NAME: SANIKA GIDYE
PRN:121A3017

Experiment No: 8

STUDY OF PACKET SNIFFER TOOLS WIRESHARK

Aim: - a. Observer performance in promiscuous as well as non-promiscuous mode.
b. Show the packets can be traced based on different filters.

Resources Required: -

1. WireShark

Procedure/Algorithm -

1. **Launch Wireshark:** Open Wireshark with administrative privileges. On most operating systems, you will need elevated permissions to capture network traffic
2. **Select the Network Interface:** Wireshark will display a list of available network interfaces. Choose the network interface you want to monitor. This interface can be in either promiscuous or non-promiscuous mode depending on your testing objectives.
3. **Configure Capture Options:**

   - Promiscuous Mode:

   If you want to observe network performance in promiscuous mode, you don't need to make any specific changes in Wireshark. It will capture all traffic on the selected interface by default.

   - Non-Promiscuous Mode:

   To capture traffic in non-promiscuous mode, you can apply a capture filter to limit the captured packets to specific criteria. For example, you can capture only traffic going to or from a specific IP address or port. Click on "Capture" > "Capture Filters" to set your filter.

4. **Start Capturing Packets:** Click the "Start" or "Capture" button in

Wireshark to begin capturing network packets on the selected interface.

5. **Stop Capturing Packets:** When you have collected enough data or want to end the monitoring session, click the "Stop" or "Capture" button in Wireshark to stop capturing packets.

Theory:

Promiscuous mode:

Promiscuous mode is a type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode. It is a network security, monitoring and administration technique that enables access to entire network data packets by any configured network adapter on a host system.
Promiscuous mode is used to monitor(sniff) network traffic.

Typically, promiscuous mode is used and implemented by a snoop program that captures all network traffic visible on all configured network adapters on a system. Because of its ability to access all network traffic on a segment, promiscuous mode is also considered unsafe. Like a system with multiple VMs, each host has the ability to see network packets destined for other VMs on that system.

This mode applies to both a wired network interface card and wireless NIC. In both cases, it causes the controller to pass *all* traffic it receives to the central processing unit instead of just the frames it is specifically programmed to receive

Promiscuous mode can also be configured so that the packet data is accessible to a guest OS or a visitor on the host system.

The packet sniffer collects all the traffic flowing through the physical interface, separates or reassembles it as required, and then logs it as per the network's requirement.

The network adapter is in promiscuous mode given the following:

- It was manually configured using the ifconfig command or the ip link set.
- A monitoring tool is used.

In a bridge network, the NIC may be required to operate in promiscuous mode. In that case, the mode must be supported by each network adapter, as well as by the input/output driver in the host OS. Some OSes require superuser privileges to enable this mode.

Non-Promiscuous mode:

In promiscuous mode, the NIC allows all frames through, so even framesintended for other machines or network devices can be read. But, in non-promiscuous mode, when the NIC receives a frame, it drops it unless it isaddressed to its specific media access control address or is a broadcast or multicast addressed frame.

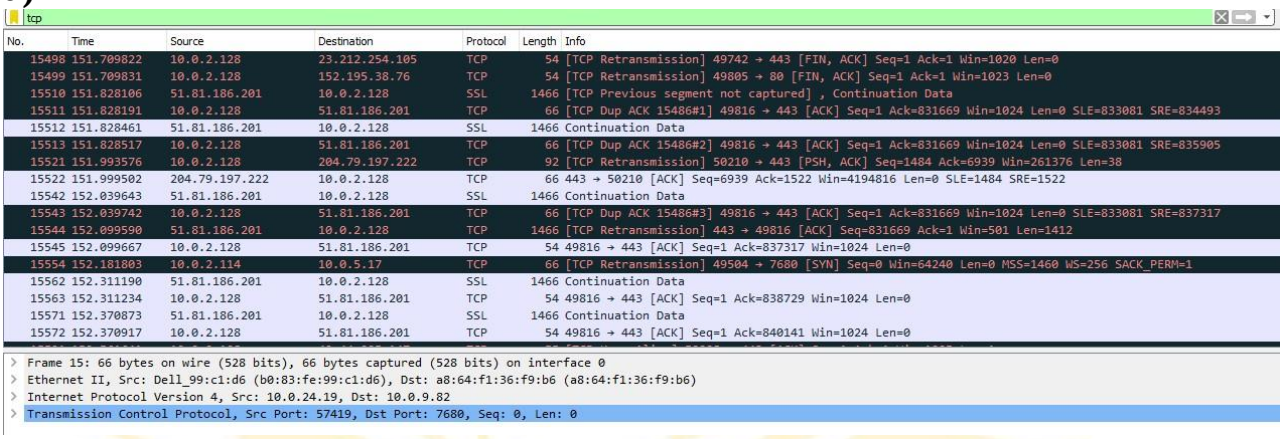
So, when a data packet is transmitted in non-promiscuous mode, all the LAN devices listen to the data to determine if their network address is included in the packet. If it's not, the packet is passed onto the next LAN device until the correct network address is reached. That device then reads the data.

If the interface is not running in promiscuous mode, it won't see any traffic that isn't intended to be seen by your machine. It will see broadcast packets, and multicast packets sent to a multicast MAC address the interface is set up to receive.

NAME: SANIKA GIDYE
PRN:121A3017

Results:

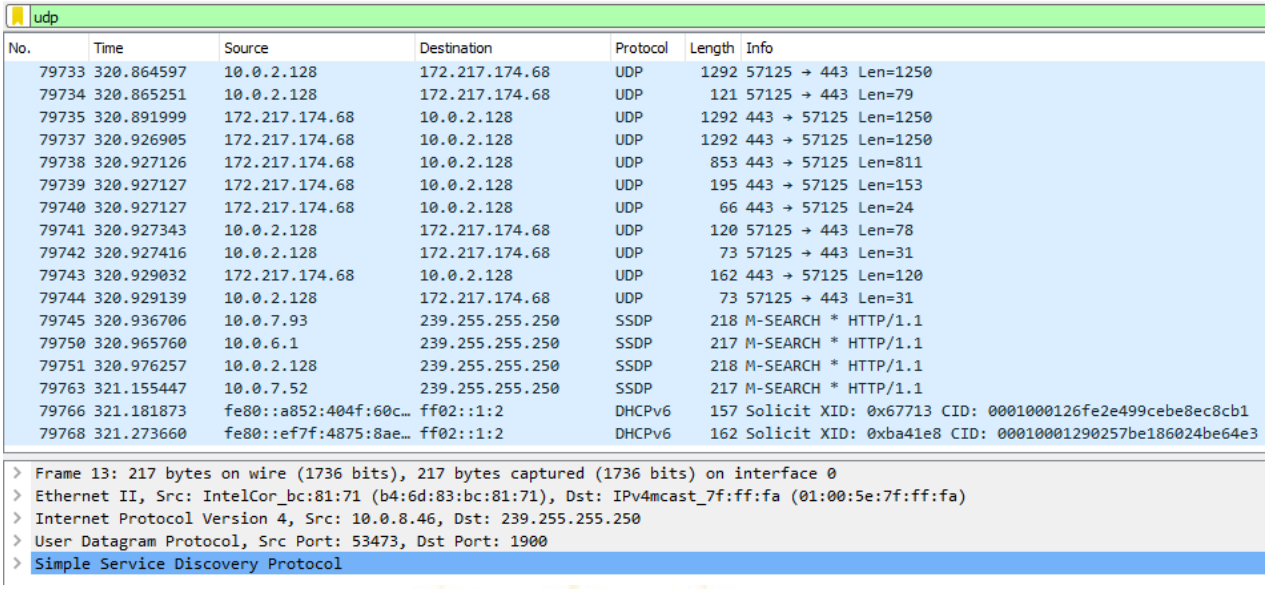
a)



tcp

No.	Time	Source	Destination	Protocol	Length	Info
15498	151.709822	10.0.2.128	23.212.254.105	TCP	54	[TCP Retransmission] 49742 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
15499	151.709831	10.0.2.128	152.195.38.76	TCP	54	[TCP Retransmission] 49805 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
15510	151.828106	51.81.186.201	10.0.2.128	SSL	1466	[TCP Previous segment not captured] , Continuation Data
15511	151.828191	10.0.2.128	51.81.186.201	TCP	66	[TCP Dup ACK 15486#1] 49816 → 443 [ACK] Seq=1 Ack=831669 Win=1024 Len=0 SLE=833081 SRE=834493
15512	151.828461	51.81.186.201	10.0.2.128	SSL	1466	Continuation Data
15513	151.828517	10.0.2.128	51.81.186.201	TCP	66	[TCP Dup ACK 15486#2] 49816 → 443 [ACK] Seq=1 Ack=831669 Win=1024 Len=0 SLE=833081 SRE=835905
15521	151.993576	10.0.2.128	204.79.197.222	TCP	92	[TCP Retransmission] 50210 → 443 [PSH, ACK] Seq=1484 Ack=6939 Win=261376 Len=38
15522	151.999502	204.79.197.222	10.0.2.128	TCP	66	443 → 50210 [ACK] Seq=6939 Ack=1522 Win=4194816 Len=0 SLE=1484 SRE=1522
15542	152.039643	51.81.186.201	10.0.2.128	SSL	1466	Continuation Data
15543	152.039742	10.0.2.128	51.81.186.201	TCP	66	[TCP Dup ACK 15486#3] 49816 → 443 [ACK] Seq=1 Ack=831669 Win=1024 Len=0 SLE=833081 SRE=837317
15544	152.099590	51.81.186.201	10.0.2.128	TCP	1466	[TCP Retransmission] 443 → 49816 [ACK] Seq=831669 Ack=1 Win=501 Len=1412
15545	152.099667	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=837317 Win=1024 Len=0
15554	152.181803	10.0.2.114	10.0.5.17	TCP	66	[TCP Retransmission] 49504 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15562	152.311190	51.81.186.201	10.0.2.128	SSL	1466	Continuation Data
15563	152.311234	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=838729 Win=1024 Len=0
15571	152.370873	51.81.186.201	10.0.2.128	SSL	1466	Continuation Data
15572	152.370917	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=840141 Win=1024 Len=0

```
> Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Dell_99:c1:d6 (b0:83:fe:99:c1:d6), Dst: a8:64:f1:36:f9:b6 (a8:64:f1:36:f9:b6)
> Internet Protocol Version 4, Src: 10.0.24.19, Dst: 10.0.9.82
> Transmission Control Protocol, Src Port: 57419, Dst Port: 7680, Seq: 0, Len: 0
```



udp

No.	Time	Source	Destination	Protocol	Length	Info
79733	320.864597	10.0.2.128	172.217.174.68	UDP	1292	57125 → 443 Len=1250
79734	320.865251	10.0.2.128	172.217.174.68	UDP	121	57125 → 443 Len=79
79735	320.891999	172.217.174.68	10.0.2.128	UDP	1292	443 → 57125 Len=1250
79737	320.926905	172.217.174.68	10.0.2.128	UDP	1292	443 → 57125 Len=1250
79738	320.927126	172.217.174.68	10.0.2.128	UDP	853	443 → 57125 Len=811
79739	320.927127	172.217.174.68	10.0.2.128	UDP	195	443 → 57125 Len=153
79740	320.927127	172.217.174.68	10.0.2.128	UDP	66	443 → 57125 Len=24
79741	320.927343	10.0.2.128	172.217.174.68	UDP	120	57125 → 443 Len=78
79742	320.927416	10.0.2.128	172.217.174.68	UDP	73	57125 → 443 Len=31
79743	320.929032	172.217.174.68	10.0.2.128	UDP	162	443 → 57125 Len=120
79744	320.929139	10.0.2.128	172.217.174.68	UDP	73	57125 → 443 Len=31
79745	320.936706	10.0.7.93	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
79750	320.965760	10.0.6.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
79751	320.976257	10.0.2.128	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
79763	321.155447	10.0.7.52	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
79766	321.181873	fe80::a852:404f:60c…	ff02::1:2	DHCPv6	157	Solicit XID: 0x67713 CID: 0001000126fe2e499cebe8ec8cb1
79768	321.273660	fe80::ef7f:4875:8ae…	ff02::1:2	DHCPv6	162	Solicit XID: 0xba41e8 CID: 00010001290257be186024be64e3

```
> Frame 13: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
> Ethernet II, Src: IntelCor_bc:81:71 (b4:6d:83:bc:81:71), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.0.8.46, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 53473, Dst Port: 1900
> Simple Service Discovery Protocol
```

NAME: SANIKA GIDYE
PRN:121A3017

arp

No.	Time	Source	Destination	Protocol	Length	Info
86217	386.319402	6c:3c:8c:02:8f:b4	Broadcast	ARP	60	Who has 10.0.2.114? Tell 10.0.5.52
86218	386.361890	Vmware_47:94:98	Broadcast	ARP	60	Who has 10.44.136.226? Tell 10.0.0.8
86219	386.395620	6c:3c:8c:00:76:34	Broadcast	ARP	60	Who has 10.0.4.163? Tell 10.0.7.227
86223	386.423909	Dell_7f:01:81	Broadcast	ARP	60	Who has 10.0.1.103? Tell 10.0.7.244
86224	386.457737	Dell_99:b8:a8	Broadcast	ARP	60	Who has 169.254.169.254? Tell 10.0.24.36
86225	386.464513	60:a4:b7:58:27:d2	Broadcast	ARP	60	Who has 10.0.0.17? Tell 10.0.9.65
86226	386.464827	60:a4:b7:58:27:d2	Broadcast	ARP	60	Who has 10.0.19.11? Tell 10.0.9.65
86227	386.464828	60:a4:b7:58:27:d2	Broadcast	ARP	60	Who has 10.0.0.38? Tell 10.0.9.65
86228	386.464829	60:a4:b7:58:27:d2	Broadcast	ARP	60	Who has 10.0.4.202? Tell 10.0.9.65
86229	386.464830	60:a4:b7:58:27:d2	Broadcast	ARP	60	Who has 10.0.25.75? Tell 10.0.9.65
86230	386.465149	60:a4:b7:58:27:d2	Broadcast	ARP	60	Who has 10.0.7.104? Tell 10.0.9.65
86232	386.515150	Dell_f0:37:48	Broadcast	ARP	60	Who has 10.0.0.19? Tell 10.0.0.33
86234	386.623732	Dell_99:02:60	Broadcast	ARP	60	Who has 10.0.16.176? Tell 10.0.24.46
86235	386.636619	6c:3c:8c:00:7a:37	Broadcast	ARP	60	Who has 10.0.4.235? Tell 10.0.4.19
86236	386.656630	Dell_b3:b5:65	Broadcast	ARP	60	Who has 10.0.9.101? Tell 10.0.1.139
86237	386.663838	Dell_0a:e6:aa	Broadcast	ARP	60	Who has 10.0.24.58? Tell 10.0.2.189
86240	386.672211	Dell_b3:b5:65	Broadcast	ARP	60	Who has 10.0.9.13? Tell 10.0.1.139

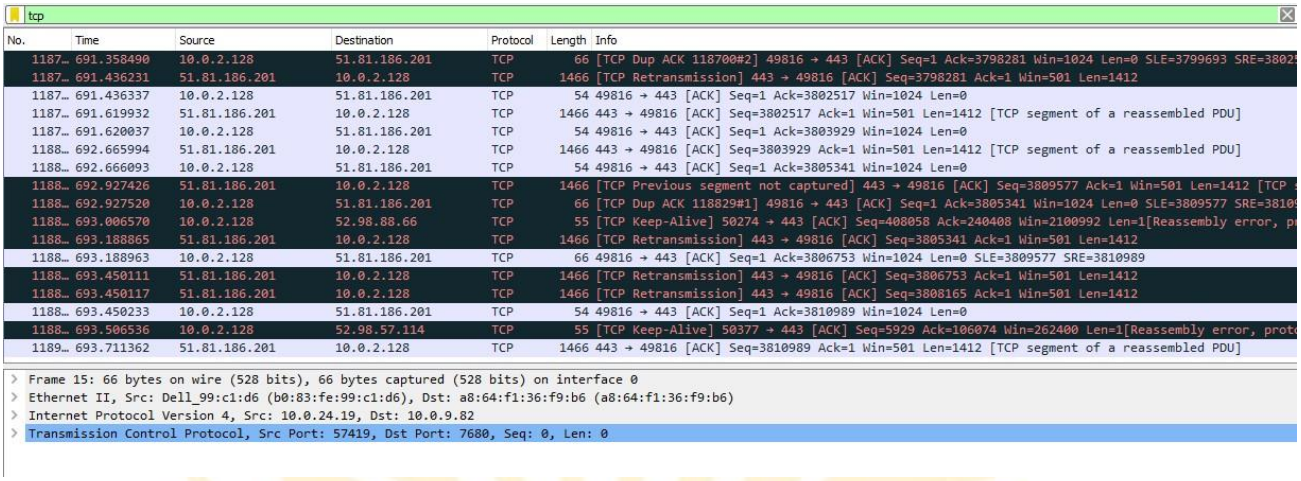
```
> Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: bc:09:1b:b4:bb:58 (bc:09:1b:b4:bb:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

ssdp

No.	Time	Source	Destination	Protocol	Length	Info
95269	479.958534	10.0.10.250	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
95276	480.097347	172.16.0.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
95277	480.120967	10.0.10.193	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
95279	480.135010	10.0.5.60	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
95282	480.143822	10.0.19.202	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
95283	480.188690	10.0.8.46	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
95289	480.295108	10.0.8.223	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
95290	480.309437	10.0.5.54	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
95293	480.347136	172.16.0.52	239.255.255.250	SSDP	178	M-SEARCH * HTTP/1.1
95294	480.367458	10.0.2.165	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
95299	480.387634	10.0.8.223	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
95302	480.455303	172.16.0.52	239.255.255.250	SSDP	178	M-SEARCH * HTTP/1.1
95314	480.533027	10.0.24.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
95319	480.574767	10.0.4.16	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
95321	480.592976	10.0.2.214	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
95328	480.723604	10.0.24.45	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
95333	480.769445	10.0.2.138	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

```
> Frame 11: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: Dell_28:ca:fc (50:9a:4c:28:ca:fc), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.0.19.202, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 38600, Dst Port: 1900
> Simple Service Discovery Protocol
```

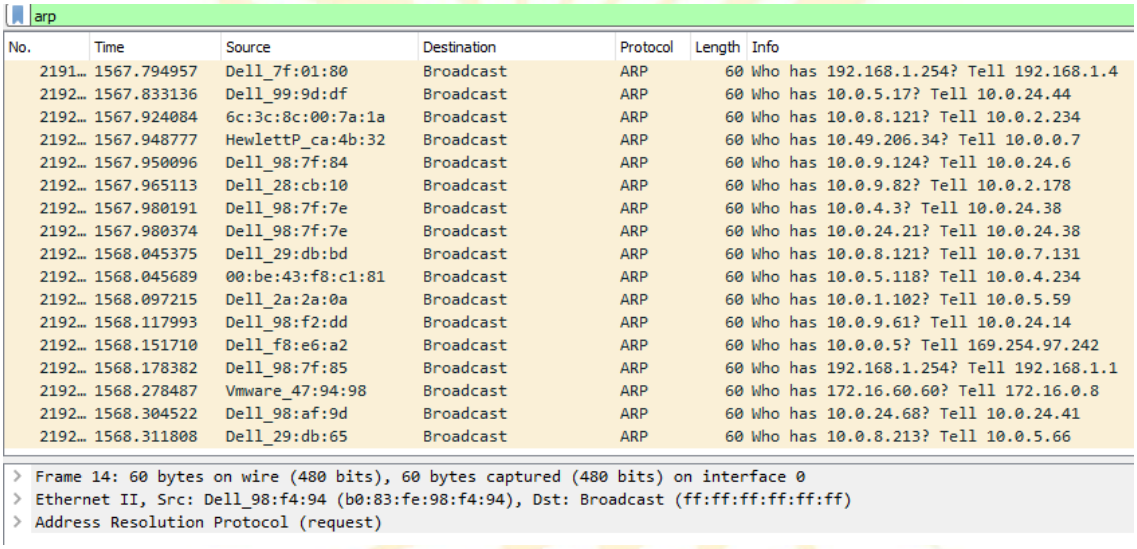
Non-Promiscuous:



tcp

No.	Time	Source	Destination	Protocol	Length	Info
1187…	691.358490	10.0.2.128	51.81.186.201	TCP	66	[TCP Dup ACK 118700#2] 49816 → 443 [ACK] Seq=1 Ack=3798281 Win=1024 Len=0 SLE=3799693 SRE=3802
1187…	691.436231	51.81.186.201	10.0.2.128	TCP	1466	[TCP Retransmission] 443 → 49816 [ACK] Seq=3798281 Ack=1 Win=501 Len=1412
1187…	691.436337	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=3802517 Win=1024 Len=0
1187…	691.619932	51.81.186.201	10.0.2.128	TCP	1466	443 → 49816 [ACK] Seq=3802517 Ack=1 Win=501 Len=1412 [TCP segment of a reassembled PDU]
1187…	691.620037	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=3803929 Win=1024 Len=0
1188…	692.665994	51.81.186.201	10.0.2.128	TCP	1466	443 → 49816 [ACK] Seq=3803929 Ack=1 Win=501 Len=1412 [TCP segment of a reassembled PDU]
1188…	692.666093	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=3805341 Win=1024 Len=0
1188…	692.927426	51.81.186.201	10.0.2.128	TCP	1466	[TCP Previous segment not captured] 443 → 49816 [ACK] Seq=3809577 Ack=1 Win=501 Len=1412 [TCP
1188…	692.927520	10.0.2.128	51.81.186.201	TCP	66	[TCP Dup ACK 118829#1] 49816 → 443 [ACK] Seq=1 Ack=3805341 Win=1024 Len=0 SLE=3809577 SRE=3810
1188…	693.006570	10.0.2.128	52.98.88.66	TCP	55	[TCP Keep-Alive] 50274 → 443 [ACK] Seq=408058 Ack=240408 Win=2100992 Len=1[Reassembly error, p
1188…	693.188865	51.81.186.201	10.0.2.128	TCP	1466	[TCP Retransmission] 443 → 49816 [ACK] Seq=3805341 Ack=1 Win=501 Len=1412
1188…	693.188963	10.0.2.128	51.81.186.201	TCP	66	49816 → 443 [ACK] Seq=1 Ack=3806753 Win=1024 Len=0 SLE=3809577 SRE=3810989
1188…	693.450111	51.81.186.201	10.0.2.128	TCP	1466	[TCP Retransmission] 443 → 49816 [ACK] Seq=3806753 Ack=1 Win=501 Len=1412
1188…	693.450117	51.81.186.201	10.0.2.128	TCP	1466	[TCP Retransmission] 443 → 49816 [ACK] Seq=3808165 Ack=1 Win=501 Len=1412
1188…	693.450233	10.0.2.128	51.81.186.201	TCP	54	49816 → 443 [ACK] Seq=1 Ack=3810989 Win=1024 Len=0
1188…	693.506536	10.0.2.128	52.98.57.114	TCP	55	[TCP Keep-Alive] 50377 → 443 [ACK] Seq=5929 Ack=106074 Win=262400 Len=1[Reassembly error, proto
1189…	693.711362	51.81.186.201	10.0.2.128	TCP	1466	443 → 49816 [ACK] Seq=3810989 Ack=1 Win=501 Len=1412 [TCP segment of a reassembled PDU]

```
> Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Dell_99:c1:d6 (b0:83:fe:99:c1:d6), Dst: a8:64:f1:36:f9:b6 (a8:64:f1:36:f9:b6)
> Internet Protocol Version 4, Src: 10.0.24.19, Dst: 10.0.9.82
> Transmission Control Protocol, Src Port: 57419, Dst Port: 7680, Seq: 0, Len: 0
```



arp

No.	Time	Source	Destination	Protocol	Length	Info
2191…	1567.794957	Dell_7f:01:80	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.4
2192…	1567.833136	Dell_99:9d:df	Broadcast	ARP	60	Who has 10.0.5.17? Tell 10.0.24.44
2192…	1567.924084	6c:3c:8c:00:7a:1a	Broadcast	ARP	60	Who has 10.0.8.121? Tell 10.0.2.234
2192…	1567.948777	HewlettP_ca:4b:32	Broadcast	ARP	60	Who has 10.49.206.34? Tell 10.0.0.7
2192…	1567.950096	Dell_98:7f:84	Broadcast	ARP	60	Who has 10.0.9.124? Tell 10.0.24.6
2192…	1567.965113	Dell_28:cb:10	Broadcast	ARP	60	Who has 10.0.9.82? Tell 10.0.2.178
2192…	1567.980191	Dell_98:7f:7e	Broadcast	ARP	60	Who has 10.0.4.3? Tell 10.0.24.38
2192…	1567.980374	Dell_98:7f:7e	Broadcast	ARP	60	Who has 10.0.24.21? Tell 10.0.24.38
2192…	1568.045375	Dell_29:db:bd	Broadcast	ARP	60	Who has 10.0.8.121? Tell 10.0.7.131
2192…	1568.045689	00:be:43:f8:c1:81	Broadcast	ARP	60	Who has 10.0.5.118? Tell 10.0.4.234
2192…	1568.097215	Dell_2a:2a:0a	Broadcast	ARP	60	Who has 10.0.1.102? Tell 10.0.5.59
2192…	1568.117993	Dell_98:f2:dd	Broadcast	ARP	60	Who has 10.0.9.61? Tell 10.0.24.14
2192…	1568.151710	Dell_f8:e6:a2	Broadcast	ARP	60	Who has 10.0.0.5? Tell 169.254.97.242
2192…	1568.178382	Dell_98:7f:85	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.1
2192…	1568.278487	Vmware_47:94:98	Broadcast	ARP	60	Who has 172.16.60.60? Tell 172.16.0.8
2192…	1568.304522	Dell_98:af:9d	Broadcast	ARP	60	Who has 10.0.24.68? Tell 10.0.24.41
2192…	1568.311808	Dell_29:db:65	Broadcast	ARP	60	Who has 10.0.8.213? Tell 10.0.5.66

```
> Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Dell_98:f4:94 (b0:83:fe:98:f4:94), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

b)

tcp

No.	Time	Source	Destination	Protocol	Length	Info
5278	47.557780	52.114.44.79	10.0.2.122	TCP	528	[TCP Retransmission] 443 → 51290 [PSH, ACK] Seq=1353 Ack=3864 Win=2047 Len=474
5279	47.559047	10.0.2.122	52.114.44.79	TCP	1466	51290 → 443 [ACK] Seq=3864 Ack=1827 Win=1024 Len=1412 [TCP segment of a reassembled PDU]
5280	47.559047	10.0.2.122	52.114.44.79	TLSv1.2	626	Application Data
5281	47.581405	10.0.2.122	52.111.252.0	TCP	55	[TCP Keep-Alive] 51047 → 443 [ACK] Seq=46 Ack=47 Win=1022 Len=1
5282	47.593749	52.111.252.0	10.0.2.122	TCP	66	[TCP Keep-Alive ACK] 443 → 51047 [ACK] Seq=47 Ack=47 Win=2050 Len=0 SLE=46 SRE=47
5343	48.647542	10.0.2.122	34.161.115.43	TCP	55	[TCP Spurious Retransmission] 51299 → 443 [ACK] Seq=66 Ack=65 Win=1024 Len=1
5359	48.905518	34.161.115.43	10.0.2.122	TCP	60	443 → 51299 [ACK] Seq=65 Ack=68 Win=501 Len=0
5361	48.916258	52.98.57.114	10.0.2.122	TCP	60	443 → 51307 [RST] Seq=1 Win=0 Len=0
5364	48.918402	10.0.2.122	40.99.31.130	TCP	66	51316 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5365	48.927509	40.99.31.130	10.0.2.122	TCP	66	443 → 51316 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM
5366	48.927621	10.0.2.122	40.99.31.130	TCP	54	51316 → 443 [ACK] Seq=1 Ack=1 Win=262400 Len=0
5367	48.928195	10.0.2.122	40.99.31.130	TLSv1	821	Client Hello
5368	48.928582	40.99.31.130	10.0.2.122	TCP	60	443 → 51316 [ACK] Seq=1 Ack=768 Win=66304 Len=0
5373	49.015076	10.0.5.23	10.0.7.148	TCP	66	[TCP Retransmission] 56395 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5381	49.126845	40.99.31.130	10.0.2.122	TCP	60	[TCP Dup ACK 5368#1] 443 → 51316 [ACK] Seq=1 Ack=768 Win=66304 Len=0
5396	49.302461	10.0.2.122	52.98.57.114	TCP	66	[TCP Retransmission] 51315 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

```
> Frame 10: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface \Device\NPF
> Ethernet II, Src: Dell_b3:af:6e (b0:83:fe:b3:af:6e), Dst: Sophos_07:36:e4 (c8:4f:86:07:36:e4)
> Internet Protocol Version 4, Src: 10.0.2.122, Dst: 34.161.115.43
> Transmission Control Protocol, Src Port: 51299, Dst Port: 443, Seq: 1, Ack: 1, Len: 66
> Transport Layer Security
```

```
0000  c8 4f 86 07 36 e4 b0 83  fe b3 af 6e 08 00 45 00   ·O··6··· ···n··E·
0010  00 6a ba 5b 00 00 80 06  dd ec 0a 00 02 7a 22 a1   ·j·[···· ·····z"·
0020  73 2b c8 63 01 bb 5a 7f  30 ff 0f 1c e5 da 50 18   s+·c··Z· 0·····P·
0030  04 01 5c 55 00 00 17 03  03 00 1a da 7b 10 f2 9f   ··\U···· ····{···
0040  6a 45 7f 71 a8 e6 46 ac  ad 17 ac b2 ed 55 b9 8b   jE·q··F· ·····U··
0050  c8 09 93 e2 27 17 03 03  00 1e 81 f9 0e aa 27 c4   ····'··· ······'·
0060  7a 84 54 0a 6e 3c 9f 0d  fb 9c 76 34 d6 8d 71 8c   z·T·n<·· ··v4··q·
0070  ec 53 78 ec 6d 47 3e fe                           ·Sx·mG>·
```

udp

No.	Time	Source	Destination	Protocol	Length	Info
8344	77.562933	10.0.4.33	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
8345	77.571421	10.0.2.129	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
8346	77.576633	10.0.9.18	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
8347	77.608477	10.0.25.179	10.255.255.255	BROWSER	243	Local Master Announcement ADMIN, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser, M
8350	77.637503	10.0.7.254	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8358	77.819742	10.0.2.186	10.255.255.255	NBNS	92	Name query NB IT86<1c>
8359	77.832597	10.0.1.139	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8363	77.909409	10.0.4.14	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
8366	78.022398	10.0.7.104	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
8367	78.023768	fe80::4e48:3797:165…	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
8368	78.031935	10.0.24.67	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
8378	78.294645	10.0.8.0	10.255.255.255	NBNS	92	Name query NB OFFICE<00>
8385	78.347057	10.0.4.39	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8388	78.440504	10.168.0.115	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
8391	78.466487	10.0.9.18	239.255.255.250	UDP	698	59387 → 3702 Len=656
8392	78.471947	10.0.7.93	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1

```
> Frame 7: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface \Device\NP
> Ethernet II, Src: Elitegro_54:99:33 (10:78:d2:54:99:33), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:
> Internet Protocol Version 4, Src: 10.0.5.232, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 62265, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 10 78  d2 54 99 33 08 00 45 00   ··^····x ·T·3··E·
0010  00 cc 57 cd 00 00 01 11  61 72 0a 00 05 e8 ef ff   ··W····· ar······
0020  ff fa f3 39 07 6c 00 b8  c9 e8 4d 2d 53 45 41 52   ···9·l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 4d 69 63 72 6f 73 6f  66 74 20 45 64 67 65 2f    Microso ft Edge/
00c0  31 31 35 2e 30 2e 31 39  30 31 2e 32 30 33 20 57   115.0.19 01.203 W
00d0  69 6e 64 6f 77 73 0d 0a  0d 0a                    indows·· ··
```

arp

No.	Time	Source	Destination	Protocol	Length	Info
11943	109.336123	TP-Link_58:27:d2	Broadcast	ARP	60	Who has 10.0.8.98? Tell 10.0.9.65
11944	109.336435	TP-Link_58:27:d2	Broadcast	ARP	60	Who has 10.0.10.5? Tell 10.0.9.65
11945	109.336435	TP-Link_58:27:d2	Broadcast	ARP	60	Who has 10.0.0.42? Tell 10.0.9.65
11946	109.336435	TP-Link_58:27:d2	Broadcast	ARP	60	Who has 10.0.6.115? Tell 10.0.9.65
11947	109.336435	TP-Link_58:27:d2	Broadcast	ARP	60	Who has 10.0.4.238? Tell 10.0.9.65
11948	109.382301	Dell_b3:af:fa	Broadcast	ARP	60	Who has 10.0.1.121? Tell 10.0.10.183
11949	109.382523	Dell_b3:af:fa	Broadcast	ARP	60	Who has 10.0.24.68? Tell 10.0.10.183
11950	109.384037	Dell_99:b8:a8	Broadcast	ARP	60	Who has 10.0.1.102? Tell 10.0.24.36
11952	109.414497	Ibm_23:d8:2a	Broadcast	ARP	60	Who has 10.0.24.71? Tell 10.0.0.9
11954	109.424106	Dell_98:7f:7e	Broadcast	ARP	60	Who has 169.254.169.254? Tell 10.0.24.38
11955	109.434413	Dell_00:74:ff	Broadcast	ARP	60	Who has 10.0.4.239? Tell 10.0.4.143
11960	109.477249	RealtekS_36:05:c6	Broadcast	ARP	60	Who has 10.0.8.83? Tell 10.0.8.23
11962	109.525103	Dell_98:f2:a7	Broadcast	ARP	60	Who has 10.0.1.160? Tell 10.0.24.40
11968	109.553915	Sophos_07:36:e6	Broadcast	ARP	60	Who has 192.168.0.104? Tell 192.168.0.5
11974	109.621347	Dell_00:77:85	Broadcast	ARP	60	Who has 10.0.1.160? Tell 10.0.7.126
11975	109.635631	Dell_99:02:60	Broadcast	ARP	60	Who has 10.0.1.171? Tell 10.0.24.46

```
> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3
> Ethernet II, Src: Dell_98:7f:a3 (b0:83:fe:98:7f:a3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff b0 83  fe 98 7f a3 08 06 00 01   ········ ········
0010  08 00 06 04 00 01 b0 83  fe 98 7f a3 0a 00 18 0b   ········ ········
0020  00 00 00 00 00 00 0a 00  18 36 00 00 00 00 00 00   ········ ·6······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Conclusion:

- Promiscuous mode is often used to monitor network activity and to diagnose connectivity issues. It is sometimes given to a network snoop server that captures and saves all packets for analysis, for example, to monitor network usage.
- However, due to its ability to access all network traffic on a segment, this mode is considered unsafe. For example, in a system with multiple virtual machines, promiscuous mode makes it possible for every host to see all network packets destined for all other VMs on that system, not just packets destined for their VMs.