

Dillen Dela Cruz

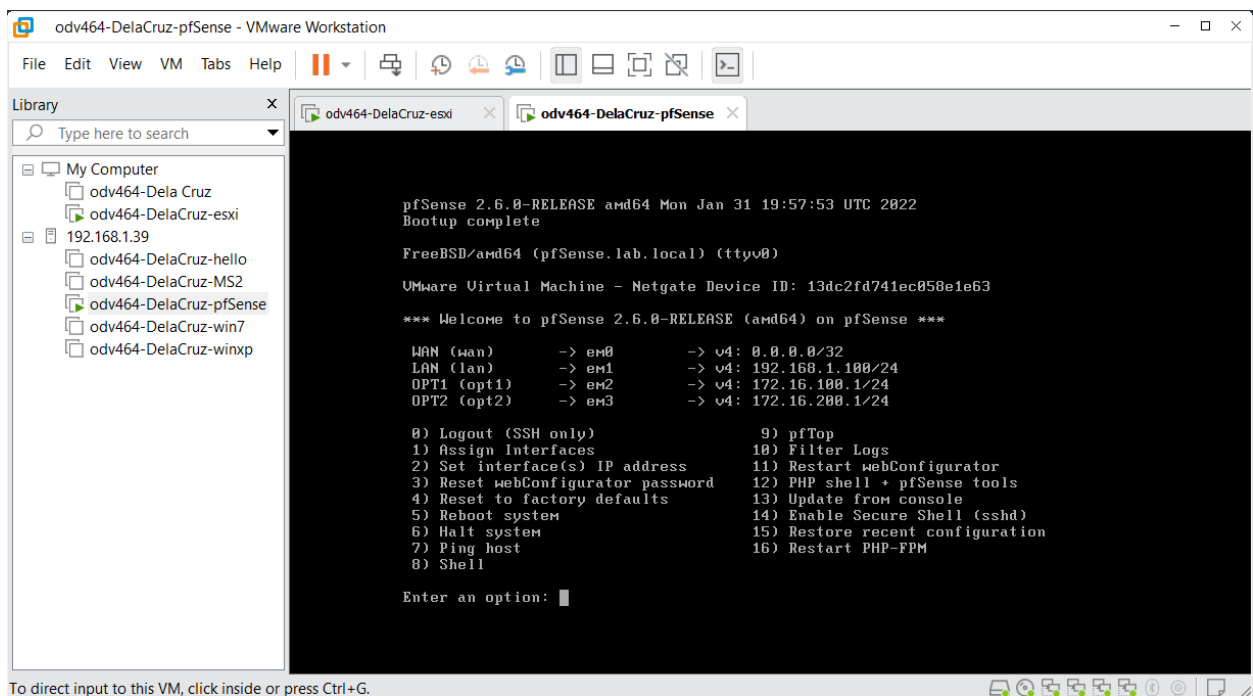
9/28/2023

IS-4543-002-202410

Lab 2 Part 2

1. Screenshot showing the pfSense virtual machine running and displaying the WAN, LAN, OPT1, and OPT2 interface information in the console interface (See Figure 17)

pfSense	192.168.1.100
ESXI	192.168.1.39
Host	192.168.1.54



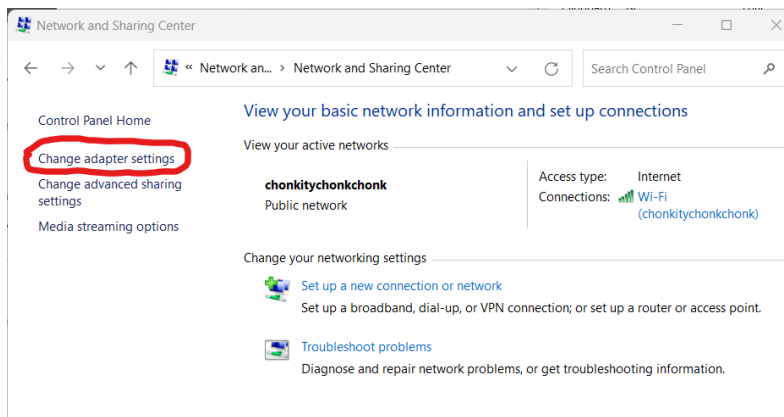


figure 1

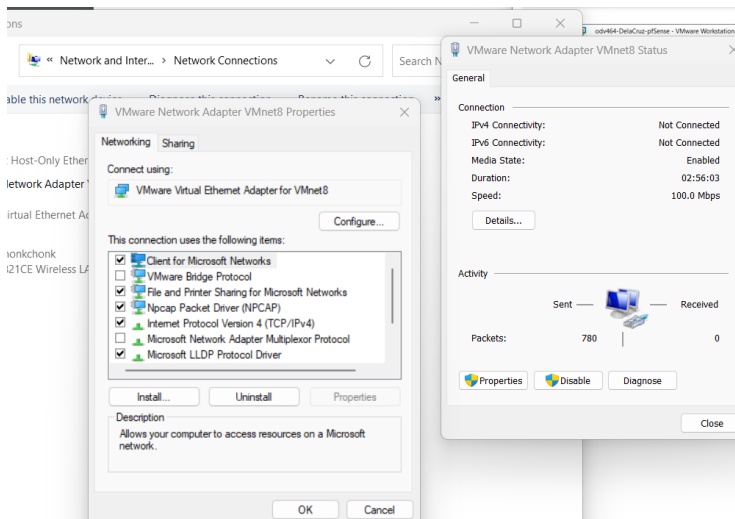


figure 2

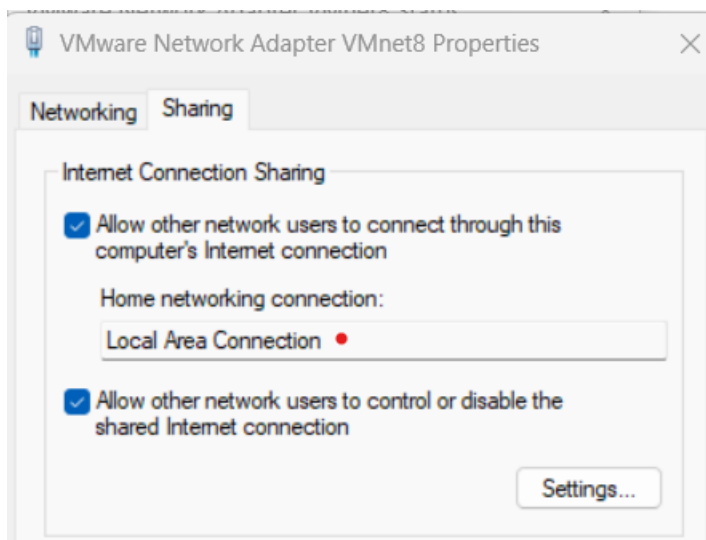


figure 3

Trouble shooting steps if your esxi web interface is unreachable (windows 11)

1. Go to 'control panel' -> 'Network and Internet' -> 'Network and Sharing Center' (figure 1)
2. Next you want to click on "Change adapter settings" on the left panel (figure 2)
3. 'Click on VMare Network Adapter VMnet8' -> 'properties' (figure 3)

4. Finally, you will hit the 'Sharing' tab and make sure to click on the first box and change the 'Home networking connection:' to 'Local Area Connection'

2. Screenshot showing the WAN, LAN, OPT, and OPT2 interface information from the pfSense web interface (See Figure 18)

The screenshot displays the pfSense web interface. At the top, a navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / Dashboard" section is visible. On the left, the "System Information" panel shows details such as Name (pfSense.lab.local), User (admin@192.168.1.54), System (VMware Virtual Machine), BIOS (Vendor: Phoenix Technologies LTD, Version: 6.00), and Version (2.6.0-RELEASE (amd64)). On the right, the "Netgate Services And Support" panel indicates "Retrieving support information". Below this, the "Interfaces" panel lists four interfaces: WAN, LAN, OPT1, and OPT2, each with a status icon (green up arrow), speed/duplex (1000baseT <full-duplex>), and IP address (0.0.0.0, 192.168.1.100, 172.16.100.1, and 172.16.200.1 respectively).

System Information			
Name	pfSense.lab.local		
User	admin@192.168.1.54 (Local Database)		
System	VMware Virtual Machine Netgate Device ID: 13dc2fd741ec058e1e63		
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020		
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE		

Netgate Services And Support			
Retrieving support information			

Interfaces			
WAN	↑	1000baseT <full-duplex>	0.0.0.0
LAN	↑	1000baseT <full-duplex>	192.168.1.100
OPT1	↑	1000baseT <full-duplex>	172.16.100.1
OPT2	↑	1000baseT <full-duplex>	172.16.200.1

3. Screenshots of the DHCP settings for OPT1 and OPT2 (see Figure 19 and Figure 20)

Not secure | https://192.168.1.100/services_dhcp.php

LANOPT1OPT2

General Options

Enable

☒ Enable DHCP server on OPT1 interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

172.16.100.0

Subnet mask

255.255.255.0

Available range

172.16.100.1 - 172.16.100.254

Range

172.16.100.100

172.16.100.150

From

To

Available range	172.16.100.1 - 172.16.100.254	
Range	<input type="text" value="172.16.100.100"/>	<input type="text" value="172.16.100.150"/>
	From	To

Additional Pools

Add

Add pool

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Servers

WINS servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS servers	<input type="text" value="DNS Server 1"/>
	<input type="text" value="DNS Server 2"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

OMAPI

OMAPI Port	<input type="text" value="OMAPI Port"/>	
	Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.	
OMAPI Key	<input type="text" value="OMAPI Key"/>	<input type="checkbox"/> Generate New Key
	Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.	Generate a new key based on the selected algorithm.
Key Algorithm	<input type="text" value="HMAC-SHA256 (current bind9 default)"/>	
	Set the algorithm that OMAPI key will use.	

Other Options

Gateway	<input type="text" value="172.16.100.1"/>
	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.



Services / DHCP Server / OPT2



LAN OPT1 OPT2

General Options

Enable ☒ Enable DHCP server on OPT2 interface

BOOTP ☐ Ignore BOOTP queries

Deny unknown clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients ☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 172.16.200.0

Subnet mask 255.255.255.0

Available range 172.16.200.1 - 172.16.200.254

Range
From To

Available range	172.16.200.1 - 172.16.200.254	
Range	<input type="text" value="172.16.200.100"/>	<input type="text" value="172.16.200.150"/>
	From	To

Additional Pools

Add

+ Add pool

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions
<input type="text"/>			

Servers

WINS servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS servers	<input type="text" value="DNS Server 1"/>
	<input type="text" value="DNS Server 2"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

OMAPI

OMAPI Port	<input type="text" value="OMAPI Port"/>	
	Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable.Only the first OMAPI configuration is used.	
OMAPI Key	<input type="text" value="OMAPI Key"/>	<input type="checkbox"/> Generate New Key
	Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.	Generate a new key based on the selected algorithm.
Key Algorithm	<input type="text" value="HMAC-SHA256 (current bind9 default)"/>	
	Set the algorithm that OMAPI key will use.	

Other Options

Gateway	<input type="text" value="172.16.200.1"/>
	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

4. Screenshots showing the (final) firewall rules that allow the VMs to ping each other from the WAN, LAN, OPT1, and OPT2 interfaces (Sample not given due to troubleshooting task.)

Firewall / Rules / WAN



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	*	*	*	*	none		WAN any-any	

Firewall / Rules / LAN



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	4 / 1.78 MiB	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	13 / 17 KiB	IPv4 *	*	*	*	*	none		LAN any-any	

Firewall / Rules / OPT1



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Floating WAN LAN OPT1 OPT2

Rules (Drag to Change Order)






<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 2 KiB	IPv4 *	*	*	*	*	none		OPT1 any-any	

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

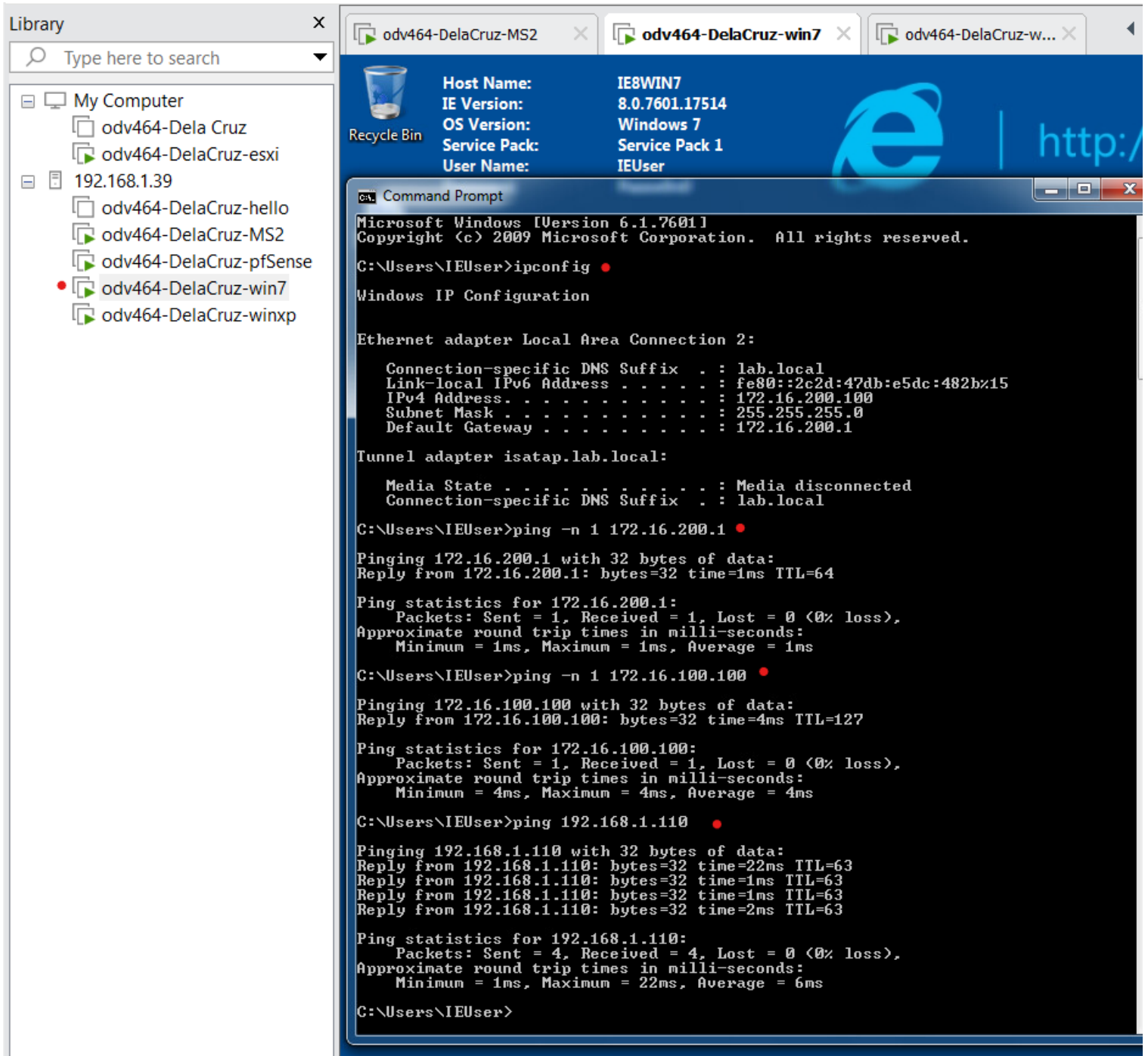
- Floating
- WAN
- LAN
- OPT1
- OPT2**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1 / 40 KiB	IPv4 *	*	*	*	*	none		OPT2 any-any	    

5. Screenshots showing the following:

- The IP address of the Win 7 VM, and it being able to ping the Win XP VM, the MS2 VM, and the pfSense interface on OPT2 (See Figure 21)



- b. The IP address of the Win XP VM, and it being able to ping the Win 7 VM, the MS2 VM, and the pfSense interface on OPT1 (See Figure 22)

The screenshot shows a virtual machine environment with a Windows XP desktop. On the left, a 'Library' pane lists several virtual machines: 'odv464-DelaCruz', 'odv464-DelaCruz-esxi', '192.168.1.39', 'odv464-DelaCruz-hello', 'odv464-DelaCruz-MS2', 'odv464-DelaCruz-pfSense', 'odv464-DelaCruz-win7', and 'odv464-DelaCruz-winxp'. The main window displays the desktop of the 'odv464-DelaCruz-winxp' VM. A 'Command Prompt' window is open, showing the following output:

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 4:

    Connection-specific DNS Suffix  . : lab.local
    IP Address. . . . . : 172.16.100.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.100.1

Ethernet adapter Local Area Connection 3:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\Administrator>ping -n 1 172.16.100.1

Pinging 172.16.100.1 with 32 bytes of data:
Reply from 172.16.100.1: bytes=32 time=44ms TTL=64

Ping statistics for 172.16.100.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 44ms, Maximum = 44ms, Average = 44ms

C:\Documents and Settings\Administrator>ping -n 1 172.16.200.100

Pinging 172.16.200.100 with 32 bytes of data:
Reply from 172.16.200.100: bytes=32 time=2ms TTL=127

Ping statistics for 172.16.200.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Documents and Settings\Administrator>ping -n 1 192.168.1.110

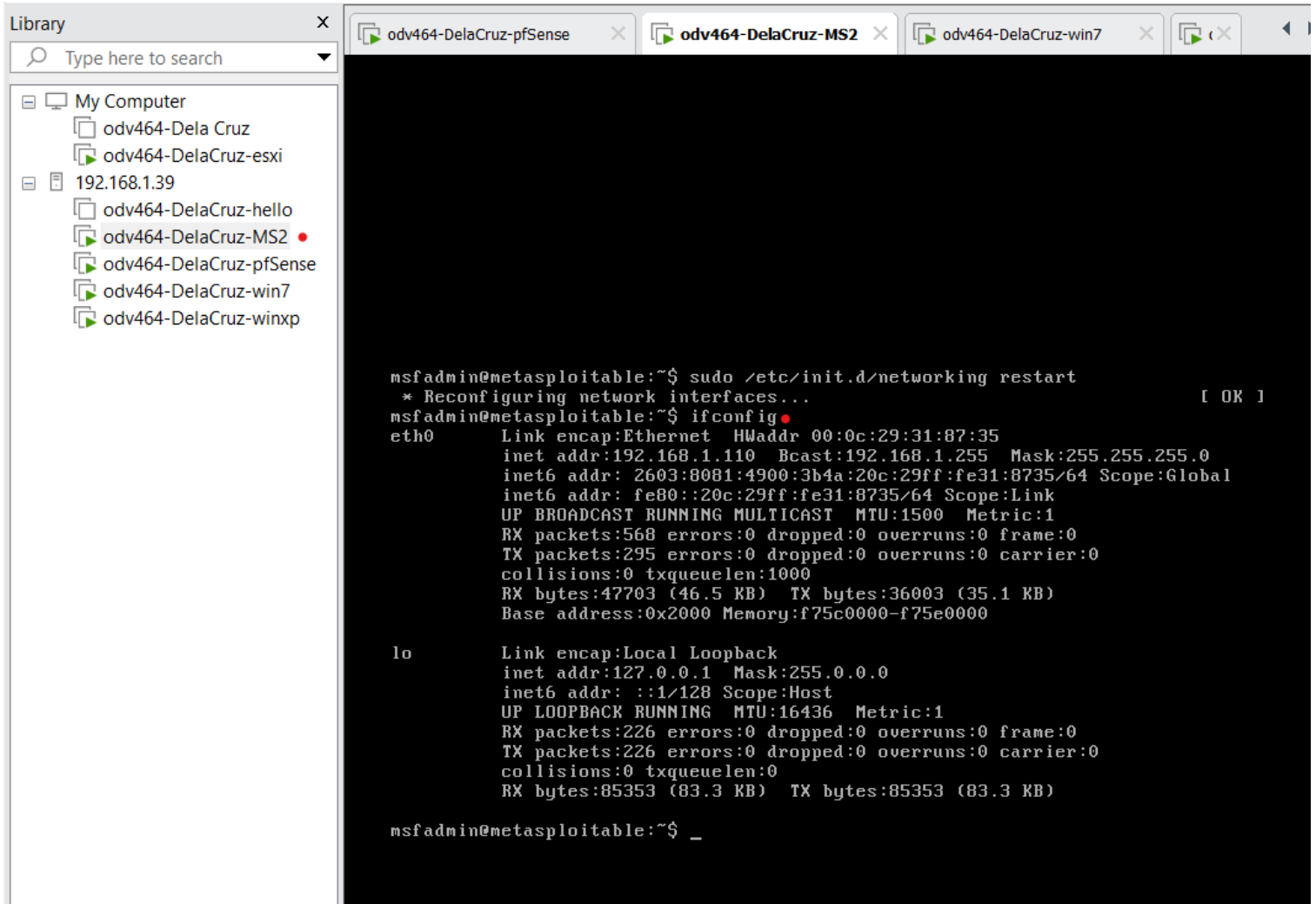
Pinging 192.168.1.110 with 32 bytes of data:
Reply from 192.168.1.110: bytes=32 time=17ms TTL=63

Ping statistics for 192.168.1.110:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 17ms, Average = 17ms

C:\Documents and Settings\Administrator>
```

The taskbar at the bottom shows the 'start' button, a 'Command Prompt' taskbar icon, and system tray icons including a clock showing 6:04 PM. Below the screenshot, a note reads: 'To direct input to this VM, click inside or press Ctrl+G.'

- c. The IP address of the MS2 VM, and it being able to ping the Win 7 VM, the Win XP VM, and the pfSense interface on LAN. This may require 2 screenshots. (See Figure 23 and Figure 24)



The screenshot shows a virtual machine interface with a 'Library' pane on the left and a terminal window on the right. The Library pane lists several VMs under 'My Computer', including 'odv464-DelaCruz-pfSense', 'odv464-DelaCruz-MS2', 'odv464-DelaCruz-win7', and others. The terminal window is titled 'odv464-DelaCruz-MS2' and shows a user 'msfadmin' at a prompt 'msfadmin@metasploitable:~\$'. The user enters the command 'sudo /etc/init.d/networking restart', which outputs '* Reconfiguring network interfaces... [OK]'. Then, the user enters 'ifconfig', which displays the configuration for the 'eth0' interface (192.168.1.110) and the 'lo' interface (127.0.0.1). The terminal output is as follows:

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:87:35
          inet addr:192.168.1.110  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2603:8081:4900:3b4a:20c:29ff:fe31:8735/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe31:8735/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:295 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:47703 (46.5 KB)  TX bytes:36003 (35.1 KB)
          Base address:0x2000 Memory:f75c0000-f75e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85353 (83.3 KB)  TX bytes:85353 (83.3 KB)

msfadmin@metasploitable:~$ _
```

Library X

Type here to search

- My Computer
 - odv464-Dela Cruz
 - odv464-DelaCruz-esxi
- 192.168.1.39
 - odv464-DelaCruz-hello
 - odv464-DelaCruz-MS2
 - odv464-DelaCruz-pfSense
 - odv464-DelaCruz-win7
 - odv464-DelaCruz-winxp

```
odv464-DelaCruz-pfSense X odv464-DelaCruz-MS2 X odv464-DelaCruz-win7 X
```

```
collisions:0 txqueuelen:0
RX bytes:85353 (83.3 KB) TX bytes:85353 (83.3 KB)

msfadmin@metasploitable:~$ ping -c 1 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=3.82 ms

--- 192.168.1.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.825/3.825/3.825/0.000 ms
msfadmin@metasploitable:~$ ping -c 1 172.16.100.100
PING 172.16.100.100 (172.16.100.100) 56(84) bytes of data.
64 bytes from 172.16.100.100: icmp_seq=1 ttl=127 time=6.97 ms

--- 172.16.100.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.974/6.974/6.974/0.000 ms
msfadmin@metasploitable:~$ ping -c 1 172.16.200.100
PING 172.16.200.100 (172.16.200.100) 56(84) bytes of data.
64 bytes from 172.16.200.100: icmp_seq=1 ttl=127 time=1.35 ms

--- 172.16.200.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.358/1.358/1.358/0.000 ms
msfadmin@metasploitable:~$
```