ELEC-5220

Info. Networks

FROM: Jacob Howard

GROUP: 6

TO: Dr. Yihan Li & Chao Yang,

DUE DATE: 11/16/21

Lab 6

Introduction

In this lab, we worked worked in groups by configurating routers for vlans and firewalls.

Part 1

Q1: Can host 1 ping host 2 and host3 successfully? Why or Why not?

Ping to host 2 was successful, ping to host 3 was timed out. Hos3 ping had 50% loss.

```
C:\Users\Authorized User>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:
Reply from 100.100.100.2: bytes=32 time=1ms TTL=128
Reply from 100.100.100.2: bytes=32 time<1ms TTL=128
Reply from 100.100.100.2: bytes=32 time<1ms TTL=128
Reply from 100.100.100.2: bytes=32 time<1ms TTL=128

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Authorized User>ping 172.25.25.2

Pinging 172.25.25.2 with 32 bytes of data:
Request timed out.
Reply from 100.100.100.3: Destination host unreachable.
Reply from 100.100.100.3: Destination host unreachable.
Request timed out.

Ping statistics for 172.25.25.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

Q2: Can two subnets connect to each other? Briefly explain why host 1 or 2 can ping host 3 without static routing table? (the answer is related to the routing entries.)

Yes. Setting up correct VLANs allows for this.

```
C:\Users\Authorized User>ping 172.25.25.2

Pinging 172.25.25.2 with 32 bytes of data:
Reply from 100.100.100.1: bytes=32 time=2ms TTL=254
Reply from 100.100.100.1: bytes=32 time=1ms TTL=254
Reply from 100.100.100.1: bytes=32 time=2ms TTL=254
Reply from 100.100.100.1: bytes=32 time=1ms TTL=254

Ping statistics for 172.25.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

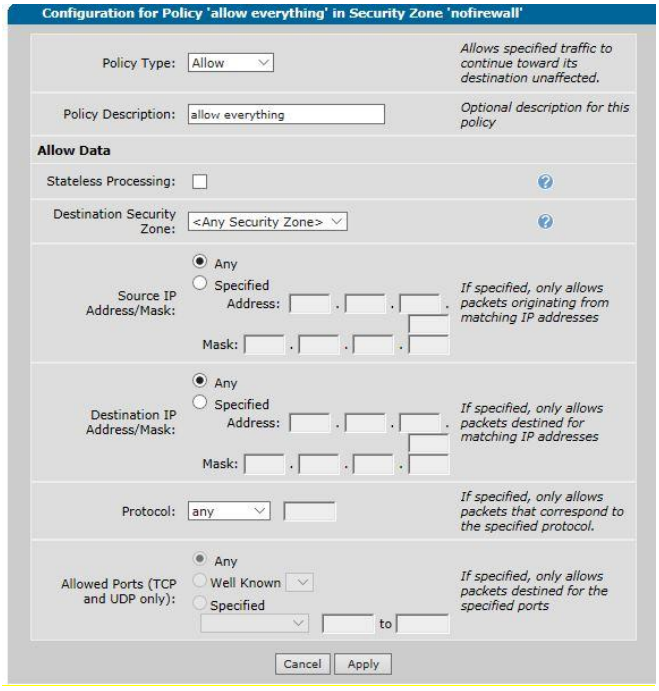
```
C:\Users\Authorized User>ping 100.100.100.1

Pinging 100.100.100.1 with 32 bytes of data:
Reply from 100.100.100.1: bytes=32 time=2ms TTL=254
Reply from 100.100.100.1: bytes=32 time=2ms TTL=254
Reply from 100.100.100.1: bytes=32 time=2ms TTL=254
Reply from 100.100.100.1: bytes=32 time=1ms TTL=254

Ping statistics for 100.100.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Q3: Briefly explain why "Public" security zone can block the transmission from host 1 to host 2, 3? (the answer should be related to the policy used in the security zone)

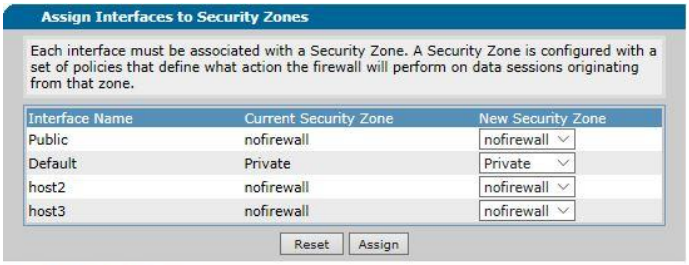
Public Network security zones have firewalls whitch prevent certain traffic from coming in. Private networks can still have firewalls, but they allow a lot more traffic in if there is a firewall present. Private networks often have no firewall.

Q4: Which policy is used in your "nofirewall" security zone? How does it work

We used the "allow" policy, as we want to allow all traffic in and out. Security zone had to be set to any security zone to work though.



Screenshots of ex2 settings below

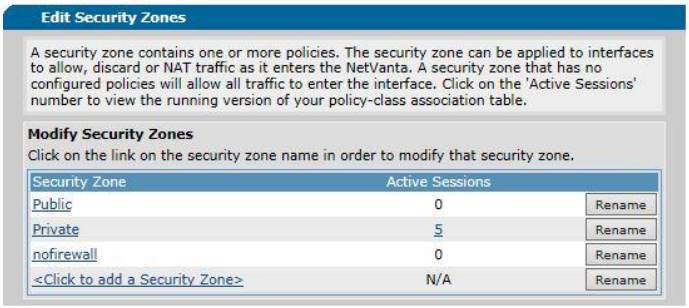


Assign Interfaces to Security Zones

Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions originating from that zone.

Interface Name	Current Security Zone	New Security Zone
Public	nofirewall	nofirewall
Default	Private	Private
host2	nofirewall	nofirewall
host3	nofirewall	nofirewall

Reset Assign



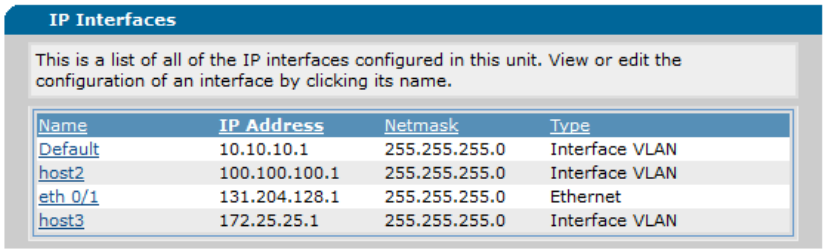
Edit Security Zones

A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

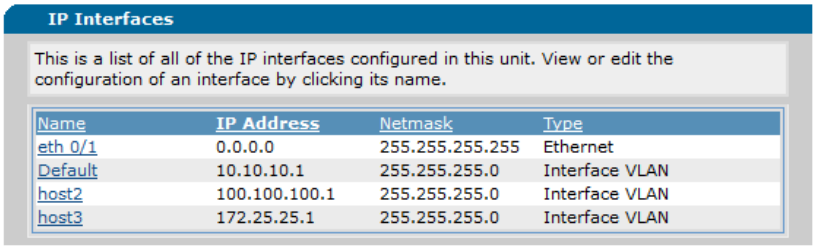
Security Zone	Active Sessions	
Public	0	Rename
Private	5	Rename
nofirewall	0	Rename
<Click to add a Security Zone>	N/A	Rename



IP Interfaces

This is a list of all of the IP interfaces configured in this unit. View or edit the configuration of an interface by clicking its name.

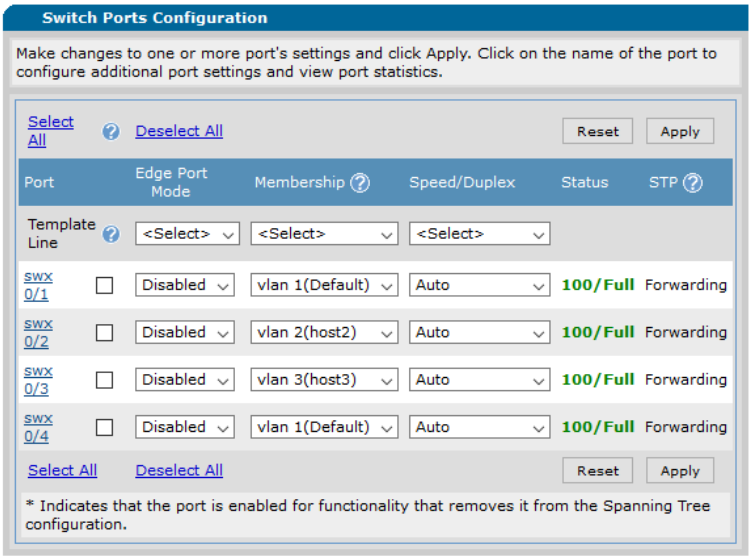
Name	IP Address	Netmask	Type
Default	10.10.10.1	255.255.255.0	Interface VLAN
host2	100.100.100.1	255.255.255.0	Interface VLAN
eth 0/1	131.204.128.1	255.255.255.0	Ethernet
host3	172.25.25.1	255.255.255.0	Interface VLAN



IP Interfaces

This is a list of all of the IP interfaces configured in this unit. View or edit the configuration of an interface by clicking its name.

Name	IP Address	Netmask	Type
eth 0/1	0.0.0.0	255.255.255.255	Ethernet
Default	10.10.10.1	255.255.255.0	Interface VLAN
host2	100.100.100.1	255.255.255.0	Interface VLAN
host3	172.25.25.1	255.255.255.0	Interface VLAN



Switch Ports Configuration

Make changes to one or more port's settings and click Apply. Click on the name of the port to configure additional port settings and view port statistics.

Select All | Deselect All | Reset | Apply

Port	Edge Port Mode	Membership	Speed/Duplex	Status	STP
Template Line	<Select>	<Select>	<Select>		
swx 0/1	Disabled	vlan 1(Default)	Auto	100/Full	Forwarding
swx 0/2	Disabled	vlan 2(host2)	Auto	100/Full	Forwarding
swx 0/3	Disabled	vlan 3(host3)	Auto	100/Full	Forwarding
swx 0/4	Disabled	vlan 1(Default)	Auto	100/Full	Forwarding

Select All | Deselect All | Reset | Apply

* Indicates that the port is enabled for functionality that removes it from the Spanning Tree configuration.

Part 2

Q1: Consider the ping request packet on both hosts, what's the source IP address? What's the destination IP address? Are these two source IP addresses same with each other? Why?

Q2: Consider the ping request packet on both hosts, what's the source IP address? What's the destination IP address? Are these two source IP addresses same with each other? Why?

The source and destination IP depends on who is pinging who. For Host1 to Host2, the source IP is 100.100.100.2 and destination IP is 131.204.120.2, and for Host2 to Host1, the source IP is 131.204.120.2 and the destination IP is 123.123.123.123. This is due to how we set up the NAT in security. Screenshots are shown below.

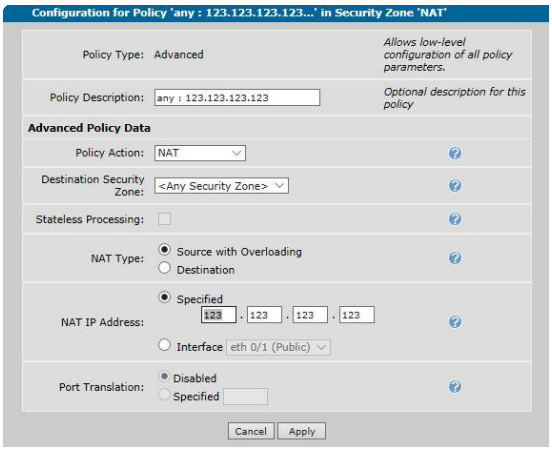
3	2.984394	100.100.100.2	131.204.128.2	ICMP	74 Echo (ping) request id=0x0001, seq=3997/40207, ttl=128 (reply in 4)
4	2.985329	131.204.128.2	100.100.100.2	ICMP	74 Echo (ping) reply id=0x0001, seq=3997/40207, ttl=127 (request in 3)
5	4.000213	Adtran_39:29:2e	Spanning-tree-(for-bridges)_00	STP	60 RST. Root = 32768/0/00:a0:c8:39:29:2b Cost = 0 Port = 0x8003
6	4.000274	100.100.100.2	131.204.128.2	ICMP	74 Echo (ping) request id=0x0001, seq=3998/40463, ttl=128 (reply in 7)
7	4.001522	131.204.128.2	100.100.100.2	ICMP	74 Echo (ping) reply id=0x0001, seq=3998/40463, ttl=127 (request in 6)
8	5.016022	100.100.100.2	131.204.128.2	ICMP	74 Echo (ping) request id=0x0001, seq=3999/40719, ttl=128 (reply in 9)
9	5.016937	131.204.128.2	100.100.100.2	ICMP	74 Echo (ping) reply id=0x0001, seq=3999/40719, ttl=127 (request in 8)
10	6.000324	Adtran_39:29:2e	Spanning-tree-(for-bridges)_00	STP	60 RST. Root = 32768/0/00:a0:c8:39:29:2b Cost = 0 Port = 0x8003
11	6.031698	100.100.100.2	131.204.128.2	ICMP	74 Echo (ping) request id=0x0001, seq=4000/40975, ttl=128 (reply in 12)
12	6.032984	131.204.128.2	100.100.100.2	ICMP	74 Echo (ping) reply id=0x0001, seq=4000/40975, ttl=127 (request in 11)
13	7.797437	WistronI_57:54:1c	Adtran_39:29:2d	ARP	42 Who has 100.100.100.1? Tell 100.100.100.2
14	7.798109	Adtran_39:29:2d	WistronI_57:54:1c	ARP	60 100.100.100.1 is at 00:a0:c8:39:29:2d
15	8.000383	Adtran_39:29:2e	Spanning-tree-(for-bridges)_00	STP	60 RST. Root = 32768/0/00:a0:c8:39:29:2b Cost = 0 Port = 0x8003
16	9.753724	100.100.100.2	100.100.100.255	BROWSER	243 Local Master Announcement BRN312-03, Workstation, Server, NT Workstation, Potential Browser, Ma
17	10.000487	Adtran_39:29:2e	Spanning-tree-(for-bridges)_00	STP	60 RST. Root = 32768/0/00:a0:c8:39:29:2b Cost = 0 Port = 0x8003
18	11.911826	Adtran_39:29:2e	LLDP_Multicast	LLDP	252 TTL = 120 System Name = NetVanta3120 System Description = NetVanta 3120, Version: 17.02.01.00.E

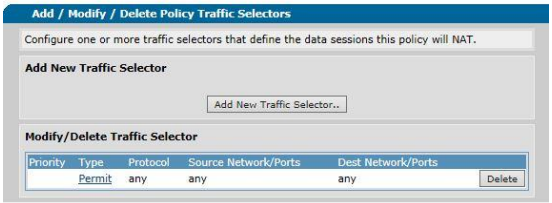
Host 1 to Host 2

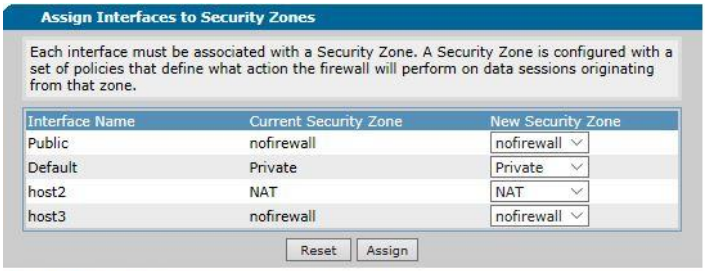
No.	Time	Source	Destination	Protocol	Length	Info
1	14:52:46.572436	123.123.123.123	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3985/37135, ttl=127 (reply in 2)
2	14:52:46.572499	131.204.128.2	123.123.123.123	ICMP	74	Echo (ping) reply id=0x0001, seq=3985/37135, ttl=128 (request in 1)
3	14:52:47.575163	123.123.123.123	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3986/37391, ttl=127 (reply in 4)
4	14:52:47.575209	131.204.128.2	123.123.123.123	ICMP	74	Echo (ping) reply id=0x0001, seq=3986/37391, ttl=128 (request in 3)
5	14:52:48.591243	123.123.123.123	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3987/37647, ttl=127 (reply in 6)
6	14:52:48.591291	131.204.128.2	123.123.123.123	ICMP	74	Echo (ping) reply id=0x0001, seq=3987/37647, ttl=128 (request in 5)
7	14:52:49.606813	123.123.123.123	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3988/37903, ttl=127 (reply in 8)
8	14:52:49.606857	131.204.128.2	123.123.123.123	ICMP	74	Echo (ping) reply id=0x0001, seq=3988/37903, ttl=128 (request in 7)
9	14:52:51.354140	WistronI_57:51:06	Adtran_39:29:30	ARP	42	Who has 131.204.128.1? Tell 131.204.128.2
10	14:52:51.354846	Adtran_39:29:30	WistronI_57:51:06	ARP	64	131.204.128.1 is at 00:a0:c8:39:29:30

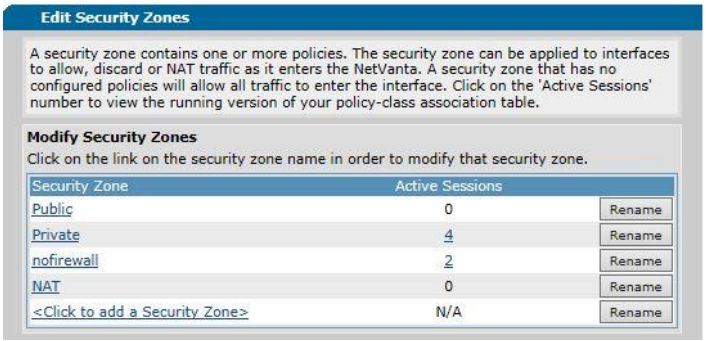
Host 2 to Host 1

Router Settings









Q3: Assume we want to configure the lab router's routing table based on the network structure. Please show its static routing entries for host2 and host3.

Unfortinately, we do not have outputs for the end of the lab. The TA checked that our setup was correct, but we could not ping anything correctly. Our routing table is shown below.