

DCN704 – Collaborative Communications

Lab # 1 (5%)

Laboratory Report

Student Name: Fatjon Dauti

Student ID #: 151413192

_____ / 10 Marks

To submit:

1. Rename this file as **LastNameFirstName_DCN704Lab1**. Save it using the same MS Word or PDF. Use a different font and color to write your answers. Resize the screenshots to make them easily readable. Upload this document including all your answers and screenshots. **[One mark]**
2. Name the PT file as **LastNameFirstName_DCN704Lab1.pkt**. Upload it as you finish all the steps. **[One mark]**

This lab is to be performed using Cisco Packet Tracer.

For all the following IOS commands each student should replace the character **x** with the **last digit** of your student ID number.

Whenever is needed use the correct slot/port numbers of the interfaces as you have the hardware on Cisco Packet Tracer.

(Insert all the required tasks answers, command printouts, and reflections as required)

Part A: Network Connectivity

Learning Objectives

Upon completion of this lab, you will be able to

- Perform basic router and switch configuration
- Configure VLANs to support data, voice, and network management traffic
- Configure VLAN trunking between a router and a switch using subinterfaces
- Configure router-based DHCP pools for voice and data devices

Scenario

A company would like to establish its new data network with the expectation of using VoIP in the near future.

Task 1: Use Packet Tracer to create this topology

Use a 2811 Router and a 2960 Switch for the following network. Rename the devices as indicated.

Step 1-1: Clear Prior Configurations

Clear any prior configuration on the router and switch, and delete the vlan.dat file before reloading both devices.

Step 1-2: Cable Router and Switch

Connect router interface Fast Ethernet 0/0 to switch port Fast Ethernet 0/1, as shown in [Figure 3-1](#). The PC will be connected later.

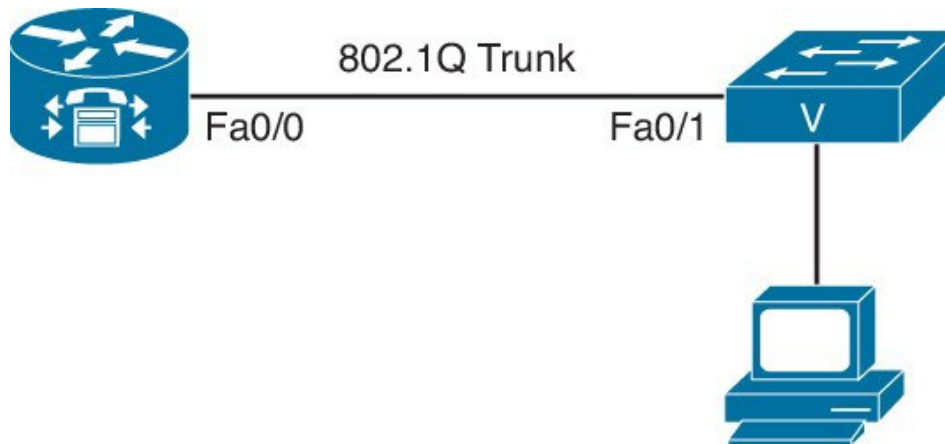


Figure 3-1. Topology Diagram

Task 2: Configure Basic Setup

This task establishes the basic configuration commands on both the router and switch.

Step 2-1: Configure Basic Setup on the Router

Note

Not all devices support the **line vty 0 15** command. If your equipment does not support this command, change it to **line vty 0 4**.

```
Router(config)# hostname RtrPodx
RtrPodx(config)# no ip domain-lookup
RtrPodx(config)# enable secret class
RtrPodx(config)# line con 0
RtrPodx(config-line)# logging synchronous
RtrPodx(config-line)# exec-timeout 120 0
RtrPodx(config-line)# password cisco
RtrPodx(config-line)#
```

```
RtrPodx(config-line)# line vty 0 15
RtrPodx(config-line)# password cisco
RtrPodx(config-line)# login
RtrPodx(config-line)# exit
```

Note

The **exec-timeout** command shown here is useful in a lab setting. It allows 120 minutes of inactivity before logging you out. (In a production environment, this could be a security risk.)

Step 2-2: Configure Basic Setup on the Switch

```
Switch(config)# hostname SwPodx
SwPodx(config)# no ip domain-lookup
SwPodx(config)# enable secret class
SwPodx(config)# line con 0
SwPodx(config-line)# logging synchronous
SwPodx(config-line)# exec-timeout 120 0
SwPodx(config-line)# password cisco
SwPodx(config-line)# login
SwPodx(config-line)# line vty 0 15
SwPodx(config-line)# password cisco
SwPodx(config-line)# login
SwPodx(config-line)# exit
```

Task 3: Configure the Switch

For the purposes of security and ease of implementing quality of service (QoS), use VLANs to keep voice traffic separate from other traffic.

Step 3-1: Create the VLANs

Create and name VLANs for data, voice, and network management.

```
SwPodx(config)# vlan x0
SwPodx(config-vlan)# name Data
SwPodx(config-vlan)# vlan x1
SwPodx(config-vlan)# name Management
SwPodx(config-vlan)# vlan x5
SwPodx(config-vlan)# name Voice
SwPodx(config-vlan)# exit
```

Step 3-2: Configure the Trunk Port

Configure the trunk port that connects the switch to the router. Layer 3 switches (such as the Cisco Catalyst 3560) require that the trunking protocol be specified with the **switchport trunk encapsulation** command before the interface can be set as a trunk. If you are using a Layer 2 switch (such as a Cisco Catalyst 2950 or 2960), the command is not needed and will be rejected.

Note

Cisco recommends in the “VLAN Security White Paper,” to prevent a double-encapsulated 802.1Q/nested VLAN attack, “always pick an unused VLAN as the native VLAN of all the trunks; don’t use this VLAN for any other purpose. Protocols like STP, DTP, and UDLD should be the only rightful users of the native VLAN and their traffic should be completely isolated from any data packets.” For this reason, the management VLAN is not the native VLAN in this lab. To improve security, it would be better to create another VLAN as the native VLAN that will remain unused, but to simplify this lab, it is not covered.

```
SwPodx(config)# interface fastethernet 0/1
SwPodx(config-if)# switchport trunk encapsulation dot1q
```

```
SwPodx(config-if)# switchport mode trunk
SwPodx(config-if)# exit
```

Step 3-3: Configure the Access Ports

Almost all Cisco IP Phones are designed with a three-port switch built inside (one physical port connected to the production switch, one physical port for a PC to connect to the phone, and one internal port for the phone itself). This built-in switch saves money in wiring costs, as existing phone cabling might not meet networking standards. This enables an existing computer to be plugged into the phone, and the phone connects to the switch in the wiring closet.

Prior to the introduction of voice VLANs, a trunk connected an IP Phone to the switch to keep the voice and data traffic separate. Current best practice configures the ports connected to phones and PCs to use access mode but adds a secondary voice VLAN. The switch ports use the access VLAN to send data traffic as untagged frames. However, if the switch detects a Cisco IP Phone using Cisco Discovery Protocol (CDP), it will inform the phone of the VLAN used for voice traffic, which will be tagged using 802.1q. This creates a pseudotrunk that allows only the data and voice VLANs on the link.

Note

If CDP is disabled, or if you are using a non-Cisco IP phone, it requires setting the voice VLAN manually on the IP phone; otherwise, the voice traffic will end up on the data VLAN. For this reason, it is recommended that CDP remains enabled for ports that might have Cisco IP Phones connected.

Use the **interface range** command to assign settings. This is the fastest way to assign settings to more than one switch port at a time.

```
SwPodx(config)# interface range fastethernet 0/2 – 24
SwPodx(config-if-range)# switchport mode access
SwPodx(config-if-range)# switchport access vlan x0
SwPodx(config-if-range)# switchport voice vlan x5
SwPodx(config-if-range)# exit
```

Note

Setting the voice VLAN automatically enables **spanning-tree portfast**, so the switch port does not have to wait for Spanning Tree Protocol (STP) and goes active right away.

Step 3-4: Configure the Switch Management Interface

Set up an interface to manage the switch remotely.

```
SwPodx(config)# interface vlan x1
SwPodx(config-if)# ip address 10.x1.0.2 255.255.255.0
SwPodx(config-if)# exit
SwPodx(config)# ip default-gateway 10.x1.0.1
```

Task 4: Configure the Router Subinterfaces

Subinterfaces allow the VLANs to cross a trunk link to the router. Each subinterface will be the default gateway for a paired subnet. When using subinterfaces on a router, it is necessary to assign the correct VLAN to the subinterface before an IP address can be entered. Because there are three VLANs, you need three subinterfaces.

Step 4-1: Configure the Data VLAN Subinterface

```
RtrPodx(config-if)# interface fastethernet 0/0.x0
RtrPodx(config-subif)# encapsulation dot1Q x0
RtrPodx(config-subif)# description Data VLAN
RtrPodx(config-subif)# ip address 10.x0.0.1 255.255.255.0
```

Step 4-2: Configure the Management VLAN Subinterface

```
RtrPodx(config-subif)# interface fastethernet 0/0.x1
RtrPodx(config-subif)# encapsulation dot1Q x1
RtrPodx(config-subif)# description Management VLAN
RtrPodx(config-subif)# ip address 10.x1.0.1 255.255.255.0
```

Step 4-3: Configure the Voice VLAN Subinterface

```
RtrPodx(config-subif)# interface fastethernet 0/0.x5
RtrPodx(config-subif)# encapsulation dot1Q x5
RtrPodx(config-subif)# description Voice VLAN
RtrPodx(config-subif)# ip address 10.x5.0.1 255.255.255.0
RtrPodx(config-subif)# exit
```

Step 4-4: Activate the Router Interface

```
RtrPodx(config)# interface fastethernet 0/0
RtrPodx(config-if)# no shutdown
```

Note

You might be thinking “What about IPv6?” CUCME does not support IPv6 until version 8.0, which requires router IOS version 15.0 or higher.

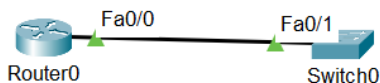
Task 5: Verification

Check the configuration to determine whether it matches what you expect. This will help to avoid future problems.

Step 5-1: Verify Switch VLAN Configuration

Use the **show vlan brief** command to verify the VLAN configuration.

Insert here this command output [0.5 marks]



Fajon Dauti

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

SwPodx#show vlan br

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

SwPodx#

Step 5-2: Verify Switch Port Assignment

Use the **show interfaces switchport** command to verify the configuration of trunk and access ports. This output is from Pod 11; your output will have different VLAN numbers. Notice that Fa0/1 is a trunk port, while Fa0/2 is a static access port and has a voice VLAN assigned to it.

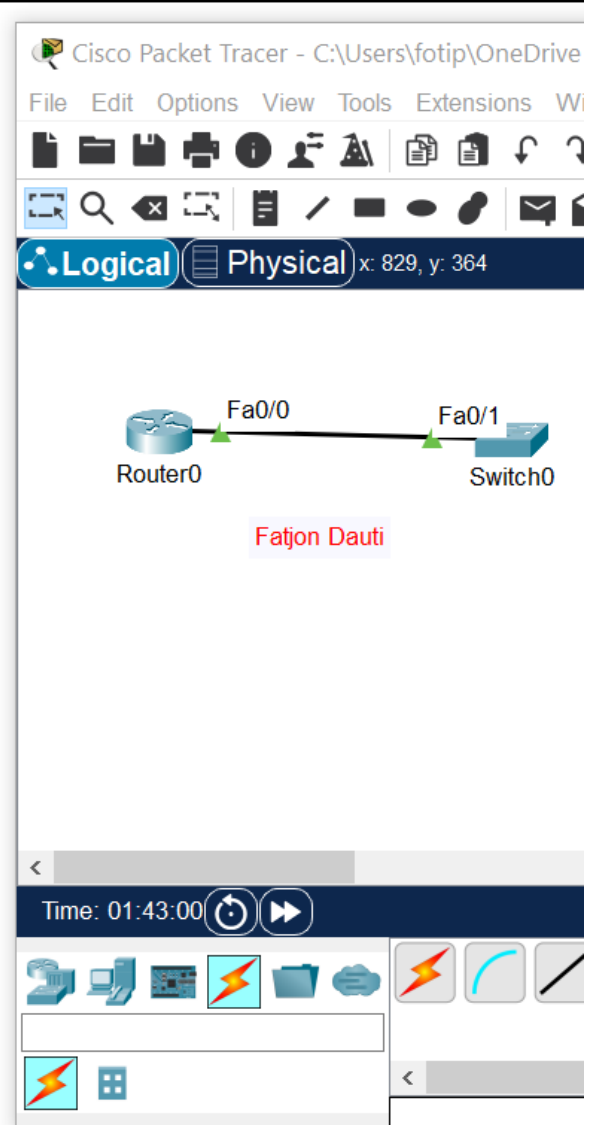
Insert here this command output [0.5 marks]

The command above by default would show all interfaces

Screenshot is cut on the first 2 for demonstration

```
SwPodx#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

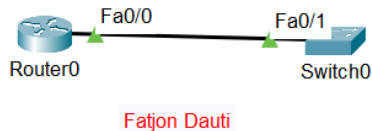
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (Data)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 25
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
```



Step 5-3: Verify Router Subinterface IP Assignment

Use the **show ip interface brief** command to verify that the trunk is assigned correctly.

Insert here this command output [0.5 marks]



```

RtrPodx#sho ip int br
Interface                IP-Address      OK? Method Status          Protocol
FastEthernet0/0          unassigned      YES unset  up              up
FastEthernet0/0.20       10.20.0.1       YES manual up              up
FastEthernet0/0.21       10.21.0.1       YES manual up              up
FastEthernet0/0.25       10.25.0.1       YES manual up              up
FastEthernet0/1          unassigned      YES unset  administratively down down
Vlan1                    unassigned      YES unset  administratively down down
RtrPodx#

```

Task 6: DHCP Services

Note

If you are using another source for DHCP, such as a Windows server or a CUCM server, you can skip this task. However, if the DHCP server is in a different subnet than the clients, it is necessary to use the **ip helper-address** command on each router subinterface to forward the DHCP requests to the server. Regardless of the DHCP server platform you use, make sure to configure the DHCP option 150 as discussed in this task.

While phones and PCs can be assigned IP addresses statically, DHCP can automatically assign IP address leases. Additionally, DHCP can provide additional information to clients, allowing them to locate necessary resources on the network at the same time they receive an IP address. Using the router as a DHCP server is a quick way to provide DHCP services to clients.

The DHCP option 150 tells Cisco IP Phones the IP address of the TFTP server with the initial configuration file. When using CUCME, the router is the TFTP server by default. This lab assigns the default gateway IP address as the option 150 address, as there is only one way to reach the call agent in this network.

Note

If there was redundancy in the network, it would be worthwhile to create a loopback interface and set the option 150 address to the loopback address, as that interface is always up.

Step 6-1: Configure DHCP Pools on the Router

Always enter the **ip dhcp exclude address** command before a DHCP pool is created. This avoids IP addresses that should be excluded from being assigned to devices. Enter the **network** statement as the last command in the pool. Otherwise, if devices are connected, they are assigned an IP address by DHCP right after the **network** statement is entered, even if the default gateway and option 150 are not configured. This can make troubleshooting difficult, as the PCs and phones will receive IP addresses, but the phones will not register and the PCs will not communicate outside their own subnet without the default router (gateway) address.

Create DHCP pools for both the data and voice networks. While it might seem that option 150 is irrelevant in data VLANs, with software on a PC able to emulate a phone (such as the Cisco IP Communicator software), it makes sense to include it for both DHCP pools.

```

RtrPodx(config)# ip dhcp excluded-address 10.x0.0.1 10.x0.0.10
RtrPodx(config)# ip dhcp pool Data
RtrPodx(dhcp-config)# default-router 10.x0.0.1
RtrPodx(dhcp-config)# option 150 ip 10.x0.0.1
RtrPodx(dhcp-config)# network 10.x0.0.0 255.255.255.0

```

```

RtrPodx(dhcp-config)# exit
RtrPodx(config)# ip dhcp excluded-address 10.x5.0.1 10.x5.0.10
RtrPodx(config)# ip dhcp pool Voice
RtrPodx(dhcp-config)# default-router 10.x5.0.1
RtrPodx(dhcp-config)# option 150 ip 10.x5.0.1
RtrPodx(dhcp-config)# network 10.x5.0.0 255.255.255.0
RtrPodx(dhcp-config)# exit

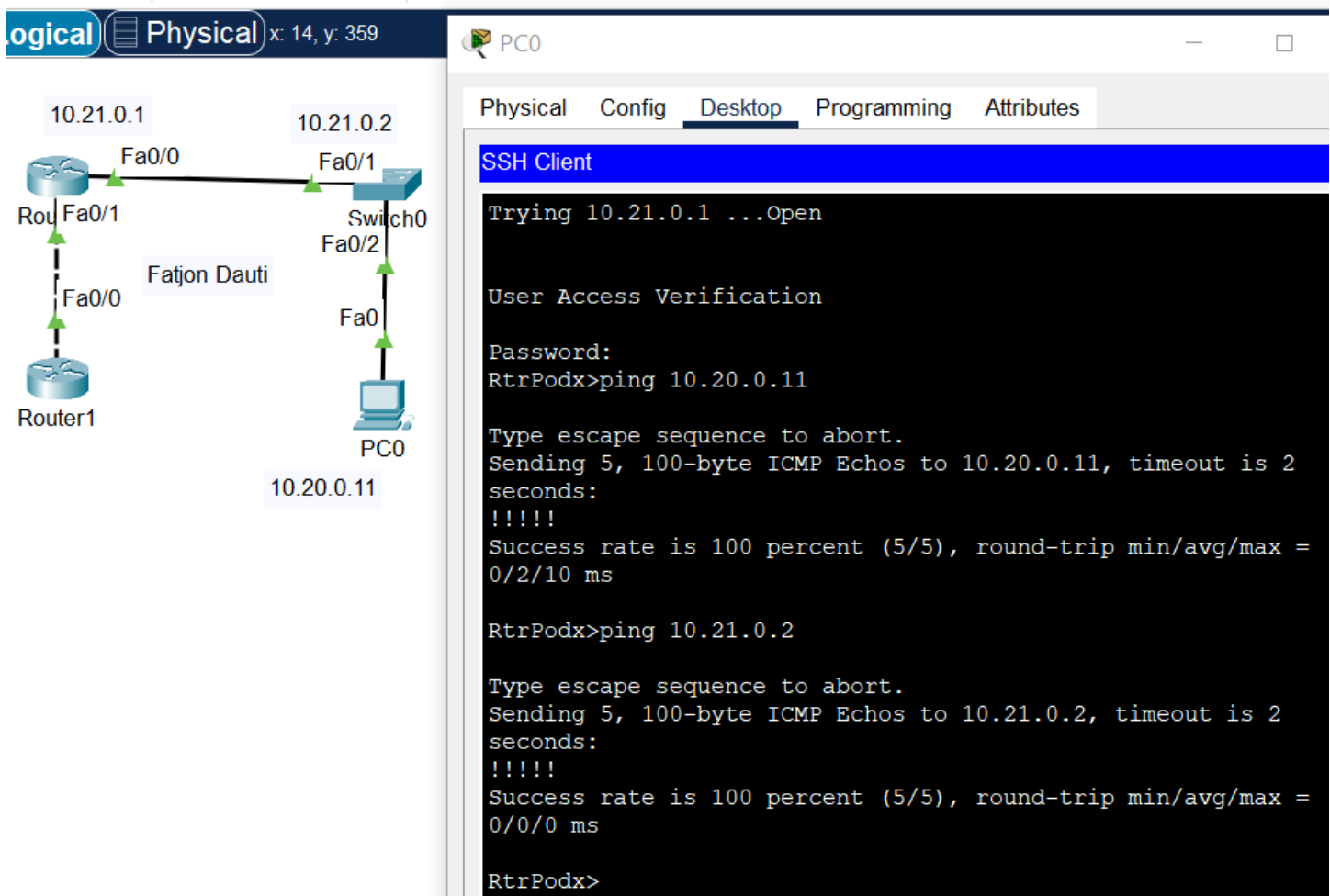
```

Task 7: Test and Cleanup

Step 7-1: Test Connectivity

Connect a PC to the switch. Verify that the PC is assigned an IP address from the 10.x0.0.0 /24 subnet. Verify that the PC can telnet to both the router and the switch management IP addresses. If not, troubleshoot the configuration.

Telneting from PC0 to Router, pinging Switch and PC from router



The image shows a network diagram on the left and a terminal window on the right. The diagram illustrates a topology with Router1 (10.21.0.1) connected to Switch0 (10.21.0.2) via Fa0/0 and Fa0/1. Router1 is also connected to a PC0 (10.20.0.11) via Fa0/0 and Fa0/2. The terminal window, titled 'SSH Client', shows the following output:

```

Trying 10.21.0.1 ...Open

User Access Verification

Password:
RtrPodx>ping 10.20.0.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.0.11, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/2/10 ms

RtrPodx>ping 10.21.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.21.0.2, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/0 ms

RtrPodx>

```

Step 7-2: Save the Configurations

Save the configurations. They will be needed for future labs.

Insert here router configuration (from show running-config command). [0.5 marks]

```

RtrPodx#show run
Building configuration...

```

Current configuration : 1432 bytes


```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname RtrPodx  
!  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
ip dhcp excluded-address 10.20.0.1 10.20.0.10  
ip dhcp excluded-address 10.25.0.1 10.25.0.10  
!  
ip dhcp pool Data  
network 10.20.0.0 255.255.255.0  
default-router 10.20.0.1  
option 150 ip 10.20.0.1  
ip dhcp pool Voice  
network 10.25.0.0 255.255.255.0  
default-router 10.25.0.1  
option 150 ip 10.25.0.1  
!  
ip cef  
no ipv6 cef  
!  
license udi pid CISCO2811/K9 sn FTX1017G01T-  
!  
no ip domain-lookup  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/0  
no ip address  
duplex auto  
speed auto  
!  
interface FastEthernet0/0.20  
description Data VLAN  
encapsulation dot1Q 20  
ip address 10.20.0.1 255.255.255.0  
!  
interface FastEthernet0/0.21  
description Management VLAN  
encapsulation dot1Q 21  
ip address 10.21.0.1 255.255.255.0  
!  
interface FastEthernet0/0.25  
description Management VLAN  
encapsulation dot1Q 25  
ip address 10.25.0.1 255.255.255.0  
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
ip flow-export version 9  
!  
line con 0  
exec-timeout 120 0
```

```
password cisco
logging synchronous
login
!
line aux 0
!
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Insert here switch configuration (from show running-config command). [0.5 marks]

```
SwPodx#
SwPodx#show run
Building configuration...

Current configuration : 3125 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SwPodx
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
```

```
switchport voice vlan 25
!
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/12
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/13
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/14
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/15
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/16
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/17
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/19
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/20
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/21
switchport access vlan 20
```

```
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/22
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/23
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface FastEthernet0/24
switchport access vlan 20
switchport mode access
switchport voice vlan 25
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan21
ip address 10.21.0.2 255.255.255.0
!
ip default-gateway 10.21.0.1
!
line con 0
password cisco
logging synchronous
login
exec-timeout 120 0
!
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Part B: Network Time Protocol



Figure 3-3. Topology Diagram

Learning Objectives

Upon completion of this part, you will be able to configure Network Time Protocol (NTP).

Scenario

The same company as in Part A, wants its new data network to use NTP to synchronize time for network devices.

NTP is not only important for synchronizing the time in network device event logs, but also for VoIP to show the correct time on the display of the phones and record the correct timestamp on voicemails, among other uses. The best way to keep everything synchronized is to use an NTP server to coordinate time.

Note

The NTP server should not be a Microsoft Windows server running the W32Time service, as this uses Simple Network Time Protocol (SNTP), which is not as accurate as NTP and will not sync with most Cisco equipment.

Task 1: NTP Services

Step 1-1: Load Prior Configurations

If necessary, load the configuration for both the switch and router.

Step 1-2: Configure Local Time Zone

NTP is calculated using UTC (Greenwich Mean Time), but you might want to see the time displayed on the router and phones using your local time zone.

Tip

Newer versions of the IOS have the 2007 updated U.S. Daylight Saving Time (DST) start and end dates included. If using an older IOS, or if you have a different DST at your location, you can enter the correct start and end dates as part of the command.

The Cisco IOS does not provide help for time-zone naming conventions. Check Cisco.com for this information.

```
RtrPodx(config)# clock timezone timezone offset-from-GMT
```

For example, U.S. Central Daylight Time would use clock timezone cdt -6.

```
RtrPodx(config)# clock summer-time zone recurring
```

clock summer-time command not supported on Packet Tracer (even older versions)

For example, U.S. Central Daylight Time would use clock summer-time cdt recurring.

Step 1-3: Manually Set the Clock

By manually setting the clock close to the correct time, you reduce the amount of time it takes to synchronize with the NTP server. Ideally, you should be within a minute or two of the correct time.

Use the privileged EXEC mode command `clock set` to manually set time:

```
RtrPodx# clock set hh:mm:ss day month year
```

```
clock set 22:38:11 28 May 2021
```

clock set command is not supported on Packet Tracer

For example, if the current day is Friday, January 22nd, 2021 and the time is 9:40 a.m., you would enter **clock set 09:40:00 22 January 2021**.

Step 1-4 Configure another Cisco Router to Act as an NTP Server

The commands in this step assume that Fast Ethernet 0/1 on the voice router is cabled to another Cisco router. Add the router to your topology.

First, configure the NTP Server router to connect to the voice router.

```
Router(config)# hostname NTP_Server
NTP_Server(config)# interface fastethernet 0/0
NTP_Server(config-if)# ip address 192.168.0.1 255.255.255.0
NTP_Server(config-if)# no shutdown
NTP_Server(config-if)# exit
```

Set the time zones and clock on the NTP_Server router to match the VoIP router (as you did in [Steps 1-2](#) and [1-3](#)).

```
NTP_Server(config)# clock timezone timezone offset-from-GMT
NTP_Server(config)# clock summer-time zone recurring #not supported
NTP_Server# clock set hh:mm:ss day month year #not supported
```

Because you are configuring a “fake” NTP server, it is best to use a higher NTP stratum number to avoid conflicting with real NTP servers. Configure the NTP_Server router to be an NTP time source with the **ntp master stratum number** command.

```
NTP_Server(config)# ntp master 4
```

Insert here NTP router configuration (from show running-config command). [0.5 marks]

```
NTP_Server#show run
Building configuration...

Current configuration : 658 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname NTP_Server
!
clock timezone est -5
!
ip cef
no ipv6 cef
!
license udi pid CISCO2811/K9 sn FTX101736RG-
```

```

!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
ntp master 4
!
end

```

Configure the VoIP router to connect to the NTP_Server router.

```

RtrPodx(config)# interface fastethernet 0/1
RtrPodx(config-if)# ip address 192.168.0.2 255.255.255.0
RtrPodx(config-if)# no shutdown
RtrPodx(config-if)# exit
RtrPodx(config)# ntp server 192.168.0.1
RtrPodx(config)# end

```

Step 1-5: Verify That the Time Is Synchronized

Use the following commands to verify that NTP is working:

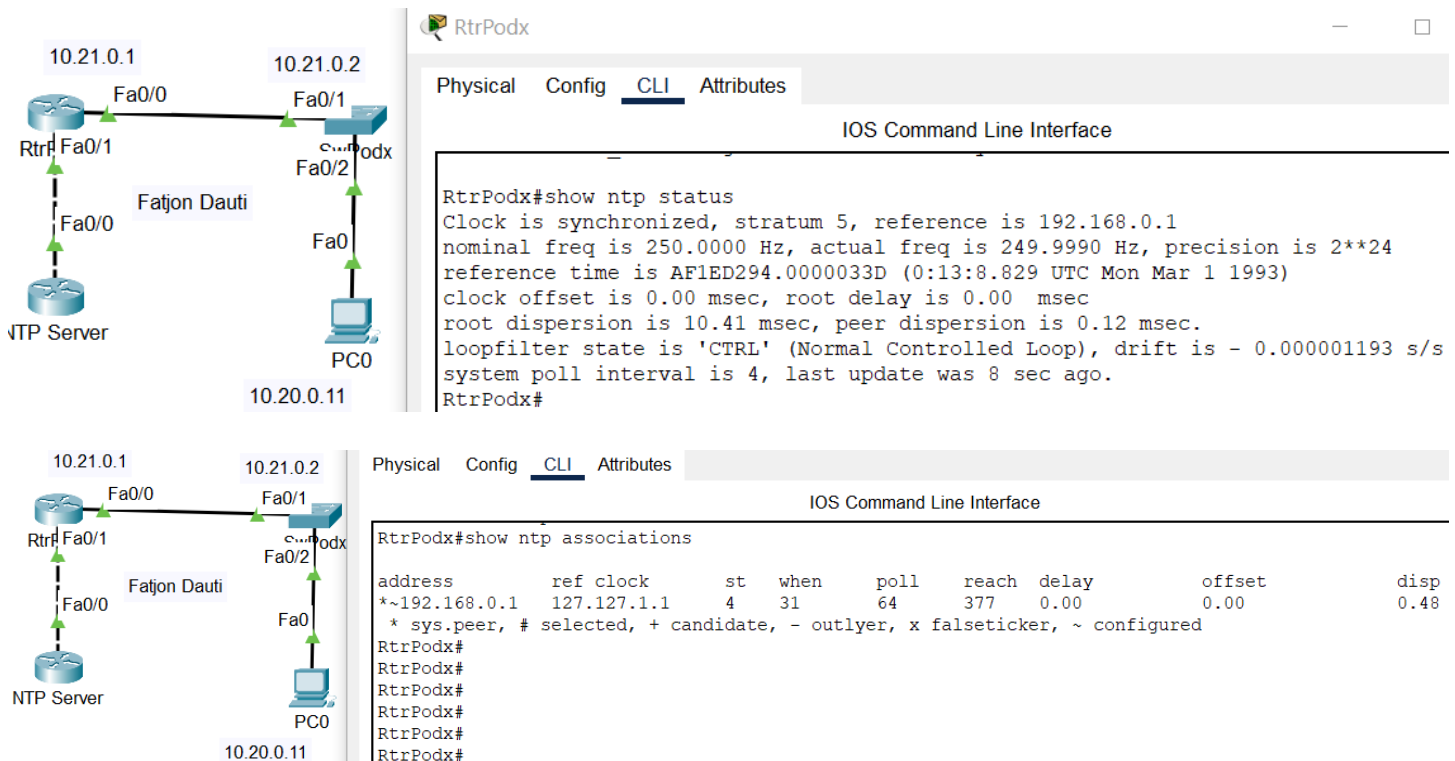
```

RtrPodx# show ntp status
RtrPodx# show ntp association
RtrPodx# show ntp association detail #not supported on packet tracer

```

Note: some of those commands may not run in some IOS versions

Insert here these three last commands outputs [0.5 marks]



show ntp association detail command is not supported on Packet Tracer

Note

It can take five to ten minutes to synchronize with the NTP server. To avoid overwhelming NTP servers, the router starts by polling the server every 64 seconds, and it takes several poll intervals for the router to establish confidence in the results.

Step 1-6: Configure the Switch to Get NTP from the Router

For the sake of making sure that all networking devices are synchronized using NTP, the switch should use the router as an NTP source.

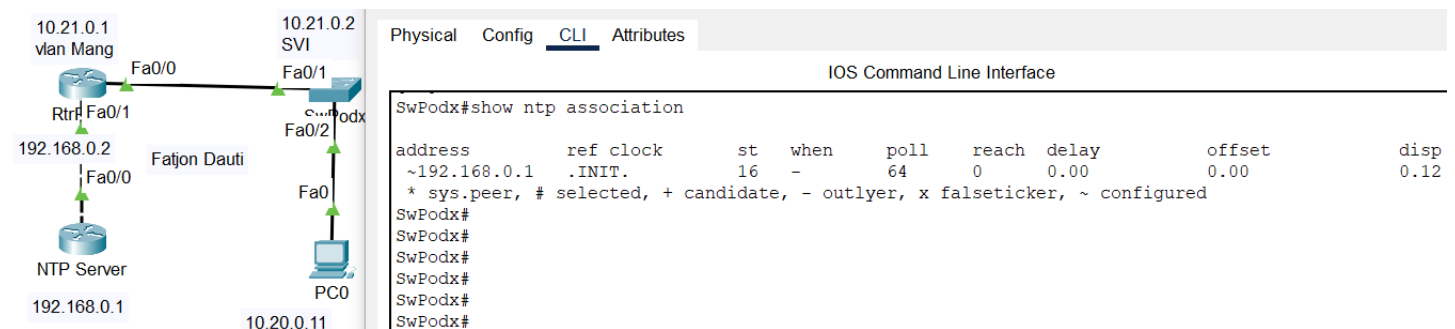
Note

To avoid overloading public NTP time servers, common practice has only a few edge devices at a company contact the public NTP servers, and all other company resources contact those edge devices.

```
SwPodx(config)# clock timezone timezone offset-from-GMT
SwPodx(config)# clock summer-time zone recurring
SwPodx(config)# ntp server 192.168.0.1
```

Issue the command to show the NTP association from the switch

Insert here the last command output here. [0.5 marks]



Step 1-7: Save the Configurations

Save the configurations into a text file for both the router and switch. They will be needed for future labs.