



ECOLE
POLYTECHNIQUE
DE BRUXELLES

IRELE - MA1 Electrical Engineering

ELEC-H417

Report Lab 5

Certificate Authority and NAT

Authors :

Amaury ARICO

Alexis BOLLENGIER

Emmeran COLOT

Sefa GÖNEN

Professor :

Jean-Michel DRICOT

Assistant :

Navid LADNER

Academic year :

2024 - 2025

Contents

0 Mission 0 - Certificate Authority	1
0.1 Question - Authentication method between PC1 and PC2 before CA	1
0.2 Question - Importance of clock generation in the CA server	1
0.3 Question - Certificate	2
1 Mission 1 - IPsec & VPN (again)	3
1.1 Question - Diffie-Hellman	3
2 Mission 2 - NAT	5
2.1 Question - What is a NAT	5
2.2 Question - Ping?	5
2.3 Question - Usage of NAT	7

Mission 0 - Certificate Authority

0.1 Question - Authentication method between PC1 and PC2 before CA

Authentication method between PC1 and PC2 before CA

Explain the authentication method used in the previous lab. On what assumption does this method works ? Why would a certificate be necessary ? How would the authentication procedure work ?

In the previous lab, we used the **Pre-Shared Key Authentication** method : a **secret key** is **shared** between PC1 and PC2 and is used to authenticate both parties before establishing connection. This method works on the assumption that this key is *kept secret* and *shared in a secure way* but more importantly that PC1 and PC2 **agreed on the secret key** (so they already met before).

In the case that a connection between two PCs that **never met**¹ must be established, the *private/public key* cryptography is used. In this approach, a certificate is necessary to prove that the public key is actually owned by the right PC. The authentication procedure would be then based on the certificates : the public key of one entity is encrypted within the certificate. Another entity can have this public key if it decrypts the certificate using the **public key of the certificate authority** (or CA). By trusting the CA, the authentication is validated and the public key can be used to establish connection. This method is based on trust between the receiver/emitter and the CA.

0.2 Question - Importance of clock generation in the CA server

Importance of clock generation in the CA server

Explain the importance of the clock set up in the router.

Every certificate has an **expiration date**. It is important to set up the clock in the router to be able to check that a certificate isn't expired. The figure 1 shows the expiration date of the CA's self-signed certificate. Having a *local* time on the router different from the one on the other devices of the network could lead to it considering an outdated certificate valid or a valid one out of date, which are situations to avoid.

¹so they didn't agree on a secret shared key before they try to contact each other on an untrusted network

```

R1#show crypto pki server
Certificate Server CA_LABS:
  Status: enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name: CN=CA_LABS
  CA cert fingerprint: 0FA73EA0 35A45CE5 CF855728 F9A99569
  Granting mode is: auto
  Last certificate issued serial number: 0x1
  CA certificate expiration timer: 00:01:35 UTC Feb 28 2005
  CRL NextUpdate timer: 06:01:35 UTC Mar 1 2002
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage

```

Figure 1: Show crypto pki server command result for CA router

0.3 Question - Certificate

Certificate

From the router perspective, will you need to accept the certificate ? Capture the certificate exchange in Wireshark.

From the router perspective, we will need to accept or refuse the certificate depending on the authentication of the CA. In fact, the crypto pki authenticate TRUSTPOINT_CA_LABS command is used by the router to authenticate the CA : the CA provides the router its self-signed certificate (which contains the public key of the CA). Once the CA has been authenticated, the router can enroll for certificates from the CA. The figure 2 shows the certificate exchange.

No.	Time	Source	Destination	Protocol	Length	Info
62	148.812839	10.0.22.2	10.0.22.22	TCP	60	14274 → 80 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
63	148.823287	10.0.22.22	10.0.22.2	TCP	60	80 → 14274 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
64	148.833682	10.0.22.2	10.0.22.22	TCP	60	14274 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
65	148.833742	10.0.22.2	10.0.22.22	HTTP	199	GET /cgi-bin/pkiclient.exe?operation=GetCACaps&message=TRUSTPOINT_CA_LABS HTTP/1.0
66	148.844813	10.0.22.22	10.0.22.2	TCP	310	80 → 14274 [ACK] Seq=1 Ack=146 Win=3983 Len=256 [TCP PDU reassembled in 67]
67	148.855045	10.0.22.22	10.0.22.2	HTTP	98	HTTP/1.1 200 OK (application/x-pki-message)
68	148.865880	10.0.22.2	10.0.22.22	TCP	60	14274 → 80 [ACK] Seq=146 Ack=302 Win=7744 Len=0
69	148.865985	10.0.22.2	10.0.22.22	TCP	60	14274 → 80 [FIN, PSH, ACK] Seq=146 Ack=302 Win=7700 Len=0
70	148.875969	10.0.22.22	10.0.22.2	TCP	60	80 → 14274 [ACK] Seq=302 Ack=147 Win=3983 Len=0
71	148.922047	10.0.22.2	10.0.22.22	TCP	60	30947 → 80 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
72	148.929873	10.0.22.22	10.0.22.2	TCP	60	80 → 30947 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
73	148.932345	10.0.22.2	10.0.22.22	TCP	60	30947 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
74	148.932379	10.0.22.22	10.0.22.22	TCP	1514	30947 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=1460 [TCP PDU reassembled in 76]
75	148.940147	10.0.22.22	10.0.22.2	TCP	60	80 → 30947 [ACK] Seq=1 Ack=1461 Win=4128 Len=0
76	149.993624	10.0.22.2	10.0.22.22	HTTP	853	GET /cgi-bin/pkiclient.exe?operation=PKIOperation&message=IIIF3AYZKoZIHvCMAQcCoIIFzTCCBckCAQExDjAMBgghkiG9w0CBQU
77	150.001241	10.0.22.22	10.0.22.2	TCP	310	80 → 30947 [ACK] Seq=1 Ack=2260 Win=3329 Len=256 [TCP PDU reassembled in 81]
78	150.052990	10.0.22.22	10.0.22.2	TCP	310	[TCP Retransmission] 80 → 30947 [ACK] Seq=1 Ack=2260 Win=3329 Len=256
79	150.056985	10.0.22.2	10.0.22.22	TCP	60	30947 → 80 [ACK] Seq=2260 Ack=257 Win=7744 Len=0
80	150.083592	10.0.22.22	10.0.22.2	TCP	91	80 → 30947 [PSH, ACK] Seq=257 Ack=2260 Win=3329 Len=37 [TCP PDU reassembled in 81]
81	150.103946	10.0.22.22	10.0.22.2	HTTP	1339	HTTP/1.1 200 OK (application/x-pki-message)
82	150.108119	10.0.22.22	10.0.22.2	TCP	60	30947 → 80 [ACK] Seq=2260 Ack=1580 Win=7707 Len=0
83	150.108141	10.0.22.22	10.0.22.2	TCP	60	30947 → 80 [FIN, PSH, ACK] Seq=2260 Ack=1580 Win=6422 Len=0
84	150.114630	10.0.22.22	10.0.22.2	TCP	60	80 → 30947 [ACK] Seq=1580 Ack=2261 Win=3329 Len=0

Frame 77: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface -, id 0	0000	c4 02 0b 69 00 10 c4 06 07 6b 00 01 08 00 45 00	...i...k...E
Ethernet II, Src: c4:06:07:6b:00:01 (c4:06:07:6b:00:01), Dst: c4:02:0b:69:00:10 (c4:02:0b:69:00:10)	0010	01 28 71 2a 00 00 ff 06 09 8e 0a 00 16 16 0a 00	...(q*.....
Internet Protocol Version 4, Src: 10.0.22.22, Dst: 10.0.22.2	0020	16 02 00 50 78 e3 a2 08 c9 98 51 46 92 43 50 10	...Px...QP CP
Transmission Control Protocol, Src Port: 80, Dst Port: 30947, Seq: 1, Ack: 2260, Len: 256	0030	0d 01 ce f4 00 00 48 54 54 50 2f 31 2e 31 20 32	...HT TP/1.1 2
	0040	30 30 20 4f 4b 0d 0e 44 61 74 65 3a 20 46 72 69	00 OK..Date: Fri
	0050	2c 20 30 31 20 4d 61 72 20 32 30 30 32 20 30 30	, 01 Mar 2002 00
	0060	2a 31 34 3a 30 35 20 47 4d 54 0d 0a 53 65 72 76	114:05 G HT- Serv
	0070	65 72 3a 20 63 69 73 63 6f 2d 49 4f 53 0d 0a 43	er: cisc o:IOS: C
	0080	6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70	otent-T ype: app
	0090	6c 69 63 61 74 69 6f 6e 2f 78 2d 70 6b 69 2d 6d	lication /x-pki-m
	00a0	65 73 73 61 67 65 0d 0a 45 78 70 69 72 65 73 3a	essage...Expires:
	00b0	20 46 72 69 2c 20 30 31 20 4d 61 72 20 32 30 30	Fri, 01 Mar 200

Figure 2: Wireshark capture between CA (10.0.22.22) and Router2 (10.0.22.2) - crypto pki enroll TRUSTPOINT_CA_LABS command result

Mission 1 - IPsec & VPN (again)

1.1 Question - Diffie-Hellman

Diffie-Hellman

Explain how a DH key exchange protocol works. Show the packets used for the protocol using Wireshark.

The **DH** (Diffie-Hellman) **key exchange protocol** is a protocol used for *securely generating a symmetric cryptographic key over a public channel*¹ and works as following :

- Both entities agree on public parameters (numbers) that don't have to be kept secret.
- They combine their private key with the public parameters, creating public keys.
- Both entities exchange these public keys with each other using the public channel.
- They recombine their private key with the received public key.
- The result is a secret key that both entities possess and wasn't shared at any point in the public channel.

The figures 1.1 and 1.2 show the packets used for the protocol.

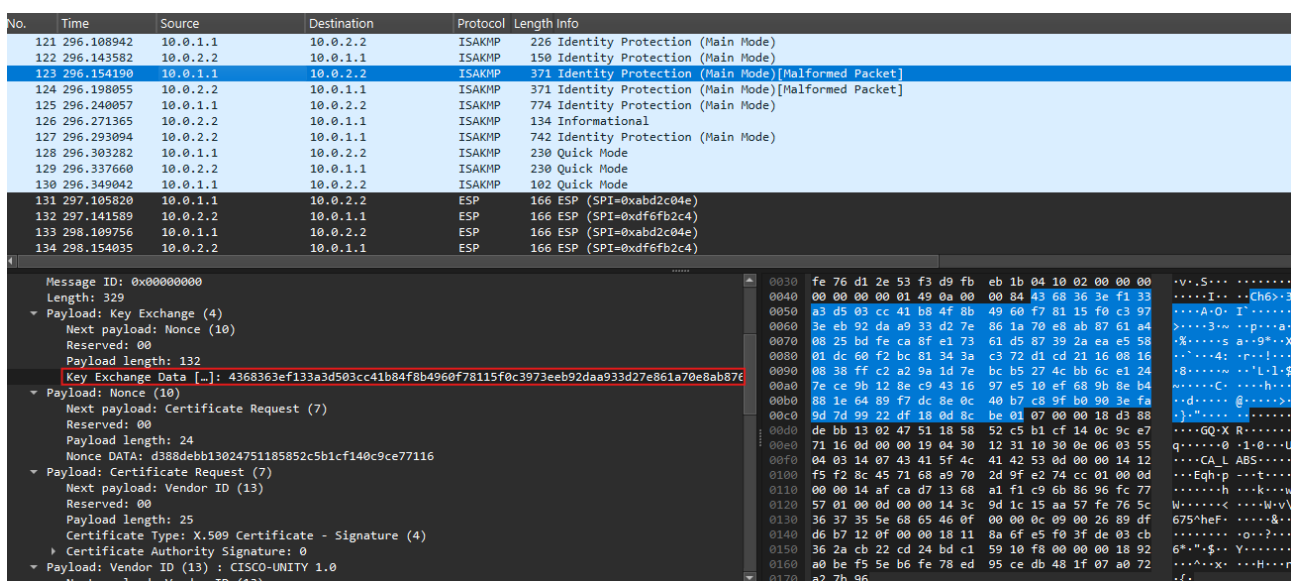


Figure 1.1: Wireshark capture between Router1 (10.0.1.1) and Internet - ping from Linux1 to Linux2 command result. Red frame shows the key exchange data from Router1 to Router2 (10.0.1.1)

¹Source: https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

No.	Time	Source	Destination	Protocol	Length	Info
121	296.108942	10.0.1.1	10.0.2.2	ISAKMP	226	Identity Protection (Main Mode)
122	296.143582	10.0.2.2	10.0.1.1	ISAKMP	150	Identity Protection (Main Mode)
123	296.154190	10.0.1.1	10.0.2.2	ISAKMP	371	Identity Protection (Main Mode)[Malformed Packet]
124	296.198055	10.0.2.2	10.0.1.1	ISAKMP	371	Identity Protection (Main Mode)[Malformed Packet]
125	296.240057	10.0.1.1	10.0.2.2	ISAKMP	774	Identity Protection (Main Mode)
126	296.271365	10.0.2.2	10.0.1.1	ISAKMP	134	Informational
127	296.293094	10.0.2.2	10.0.1.1	ISAKMP	742	Identity Protection (Main Mode)
128	296.303282	10.0.1.1	10.0.2.2	ISAKMP	230	Quick Mode
129	296.337660	10.0.2.2	10.0.1.1	ISAKMP	230	Quick Mode
130	296.349042	10.0.1.1	10.0.2.2	ISAKMP	102	Quick Mode
131	297.105820	10.0.1.1	10.0.2.2	ESP	166	ESP (SPI=0xabd2c04e)
132	297.141589	10.0.2.2	10.0.1.1	ESP	166	ESP (SPI=0xdf6fb2c4)
133	298.109756	10.0.1.1	10.0.2.2	ESP	166	ESP (SPI=0xabd2c04e)
134	298.154035	10.0.2.2	10.0.1.1	ESP	166	ESP (SPI=0xdf6fb2c4)

Message ID: 0x00000000	0030	fe 76 d1 2e 53 f3 d9 fb eb 1b 04 10 02 00 00 00	-v..S.....
Length: 329	0040	00 00 00 00 01 49 0a 00 00 84 61 d4 31 09 3b e3I...a-1;.
▼ Payload: Key Exchange (4)	0050	52 b5 b8 d2 37 77 c5 71 4c 9b b0 17 3a d3 50 e1	R...7w;q L...:P.
Next payload: Nonce (10)	0060	6b 5a 89 81 93 0e ff 06 eb e3 dc 86 4a 24 5e b6	kZ.....:S^.
Reserved: 00	0070	f1 ed 67 ec e9 70 cd 31 29 83 39 2d 50 24 7a a5	..B..p-1).9-P\$.
▼ Payload length: 132	0080	8a 3d d3 8f b7 56 cc c6 11 82 b9 5d 2b 6f 2a 50	...+V...]+o+P
Key Exchange Data [-]: 61d431093be352b5b8d23777c5714c9bb0173ad350e16b5a8981938eff06ebe3dc864a245	0090	17 4d 59 1d e1 be ca b4 c5 10 aa 04 3a 9e 73 1b	-MY.....:@:s.
▼ Payload: Nonce (10)	00a0	0a 35 5f 0e 4f d4 41 57 cc 11 04 5c 2c e2 ff 57	..S..O:AW...:..W
Next payload: Certificate Request (7)	00b0	69 31 69 7e 85 4c e2 79 8f 70 74 08 c2 72 2f 63	iiI...L.y..pt...r/c
Reserved: 00	00c0	fe fc c9 f4 de 9b 87 46 fd 52 07 00 00 18 93 caF..R.....
▼ Payload length: 24	00d0	ec 88 c8 ef 80 3d 97 cd 6f ca 1d 2f 2f fd 2a 92= o...//.*.
Nonce DATA: 93cae88c8ef803d97cd6fca1d2f2ffd2a924185	00e0	41 85 0d 00 00 19 04 30 12 31 10 30 0e 06 03 55	A.....o..1-0...U
▼ Payload: Certificate Request (7)	00f0	04 03 14 07 43 41 5f 4c 41 42 53 0d 00 00 14 12CA_L ABS....
Next payload: Vendor ID (13)	0100	f5 f2 0c 45 71 68 a9 70 2d 9f e2 74 cc 01 00 0d	...Eqh:p...t....
Reserved: 00	0110	00 00 14 af ca d7 13 68 a1 f1 c9 6b 86 96 fc 77h...k...w
▼ Payload length: 25	0120	57 01 00 0d 00 00 14 24 e9 f4 ee d9 fa eb 1b 80	W.....\$
Certificate Type: X.509 Certificate - Signature (4)	0130	b6 83 80 71 82 ab 28 0f 00 00 0c 09 00 26 89 df	...q:(.....&...
Certificate Authority Signature: 0	0140	d6 b7 12 0f 00 00 18 92 a0 be f5 5e b6 fe 78 ed^.....x...
▼ Payload: Vendor ID (13) : CISCO-UNITY 1.0	0150	95 ce db 48 1f 07 a0 72 a2 7b 96 00 00 00 18 11	...H...r..{.....
Next payload: Vendor ID (13)	0160	8a 6f e5 f0 3f de 03 cb 36 2a cb 22 cd 24 bd c1	..o-?-...6*..".\$..
	0170	59 10 f8	Y...

Figure 1.2: Wireshark capture between Router1 (10.0.1.1) and Internet - ping from Linux1 to Linux2 command result. Red frame shows the key exchange data from Router2 (10.0.2.2) to Router1 (10.0.1.1)

2.1 Question - What is a NAT

What is a NAT

Explain in a few words what is a NAT and how it is suppose to work.

NAT or Network Address Translation is a method used to manipulate the IP address of incoming/outgoing packets in a local network : all devices in a local network **share just one public IPv4 address**. In other words, the NAT changes the IP address of all packets going out of the local network to one source NAT IP address. The port associated to each packet however depends on the source IP and port. The mapping (public IP + public port \Leftrightarrow local IP + port) is stored in a table, the NAT table, which is used to forward the incoming packets to the intended receiver.

Incoming packets use the source NAT IP address and the new port number as destination address and destination port number. Then the NAT uses its table to translate this port number to the right local IP address and port number.

2.2 Question - Ping ?

Ping ?

Try to ping using the following commands:

1. PC3 port 8080 to PC6 port 80
2. PC3 port 80 to PC6 port 80
3. PC4 port 80 to PC6 port 80
4. PC6 port 80 to PC3 port 80
5. PC6 port 80 to PC3 port 1111
6. PC6 port 80 to Router3 port 1111
7. PC6 port 80 to Router3 port 2222

What do you observe ? Explain the results you see on the terminal and on Wireshark.

1. There is nothing unusual, the packets are showing PC3's IP address, see figure 2.1

2. In this case, the NAT translates the IP of PC3. That's because we are sending the ping requests with source port 80 of PC3 : we've set up the NAT to translate everything coming from PC3 (192.168.3.3) with port number 80 to 10.0.3.3:1111 NAT IP address and port number, see figure 2.2.
3. Again, the NAT translates the IP and port number of the packets to 10.0.3.3:2222 (we've set up it like that in our table).
4. We get a timeout. PC6 expects a response from PC3 (192.168.3.3:80) but it is the translated packet that it receives (10.0.3.3:1111), see figure 2.3.
5. Because we didn't set the port 1111 of PC3 to be translated by the NAT, we get an usual ping command result.
6. This time, we resolve the timeout we got at the 4th point. The ping requests arrive at the router 3 (10.0.3.3:1111) but because of the NAT, the packets are redirected to PC3. So rather than router 3 responding to the ping, we have in fact packets going from router 3 to PC3. This case is similar to the second point.
7. This exactly the same case as before but this time, it is PC4 that responds to the ping requests because in the NAT table, the port 2222 is mapped to PC4 (192.168.3.4:80).

No.	Time	Source	Destination	Protocol	Length	Info
471	1101.062569	192.168.3.3	192.168.4.6	UDP	98	8880 → 80 Len=56
472	1101.114648	192.168.4.6	192.168.3.3	UDP	98	80 → 8880 Len=56
473	1102.124215	192.168.3.3	192.168.4.6	UDP	98	8880 → 80 Len=56
474	1102.151786	192.168.4.6	192.168.3.3	UDP	98	80 → 8880 Len=56
475	1103.163161	192.168.3.3	192.168.4.6	UDP	98	8880 → 80 Len=56
476	1103.195369	192.168.4.6	192.168.3.3	UDP	98	80 → 8880 Len=56
477	1104.218638	192.168.3.3	192.168.4.6	UDP	98	8880 → 80 Len=56
478	1104.259351	192.168.4.6	192.168.3.3	UDP	98	80 → 8880 Len=56
479	1105.276701	192.168.3.3	192.168.4.6	UDP	98	8880 → 80 Len=56
480	1105.302119	192.168.4.6	192.168.3.3	UDP	98	80 → 8880 Len=56

Frame 471: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 Ethernet II, Src: c4:03:0d:84:00:01 (c4:03:0d:84:00:01), Dst: c4:04:0d:ae:00:10 (c4:04:0d:ae:00:10)
 Internet Protocol Version 4, Src: 192.168.3.3, Dst: 192.168.4.6
 User Datagram Protocol, Src Port: 8880, Dst Port: 80
 Data (56 bytes)

Figure 2.1: Wireshark capture between Router3 (10.0.3.3) and Internet - ping from PC3 port 8080 to PC6 port 80 result

No.	Time	Source	Destination	Protocol	Length	Info
522	1241.668118	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
523	1241.720985	192.168.4.6	10.0.3.3	UDP	98	80 → 1111 Len=56
524	1242.740279	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
525	1242.769412	192.168.4.6	10.0.3.3	UDP	98	80 → 1111 Len=56
526	1243.782678	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
527	1243.809312	192.168.4.6	10.0.3.3	UDP	98	80 → 1111 Len=56
528	1244.824993	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
529	1244.867591	192.168.4.6	10.0.3.3	UDP	98	80 → 1111 Len=56
530	1245.885368	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
531	1245.926751	192.168.4.6	10.0.3.3	UDP	98	80 → 1111 Len=56

Frame 522: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 Ethernet II, Src: c4:03:0d:84:00:01 (c4:03:0d:84:00:01), Dst: c4:04:0d:ae:00:10 (c4:04:0d:ae:00:10)
 Internet Protocol Version 4, Src: 10.0.3.3, Dst: 192.168.4.6
 User Datagram Protocol, Src Port: 1111, Dst Port: 80
 Data (56 bytes)

Figure 2.2: Wireshark capture between Router3 (10.0.3.3) and Internet - ping from PC3 port 80 to PC6 port 80 result. The NAT translates 192.168.3.3:80 to 10.0.3.3:1111

No.	Time	Source	Destination	Protocol	Length	Info
813	2223.312383	192.168.4.6	192.168.3.3	UDP	98	80 → 80 Len=56
814	2223.334182	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
815	2224.244091				126	<Ignored>
816	2225.315465	192.168.4.6	192.168.3.3	UDP	98	80 → 80 Len=56
817	2225.337520	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
818	2227.315311	192.168.4.6	192.168.3.3	UDP	98	80 → 80 Len=56
819	2227.335893	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56
820	2229.320125	192.168.4.6	192.168.3.3	UDP	98	80 → 80 Len=56
821	2229.342435	10.0.3.3	192.168.4.6	UDP	98	1111 → 80 Len=56

Frame 813: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 Ethernet II, Src: c4:04:0d:ae:00:10 (c4:04:0d:ae:00:10), Dst: c4:03:0d:84:00:01 (c4:03:0d:84:00:01)
 Internet Protocol Version 4, Src: 192.168.4.6, Dst: 192.168.3.3
 User Datagram Protocol, Src Port: 80, Dst Port: 80
 Data (56 bytes)

Figure 2.3: Wireshark capture between Router3 (10.0.3.3) and Internet - ping from PC6 port 80 to PC3 port 80 result

2.3 Question - Usage of NAT

Usage of NAT

Explain how a NAT could be useful in terms of security. Develop some advantages and disadvantages.

NAT offers some security benefits. It masks private/local IP addresses, preventing external access. NAT also helps reducing the number of IPv4 addresses (limited number of possible IPv4 Addresses) and with NAT, it is possible to change addresses in the local network without notifying the outside world as well as changing the ISP without changing addresses of the devices in the local network.

However, NAT does have its disadvantages. First, in order to get a packet from some server, you must connect to it at least once. Also, there is a limited amount of ports (64k ports) and the table needs to be cleaned. Moreover, the NAT adds a bottleneck (all traffic goes through the NAT) and a layer of complexity, which can make troubleshooting more difficult. Some protocols, such as Voice over IP (VoIP) or File Transfer Protocol (FTP), may encounter problems with NAT, requiring adjustments.