

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 in groups by configuring 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. Host 3 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 which 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.

Configuration for Policy 'allow everything' in Security Zone 'nofirewall'	
Policy Type: <input type="text" value="Allow"/>	Allows specified traffic to continue toward its destination unaffected.
Policy Description: <input type="text" value="allow everything"/>	Optional description for this policy
Allow Data	
Stateless Processing: <input type="checkbox"/>	
Destination Security Zone: <input type="text" value="<Any Security Zone>"/>	
Source IP Address/Mask: <div> <input checked="" type="radio"/> Any <div> <input type="radio"/> Specified Address: <input type="text" value=""/><input type="text" value=""/><input type="text" value=""/> Mask: <input type="text" value=""/><input type="text" value=""/><input type="text" value=""/> </div> </div>	If specified, only allows packets originating from matching IP addresses
Destination IP Address/Mask: <div> <input checked="" type="radio"/> Any <div> <input type="radio"/> Specified Address: <input type="text" value=""/><input type="text" value=""/><input type="text" value=""/> Mask: <input type="text" value=""/><input type="text" value=""/><input type="text" value=""/> </div> </div>	If specified, only allows packets destined for matching IP addresses
Protocol: <input type="text" value="any"/>	If specified, only allows packets that correspond to the specified protocol.
Allowed Ports (TCP and UDP only): <div> <input checked="" type="radio"/> Any <div> <input type="radio"/> Well Known <input type="text" value=""/> <input type="radio"/> Specified <input type="text" value=""/> to <input type="text" value=""/> </div> </div>	If specified, only allows packets destined for the specified ports
<div> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> </div>	

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	<input type="checkbox"/> Disabled ▼	vlan 1(Default) ▼	Auto ▼	100/Full	Forwarding
SWX 0/2	<input type="checkbox"/> Disabled ▼	vlan 2(host2) ▼	Auto ▼	100/Full	Forwarding
SWX 0/3	<input type="checkbox"/> Disabled ▼	vlan 3(host3) ▼	Auto ▼	100/Full	Forwarding
SWX 0/4	<input type="checkbox"/> 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.

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	Public	Public <input type="button" value="v"/>
Default	Private	Private <input type="button" value="v"/>
host2	nofirewall	nofirewall <input type="button" value="v"/>
host3	nofirewall	nofirewall <input type="button" value="v"/>

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	<input type="button" value="Rename"/>
Private	2	<input type="button" value="Rename"/>
nofirewall	0	<input type="button" value="Rename"/>
<Click to add a Security Zone>	N/A	<input type="button" value="Rename"/>

Route Table

This is the running version of your route table. Click on the name of a route to use it as a template for a new route in the table above. Only static routes can be deleted.

Route Type : Please select the route type you wish to display.

rows per page Page 1 of 1

Destination	Mask	Next Hop	Dist	Type	
0.0.0.0	0.0.0.0	10.10.10.1	1	Static	<input type="button" value="Delete"/>
10.10.10.0	255.255.255.0	0.0.0.0	0	Connected	
100.100.100.0	255.255.255.0	0.0.0.0	0	Connected	

rows per page Page 1 of 1

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

Configuration for Policy 'any : 123.123.123.123...' in Security Zone 'NAT'

Policy Type: Advanced

Allows low-level configuration of all policy parameters.

Policy Description: any : 123.123.123.123

Optional description for this policy

Advanced Policy Data

Policy Action: NAT

Destination Security Zone: <Any Security Zone>

Stateless Processing: ☐

NAT Type: ☒ Source with Overloading ☐ Destination

NAT IP Address: ☒ Specified 123, 123, 123, 123 ☐ Interface eth 0/1 (Public)

Port Translation: ☒ Disabled ☐ Specified

Cancel

Apply

Add / Modify / Delete Policy Traffic Selectors

Configure one or more traffic selectors that define the data sessions this policy will NAT.

Add New Traffic Selector

Add New Traffic Selector...

Modify/Delete Traffic Selector

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports	
	Permit	any	any	any	Delete

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	NAT	NAT
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	4	Rename
nofirewall	2	Rename
NAT	0	Rename
<Click to add a Security Zone>	N/A	Rename

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.

Unfortunately, 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.

Add a Static Route to the Route Table

Static Routes are often required to reach networks that are not learned via a dynamic routing protocol. Enter the appropriate information below to add a static route or click on a route below to use it as a template for a new route. [IP Routing](#) must be enabled in order to add static routes.

Destination Address:	<input type="text" value="128"/> . <input type="text" value="238"/> . <input type="text" value="66"/> . <input type="text" value="0"/>	Enter the network to add to the route table.
Destination Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>	Enter the appropriate mask for this network.
Gateway:		
<input checked="" type="radio"/> Address	<input type="text" value="131"/> . <input type="text" value="204"/> . <input type="text" value="128"/> . <input type="text" value="2"/>	Enter the gateway address to reach this network.
<input type="radio"/> Interface	<Select Interface> ▾	- OR - Select the interface to be used as the gateway.
Administrative Distance (optional):	<input type="text" value="1"/>	The Distance metric for this network. (Optional parameter)
Tag (optional):	<input type="text" value="0"/>	Set an administrative tag on this route (Optional parameter)
Track Name (optional):	None ▾	Activates this route only while the specified track is not failing. (Optional parameter used when network monitoring is active.)

Route Table

This is the running version of your route table. Click on the name of a route to use it as a template for a new route in the table above. Only static routes can be deleted.

Route Type :

All

Please select the route type you wish to display.

10

 rows per page

Page 1 of 1

Destination	Mask	Next Hop	Dist	Type	
0.0.0.0	0.0.0.0	10.10.10.1	1	Static	<div>Delete</div>
10.10.10.0	255.255.255.0	0.0.0.0	0	Connected	
100.100.100.0	255.255.255.0	0.0.0.0	0	Connected	
128.238.66.0	255.255.255.0	131.204.128.2	1	Static	<div>Delete</div>
131.204.128.0	255.255.255.0	0.0.0.0	0	Connected	

10

 rows per page

Page 1 of 1