UNIVERSITAT DE LLEIDA
Escola Politècnica Superior
Grau en Enginyeria Informàtica
XARXES

Anàlisi de la xarxa mitjançant l'analitzador de protocols de xarxa Wireshark

Sergi Simón Balcells
21040111X
GM3

Professorat : E. Guitart, C. Mateu
Data : Diumenge 19 de Maig

Índex

Llista d'imatges

Llista de Taules

1 Introducció

2 Caractarístiques de la xarxa

2.1 Tipus d'adreçament a la capa de xarxa

Per a trobar el tipus d'adreçament a la xarxa, s'ha mirat els paquets tipus ARP per a observar diferents direccions IP de la xarxa.

Observant les diferents direccions que es mouen dins de la xarxa, podem extreure que les direccions de la xarxa són 172.16.x.x, sent les x valors entre 0 i 255, és a dir, l'adreça de xarxa és 172.16.0.0/16 i per tant és de **classe B**.

2.2 Adreça de xarxa

Com s'ha extret en l'anterior secció, la adreça de xarxa és 172.16.0.0.

2.3 Adreça de broadcast

Sabent l'adreça de xarxa, podem concloure que l'adreça de broadcast és 172.16.255.255, ja que aquesta és l'última adreça disponible de tota la xarxa, és a dir, la part del host de l'adreça a valor actiu a tots els bits. Inclús amb aquesta informació, per confirmar que no hi hagi hagut cap error, s'ha procedit a mirar l'adreça de broadcast en els paquets tipus:

```
!arp && eth.dst == ff:ff:ff:ff:ff:ff
```

Els paquets d'aquest tipus mostren com a direcció IP 172.16.255.255 per destí, es pot confirmar la informació extreta en aquest apartat.

2.4 Porta d'enllaç

S'ha vist en la xarxa que s'empra el protocol DHCP, pel que, primerament es busca aquels paquests que siguin DHCP ACK:

```
bootp.option.dhcp == 5
```

En aquest protocol i en aquest tipus de paquet, es pot trobar la informàció referent al router, dins de Bootstrap Protocol (ACK), en opcions de router. En aquest camp s'especifíca que l'adreça és 172.16.20.1.

3 Anàlisi de nivell de enllaç i xarxa

3.1 Protocols encapsulats en les trames de nivell 2

Al llarg de tota la trama, es poden veure 2 protocols de nivell 2 de xarxa, **Ethernet II** i **IEEE 802.3 Ethernet**. En les següents subseccions s'explicarà

el tipus d'encapsulament d'aquests

3.1.1 Ethernet II

Aquest tipus de trama s'utilitza en l'àmbit general, i es pot trobar en la majoria de paquets de la captura. La seva estructura segueix la següent:

3.1.2 IEEE 802.3 Ethernet

Aquesta classe s'utilitza en els protocols de LLC. La seva estructuar és la següent:

3.2 Protocols encapsulats en trames de nivell 2

Per a trobar els diferents protocols utilitzats, s'utilitza la eina de *Protocol Hierarchy*, accessible dins del menú d'estadístiques del Wireshark. En aquest menú, podem veure com és divideix els protocols segons els nivells, començant pel nivell físic, i seguint amb Ethernet. Dins d'aquest menú es pot veure els següents tipus de paquets, que són: Logical-Link Control (LLC), Internetwork Packet eXchange (IPX), Internet Protocol Version 6 (IPv6), Internet Protocol Version 4 (IPv4), Address Resolution Protocol (ARP), que s'explicaran a continuació, juntament amb el seu valor de tipus.

- ARP, amb valor 0x0806, s'encarrega de resoldre i mantenir de manera automàtoca la taula d'equivalències entre les adreces MAC i les adreces IP dels nodes o màquines que es comuniquen.
- IPv4, amb valor 0x0800, és el protocol per excelència d'Internet. Serveix per a la identiciació i connexió de nodes.
- IPv6, amb valor 0x86dd, neix com a un protocol per a substituir IPv4, i treure els problemes que sorgeixen amb aquest, com és la falta d'adreces, seguretat i qualitat de servei. Moltes de les seves funcionalitats s'han portat enrere per al protocol de IPv4.
- IPX, amb valor 0x8137, s'utilitza per a transmetre datagrames entre els diferents serviors i els programes de les estacions de treball.
- LLC, sense valor donat que està encapsulat amb IEEE 802.3 Ethernet i aquest no te nombre reservat pel tipus, defineix la forma en què les dades són transferides sobre el medi físic, proporcionant servei a les capes superiors.

3.3 Equips amb adreçament IPX i IPv4

Per aquesta secció, s'ha mirat manualment els equips que utilitzen IPX la seva adreça MAC, i, utilitzant aquesta valor s'ha mirat si hi havia un paquet que amb aquesta MAC que utilitzes IPv4 amb la comanda, substituint l'adreça MAC per aquelles trobades amb l'anterior cerca:

```
(eth.src == 00:00:74:99:b5:0b || eth.dst == 00:00:74:99:b5:0b) && ip
```

En la primera cerca dins dels paquests IPX s'ha trobat aquestes adreces i MAC, com es mostra en la taula 1 Finalment, buscant totes les MACS abans trobades

Adreces IPX	Adreces MAC
00000000.00007499b50b	00:00:74:99:b5:0b
00000000.000074aee28d	00:00:74:ae:e2:8d
00000000.000074b4dbcd	00:00:74:b4:db:cd
00000000.000074d5923f	00:00:74:d5:92:3f
00000000.000074da5833	00:00:74:da:58:33
00000000.000074dab870	00:00:74:da:b8:70
00000000.000074ddfd6c	00:00:74:dd:fd:6c
00000000.000074e03eaf	00:00:74:e0:3e:af
00000000.000074e04ef9	00:00:74:e0:4e:f9
00000000.000074e08d60	00:00:74:e0:8d:60
00000009.00080228befa	00:08:02:28:be:fa

Taula 1: Adreces MAC i IPX d'equips que utilitzen IPX

i eliminant aquelles files que no s'han trobat paquets d'IPv4 en la trama tenim la taula 2.

Adreça MAC	Adreça IPX	Adreça IPv4
00000000.000074da5833	00:00:74:da:58:33	172.16.40.6
00000000.000074ddfd6c	00:00:74:dd:fd:6c	172.16.40.11
00000000.000074e04ef9	00:00:74:e0:4e:f9	172.16.40.4
00000000.000074e08d60	00:00:74:e0:8d:60	172.16.40.3

Taula 2: Taula de adreces IPX que han utilitat protocol IPv4 i ha sigut captat.

3.4 Adreces IPv4 dels nodes que envien paquests IPv6 a ff02::1

En aquesta subsecció s'explicarà com s'ha trobat aquells equips que envien paquets d'IPv6 a tots els nodes de l'enllaç local, es a dir, a ff02::1.

Per a dur a terme aquest propòsit, es mira quins paquets d'IPv6 tenen com

a destí l'adreça ff02::1. Primarement es volia buscar les adreces MAC i veure si aquests utilitzaven algun protocol de xarxa IPv4, però aquest tipus de paquet està encapsulat dins de IPv4 dins d'UDP, per que en un sol pas s'ha trobat els 5 nodes que fan aquest tipus de connexió, que es poden veure a la taula 3.

Adreces IPv6	Adreces IPv4
2001:0:9d38:6ab8:2470:3837:3e6f:f31d	172.16.103.254
2001:0:5ef5:79fb:2cfb:2fe0:3e6f:f31d	172.16.118.198
2001:0:9d38:6ab8:30ba:1553:3e6f:f31d	172.16.104.180
2001:0:9d38:6abd:2455:1c81:3e6f:f31d	172.16.105.251
2001:0:9d38:6ab8:496:259b:3e6f:f31d	172.16.121.59

Taula 3: Taula d'adreces IPv6 i IPv4 d'un mateix node.

3.5 Adreces Multicast

Per a trobar les diferents adreces multicast s'ha utilitzat el filtre:

```
eth.dst[0] & 1 and !eth.dst == ff:ff:ff:ff:ff:ff
```

Ha donat el resultat de la taula 4. S'ha extret les adreces del tipus ff02:1:ff00:0/104, donat que s'utiitza pel mateix protocol. Si es desitja, es pot veure a l'annex la resta de les dades, a la taula 10 A continuació, s'explicarà un per un els proto-

Adreces multicast	Protocols
03:00:00:00:00:01	BROWSER
224.0.0.1	BJNP, ICMP, IGMPv2
224.0.0.251	IGMPv2, IPv4, MDNS
224.0.0.252	LLMNR
ff02::1	ICMPv6, IPv6
ff02::16	ICMPv6
ff02::1:2	DHCPv6
ff02::1:3	LLMNR
ff02::1:ff00:0/104	ICMPv6
ff02::2	ICMPv6
ff02::c	SSDP, UDP
ff02::fb	MDNS

Taula 4: Diferents adreces multicast i els seus protocols

cols que s'han trobat utilitzant aquest tipus de servei:

- BROWSER: aquest protocol és usat pels ordinadors amb el sistema operatiu de Windows per a navegar fàcilment i localitzar els fitxers compartits en una xarxa.

- BJNP: aquest protocol es utilitzat per les impressores Canon amb la finalitat que els ordinadors puguin autodescobrir les impressores connectades a una xarxa.
- ICMP: informa de l'estat i situacons d'error en el funcionament de la xarxa. Amb exepció de l'aplicació Ping, aquest protocol no s'utilitza directament sobre les aplicacions d'usuari.
- IGMPv2: protocol que permet establir grups de multicast en una xarxa d'IPv4.
- IPv4: protocol que permet identificar inequívocament un dispositiu lògic connectat a la xarxa, per així poder connectar nodes.
- MDNS: *Multicast Domain Name Service*, permet resoldre noms de host (i.e.: www.google.com) a adreces IP dins de petites xarxes que no inclouen un servidor DNS. És un servei que requereix zero configuració. Tot i que no va estar dissenyat per a servidors dee DNS propis, pot ser utilitzat amb aquests.
- LLMNR: és un protocol basant en el DNS per a trobar noms de domini en el mateix link local. És inclòs en la majoria de Windows, així com està implementat per systemd en Linux.
- IPv6: protocol que cerca solucionar els problemes de quantitat d'adreces disponibles, qualitat de servei i seguretat per a l'adreçament d'Internet. Algunes de les seves funcionalitats han sigut portades a IPv4.
- ICMPv6: ICMP per a IPv6, és una simplificació de IGMP, ICMP i ARP pel protocol d'IPv6, introduint, a més a més, algunes simplificacions i eliminant missatges obsolets.
- DHCPv6: proporciona una configuració administrada sobre els dispositius d'IPv6, és a dir, entre altres coses, donen una adreça IPv6 als clients que la soliciten.
- SSDP: protocol que serveix per a descobrir serveis dins d'una mateixa xarxa. És un dels protocols utilitzats per ***U****niversal* ***P****lug a****n****d* ***P****lay* (UPnP).
- UDP: protocol per a enviar datagrames. En contraposició a TCP, no garanteix res, més enllà dels paquests rebuts saber en quina aplicació estan mitjançant el port.

3.6 Gràfica de distribució dels protocols de nivell 3

Per a dur a terme aquesta gràfica, s'ha extret les dades de "*Statistics ¿ Protocol Hierearchy*. En aquest menú, hem aconseguit extreure l'informació de la taula 5

Amb aquestes dades, s'ha generat el gràfic 1

Protocol	Nombre de paquets	Percentatge de paquets
LLC	97	0.6%
IPX	91	0.6%
IPv6	550	3.5%
IPv4	5616	35.5%
ARP	9451	59.8%

Taula 5: Taula de protocols de nivell 3

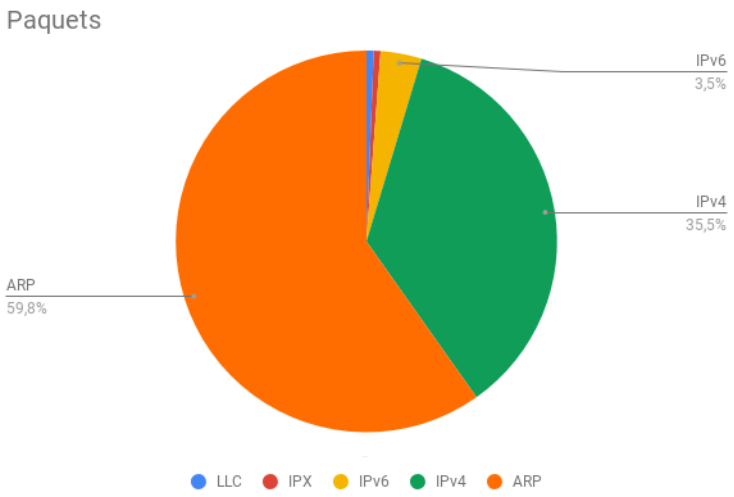

Figura 1: Gràfic de sectors dels protocols de nivell 3

4 Anàlisi nivell de transport

Abans de començar s'ha de desestimar certs paquets i protocols per a dur a terme les diferents qüestions. A continuació, s'exposarà els filtres que s'utilitzaran per a cada un dels punts.

- Pels paquets que tenen com a destí l'adreça de broadcast de nivell 2, s'empraràla comanda:

  `!eth.dst == ff:ff:ff:ff:ff:ff`

- Pels paquets d'IPv6, s'utilitzarà:

  `!ipv6`

- Pels paquets de multicast, s'aplicarà el filtre:

```
!(eth.dst[0] & 1)
```

Que no utilitza la segona clausula donat que el paquets de broadcast ja han estat eliminats.

- Pel protocols ARP, DNS i NTP s'emprarà:

```
!arp and !dns and !ntp
```

Aplicant totes les condicions obtenim el filtre:

```
!(eth.dst[0] & 1) and !arp and !dns and !ntp
and !ipv6 and !eth.dst == ff:ff:ff:ff:ff:ff
```

A causa de que l'adreça de broadcast ethernet té el primer valor a 1, la filtre per a detectar multicast simplifica el filtre fins a tenir:

```
!(eth.dst[0] & 1) and !arp and !dns and !ntp
and !ipv6
```

4.1 Connexions TCP no dutes a terme

S'ha utilitzat el filtre:

```
tcp and tcp.flags.reset == 1
```

Per a veure les connexions que han acabat per resposta del servidor. Per a les altres connexions, s'ha mirat una per una les converses de TCP, veient si aquestes havien finalitzat de forma excepcional o si es podia treure conclusions d'aquests. Per a visualtizar les diferents connexions, s'ha utilitzat la eina *Statistics ¿ Conversations ¿ TCP*. Amb la informació obtinguda s'ha elaborat la taula 6.

S'ha tingut en compte el temps de l'últim SYN enviat i el temps de connexió gravat per a decidir s'ha realment s'havia perdut la connexió o el paquet de resposta no s'ha gravat en la sel·lecció de la trama.

4.2 Connexions TCP completes

En aquesta subsecció, es diran aquelles connexions TCP que han sigut completes i com s'han trobat. Per a fer-ho, s'han subdividit aquelles connexions que són comunicacions HTTP i HTTPS, i la resta de comunicacions.

4.2.1 HTTP i HTTPS

Per a cercar les converses que han tingut alguna connexió TCP, s'ha utilitzat el filtre:

```
tcp.port == 80 or tcp == 443
```

IP origen	Port Origen	IP Destí	Port Destí	Motiu Fallida
172.16.0.112	34640	10.35.12.34	1759	No hi ha hagut resposta per part del destí al SYN
172.16.0.112	60158	10.50.54.87	9876	No hi ha hagut resposta per part del destí al SYN
172.16.0.102	43384	172.0.16.111	1759	No hi ha hagut resposta per part del destí al SYN
84.88.27.7	80	172.16.0.113	42901	S'ha rebut un paquet amb el flag RST
172.16.0.109	33764	172.16.0.113	80	S'ha rebut un paquet amb el flag RST
172.16.0.105	44730	172.16.0.122	80	S'ha rebut un paquet amb el flag RST
172.16.0.106	42542	172.16.0.118	6591	S'ha rebut un paquet amb el flag RST

Taula 6: Connexions TCP fallides

Una vegada utilitzat, s'ha utilitzat la eina per a veure converses del Wireshark, amb la opció de només veure les que estiguin dins del filtre, per a veure quines converses s'han matingut en aquests ports. L'única conversa en HTTPS és la que té per IP origen i destí els valors 172.16.0.112 i 213.175.193.206, per a simplificar la taula 7, s'ha unificat amb una sola taula en haver-se esmentat ja els valors.

4.2.2 Connexions no HTTP i HTTPS

Per a dur a buscar aquestes connexions, s'ha utilitzat el filtre:

```
!(tcp.port == 80 or tcp.port == 443)
```

Utilitzant el mateix procediment d'abans, s'ha emprat la eina de Converses del Wireshark i s'han mirat una per una si les connexions eren completes o no. Amb aquesta premisa s'ha extret l'anàlisi de la taula 8. Per a calcular l'MTU, s'ha afegit 40 bytes al camp proporcionat pel protocol TCP sobre el segment més llarg, a causa de la mida de les capçaleres mínima de les capçaleres TCP i IP (20 bytes cada una).

IP origen	IP destí
172.16.0.109	10.69.4.176
172.16.0.109	91.195.125.127
172.16.0.109	147.91.204.28
172.16.0.109	13.219.28.2
172.16.0.109	94.75.223.121
172.16.0.109	129.177.13.120
172.16.0.109	5.135.162.176
172.16.0.109	178.33.193.139
172.16.0.109	91.210.88.42
172.16.0.109	217.31.202.63
172.16.0.112	209.132.181.16
172.16.0.112	213.175.193.206
172.16.0.112	84.88.27.7

Taula 7: Conversacions completes en HTTP i HTTPS

Origen				Destí			
IP	Port	MTU	Finestra inicial	IP	Port	MTU	Finestra inicial
172.16.0.102	48009	1500	14600	172.16.0.105	9642	1500	14480
172.16.0.104	36664	1500	14600	172.16.0.111	1759	1500	14480
172.16.0.104	45737	1500	14600	172.16.0.125	22	1500	14480
172.16.0.105	52193	1500	14600	172.16.0.108	7856	1500	14480
172.16.0.106	45874	1500	14600	172.16.0.112	22	1500	14480
172.16.0.106	52180	1500	14600	172.16.0.108	7856	1500	14480
172.16.0.106	50316	1500	14600	172.16.0.103	21	1500	14480
172.16.0.106	38368	1500	14600	172.16.0.115	7658	1500	14480
172.16.0.109	49608	1500	14600	172.16.0.108	7856	1500	14480
172.16.0.112	42095	1500	14600	172.16.0.102	21	1500	14480

Taula 8: Conversacions completes no pertanyens a HTTP i HTTPS

4.3 Connexions UDP no dutes a terme

UDP no és un protocol orientat a connexió, pel que dins del protocol costarà saber si alguna connexió UDP no s'ha dut a terme. Però, el protocol ICMP avisa quan algun host, port o destí no ha sigut trobat, donant així una connexió UDP fallida. Utilitzant el filtre:

```
upd and icmp
```

Trobarem els missatges de xarxa produits per aquest tipus de connexió. Però, donat que hi ha molts missatges de *Time to live*, i, a causa de que aquest missatge podria ser tractat per una capa superior, s'ha desestimat tots aquests paquets treient el seu camp amb el filtre:

```
!icmp.type == 11
```

D'aquesta forma, es facilita adquirir les dades amb les quals, s'ha efectuat la taula 9.

Origen		Destí		Motiu
IP	Port	IP	Port	
172.16.0.111	55864	172.16.0.112	1034	Port inabastible
131.206.192.49	35430	172.16.0.113	33504	Port inabastible
130.206.192.49	54863	172.16.0.113	33505	Port inabastible
130.206.192.49	50066	172.16.0.113	33503	Port inabastible
130.206.192.49	41967	172.16.0.113	33507	Port inabastible
130.206.192.49	41722	172.16.0.113	33508	Port inabastible
130.206.192.49	58040	172.16.0.113	33509	Port inabastible

Taula 9: Connexions TCP fallides

5 Conclusions

6 Annex

Adreces multicast
ff02::1:ff16:f8e9
ff02::1:ff3a:5c61
ff02::1:ff4e:9436
ff02::1:ff52:275
ff02::1:ff5f:1802
ff02::1:ff62:ce40
ff02::1:ff74:9938
ff02::1:ff84:f581
ff02::1:ff90:170b
ff02::1:ff92:210f
ff02::1:ff9e:c17f
ff02::1:ffac:b684
ff02::1:ffb5:ecdb
ff02::1:ffbf:a6df
ff02::1:ffc8:6083
ff02::1:ffca:c1b3
ff02::1:ffdb:187
ff02::1:ffe1:112f
ff02::1:ffeb:4add

Taula 10: Adreces multicast de format ff02::1:ff00:0/104