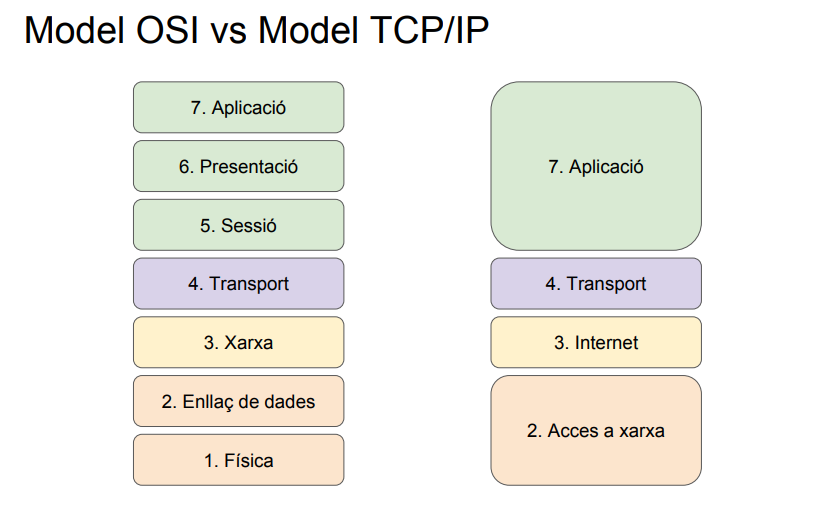
***Model OSI (Open System Interconnection)***

● Esquema utilitzat per explicar la divisió que existeix en les diferents parts de comunicació entre xarxes

● Cada capa representa una caixa negra que processa les dades i les envia cap a la capa inferior quan enviem dades i cap a la capa superior quan les rebem

● D’aquesta forma genera un canal virtual de comunicació entre capes on cada capa utilitza el mateix protocol de comunicació

● Cada capa afegeix o interpreta les capçaleres amb dades extres per comunicar-se amb la seva capa en l’altre computadors



***Capa d’aplicació***

● Defineix els protocols que faran servir les aplicacions

● La informació que s’envia i arriba com un flux de dades (stream)

● Virtualitza una xarxa orientada a connexió

● Alguns exemples de protocols d’aquesta capa són: ○ dns, http, ftp, smtp, ssh telnet, ldap, etc…

***Capa de presentació***

● S’encarrega de donar el format correcte a les dades

● Si és necessari xifra les dades per crear un canal segur de comunicació

● També s’encarrega de comprimir o descomprimir les dades

***Capa de sessió***

● Permet mantenir una sessió entre dos ordinadors oberta, encara que la

connexió es perdi

● Si la connexió cau és aquesta capa la que s’encarrega de recuperar la sessió

anterior

***Capa de transport***

● S’encarrega de transportar les dades d’un punt a l’altre correctament com si fos un flux de dades

● Proporciona un mecanisme per poder tindre múltiples connexions a l’hora i poder distingir cada connexió fent servir el concepte de ports

● Segmenta les dades per enviar-les en paquets que es puguin enviar per la xarxa

● La seva unitat de dades de protocol (PDU) es diu segment o datagrama

● Numera els segments perquè quan arribin al destí pugui ordenar-los correctament

● Si és necessari, afegeix un CRC (Cyclic Redundancy Check)

● Exemple de protocols: TCP i UDP

***Capa de xarxa***

● S’encarrega de transportar les dades entre diferents xarxes

● S’encarrega de fer l’adreçament logic (IP)

● Calcula la millor ruta per enviar les dades entre les diferents xarxes

● El seu PDU es diu paquet

● Exemples protocols: IP, IPX, APPLETALK

***Capa d’enllaç de dades***

● Aquesta capa s’encarrega de la comunicació en la mateixa xarxa o LAN

● Estableix un adreçament fisic (MAC) per cada terminal de la xarxa

● El seu PDU es diu trama

● Segmenta els paquets per enviar-los a través de la xarxa

● Assegura l’ordenació de les trames i la detecció d’errors

● Un exemple de protocol és: ethernet (IEEE 802.3) o WIFI (IEEE 802.11)

● Exemples de protocols: ARP, NDP(IPv6)

***Capa física***

● Envia un flux de bits a través d’un medi

● Garanteix la connexió entre terminals

● Defineix el medi físic pel que viatjara la comunicació

● Defineix les característiques dels materials

***Terminals***

● Client:

○ Dispositiu terminal connectat a la xarxa per un medi físic

● Client Mòbil:

○ Dispositiu terminal connectat a la xarxa per un medi sense fils

● Servidor:

○ Dispositiu que dóna serveis als clients, ex: web, fitxer, correu

***Hub (Concentrador)***

● Dispositiu que connecta diferents terminals

● Opera només a la capa física del model OSI

● Utilitza un sol canal de comunicació

● Pot provocar col·lisions

● És economic

***Switch (Commutador)***

● Dispositiu que connecta diferents terminals

● Opera en la capa 1(física) i 2 (enllaç de dades) del model OSI

● Envia els paquets d’un port a un altre port sense ocupar el

canal d’altres ports

● Filtra comunicacions punt a punt que no interenssen

● Evita col·lisions

● Té un cost més elevat que un HUB

● Permet fer VLAN

***Bridge (Pont)***

● Connecta dues xarxes normalment de diferent topologia

● Opera en la capa 1(física) i 2 (enllaç de dades) del model OSI

● Filtra el tràfic entre xarxes

***Router (Encaminador)***

● Encamina els paquets IP cap a un port on pugui trobar el

destinatari

● Opera en la capa 3 (xarxa) del model OSI

● Filtra el tràfic de broadcast de la capa d’accés a dades

***Tipus de xarxa segons la mida***

● Local area network (LAN)

○ La seva extensió es medeix en metres

○ Son instal·lades en edificis

○ Son matenides per una persona o empresa

○ Permet una connexió interna d’alta velocitat

● Metropolitan area network (MAN)

○ La seva extensió es medeix uns pocs kilometres

○ Son instal·lades en ciutats

○ Son mantenides per ajuntaments o comunitats

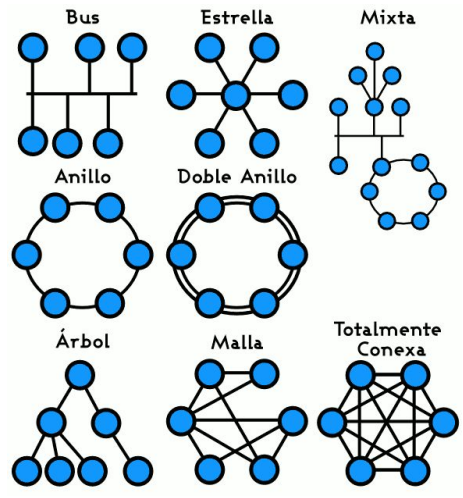
● Wide area network (WAN)

○ La seva extensió es medeix en kilometres

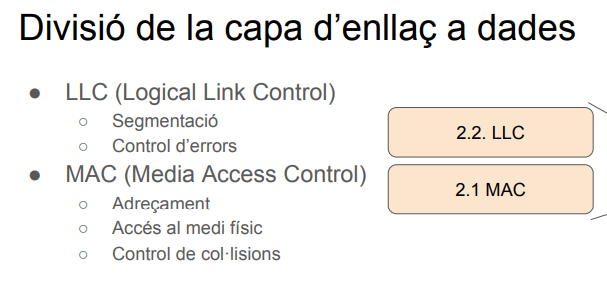
○ Son instal·lacions que interconectes ciutats i paisos

○ Son mantenides per companyes de telecomunicacions i governs

***Tipus de xarxes segons la tipologia***



***Tema 6: Enllaç a dades***



***Adreça MAC***

● Identificador de 48 bits en 6 blocs de 2 caracters hexadecimals

● Identifica una NIC o targeta de xarxa

● Els primers 24 bits indican el frabicant

Estandar IEEE 802

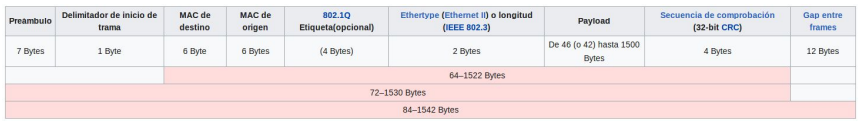
● La família d’estàndards IEEE 802 agrupa un conjunt d’estàndards de comunicació de la capa d’enllaç de dades, aquests són els més coneguts

○ LLC ■ 802.2

○ MAC ■ 802.3 Ethernet ■ 802.11 Wifi ■ 802.5 TokenRing ■ 802.16 WiMAX

● Altres protocols que són de la capa d’accés a dades: ○ PPP (Protocol punt a punt) ○ SLIP (Protocol d’internet de línea serial) ○ Frame Relay (Circuits virtuals)

***Capçalera de la trama Ethernet***



***Protocol ARP***

● Aquest protocol ens permet esbrinar que MAC pertany a una determinada IP

dins de la mateixa xarxa

● Des del SO podem consultar la taula que te en memòria amb aquesta relació

i fins i tot la podem afegir o esborrar elements manaulment

***Tipus de connexió Ethernet***

● Simplex ○ Nomes permet la comunicació en un sentit

● Half-duplex ○ Permet la comunicació en dos sentits sobre el mateix medi de comunicació

● Full-duplex ○ Permet la comunicació en dos sentits amb un medi independent per cada sentit de la comunicació

***Col·lsions***

● Quan el medi de transmissió es compartit és possible que dos computadors

transmetin al mateix temps provocant una col·lisió.

● Quan es produeix una col·lisió les senyals es barrejan i ja no es poden llegir

***Tecniques d’accès al medi per control d’accès***

● Per evitar les col·lisions existeixen diferents tècniques:

○ Pas de testimoni: Es va passant el torn per emetre passant el testimoni al següent

computador

● Pros: Fa un ús més eficient del temps de transmissió

● Contra: susceptible a errors (per inanició del testimoni)

○ Separació per temps: S’assigna un període de temps a cada computador en el qual pot emetre

● Pros: No es produirà inanició

● Contras: Pèrdua de tassa de transferència quan hi ha computadors que no tenen

res a enviar.

***Tècniques d’accès al medi per Contenció de col·lisions***

● CSMA/CD: Accés múltiple per detecció de portadora i detecció de col·lisions

○ Pros: Detecta les col·lisions

○ Contra: Els computadors han d’estar a prop per poder escoltar el senyal de col·lisió JAM

(de 4 bytes) que s’ha produït una col·lisió i límit de computadors connectat a la mateixa xarxa

● CSMA/CA: Accés múltiple per detecció de portadora i prevenció de col·lisions

○ Pros: Detecta les col·lisions, no fa falta escoltar la senyal de col·lisió(JAM)

○ Contra: L’emissor espera una ACK del receptor reduint la taxa de transferència

***Tema 3: Capa de transport***

***Transmission Control Protocol (TCP)***

● Negocien l’inici i finalització de la comunicació entre dos hosts, simulant una

comunicació orientada a connexió

● Segmenta el flux de dades en segments amb una capçalera amb informació

● Ordena les dades marcant a cada segment el byte del flux de dades on

comença el segment (Número de sequencia)

● Permet demanar dades que no han arribat amb una confirmació o ‘acuse de

recibo’ (ACK)

● Permet controlar la velocitat d’enviament reduint la finestra d’enviament o la

mida de cada segment.

● Permet múltiples connexions amb el concepte de Port

es basa en conexiones punt a punt és a dir te un origen i un destí. es verifica que la conexion esta establecida i es van confirmando que els paquets arriben.

***Establiment de la comunicació (3 hand-shake)***

● Valida que la connexió es pot dur a terme, verificant que pot arribar a l’adreça

i port que s’ha indicat

● Permet la negociació de la mida de la finestra de recepció inicial

● Aquesta comunicació sempre es passiva i és necessari que un client inici la

comunicació

● La comunicació comença amb el flag SYC activat

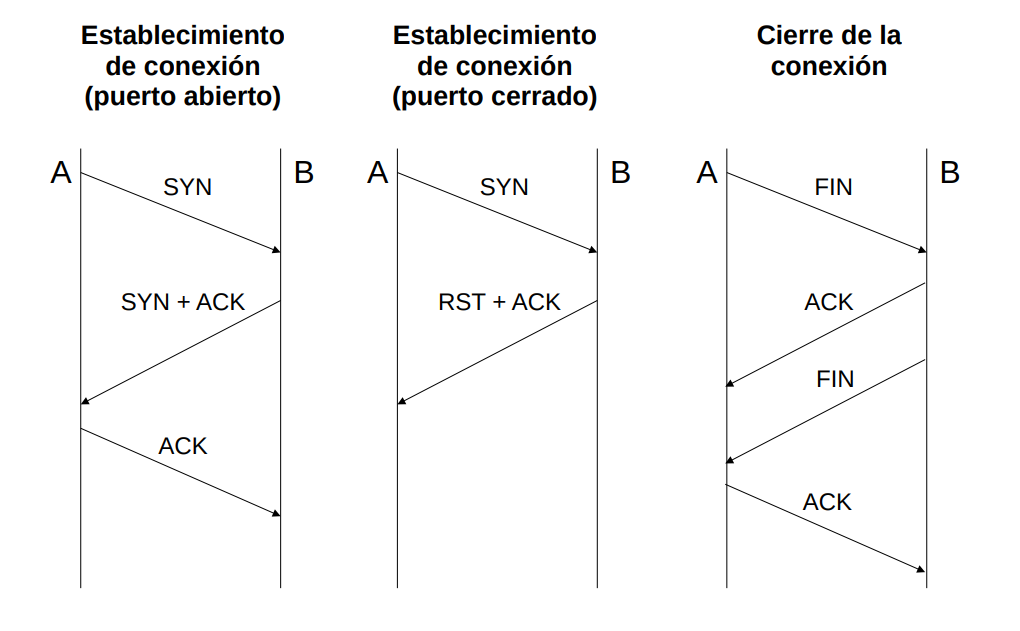
● Si el servidor rebutja la connexió, envia un missatge de resposta amb el flag

RST indicant que la comunicació s’ha de reiniciar

● Un cop feta tota la comunicació el flag FIN s’activa per indicar al client que el

servidor tanca la comunicació

Cuando un ordenador quiere conectarse con otro le envía una Flag de sincronización (SYNC). Si el ordenador que la recibe puede atender la solicitud le envía un syn ack. Si no, le envía un RST. Para confirmar que se establece la conexión le envía un ack



***Finestra de recepció i acknowledge (ACK)***

● Permet la recuperació de paquets perduts

● Controla la taxa de transferència de la connexió

● Envia múltiples segmets abans d’esperar la confirmació

● Si es produeixen errors, la finestra disminueix evitant enviar dades que seran

descartades

***Rang de ports***

● 1 - 1023 ports reservats o coneguts. Son ports d’aplicacions molt conegudes

com http, https, ftp, smtp, etc... Aquets ports requereix l’usuari root per poder

obrir-los

● 1024 - 49151 ports registrats permet a qualsevol aplicació obrir un port en

aquest rang

● 49152 - 65535 ports dinàmics són ports utilitzats com a ports temporals,

quan un client vol connectar-se a un servidor fa servir un port dinàmic

***User Datagram Protocol (UDP)***

● Estableix una comunicació no orientada a connexió

● No té confirmació de les dades rebudes

● No controla l’ordenació dels paquets enviats

● Es fa servir per aplicacions de temps real com comunicació d’àudio o vídeo

● També es fa servir per protocols on la informació que s’ha d’intercanviar és molt petita i no fa falta una comunicació orientada a connexió com són els casos de DNS, DHCP o BOOTP

“es un protocol que envia dades sense esperar que es confirmi la seva rebuda com podria ser un stream “ se usa para conexiones a tiempo real.

***Tema 4: Protocols d’aplicació***

Introducció

● La capa d’aplicació gestiona els protocols de comunicació que fa servir les

diferents aplicacions.

● Normalment l’usuari no interactua amb aquesta capa si no és l’aplicació qui

interactua i mostra els resultats d’aquesta comunicació a l’usuari per pantalla

● Els protocols més coneguts són: DHCP, DNS, HTTP, POP, SMTP, FTP, SSH

i TELNET

● En aquest apartat estudiarem alguns dels protocols més coneguts per la

configuració i ús de les xarxes

***Dynamic Host Configuration Protocol (DHCP)***

● Permet configurar automàticament:

○ Adreça IP

○ Mascara de xarxa,

○ Servidor de DNS

○ Porta d’enllaç per defecte (default gateway)

● Manté una assignació IP única de cada client

● És útil per poder configurar clients que es connecten de manera intermitent a

la xarxa

● Tipus d’adreçament

○ Manual: Manté una taula amb la relació MAC adreça IP que ha de assignar

○ Dinàmic: Assigna la primera IP disponible del rang de IPs que pot assignar amb una caducitat

associada

● El seu port assignat és el 67

***Domain Name System (DNS)***

● Sistema descentralitzat que gestiona una base de dades de les relacions

entre la IP i el nom d’un host d’internet

● Fan servir un sistema de noms jeràrquics ex: google.es, smtp.google.es,

www.gogle.es

● Quan un client no sap quina adreça té un determinat nom fa una consulta al

servidor de DNS que tingui configurat per tal d’obtenir la seva IP

● És útil per tal de poder modificar la IP d’un host sense que els clients tinguin

que aprendre la nova adreça

● El seu port assignat és el 53

se basa en pasar una ip a un “nombre” y un nombre a una ip

***Post Office Protocol (POP)***

● Obté els missatges emmagatzemats i els deixa guardats en el client

● Un cop emmagatzemat en el client esborra el missatges del servidor

● El protocol IMAP no esborra els missatges i sempre estan disponibles al

servidor

● La versió que es fa servir actualment és POP3 però també existeixen POP1,

POP2

● El seu port assignat és el 110

***Simple Mail Transfer Protocol (SMTP)***

● S’encarrega de l’enviament de correus electòrnics

● Fa servir servidors de DNS per poder trobar el domini a qui pertany el correu

ex: per user@domain1.com el servidor preguntarà qui és ‘domain1.com’ per

poder enviar el missatge a aquell servidor

● El seu port assignat és el 25

Usa el dns para l’enviament de correus electòrnics

***Hypertext Transfer Protocol HTTP***

● Protocol de comunicació per l’intercanvi de dades entre els clients i els

servidors webs

● permet l’ús de mètodes per poder fer diferents accions. Ex: GET, POST, PUT

i DELETE

● La comunicació es fa sense xifrar i a vegades es necessari posar-li una capa

de seguretat TLS o SSL. Aquest protocol es coneix com a HTTPS

● El seu port assignat és el 80

***File Transfer Protocol (FTP)***

● Permet descarregar o pujar fitxers a un servidor

● Aquest sistema envia totes les dades sense xifrar. Es fa servir el protocol

SFTP per assegurar les dades.

● El seu port assignat és el 20(port de dades) i 21(port de control)

● Té dos modes de funcionament l’actiu i el passiu

○ El mode actiu necessita poder accedir a un rang de ports del host client per connectar-se al

port de dades

○ El mode passiu és el client el que inicia la comunicació en els dos ports informant prèviament

quin port farà servir per connectar amb servidor amb el segon port (port de dades)

[01-Tipus de xarxes i els seus components](https://campus.institutpedralbes.cat/mod/resource/view.php?id=95310)

[Fitxer](https://campus.institutpedralbes.cat/mod/resource/view.php?id=95310)

PAQUETE MODEL OSI



NIVELES Y PROTOCOLOS

IP: encargado de que los datos lleguen a su destino, escogiendo el camino por el que enviar los paquetes de información.

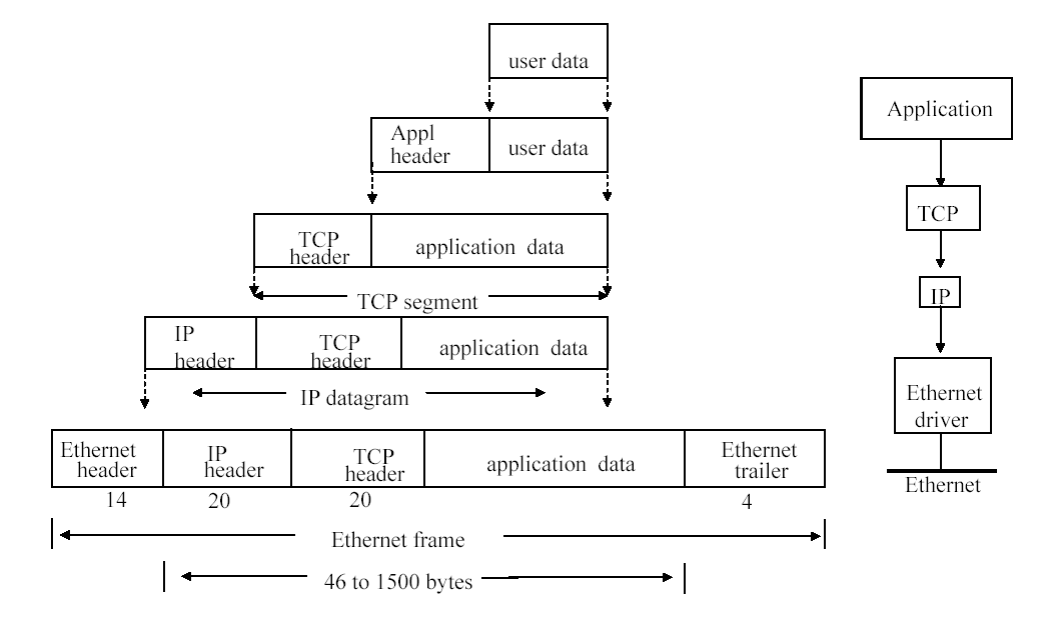
• TCP: encargado de que la información se reconstruya de forma correcta cuando llegue a su destino, para pasarla a la aplicación.

• UDP: lo mismo que TCP pero en sencillo (más inseguro pero más rápido).

• ICMP: mensajes de error que ayudan al nivel IP.

• DNS: convierte nombre de Internet (nombre\_máquina.nombre\_dominio) en dirección de Internet (IP).

• ARP: convierte dirección de Internet (IP) en dirección física (MAC).



• Versión (del protocolo IP): formato de la cabecera (IPv4 = 4, IPv6 = 6).

• Long. cab.: longitud de la cabecera IP en múltiplo de 32 bits (sin opciones = 5, con opciones = ?).

• Tipo de servicio (TOS): Se utiliza para priorizar paquetes IP. - Bits 0-2 (precedencia): nivel de prioridad del paquete. - Bits 3-6 (tipo de servicio): cómo debe la red equilibrar entre espera, rendimiento, fiabilidad y coste al encaminar el paquete IP. - Bit 8 (MBZ): no se utiliza y debe ser cero.

• Longitud total: longitud en bytes del paquete IP (incluyendo la cabecera).

• Número de identificación, indicadores y desplazamiento de fragmento: se utilizan para el seguimiento de las partes cuando un paquete se deba partir, por ejemplo, porque se reenvíe por una red para la cual es demasiado grande.

• Tiempo de vida: Número máximo de routers a través de los que puede pasar el paquete IP. Dicho número se decrementa cada vez que el paquete pasa a través de un sistema. Cuando llega a cero, el paquete se destruye y se envía un mensaje ICMP al origen.

• Protocolo: número que indica cual es el protocolo del paquete contenido dentro de la sección de datos del paquete IP (1 = ICMP, 6 = TCP, 17 = UDP)

• Suma de verificación de cabecera: permite comprobar si la cabecera se dañó durante el transporte. No hay suma de comprobación de datos.

• Dirección IP de origen: para saber de donde viene el paquete.

• Dirección IP destino: para que las puertas de enlace intermedias sepan hacia donde deben dirigir el paquete.

• Opciones IP: información adicional para controlar funciones como la seguridad y el encaminamiento (no operación, seguridad, ruta de origen desconectada, ruta de origen estricta, registro de ruta, identificador de flujo y marcas de tiempo).

***Limitaciones de IPv4:***

• El espacio de direcciones IPv4 quedará exhausto entre 2005 y 2011.

• Tablas de encaminamiento cada vez más grandes.

• Necesidad de nuevas características: multimedia, seguridad, ...

• Oportunidad de implementar mejoras que han ido apareciendo.

***Ventajas de IPv6 (que es compatible con IPv4):***

• Mayor espacio de direcciones: 128 bits.

• Soporte para tiempo real.

• Autoconfiguración de estaciones de trabajo.

• Seguridad.

En IPv6, la dirección IP tiene una longitud de 128 bits, expresada como ocho

números hexadecimales de dos bytes separados por dos puntos.

Por ejemplo: 1080:0:0:0:8:800:200C:417A → 1080::8:800:200C:417A

• ***Unicast:*** Representa un interfaz de red. Cada paquete enviado a una

dirección unicast se entrega a la interfaz identificada por esa dirección.

• ***Anycast:*** Representa un conjunto de interfaces de red. Cada paquete

enviado a una dirección anycast se entrega a una de las interfaces.

• ***Multicast:*** Representa un conjunto de interfaces de red. Cada paquete

enviado a una dirección multicast se entrega a todas las interfaces.

***Migración IPv4 a IPv6:***

1.Actualizar los servidores de DNS para que manipulen direcciones IPv6.

2.Introducir sistemas con pilas duales, que soporten IPv4 e IPv6.

3.Conectar redes IPv6 separadas por redes IPv4 a través de túneles.

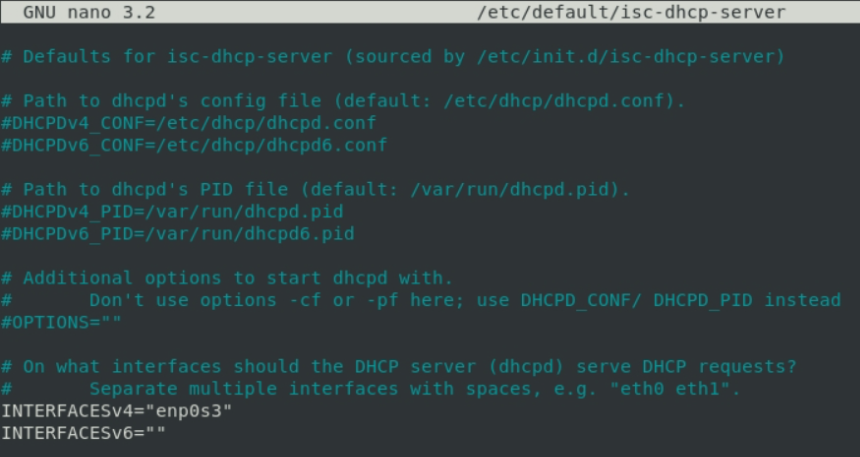
4.Eliminar el soporte para IPv4.

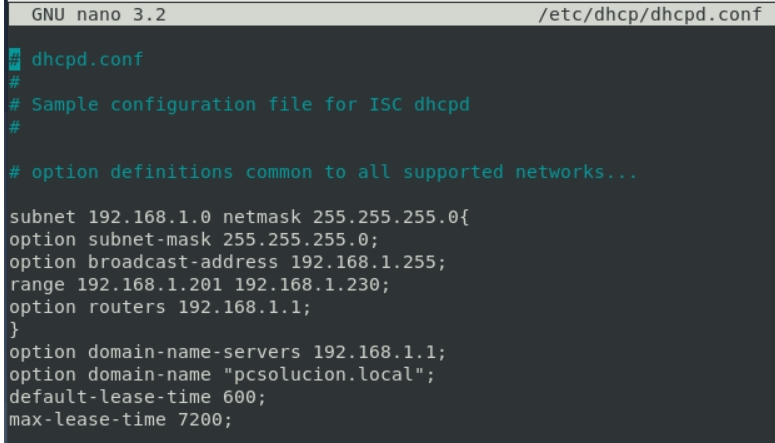
5.Utilizar traslación de cabeceras para sistemas que sólo utilicen IPv4.

DHCPenp0s3

apt-get install isc-dhcp-server

sudo nano /etc/default/isc-dhcp-server



nano /etc/dhcp/dhcpd.conf

Client

apt-get install isc-dhcp-client

