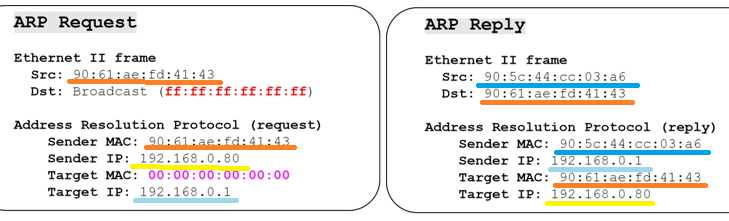
* aa (authoritative answer): indica que la respuesta fue autoritativa. Significa que el servidor es autoritativo del dominio solicitado. (DNS)
* Agente de usuario: interfaz entre el usuario y la aplicación de red.
* ALPN: application layer protocol negotiation
* Anycast: se le asigna la misma ip a varios dispositivos y se le destina el mensaje al primero que lo resuelva, el más cercano. O algo así(?
* ARP: address resolution protocol. Asocia direcciones de red (IP) a direcciones de enlace (MAC). Si un host A necesita hablarle a otro B, A no conoce la MAC de B (la tabla ARP no contiene esa entrada) pero sí su IP:

1. Se emite una solicitud ARP, que se envía en broadcast a todos los dispositivos de la LAN Ethernet. La trama contiene un paquete de solicitud ARP con la dirección IP del host de destino.

2. El nodo receptor que es dueño de esa IP responde enviando un paquete de respuesta de ARP al emisor con una trama unicast.

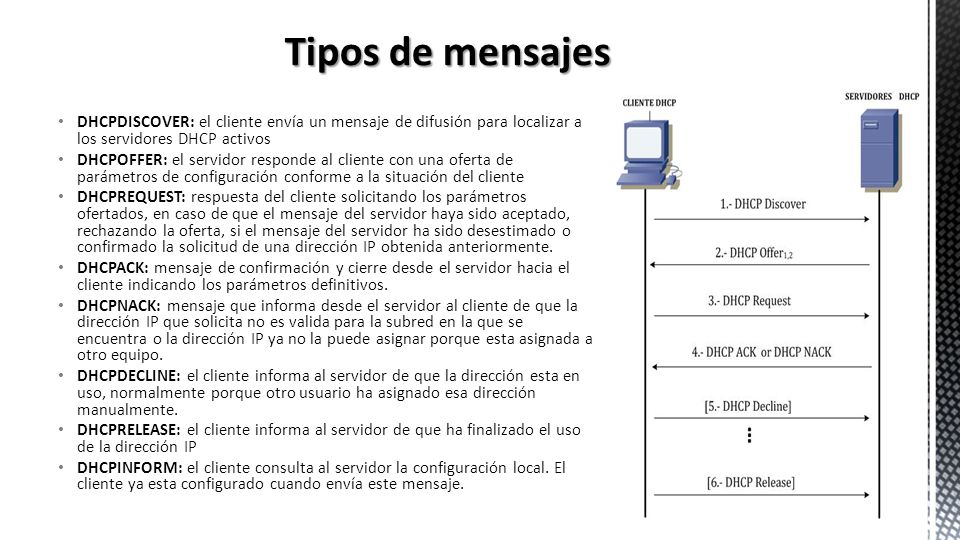
3. Con esta respuesta se crea una entrada nueva en la tabla ARP.

* Tabla arp: contiene un mapeo de ip/mac para algunos nodos de la LAN.
* ARP reply: cuando solicita la info que necesita (Una mac);
* ARP request: cuando el host dueño de esa mac le responde con la info.



* ASN:
* AP: access points
* ARQ: automatic repeat request. junto con ventana deslizante y rnr hacen control de flujo
* best effort o mejor esfuerzo: no es seguro, puede perder lo que transporta
* BOOTP
* CA: congestion avoidance. Fase de mantenimiento en control de congestión.
* CIDR: classless inter domain routing. enrutamiento entre dominios sin clases, es un método de asignación de direcciones IP que mejora la eficiencia del enrutamiento de datos en Internet al agrupar entradas de tabla de enrutamiento en una sola.

CIDR consiste en permitir máscaras de subred de longitud variable (VLSM) para optimizar la asignación de direcciones IP y utilizar resumen de rutas para disminuir el tamaño de las tablas de enrutamiento. Con resumen se refiere a agrupar rutas, es decir de 4 rutas en 1 sola (hablando de la base de CIDR).

* CMPT
* CRC: ciclic redundancy check. Método de control de errores que trata los bits como polinomios, agrega otra polinomio y hace alguna operación.
* CSMA: carrier sense multiple access. (Protocolo de particionado de canal, capa de enlace). Escuchas que nadie transmita y transmitís.
* CURL comandos:
  + -I, --head: Recupera únicamente el header de HTTP en el request (Información del recurso)
  + -H, --header <cabecera/archivo>: agregar información personalizada al header del request, es decir, la solicitud. También para reemplazar los valores por defecto que utilizará curl.
  + -X, --request <comando>: Especifica un método de request específico para usar en la comunicación (el default es GET).
  + -s, --silent: Modo silencio. No muestra los mensajes de error ni la barra de progreso.
  + –z: se quiere obtener la página solo si su última modificación fue realizada en una fecha menor o igual a la dada. Por ej: curl –z ‘Wed, 17 Sep 2017’ www.redes.unlp.edu.ar)
  + -v verbose, que lo haga detallado, que escriba todo
* cut through: Mecanismo de conmutación del switch. Lee hasta dirección de destino, más rapido. No realiza FCS
* cwnd: ventana de congestión, considera el estado de la red
* CWR: congestión windows reduced. Bit dentro de segmento tcp lo marca. Una vez que el receptor recibe un segmento del router informando que hay congestion, le informa esto al emisor (ECE). Este lo marca para notificar que tomó medidas.
* DA
* DAD: duplicate address detection
* default gateway: router por default. Conecta la red con otra o con internet. Se configura manualmente o con algun protocolo
* Destination 0000 (ruta por defecto): A donde se mandan los paquetes cuyo destino no está en la tabla de ruteo. Van a terminar llegando a otro router, que repite el procedimiento.
* DF bit/frag: do not fragment. Si no se quiere fragmentar y no pasa, el router le avisa a origen para que mande fragmentos mas chicos.
* DHCP: dynamic host configuration protocol o protocolo de configuración dinámica de host que permite a un servidor DHCP/servidor de red asignar dinámicamente la dirección IP, la máscara de subred, los gateways predeterminados y otros parámetros de configuración de red a los dispositivos que lo soliciten. Mensajes:

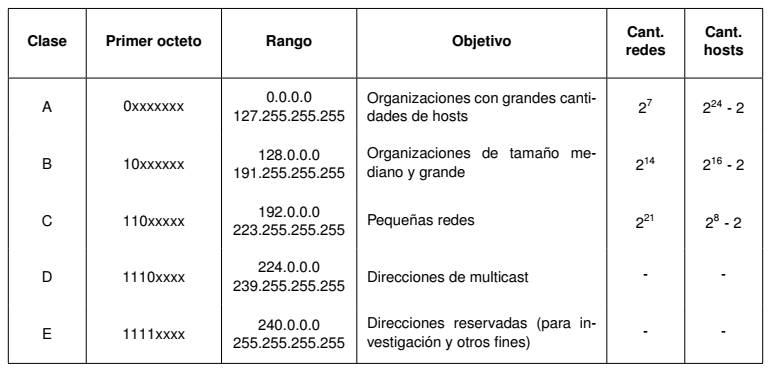
Los routers de borden obtienen su ip publica de un servidor dhcp del proveedor, y los host internos de un dhcp del router.

* Direcciones privadas: Clase A: 10.0.0.0/8

Clase B: 172.16.0.0/12

Clase C: 192.168.0.0/16

Según RFC 1918



* DHCP6: opción de autoconfiguración en ipv6. Requiere RA.
* Dominio de colisión: hasta donde pueden extenderse las colisiones en una red.
* DNS: sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como internet o una red privada
* DST y SRC
* ECE: explicit congestion enable. Bit dentro del segmento tcp lo marca. Indica que el router está a punto de congestionarse, es decir, que su buffer está casi lleno para que el emisor disminuya la transferencia.
* ECN: explicit congestion notification. Se negocia al establecerse la conexión TCP. Va en el datagrama IP
* EDC: error detection and correction
* FCS: frame check sequence
* FDMA: frequency multiple access. (Protocolo de particionado de canal, capa de enlace)
* FIB: forwarding information base/ forwarding table.
* Forwarding/despacho/switching: envio y recepción de paquete (ip). Pasar el paquete desde una entrada a una salida, solo los routers. Selecciona un port de salida según la dirección de destino y la tabla de ruteo.
* FQDN: Fully Qualified Domain Name → lista de etiquetas (labels) separadas por puntos.
* fragment free: mecanismo de conmutación de switch. Lee los primeros 64 bits.
* Full duplex: ambos dispositivos pueden transmitir y recibir datos en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para que ambos nodos transmitan en cualquier momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos.
* FTP: file transfer protocol. Dos conexiones: control y datos. Tiene modo activo (El servidor se conecta al cliente para generar la conexion de datos) y pasivo (El cliente se conecta a un puerto indicado por el servidor). Versiones:
  + FTPS: version segura
  + SCP (Secure remote copy)
  + SFTP (Secure FTP)
* FXD: algo de udp y tcp y una p\*\*\* marca de ropa si googleas(?
* gateway: router(?

Gateway: a donde tengo que enviar el datagrama para llegar a “Destino”.

Gateway 0000: indica que estoy en la red a la cual quería llegar (Red destino), y debo mandar el datagrama al dispositivo final.

* Un Glue Record es un registro DNS que permite asociar una dirección IP a un subdominio de forma que pueda usarse como un nombre de servidor de DNS.

Se utiliza un Glue Record cuando queremos utilizar nuestro propio servidor cloud como servidor DNS. Así, con este tipo de registro DNS A, se garantiza que la IP del servidor DNS resuelve correctamente. Por ejemplo, si en lugar de utilizar los nameservers de tu proveedor quieres utilizar los tuyos propios, deberás crear dos subdominios que cumplan con esta función:

* + ns1.midominio.com
  + ns2.midominio.com

Y, además, crear los Glue Records necesario que el DNS, el sistema de nombres de dominio, sepa dónde están los servidores DNS a los que apunta tu dominio. De lo contrario, cada vez que alguien intentara acceder a midominio.com, el DNS no sabría dónde tiene que consultar para resolver esa IP; ya que para llegar a un subdominio, primero tiene que poder accederse al dominio principal. Sin Glue Record, la tarea de resolver una IP se convierte en un bucle infinito.

* Go back n: (Va con el tema de ventana deslizante) necesita que lleguen todos en orden. Si faltan 2 y 3 no puede dar confirmar el 4. Selective repeat si.
* GTLD (Generic Top-Level Domain): contiene dominios con propósitos particulares (.com para páginas comerciales, .org para organizaciones, etc)
* GZIP: compresión http2
* half-duplex: los nodos en los extremos del enlace pueden transmitir, pero no al mismo tiempo
* HDLC: high level data link control
* HPACK: compresor de headers (http2)
* HTCP: hyper text caching protocol
* HTTP: protocolo que permite intercambiar el contenido entre un dispositivo y el servidor web. cuando el contenido llega, se procesa (No tiene que ver el protocolo). 1.1 trabaja con ascii.
* IANA
* ICANN: internet corporation for assigned names and numbers. Controla el funcionamiento de DNS.
* ICMP: internet control message protocol o Protocolo de control de mensajes de Internet. Apoya a IP, cuando se descarta algo le avisa al origen, pero sus mensajes tamb se pueden perder. Por ejemplo, se pueden generar mensajes para avisar que los destinos o routers intermedios están congestionados, para avisar que un host o red es inalcanzable, que ttl llegó a 0, etc. Imprescindible en ipv6 ya que resuelve MLD, NDP y mensajes de control de errores (ping).
* ICP: internet cache protocol
* IGMP: manejar grupos de multicast
* IID: interface identifier. IPv6, de 64 o 48 bits, generadas en forma manual o automática con direcciones físicas o mac.
* IMAP: Protocolo de acceso de correo (Para recibir)
* IP: internet protocol. Un monton de servicios y otros protocolos corren sobre este. Se usa para encaminar los paquetes.Sirve para identificar a un equipo dentro de la red.
* IPC: inter process comunication. Comunicacion entre procesos dentro del mismo SO.
* IP-ng: ip v6
* ISN: initial sequence number (es de tcp)
* ISP: proveedor de internet
* IW: init windows. La cantidad de segmentos con las que inicia el control de congestion (1 a 3)
* LAN: local area network. red concentrada en un area concreta, una oficina, un piso, etc.
* LDP
* Loopback / localhost: direcciones del rango '127.0.0.0/8'. Se suele utilizar cuando una transmisión de datos tiene como destino el propio host. También se suele usar en tareas de diagnóstico de conectividad y validez del protocolo de comunicación. Crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.
* M2M: machine to machine, modelo de comunicación
* MF bit/flag: more fragments. Significa que quedan fragmentos por llegar.
* MIME
* MLD: multicast listener discovery
* MSS: maximum segument size. Valor adecuado entre ambos puntos, lo maximo que puede recibir(?. RMSS=> para el receptor. SMSS=> Para el emisor

MSS, o tamaño máximo de segmento, es la cantidad máxima de bytes o carga útil de datos más grande que un dispositivo aceptará de una conexión de red, es decir, lo máximo que se puede enviar o recibir.

Si se recibe una cantidad mayor, se produce fragmentación, lo cual suma overhead.

Se envía dentro de Options, ya que sólo se negocia una vez por conexión.

Según la RFC-879, el valor mínimo recomendado es de 536 bytes, usando una Unidad de Transmisión Máxima (MTU) de 576 bytes, y 40 bytes de cabeceras TCP/IP

MTU - (encabezado TCP + encabezado IP) = MSS

El MSS se negocia en el saludo de 3 vías.

* MTU:unidad máxima de transferencia. Tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.
* NAK: aviso de que no llegó bien el dato. Contrario a ACK, que confirma que sí
* NAPT: network address port translation. Mapea un conjunto de direcciones privadas a una publica. Se pierde end to end.
* NAT: network address translation. Permite que redes de PC utilicen IPs privadas y se conecten a Internet usando una única dirección IP (IP pública). Traduce las direcciones de un espacio privado (No enrutable en internet) a un espacio público. Se pierde end to end.
* ND: neighbor discovery (Descubrimiento de vecinos). Equivalente en IPv6 de ARP (Ipv4) pero agrega más funcionalidades.
* NDP: ND protocol (Es lo mismo)
* neighbor advertisement
* neighbor solicitacion
* NFS:
* NIC: network interface card. Adaptador/placas de red
* NUD: neighbor unreach detection
* Orientado a conexión: de antemano se establece el camino del paquete???? Se espera confirmación de recepcion, y, en el caso de TCP, que lo implementa, se realiza saludo de 3 vias. Contrario a conmutacion de paquetes, implementado por IP
* OUI: organizationally unique identificar. 3 primeros octetos de una mac que son para los fabricantes.
* PDU: unidad de datos del protocolo (Si es datagrama, segmento, trama, etc).
* pfxlen: longitud del prefijo, “”Máscara”” en IPv6. Indica hasta donde es red y subred y donde host. Se recomienda dejarla en 64 bits.
* Piggybacking: técnica de transmisión de datos bidireccional en la capa de enlace de datos. Con esta técnica, en vez de enviar ACK en un paquete individual, este es incluido dentro del próximo paquete a enviar.
* PING: Mensaje ICMP. Cuando llega el paquete echo request responde con otro (echo reply), lo que permite ver que está activo y es alcanzable, es decir, prueba la conectividad IP entre dos host.
* POP3: (Post Office Protocol -- Version 3).Para recibir.
* QR (Query/Response): Informa de que el mensaje es de respuesta. (DNS)
* RA (recursion available): flag que indica que el servidor puede responder recursivamente, por lo que la respuesta también lo fue (DNS)
* RA (Flags RST y ACK activados) TCP.
* RARP: reverse address resolution protocol. mapea macs a ip (Opuesto de ARP).Está en desuso, se cambio por boothp/dhcp
* rd (recursion desired): flag que indica que la solicitud fue recursiva (DNS)
* rdt: reliable data transfer
* RED: random early detection. maneja las colas de routers viendo que esta próximo a congestionarse.
* Registro A, AAAA: Address → El valor del registro es una IP (ej.: berlin.cities.org. IN A 172.20.1.100), o una IPv6 (ej.: berlin.cities.org. IN AAAA 2001:db8:1234:4567::100) que es la dirección real del dominio.
* Registro axfr, permite transferencia de zona
* Registros CNAME (Canonical Name): nombre ! nombre.
* Registros HINFO (Hardware Info): nombre ! info.
* Registro MX (Mail Exchanger) nombre-dom ! → Indica la lista de servidores para un dominio determinado.
* Registros NS (Name Server): nombre-dom ! dns server(s).
* Registros SOA (Start Of Authority): params. de dominio.
* Registros PTR (Pointer): IP ! nombre.
* Registros TXT (Textual): nombre ! info.
* RIB
* RIRs: regional internet registers. ARIN, RIPE, APNIC, LACNIC (Latam y caribe), AFRINIC.
* ROM
* ROOTs servers: servidores raíz de DNS.
* Router advertisement (RA): el router lo manda multicast cada 3 o 4 minutos y el host lo puede tomar para saber en que red esta y ahi hacer la autoconfiguración (IPV6).
* Router solicitation (RS): cuando el nodo arranca pide que se le envien los datos para la autoconfiguracion, esto es, la red en la que esta. La respuesta puede ir unicast al que la pidio o multicast y lo toma el que pidio. El nodo puede mandarlo o esperar RA
* RTO: ver T1
* RTT: Round Time Trip. El tiempo de ida y vuelta hace referencia, en el mundo de las telecomunicaciones y redes informáticas, al tiempo que un paquete de datos tarda en volver a su emisor habiendo pasado por su destino.

Las marcas de tiempo (Timestamp) en TCP permiten que los puntos finales mantengan una medición actual del tiempo de ida y vuelta o tiempo de envio + confirmación de su recepción (RTT) de la red entre ellos. Este valor ayuda a cada pila TCP a establecer y ajustar su temporizador de retransmisión.

* RUDP: reliable user datagram protocol. Otro como udp y tcp.
* Ruteo o enrutamiento (Una es una cosa, la otra es otra, se pisan las definiciones según donde busques): proceso por el cual se construye la tabla de ruteo / función de seleccionar por cuál interfaz se enviará un dato
* rwnd: ventana de recepcion recibida
* SA (Flags SYN y ACK activados).TCP
* SCTP: Stream control transmission Protocol (Otro como tcp y udp que se usa menos y es un intermedio entre ambos)
* Selective repeat: (Va con ventana deslizante). Permite huecos en buffer. Si llegan retrasados o en desorden se ponen donde van y cuando se tiene el espacio completo (No falta nada en el medio) se manda a la capa usuario. Se ordena por nº seq. Opuesto a go back n.
* server push: el servidor envía varias respuestas a una única solicitud del cliente, es decir, además de la respuesta a la solicitud original, el servidor puede enviar recursos adicionales, lo que ahorra mensajes innecesarios. Esto es así porque una página web está formada por decenas de archivos referenciados. En HTTP 2.0 el cliente puede indicar si quiere activar ‘server push’.
* Servidores DNS: Uno puede tener varios roles.
  + Servidor Raiz: servidor que delega a todos TLD. No deberia permitir recursivas.
  + Servidor Autoritativo: servidor con una zona o sub-dominio de nombres a cargo. podría sub-delegar. Dueño del registro, impone su valor
  + Servidor Local/Resolver Recursivo: es un servidor que es consultado dentro de una red. mantiene cache. Puede ser Servidor Autoritativo. Permite recursivas \internas". También llamado Caching Name Server.
  + Open Name Servers: servidores de DNS que funcionan como locales para cualquier cliente. Por ejemplo 8.8.8.8. Pueden consultarse estos directamente sin resolver local.
  + Forwarder Name Server: interactúan directamente con el sistema de DNS exterior. Son DNS proxies de otros DNS internos.
  + Servidor Primario y Secundario: solo una cuestión de implementación donde se modifican los datos realmente. El cliente no nota la diferencia. El primario configura la información y el secundario la copia. Ambos son igual de autoritativos. Puede haber 1, 2…n, y si todos se configuran a mano son todos primarios.
* semiduplex: un mismo nodo no puede transmitir y recibir al mismo tiempo.
* S&W: Stop & wait (es de envío y recepción en la capa de transporte). Envía un dato por vez, lo que lo hace ineficiente.
* SLAAC: opcion de autoconfiguración en ipv6.permite obtener la configuración básica para internet, prefijo, router y dns. Hay equipos que no soportan la configuración dns y requieren DHCP6.
* SLL
* SMPT: Protocolo para transferencia simple de correo (Para enviar)
* SNMP
* Socket: puertas. los procesos envían y reciben mensajes desde estos. Son fijos, no importa el ID de proceso que se establece.
* SPDY: compresion en http2
* SS: slow start. Fase de crecimiento inicial en el control de congestión
* SSH
* ssthresh: slow start threshold (umbral). Relacionado a la detección de la utilización de red y su congestión.
* ST: internet stream protocol
* STP: spanning tree protocol. Protocolo de gestión de la de la capa de enlace que pone a disposición la redundancia de caminos pero previene de posibles loops en la red de switches. En todo momento se asegura de que solo haya un camino activo entre 2 switches.
* Store & forward: forma de trabajo de los routers, reciben un paquete y deciden para donde routearlo. lee toda la trama y chequea CRC, realiza FCS. Los routers y los switchs lo son.
* T1 o RTO: timer que inicia al transmitir (ventana deslizante)
* TCAM
* TCP: transport control protocol
* TDMA: time division multiple access. (Protocolo de particionado de canal, capa de enlace)
* TFTP
* TLD: top level domain (jerarquía dns). Se clasifican en:
  + GTLD: generic TLD, que contienen dominios con propósitos particulares (.com, .net, etc).
  + ccTLD: country code TLD, que contienen dominios delegados a los países (.ar, .us, .co, etc).
  + ARPA TLD: resolución de reversos, de ip a nombre.
* TTL: tiempo de vida. Evita que un paquete quede dando vuelta por la red indefinidamente. Lo define el SO y en cada salto se decrementa en 1. Si llega a 0 el router lo descarta, a menos que ya haya llegado a su red destino. Máximo: 255

En ARP: tiempo después del que el mapeo de direcciones debe ser olvidado.

TLS

* Transferencia de zona: en servidores dns, es la operación por la cual se sincronizan servidores primarios y secundarios que comparten la información.
* UDP: user datagram protocol
* UI: interfaz de usuario
* URI: uniform resourse id
* URL: uniform resource location
* URN: no indica ubicacion, solo categorias.
* VC: virtual circuits (en el propio paquete se indica cual es el camino que tiene que seguir, en IP se sabe el destino pero no por donde llegar).
* VLAN: virtual local área network. crear redes lógicas independientes dentro de una red física.
* VLSM: variable length subnet mask. aprovecha el espacio de direcciones asinando diferentes mascaras para cada subred.
* WCCP: web cache control protocol
* XDR: external data representation

**PORTS:**

* Bittorrent: 6881
* DNS: 53
* FTP: conexión de control: 21. Datos en modo activo: 20, modo pasivo: puerto no privilegiado.
* HTTP: 80
* HTTPS: 443
* IMAP: 143
* Mail: 25
* MSA: 587
* No privilegiados: número > 1023, los suelen agarrar los clientes para conectar con los servidores de diferentes protocolos
* POP3: 110
* SMPT: 25
* SSH: 22

Weas:

Cuando se haria una apertura de conexion (Saludo de 3 vias) en simultanteo?

En ventana deslizante,ver relacion entre tamaño de ventana, RTT y timer para retransmitir

ventana selectiva?? relacion con selective repeat?

Que hace tcp con segmentos fuera de orden? los confirma? los deja en buffer? los descarta? (se contradice en algunas partes, creo)

Ver en que casos se manda ACK del ultimo que llego y en que casos del que esta esperando (Aparecen ambos casos en la teoria)

En ventana deslizante de TCP, si hay capacidad para enviar que determina que se envien o no? (Por el ejemplo de teoria que no manda 601…700 aunque hay lugar)

Ver en lo de SS y CA lo de umbral (empieza a subir de a uno) y congestion (baja a la mitad). cuando es cada uno, y eso.

Ver bien que onda lo de los 3 ACK duplicados en fast recovery y fast retransmit (Reno)

un router tiene varias ips. Por? Cada red que conecta?

ver como pasar de mac a ipv6 (pract 9 ejercicio 6)

ver que era genmask en las tablas feas

Por que en ftp een modo activo primero sale el comando y despues la conex tcp?