CCNA ENSA   **Lab 3**

Team-No.: 3   **Names:** Shezan Hossain Mahmud,Md Sakhawat Abedin

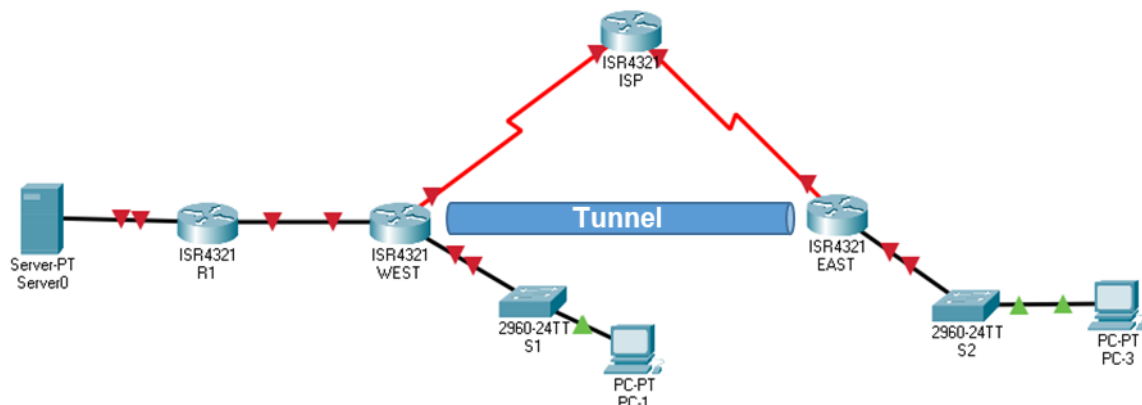**ENSA Module Group Exams**   **6 – 8** **WAN Concepts Exam (esp. Chap 8)**

                          9 – 12 **Optimize, Monitor, and Troubleshoot**

                          Networks

GRE VPN Tunnel

Network Time Protocol (NTP)

Network Management Protocols (Syslog - SNMP)

Homework

Lab Instructions

Task 1   Point-to-point GRE VPN Tunnel

Task 2   NTP and Syslog

Task 3   Simple Network Management Protocol (SNMP)

Deliverables and Due Dates

Homework / Lab Preparation

Part 1: Cisco IOS Basic Configuration Commands

a. Read the **Lab Instructions** of this Lab

b. Check the **IOS Command List**, provided for the Labs and review configuration commands.

Part 2: GRE IP Tunneling

a. Refer to the IN class, and Cisco IOS Command List.
   Which configuration steps are necessary to establish a GRE tunnel between two sites?

Create GRE tunnel interface
(tunnel mode default is GRE IP)
(config)# interface tunnel 0
(config-if)# tunnel mode gre ip
(config-if)# ip address <ip address> <mask>
(config-if)# tunnel source <interface name>
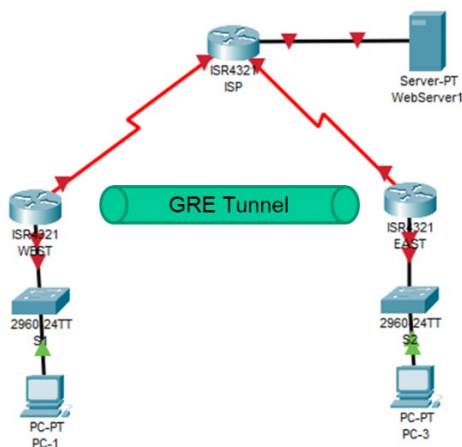(config-if)# tunnel destination <ip address>

Add tunnel network to routing
(config)# router ospf 1
(config-router)# network <tunnel ip network> <wildcard mask> area <no>
or any other routing means

b. GRE IP tunneling configuration

Check the following topology and IP addressing table.

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/0	209.165.201.18	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	G0/0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.17	255.255.255.252	N/A
	S0/1/1	209.165.203.21	255.255.255.252	N/A
EAST	G0/0/0	192.168.3.1	255.255.255.0	N/A
	S0/1/0	209.165.203.22	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-3	NIC	192.168.3.3	255.255.255.0	192.168.3.1
WebServer1	NIC	209.165.200.226	255.255.255.224	209.165.200.225

The grey marked router interfaces of router WEST, ISP and EAST and of PC-1, PC-3 and WebServer1 are already configured.

At router WEST configure a GRE tunnel interface Tunnel0, which encapsulated inner IP packets into GRE, with given IP address and tunnel source and destination. Use the interface name for tunnel source and the IP address of router EAST interface S0/1/0 for tunnel destination.

```
WEST(config)#interface tunnel 0
            (config-if)# tunnel mode gre ip
            (config-if)# ip address 172.16.12.1 255.255.255.252
            (config-if)# tunnel source s0/1/0
            (config-if)# tunnel destination 209.165.201.17
```

At router WEST, for the same topology, configure a static route to PC-3 LAN where next hop is Tunnel0 interface IP address of router EAST.

```
WEST(config)# ip route 192.168.3.0 255.255.255.0 172.16.12.2
```

c. Traffic from PC-1 to PC-3 is routed through a GRE-tunnel from Router WEST to EAST. On PC-1, a traceroute command is issued for the IP address of PC-3.

Which hops (responding IP addresses) will you receive in traceroute?

1. 192.168.1.1

2. 172.16.12.2

3. 192.168.3.3

Part 3:   System Time and NTP

Refer to the IN class, and Cisco IOS Command List.

a. Check the IOS **clock** command list. For more information regarding this command, research the **clock timezone** command at www.cisco.com to determine the zone for your region.

Which time zone is valid in Cologne?

b. Display the actual time of router R1.

```
R1# show clock
```

c. Which command is necessary to set the time & date of a router?

```
R1# clock set 13:00:00 16 Jun 2021
```

d. Which command is necessary to configure a router as NTP master?

```
R1# ntp server <master's ip address>
     #ntp update-calendar
```

e. Why would you use NTP on network devices like routers & switches?

NTP is used to allow network devices to synchronize their clocks with a central source clock to show the accurate time and date

f. What is the "stratum" value? Please explain what is it used for and name typical values.

Stratum is defined as the distance from an authoritative time source to the network devices. Each level of this hierarchy is assigned a number, starting with zero (0) for the reference clock at the top. Stratum 0 means that a device is directly connected to the atomic clock e.g., a GPS antenna.

g. Which transport protocol & ports is used for the NTP protocol?

NTP used UDP-based service. NTP servers use 123 port communicate with NTP clients.

h. Which modes of operation can be used on Cisco routers for NTP?
Cisco routers use 3 different NTP modes:
NTP client mode.
NTP server mode.
NTP symmetric active mode.

i. Which technologies might be used as an acceptable master clock (stratum level 0)?

A reference clock source that relays Coordinated Universal Time (UTC) and has little or no delay is known as a Stratum 0 device. Stratum level 0 is directly connected to computers that then operate as primary time servers.

Part 4: Syslog

Refer to the IN class, and Cisco IOS Command List.

a. Which transport protocol & ports is used by the SYSLOG service?
    514 (UDP) server. 601 (TCP) syslog-conn

b. In IOS, which command is necessary to log syslog messages to syslog server 192.168.42.1?
    #logging host 192.168.42.1

c. Which logging level is mapped to which severity level? Provide logging level names.

    Severity = 0: Emergencies: System shutting down due to missing fan tray

    Severity = 1: Alerts: Temperature limit exceeded

    Severity = 2: Critical : Memory allocation failures

    Severity = 3: Errors: Interface Up/Down messages

    Severity = 4: Warnings : Configuration file written to server, via SNMP request

    Severity = 5: Notifications: Line protocol Up/Down

    Severity = 6: Information: Access-list violation logging

    Severity = 7: Debugging: Debug messages

Part 5: SNMP

Refer to the IN class, and Cisco IOS Command List.

a. What are the main differences of SNMPv2c and SNMPv3?

    SNMPV2 is the second version of SNMP and SNMPV3 is the third version.
    SNMPV2 and SNMPV3 differ in terms of security and remote configuration model.
    SNMPV2 uses complex party-based security systems, on the other hand, SNMPV3 uses an enhanced cryptographic security system.

b. Which transport encapsulation and port(s) are used by SNMP?

    SNMP is a request/response protocol. UDP port 161 is its well-known port. SNMP uses UDP as its transport protocol

c. For what functionality do you use the "trap" feature, although you get all information via SNMP GET requests?

    A trap is an alert message—for example, a trap might alert the SNMP manager to the failure of a device.

d. Configure router R1 as SNMP-server with the following features: There should be read access for everyone (community "public"), however write access should only be possible with community "admin" from PC 192.168.42.1.

```
R1(config)# snmp-server community public ro SNMP_ACL
         #snmp-server host 192.168.42.1 version 2c pulic
         #snmp-server location snmp_manager_server
         #snmp-server contact public_admin
         # snmp-server enable traps
         #ip access-list standard SNMP_AC
         #permit host 192.168.42.1
```

e. In the appendix you find the MIB-2 subtree for managed objects (MO) in the IP group. Which numerical OID and alphanumerical OID is given for the MO **ipDefaultTTL**?
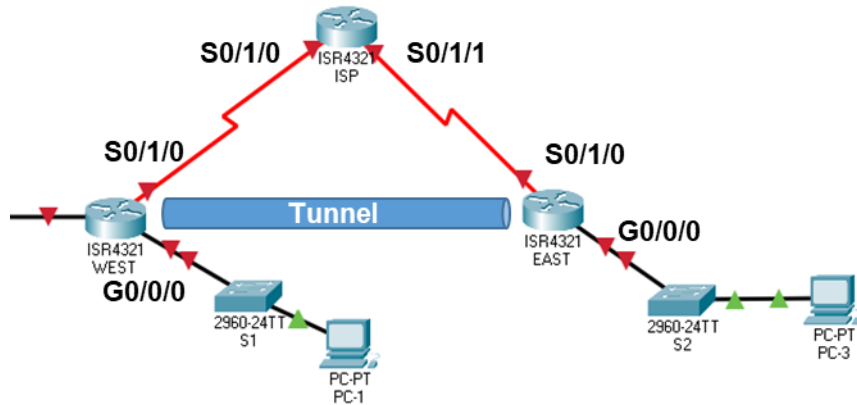
OID (numerical): 1.3.6.1.2.1.4.2

OID (alphanumerical): 1.3.6.1.2.1.4 - ip
1.3.6.1.2.1 - SNMP MIB-2
1.3.6.1.2 - IETF Management
1.3.6.1 - OID assignments from 1.3.6.1 - Internet
1.3.6 - US Department of Defense
1.3 - ISO Identified Organization
1 - ISO assigned OIDs

Appendix:

SNMP MIB-2 group

OID: iso.org.dod.internet.mgmt.mib-2.ip. ...

OID: .1.3.6.1.2.1.4. ...)

ip			
	ipForwarding		
	ipDefaultTTL		
	ipInReceives		
	ipInHdrErrors		
	ipInAddrErrors		
	ipForwDatagrams		
	ipInUnknownProtos		
	ipInDiscards		
	ipInDelivers		
	ipOutRequests		
	ipOutDiscards		
	ipOutNoRoutes		
	ipReasmTimeout		
	ipReasmReqds		
	ipReasmOKs		
	ipReasmFails		
	ipFraqOKs		
	ipFraqFails		
	ipFraqCreates		
	ipAddrTable	ipAddrEntry	ipAdEntAddr
			ipAdEntIndex
			ipAdEntNetMask
			ipAdEntBcastAddr
			ipAdEntReasmMaxSize
	ipRouteTable	ipRouteEntry	ipRouteDest
			ipRouteIfIndex
			ipRouteMetric1
			ipRouteMetric2
			ipRouteMetric3
			ipRouteMetric4
			ipRouteNextHop
			ipRouteType
			ipRouteProto
			ipRouteAge
			ipRouteMask
			ipRouteMetric5
			ipRouteInfo
	ipNetToMediaTable	ipNetToMediaEntry	ipNetToMediaIfIndex
			ipNetToMediaPhysAddress
			ipNetToMediaNetAddress
			ipNetToMediaType
	ipRoutingDiscards		
	ipForward	ipForwardNumber	
		ipForwardTable	ipForwardEntry	ipForwardDest

ipForwardEntry	ipForwardDest
	ipForwardMask
	ipForwardPolicy
	ipForwardNextHop
	ipForwardIfIndex
	ipForwardType
	ipForwardProto
	ipForwardAge
	ipForwardInfo
	ipForwardNextHopAS
	ipForwardMetric1
	ipForwardMetric2
	ipForwardMetric3
	ipForwardMetric4
	ipForwardMetric5

Task 1 – Point-to-point GRE VPN Tunnel

Topology Part1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/0	209.165.201.18	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	G0/0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.17	255.255.255.252	N/A
	S0/1/1	209.165.203.21	255.255.255.252	N/A
EAST	G0/0/0	192.168.3.1	255.255.255.0	N/A
	S0/1/0	209.165.203.22	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-3	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Part 1:   Build the Switched Network and Verify Connectivity

Step 1:   Build topology in Packet Tracer.

COVID-19 Version: Build topology in **Packet Tracer**. Use and re-label the following devices:

a. Build the network with ISR4321 router, 2960 switches, PCs and Servers in Packet Tracer. Rename the devices.

b. Cable the network according to the topology with straight-through TP cables .

c. Implement NIM-2T modules at each router, and connect these interfaces by serial cables.

d. We will use the CLI window of the network devices directly for configurations.

Step 2:   Basic settings for each router.

    a.   Disable DNS lookup.

    b.   Configure the device name.

    c.   Assign **class** as the encrypted privileged EXEC mode password.

    d.   Assign **cisco** as console password, set console logging to synchronous mode, enable login.

    e.   Assign **cisco** as vty password, and enable login.

    f.   Encrypt plain text passwords.

Step 3:   Ethernet and Serial Interface at each routers WEST, EAST, and ISP

    a.   Configure the Ethernet interfaces according to the Addressing Table and switch on the interfaces.

    b.   Configure the Serial interfaces according to the Addressing Table
       - Set the clock rate for all DCE serial interfaces to **128 kHz,**
       - (DCE or DTE V.35 interface mode can be checked by **show controllers serial <x/y/z>**)
       - and switch-on interfaces.
       Note: Depending on how you implemented the serial cable, DCE location may be flipped.

Step 4:   Configure Default Routes at Router WEST and EAST

    a.   Create a static default route at router WEST using serial interface s0/1/0.

    b.   Create a static default route at router EAST using serial interface s0/1/0.

Step 5:   Verify router connectivity.

    a.   Test connectivity by a ping from router WEST to Router ISP serial interface. Connectivity (y/n)? y

    b.   Test connectivity by a ping from router WEST to Router EAST serial interface. Connectivity (y/n)?y

    Note: Troubleshoot, if connectivity is not successful.

Step 6:   Configure the PC Hosts

    Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 7:   Verify LAN connectivity.

    a.   Test connectivity by a ping from PC-1 to its default gateway. Successful (y/n)? y

    b.   Try to ping Router EAST from PC-1. Why is it not working?
       Because static route for PC-1 LAN has not been configured on Router WEST

Part 2:   GRE Tunnel configuration

Background / Scenario

    GRE is a tunneling protocol, tunneling IP packets in IP packets and can be used for e.g. connecting IPv6 networks over IPv4 networks, and with Multicast packets, such as OSPF, EIGRP, and streaming applications, or even in secured IPsec connections.

Step 1:   GRE tunnel interfaces.

    a.   Configure the tunnel interface Tunnel0 on the WEST router. Use S0/1/0 on WEST as the tunnel source interface and IP address 209.165.203.22 as the tunnel destination on the EAST router.

    b.   Configure the tunnel interface Tunnel0 on the EAST router. Use S0/1/0 on EAST as the tunnel source interface and IP address 209.165.201.18 as the tunnel destination on the WEST router.

Step 2: Verify that the GRE tunnel is functional.

a. Check **briefly** the IP address of tunnel interface on the EAST router. Record your command.

`EAST#` show ip interface brief | include Tunnel
Tunnel0 172.16.12.2 YES manual up up

b. Issue the **show interface tunnel 0** command on router EAST to verify the tunneling protocol, tunnel source, and tunnel destination used in this tunnel.

Are IP addresses of tunnel source and destination correct (y/n)? y

c. Ping and traceroute across the tunnel from the EAST router to the WEST router using the IP address of the tunnel interface. Record the responding interfaces IP address.

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/35 ms
Explain why these interface(s) respond to the traceroute ECHO REQUEST?

for tunnel interface it is directly connected

Part 3: Enable OSPF Routing over the GRE Tunnel

After the GRE tunnel is set up, a routing protocol for the tunneled LAN can be implemented. For GRE tunneling, a network statement will include the IP network of the tunnel, instead of the network associated with the serial interface.

Note: The ISP router is not participating in this routing process.

Step 1: OSPF routing for area 0 over the tunnel.

a. Configure OSPF process ID 1 using area 0 on the WEST router and advertise both local networks (private IP LANs). Which two networks must be advertised at router WEST?

192.168.1.0
172.16.12.1

b. Configure OSPF process ID 1 using area 0 on the EAST router and advertise both local (private) networks. Which two networks must be advertised at router EAST?

192.168.3.0
172.16.12.0

Step 2: Verify OSPF routing and end-to-end connectivity.

a. From the EAST router, issue the **show ip route** command to verify the route to 192.168.1.0/24 LAN on the WEST router. What is the exit interface and IP address to reach the 192.168.1.0/24 LAN?

192.168.1.0/24 [110/1001] via 172.16.12.1, 00:02:53, Tunnel0

b. Ping from PC-1 to PC-3. Sucessful (y/n)? y

c. Traceroute from PC-1 to PC-3 and record the path.

Tracing route to 192.168.3.3 over a maximum of 30 hops:
1 0 ms   0 ms   0 ms   192.168.1.1
2 2 ms   1 ms   2 ms   172.16.12.2
3 3 ms   11 ms 11 ms 192.168.3.3

Reflection

1. If you add more LANs to the WEST or EAST routers, what must be done to ensure, that these networks are routed using the GRE tunnel?

2. What options do you have to secure data sent over a GRE tunnel?
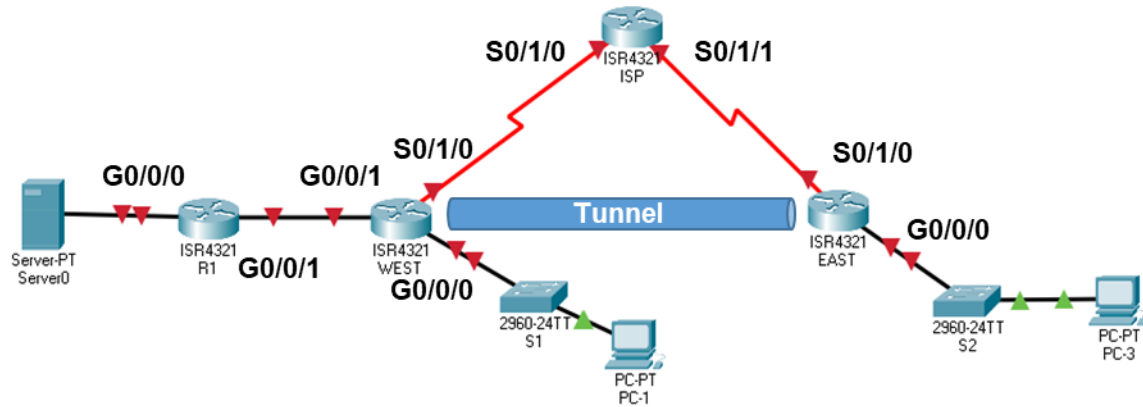
   Encapsulates with GRE header

3. Which IP tunneling protocol provides embedded encryption and authentication?

   The ESP protocol provides secure transmission through both encryption and authentication.

Task 2 – Network Time Protocol (NTP) and Syslog

Topology Part2

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/0/0	192.168.1.1	255.255.255.0	N/A
	S0/1/0	209.165.201.18	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
	G0/0/1	10.1.1.1	255.255.255.252	N/A
ISP	G0/0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.17	255.255.255.252	N/A
	S0/1/1	209.165.203.21	255.255.255.252	N/A
EAST	G0/0/0	192.168.3.1	255.255.255.0	N/A
	S0/1/0	209.165.203.22	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
R1	G0/0/1	10.1.1.2	255.255.255.252	N/A
	G0/0/0	172.16.2.1	255.255.255.0	N/A
PC-1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-3	NIC	192.168.3.3	255.255.255.0	192.168.3.1
Server0	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Part 1:   Extend Topology and Configuration.

Step 1:   Extend topology in Packet Tracer.

a. Add router R1 and Server0 to topology.

b. Cable the network as shown in the topology

c. Rename the devices.

Step 2:   **Configure Basic Settings for Router R1**

    a.   Disable DNS lookup.

    b.   Configure the device name.

    c.   Assign **class** as the encrypted privileged EXEC mode password.

    d.   Assign **cisco** as the console and vty password and enable login, set console logging to synchronous.

    e.   Encrypt plain text passwords.

Step 3:   **Configure Interfaces of Router R1 and Router WEST**

    a.   At router R1, apply the IP addresses to Gigabit Ethernet interfaces G0/0/0 and G0/0/1 according to the Addressing Table and activate the physical interfaces.

    b.   At router WEST, apply the IP address to Gigabit Ethernet interface G0/0/1 according to the Addressing Table and activate the physical interface.

Step 4:   **Configure OSPF Routing**

    a.   Enable OSPF at R1 with process ID 1. Add all connected networks into the OSPF process for area 0.

    b.   At WEST, add network 10.1.1.0 / 30 into the OSPF process for area 0.

Step 5:   **Syslog Server Connectivity**

    a.   Configure the IP address and default gateway for Server0 according to the Addressing Table.

Step 6:   **Verify end-to-end connectivity.**

    a.   Verify that Server0 can ping Router R1, Router WEST and PC-1 in the network successfully. If not, troubleshoot until there is end-to-end connectivity.

    b.   Check ping from Server0 to PC-1. Successful (y/n) y

Step 7:   **Save the running configuration to the startup configuration.**

Part 2:   NTP – Network Time Protocol

Synchronized time is important for syslog and debug functions. If the time is not synchronized, it is difficult to determine what network event caused the message. Router WEST will become the NTP server and router R1 acts as the NTP client.

Step 1:   **Router WEST Clock Evaluation**

Issue the **show clock detail** command to display the current time on WEST. Record the information regarding the current time displayed in the following table.

Date	Time	Time Zone	Time Source
Mar 1 1993	*3:36:0.732	UTC	hardware calendar

Step 2:   **Set the time.**

    a.   Use the **clock set** command to set the time on WEST. Which time zone is used by default? Which offset do we have to the local time zone?   UTC +2

Step 3:   Router WEST NTP Master Server

a. Configure WEST as the NTP master by using the **ntp master** *stratum-number* command in global configuration mode. The stratum number indicates the number of NTP hops away from an authoritative time source.

Note: The NTP Stratum model is a representation of the hierarchy of time servers in an NTP network, where the Stratum level (0-15) indicates the device's distance to the reference clock. Stratum 0 means a device is directly connected to e.g., a GPS antenna.

In this lab, the stratum level of this NTP server shall be 4. Which command must be used?

`WEST(config)#` ntp master 4

Step 4:   Router R1 NTP Client

a. Issue the appropriate command on R1 to see the configured time. Record the current time displayed in the following table.

Date	Time	Time Zone
Thu Jun 17 2021	8:18:32.871	UTC

b. Configure R1 as the NTP client. Use the **ntp server** command to point to the IP address or hostname of the NTP server.

The **ntp update-calendar** command periodically updates the calendar or hardware clock by software NTP time.

Your necessary commands:

`R1(config)#` ntp server 10.1.1.1

`R1(config)#` ntp update-calendar

Step 5:   Verify NTP configuration.

a. Use the **show ntp status** command to check the clock of router WEST.

Which precision has the hardware clock of WEST?

Which drift [in μs per second] is given with the clock?

0.000001193 s/s system poll

b. Use the **show ntp status** command to check the clock of router R1. Is router R1 synchronized (y/n)?

Clock is synchronized, stratum 16, reference is 10.1.1.

c. Use the **show ntp associations** command to verify that R1 has an NTP association with WEST.

How many NTP polls did R1 perform?   16

d. Issue **show clock** on WEST and R1 to compare the timestamp.

Are WEST and R1 synchronized (y/n)? y

Note: It could take several minutes before the timestamp on R1 is synchronized with WEST.
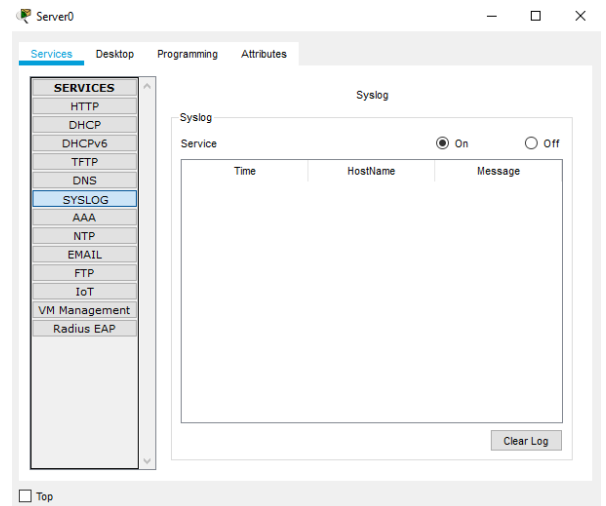
Part 3:   Syslog Logging

Step 1:   Syslog server at Server0.

Syslog messages from network devices can be collected and archived on a syslog server.

A network administrator can control the types of messages that can be sent to the syslog server.

Check, if Syslog Server is running on Server0. If not, start the Syslog Server (y/n).

Step 2:   Verify timestamp service on R1.

Check the running configuration to check **timestamp services** for logging on R1.

Which timestamp services are enabled?
#service timestamps log datetime msec

If the timestamp service for logging is not enabled, use this command to enable it for both routers R1 and WEST.

```
R1(config)# service timestamps log datetime msec
WEST(config)# service timestamps log datetime msec
```

Step 3:   Logging syslog messages from R1 to syslog server.

Configure R1 to send Syslog messages to the syslog server, Server0.

```
R1(config)# logging host <ip address>
```

Step 4:   Display the R1 default logging settings.

Use the **show logging** command to display the default logging settings. Record some Syslog default logging settings.

Syslog server:172.16.2.3

Number of log messages: 2

Trap logging level: level informational

Which transport protocol and port is used by Syslog?udp port 514

Step 5:   Check severity levels on R1.

a. Use the **logging trap ?** command to check, which trap levels are availability.

Syslog trap level number: severity=7

Corresponding severity level (name): Debugging messages

Enable highest trap logging level.

b. Create interface Loopback0 on R1 and observe the log messages on both the terminal window and the Syslog server window

```
R1(config)# interface lo0
```

How many logging messages are created at the condole output? 1
(**Note**: If no messages are shown, change the service HTTP and back to SYSLOG).

Compare the syslog messages at the console and at the syslog server. Which differences do you find?

no log appeared

Step 6: Check logging messages for OSPF events

a. On router WEST, shut-off interface G0/0/1. Which Syslog messages are created on WEST?

un 17, 04:56:19.5656: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to administratively down
*Jun 17, 04:56:19.5656: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to down
*Jun 17, 04:56:19.5656: 04:56:19: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet0/0/1 from EXSTART to DOWN, Neighbor Down: Interface down or detached

How are these Syslog events received at Syslog server?   2

b. On router WEST, switch-on interface G0/0/1 again and compare WEST Syslog messages and Server0 Syslog messages.

How fast do we get information about link state changes?

How fast do we get information about OSPF routing state changes?

Reflection

Why is it important to time-synchronized logging and other management functions in a network?

In modern computer networks, time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events happen. ... Without synchronized time, accurately correlating log files between these devices is difficult, even impossible

What is the problem with setting the level of severity very high (lowest level number)?

Setting it too high (lowest level number) could generate logs that missed some very useful but not critical messages

What is the problem with setting the level of severity very low (highest level number) for syslog?

Setting it too low (highest level number) could generate a large number of messages and fill up the logs with unnecessary information.

Task 3 – Simple Network Management Protocol (SNMP)

Topology
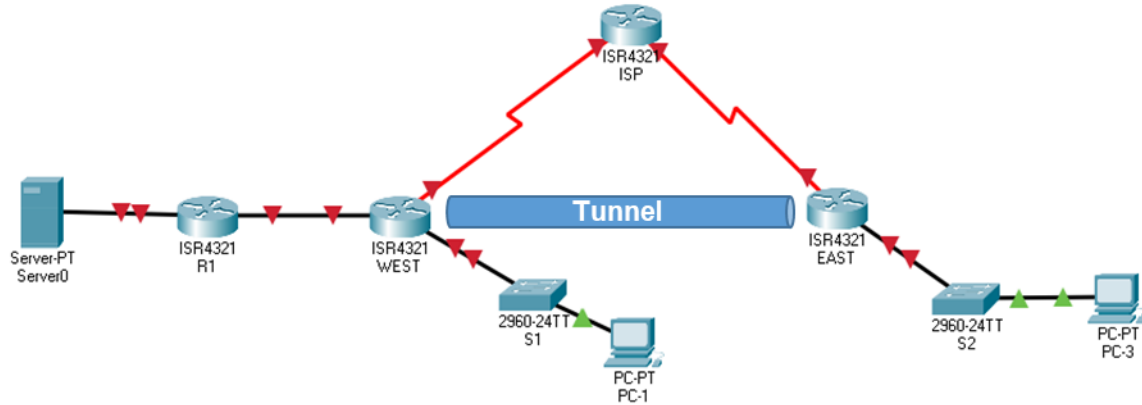
Proceed with Topology of Part 2

Part 1:   SNMP Agents and Manager

### Step 1:   PT configuration of SNMP agent on WEST.

PT allows limited SNMP functionality.

At router WEST, enter the following commands from the global configuration mode to configure the router as an SNMP agent for community ciscolab with read-only policy.

```
WEST(config)# snmp-server community ciscolab ro
```

Step 2:   Configure SNMP MIB Browser at PC-1.

a.   Select MIB Browser at PC-1

b.   Configure MIB Browser to access the router WEST interface G0/0/0 for SNMP management.

c.   Edit Advanced SNMP Options to set the correct values.

  -   SNMP Agent IP address

  -   R/O community sting

  -   R/W same community sting

  -   SNMP Version 1
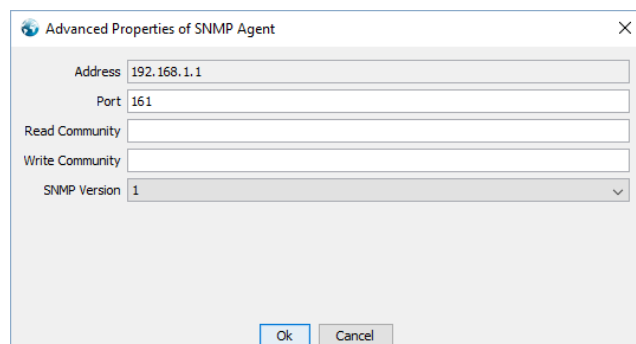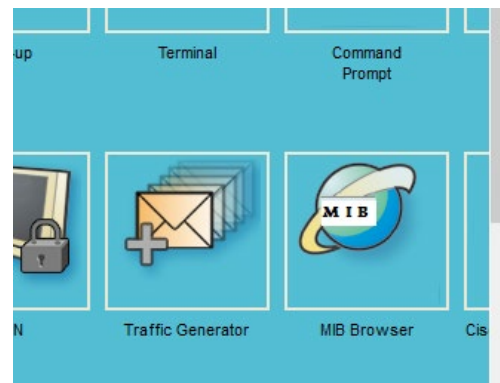
d. Check connectivity and read the OID of **systemDescr (OID .1.3.6.1.2.1.1.1.0)** by following
MIB Tree => router_std MIB => etc. until you reach the requested OID for System Description,
selecting GET command and press GO to read it.
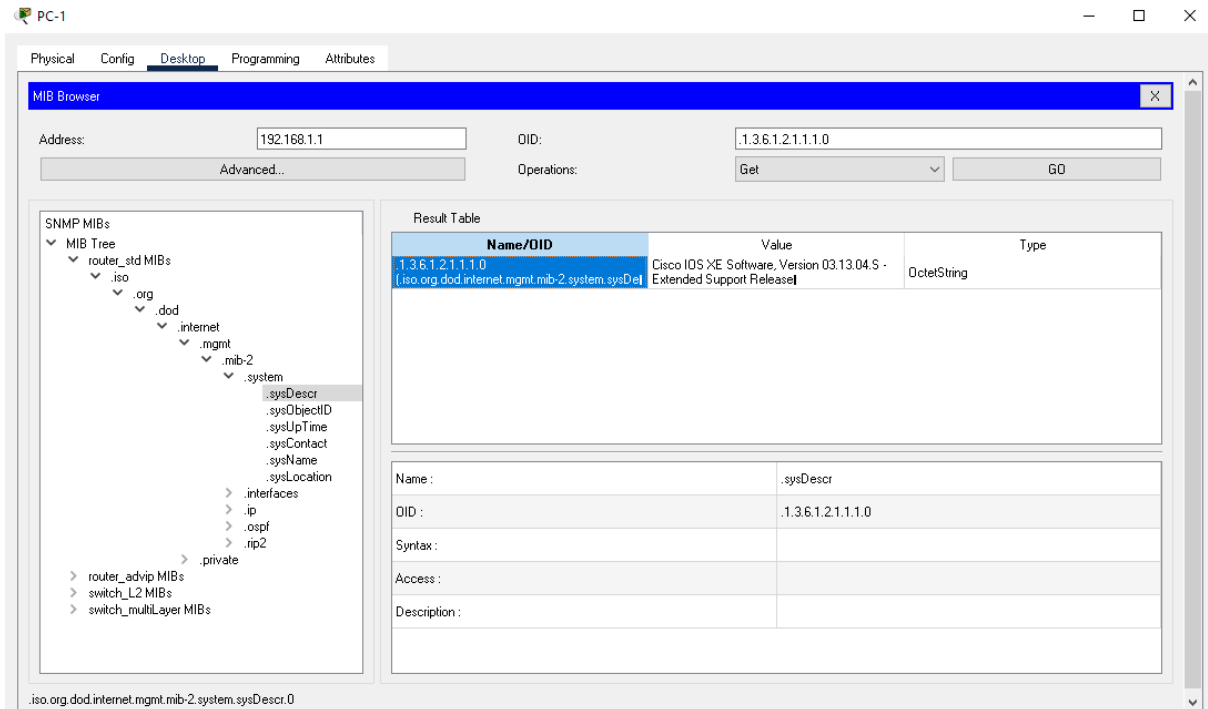
Record the IOS Version of router WEST. (Troubleshoot, if necessary.)

.1.3.6.1.2.1.1.1.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0)

Step 3: Discover SNMPv1 WEST agent.

a. At this point, you may read Managed Objects (MOs) of WEST by SNMP **Get**.

Read the System UpTime since last (re-)start of SNMP daemon.

sysUpTime numerical OID: .1.3.6.1.2.1.1.3.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0)

sysUpTime Value: 5 hours 17 minutes 55 seconds   Type TimeTicks

b. Read the System Name of router R1 (MO sysName).

sysName numerical OID: .1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysName.0)

sysName Value: west   Type OctetString

c. Try to change the router name from WEST to R11 with SNMP **Set** request. Test your action with the
corresponding SNMP Get request.

Explain why this does not work.
GET REQUEST Is used to request a specific data record, a unique OID must be specified.in this case WEST router permit PC-1

Step 4: Check SNMPv2 Get Bulk requests from router WEST.

a. Try to read the routing table of router WEST by SNMP **Get Bulk** request for a group of MOs in
ipRouteTable.

ipRouteTable which numerical OID: .1.3.6.1.2.1.1.5.0

Did it work? If it failed, explain why. SNMP version 1 doesnot support get bulk

If necessary, adjust your Get Bulk request to the required SNMP version and try it again.

How many entries do you get for the 192.168.1.0/24 network?

.1.3.6.1.2.1.4.21.1.1.192.168.1.0 (.iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable.ipRouteEntry.ipRouteDest.192.168.1.0)
.1.3.6.1.2.1.4.21.1.1.192.168.1.1 (.iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable.ipRouteEntry.ipRouteDest.192.168.1.1)

Part 2: Simulated SNMP traps / notifications

Step 1: SNMP trap notification.

Because Packet Tracer does not support SNMP traps, we provide some results from DN.lab in combination with your PT actions.

We enabled interface G0/0/1 of router WEST to generate an SNMP trap notification to be sent to the SNMP Manager at PC-1.

a) Your task in PT at router WEST, switch off the inter-router link interface G0/0/1.

Record the summary logging information from console.

Console logging: level debugging, 10 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 10 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 10 message lines logged

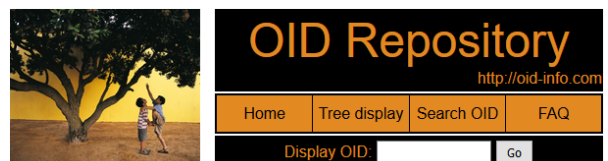b) The SNMP manager in PC-1 received the following private Enterprise/OID and code numbers, visible in a traps window.

Time	Sender	Originator	Enterprise/OID
7/9/2013 12:01:01 PM		192.168.1.2:53977	1.3.6.1.2.1.17.0.2
7/9/2013 12:01:04 PM		192.168.1.1:51117	1.3.6.1.4.1.9.9.41.2.0.1
7/9/2013 12:01:05 PM		192.168.1.1:51117	1.3.6.1.6.3.1.1.5.4

Step 2: Decode SNMP MIB/OID messages.

In the following, we find information about the given OID in the Internet.

You might use the Cisco **SNMP Object Navigator** tool from http://www.cisco.com (search for MIB Locator and follow SNMP Object Navigator), but you need a separate **login account** at **cisco.com**.

Another option is the OID Repository Website http://www.oid-info.com , which does not require any **login**.

OID Repository
http://oid-info.com

| Home | Tree display | Search OID | FAQ |

Display OID: [   ] Go

Basic search

▸Advanced search
▸ Number of OIDs in the database

a. The OID message objects, which has been found, are given in Step1 Task b).

Record the source MIB (RFC mib-2 or enterprises tree) and the meaning of the notifications.

OID 1.3.6.1.2.1.17.0.2   MIB: topologyChange

Managed Object:

OID 1.3.6.1.4.1.9.9.41.2.0.1   MIB: clogMessageGenerated

Managed Object: clogHistFacility,
clogHistSeverity,
clogHistMsgName,
clogHistMsgText,
clogHistTimestamp

OID 1.3.6.1.6.3.1.1.5.4　　　　　　　　　　MIB: linkUp

Managed Object: ifIndex, ifAdminStatus, ifOperStatus

How do these SNMP trap events map to the logging info of Step1 Task a)?

Reflection

1. What are some of the potential benefits of monitoring a network with SNMP, compared to Syslog?

    The SNMP protocol allows to remote monitor and control network devices. Syslog is just an alerting mechanism - it won't allow to remotely take action when an alarm happens. Syslog is often used for troubleshooting and debugging, while SNMP messages are used for device management and reporting.

2. Why is it preferable to solely use read-only access when working with SNMPv1 or SNMPv2?

    Read only community string - enables a remote device to retrieve "read-only" information from a device. Intermapper uses this information from devices on its maps.

3. Comparing SNMP MO data format, do you now other data formats, which are actual and which are more appropriate for automated machine-based parsing and processing?

Deliverables

Lab Teams

This lab may be solved in teams of max. 3 students. All teams have to provide their deliverables in time.

Teams are grouped into 2 groups, which have different due dates and presentation dates.

Module Group Exams

Each team member must solve the requested **Module Group Exams** before delivery date.

Deliverables

Each teams delivers the following documents and files:

- One **PDF-File (.pdf)** with the completed **Homework and Instructions**.
  All tasks and questions must be answered.

- One **PacketTracer-File** (.pkt) in PacketTracer Version 8 with your **final configuration**.

- One **Text-File in** ASCII-Format (.txt, simple Text Editor) with the **running configurations of Router WEST and Router R1.**

Due Dates

Group 1	Teams 1-10	Due Date
	Module Group Exams 6-12	20.6.- EOB
	Deliverable Upload	20.6. - EOB
	CCNA ZOOM Presentation	23.6. - 16:45 ff.

Group 2	Teams 11-20	Due Date
	Module Group Exams 6-12	27.6. - EOB
	Deliverable Upload	27.6. - EOB
	CCNA ZOOM Presentation	30.6. - 16:45 ff.

ENSA Final Exam and Skill Test

all	Module Group Exams 13-14	4.7. - EOB
all	ENSA Final Exam	7.7. – 16:45
all	ENSA Skill Test	7.7. – after F. E. latest 18:15