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.