

This topology is structured to illustrate the following:

1. Traditional network management via command line interface working with routers and switches configuration.
2. Modern SDN-based administration using the PT-Controller.
3. A comparative analysis of the efficiency, scalability, and ease of use of both approaches.

2.5 Diagram of the Network Topology

Figure 1 allows the system designer to see the composition of the actual network on the physical plane, as well as the topological interconnection between the elements of the network.

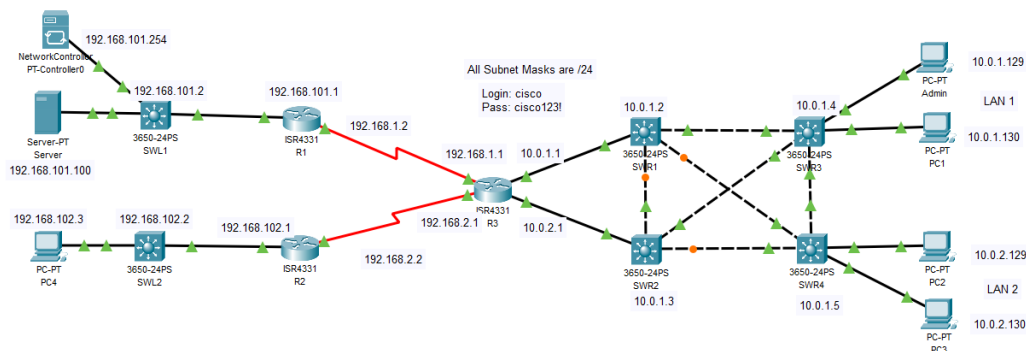


Figure 1: Network topology

2.6 Summary

This network structure was deliberately chosen for assessing the CLI based as well as the SDN based network management solutions. It comprises both conventional and advanced parts so as to offer an all-in-all approach to contribute towards a vigorous research system.

3 Device Configuration and Management

The network topology implements the OSPF protocol with dynamic routing in all routers in the network topology. The information in this section describes the configurations and policies applied to the routers and switches in the topology.

3.1 Router Configuration

To ensure proper routing execution, routers R1 and R2 are configured with similar settings to support OSPF routing for network scalability. The configurations involve the following key steps:

3.1.1 Assigning IP Addresses to Interfaces:

Every router interface is assigned IP addresses of the subnets to which they are connected.

```
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#ip addr 192.168.101.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

Figure 2: Router 1 Gigabit Interface

```
R1(config)#interface Serial0/1/0
R1(config-if)#ip addr 192.168.1.2 255.255.255.0
R1(config-if)#no shutdown
```

Figure 3: Router 1 Serial Interface

Figures 2 and Figure 3 show the commands to configure ip addresses on two different interfaces of Router 1.

```
R2(config)#interface Serial0/1/1
R2(config-if)#ip addr 192.168.2.2 255.255.255.0
R2(config-if)#no shutdown
```

Figure 4: Router 2 Serial Interface

Figure 5 and Figure 4 show the commands to configure ip addresses on two different interfaces of Router 2.

```

R2(config)#interface GigabitEthernet0/0/0
R2(config-if)#ip addr 192.168.102.1 255.255.255.0
R2(config-if)#no shutdown

```

Figure 5: Router 2 Gigabit Interface

3.1.2 Enabling OSPF Routing Protocol:

This is done following the appropriate process IDs of OSPF, and also the networks are advertised.

3.1.3 Verifying OSPF Configuration:

Like other OSPF link state protocols, the neighbor relationships and route exchanges are normally checked by prominent commands. Figure 6 verifies the OSPF routing protocol on Router 1.

```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 2 subnets
O       10.0.1.0/24 [110/65] via 192.168.1.1, 4294967273:4294967290:4294967264,
Serial0/1/0
O       10.0.2.0/24 [110/65] via 192.168.1.1, 4294967273:4294967290:4294967264,
Serial0/1/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/1/0
L       192.168.1.2/32 is directly connected, Serial0/1/0
O       192.168.2.0/24 [110/128] via 192.168.1.1, 4294967273:4294967290:4294967264,
Serial0/1/0
    192.168.101.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.101.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.101.1/32 is directly connected, GigabitEthernet0/0/0
O       192.168.102.0/24 [110/129] via 192.168.1.1, 4294967273:4294967290:4294967264,
Serial0/1/0
S*    0.0.0.0/0 is directly connected. Serial0/1/0

```

Figure 6: Verifying OSPF Configuration on Router 1

Network Device + DEVICE						
	Hostname	Type	IP	Up Time	Last Updated	Collection Status
	SWL1	MultiLayerSwitch	192.168.101.2	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	R1	Router	192.168.1.2	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	R3	Router	192.168.2.1	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	R2	Router	192.168.2.2	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	SWR1	MultiLayerSwitch	10.0.1.2	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	SWR2	MultiLayerSwitch	10.0.1.3	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	SWL2	MultiLayerSwitch	192.168.102.2	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	SWR4	MultiLayerSwitch	10.0.1.5	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed
	SWR3	MultiLayerSwitch	10.0.1.4	1 hours, 37 minutes, 2 seconds	2024-12-06 23:17:23	Managed

Figure 7: Network Devices being managed by the Controller

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 2 subnets
O       10.0.1.0/24 [110/65] via 192.168.2.1, 00:01:20, Serial0/1/1
O       10.0.2.0/24 [110/65] via 192.168.2.1, 00:01:20, Serial0/1/1
O       192.168.1.0/24 [110/128] via 192.168.2.1, 00:01:20, Serial0/1/1
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Serial0/1/1
L       192.168.2.2/32 is directly connected, Serial0/1/1
O       192.168.101.0/24 [110/129] via 192.168.2.1, 00:01:20, Serial0/1/1
    192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.102.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.102.1/32 is directly connected, GigabitEthernet0/0/0
S*    0.0.0.0/0 is directly connected, Serial0/1/1

```

Figure 8: Verifying OSPF Configuration on Router 2

Figure 8 verifies the OSPF routing protocol on Router 2.

Subnets that are directly connected are listed as C. OSPF routes are displayed with the code O.

3.2 Switch Configuration

Switches include SWR1, SWR2, SWR3, SWR4, SWL1, and SWL2 to facilitate the forwarding of data across the network. Key steps include:

3.2.1 Assigning Management IP Addresses:

These switches are provided with a management IP address for out of band management.

3.2.2 Configuring VLANs:

VLANs are used for the segmentation and traffic flow, while VLAN details vary with the network implementation plan.

```

-----
SWR1#show vlan brief

```

VLAN Name	Status	Ports
1 default	active	Gig1/0/1, Gig1/0/4, Gig1/0/6, Gig1/0/7 Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11 Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15 Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19 Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23 Gig1/0/24, Gig1/1/1, Gig1/1/2, Gig1/1/3 Gig1/1/4
2 VLAN0002	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```

SWR1#

```

Figure 9: VLAN Interfaces on Switch


```

SWR1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Gig1/0/2   on        802.1q         trunking    1
Gig1/0/3   on        802.1q         trunking    1
Gig1/0/5   on        802.1q         trunking    1

Port      Vlans allowed on trunk
Gig1/0/2   1-1005
Gig1/0/3   1-1005
Gig1/0/5   1-1005

Port      Vlans allowed and active in management domain
Gig1/0/2   1,2
Gig1/0/3   1,2
Gig1/0/5   1,2

Port      Vlans in spanning tree forwarding state and not pruned
Gig1/0/2   1,2
Gig1/0/3   none
Gig1/0/5   none

SWR1#

```

Figure 10: VLAN Trunk on Interfaces

3.3 Device Management

3.3.1 Accessing Devices:

All devices can be configured only through CLI or through SDN controller: All devices are capable of being configured only by using CLI or by being controlled through the SDN controller. SSH is used for accessing routers and switches using the command:

3.3.2 SDN Controller:

The SDN controller conveys and automates configurations on the network. Policy application, network topology identification, and scans are done through the controller port.

3.3.3 Network Monitoring and Logging

Network events and status are monitored by using system logs also known as syslog and other tools.

```

R1#show run | include logging
logging 192.168.101.100

```

Figure 11: Enabling Logging on Router

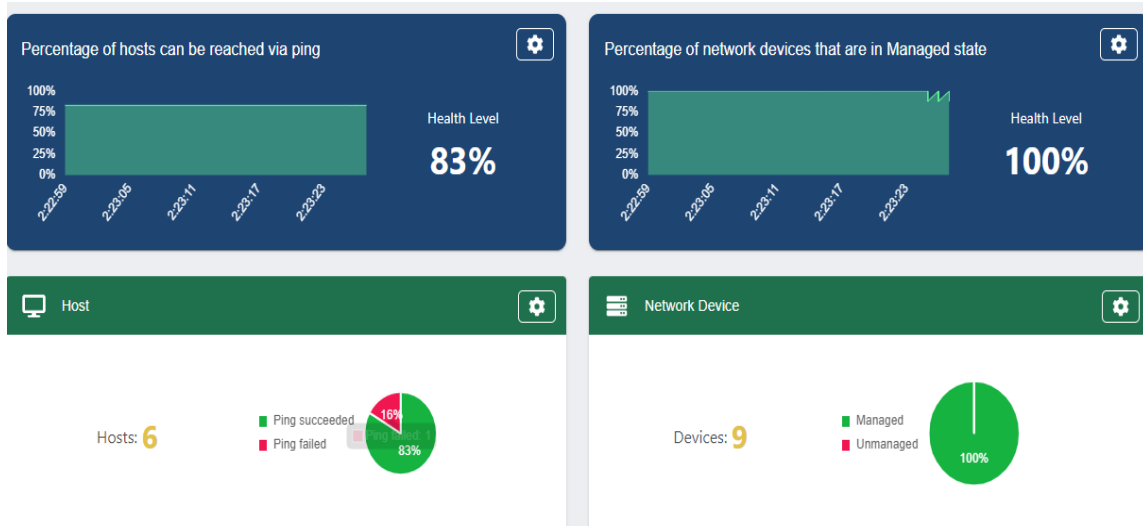


Figure 12: Network Controller Dashboard

CLI Credentials			+ CREDENTIAL
ID	Username	Description	Action
cb2c9f9c-9d81-48f5-ab52-1eb9723863f9	cisco	Admin credentials	

Figure 13: Network Controller Credentials

4 Command Line Interface Operations

The configuration, management and verification of the network devices, in the project, is done through the Command-Line Interface (CLI). CLI operations provide program management, hence making it an essential part of conventional networking management. This part describes various CLI activities carried out during the course of the project implementation.

4.1 Device Access and Authentication

Specifically, routers and switches used for management were connected using Secure Shell (SSH).

- Username: cisco
- Password: cisco123!

```

SWR4#show version | include RELEASE
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.2,
RELEASE SOFTWARE (fc4)
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.26, RELEASE SOFTWARE (P)
SWR4#ssh -l cisco 10.0.1.2

Password:

SWR1#show version | include RELEASE
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.2,
RELEASE SOFTWARE (fc4)
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.26, RELEASE SOFTWARE (P)
SWR1#ssh -l cisco 10.0.1.3

Password:

SWR2#show version | include RELEASE
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.2,
RELEASE SOFTWARE (fc4)
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.26, RELEASE SOFTWARE (P)
SWR2#ssh -l cisco 10.0.1.1

Password:

R3#show version | include RELEASE
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5,
RELEASE SOFTWARE (fc2)
R3#ssh -l cisco 192.168.1.2

Password:

R1#show version | include RELEASE
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5,
RELEASE SOFTWARE (fc2)
R1#ssh -l cisco 192.168.2.2

```

Figure 14: Verifying versions on Devices

4.2 Verification Commands

Verifications and corrections in the network setting were made using the following show commands.

- **Verify OSPF Neighbors**

```

R2#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
192.168.2.1      0     FULL/ -         00:00:34    192.168.2.1    Serial0/1/1
R2#

```

Figure 15: Verifying OSPF Neighbors on Router 2

- **View Device Status**

Summarizes the status of all interfaces of devices.

```

R1#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0  192.168.101.1  YES manual up          up
GigabitEthernet0/0/1  unassigned      YES unset  administratively down down
GigabitEthernet0/0/2  unassigned      YES unset  administratively down down
Serial0/1/0         192.168.1.2    YES manual up          up
Serial0/1/1         unassigned      YES unset  administratively down down
Vlan1             unassigned      YES unset  administratively down down

```

Figure 16: Router 1 Interface Brief

4.3 Debug Commands

For the purpose of real-time monitoring during the configuration, debug commands were used.

```

R2#debug ip ospf events
OSPF events debugging is on
R2#
23:30:00: OSPF: Rcv hello from 192.168.2.1 area 0 from Serial0/1/1 192.168.2.1
23:30:00: OSPF: End of hello processing
23:30:10: OSPF: Rcv hello from 192.168.2.1 area 0 from Serial0/1/1 192.168.2.1
23:30:10: OSPF: End of hello processing

```

Figure 17: Debugging Router 2 Events

```

C:\>ping 192.168.101.254

Pinging 192.168.101.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.101.254: bytes=32 time=1ms TTL=126
Reply from 192.168.101.254: bytes=32 time=1ms TTL=126
Reply from 192.168.101.254: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.101.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

```

Figure 18: Pinging the Network Controller

```
R1#show run | begin ip domain
ip domain-name www.example.com
ip name-server 192.168.101.100
!
!
spanning-tree mode pvst
!
!
!
!
!
!
```

Figure 19: Router DNS Config

5 Features of SDN Controller

The Software-Defined Networking (SDN) Controller is an innovative component that consolidates and oversees the network's control plane. In this project, the SDN controller offered several other new features, which promoted the improvement of the network on the aspects of offer, control, and utilization. Below are the key features utilized:

1. Centralized Network Management

- They are SDN controller which is used as a centralized point to view and control all the devices in a network including the switches and routers.
- It does away with the conventional configurations that require separate CLI on every device in the network thus boosting efficiency in network management.

2. Automated Device Discovery

- The controller can discover connect devices and network topology for the computer and laptop by itself.
- Information about the device interfaces, IP addresses, and the hardware properties, is presented in a clear format on the panel.

3. Path Tracing and Traffic Flow Analysis

- In the context of the controller, Path Tracing tools help to represent visually the flows of packets from source toward the destination devices.
- Actual path tracing (Pathtrace 1 and Pathtrace 2) were adopted in order to illustrate and assess routing and switching in the network.

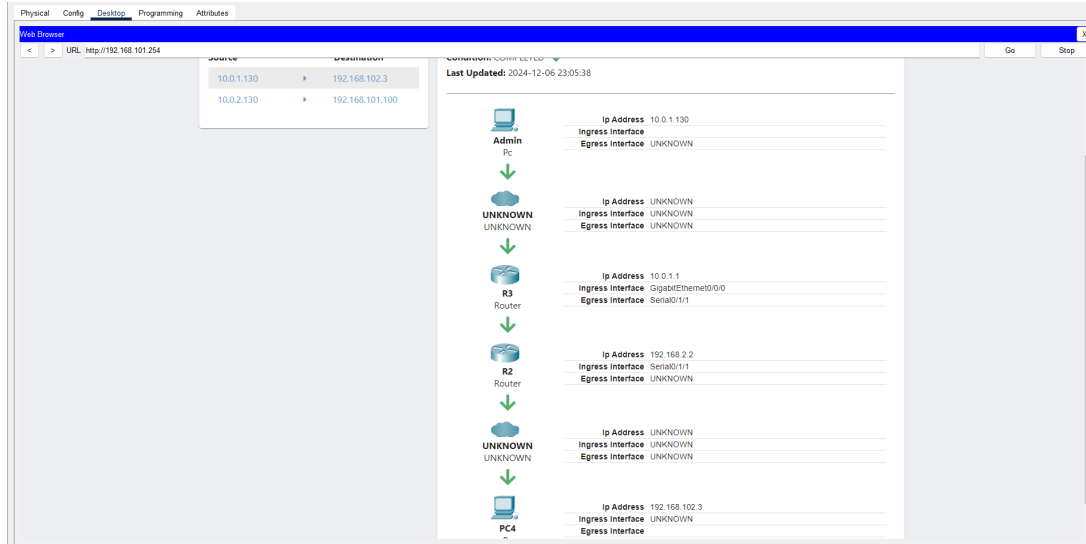


Figure 20: Tracing Path from 10.0.1.130 to 192.168.102.3

4. Secure Access and Credential Management

- The SDN controller has mechanisms for user authentication and ensures only permitted individuals change the network architecture.
- It has credential management for devices login in a centralize way to enhance security.

5. Policy Based Management

- These are easy to implement across the whole network using the controller through policies such as Access Control, QoS and traffic prioritization.
- It can be easily defined at the policy level and implemented instantly on multiple devices at once.

6 Comparative Analysis

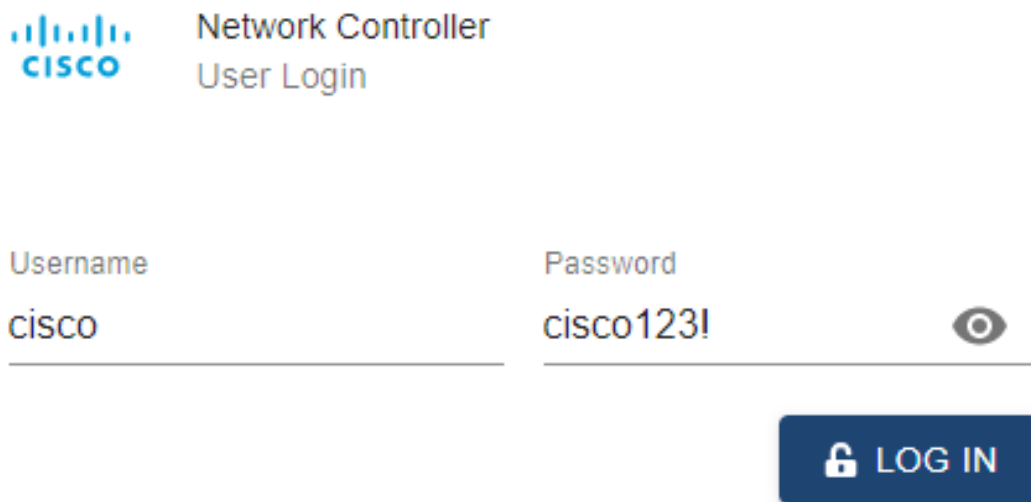
This part of the research focuses to compare the basic CLI operations with the enhanced functionality of the SDN Controller. Both approaches were used in the project to control and adjust the network, and below some characteristics of the compared approaches are presented in terms of the management, efficiency, and usability.

6.1 Configuration and Management

1. CLI Operations

Works on a command basis where the setting is made on a device-by-device basis. Currently, administrators must enter the network to each device to make changes separately. Manual configuration creates exposures for human errors in large wired and wireless network installations.

Example: Implementing OSPF routing on each router, whereby you enable OSPF routing by entering the network and router ospf commands.



Network Controller
User Login

Username: cisco

Password: cisco123!

LOG IN

Figure 21: Authentication when accessing controller

2. SDN Controller

The fact that there is a centralized organization, means that all the devices can be managed with this single method. It is used to minimize tasks that engage a large part of an individual's ingenuity, for instance, the policy updates or firmware.

A graphical user interface and the automatic application of policies result in reduced configuration time and minimization of errors.

6.2 Network Monitoring

1. CLI Operations

Monitoring is done by actual command typing on the individual devices (like show ip route, show logging etc).

Based on the results, logs and real-time data must be collected and analyzed for every device. Network blind spots; the topology and flow of traffic across the network

2. SDN Controller

This allows real-time network monitoring and assurance by using a single and easy-to-navigate dashboard. Gives a whole picture of the topology, revealing the statuses of the devices in the network, traffic patterns, and connection problems, if there are any.

Some of the features are Path Tracing for flow from end to end, which cannot be done directly on the CLI.

6.3 Troubleshooting and Debugging

1. CLI Operations

To troubleshoot, one must know commands, as well as configuration for the devices that are in use. Administrators ultimately use executable commands which include ping, traceroute and show outputs for debugging.

Some problems affect several devices: one must check each, leading to improved resolution time.

2. SDN Controller

The approach of logging and tracking provides significant events and easy identification of the root cause. Complex solutions such as Path Tracing, real-time notifications, graphs make it easier to identify and solve problems.

Even when it comes to log correlation from individual devices, time is saved since all log messages are channeled through Syslog.

6.4 Security and Access Control

1. CLI Operations

The fact is device credentials have more unique identities, and this raises the administrative costs. The biggest drawback of access control is that access is controlled at the device level, and this is relative to the network.

2. SND Controller

Eliminates a single point of failure for network authentication and supplies RBAC to the whole network. This makes the handling of credentials easier and more secure in that it cuts across inconsistencies. Records user exercise for transparency purposes.

6.5 Scalability

1. CLI Operations

New devices' integration or networking expansion involve manually setting up configuration of the new device. As the scale goes up, we have more people involved, more effort, and it takes more time, which makes the network more vulnerable to errors.

2. SDN Controller

Automates the process of finding and configuring devices to support organisational scalability quickly and easily. Both new and the existing devices can set similar policies and settings with multiple devices given a similar policy or setting at the same time. Make large scale networks expansion easier.