



**KOLEJ PROFESIONAL MARA BERANANG**

**DIPLOMA IN COMPUTER SCIENCE (DCS)**

---

<b>COURSE NAME</b>	: LOCAL AREA NETWORKING TECHNOLOGIES
<b>COURSE CODE</b>	: CSC2773
<b>ACADEMIC SESSION</b>	: SESSION 1 2024
<b>TYPE OF ASSESSMENT</b>	: ASSIGNMENT 1
<b>DURATION</b>	: 2 WEEKS (07/05/2024 – 28/05/2024)

---

**CLO 2:** Analyse LAN issues using suitable LAN performance measurement tools and troubleshooting methodology. (C4, PLO2)

**INSTRUCTION TO CANDIDATES:**

1. This assessment consist of 4 tasks. Answer ALL the task given.
2. Any late submission will be penalized.
3. **Report** should be written in using:

Font type for content: Arial

Size for content: 11 pts

Size for title: 12 pts

Line Spacing: 1.5

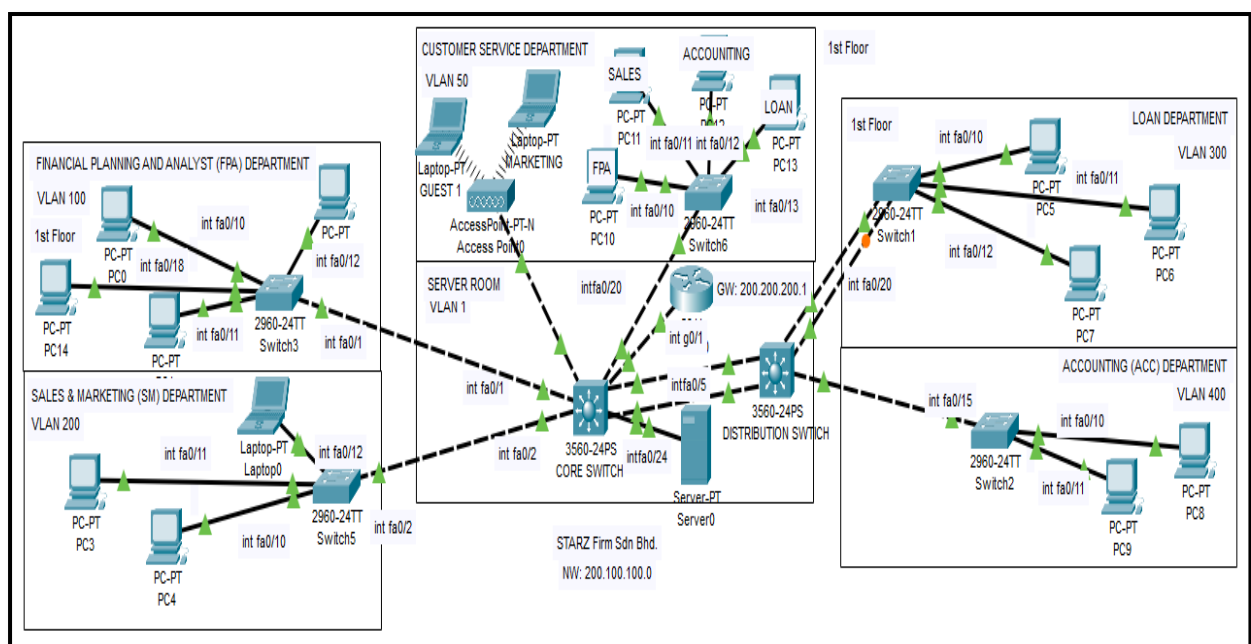
Content: Consistently organized

Personal Details	
<b>Name</b>	MUHAMMAD EQMAL BIN NOOR RANIZ
<b>I/D Number</b>	BCS2211-026
<b>Class</b>	DCS 5B
<b>Lecturer</b>	PN. SITI AZEYRAH BT RAMLI

Section / Question No.	Marks
Task 1	
Task 2	
Task 3	
Task 4	
<b>Total</b>	<b>/40</b>

## Scenario

STARZ Firm Sdn. Bhd. is an accounting firm in Beranang. This company consist of 4 different departments that have their own networking system and broadcast domain. The departments involve are Financial Planning and Analysis, Sales and Marketing, Loan and Accounting department. The company provides loan services and accounting services. Currently, the company has a customer service level located on the 1<sup>st</sup> floor that is exposed to the end users and guests of this firm. Due to the lack of experience of the new staff hired by the company, the existing network of this company has become unstable and has created errors. Figure 1.0 shows the STARZ Firm Sdn Bhd. network.



**Figure 1.0: STARZ Firm Sdn Bhd.**

As the company's new IT support, you have been appointed by the network administrator to analyse the existing network problem and troubleshoot the problem using any suitable Local Area Networking (LAN) technology to solve the problem. You are required to identify the possible problems by using troubleshooting methodologies. Finally, you are required to recommend any appropriate tools for monitoring and testing the network's configuration.

**Task:**

Below are the tasks that you need to do in order to manage the LAN infrastructure for the new network system design at STARZ Firm network:

1. Analyse any **two (2)** issues that could happen in the access layer connectivity by using troubleshooting methodology.
2. Analyse any **two (2)** issues that could happen in core/distribution layer connectivity connection to the buildings by using troubleshooting methodology.
3. Choose a suitable **network monitoring** tool to monitor the performance of LAN in STARZ Firm network.
4. Choose a suitable tool to monitor **user access** performance issues in the LAN in the STARZ Firm network.

## Assessment Rubrics:

Task		Mark				Mark Obtained
1.	Analyse any <b>two (2)</b> issues that could happen in the access layer connectivity by using troubleshooting methodology.					
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	
	i. Define the problem.	Identify any <b>one (1)</b> issue or problem that occurs in in the access layer connectivity.	Explain any <b>two (2)</b> issues or problems that occur in the access layer connectivity.			
	ii. Gather detailed information.	Explain any <b>one (1)</b> general symptom of the issue or problem.	Briefly explain <b>two (2)</b> symptoms that relate to the <b>two (2)</b> issues or problems.	Explain in detail <b>two (2)</b> symptoms that relate to the <b>two (2)</b> issues or problems.		
	iii. Consider probable cause for the failure.	Explain <b>one (1)</b> cause of the issue or problem from <b>one (1)</b> issue or problem.	Explain <b>two (2)</b> causes that relate to the <b>two (2)</b> issues or problems correctly.			
	iv. Create a plan to solve the problem.	Explain <b>one (1)</b> possible solution to solve <b>one (1)</b> issue or problem.	Explain <b>two (2)</b> possible solutions to solve <b>two (2)</b> issues or problems.  Explain a suitable troubleshooting approach for each of the identified issues.			
	v. Implement the plan.	Explain all detail steps involved in solving <b>one (1)</b> issue or problem.	Briefly explain the general steps involved in solving the <b>two (2)</b> issues or problems.	Explain all the detailed steps involved in solving the <b>two (2)</b> issues or problems.		
	vi. Observe the results of the implementation.	Explain the result generally based on the problem solving that apply the <b>one (1)</b> issue or problem.	Explain the result based on the problem solving that apply to the <b>two (2)</b> issues or problems.			
	vii. Document the changes made to solve the problem.	Partially provide correct documentation format.	Provide a good and correct documentation format. The content is well-constructed and consistently presented.			

Task		Mark				Mark Obtained
2.	Analyse any <b>two (2)</b> issues that could happen in the core/distribution layer connectivity to the buildings by using troubleshooting methodology.					
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	
	i. Define the problem.	Identify any <b>one (1)</b> issue or problem that occurs in the distribution/core layer connectivity.	Explain any <b>two (2)</b> issues or problems that occur in the distribution/core layer connectivity.			
	ii. Gather detailed information.	Explain any <b>one (1)</b> general symptom of the issue or problem.	Briefly explain <b>two (2)</b> symptoms that relate to the <b>two (2)</b> issues or problems.	Explain in detail <b>two (2)</b> symptoms that relate to the <b>two (2)</b> issues or problems.		
	iii. Consider probable cause for the failure.	Explain <b>one (1)</b> cause of the issue or problem from <b>one (1)</b> issue or problem.	Explain <b>two (2)</b> causes that relate to the <b>two (2)</b> issues or problems correctly.			
	iv. Create a plan to solve the problem.	Explain <b>one (1)</b> possible solution to solve <b>one (1)</b> issue or problem.	Explain <b>two (2)</b> possible solutions to solve <b>two (2)</b> issues or problems.  Explain a suitable troubleshooting approach for each of the identified issues.			
	v. Implement the plan.	Explain all detailed steps involved in solving <b>one (1)</b> issue or problem.	Briefly explain the general steps involved in solving the <b>two (2)</b> issues or problems.	Explain all the detailed steps involved in solving the <b>two (2)</b> issues or problems.		
	vi. Observe the results of the implementation.	Explain the result generally based on the problem solving that apply the <b>one (1)</b> issue or problem.	Explain the result based on the problem solving that apply to the <b>two (2)</b> issues or problems.			

Task		Mark				Mark Obtained
	vii. Document the changes made to solve the problem.	Partially provide correct documentation format.	Provide a good and correct documentation format. The content is well-constructed and consistently presented.			
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	
3.	Choose a suitable <b>network monitoring</b> tool to monitor the performance of LAN in STARZ Firm network.	Predict a suitable <b>Network Monitoring</b> tool for the given scenario.	<p>Predict a general network performance issue for the given scenario.</p> <p>Choose a suitable <b>Network Monitoring</b> tool for handling the above issue to show its effectiveness (at least one (1)) in relation to the scenario.</p> <p>Attach references from the Internet.</p>	<p>Predict a network performance issue that is possible to occur in the given scenario.</p> <p>Choose a suitable <b>Network Monitoring</b> tool for handling the above issue to show its effectiveness (at least one (1)) in relation to the scenario.</p> <p>Attach references from the Internet.</p>	<p>Predict a network performance issue that is highly likely to occur in the given scenario.</p> <p>Choose a suitable <b>Network Monitoring</b> tool for handling the above issue to show its effectiveness (at least two (2)) in relation to the scenario.</p> <p>Attach references from the Internet.</p>	

Task		Mark				Mark Obtained
		1	2	3	4	
4.	Choose a suitable tool to monitor <b>user access</b> performance issues in the LAN in the STARZ Firm network.	Predict a suitable <b>User Access</b> performance tool for the given scenario.	<p>Predict a general user access performance issue for the given scenario.</p> <p>Choose a suitable <b>User Access</b> performance tool for handling the above issue to show its effectiveness (at least one (1)) in relation to the scenario.</p> <p>Attach references from the Internet.</p>	<p>Predict a user access performance issue that is possible to occur in the given scenario.</p> <p>Choose a suitable <b>User Access</b> performance tool for handling the above issue to show its effectiveness (at least two (2)) in relation to the scenario.</p> <p>Attach references from the Internet.</p>	<p>Predict a user access performance issue that is highly likely to occur in the given scenario.</p> <p>Choose a suitable <b>User Access</b> performance tool for handling the above issue to show its effectiveness (at least two (2)) in relation to the scenario.</p> <p>Attach references from the Internet.</p>	
Total Marks Earned						/ 40
Total Percentage (30%)						

**TASK 1:** Analyze Any Two (2) Issues That Could Happen in The Access Layer Connectivity By Using Troubleshooting Methodology.

**First Issue:** Incorrect Vlan Assignment at Sales and Marketing (SM) Department.

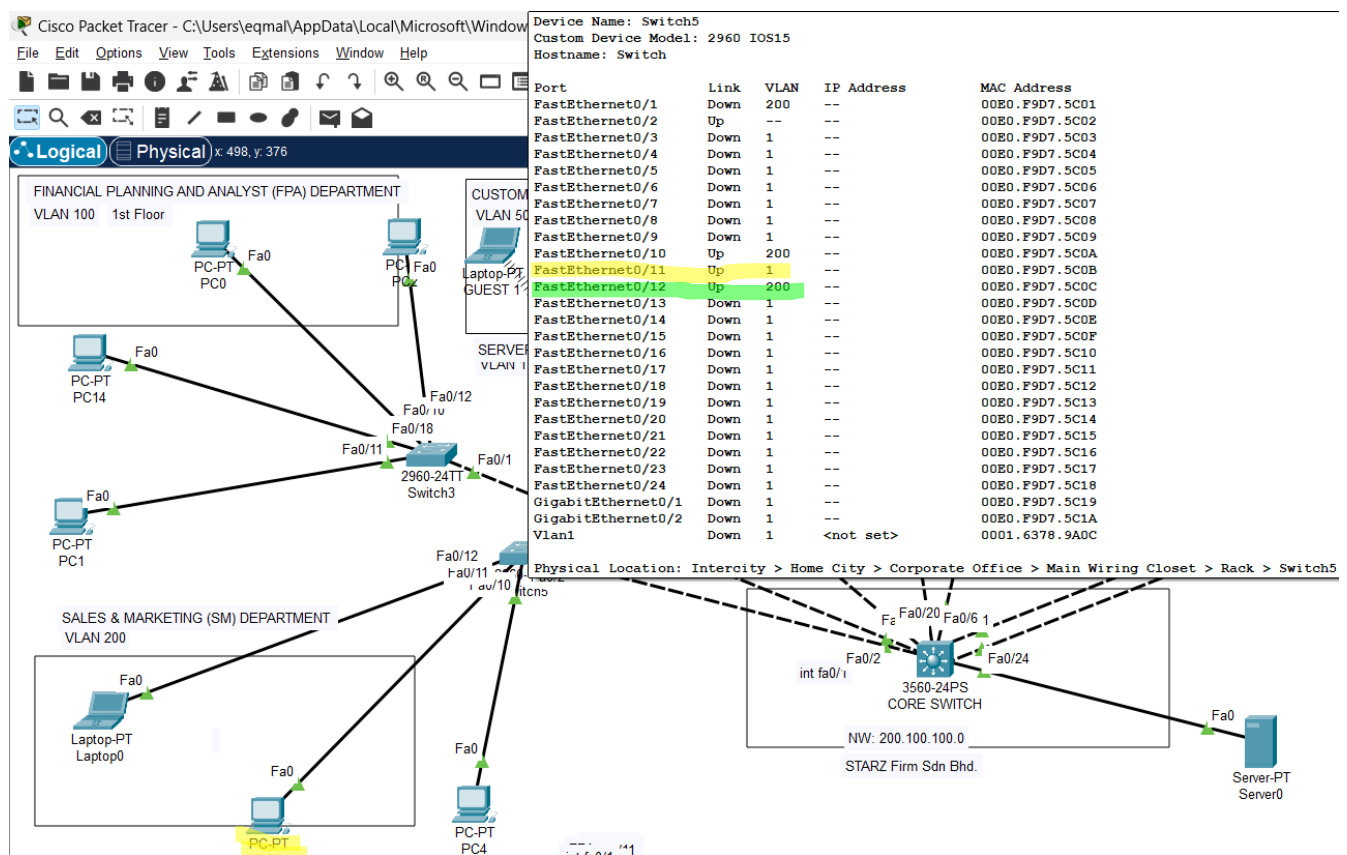
### Problem Faced:

#### I) Inability to Communicate with Department Resources

The misconfigured computer on VLAN 1 will be unable to communicate with other devices in the Sales and Marketing department that are correctly configured on VLAN 200.

#### II) Access to Incorrect Network Resources

The misconfigured computer on VLAN 1 might gain access to network resources that are not intended for the Sales and Marketing department, potentially leading to security concerns or unauthorized access.





## **Detailed Problem Information**

**I)** The reason for the incapacity to communicate with department resources is the isolation of VLAN 1 and VLAN 200. Only devices on the same VLAN may connect with each other, including devices fa0/11 on VLAN 1 and the other PC on VLAN 200. Because the Sales and Marketing department's devices, services, and resources are properly configured on VLAN 200, a computer configured on VLAN 1 will not be able to access them. Many operational problems, such the inability to access shared disks, internal apps, or departmental printers, are caused by this misconfiguration.

**II)** Access to the wrong network resources raises serious security issues. It is possible that computer fa0/11 on VLAN 1 will unintentionally access resources that are not meant for the department of sales and marketing. Due to this misconfiguration, sensitive data and important systems from other departments may become accessible to unauthorized parties. Incorrect VLAN assignments can compromise the departmental role-based access control and limitation that VLANs are intended to provide. Unauthorized access to private documents, corporate databases, or administrative tools intended for other departments are examples of potential threats. Data security is jeopardized, and there is also a chance of data leakage and noncompliance with company policies and data protection laws.

## **Cause For the Failure:**

### **I) Misconfigured Switch Port**

Human error could occur during configuring. Human error is possible while manually configuring switch ports by a network administrator. Since many network switches use VLAN 1 as their default VLAN, it is possible for a port intended for VLAN 200 to accidentally be configured for VLAN 1. A switch port may default to VLAN 1 if it is not specifically configured for VLAN 200, which could lead to misconfiguration.

### **II) Incorrect VLAN Tagging on the Computer's Network Interface**

Error with Manual VLAN Tagging VLAN tagging can be manually configured on the computer's network interface card (NIC). The PC will be misconfigured if VLAN 1 is configured instead of VLAN 200 due to the incorrect VLAN ID. moreover, there might be Error in Automated Deployment Script When network interface configuration is automated in environments using deployment scripts, a typo in the script may cause the NIC to be assigned the incorrect VLAN ID.

```
Switch>show vlan
```

VLAN Name		Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/11 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
200	SM_DEPT	active	Fa0/1, Fa0/10, Fa0/12
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
200	enet	100200	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0

--More--

Copy

Paste

## Plan To Solve the Problem:

### I) Follow the Path Approach

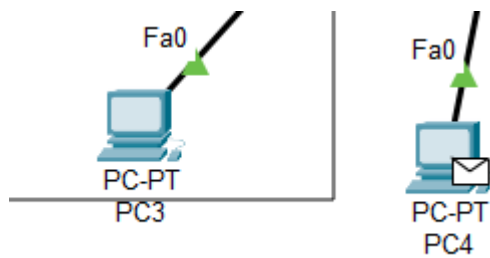
To move the PC from VLAN 1 to VLAN 200, first, find the computer and note its details, like its IP address or MAC address. Then, trace the network connection from the PC to the switch it's plugged into. You can use network management tools to help with this. Once you identify the switch and the specific port the PC is connected to, log into the switch and change the port's VLAN setting from VLAN 1 to VLAN 200. After making the change, verify that the PC is now on VLAN 200 by checking the switch settings and testing the PC's network connectivity.

## Implement The Plan

### Reconfigure the Misconfigured Computer

```
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int Fa0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switch access vlan 200
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

After Reconfigure the Misconfigured Computer It Can Send and Receive Data Normally



Successful PC4 PC3 ICMP 0.000 N 11 (edit)

### Implement Port Security with VLAN Assignment

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface Fa0/11
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down

Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Following the implementation of port security, access will be restricted.

```
Switch#show port-security interface Fa0/11
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 000A.4114.74D8:200
Security Violation Count : 0
```

## Result Of the Implementation

### Reconfigure the Misconfigured Computer

Correct VLAN membership, better network segmentation, increased security, effective use of network resources, adherence to network policies, and potential conflict avoidance are all achieved by reconfiguring the incorrectly configured PC to VLAN 200. This modification preserves the overall integrity and performance of the local area network (LAN) by guaranteeing that the computer operates as intended inside its assigned network segment.

```
Switch>show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
200 SM_DEPT	active	Fa0/1, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
200	enet	100200	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0

```
Switch>
```

## Implement Port Security with VLAN Assignment

By imposing limitations based on MAC addresses, port security with VLAN assignment improves network security. By automatically allocating devices to the correct VLAN according to their MAC address, this system lowers the possibility of security breaches and stops illegal access to other VLANs.

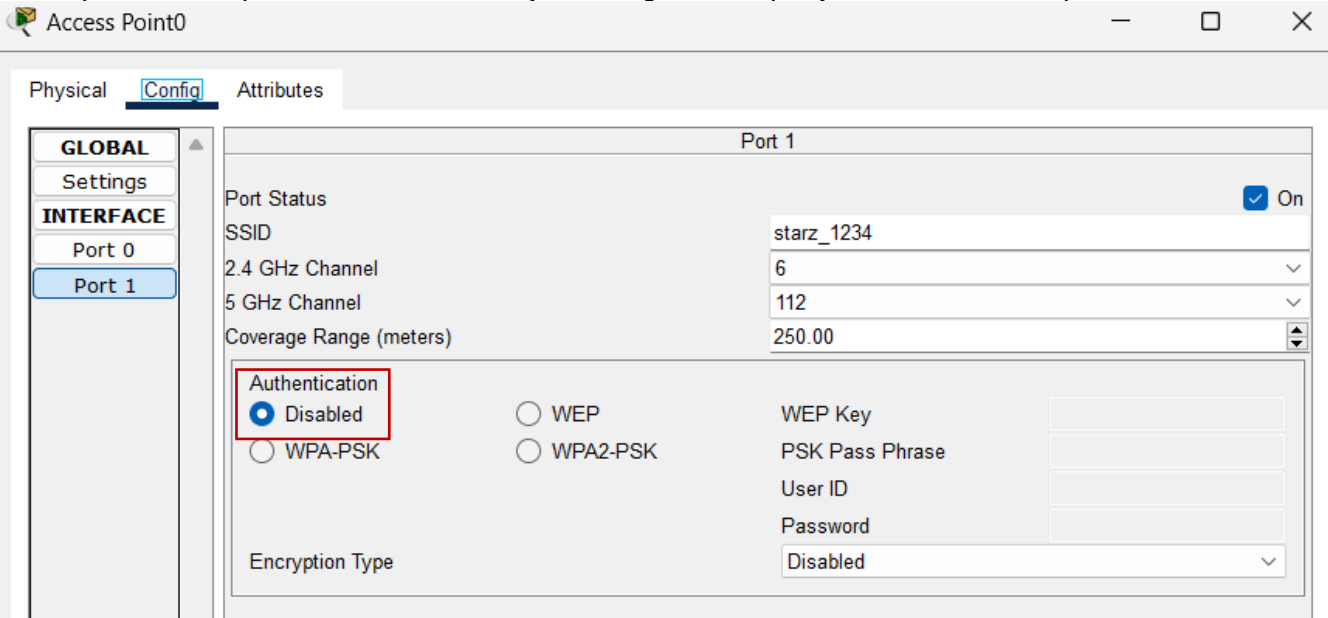
```
Switch#show port-security interface Fa0/11
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 000A.4114.74D8:200
Security Violation Count : 0
```

**Second Issue:** At the customer service department's access point, there is no security or password.

**Problem Faced:**

I) Data Breach

The customer care department's access point could have serious issues if security precautions like passwords are missing. Without adequate security, unauthorized users could gain easy access to the system, which could result in data breaches when private client information is exposed. This vulnerability may lead to financial fraud, identity theft, and a decline in client confidence. Furthermore, if security protocols aren't in place, bad actors could change or remove important data, interfering with the department's operations and seriously harming the company's finances and reputation.



**Detailed Problem Information**

One major issue is that the customer service department's access point lacks security safeguards like passwords. Sensitive client data is at risk because without these safeguards, unauthorized users from the two customer service laptops might simply access the system. Identity theft, financial fraud, and the sale of personal information on the dark web are possible outcomes of this. Furthermore, hackers might alter or remove crucial data, which would interfere with departmental operations and cause a delay in responding to client requests. Legal repercussions, fines, and expensive repairs may follow from this.

## Cause For the Failure

### I) Lack of Awareness

Lack of knowledge about cybersecurity is one of the main reasons the customer service department's access point lacks security measures like passwords. Workers might not be aware of the hazards, such as data breaches and unauthorized access, or how crucial it is to secure these locations. This ignorance is frequently caused by insufficient cybersecurity training and communication. Employees who don't receive regular cybersecurity training tend to focus on their current tasks and ignore critical security procedures because they believe there isn't a threat right now.

## Plan To Solve the Problem:

### I) Follow the Path Approach

The "Follow the Path" approach involves understanding the current situation, identifying the root causes, and implementing targeted solutions. We need to identify all access points to the customer service department and examine the existing security measures in place, if any. Next, it's crucial to determine why there is no security or password. This could be due to oversight, resource limitations, or a deliberate decision based on perceived needs. Once we have a clear understanding of the situation, we can proceed to implement appropriate security measures. For example, setting up a secure Wi-Fi network with a strong password, implementing access control systems like key cards or biometric authentication, and educating staff on the importance of maintaining security protocols. Continuous monitoring and periodic reviews are essential to ensure that the implemented measures remain effective and up to date with evolving security standards.

## Implement The Plan

Click On the Access Point and Enable the Authentication Option

The screenshot displays a network configuration interface with three tabs: 'Physical', 'Config' (selected), and 'Attributes'. On the left, a sidebar shows 'GLOBAL' and 'INTERFACE' sections. Under 'INTERFACE', 'Port 1' is selected. The main area is titled 'Port 1' and contains the following settings:

- Pass Phrase**: A red error message states 'Pass Phrase should not be empty.' A checkbox labeled 'On' is checked.
- Port Status**: A checkbox labeled 'On' is checked.
- SSID**: A text field containing 'starz\_1234'.
- 2.4 GHz Channel**: A dropdown menu set to '6'.
- 5 GHz Channel**: A dropdown menu set to '112'.
- Coverage Range (meters)**: A text field containing '250.00'.
- Authentication**: A section with four radio buttons: 'Disabled', 'WEP', 'WPA-PSK', and 'WPA2-PSK'. The 'WPA2-PSK' option is selected and highlighted with a red box.
- Encryption Type**: A dropdown menu set to 'AES'.
- WEP Key**: A text field.
- PSK Pass Phrase**: A text field.
- User ID**: A text field.
- Password**: A text field.

Enter The Desired Password and Save It

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status

On

SSID

starz\_1234

2.4 GHz Channel

6

5 GHz Channel

112

Coverage Range (meters)

250.00

Authentication

Disabled

WPA-PSK

WEP

WPA2-PSK

WEP Key

PSK Pass Phrase

CSDAP2024

User ID

Password

Encryption Type

AES

Result Of the Implementation

Implementing a password at the customer service department's access point significantly enhances the overall security posture of the organization. It protects sensitive data, improves network performance, ensures regulatory compliance, and builds customer trust. While there may be some challenges during the initial implementation phase, the long-term benefits far outweigh these temporary hurdles. Regular updates and employee training are essential to maintaining the effectiveness of the password and ensuring the ongoing security of the network.

Wireless Network Name

CH

Signal

starz\_1234

1

95%

Site Information

Wireless Mode

Infrastructure

Network Type

Mixed B/G/N

Radio Band

Auto

Security

WPA2-PSK

MAC Address

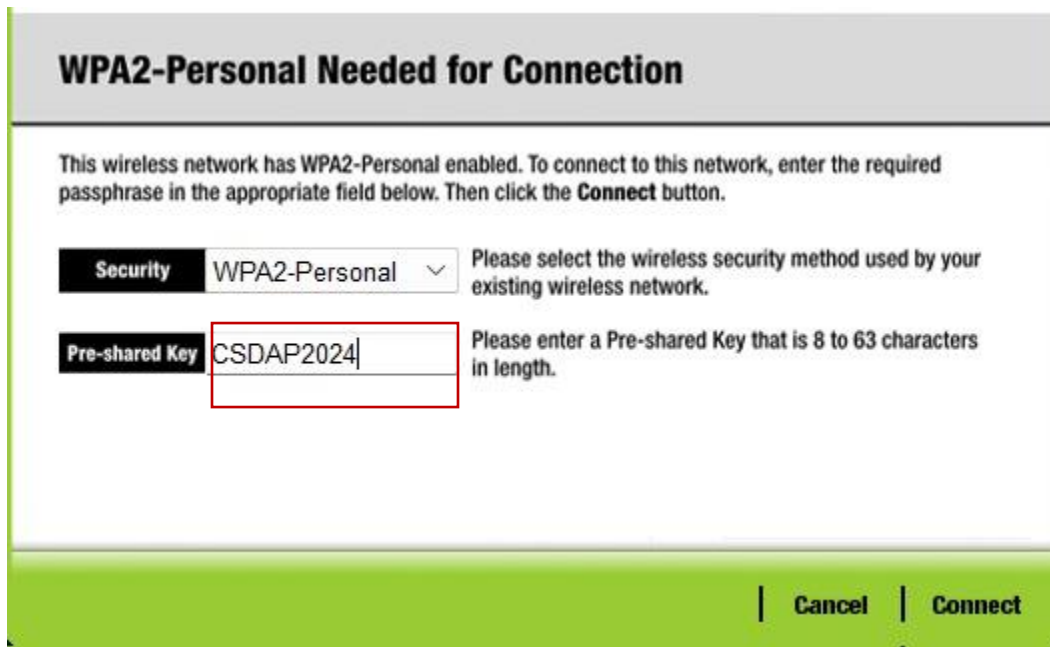
00E0.B088.9710

Refresh

Connect



After Applying The Password At The Access Point The Computer That Want To Access It Must Key In The Password First Before They Can Use It.



**WPA2-Personal Needed for Connection**

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

**Security** WPA2-Personal  Please select the wireless security method used by your existing wireless network.

**Pre-shared Key** CSDAP2024 Please enter a Pre-shared Key that is 8 to 63 characters in length.

Prove That After the Computer Key In The Password They Could Use The Internet.



**TASK 2:** Analyze any two (2) issues that could happen in the core/distribution layer connectivity to the buildings by using troubleshooting methodology.

### First Issue: EtherChannel Not Applied at Core Switch and Distribution Switch

### Problem Faced:

### I) No Load Balancing

There Would Be No Load Balancing Among the Several Links If EtherChannel Didn't Exist. Congestion And Less-Than-Ideal Network Performance May Result from All Traffic Passing Through the One Active Link Between the Two EtherChannel Connected To The Core Switch And Distribution Layer Switch. Conversely, Traffic Can Be Dispersed Throughout All Bundled Links Via EtherChannel, Which Improves Load Balancing and Increases Aggregate Bandwidth.

## II) Spanning Tree Protocol (STP) Blocking

The Spanning Tree Protocol (STP) treats each physical link as a separate link in the absence of EtherChannel. STP blocks redundant pathways, which keeps a network free of loops. To stop a loop, one of the two wires that connects the distribution layer switch and access layer switch STP will be blocked. This implies that the bandwidth of the second link will be wasted and that only one link will be active at a time.

```
Switch#en
Switch#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 0
Number of aggregators:          0
```

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

Switch#

```

Switch#
Switch#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SD)          LACP        Fa0/5 (I) Fa0/6 (I)
Switch#

```

## Detailed Problem Information

Change Switch at the distribution layer and at the core layer the two cables that connect them are fa0/5 and fa0/6. Data from Switch at core layer to Switch at distribution layer can only use one cable at a time without EtherChannel. This indicates that fa0/6 is left empty if data passes through fa0/5. The active cable (such as fa0/5) may become overwhelmed with increased traffic, leading to delays and congestion. Fa0/5 and Fa0/6 work together as a single large wire when using EtherChannel. More evenly distributed data means that no single cable is overloaded. This increases the reliability and speed of data transport, particularly on crowded networks.

## Cause For the Failure

### EtherChannel Not Configured

All network traffic between switches must pass over a single cable at a time if EtherChannel is not configured between them. When a lot of data is flowing over the cable, this may cause it to get overwhelmed. The other cable is idle in the absence of EtherChannel. This reduces the network's efficiency and wastes potential bandwidth. There is also no fallback option in the event that the active cable fails without EtherChannel. If there's an issue with that one cable, this might bring down the network.

## At Core Switch EtherChannel Not Configured

```
Switch#en
Switch#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 0
Number of aggregators:           0
```

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

-----+-----+-----+-----
-------------------------

Switch#

### Plan To Solve the Problem:

#### Spot The Difference Approach

To apply and reconfigure EtherChannel on both the Core Switch and Distribution Switch using the "Spot the Difference" approach, we'll start by gathering and documenting the current configurations of both switches. Then, we'll outline the desired EtherChannel settings for each switch.

Next, we'll compare the current configurations with the desired ones to identify any differences. Once we spot these discrepancies, we'll plan the necessary adjustments and make sure they are compatible with existing network protocols.

For the Distribution Switch, we'll access it and modify the EtherChannel settings to match the desired configuration. This includes adjusting port assignments, load-balancing methods, and EtherChannel modes as needed. After making the changes, we'll verify the new configuration to ensure it aligns with our desired state.

We'll follow a similar process for the Core Switch, making the necessary adjustments to its EtherChannel settings and verifying the configuration.

After reconfiguring both switches, we'll conduct tests to ensure that EtherChannel is working correctly and providing the expected performance and resilience. We'll monitor the network performance to make sure everything is stable and make any necessary adjustments based on our findings.

Finally, we'll document all the changes made to the EtherChannel configurations for future reference, detailing the port settings, load-balancing methods, and any other adjustments we made. This approach helps us systematically reconfigure EtherChannel, ensuring the network is optimized and resilient.

## Implement The Plan

Before executing the other plan, switchport must first be changed to trunk encapsulation.

```
Switch(config)#interface fa0/5
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#exit
Switch(config)#exit
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/6
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

**Configure It for Each Physical Cable That Is Connected to The Two Switch.**

**After That Execute EtherChannel Configuration at Distribution layer**

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/5-6
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-3-UPDOWN: Interface Port-channel1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#int port-channel 1
Switch(config-if)#s
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

% Ambiguous command: "s"
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
```

## Next Configure the EtherChannel Configuration At The Core Layer

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/5
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/6
Switch(config-if)#switchport
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with Switch
FastEthernet0/1 (1).

Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with Switch
FastEthernet0/1 (1).

Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/5-6
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#int port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```



## Result Of the Implementation

Apply And Reconfigure EtherChannel at Core Switch and Distribution Switch

When you configure EtherChannel, you are integrating several physical links into a single logical connection between the distribution and core switches. This increases bandwidth and guarantees traffic flow even in the event of a link failure. It is imperative that both switches have identical configurations to avoid network issues. For improved network efficiency and dependability after setup, you'll keep an eye on traffic distribution and make sure everything is operating as it should.

```
Switch#shown eth summary
^
% Invalid input detected at '^' marker.

Switch#show eth summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          LACP       Fa0/5(P) Fa0/6(P)
Switch#
```

(At Core Layer and Distribution Layer)

## **Second Issue: Native Vlan Switch 3 Mismatch with Core Switch**

### **Problem Faced**

#### **I) Communication Failures**

Inappropriate handling of untagged frames might cause intermittent connectivity problems or communication failures on networked devices. Degradation in service quality or possible outages may result from this impacting the performance and dependability of the network. In particular, these problems may be made worse by a natural VLAN mismatch between the core switch at Starz Firm SDN BHD and Switch 3 at the distribution layer. To ensure the best possible network performance and dependability, it is essential to make sure that the VLAN configuration and alignment between these switches are correct.

```
%CDP-4-NATIVE VLAN MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with Switch FastEthernet0/1 (99)
```

### **Detailed Problem Information**

Devices on the network might experience communication failures or intermittent connectivity issues due to improper handling of untagged frames. This can negatively impact network performance and reliability, potentially leading to downtime or degraded service quality. One common issue is a native VLAN mismatch, which occurs when the native VLAN configuration on Switch 3 at the distribution layer does not match the configuration on the core switch at Starz Firm SDN BHD. For instance, on Switch 3, port fa0/1 is set to native VLAN 99, while the other ports are set to native VLAN 1. This mismatch can cause untagged frames to be improperly routed, resulting in communication failures and connectivity problems. To prevent these issues, it is essential to ensure that the native VLAN settings are consistently configured across all switches in the network, particularly between Switch 3 and the core switch. Proper VLAN alignment will help maintain optimal network performance and reliability.

### **Cause For the Failure**

#### **I) Misconfigured VLAN Settings**

A network infrastructure discrepancy inside Starz Firm SDN BHD has resulted from an incorrect configuration of the native VLAN settings on switch 3's fa0/1 port. More specifically, fa0/1 at both the distribution and core layers has been mistakenly changed to VLAN 99, even though interfaces across other components are configured to function on native VLAN 1. This discrepancy in VLAN setup interferes with network segmentation and may jeopardize the organization's operational effectiveness and network security.



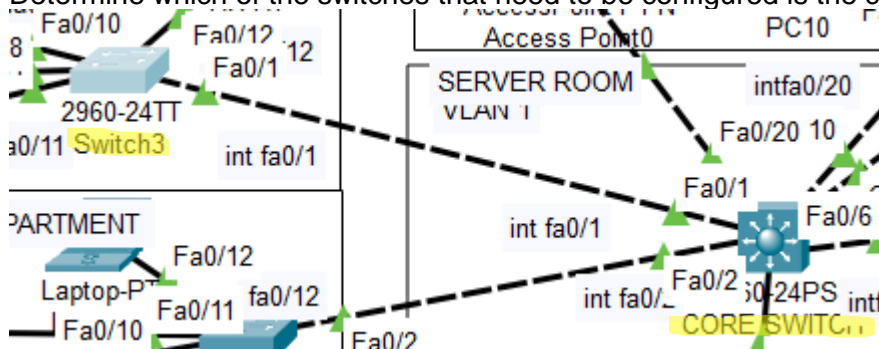
## Plan To Solve the Problem

### Spot The Difference

To understand the current setup, begin by analyzing the existing VLAN configuration. Focus on identifying VLAN 99, the one that needs adjustment. This VLAN should be changed to VLAN 1, aligning with the other VLANs, based on network expansion or specific requirements. To minimize disruptions during this reconfiguration, it's important to work closely with the relevant parties. For effective network management, plan new subnet and VLAN assignments. Document all changes in detail to provide a reference for future use and troubleshooting. Before making these VLAN changes live, test them in a controlled environment to ensure they work as expected. Communicate the planned changes to everyone involved, and if necessary, schedule downtime to implement them. After making the changes, monitor the network's performance to ensure everything is functioning correctly. First, analyze the current VLAN configuration to identify VLAN 99. Next, compare it with the setup of the other VLANs, which are set to VLAN 1. Spot the difference and make the necessary adjustment by changing VLAN 99 to VLAN 1. Collaborate with stakeholders to plan and minimize disruption, document all changes meticulously, test the adjustments in a controlled environment, notify all involved parties, arrange for any required downtime, and monitor the network post-implementation to confirm it is performing as expected.

### Implement The Plan

Determine which of the switches that need to be configured is the core switch first.



Configure The Mismatched Vlan To Match With The Others

```

Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%CDP-4-NATIVE VLAN MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with Switch
FastEthernet0/1 (1).

Switch(config-if)#switchport trunk native vlan 1
Switch(config-if)#end
Switch#
%SYS-5-CONFIG I: Configured from console by console

```

## Result Of the Implementation

Following the VLAN reconfiguration, the network ought to have better organization and segmentation. By improving traffic isolation, broadcast storms will be less likely to occur and network performance will be improved overall. VLAN and subnet allocations will be more clearly defined, leading to more efficient management of network resources. There won't be any interruptions to communication between various network components during and after the changeover. All things considered, the deployment ought to produce a more reliable and expandable network architecture that efficiently satisfies both present and future operating requirements.

```
Switch#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol	on	802.1q	trunking	1
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
Fa0/10	auto	n-802.1q	trunking	1
Fa0/20	on	802.1q	trunking	1

```
Port Vlans allowed on trunk
```

Pol	1-1005
Fa0/1	1-1005
Fa0/2	1-1005
Fa0/10	1-1005
Fa0/20	1-1005

```
Port Vlans allowed and active in management domain
```

Pol	1,100,200,400
Fa0/1	1,100,200,400
Fa0/2	1,100,200,400
Fa0/10	1,100,200,400
Fa0/20	1,100,200,400

```
Port Vlans in spanning tree forwarding state and not pruned
```

```
--More--
```

**Task 3:** Choose a suitable **network monitoring** tool to monitor the performance of LAN in STARZ Firm network.

Predicted Network Performance Issue:

Bandwidth saturation during peak usage times, causing slowdowns in cloud-based application access and data transfer speeds.

Suitable Network Monitoring Tools:

PRTG Network Monitor is a robust choice for addressing and mitigating such network performance issues. Here are two key features of PRTG Network Monitor that demonstrate its effectiveness in handling bandwidth saturation:

Bandwidth Monitoring and Analysis:

PRTG Network Monitor excels in monitoring bandwidth usage across the network in real-time. It provides detailed insights into which applications or users are consuming the most bandwidth during peak hours. With customizable alerts and thresholds, network administrators can proactively identify potential bottlenecks before they impact user experience. PRTG's graphical representation of bandwidth usage over time allows administrators to pinpoint trends and forecast future capacity needs, ensuring that bandwidth resources are optimized and performance issues are minimized.

Quality of Service (QoS) Monitoring:

Another crucial feature of PRTG is its ability to monitor Quality of Service parameters. QoS monitoring allows administrators to prioritize critical traffic such as cloud-based applications over less essential traffic during peak usage times. By setting up QoS policies and monitoring their effectiveness through PRTG, administrators can ensure that bandwidth resources are allocated appropriately to maintain optimal performance for business-critical applications. This proactive approach helps in mitigating the impact of bandwidth saturation on user experience and productivity.

These features of PRTG Network Monitor illustrate its effectiveness in handling and mitigating network performance issues related to bandwidth saturation, ensuring smooth operations of cloud-based applications in a corporate environment.

Overall, PRTG Network Monitor stands out for its user-friendly interface, scalability, and powerful monitoring capabilities, making it a valuable tool for organizations looking to maintain a reliable and secure VLAN infrastructure. By leveraging PRTG, network administrators can proactively manage VLAN configurations, mitigate risks associated with misconfigurations, and ensure smooth network operations.

## References:

Paessler. (n.d.). PRTG Network Monitor. Retrieved from PRTG Network Monitor

Paessler. (n.d.). Bandwidth Monitoring with PRTG. Retrieved from Bandwidth Monitoring with PRTG

The screenshot shows the Paessler PRTG Network Monitor website. The header includes the Paessler logo (THE MONITORING EXPERTS) and navigation links: PRODUCTS, PRICING, SOLUTIONS, SERVICES, RESOURCES, and PARTNERS. A 'FREE TRIAL' button and a search icon are also present. The main content area has a blue background with the heading 'Monitor everything'. Below this, there are three bullet points: '✓ Monitor all systems, devices, traffic, and applications', '✓ Monitor LANs, WANs, servers, and more', and '✓ Monitor websites, applications, services, and more'. To the right of these points is an icon of a Wi-Fi signal and a document. Below the bullet points is a cluster of hexagonal icons representing various protocols: SSH, SNMP, HTTP, SMTP, POP3, IMAP, and REST API. To the right of this cluster is the heading 'Integrated technologies' followed by three bullet points: '✓ All important technologies are supported', '✓ Ping, SNMP, WMI, SSH, HTTP requests, and more', and '✓ Flow protocols (IPFIX, jFlow, sFlow, NetFlow)'.

PAESSLER  
THE MONITORING EXPERTS

PRODUCTS PRICING SOLUTIONS SERVICES RESOURCES PARTNERS

FREE TRIAL

### Monitor everything

- ✓ Monitor all systems, devices, traffic, and applications
  - ✓ Monitor LANs, WANs, servers, and more
  - ✓ Monitor websites, applications, services, and more

SSH SNMP HTTP SMTP POP3 IMAP REST API

### Integrated technologies

- ✓ All important technologies are supported
- ✓ Ping, SNMP, WMI, SSH, HTTP requests, and more
- ✓ Flow protocols (IPFIX, jFlow, sFlow, NetFlow)

[https://www.paessler.com/prtg?gad\\_source=1&gclid=Cj0KCQjw3tCyBhDBARIsAEY0XNkGT6mttv-5kVTx\\_UI0XLdXpV920526yG0uLsMgUePutBPhdEsUUFMaAg5lEALw\\_wcB](https://www.paessler.com/prtg?gad_source=1&gclid=Cj0KCQjw3tCyBhDBARIsAEY0XNkGT6mttv-5kVTx_UI0XLdXpV920526yG0uLsMgUePutBPhdEsUUFMaAg5lEALw_wcB)

**Task 4:** Choose a suitable tool to monitor user access performance issues in the LAN in the STARZ Firm network.

#### Another Potential User Access Performance Issue

Another critical issue that might occur in STARZ Firm's LAN is security breaches, either due to unauthorized access attempts or malware spreading through the network. This can impact user access performance and overall network stability.

#### Suitable User Access Performance Tool for Security Monitoring

For security monitoring in a LAN environment, Security Information and Event Management (SIEM) tools are highly effective. One such tool is Splunk.

Splunk is a SIEM platform that aggregates and analyzes security data from various sources across the network. It provides real-time insights into security incidents, detects anomalies, and facilitates incident response.

#### Effectiveness of Splunk:

**Real-time Threat Detection:** Splunk can detect and alert suspicious activities in real-time, helping mitigate security threats promptly.

**Forensic Analysis:** It enables detailed forensic analysis of security incidents, allowing IT teams to understand the scope and impact of breaches on user access performance.

#### References:

Splunk official site: [https://www.splunk.com/en\\_us/download/splunk-cloud.html?utm\\_campaign=google\\_apac\\_south\\_mys\\_en\\_search\\_brand&utm\\_source=google&utm\\_medium=cpc&utm\\_content=cloud\\_signup\\_product&utm\\_term=splunk&device=c&bt=690474868016&bm=e&bn=g&gad\\_source=1&gclid=Cj0KCQjw3tCyBhDBARIsAEY0XNllwjSZWQCOPuR5hscBcfTeHvdTRU0cDLPh0D4n1sQn6v1yKPpw\\_-AaAhj\\_EALw\\_wcB](https://www.splunk.com/en_us/download/splunk-cloud.html?utm_campaign=google_apac_south_mys_en_search_brand&utm_source=google&utm_medium=cpc&utm_content=cloud_signup_product&utm_term=splunk&device=c&bt=690474868016&bm=e&bn=g&gad_source=1&gclid=Cj0KCQjw3tCyBhDBARIsAEY0XNllwjSZWQCOPuR5hscBcfTeHvdTRU0cDLPh0D4n1sQn6v1yKPpw_-AaAhj_EALw_wcB)



### Data Privacy

As a big data company, Splunk understands the importance of data privacy. Our programs, products and services are structured to provide effective data privacy protections for Splunk, its customers, partners and employees.

[Data Privacy Overview >](#)

[Region-specific Privacy >](#)



### Security

Security by Design is top-of-mind throughout our development process. Our products and services are designed to meet your data security needs, including access controls, monitoring and encryption.

[Cloud Security >](#)

[Corporate Security >](#)

[Product Security >](#)



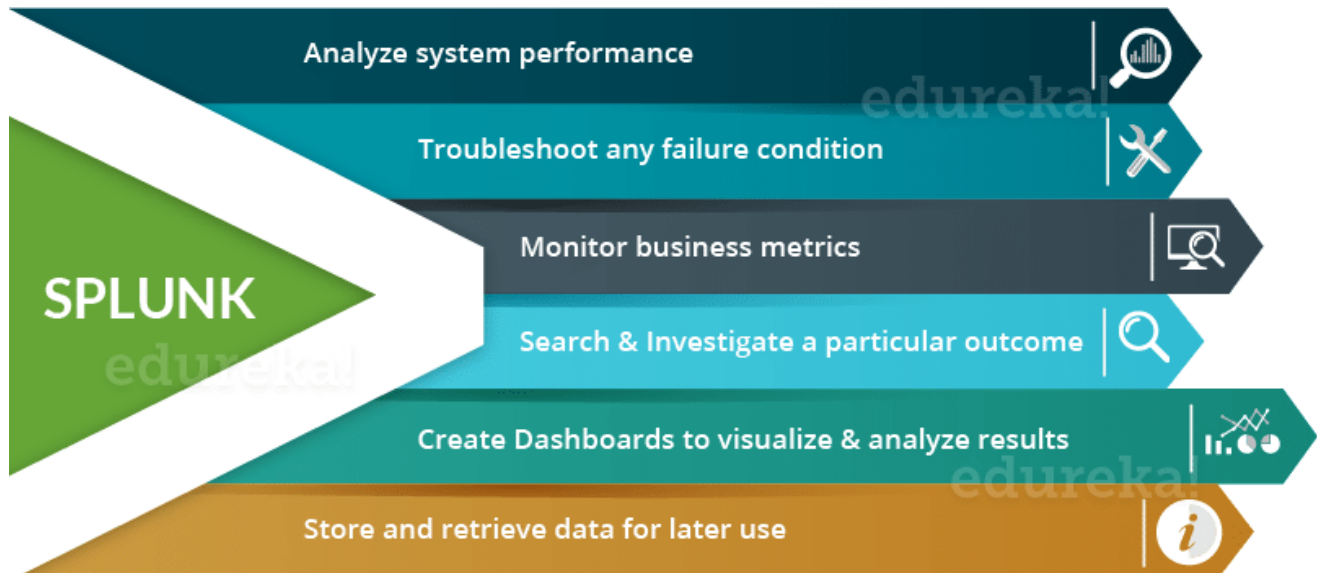
### Compliance

Splunk complies with industry and international security standards. This includes participating in rigorous third-party audits that verify security controls for our Cloud services.

[Compliance Overview >](#)

[Product-specific Compliance >](#)

[Certifications List >](#)



By using tools like Wireshark for network performance monitoring and Splunk for security monitoring, STARZ Firm can enhance its LAN performance management capabilities, ensuring smooth and secure user access to network resources.