

CS 5700 -- Computer Security and Information Assurance
Fall 2018

Prof. Leszek Lilien / TA: Abduljaleel Al-Hasnawi
Department of Computer Science
Western Michigan University

LAB ASSIGNMENT - 2

NAME: SAMPATH TALLURI

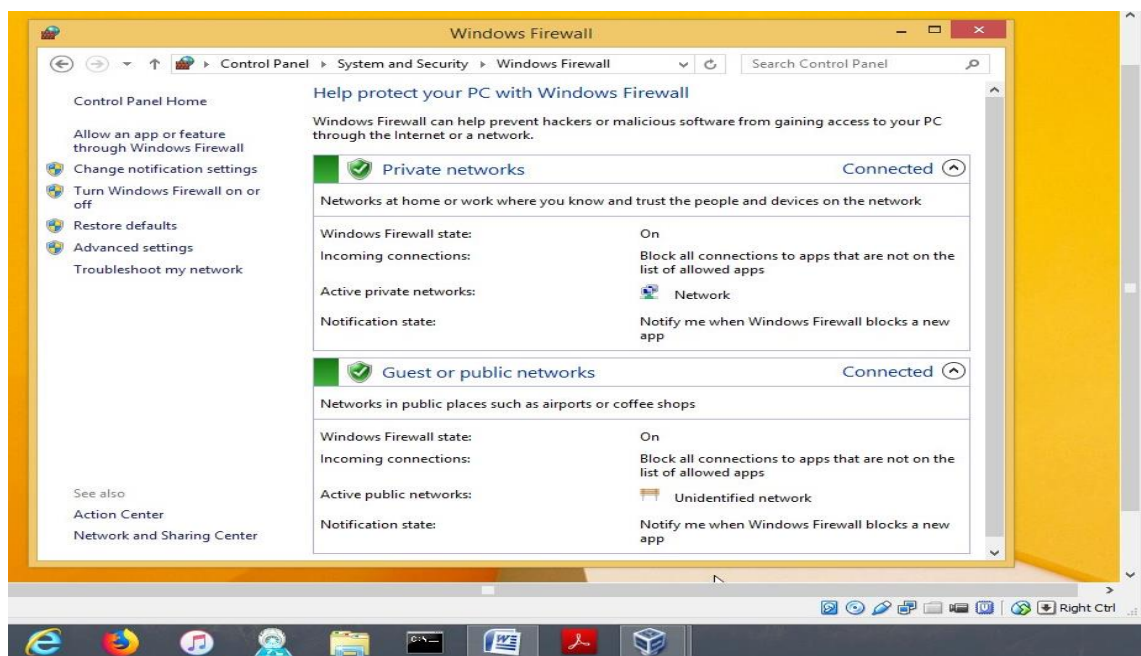
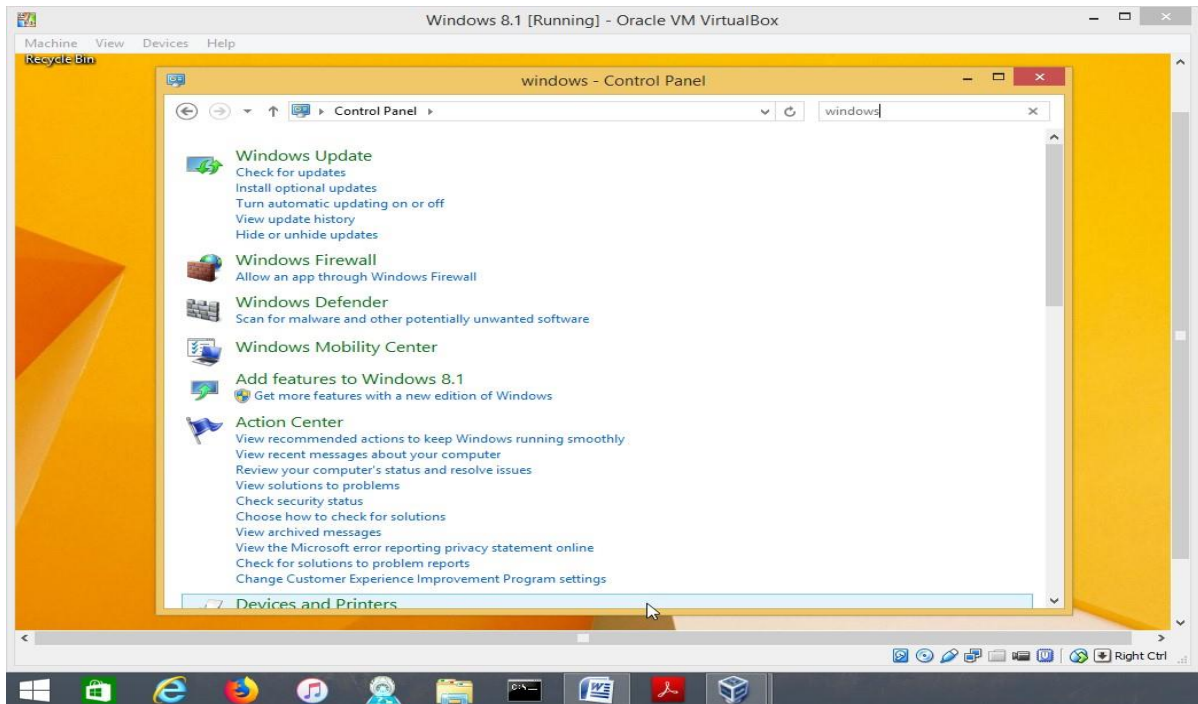
TABLE OF CONTENTS

1. Introductory Part: Enable Inbound Rules for IPv4 and IPv6	3
1.1. Step 1: Enable Inbound Rules for IPv4 and IPv6 on Win8.1.	3
1.2. Step 2: Enable Inbound Rules for IPv4 and IPv6 on W2K12.	4
2. Lab 1.1w: Windows Client Configuration	5
2.1. Step 1: Start Win8.1	5
2.2. Step 2: View and Record the Network Configuration	6
2.3. Step 3: Change the IP Address of Win8.1	8
2.4. Step 4: Change the IP Address of W2K12 Server.	10
2.5. Step 5: From Win8.1 Ping the W2K12 Server	12
2.6. Step 6: View and Modify the ARP Table	13
3. Lab 1.2w: Name Resolution in Windows	14
3.1. Step 1: Login to Win8.1 as administrator	14
3.2. Step 2: Ping Win8.1	15
3.3. Step 3: View and Modify the Host File.....	15
4. Lab 1.3w: Windows IPv6 Basics	18
4.1. Step1: Verify IPv6 Setting for Win8.1 and W2K12	18
4.2. Step2: Install Wireshark on Win8.1	19
5.Issues.....	21
6.Recorded Time.....	22

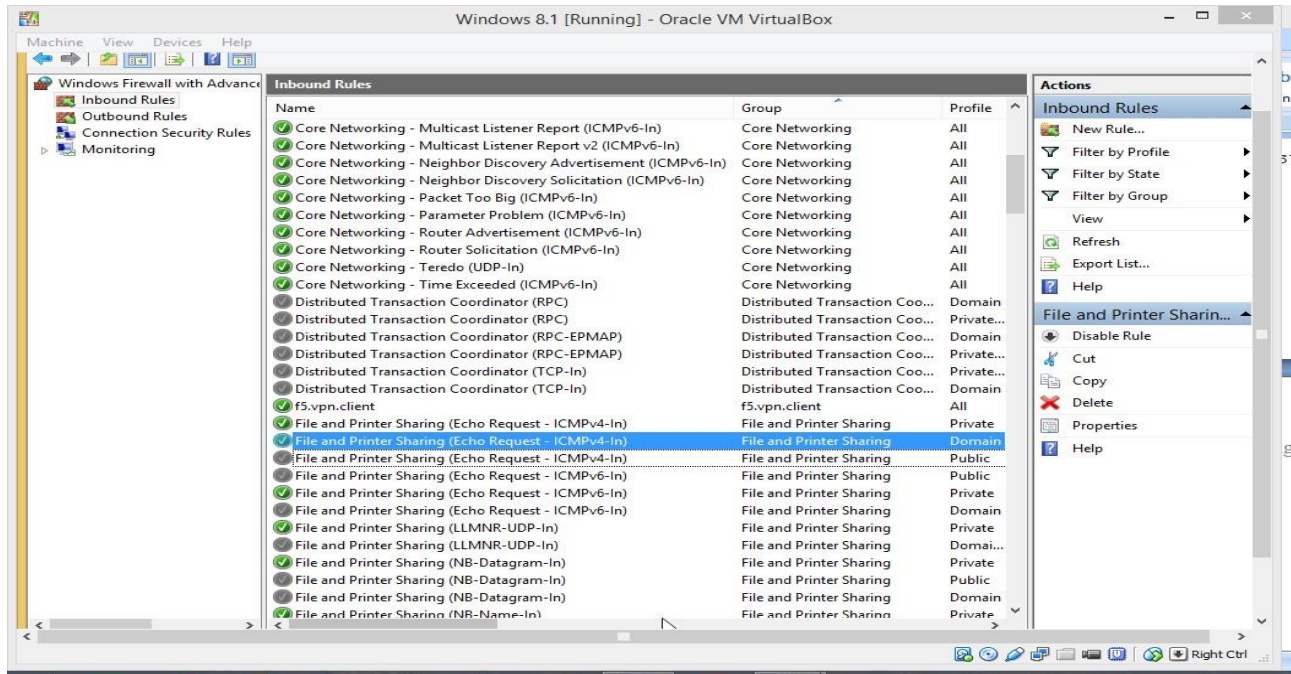
1. Introductory Part: Enable Inbound Rules for IPv4 and IPv6

->Step1: Enable Inbound Rules for IPv4 and IPv6 on Win8.1.

-Run Windows 8.1 on VM ware, and go to Control Panel ->Windows Firewall to make changes in the advanced setting on the system.

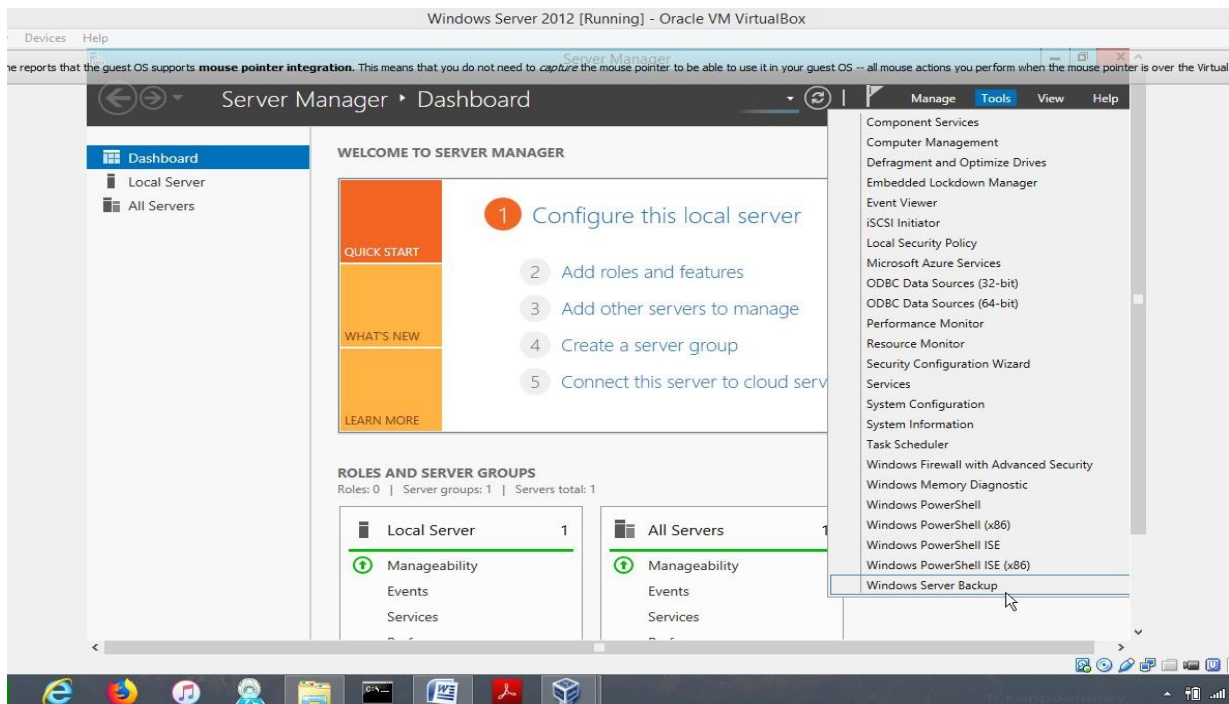


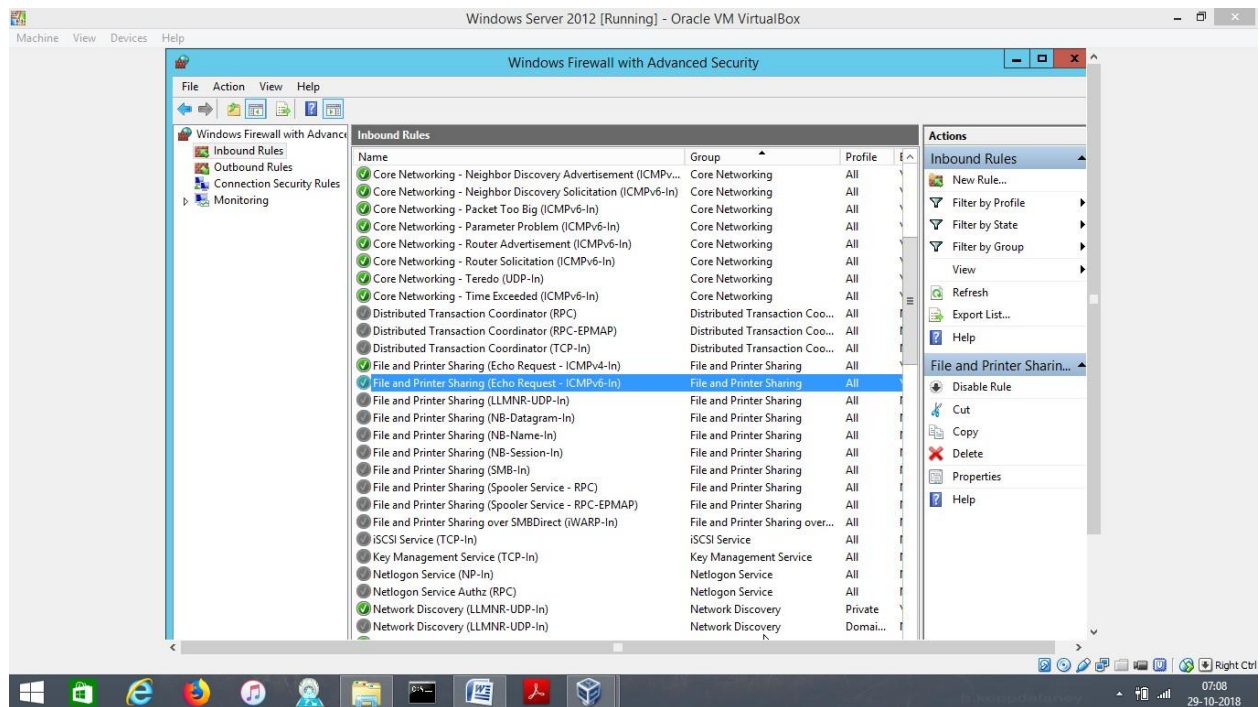
-Go to Advanced setting and select inboundRules, which will display set of settings in which we need to enable the rules for both IPv4 and IPV6 (File and sharing) as shown below



Step2: Enable Inbound Rules for IPv4 and IPv6 on W2K12.

Follow the same steps on Windows Server 2012 to enable the rules.

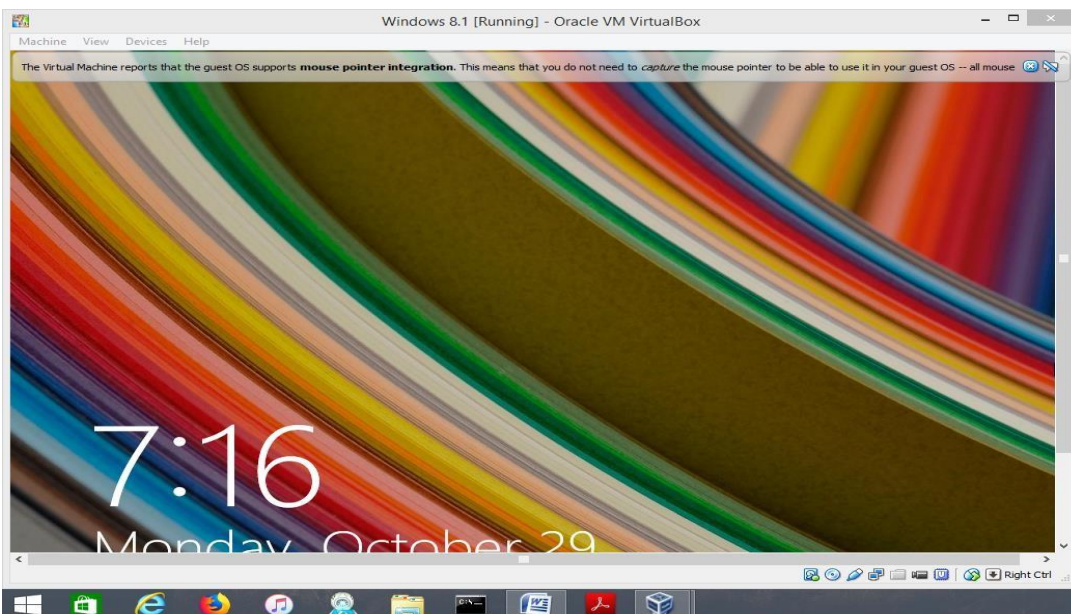




2 .Lab 1.1w: Windows Client Configuration

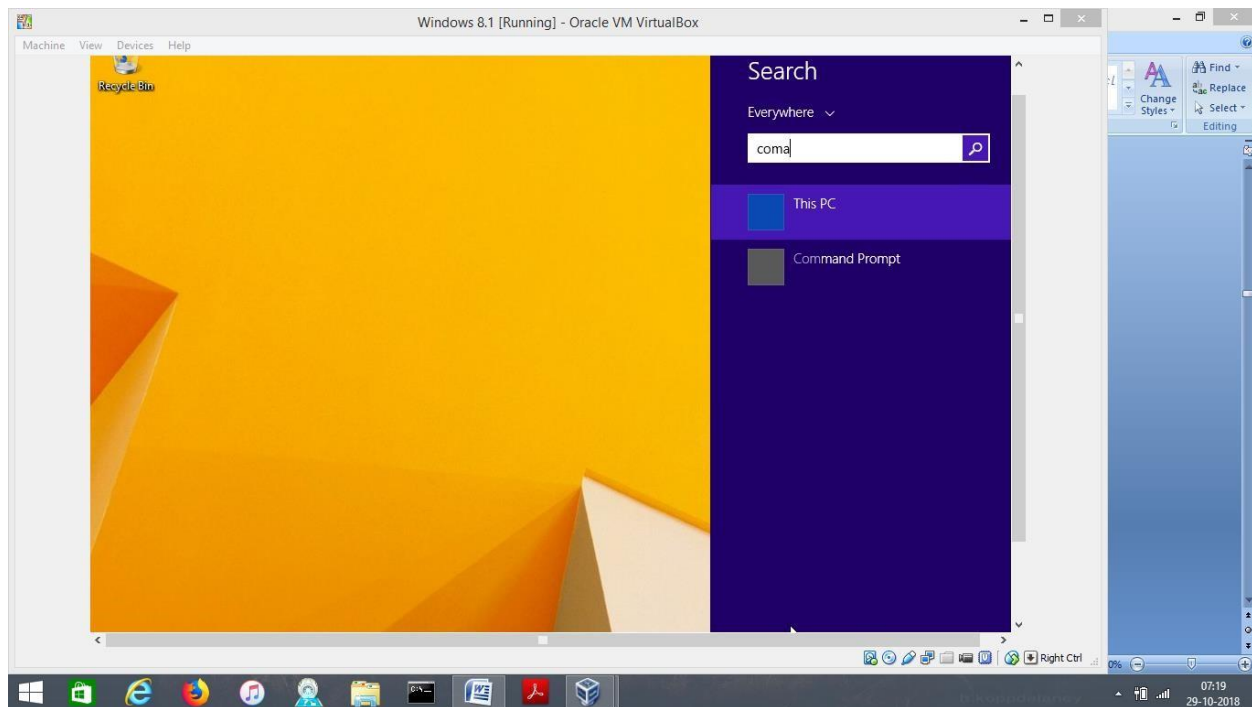
2.1. Step 1: Start Win8.1.

Start Windows 8.1.

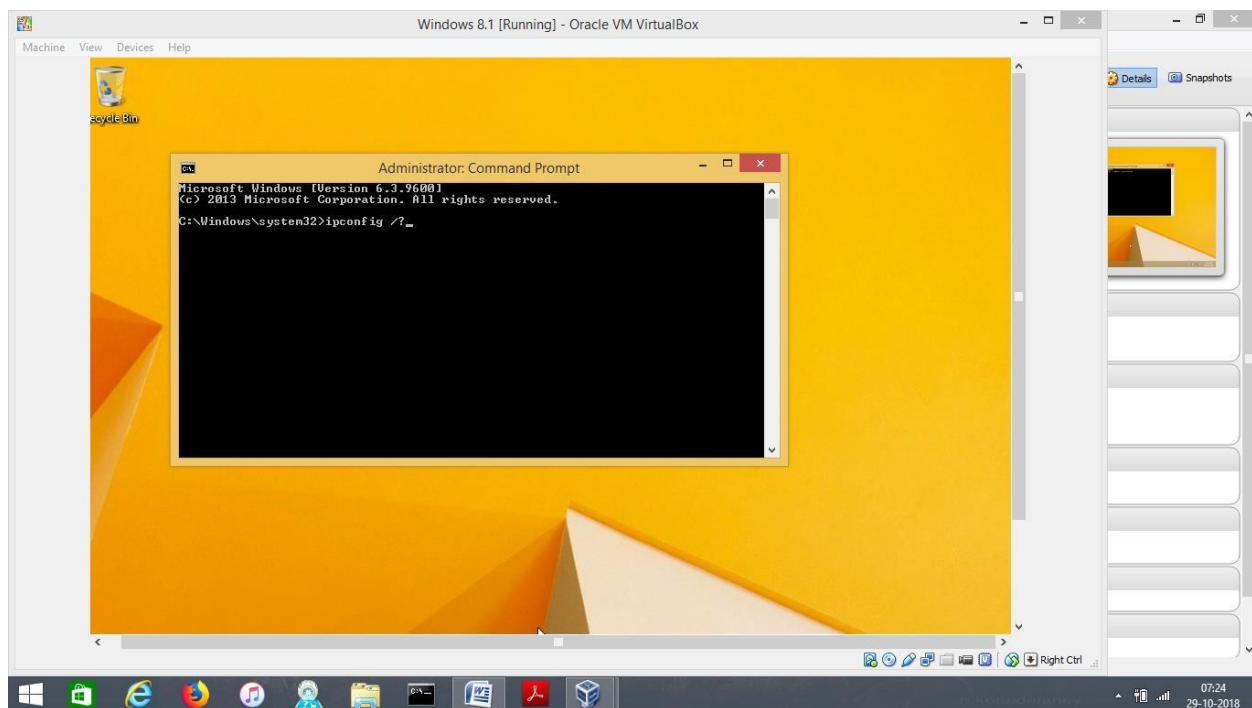


Step 2: View and Record the Network Configuration.

On Windows 8.1, open command Prompt and run as administrator as shown below.



-Type `ipconfig /?`, which will display you the ip configuration of the guest system.

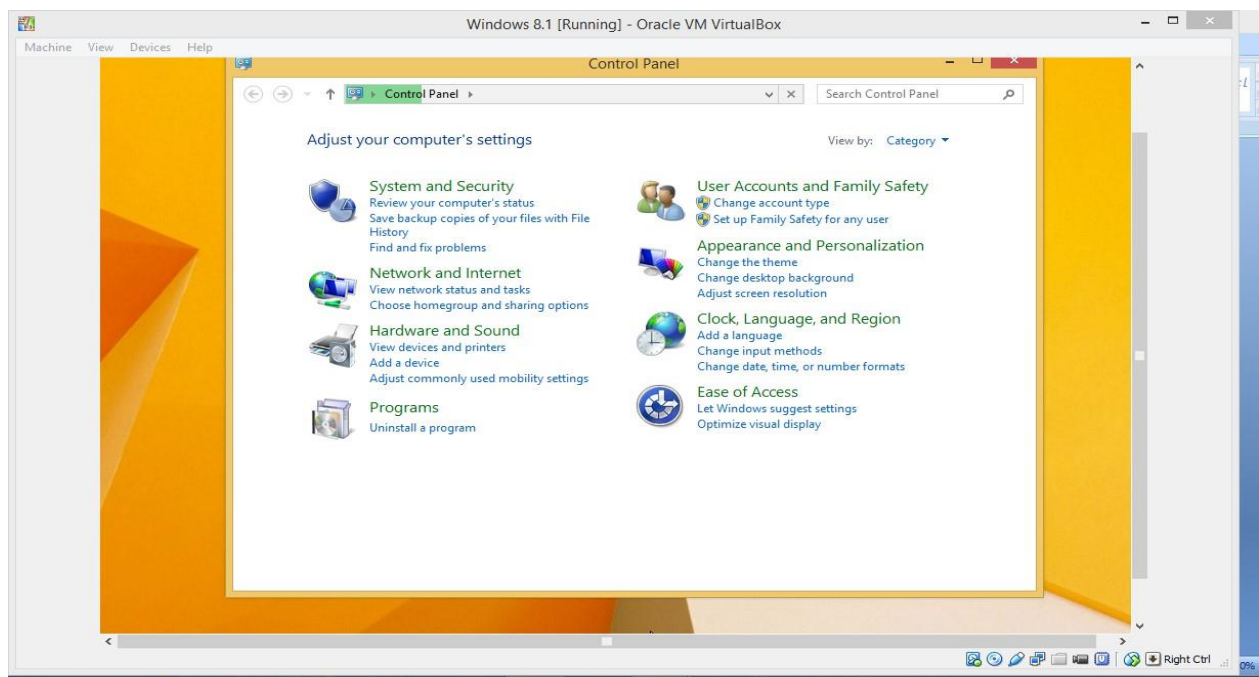


-Type `ipconfig /all`, which will then show you the overall system configurations, connections (Ethernet Adaptor configurations)

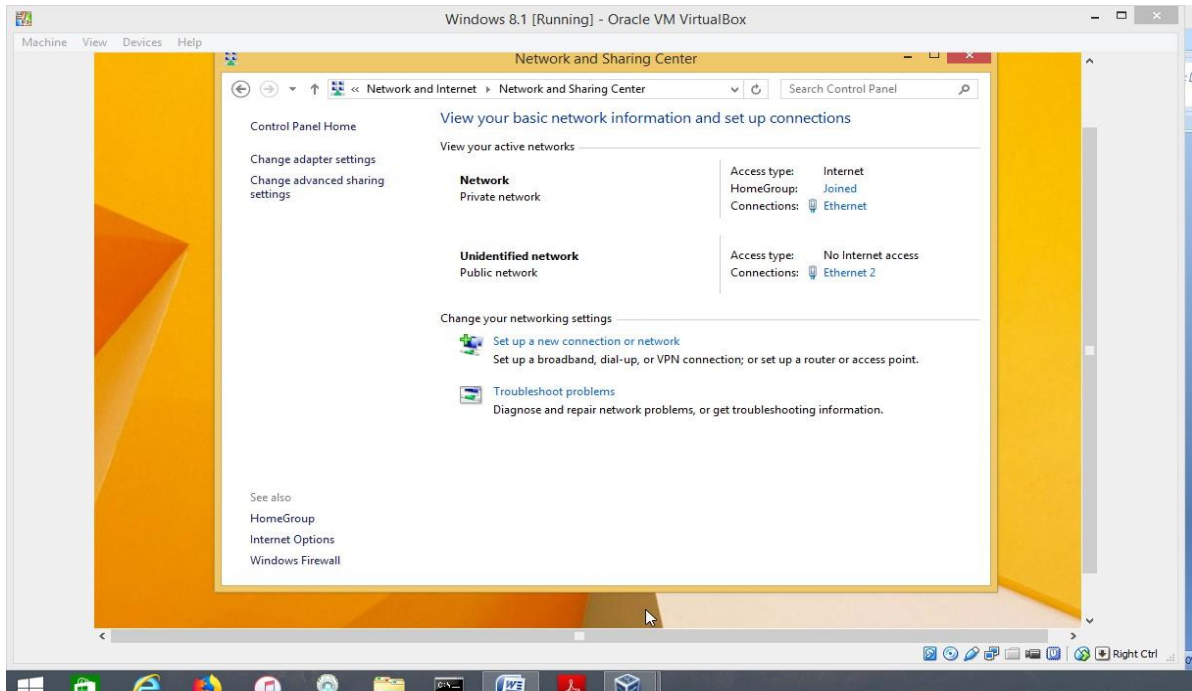
```
Command Prompt
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
IPv6 Address. . . . . : 2600:6c4a:7c7f:d1cb:0:ad3b:574a:62d1
IPv6 Address. . . . . : 2600:6c4a:7c7f:d1cb:bde1:468d:c263:5bd
Temporary IPv6 Address. . . . : 2600:6c4a:7c7f:d1cb:5041:3929:b593:adb7
Link-local IPv6 Address . . . . : fe80::bde1:468d:c263:5bd%18
IPv4 Address. . . . . : 192.168.1.219
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::5a90:43ff:fe16:bb82%18
192.168.1.1
Ethernet adapter Bluetooth Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\sampa>
```

Step 3: Change the IP Address of Win8.1.

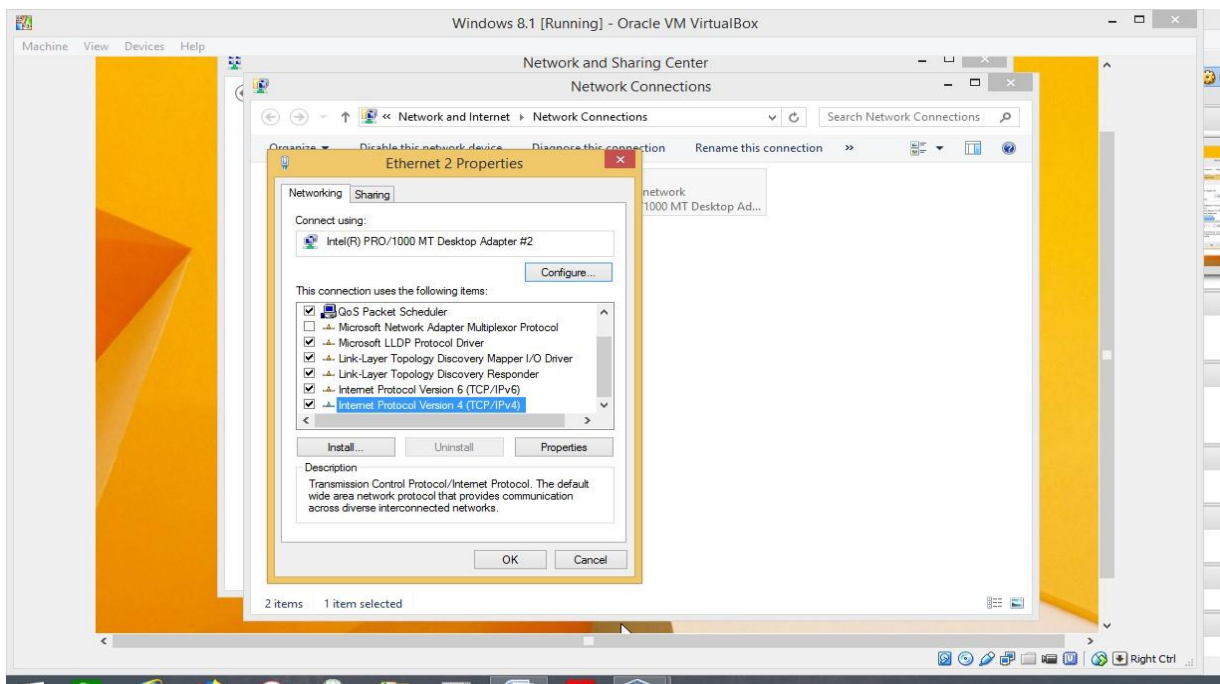
-On Windows 8.1, Go to Control Panel and then go to Network And Internet.



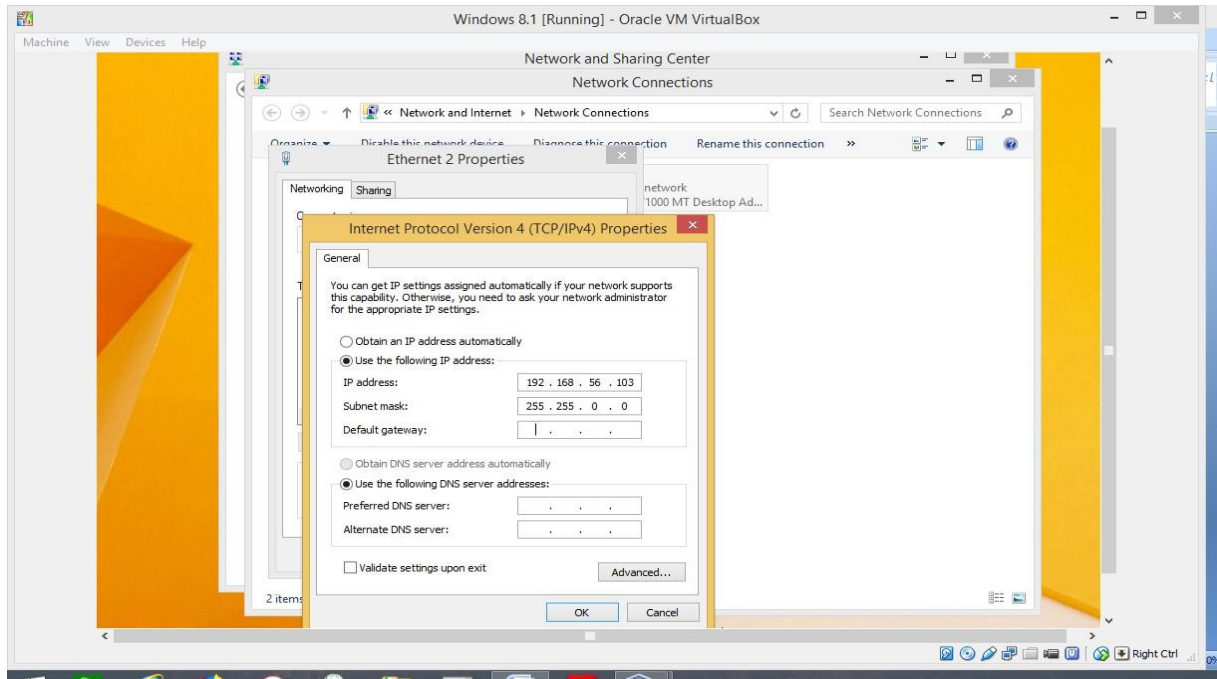
-SELECT NETWORK AND SHARING CENTER.



-HERE WE NEED TO GO TO CHANGE ADAPTER SETTINGS. AND GO TO ETHERNET PROPERTIES TO SELECT (INTERNET PROTOCOL VERSION 4)



GO TO THE PROPERTY SETTINGS AND CHANGE THE IP ADDRESS AS SHOWN IN THE FIGURE.



-AGAIN GO TO COMMAND PROMPT AND CHECK THE IP CONFIGURATION CHANGE BY TYPING (IPCONFIG)

```

Command Prompt
Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : home
IPv6 Address. . . . . : 2600:6c4a:7c7f:d1cb:0:ad3b:574a:62d1
IPv6 Address. . . . . : 2600:6c4a:7c7f:d1cb:bde1:468d:c263:50d
Temporary IPv6 Address. . . . . : 2600:6c4a:7c7f:d1cb:3829:b593:a6b7
Link-local IPv6 Address . . . . . : fe80::bde1:468d:c263:50d%18
IPv4 Address. . . . . : 192.168.1.219
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::5a90:43ff:fe16:bb82%18
192.168.1.1

Ethernet adapter Bluetooth Network Connection 2:

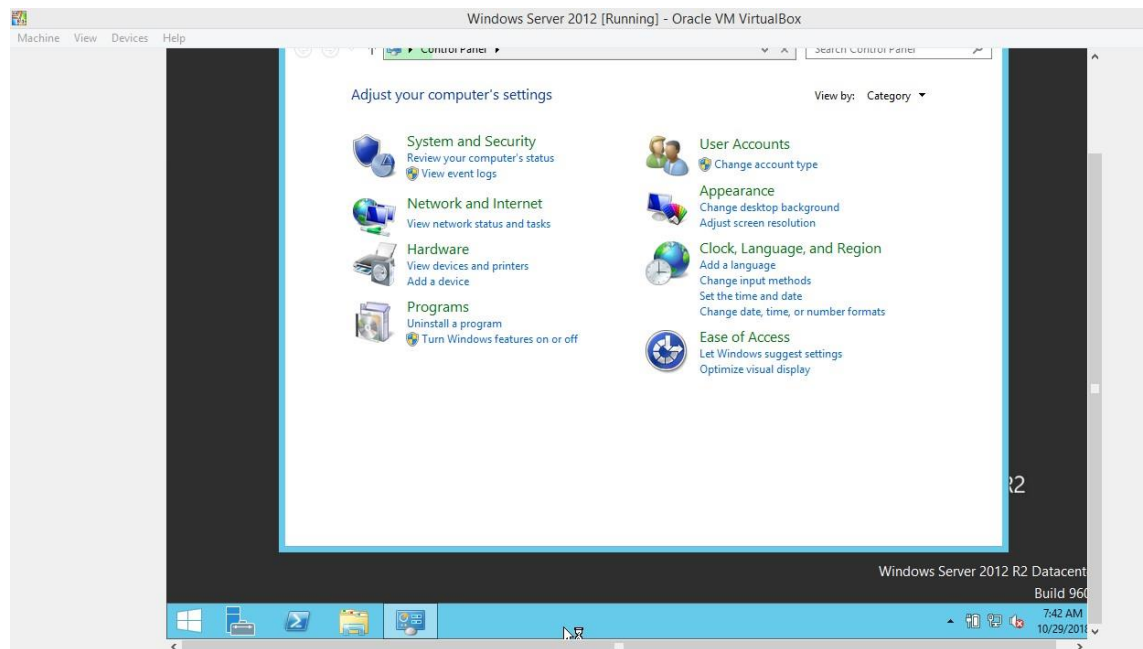
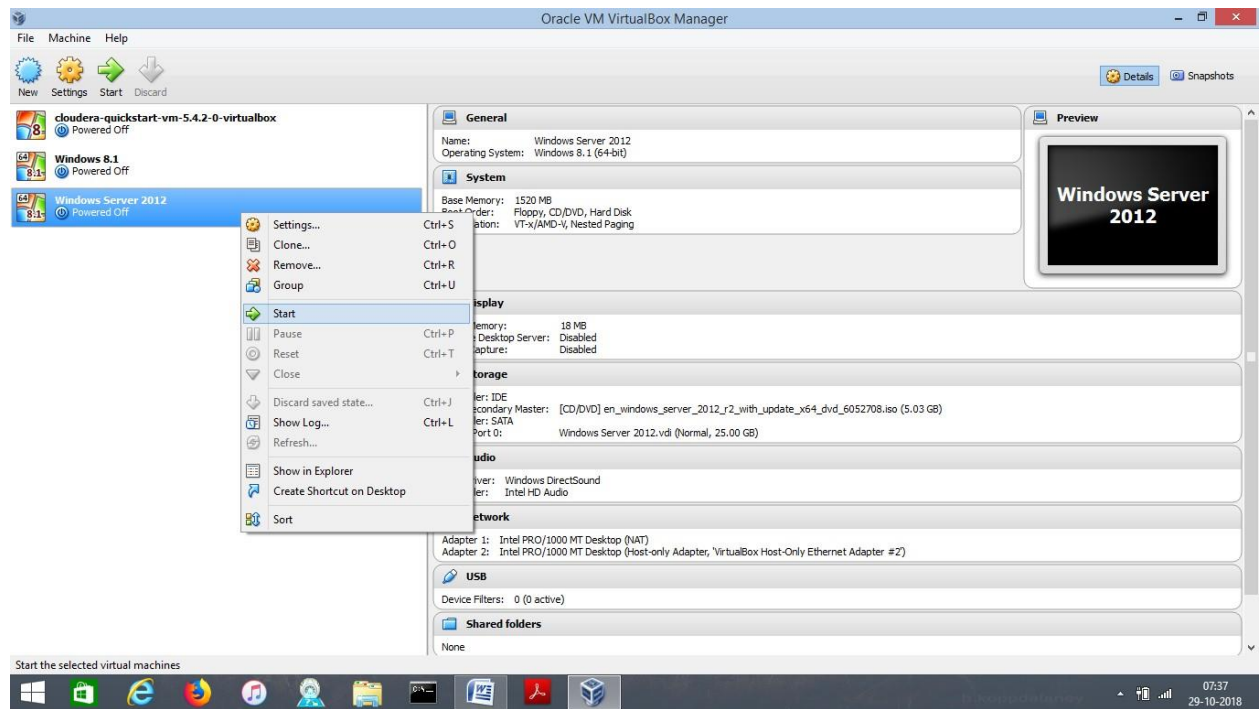
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

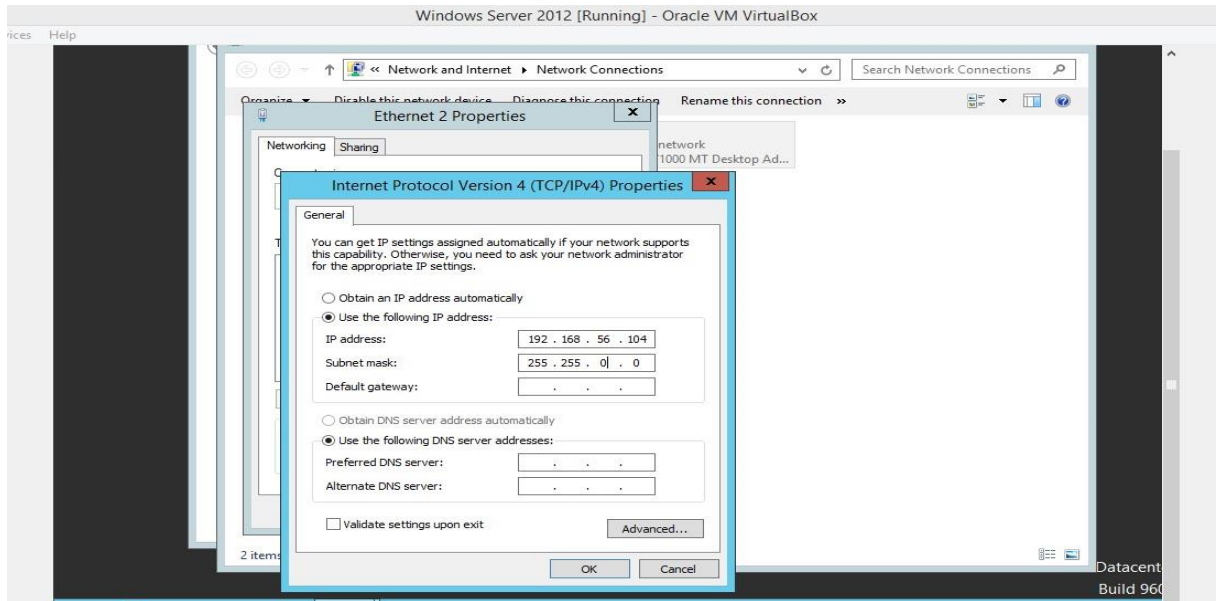
C:\Users\sampa>

```

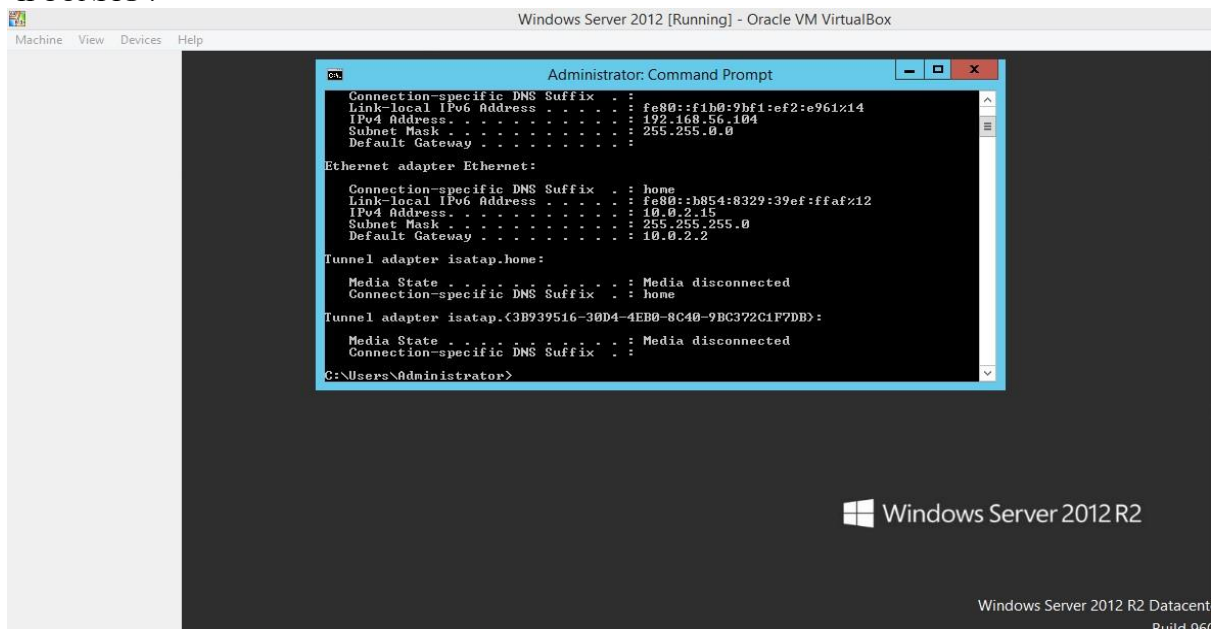
Step 4: Change the IP Address of W2K12.

-Follow the same steps and change ip address of W2k12 as shown below.



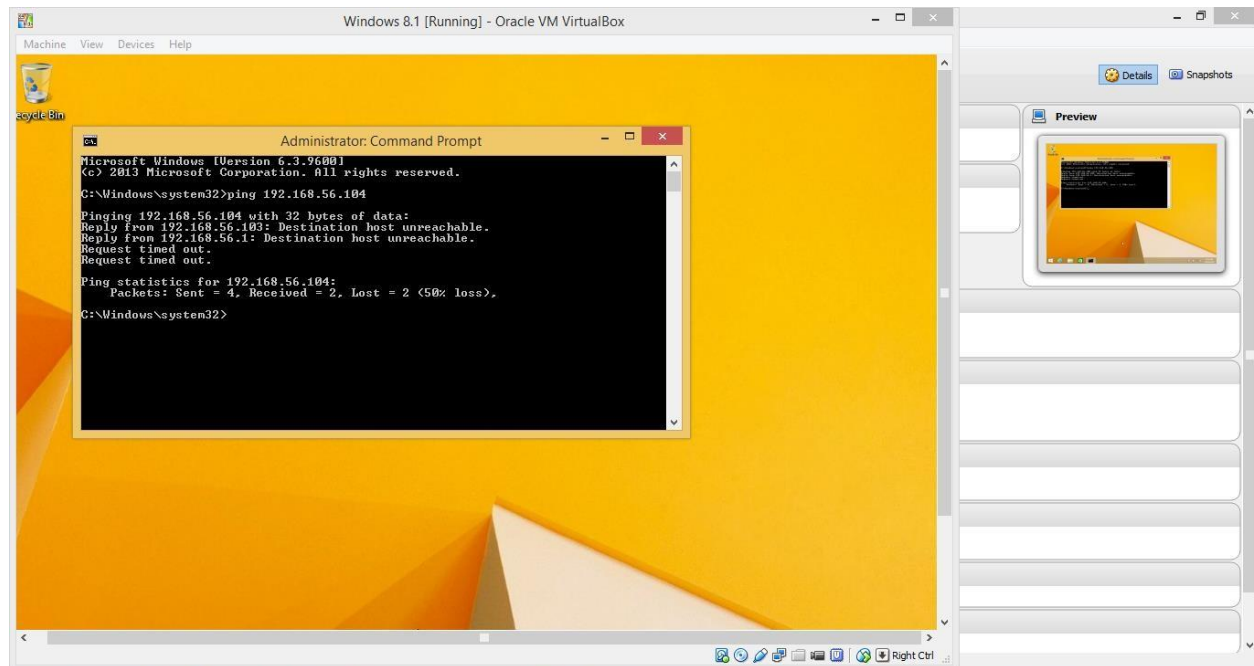


-GO TO COMMAND PROMPT TO OBSERVE THE CHANGES MADE IN THE IP ADDRESS BY TYPING 'IPCONFIG'.



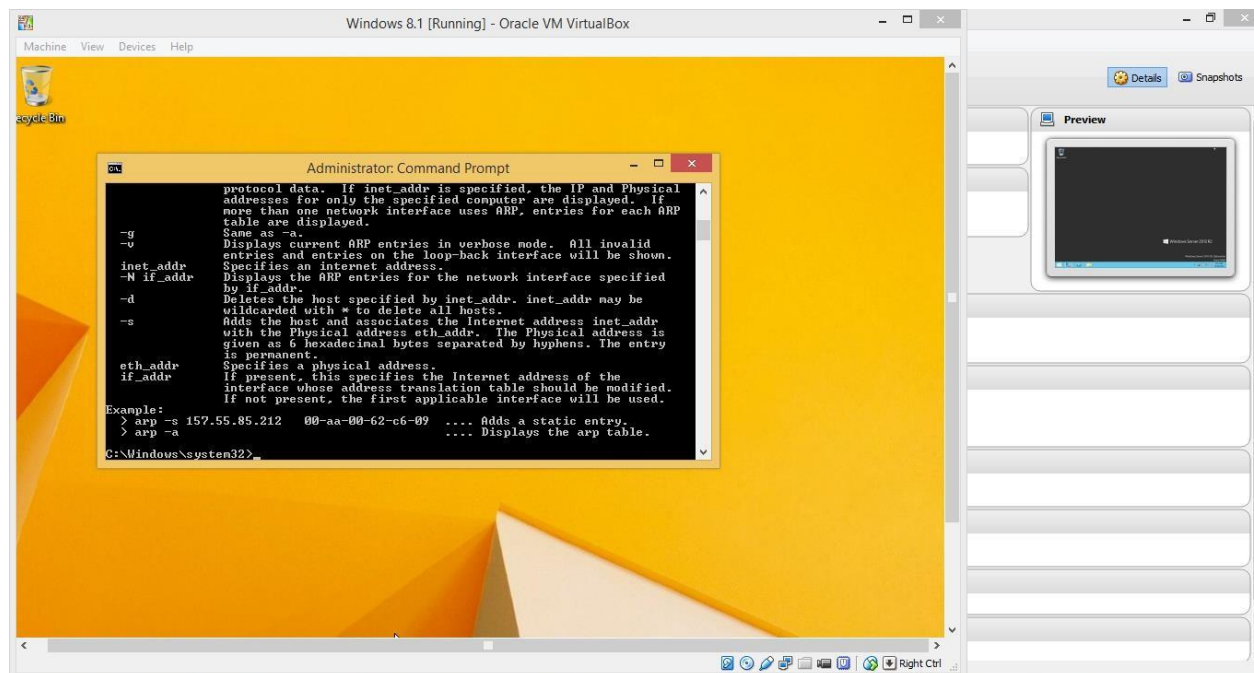
Step 5: From Win8.1, Ping the W2K12 Server

In this step we need to ping server w2k12 from 8.1, on windows 8.1 , command prompt type ping 192.168.56.104

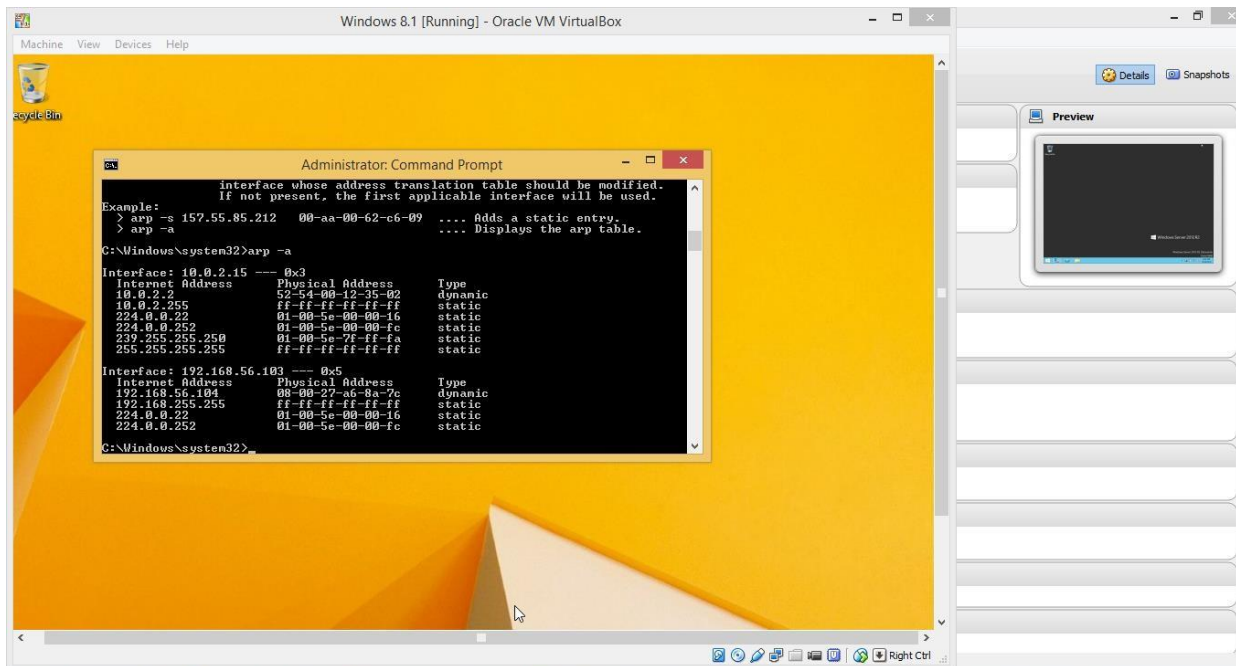


Step 6: View and Modify the ARP Table.

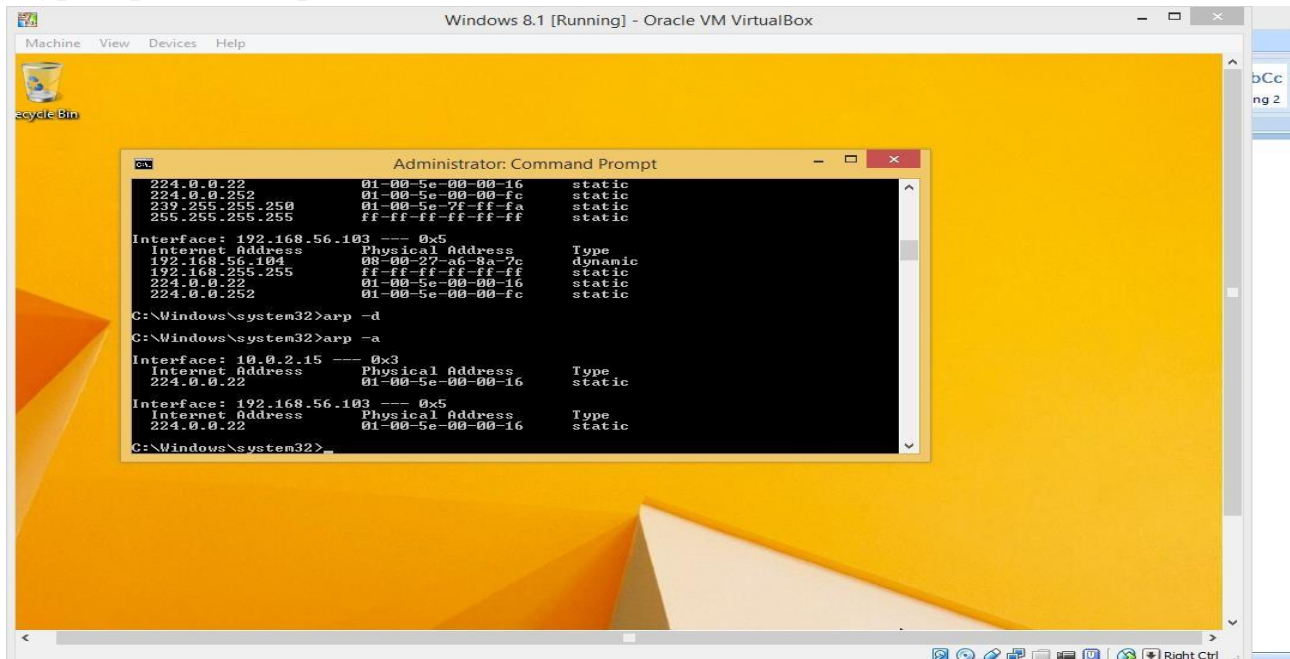
-Type arp /?



-Type arp -a



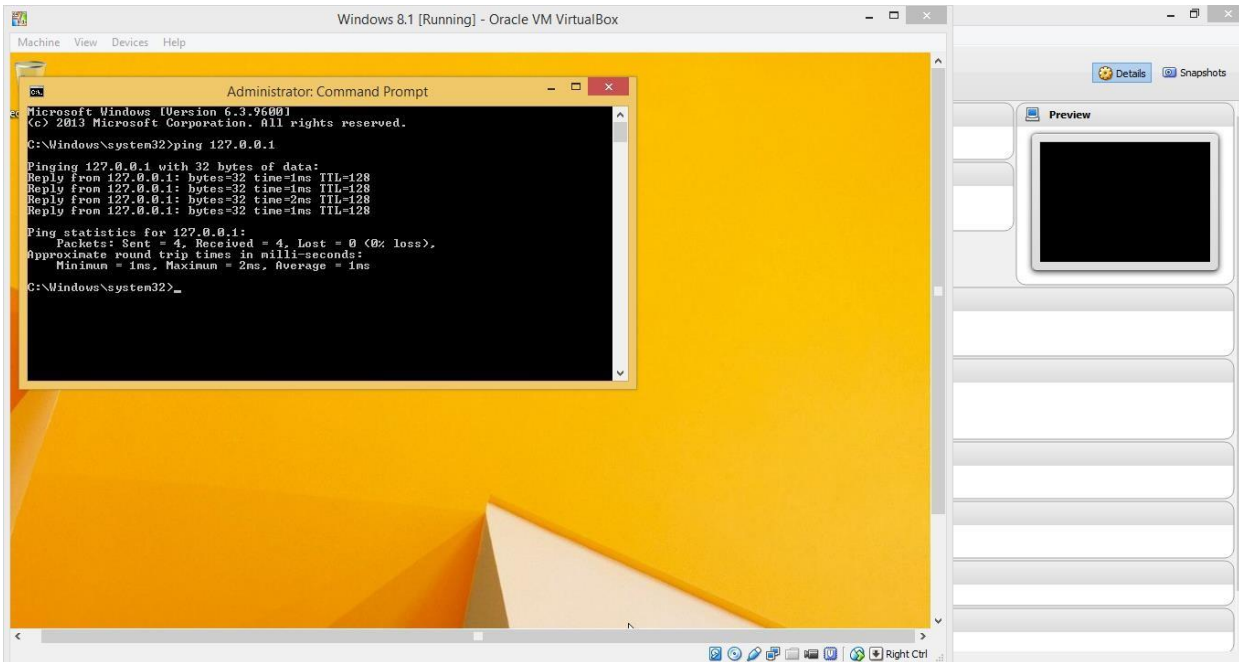
-Type arp -d and arp -a, and observe.



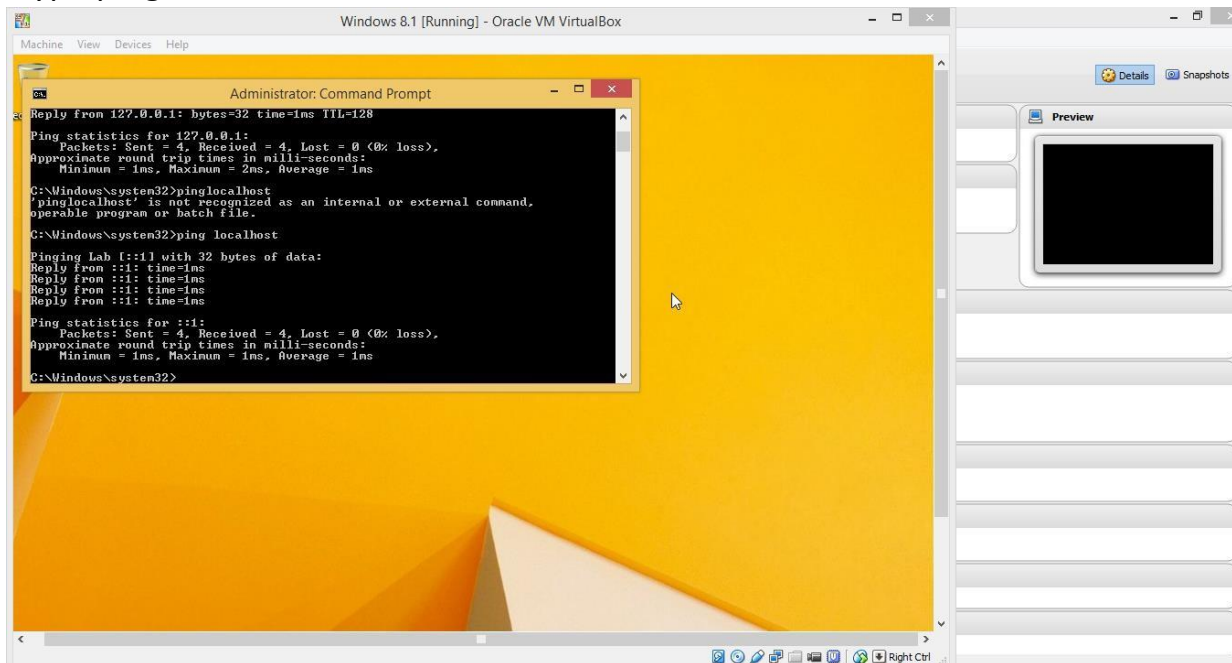
3 Lab 1.2w: Name Resolution in Windows

Step 1: Login to Win8.1 as administrator and ping local host -ping

127.0.0.1, and you can see the transactions.

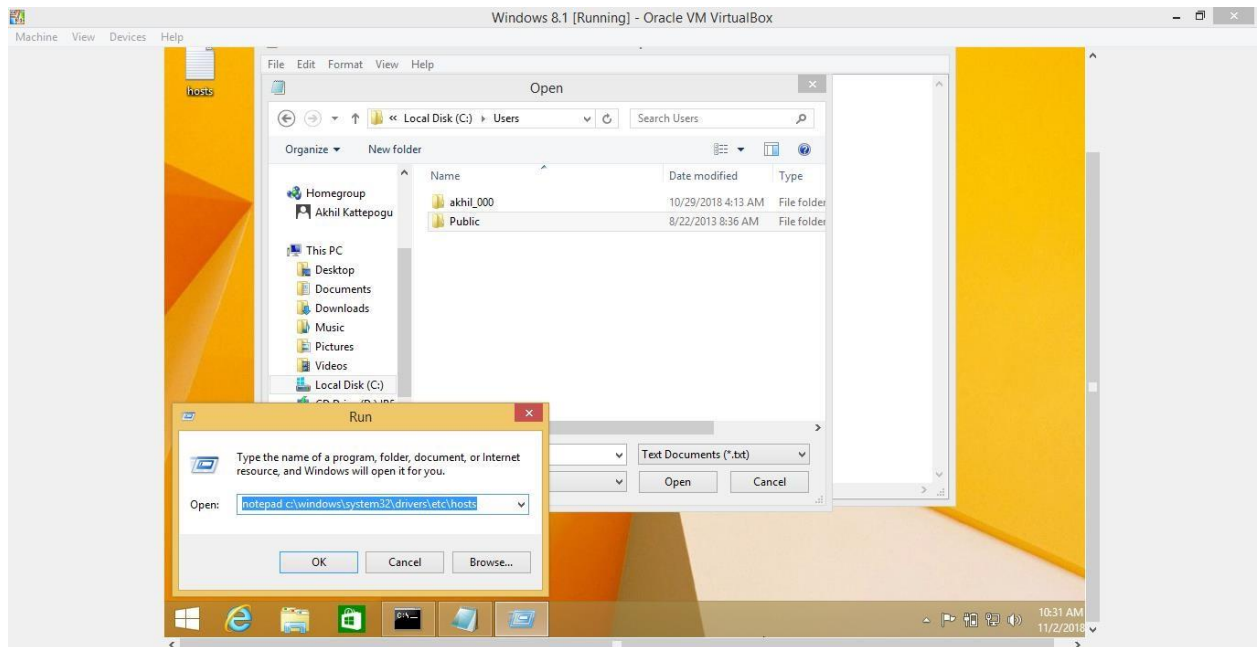


-Type ping localhost.

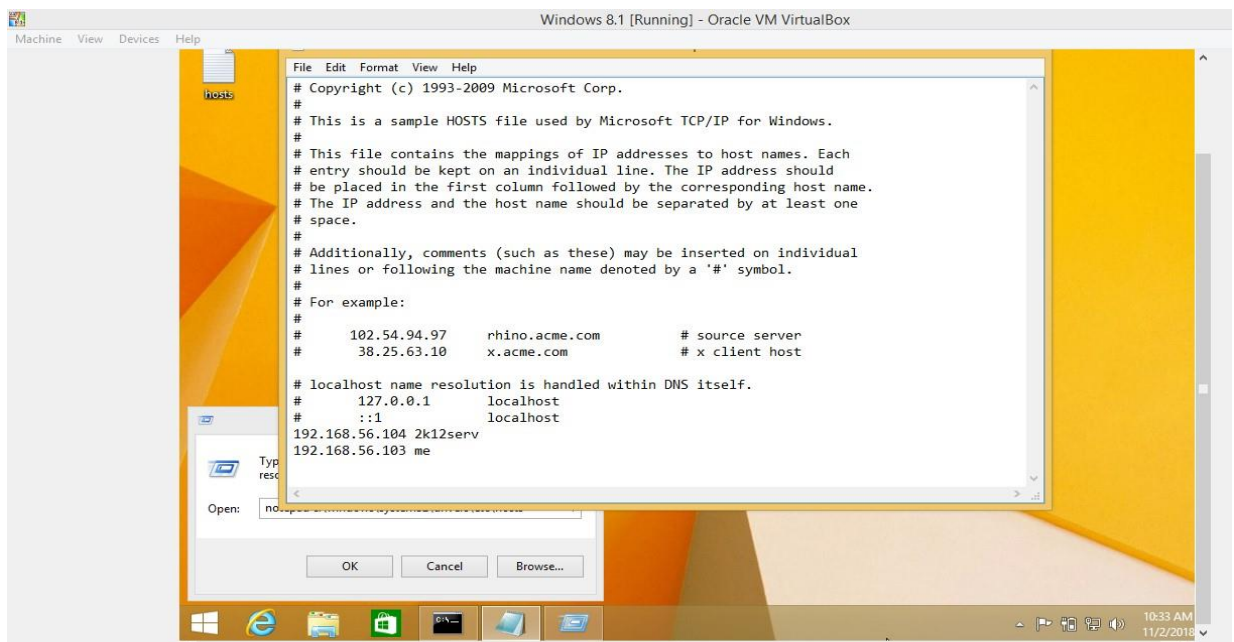


Step 3: View and Modify the Host File.

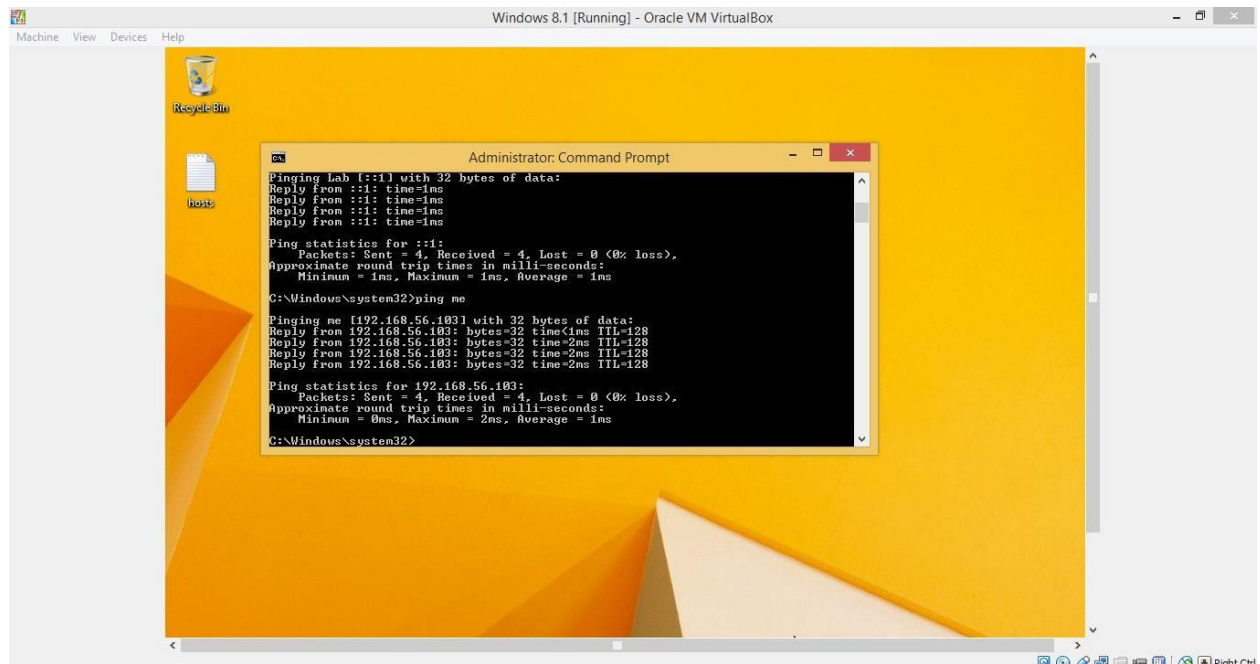
-On Windows 8.1, go to run and type notepad
c:\windows\system32\drivers\etc\hosts and a hosts file opens



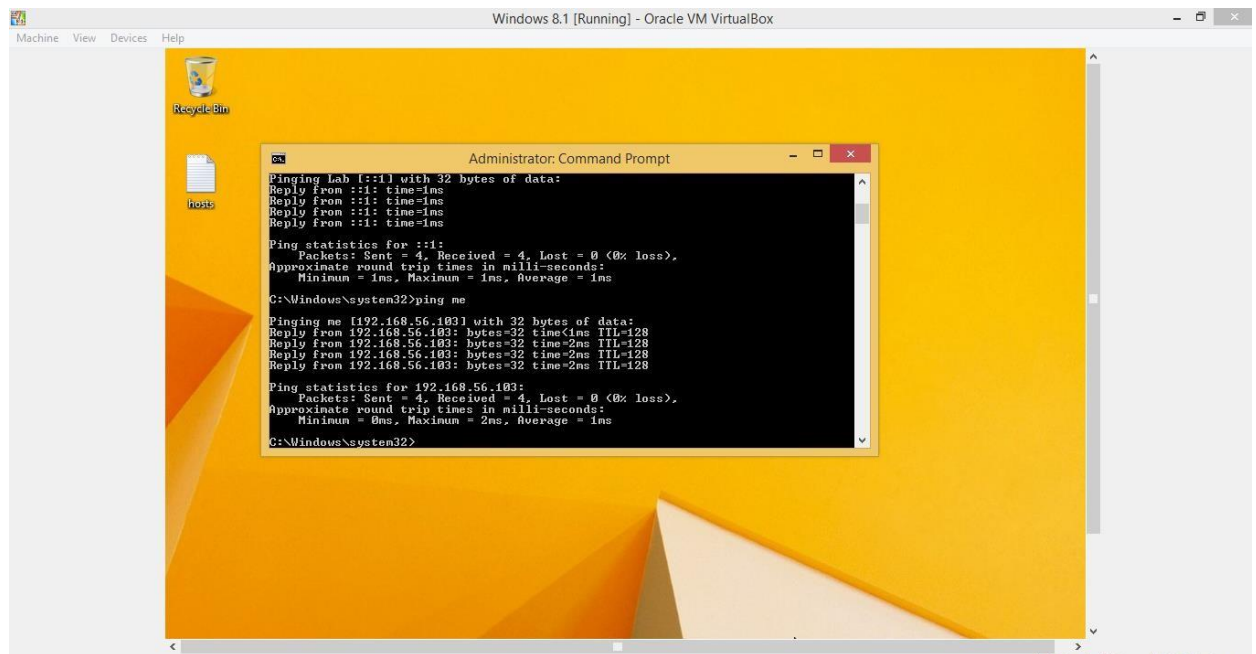
-Add ip address as shown below to the hosts file and save the changes.



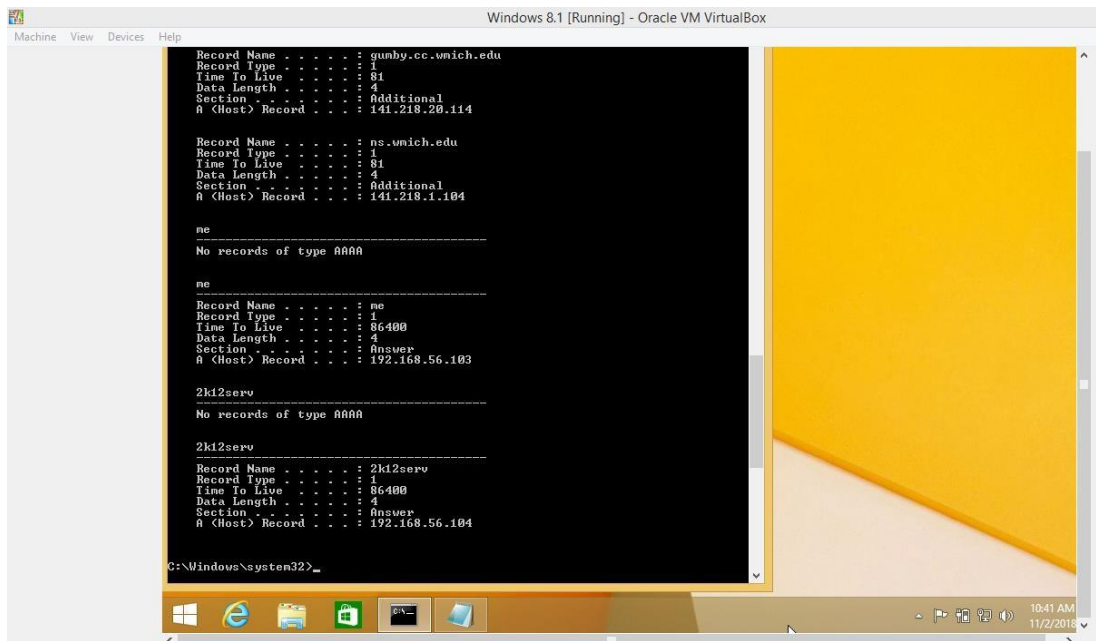
-Type ping me on command prompt



-Type ping 2k12serv on CMD and we can see the reply from the server.



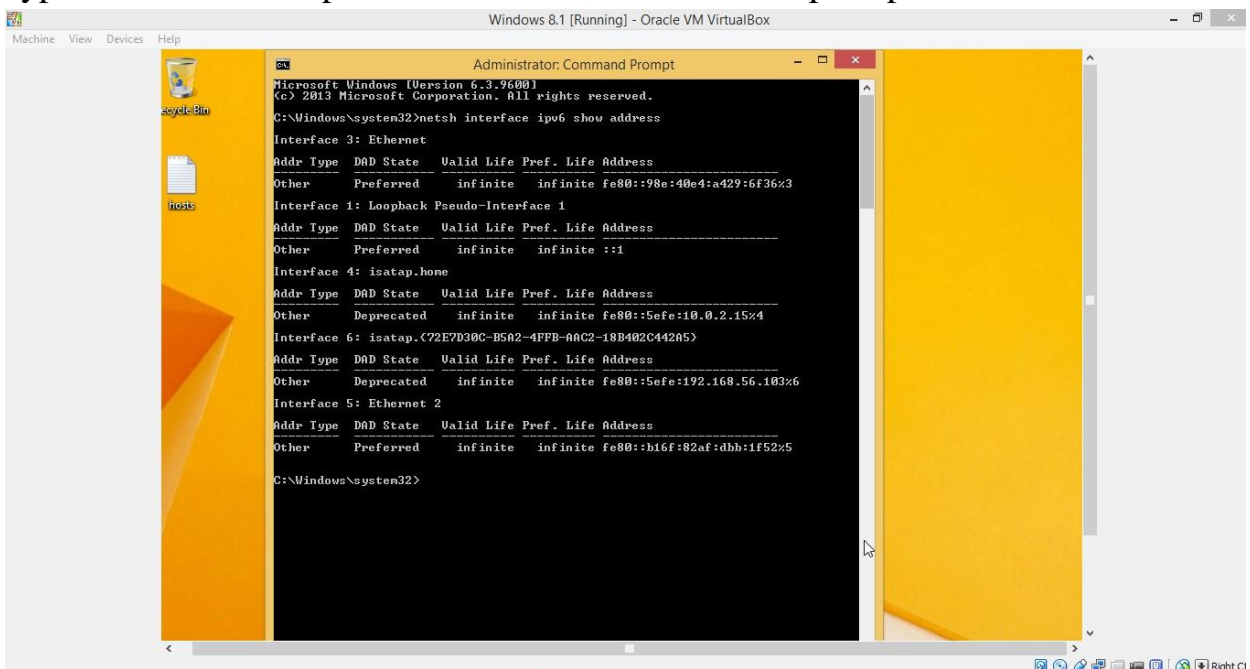
-Type ipconfig /displaydns



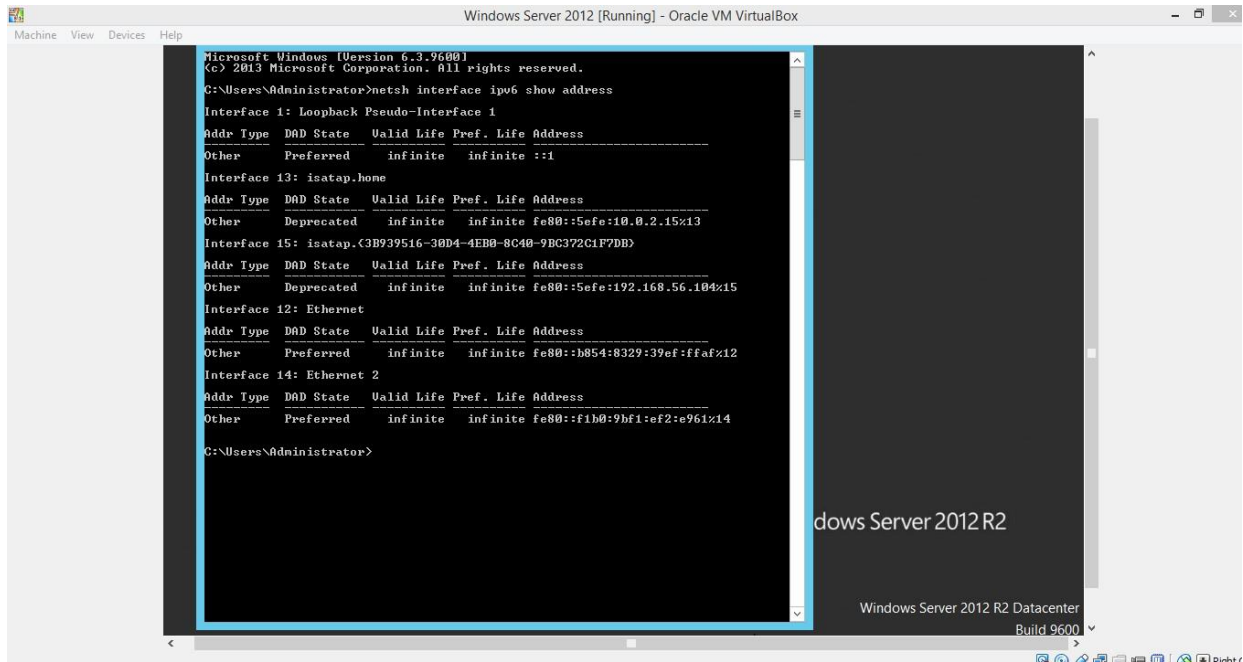
4 Lab 1.3w: Windows IPv6 Basics

Step 1: Verify IPv6 Setting for Win8.1 and W2K12.

-Type netsh interface ipv6 show address, on command prompt on Windows8.1

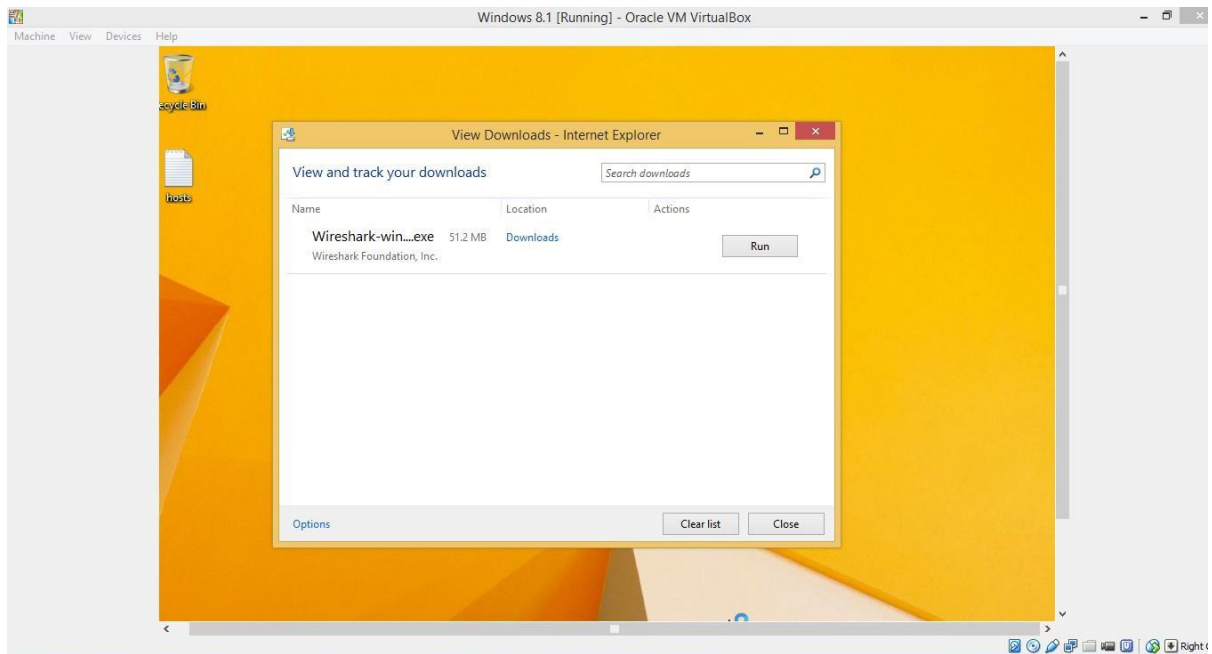


On W2k12, type netsh interface ipv6 show address on command prompt.

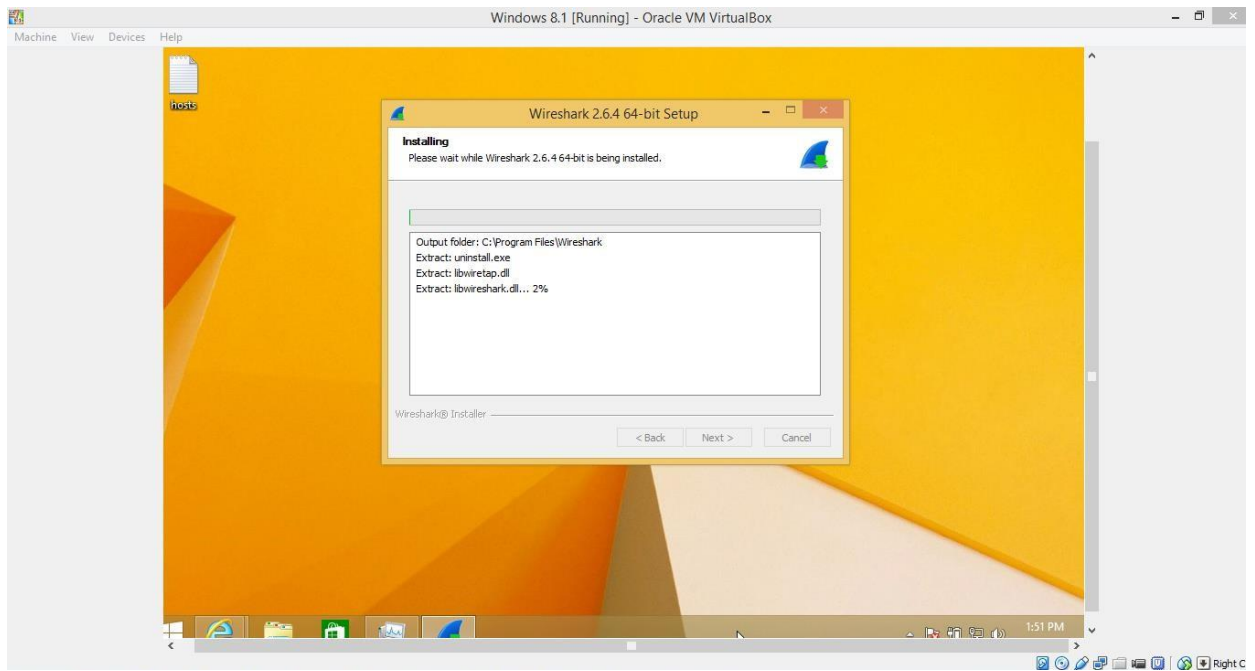
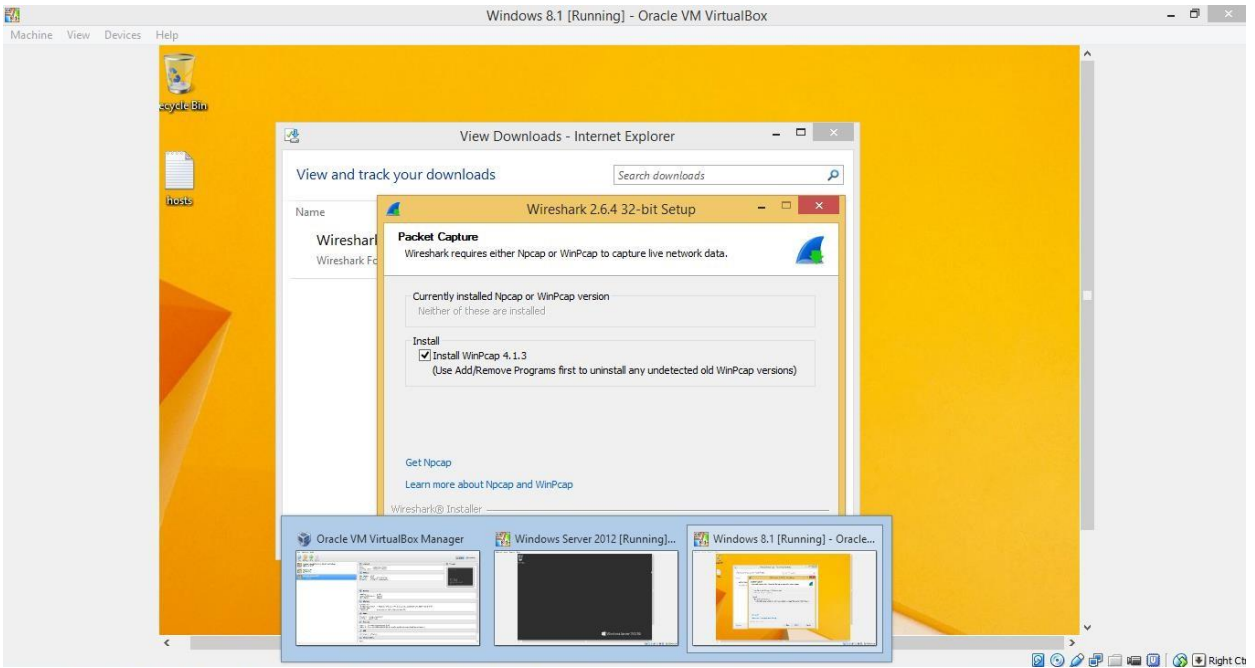


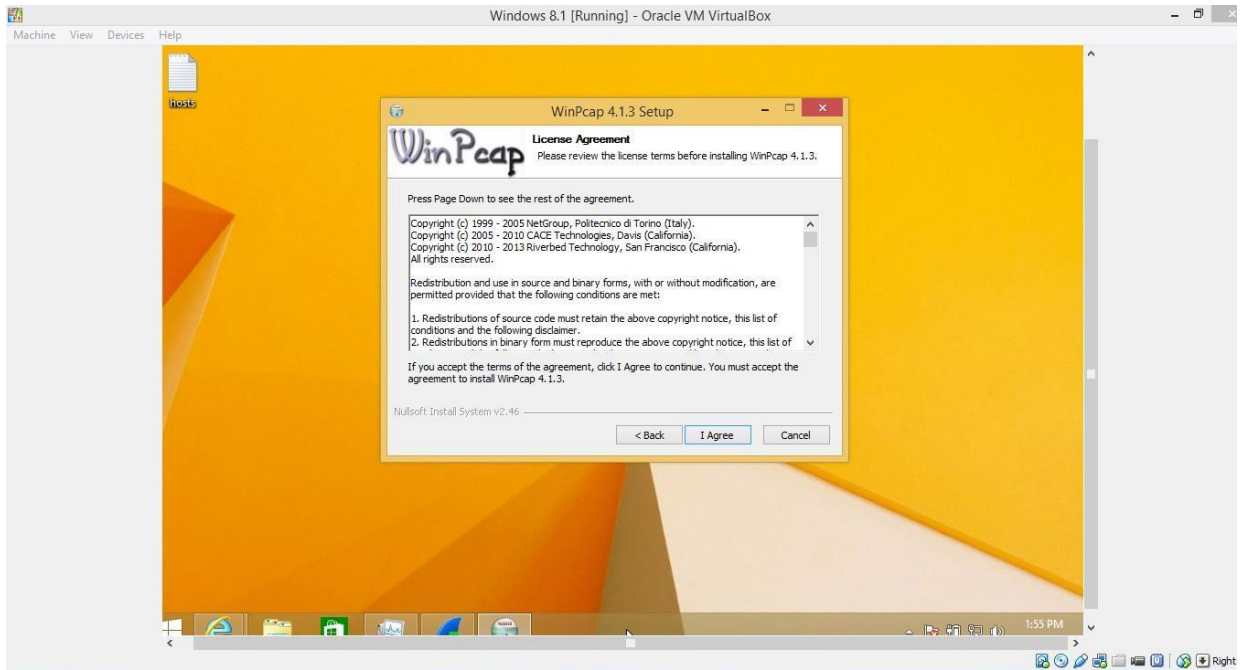
Step 2: Install Wireshark on Win8.1.

-From website www.wireshark.org/download.html , download wireshark.



-Follow the steps and install wireshark.





Download Wireshark

The current stable release of Wireshark is 2.4.4. It supersedes all previous releases. You can also download the latest development release (2.5.0) and documentation.

Stable Release (2.4.4)

- Windows Installer (64-bit)
-  Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.6 and later Intel 64-bit .dmg
- Source Code

Old Stable Release (2.2.12)

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?



Currently installed WinPcap version

WinPcap is currently not installed

Install

☒ Install WinPcap 4.1.3
(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)

What is WinPcap?

Wireshark Installer (tm)

< Back

Next >

Cancel

Install USBPcap?

USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?



Currently installed USBPcap version

USBPcap is currently not installed

Install

☒ Install USBPcap 1.2.0.3
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)

Important notice

In case of issue after installation, please use the system restore point created or read <https://github.com/desowin/usbpcap/issues/3>

What is USBPcap?

Wireshark Installer (tm)

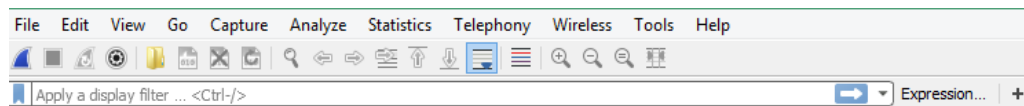
< Back

Install

Cancel

OPENING WIRESHARK

10:17 PM



Welcome to Wireshark

Capture

...using this filter: All interfaces shown

- ☒ Intel(R) PRO/1000 MT Desktop Adapter: Ethernet 2
- ☐ MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter
- ☐ Intel(R) PRO/1000 MT Desktop Adapter: Ethernet
- ☒ USBPcap1

Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.6.4 (v2.6.4-0-g29d48ec8). You receive automatic updates.

STARTING CONFIGURATION 10:31 PM

The image shows the main Wireshark packet capture window. The top part displays a list of captured packets. The bottom part shows the details of the selected packet (Frame 1).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID
2	0.990188	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID
3	2.000015	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID
4	4.020367	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID
5	8.021678	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID
6	16.036261	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID
7	30.916354	192.168.56.101	192.168.56.255	BROWSER	243	Host Announcement DESKTOP
8	32.036269	fe80::f5c6:82f3:78d...	ff02::1:2	DHCPv6	145	Solicit XID: 0xb437d9 CID

Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
 Ethernet II, Src: PcsCompu_a6:02:33 (08:00:27:a6:02:33), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
 Internet Protocol Version 6, Src: fe80::f5c6:82f3:78db:4c3, Dst: ff02::1:2
 User Datagram Protocol, Src Port: 546, Dst Port: 547
 DHCPv6

Offset	Hex	ASCII
0000	33 33 00 01 00 02 08 00 27 a6 02 33 86 dd 60 00	33...3...
0010	00 00 00 5b 11 01 fe 80 00 00 00 00 00 00 f5 c6	...[...]
0020	82 f3 78 db 04 c3 ff 02 00 00 00 00 00 00 00 00	...x...]
0030	00 00 00 01 00 02 02 22 02 23 00 5b 3b 51 01 b4	..."-#;Q...
0040	37 d9 00 08 00 02 00 00 00 01 00 0e 00 01 00 01	7... ..
0050	22 4b 1e 76 08 00 27 1b 8b 8b 00 03 00 0c 09 08	"K.v...' ..
0060	00 27 00 00 00 00 00 00 00 00 00 27 00 05 00 03	...'...' ..
0070	4c 61 62 00 10 00 0e 00 00 01 37 00 08 4d 53 46	Lab...7..MSF
0080	54 20 35 2e 30 00 06 00 08 00 18 00 17 00 11 00	T 5.0... ..
0090	27	,

PING -6 COMMAND 10:39 PM

```

C:\Users\Administrator>netsh interface ipv6 show address

Interface 3: Ethernet
Addr Type   DAD State   Valid Life   Pref. Life   Address
-----
Other       Preferred   infinite     infinite     fe80::55ae:5bf3:fc25:cc6c%3

Interface 1: Loopback Pseudo-Interface 1
Addr Type   DAD State   Valid Life   Pref. Life   Address
-----
Other       Preferred   infinite     infinite     ::1

Interface 5: isatap.{1D9BBA2-D02B-4E39-B223-D39D5E2CB302}
Addr Type   DAD State   Valid Life   Pref. Life   Address
-----
Other       Deprecated   infinite     infinite     fe80::5efe:192.168.56.103%5

Interface 8: isatap.{CC6770F5-E342-4F7C-B327-E8C998D1AECB}
Addr Type   DAD State   Valid Life   Pref. Life   Address
-----
Other       Deprecated   infinite     infinite     fe80::5efe:169.254.16.15%8

Interface 6: Ethernet 2
Addr Type   DAD State   Valid Life   Pref. Life   Address
-----
Other       Preferred   infinite     infinite     fe80::f5c6:82f3:78db:4c3%6

Interface 7: Npcap Loopback Adapter
Addr Type   DAD State   Valid Life   Pref. Life   Address
-----
Other       Preferred   infinite     infinite     fe80::ac5f:c0eb:d3b1:100f%7

C:\Users\Administrator>_

```

SESSION CAPTURED IN WIRESHARK 10:46 PM

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

- Packet List:** A table showing captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The packets listed are:

No.	Time	Source	Destination	Protocol	Length	Info
46	77.842551	192.168.56.101	224.0.0.251	MDNS	81	Standard query 0x0000 AAA
47	77.842655	fe80::d96c:2de6:e15...	ff02::fb	MDNS	101	Standard query 0x0000 AAA
48	77.843514	192.168.56.101	224.0.0.251	MDNS	81	Standard query 0x0000 AAA
49	77.843619	fe80::d96c:2de6:e15...	ff02::fb	MDNS	101	Standard query 0x0000 AAA
50	77.843893	fe80::d96c:2de6:e15...	ff02::1:3	LLMNR	95	Standard query 0x29de A D
51	77.843894	192.168.56.101	224.0.0.252	LLMNR	75	Standard query 0x29de A D
52	77.844169	fe80::d96c:2de6:e15...	ff02::1:3	LLMNR	95	Standard query 0xc484 AAA
53	77.844294	192.168.56.101	224.0.0.252	LLMNR	75	Standard query 0xc484 AAA
- Packet Details:** A tree view showing the structure of the selected packet (Frame 52). It includes:
 - Frame 52: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
 - Ethernet II, Src: PcsCompu_00:84:b6 (08:00:27:00:84:b6), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
 - Internet Protocol Version 6, Src: fe80::d96c:2de6:e15:fde9, Dst: ff02::1:3
 - User Datagram Protocol, Src Port: 55664, Dst Port: 5355
 - Link-local Multicast Name Resolution (query)
- Packet Bytes:** A hex dump of the packet data, showing the raw bytes in hexadecimal and their ASCII representation. The data starts with 33 33 00 01 00 03 08 00, which corresponds to the IPv6 multicast address ff02::1:3.

CLEARING THE ARP CASH,TYPE ARP-A 10:51 PM


```

-----
Other      Deprecated      infinite      infinite      fe80::5efe:169.254.16.15%8
Interface 6: Ethernet 2
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Other      Preferred      infinite      infinite      fe80::f5c6:82f3:78db:4c3%6
Interface 7: Npcap Loopback Adapter
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Other      Preferred      infinite      infinite      fe80::ac5f:c0eb:d3b1:100f%7

C:\Users\Administrator>arp -a

Interface: 10.0.2.15 --- 0x3
Internet Address      Physical Address      Type
10.0.2.2              52-54-00-12-35-02     dynamic
10.0.2.255            ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.103 --- 0x6
Internet Address      Physical Address      Type
192.168.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static

Interface: 169.254.16.15 --- 0x7
Internet Address      Physical Address      Type
169.254.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>

```

TYPING ARP-P AND ARP-A AGAIN IN COMMAND PROMPT 10:59 PM

```

-----
Other      Deprecated      infinite      infinite      fe80::5efe:169.254.16.15%8
Interface 6: Ethernet 2
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Other      Preferred      infinite      infinite      fe80::f5c6:82f3:78db:4c3%6
Interface 7: Npcap Loopback Adapter
Addr Type  DAD State  Valid Life  Pref. Life  Address
-----
Other      Preferred      infinite      infinite      fe80::ac5f:c0eb:d3b1:100f%7

C:\Users\Administrator>arp -a

Interface: 10.0.2.15 --- 0x3
Internet Address      Physical Address      Type
10.0.2.2              52-54-00-12-35-02     dynamic
10.0.2.255            ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.103 --- 0x6
Internet Address      Physical Address      Type
192.168.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static

Interface: 169.254.16.15 --- 0x7
Internet Address      Physical Address      Type
169.254.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>

```

START CAPTURING WIRESHARK SESSION 11:00PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression ...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_7f:2a:9c	Broadcast	ARP	60	Gratuitous ARP for 10.70.141.115 (Reply)
2	0.036824	10.91.2.29	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xfdb81c14
3	0.079211	Cisco_bf:61:8c	PVST+	STP	64	Conf. Root = 4096/140/3c:df:1e:8f:b0:c0 Cost = 6660 Port = 0x08ad
4	0.114095	141.218.147.167	255.255.255.255	UDP	60	59231 → 2008 Len=10
5	0.116369	141.218.148.32	255.255.255.255	GVCP	60	> DISCOVERY_CMD
6	0.131165	141.218.143.78	141.218.143.13	TLSv1.2	858	Application Data, Application Data, Application Data, Application Data, Application...
7	0.186800	141.218.141.12	255.255.255.255	GVCP	60	> DISCOVERY_CMD
8	0.224854	fe80::592c:a448:a1c...	ff02::1:3	LUNWR	95	Standard query 0xeb96 ANY DESKTOP-75TTA6A
9	0.224986	141.218.147.111	224.0.0.252	LUNWR	75	Standard query 0xeb96 ANY DESKTOP-75TTA6A
10	0.235623	141.218.141.192	255.255.255.255	UDP	82	64438 → 1947 Len=40
11	0.252829	fe80::a561:8612:da1...	ff02::1:2	DHCPv6	150	Solicit XID: 0xe9ec87 CID: 000100011a69ba37f8b156c2f3af
12	0.264394	141.218.147.227	255.255.255.255	GVCP	60	> DISCOVERY_CMD
13	0.265821	fe80::b0bf:dfad:780...	ff02::1:2	DHCPv6	151	Solicit XID: 0xff4843 CID: 0001000120e54d10050568517b5
14	0.275536	141.218.148.165	255.255.255.255	GVCP	60	> DISCOVERY_CMD
15	0.276707	Cisco_bf:61:8c	PVST+	STP	64	Conf. Root = 4096/591/3c:df:1e:8f:b0:c0 Cost = 6660 Port = 0x08ad
16	0.317130	141.218.147.167	255.255.255.255	UDP	60	59232 → 2008 Len=10

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Cisco_7f:2a:9c (f4:0f:1b:7f:2a:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (reply/gratuitous ARP)

```
0000 ff ff ff ff ff ff f4 0f 1b 7f 2a 9c 08 06 00 01 .....*. ....
0010 08 00 06 04 00 02 f4 0f 1b 7f 2a 9c 0a 46 8d 73 .....*.F.s
0020 ff ff ff ff ff ff 0a 46 8d 73 00 00 00 00 00 00 .....F.s.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... ..
```

STOP CAPTURING SESSION 11:01 PM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression ...

No.	Time	Source	Destination	Protocol	Length	Info
865	8.958130	35.46.125.117	224.0.0.251	MDNS	189	Standard query response 0x0000 PTR EPSON WF-3520 Series._http._tcp.local A, cache flush 35.46.125.
866	8.958425	fe80::b2e8:92ff:fe0...	ff02::fb	MDNS	209	Standard query response 0x0000 PTR EPSON WF-3520 Series._http._tcp.local A, cache flush 35.46.125.
867	8.961349	141.218.147.111	141.218.147.255	NBNS	92	Name query NB ESAJTLPSLM<00>
868	8.961350	141.218.147.111	141.218.147.255	NBNS	92	Name query NB BUJFJULFQ<00>
869	8.961568	141.218.147.216	141.218.147.255	NBNS	92	Name query NB WORKGROUP<id>
870	8.961636	141.218.146.18	224.0.0.251	MDNS	198	Standard query response 0x0000 PTR Officejet Pro 8600 [DCAB35]_http._tcp.local A, cache flush 14.
871	8.962209	fe80::da9d:67ff:fed...	ff02::fb	MDNS	218	Standard query response 0x0000 PTR Officejet Pro 8600 [DCAB35]_http._tcp.local A, cache flush 14.
872	8.963250	141.218.147.111	141.218.147.255	NBNS	92	Name query NB PXGYNACAMBGK<00>
873	8.966805	fe80::220:6bff:fea3...	ff02::fb	MDNS	217	Standard query response 0x0000 PTR KONICA MINOLTA bizhub C258(A3:ED:88)_http._tcp.local AAAA, ca...
874	8.970006	fe80::b9bb:b1cf:d5b...	ff02::1:2	DHCPv6	149	Solicit XID: 0x8c09b5 CID: 00010001200b081cb989096e33a8f
875	9.015018	141.218.147.86	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
876	9.025751	141.218.147.167	255.255.255.255	UDP	60	59277 → 2008 Len=10
877	9.064650	141.218.147.167	141.218.147.255	NBNS	92	Name query NB D7LL9SML<20>
878	9.066074	fe80::e053:b1d:4ae2...	ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
879	9.066217	141.218.147.123	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
880	9.066560	fe80::e053:b1d:4ae2...	ff02::c	SSDP	179	M-SEARCH * HTTP/1.1

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Cisco_7f:2a:9c (f4:0f:1b:7f:2a:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (reply/gratuitous ARP)

```
0000 ff ff ff ff ff ff f4 0f 1b 7f 2a 9c 08 06 00 01 .....*. ....
0010 08 00 06 04 00 02 f4 0f 1b 7f 2a 9c 0a 46 8d 73 .....*.F.s
0020 ff ff ff ff ff ff 0a 46 8d 73 00 00 00 00 00 00 .....F.s.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... ..
```

SESSION

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

Apply a display filter ... <Ctrl-F>Expression...

No.	Time	Source	Destination	Protocol	Length	Info
865	8.958130	35.46.125.117	224.0.0.251	MDNS	189	Standard query response 0x0000 PTR EPSON WF-3520 Series._http._tcp.local A, cache flush 35.46.125.
866	8.958425	fe00::b2e8:92ff:fe0...	ff02::fb	MDNS	209	Standard query response 0x0000 PTR EPSON WF-3520 Series._http._tcp.local A, cache flush 35.46.125.
867	8.961349	141.218.147.111	141.218.147.255	NBNS	92	Name query NB ESAJTLPSL<00>
868	8.961350	141.218.147.111	141.218.147.255	NBNS	92	Name query NB BUFJULFQ<00>
869	8.961568	141.218.147.216	141.218.147.255	NBNS	92	Name query NB WORKGROUP<id>
870	8.961636	141.218.146.18	224.0.0.251	MDNS	198	Standard query response 0x0000 PTR Officejet Pro 8600 [DCAB35]_http._tcp.local A, cache flush 14.
871	8.962209	fe00::da9d:67ff:fed...	ff02::fb	MDNS	218	Standard query response 0x0000 PTR Officejet Pro 8600 [DCAB35]_http._tcp.local A, cache flush 14.
872	8.963250	141.218.147.111	141.218.147.255	NBNS	92	Name query NB PXGYNAACAMBGK<00>
873	8.966085	fe00::220:6bff:fea3...	ff02::fb	MDNS	217	Standard query response 0x0000 PTR KONICA MINOLTA bizhub C258(A3:ED:88)_http._tcp.local AAAA, ca.
874	8.970086	fe00::b9bb:b1cf:d5b...	ff02::1:2	DHCPv6	149	Solicit XID: 0x8c09b5 CID: 00010001200b01cb989096e33a8f
875	9.015018	141.218.147.86	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
876	9.025751	141.218.147.167	255.255.255.255	UDP	60	59277 → 2000 Len=10
877	9.064650	141.218.147.167	141.218.147.255	NBNS	92	Name query NB D7LL9SIL<20>
878	9.066074	fe00::e053:b1d:4ae2...	ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
879	9.066217	141.218.147.123	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
880	9.066560	fe00::e053:b1d:4ae2...	ff02::c	SSDP	179	M-SEARCH * HTTP/1.1

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Cisco_7f:2a:9c (f4:0f:1b:7f:2a:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (reply/gratuitous ARP)

0000

ff ff ff ff ff ff f4 0f 1b 7f 2a 9c 08 06 00 01

0010

08 00 06 04 00 02 f4 0f 1b 7f 2a 9c 0a 46 8d 73

0020

ff ff ff ff ff ff 0a 46 8d 73 00 00 00 00 00 00

0030

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PORT CONNECTION STATUS 011: 14 PM

TYPE NETSTAT IN COMMAND PROMPT

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a          Displays all connections and listening ports.
-b          Displays the executable involved in creating each connection or
           listening port. In some cases well-known executables host
           multiple independent components, and in these cases the
           sequence of components involved in creating the connection
           or listening port is displayed. In this case the executable
           name is in [] at the bottom, on top is the component it called,
           and so forth until TCP/IP was reached. Note that this option
           can be time-consuming and will fail unless you have sufficient
           permissions.
-e          Displays Ethernet statistics. This may be combined with the -s
           option.
-f          Displays Fully Qualified Domain Names (FQDN) for foreign
           addresses.
-n          Displays addresses and port numbers in numerical form.
-o          Displays the owning process ID associated with each connection.
-p proto    Shows connections for the protocol specified by proto; proto
           may be any of: TCP, UDP, ICMPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r          Displays the routing table.
-s          Displays per-protocol statistics. By default, statistics are
           shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
           the -p option may be used to specify a subset of the default.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
           endpoints.
-y          Displays the TCP connection template for all connections.
           Cannot be combined with the other options.
interval    Redisplays selected statistics, pausing interval seconds
           between each display. Press CTRL+C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.

```

TYPE NETSTAT-A 06:21 PM

```

C:\Users\Administrator>netstat -na

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:554              0.0.0.0:0               LISTENING
TCP   0.0.0.0:2869             0.0.0.0:0               LISTENING
TCP   0.0.0.0:5357             0.0.0.0:0               LISTENING
TCP   0.0.0.0:10243            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49152            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49153            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49154            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49155            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49156            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49160            0.0.0.0:0               LISTENING
TCP   169.254.118.237:139      0.0.0.0:0               LISTENING
TCP   [::]:135                 [::]:0                  LISTENING
TCP   [::]:445                 [::]:0                  LISTENING
TCP   [::]:554                 [::]:0                  LISTENING
TCP   [::]:2869                [::]:0                  LISTENING
TCP   [::]:5357                [::]:0                  LISTENING
TCP   [::]:10243               [::]:0                  LISTENING
TCP   [::]:49152               [::]:0                  LISTENING
TCP   [::]:49153               [::]:0                  LISTENING
TCP   [::]:49154               [::]:0                  LISTENING
TCP   [::]:49155               [::]:0                  LISTENING
TCP   [::]:49156               [::]:0                  LISTENING
TCP   [::]:49160               [::]:0                  LISTENING
UDP   0.0.0.0:68               *:*:                     LISTENING
UDP   0.0.0.0:3702             *:*:                     LISTENING
UDP   0.0.0.0:3702             *:*:                     LISTENING
UDP   0.0.0.0:5004             *:*:                     LISTENING
UDP   0.0.0.0:5005             *:*:                     LISTENING
UDP   0.0.0.0:56866            *:*:                     LISTENING
UDP   127.0.0.1:1900           *:*:                     LISTENING
UDP   127.0.0.1:57851          *:*:                     LISTENING
UDP   169.254.118.237:137      *:*:                     LISTENING
UDP   169.254.118.237:138      *:*:                     LISTENING
UDP   169.254.118.237:1900     *:*:                     LISTENING
UDP   [::]:3702                *:*:                     LISTENING
UDP   [::]:3702                *:*:                     LISTENING
UDP   [::]:5004                *:*:                     LISTENING
UDP   [::]:5005                *:*:                     LISTENING
UDP   [::]:56867               *:*:                     LISTENING
UDP   [::]:1900                *:*:                     LISTENING
UDP   [::]:57850               *:*:                     LISTENING
UDP   [fe80::c8ea:f3ee:6e7c:76ed%3]:1900 *:*:

```

I THINK YOU ARE ASKED TO DO HERE.SO ,IT IS DONE TILL HERE

Best Sampath Talluri.

