

Group 9F

Authors :

Praveen Kumar Pendyala - 2919474

Shrikanth Diwakar - 2492658

Ankush Chikhale - 2973449

Task 1.1: Is the network traffic in plaintext? Can you look into every packet which is sent through the network?

The network traffic is in plaintext. However, we can see only the broadcast traffic and the packets intended for us. Under normal circumstances, we cannot see every packet which is sent through the network.

Task 2.1: What is ARP spoofing? Describe the attack and the impact of such an attack on the network topology. What can an attacker achieve by spoofing a MAC-address of another network client?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate device on the network.

Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. The attacker could also falsify the network's Default Gateway address and thus gain access to all traffic flowing through the network.

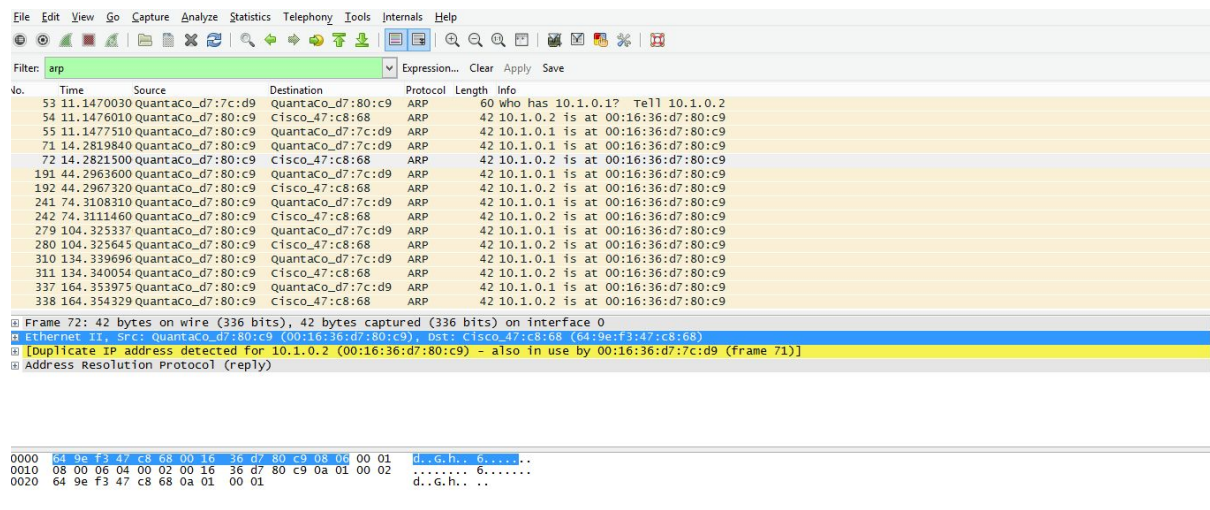
ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. A wide range of attacks such as, not limited to, Denial-of-service, Man-in-the-middle and Session hijacking are possible through ARP spoofing.

Task 2.2: Would it be also possible for an attacker to spoof the MAC-address with an ARP spoofing attack if he is connected to switch 2? Justify your answer.

No, it is not possible to perform an ARP spoofing attack on the client machines connected to switch 1. ARP messages are broadcast messages that are flooded within a broadcast domain. Here, router segregates the LAN and hence ARP request/reply from the attacker connected to switch 2 cannot get past the router 1 to reach the Victim, in this case PC0, who is connected to switch 1.

However, the attacker can still perform an ARP spoofing attack on clients that are within in his broadcast - clients connected, if any, between router 1 and 2.

Task 2.3: Try to perform an ARP spoofing attack in your network environment. Run the tool Cain & Abel on desktop 1 and try to spoof the MAC-address of router 1. Monitor this process with Wireshark from desktop 1. Append a screenshot to your solution on which the ARP spoofing attack is visible and briefly describe the attack operation by explaining the related messages.



No.	Time	Source	Destination	Protocol	Length	Info
53	11.1470030	Quantaco_d7:7c:d9	Quantaco_d7:80:c9	ARP	60	Who has 10.1.0.1? Tell 10.1.0.2
54	11.1476010	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
55	11.1477510	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
71	14.2819840	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
72	14.2821500	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
191	44.2963600	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
192	44.2967320	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
241	74.3108310	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
242	74.3111460	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
279	104.325337	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
280	104.325645	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
310	134.339696	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
311	134.340054	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
337	164.353975	Quantaco_d7:80:c9	Quantaco_d7:7c:d9	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
338	164.354329	Quantaco_d7:80:c9	Cisco_47:c8:68	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9

Frame 72: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Quantaco_d7:80:c9 (00:16:36:d7:80:c9), Dst: Cisco_47:c8:68 (64:9e:f3:47:c8:68)
[Duplicate IP address detected for 10.1.0.2 (00:16:36:d7:80:c9) - also in use by 00:16:36:d7:7c:d9 (frame 71)]
Address Resolution Protocol (Reply)

```
0000  64 9e f3 47 c8 68 00 16 36 d7 80 c9 0a 01 00 02  00:16:36:d7:80:c9 -> 10.1.0.2: ARP Request  
0010  08 00 06 04 00 02 00 16 36 d7 80 c9 0a 01 00 02  00:16:36:d7:80:c9 -> 10.1.0.2: ARP Reply  
0020  64 9e f3 47 c8 68 0a 01 00 01                    d..G.h.. ..
```

ARP Spoofed network traffic. Filtered for ARP packets only.

In the above network log capture screenshot, we can see a warning, in yellow, which states “Duplicate IP address detected for ..” This is basically hinting about ARP poisoning. The attack works by poisoning the ARP tables of the devices in the network.

Here, the attacker is interested in bidirectional traffic of a victim.

1. **For victim’s Incoming traffic:** The attacker poisons the ARP table entries of every device in the network by pointing his MAC address for Victims IP address. We can see that in the highlighted ARP broadcast packet for 10.1.0.2. All traffic addressed to victim would go through attacker.
2. **For victim’s Outgoing traffic:** The attacker poisons the ARP table entries of every device in the network by pointing his MAC address for Gateway IP. We can see that in the highlighted ARP broadcast packet for 10.1.0.1.

Task 2.4: If your attack is successful, contact one of the advisors to login to a service on the server (10.1.2.3) from desktop 0. Then, write down the credentials you were able to obtain via Cain & Abel.

Credentials obtained from logs on the attacker machine.

username : netsec
password : Giflor

Task 2.5: How can an ARP spoofing attack be detected in the network? List some possible indications for such an attack.

Possible ways to detect ARP spoofing.

1. By checking ARP cache to see if there are multiple IPs mapped on to same MAC address. This may however lead to false positives in some cases.
2. By raising an alert whenever an ARP cache entry is updated to a different value.
3. We can check for suspicious messages on Wireshark. As shown in an earlier screenshot, Wireshark warns about duplicate IPs for the same MAC address.

Other possible indications of ARP attack in some special scenarios :

1. Delay in receiving packets.
2. Denial-of-Service from an otherwise trustworthy link/server.

Task 2.6: What kind of countermeasures could protect against an ARP spoofing attack?

Possible countermeasures against ARP spoofing.

1. Static ARP entries : IP-to-MAC mappings in the local ARP cache may be statically entered so that hosts ignore all ARP reply packets.
2. Disabling gratuitous ARP : In this case, an alternative mechanism to update ARP entries should be employed.
3. OS security : There different tools to address ARP spoofing by patching OS at a kernel level. For example : AntiARP for Windows and ArpStar for Linux.

Task 3.1: What is the purpose of the monitor port? Is the result of using such a monitor port comparable with the ARP spoofing attack you performed in the previous task? What kind of device is usually connected to such a monitor port?

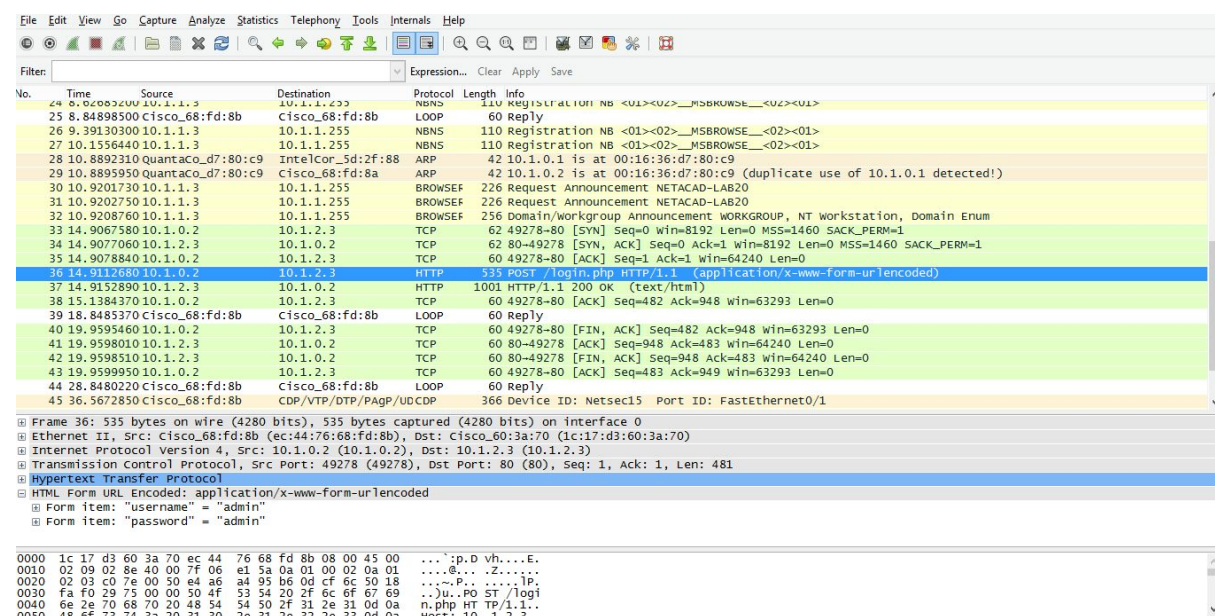
Purpose of a monitor port is to passively observe all the traffic that passes through the switch. Monitor ports are generally used for debugging and Intrusion Detection.

Yes, it is comparable to ARP spoofing (only passive) in the sense that we can sniff all the traffic between router 1 and router 2. However, we cannot modify the traffic, which is possible with ARP spoofing.

Intrusion detection systems, Desktops running tools like Wireshark to capture packets for debugging purpose are some of the devices connected to this port.

Task 3.2, 3.3

In this case, all network traffic is visible.



No.	Time	Source	Destination	Protocol	Length	Info
24	0.000000	10.1.1.1	10.1.1.2	ND	110	Registration NB <01><02>__MSBROWSE__<02><01>
25	8.84898500	Cisco_68:fd:8b	Cisco_68:fd:8b	LOOP	60	Reply
26	9.39130300	10.1.1.3	10.1.1.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
27	10.1556440	10.1.1.3	10.1.1.255	NBNS	110	Registration NB <01><02>__MSBROWSE__<02><01>
28	10.8892310	Quantaco_d7:80:c9	IntelCor_3d:2f:88	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9
29	10.8895950	Quantaco_d7:80:c9	Cisco_68:fd:8a	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9 (duplicate use of 10.1.0.1 detected!)
30	10.9201730	10.1.1.3	10.1.1.255	BROWSE	226	Request Announcement NETACAD-LAB20
31	10.9202750	10.1.1.3	10.1.1.255	BROWSE	226	Request Announcement NETACAD-LAB20
32	10.9208760	10.1.1.3	10.1.1.255	BROWSE	256	Domain/workgroup Announcement WORKGROUP, NT workstation, Domain Enum
33	14.9067580	10.1.0.2	10.1.2.3	TCP	62	49278->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 SACK_PERM=1
34	14.9077060	10.1.2.3	10.1.0.2	TCP	62	80->49278 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1
35	14.9078840	10.1.0.2	10.1.2.3	TCP	60	49278->80 [ACK] Seq=1 Ack=1 win=64240 Len=0
36	14.9112630	10.1.0.2	10.1.2.3	HTTP	535	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
37	14.9152890	10.1.2.3	10.1.0.2	HTTP	1001	HTTP/1.1 200 OK (text/html)
38	15.1384370	10.1.0.2	10.1.2.3	TCP	60	49278->80 [ACK] Seq=482 Ack=948 win=63293 Len=0
39	18.8485370	Cisco_68:fd:8b	Cisco_68:fd:8b	LOOP	60	Reply
40	19.9595460	10.1.0.2	10.1.2.3	TCP	60	49278->80 [FIN, ACK] Seq=482 Ack=948 win=63293 Len=0
41	19.9598010	10.1.2.3	10.1.0.2	TCP	60	80->49278 [ACK] Seq=948 Ack=483 win=64240 Len=0
42	19.9598510	10.1.2.3	10.1.0.2	TCP	60	80->49278 [FIN, ACK] Seq=948 Ack=483 win=64240 Len=0
43	19.9599950	10.1.0.2	10.1.2.3	TCP	60	49278->80 [ACK] Seq=483 Ack=949 win=63293 Len=0
44	28.8480220	Cisco_68:fd:8b	Cisco_68:fd:8b	LOOP	60	Reply
45	36.5672850	Cisco_68:fd:8b	Cisco_68:fd:8b	CDP/VTP/DTP/PagP/UDCDP	366	Device ID: NetSec15 Port ID: FastEthernet0/1

Frame 36: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
Ethernet II, Src: Cisco_68:fd:8b (ec:44:76:68:fd:8b), Dst: Cisco_60:3a:70 (1c:17:d3:60:3a:70)
Internet Protocol Version 4, Src: 10.1.0.2 (10.1.0.2), Dst: 10.1.2.3 (10.1.2.3)
Transmission Control Protocol, Src Port: 49278 (49278), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 481
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "username" = "admin"
Form item: "password" = "admin"

0000 1c 17 d3 60 3a 70 ec 44 76 68 fd 8b 08 00 45 00 ...:p.D vh....E.
0010 02 09 02 8e 40 00 7f 06 e1 5a 0a 01 00 02 0a 01 ...@...:Z....
0020 02 03 c0 7e 00 50 e4 a6 a4 95 b6 0d cf 6c 50 18 ...P...TP.
0030 fa f0 29 75 00 00 50 4f 53 34 20 2f 6c 6f 67 69 ...u..PO ST /logi
0040 6e 26 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a n.php HT TP/1..
0050 48 6f 22 74 25 20 21 20 2a 21 2a 22 2a 22 0d 0a host: 10.1.2.3

Wireshark log as seen from the Monitor port

Task 4.1: Save the monitored traffic and compare it to the one captured in Task 3.3. What kind of information is still in plain text and which information is encrypted?

We see that Ethernet and IP headers are still in plain text.

However, IP payload is encrypted - this includes all TCP headers, except IP values, and TCP payload data. We can only infer information such as the number of messages that are being exchanged between two IP addresses.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Cisco_47:c8:68	Cisco_27:ab:83	LOOP	60	Reply
2	4.72153500	QuantaCo_d7:7c:d9	Cisco_48:b3:e8	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
3	4.72187600	QuantaCo_d7:80:c9	QuantaCo_d7:7a:f3	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9 (duplicate use of 10.1.0.2 detected!)
4	10.0002970	Cisco_47:c8:68	Cisco_47:c8:68	LOOP	60	Reply
5	20.0972410	Cisco_47:c8:68	Cisco_47:c8:68	LOOP	60	Reply
6	28.6394050	10.1.1.1	10.1.1.2	ESP	118	ESP (SPI=0x1cef3f50)
7	28.6400910	10.1.1.2	10.1.1.1	ESP	118	ESP (SPI=0x113860eb)
8	28.6406110	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0x1cef3f50)
9	28.6410000	10.1.1.1	10.1.1.2	ESP	718	ESP (SPI=0x1cef3f50)
10	28.6433240	10.1.1.2	10.1.1.1	ESP	534	ESP (SPI=0x113860eb)
11	28.6469050	10.1.1.1	10.1.1.2	ESP	718	ESP (SPI=0x1cef3f50)
12	28.6493400	10.1.1.2	10.1.1.1	ESP	918	ESP (SPI=0x113860eb)
13	28.7849280	Cisco_47:c8:68	Cisco_47:c8:68	CDP/VTP/DTP/PagP/UDCDP	371	Device ID: router1 Port ID: GigabitEthernet0/1
14	28.8486450	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0x1cef3f50)
15	30.0970120	Cisco_47:c8:68	Cisco_47:c8:68	LOOP	60	Reply
16	34.1590560	10.1.1.2	10.1.1.1	ESP	110	ESP (SPI=0x113860eb)
17	34.1596120	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0x1cef3f50)
18	34.7360640	QuantaCo_d7:80:c9	Cisco_27:ab:83	ARP	42	10.1.0.2 is at 00:16:36:d7:80:c9
19	34.7362040	QuantaCo_d7:80:c9	QuantaCo_d7:7a:f3	ARP	42	10.1.0.1 is at 00:16:36:d7:80:c9 (duplicate use of 10.1.0.2 detected!)
20	36.8883310	QuantaCo_d7:80:c9	Broadcast	ARP	42	who has 10.1.1.1? Tell 10.1.1.3
21	36.8883670	QuantaCo_d7:80:c9	Broadcast	ARP	42	who has 192.168.100.1? Tell 10.1.1.3
22	38.6543590	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0x1cef3f50)

Frame 10: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
 Ethernet II, Src: Cisco_48:d5:18 (64:9e:f3:48:d5:18), Dst: Cisco_47:c8:68 (64:9e:f3:47:c8:68)
 Internet Protocol Version 4, Src: 10.1.1.2 (10.1.1.2), Dst: 10.1.1.1 (10.1.1.1)
 Encapsulating Security Payload

0000 64 9e f3 47 c8 68 64 9e f3 48 d5 18 08 00 45 00 d..G..hd..H....E.
 0010 02 08 00 12 40 00 ff 32 63 ad 0a 01 01 02 0a 01 ...@...2 C.....
 0020 01 01 11 38 60 eb 00 00 00 09 0c 95 ef 94 32 06 ...8'... ..2..
 0030 75 36 ef ff e0 b6 82 7a 9e cf 9e f8 38 0d 41 1e u6.....28.A.
 0040 38 4d 8a e4 ef f4 0c 82 c5 fd e6 09 f6 63 a7 25 8M.....+...C.%
 0050 f5 76 2b 50 17 b6 77 d5 7c 7a b3 46 e6 1c 71 67 B.V...w 8'f'lk

Wireshark log of IPsec traffic encrypted using ESP

Task 4.2: According to Task 4.1 some information is still in plain text and can be monitored by an attacker. Why is it not possible to encrypt this information?

Since we are using ESP protocol in tunnel mode, some part of the packet such as Ethernet and IP headers are not encrypted. This cannot be encrypted to be able to route the packet to the destination. All the intermediate network devices will lookup IP-MAC pair present in the header to route the packet to destination.

Task 4.3: Could IPsec be combined with security mechanisms on other layers? What would be advantages and disadvantages?

Yes. IPsec can be transparently combined with the security mechanisms on layers above it. For example IPsec can be using in conjugation with the Transport layer security protocols like SSH or TLS.

Advantages:

This allows the protection of the otherwise unprotected header fields of the higher layers. It also offers additional security guarantees in both the layers. In case of SSL with IPsec, security guarantees are provided at both Transport and Network layer. All header fields of the SSL protocol will be encrypted by IPsec.

Disadvantages:

Computational and temporal overhead in enforcing security on different layers. Redundant Encryption and Hashing of the same application data at different layers. The redundant work has to be performed both at server and client end.