Unit 2 Performance Assessment 2 – SPAN port and Sniffer

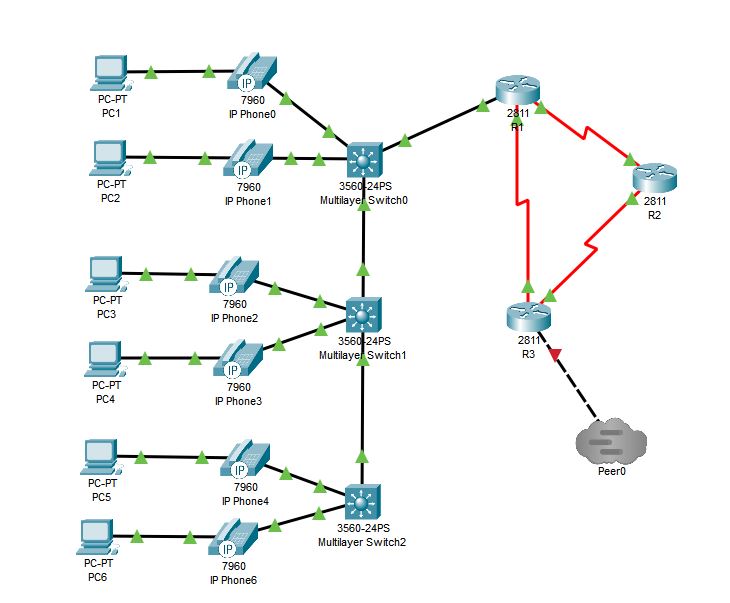
In this lab you will be using Packet Tracer. Make sure you save your lab as you will be using it to build the unit 3 Performance Assessments as well.

Your network will a class B network based on a number assigned by your professor, which you will be using for the duration of the class. In the lab anytime you see an underline you should fill in this number.

**Student network: 10.\_\_\_\_.0.0/16**

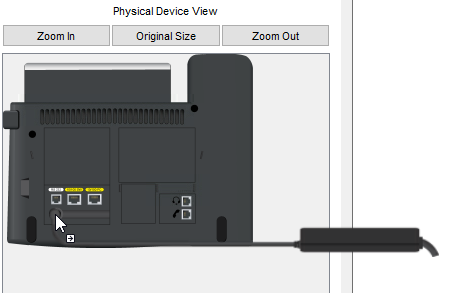
**Task 1 – Build network with IP phones**

**Using packet tracer create the network below. You will be using this network for the next two labs so make sure to get everything working properly. Note that you are using 3560 switches and 2811 routers. Keep in mind you will have to add serial modules to your routers.**

****

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System** | **Port** | **IP address** | **Subnet Mask** | **Clock Rate** | **Connect to** |
| R1 | Fa0/0.10 | 10.\_\_\_.1.1 | 255.255.255.192 |  | Sw1 |
|  | Fa0/0.20 | 10.\_\_\_.1.65 | 255.255.255.192 |  | Sw1 |
|  | S0/0/0 | 10.\_\_\_.5.1 | 255.255.255.252 | 500000 | R2 |
|  | S0/0/1 | 10.\_\_\_.5.10 | 255.255.255.252 |  | R3 |
| R2 | S0/0/0 | 10.\_\_\_.5.5 | 255.255.255.252 | 500000 | R3 |
|  | S0/0/1 | 10.\_\_\_.5.2 | 255.255.255.252 |  | R1 |
|  | Fa0/0 | 10.\_\_.2.1 | 255.255.255.0 |  | Sniffer (Task 3) |
| R3 | S0/0/0 | 10.\_\_\_.5.9 | 255.255.255.252 | 500000 | R1 |
|  | S0/0/1 | 10.\_\_\_.5.6 | 255.255.255.252 |  | R2 |
|  | Fa0/0 | 11.0.0.\_\_\_ | 255.255.255.0 |  | Peer0 |

You are going to be adding IP telephones to your network so drag them over into the network between the switch and the PC. You’ll also need to attach a power cord to the phone as shown below.



FA0/0.10 on R1 will be the default gateway for VLAN 10, and FA0/0.20 on R1 will be the default gateway for VLAN 20. You will need to configure each as a trunk for their respective VLANs.

***R1(config)#int fa0/0.10***

***R1(config-subif)#encapsulation dot1Q 10***

***R1(config-subif)#ip add 10.\_\_.1.1 255.255.255.192***

***R1(config)#int fa0/0.20***

***R1(config-subif)#encapsulation dot1Q 20***

***R1(config-subif)#ip add 10.\_\_.1.65 255.255.255.192***

When everything is powered up and working correctly put two DHCP pools onto the R1 router and pull an address to each PC.

Add DCHP Pools on R1 for VLAN 10 and VLAN 20

***R1(config)# ip dhcp pool mypool1***

***R1 (dhcp-config)# network 10.\_\_1.0 255.255.255.192***

***R1 (dhcp-config)# default-router 10.\_\_1.1***

***R1(config)# ip dhcp pool mypool2***

***R1 (dhcp-config)# network 10.\_\_1.64 255.255.255.192***

***R1 (dhcp-config)# default-router 10.\_\_1.65***

Configure VLANs and trunk ports on the switches. Here is an example of this for the top switch.

***Sw0 (config)# interface fa0/1***

***Sw0 (config)# switch mode access***

***Sw0 (config)# switcport access vlan 10***

***Sw0 (config)# interface fa0/2***

***Sw0 (config)# switch mode access***

***Sw0 (config)# switcport access vlan 20***

Now we need to configure the trunk ports- you will configure the port from the top switch connected to the router as a trunk port, as well as each interface that connect the switches together. Here is an example of how you should configure each trunk port.

***Sw0 (config)# interface range gig0/1-2***

***Sw0 (config)# switchport trunk encapsulation dot1q***

***Sw0 (config)# switchport mode trunk***

Add OSPF to each router

***R1(config)# router ospf 1***

***R1(config-router)# network 10.\_\_.1.0 0.0.0.63 area 1***

***R1(config-router)# network 10.\_\_.1.64 0.0.0.63 area 1***

***R1(config-router)# network 10.\_\_.5.0 0.0.0.3 area 0***

***R1(config-router)# network 10.\_\_.5.8 0.0.0.3 area 0***

***R2(config)# router ospf 1***

***R2(config-router)# network 10.\_\_.5.0 0.0.0.3 area 0***

***R2(config-router)# network 10.\_\_.5.4 0.0.0.3 area 0***

***R3(config)# router ospf 1***

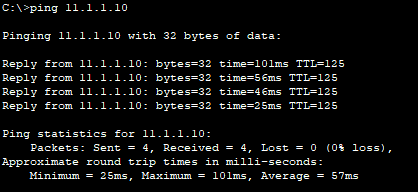
***R3(config-router)# network 10.\_\_.5.4 0.0.0.3 area 0***

***R3(config-router)# network 10.\_\_.5.8 0.0.0.3 area 0***

***R3(config-router)# network 11.0.0.0 0.0.0.255 area 0***

Pull your **show ip route** from the R2 router. Take a screenshot

Connect your network to the Tier1 network and ping from PC1 to the Tier1 Internet Server



**Deliverables**

* Screenshot of your working network
* Screenshot of *show ip route* from the R2 router
* Screenshot of a *ping* from PC1 to the Tier1 Internet Server

PASTE SCREENSHOTS BELOW

**Task 2 – Add SPAN**

Switched Port Analyzer (SPAN) protocol is implemented in the switch and involves programming the switch to duplicate or mirror packets going in or out of the ports on the switch. To do this, use the *monitor session number source interface interface-type interface-number* command. This specifies the source interface that is the interface to be monitored. If you are putting the monitor on more than one interface you can put a space, dash, space and the end number of the monitor. The destination interface is specified in a similar way using the monitor session number destination interface interface-type interface-number command. You must use the same session number in both lines, indicating that they are the same monitoring session.

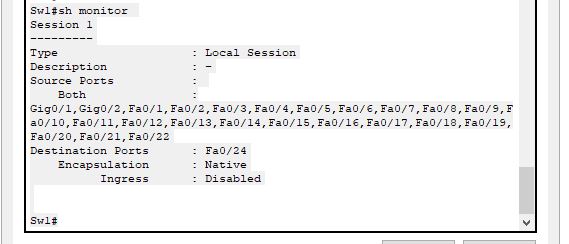
*Sw1(config)#* ***monitor session 1 source interface FastEthernet 0/1 – 23***

*Sw1(config)#* ***monitor session 1 source interface GigabitEthernet 0/1 - 2***

*Sw1(config)#* ***monitor session 1 destination interface fastethernet 0/24***

It is important to note that when an interface is a SPAN destination interface, the only traffic sent out of the destination interface is the traffic from the SPAN session so no network communication is possible on the SPAN port. The SPAN port is for monitoring only.

You can verify the configuration using the ***show monitor*** command. Take a screenshot.



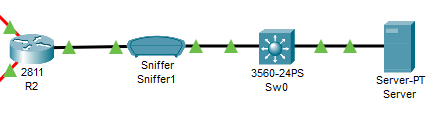
**Deliverables**

* Screenshot the *show monitor* command on Sw1

PASTE SCREENSHOTS BELOW

**Task 3 – Add a sniffer**

In this task you will add a sniffer, switch and a sever to your network and connect to R2 router. Add the sniffer and these devices per the image below:

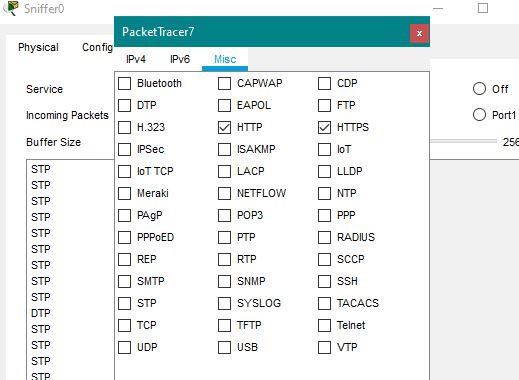
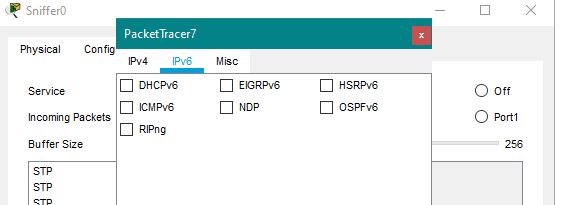
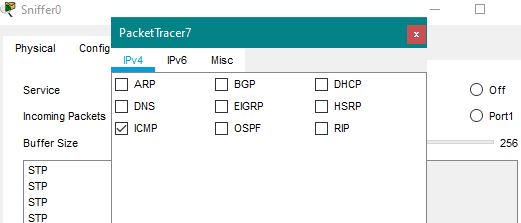


Your new network on R2 will be 10.\_\_\_.2.0/24 and you will need to assign your server a static address in this network (don’t forget the subnet mask and default gateway as well). Add the new network into your OSPF networks:

***R2(config)# router ospf 1***

***R2(config-router)# network 10.\_\_\_.2.0 0.0.0.255 area 0***

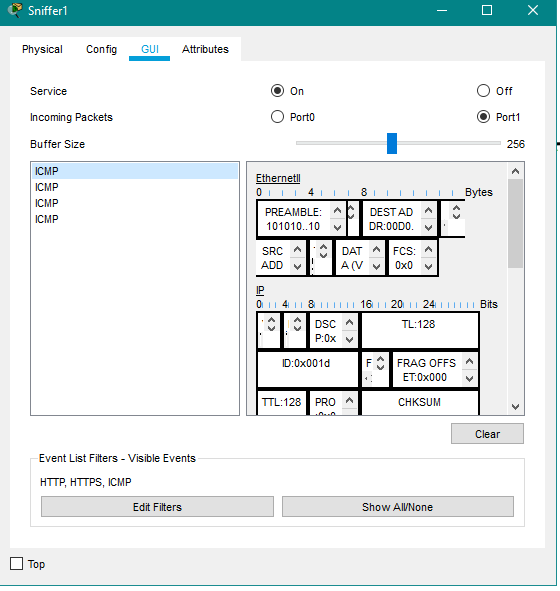
Now we will configure the sniffer to only capture ICMP, HTTP and HTTPS packets.





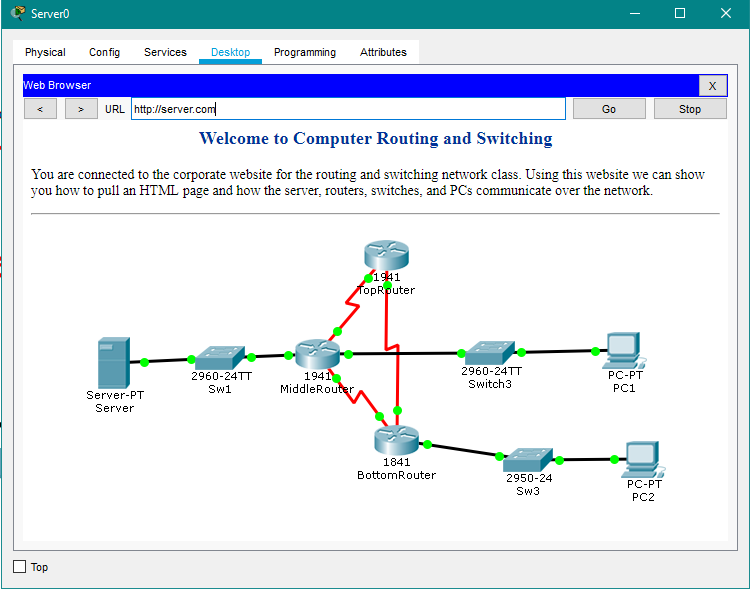
This means your sniffer will only display packet types of HTTP, HTTPS, and ICMP.

Verify that your sniffer is working properly by pinging from the server to the Tier1 Internet Server. Take a screenshot of your working network.



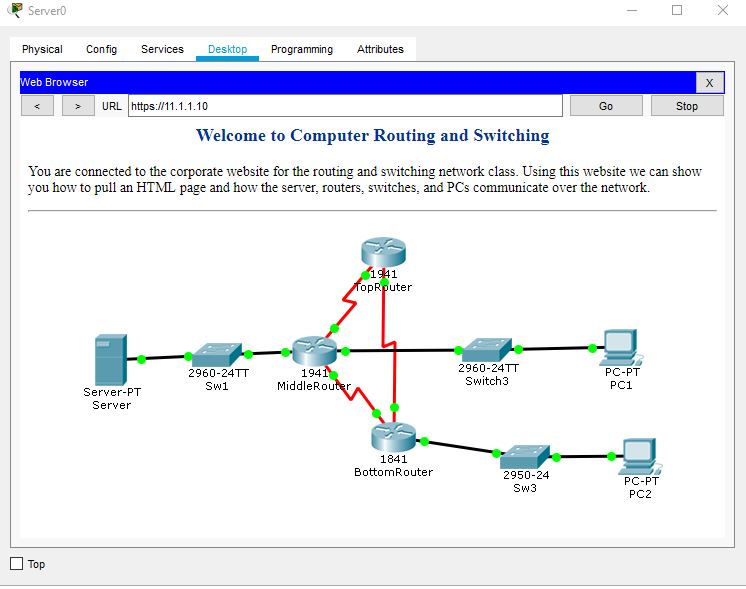
Click on one of the ICMP packets. What is the source IP? What is the destination IP? What other interesting information do you see in the packet?

Go to server and configure 11.1.1.10 as its DNS Server (the Internet Server’s address) and pull up the webpage on the Tier1 Internet Server. What type of packets were captured in the sniffer? How do they differ from the ICMP packets?



Finally go into the server and pull the secure webpage using https://11.1.1.10.

What is the difference between these packets (HTTPS) and the HTTP packets?



**Deliverables**

* Screenshot of you working network
* Answer question about ICMP packets
* Answer question about HTTP packets
* Answer question about HTTPS packets

PASTE SCREENSHOTS BELOW