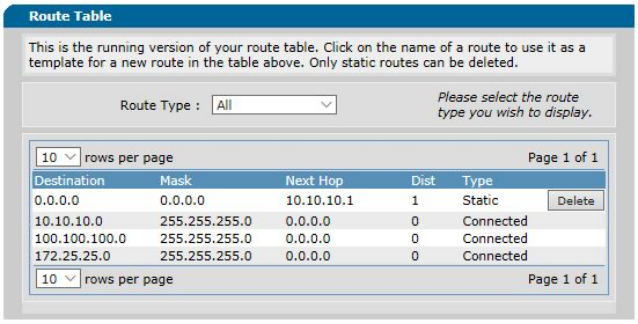
Gabriel Emerson
ELEC 5220 - Lab 6
11/16/21

Exercise 1-1

```
Command Prompt
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Authorized User>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ecbd:43cd:2a6:ce6e%15
   IPv4 Address. . . . . . . . . . . : 10.10.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1

C:\Users\Authorized User>
```



Route Table

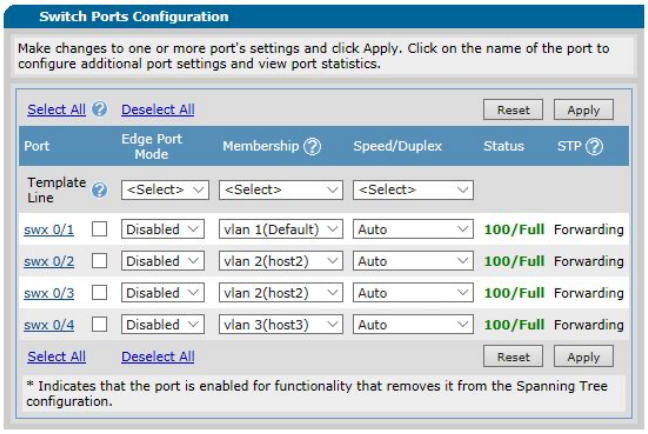
This is the running version of your route table. Click on the name of a route to use it as a template for a new route in the table above. Only static routes can be deleted.

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	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	
172.25.25.0	255.255.255.0	0.0.0.0	0	Connected	

10 rows per page — Page 1 of 1



Switch Ports Configuration

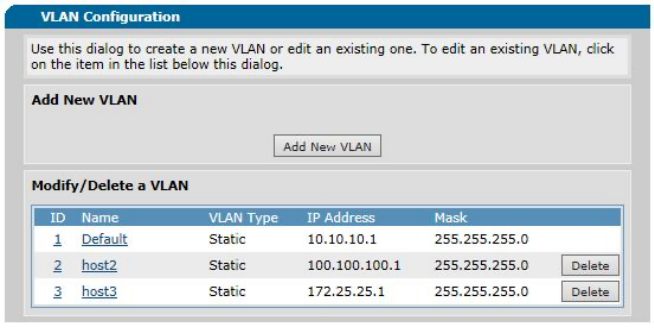
Make changes to one or more port's settings and click Apply. Click on the name of the port to configure additional port settings and view port statistics.

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 2(host2)	Auto	100/Full	Forwarding
swx 0/4	Disabled	vlan 3(host3)	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.



VLAN Configuration

Use this dialog to create a new VLAN or edit an existing one. To edit an existing VLAN, click on the item in the list below this dialog.

Add New VLAN

Add New VLAN

Modify/Delete a VLAN

ID	Name	VLAN Type	IP Address	Mask	
1	Default	Static	10.10.10.1	255.255.255.0	
2	host2	Static	100.100.100.1	255.255.255.0	Delete
3	host3	Static	172.25.25.1	255.255.255.0	Delete

Setup Exercise 1-2

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

Configuration for Policy 'any : eth 0/1' in Security Zone 'nofirewall'

Policy Type: Advanced — *Allows low-level configuration of all policy parameters.*

Policy Description: any : eth 0/1 — *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 . . . . / 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	nofirewall	nofirewall
host3	nofirewall	nofirewall

Reset Assign

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
Default	Private	Private
host2	Private	Private
host3	Private	Private

Reset Assign

Exercise 2-1

```
C:\Users\Authorized User>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 100.100.100.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 100.100.100.1

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 = 0ms, Average = 0ms

C:\Users\Authorized User>172.25.25.2
'172.25.25.2' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Authorized User>ping 172.25.25.2

Pinging 172.25.25.2 with 32 bytes of data:
Reply from 172.25.25.2: bytes=32 time=5ms TTL=127
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127

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 = 5ms, Average = 2ms
```

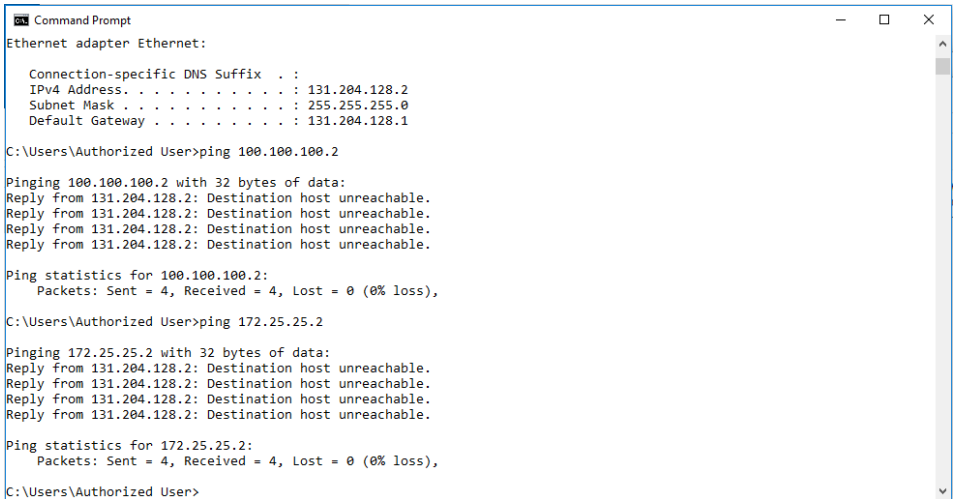
Q1: Can host 1 ping host 2 and host3 successfully? Why or Why not?

Yes, the host 1 can see both host 2 and 3 currently through the router.

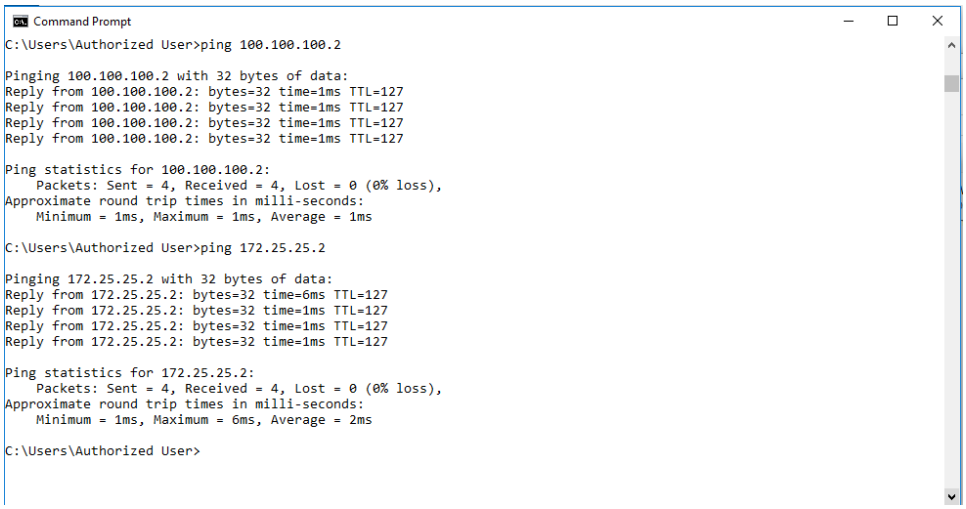
Q2: Can two subnets connect to each other? Briefly explain why host 1 or 2 can ping host 3 without static routing table?

They can. Static routing (through routing entries) is used to define an exit point from the router when no other points are seen.

Exercise 2-2



Pre-Firewall



Post-Firewall

Q3: Briefly explain why “Public” security zone can block the transmission from host 1 to host 2, host3? (the answer should be related to the policy used in the security zone).

The "public" security zone doesn't work because host 2 and 3 are on the other side of the firewall from host 1.

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

The policy we used in the "nofirewall" security zone was Many:1 NAPT. It simply makes host 1's IP an access point, so we can avoid the firewall block completely.

Exercise 2-1 Part 2

```
Microsoft Windows [Version 10.0.16299.19]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Authorized User>ping 172.25.25.2

Pinging 172.25.25.2 with 32 bytes of data:
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127
Reply from 172.25.25.2: bytes=32 time=1ms TTL=127

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 = 1ms, Average = 1ms

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=2ms TTL=127
Reply from 100.100.100.2: bytes=32 time=1ms TTL=127
Reply from 100.100.100.2: bytes=32 time=1ms TTL=127
Reply from 100.100.100.2: bytes=32 time<1ms TTL=127

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 = 2ms, Average = 1ms

C:\Users\Authorized User>
```

Host 1→3 and Host 3 →1

→	1 0.000000	131.204.128.1	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1517/60677, ttl=127 (reply in 2)
←	2 0.000062	131.204.128.2	131.204.128.1	ICMP	74	Echo (ping) reply id=0x0001, seq=1517/60677, ttl=128 (request in 1)
	3 1.008542	131.204.128.1	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1518/60933, ttl=127 (reply in 4)
	4 1.008586	131.204.128.2	131.204.128.1	ICMP	74	Echo (ping) reply id=0x0001, seq=1518/60933, ttl=128 (request in 3)
	5 2.013042	131.204.128.1	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1519/61189, ttl=127 (no response found!)
	6 2.013088	131.204.128.2	131.204.128.1	ICMP	74	Echo (ping) reply id=0x0001, seq=1519/61189, ttl=128 (request in 5)
	7 3.028555	131.204.128.1	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1520/61445, ttl=127 (reply in 8)
	8 3.028603	131.204.128.2	131.204.128.1	ICMP	74	Echo (ping) reply id=0x0001, seq=1520/61445, ttl=128 (request in 7)
	9 4.644086	WistronI_57:51:06	Adtran_39:27:80	ARP	42	Who has 131.204.128.1? Tell 131.204.128.2
	10 4.644809	Adtran_39:27:80	WistronI_57:51:06	ARP	64	131.204.128.1 is at 00:a0:c8:39:27:80 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]

	1 0.000000	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	2 2.000109	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	3 4.000162	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	4 5.491448	Adtran_39:27:7f	LLDP_Multicast	LLDP	252	TTL = 120 System Name = NetVanta3120 System Description = NetVanta 3120, Version: 17.02.01.00.E, Date: Fri Apr 04 07:16:54 2008
	5 6.000300	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	6 8.000169	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	7 9.447694	172.25.25.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1517/60677, ttl=128 (no response found!)
	8 9.448803	131.204.128.2	172.25.25.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1517/60677, ttl=127 (request in 7)
	9 10.000421	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	10 10.456291	172.25.25.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1518/60933, ttl=128 (reply in 11)
	11 10.457518	131.204.128.2	172.25.25.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1518/60933, ttl=127 (request in 10)
	12 11.460747	172.25.25.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1519/61189, ttl=128 (reply in 13)
	13 11.461943	131.204.128.2	172.25.25.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1519/61189, ttl=127 (request in 12)
	14 12.000504	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	15 12.476478	172.25.25.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=1520/61445, ttl=128 (no response found!)
	16 12.477487	131.204.128.2	172.25.25.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1520/61445, ttl=127 (request in 15)
	17 14.000569	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004
	18 14.013432	WistronI_57:51:09	Adtran_39:27:7f	ARP	42	Who has 172.25.25.1? Tell 172.25.25.2
	19 14.014283	Adtran_39:27:7f	WistronI_57:51:09	ARP	60	172.25.25.1 is at 00:a0:c8:39:27:7f
	20 16.000671	Adtran_39:27:7f	Spanning-tree-(for-b…	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8004

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?

No they are not the same. This is due to not being routed through the NAT security zone, so host1 does not see all properties of host3 and vice versa.

Host 1→2 and Host 2 →1

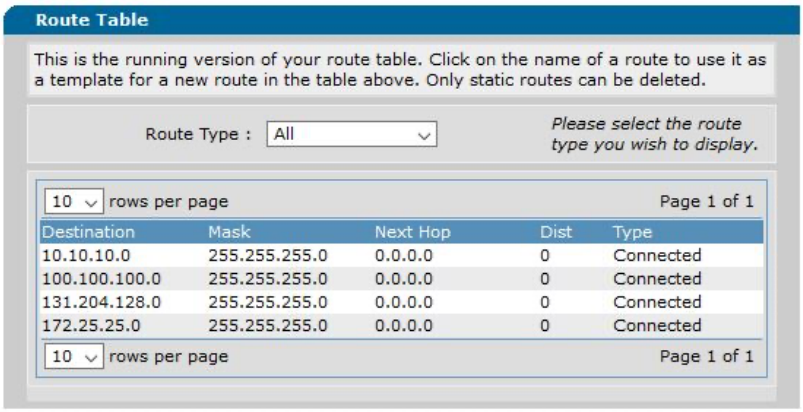
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3610/6670, ttl=127 (reply in 2)
2	0.000050	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3610/6670, ttl=128 (request in 1)
3	1.002703	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3611/6926, ttl=127 (reply in 4)
4	1.002748	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3611/6926, ttl=128 (request in 3)
5	2.018276	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3612/7182, ttl=127 (no response found!)
6	2.018324	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3612/7182, ttl=128 (request in 5)
7	3.034302	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3613/7438, ttl=127 (reply in 8)
8	3.034354	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3613/7438, ttl=128 (request in 7)
9	4.940672	WistronI_57:51:06	Adtran_39:27:80	ARP	42	Who has 131.204.128.1? Tell 131.204.128.2
10	4.941409	Adtran_39:27:80	WistronI_57:51:06	ARP	64	131.204.128.1 is at 00:a0:c8:39:27:80 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]

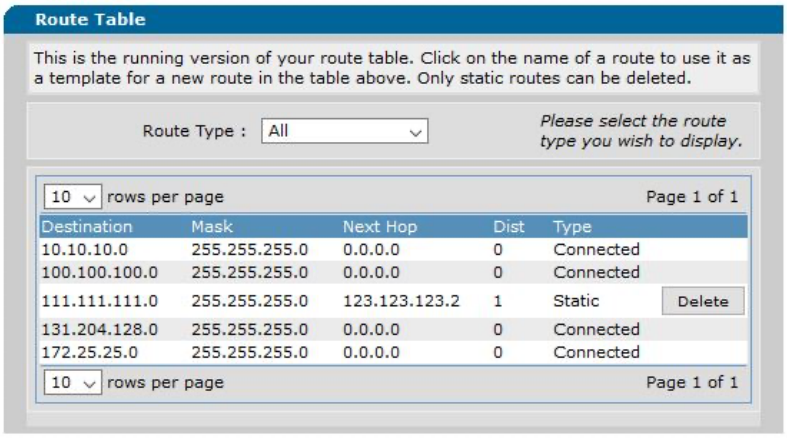
1	0.000000	Adtran_39:27:7e	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8003
2	2.000078	Adtran_39:27:7e	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8003
3	4.000135	Adtran_39:27:7e	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8003
4	4.057675	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3610/6670, ttl=128 (reply in 5)
5	4.060248	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3610/6670, ttl=127 (request in 4)
6	5.061423	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3611/6926, ttl=128 (reply in 7)
7	5.062563	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3611/6926, ttl=127 (request in 6)
8	6.000203	Adtran_39:27:7e	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8003
9	6.077139	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3612/7182, ttl=128 (reply in 10)
10	6.078097	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3612/7182, ttl=127 (request in 9)
11	7.092877	100.100.100.2	131.204.128.2	ICMP	74	Echo (ping) request id=0x0001, seq=3613/7438, ttl=128 (reply in 12)
12	7.094131	131.204.128.2	100.100.100.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3613/7438, ttl=127 (request in 11)
13	8.000266	Adtran_39:27:7e	Spanning-tree-(for-bridges)_00	STP	60	RST. Root = 32768/0/00:a0:c8:39:27:7b Cost = 0 Port = 0x8003
14	8.386049	Adtran_39:27:7e	LLDP_Multicast	LLDP	252	TTL = 120 System Name = NetVanta3120 System Description = NetVanta 3120, Version: 17.02.01.00.E, Date: Fri Apr 04 07:16:54 2008
15	8.874249	WistronI_57:54:1c	Adtran_39:27:7d	ARP	42	Who has 100.100.100.1? Tell 100.100.100.2
16	8.874965	Adtran_39:27:7d	WistronI_57:54:1c	ARP	60	100.100.100.1 is at 00:a0:c8:39:27:7d

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?

They are the same. Because they are both being routed through the NAT.

Exercise 2-2 Part 2





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.

Did not get screenshots -- These would look similar to how the screenshots above look, however, it would be the destination, and mask of host 2 and of host 3.