Protocolos de Redes: Ethernet y TCP/IP

Alejandro Furfaro

7 de septiembre de 2023

Temario

Temario

Protocolo

¿Que es un protocolo?

Protocolo

¿Que es un protocolo?

Un protocolo es en general, un conjunto de convenios y formatos necesario para comunicar dos nodos de un sistema de comunicaciones independientemente de la arquitectura particular de cada uno.
Debe asegurar que no solo llegue la información libre de errores sino que tenga el formato adecuado para que el otro extremo la pueda interpretar sin lugar a dudas.

Temario

Introducción a Ethernet

- Desarrollado a mediados de la década de 1970 por investigadores del Centro de Investigación de Palo Alto (PARC) de Xerox.

Introducción a Ethernet

- Desarrollado a mediados de la década de 1970 por investigadores del Centro de Investigación de Palo Alto (PARC) de Xerox.
- Basado en una Red de datos de la Universidad de Hawuaii llamada Alhoa, que vinculaba de manera inalámbrica un campus diseminado en diferentes islas.

Introducción a Ethernet

- Desarrollado a mediados de la década de 1970 por investigadores del Centro de Investigación de Palo Alto (PARC) de Xerox.
- Basado en una Red de datos de la Universidad de Hawuaii llamada Alhoa, que vinculaba de manera inalámbrica un campus diseminado en diferentes islas.
- Como Alhoa es una red del tipo acceso múltiple, es decir los nodos están conectados a través de un driver a un link como si éste fuese un bus.

Introducción a Ethernet

- Desarrollado a mediados de la década de 1970 por investigadores del Centro de Investigación de Palo Alto (PARC) de Xerox.
- Basado en una Red de datos de la Universidad de Hawuaii llamada Alhoa, que vinculaba de manera inalámbrica un campus diseminado en diferentes islas.
- Como Alhoa es una red del tipo acceso múltiple, es decir los nodos están conectados a través de un driver a un link como si éste fuese un bus.
- Actualmente, compite principalmente con redes inalámbricas 802.11, pero sigue siendo extremadamente popular en las redes de campus y centros de datos.

Introducción a Ethernet

- Desarrollado a mediados de la década de 1970 por investigadores del Centro de Investigación de Palo Alto (PARC) de Xerox.
- Basado en una Red de datos de la Universidad de Hawuaii llamada Alhoa, que vinculaba de manera inalámbrica un campus diseminado en diferentes islas.
- Como Alhoa es una red del tipo acceso múltiple, es decir los nodos están conectados a través de un driver a un link como si éste fuese un bus.
- Actualmente, compite principalmente con redes inalámbricas 802.11, pero sigue siendo extremadamente popular en las redes de campus y centros de datos.
- El nombre más general de la tecnología detrás de la red Ethernet se debe al protocolo de acceso al medio conocido como **CSMA** / **CD** (por **C**arrier **S**ense **M**ultiple **A**ccess / with **C**olision **D**etect).

Introducción a Ethernet

- En 1978 Intel y Data Equipment Corporation (DEC) junto con Xerox, escriben la especificación de un protocolo de transmisión Ethernet que permita transmitir y recibir tramas a razón de 10 Mbps.

Introducción a Ethernet

- En 1978 Intel y Data Equipment Corporation (DEC) junto con Xerox, escriben la especificación de un protocolo de transmisión Ethernet que permita transmitir y recibir tramas a razón de 10 Mbps.
- Adoptan el sistema de acceso múltiple CSMA y le agregan detección de colisiones.

Introducción a Ethernet

- En 1978 Intel y Data Equipment Corporation (DEC) junto con Xerox, escriben la especificación de un protocolo de transmisión Ethernet que permita transmitir y recibir tramas a razón de 10 Mbps.
- Adoptan el sistema de acceso múltiple CSMA y le agregan detección de colisiones.
- Se adopta como medio de transmisión el cable Coaxil lo cual permitió tener enlaces de hasta 500m

Introducción a Ethernet

- En 1978 Intel y Data Equipment Corporation (DEC) junto con Xerox, escriben la especificación de un protocolo de transmisión Ethernet que permita transmitir y recibir tramas a razón de 10 Mbps.
- Adoptan el sistema de acceso múltiple CSMA y le agregan detección de colisiones.
- Se adopta como medio de transmisión el cable Coaxil lo cual permitió tener enlaces de hasta 500m
- A popsteriori el IEEE asume la estandarización de este protocolo en el Proyecto 802.3

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.
- Objetivo: “identificar y dar forma a standards de LAN con tasas de transmisión de hasta ***20 Mbps*** ”.

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.
- Objetivo: “identificar y dar forma a standards de LAN con tasas de transmisión de hasta ***20 Mbps*** ”.
- El conjunto de estándares 802 subdividió la capa 2 del Modelo OSI en dos sub-capas:

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.
- Objetivo: “identificar y dar forma a standards de LAN con tasas de transmisión de hasta ***20 Mbps*** ”.
- El conjunto de estándares 802 subdividió la capa 2 del Modelo OSI en dos sub-capas:
- Control de Acceso al Medio (MAC = Media Access Control)

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.
- Objetivo: “identificar y dar forma a standards de LAN con tasas de transmisión de hasta ***20 Mbps*** ”.
- El conjunto de estándares 802 subdividió la capa 2 del Modelo OSI en dos sub-capas:
- Control de Acceso al Medio (MAC = Media Access Control)
- Limita con el nivel inferior en la jerarquía OSI (Nivel Físico), y determina la técnica con que se accede al medio físico compartido.

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.
- Objetivo: “identificar y dar forma a standards de LAN con tasas de transmisión de hasta ***20 Mbps*** ”.
- El conjunto de estándares 802 subdividió la capa 2 del Modelo OSI en dos sub-capas:
- Control de Acceso al Medio (MAC = Media Access Control)
- Limita con el nivel inferior en la jerarquía OSI (Nivel Físico), y determina la técnica con que se accede al medio físico compartido.
- Control de Enlace Lógico (LLC = Logic Link Control).

Proyecto IEEE 802

- Febrero de 1980: IEEE lanza el proyecto 802.
- Objetivo: “identificar y dar forma a standards de LAN con tasas de transmisión de hasta ***20 Mbps*** ”.
- El conjunto de estándares 802 subdividió la capa 2 del Modelo OSI en dos sub-capas:
- Control de Acceso al Medio (MAC = Media Access Control)
- Limita con el nivel inferior en la jerarquía OSI (Nivel Físico), y determina la técnica con que se accede al medio físico compartido.
- Control de Enlace Lógico (LLC = Logic Link Control).
- Interactúa con el Nivel OSI superior (Nivel de Red) de modo tal de garantizarle independencia de la forma en que se accede al medio físico.

Derivaciones del 802...

Dos subcapas

En parte la decisión de dividir en dos subcapas el nivel 2 de OSI derivó en una enorme cantidad de variantes, en las cuales la LLC es similar, y la que se relaciona con la capa física cambia fuertemente. Al punto de tener protocolos de capa 2 inalámbricos y cableados dentro del 802

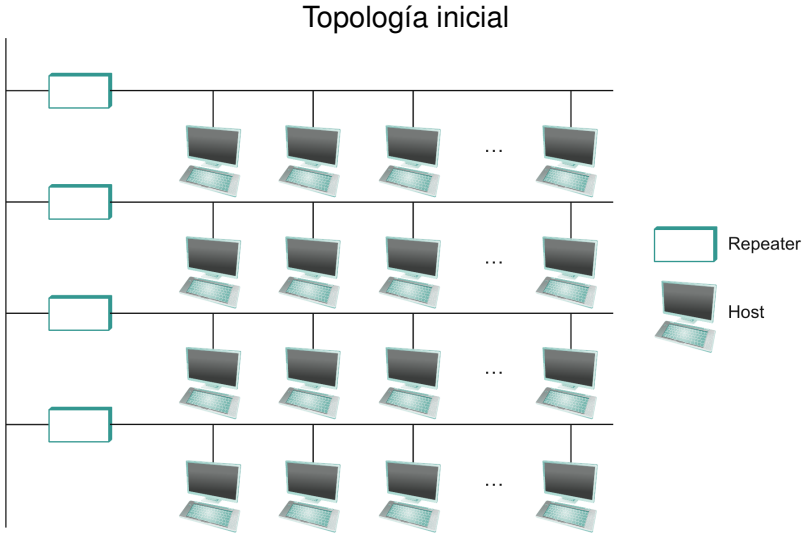
Un grupo de trabajo por cada estándar

802.1	Normalización de interfaz.
802.1d	Spanning Tree Protocol
802.1p	Asignación de Prioridades de tráfico
802.1q	Virtual Local Area Networks (VLAN)
802.1x	Autenticación en redes LAN
802.1aq	Shortest Path Bridging (SPB)
802.2	Control de enlace lógico LLC
802.3	CSMA / CD (ETHERNET)
802.3a	Ethernet delgada 10Base2
802.3c	Especificaciones de Repetidor en Ethernet a 10 Mbps
802.3i	Ethernet de par trenzado 10BaseT
802.3j	Ethernet de fibra óptica 10BaseF
802.3u	Fast Ethernet 100BaseT
802.3z	Gigabit Ethernet parámetros pa ra 1000 Mbps
802.3ab	Gigabit Ethernet sobre 4 pares de cable UTP Cat5e o superior
802.3ae	10 Gigabit Ethernet

Derivaciones del 802...

- 802.4 Token bus LAN (Disuelto)
- 802.5 Token ring LAN (topología en anillo) Inactivo
- 802.6 Redes de Área Metropolitana (MAN) (ciudad) (fibra óptica) Disuelto
- 802.7 Grupo Asesor en Banda ancha (Disuelto)
- 802.8 Grupo Asesor en Fibras Ópticas (Disuelto)
- 802.9 Servicios Integrados de red de Área Local (redes con voz y datos integrados) (Disuelto)
- 802.10 Seguridad de red (Disuelto)
- 802.11 Redes inalámbricas WLAN. (Wi-Fi)
- 802.12 Acceso de Prioridad por demanda 100 Base VG-Any Lan (Disuelto)
- 802.13 Se ha evitado su uso por superstición. (Sin uso)
- 802.14 Módems de cable (Disuelto)
- 802.15 WPAN (Bluetooth)
- 802.16 Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX)
- 802.17 Anillo de paquete elástico script
- 802.18 Grupo de Asesoría Técnica sobre Normativas de Radio (En desarrollo a día de hoy)
- 802.19 Grupo de Asesoría Técnica sobre Coexistencia
- 802.20 Mobile Broadband Wireless Access
- 802.21 Media Independent Handoff
- 802.22 Wireless Regional Area Network

Topologías



Codificación

- Problema General: Como transmitir una trama de bits como una señal por un medio de ancho de banda (en principio) limitado.

Codificación

- Problema General: Como transmitir una trama de bits como una señal por un medio de ancho de banda (en principio) limitado.
- Agregamos que la transmisión es asincrónica.

Codificación

- Problema General: Como transmitir una trama de bits como una señal por un medio de ancho de banda (en principio) limitado.
- Agregamos que la transmisión es asincrónica.
- Claves:

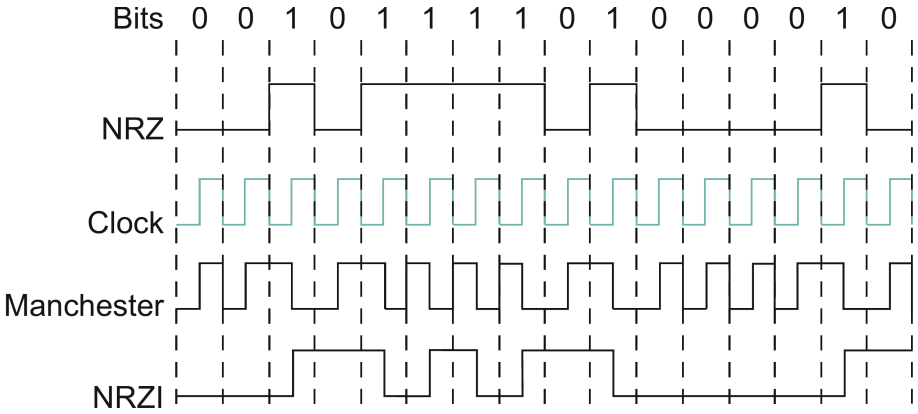
Codificación

- Problema General: Como transmitir una trama de bits como una señal por un medio de ancho de banda (en principio) limitado.
- Agregamos que la transmisión es asincrónica.
- Claves:
  - Minimizar las transiciones de la señal codificada.

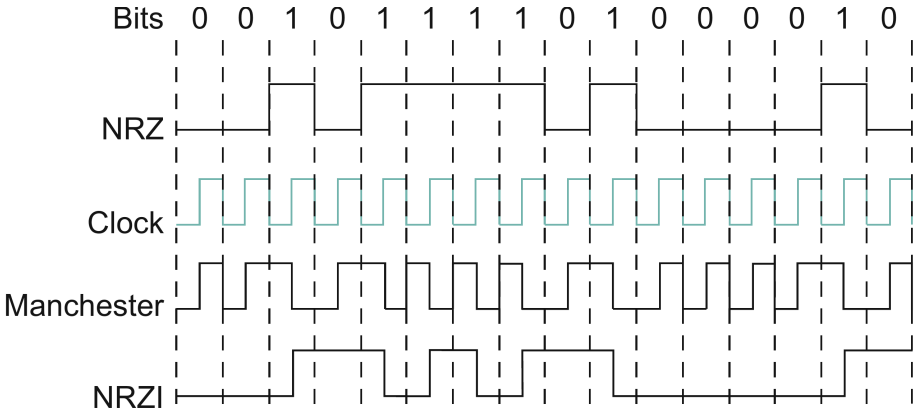
Codificación

- Problema General: Como transmitir una trama de bits como una señal por un medio de ancho de banda (en principio) limitado.
- Agregamos que la transmisión es asincrónica.
- Claves:
  - Minimizar las transiciones de la señal codificada.
  - Como manejar tiras largas de ’0’s o de ’1’s sin perder sincronismo

Codificación

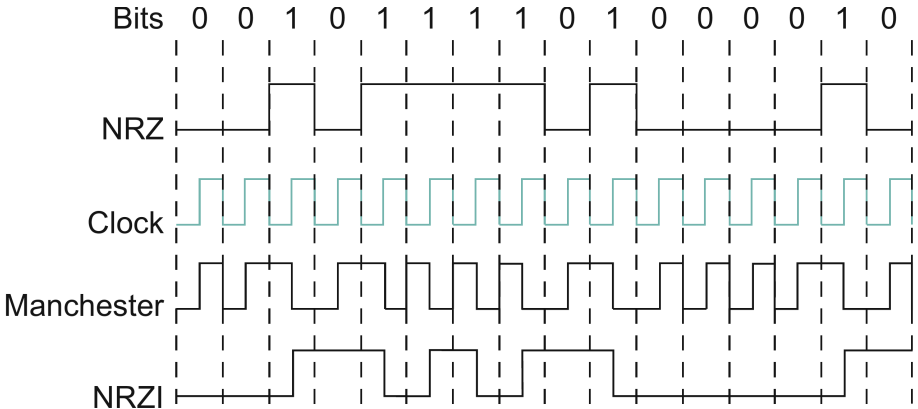


Codificación



- Se descartaron NRZ y NRZI.

Codificación



- Se descartaron NRZ y NRZI.

Para 10 Mbps se implementó Manchester. El problema es que duplica las transiciones.

Codificación 4B/5B para 100Mbps

4-Bit Data Symbol	5-Bit Code
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.
- A estas velocidades de transmisión 4B/5B se volvió insuficiente.

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.
- A estas velocidades de transmisión 4B/5B se volvió insuficiente.
- 8B/10B es la codificación elegida. Cada Trama de 8 bits se reemplaza por una de 10 bits.

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.
- A estas velocidades de transmisión 4B/5B se volvió insuficiente.
- 8B/10B es la codificación elegida. Cada Trama de 8 bits se reemplaza por una de 10 bits.
- Dicho de otro modo transforma los 256 posibles valores en otros que se seleccionan desde 1024 posibles.

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.
- A estas velocidades de transmisión 4B/5B se volvió insuficiente.
- 8B/10B es la codificación elegida. Cada Trama de 8 bits se reemplaza por una de 10 bits.
- Dicho de otro modo transforma los 256 posibles valores en otros que se seleccionan desde 1024 posibles.
- Restricciones: No tener mas de 5 ’0’s o 5 ’1’s consecutivos.

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.
- A estas velocidades de transmisión 4B/5B se volvió insuficiente.
- 8B/10B es la codificación elegida. Cada Trama de 8 bits se reemplaza por una de 10 bits.
- Dicho de otro modo transforma los 256 posibles valores en otros que se seleccionan desde 1024 posibles.
- Restricciones: No tener mas de 5 ’0’s o 5 ’1’s consecutivos.
- Se usa 8B/10B?

8B/10B

- Giga Ethernet arranca con tramas de velocidad de 1Gbps, y actualmente se llega a 10Gbps.
- A estas velocidades de transmisión 4B/5B se volvió insuficiente.
- 8B/10B es la codificación elegida. Cada Trama de 8 bits se reemplaza por una de 10 bits.
- Dicho de otro modo transforma los 256 posibles valores en otros que se seleccionan desde 1024 posibles.
- Restricciones: No tener mas de 5 ’0’s o 5 ’1’s consecutivos.
- Se usa 8B/10B?

- Serial Advanced Technology Attachment
- Serial Attached SCSI
- Fibre Channel
- PCI Express
- IEEE 1394b
- Gigabit Ethernet (excepto para par trenzado 1000Base-T)
- InfiniBand
- DVB
- HyperTransport
- DVI
- HDMI
- USB v3

8B/10B

- Si hay 1024 valores posibles al utilizar códigos de 10 bits, sólo se emplean aquellos que tienen un número similar de ceros y unos. Son tres posibilidades de acuerdo con una propiedad denominada disparidad (diferencia entre ´ 0's y '1's):

8B/10B

- Si hay 1024 valores posibles al utilizar códigos de 10 bits, sólo se emplean aquellos que tienen un número similar de ceros y unos. Son tres posibilidades de acuerdo con una propiedad denominada disparidad (diferencia entre ´ 0's y '1's):
- Códigos con 5 unos y 5 ceros (disparidad neutra).

8B/10B

- Si hay 1024 valores posibles al utilizar códigos de 10 bits, sólo se emplean aquellos que tienen un número similar de ceros y unos. Son tres posibilidades de acuerdo con una propiedad denominada disparidad (diferencia entre ´ 0's y '1's):
- Códigos con 5 unos y 5 ceros (disparidad neutra).
- Códigos con 6 unos y 4 ceros (disparidad positiva).

8B/10B

- Si hay 1024 valores posibles al utilizar códigos de 10 bits, sólo se emplean aquellos que tienen un número similar de ceros y unos. Son tres posibilidades de acuerdo con una propiedad denominada disparidad (diferencia entre ´ 0's y '1's):
- Códigos con 5 unos y 5 ceros (disparidad neutra).
- Códigos con 6 unos y 4 ceros (disparidad positiva).
- Códigos con 4 unos y 6 ceros (disparidad negativa).

8B/10B

- Si hay 1024 valores posibles al utilizar códigos de 10 bits, sólo se emplean aquellos que tienen un número similar de ceros y unos. Son tres posibilidades de acuerdo con una propiedad denominada disparidad (diferencia entre ´ 0's y '1's):
- Códigos con 5 unos y 5 ceros (disparidad neutra).
- Códigos con 6 unos y 4 ceros (disparidad positiva).
- Códigos con 4 unos y 6 ceros (disparidad negativa).
- Disparidad pequeña o nula ocasiona que el nivel de la componente continua de la señal eléctrica sea nulo permanentemente.

Algoritmo de transmisión

- Si el adaptador de red encuentra la línea disponible (No Carrier), transmite directamente sin negociación alguna su frame.

Algoritmo de transmisión

- Si el adaptador de red encuentra la línea disponible (No Carrier), transmite directamente sin negociación alguna su frame.
- El frame tiene a lo sumo 1500 bytes. Esto representa su máximo tiempo en el medio de transmisión

Algoritmo de transmisión

- Si el adaptador de red encuentra la línea disponible (No Carrier), transmite directamente sin negociación alguna su frame.
- El frame tiene a lo sumo 1500 bytes. Esto representa su máximo tiempo en el medio de transmisión
- Si el adaptador detecta una portadora en el medio de transmisión se inhibe de transmitir.

Algoritmo de transmisión

- Si el adaptador de red encuentra la línea disponible (No Carrier), transmite directamente sin negociación alguna su frame.
- El frame tiene a lo sumo 1500 bytes. Esto representa su máximo tiempo en el medio de transmisión
- Si el adaptador detecta una portadora en el medio de transmisión se inhibe de transmitir.
- Una vez que la línea queda si portadora antes de transmitir introduce un delay de 9,6 μseg. (espacio entre frames a 10 Mbps).

Algoritmo de transmisión

- Si el adaptador de red encuentra la línea disponible (No Carrier), transmite directamente sin negociación alguna su frame.
- El frame tiene a lo sumo 1500 bytes. Esto representa su máximo tiempo en el medio de transmisión
- Si el adaptador detecta una portadora en el medio de transmisión se inhibe de transmitir.
- Una vez que la línea queda si portadora antes de transmitir introduce un delay de 9,6 μseg. (espacio entre frames a 10 Mbps).
- Transcurrido este lapso, si existe en la estación un paquete de datos esperando para su transmisión, la estación inicia su transmisión.

Algoritmo de transmisión

- Si el adaptador de red encuentra la línea disponible (No Carrier), transmite directamente sin negociación alguna su frame.
- El frame tiene a lo sumo 1500 bytes. Esto representa su máximo tiempo en el medio de transmisión
- Si el adaptador detecta una portadora en el medio de transmisión se inhibe de transmitir.
- Una vez que la línea queda si portadora antes de transmitir introduce un delay de 9,6 μseg. (espacio entre frames a 10 Mbps).
- Transcurrido este lapso, si existe en la estación un paquete de datos esperando para su transmisión, la estación inicia su transmisión.
- Si la estación no tiene datos para transmitir, reinicia la actividad de sensado de portadora.

Colisiones

Colisiones

- El tiempo de propagación del medio, es 0,65 veces en los cables de par de cobre trenzado.

Colisiones

- El tiempo de propagación del medio, es 0,65 veces en los cables de par de cobre trenzado.
- Una estación que necesita transmitir, lo hará siempre que haya detectado ausencia de portadora. Sin embargo, no puede conocer el estado de encolamiento de frames para transmitir en las restantes estaciones.

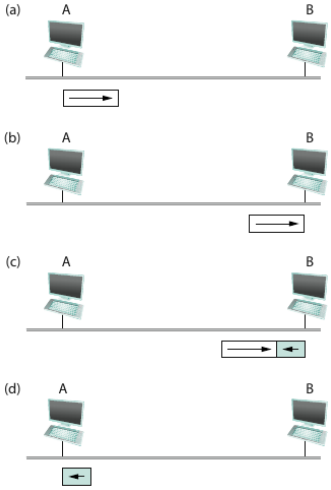
Colisiones

- El tiempo de propagación del medio, es 0,65 veces en los cables de par de cobre trenzado.
- Una estación que necesita transmitir, lo hará siempre que haya detectado ausencia de portadora. Sin embargo, no puede conocer el estado de encolamiento de frames para transmitir en las restantes estaciones.
- Este pequeño delay, es suficiente como para que las estaciones que en un instante t_0 sensan presencia de portadora no lleguen a recibir, el dato que una estación pone en el medio para iniciar su transmisión en ese mismo instante t_0. El mismo será recibido por estas en $t_0 + \delta$, en donde δ es un tiempo proporcional a la distancia en metros de cada estación.

Colisiones

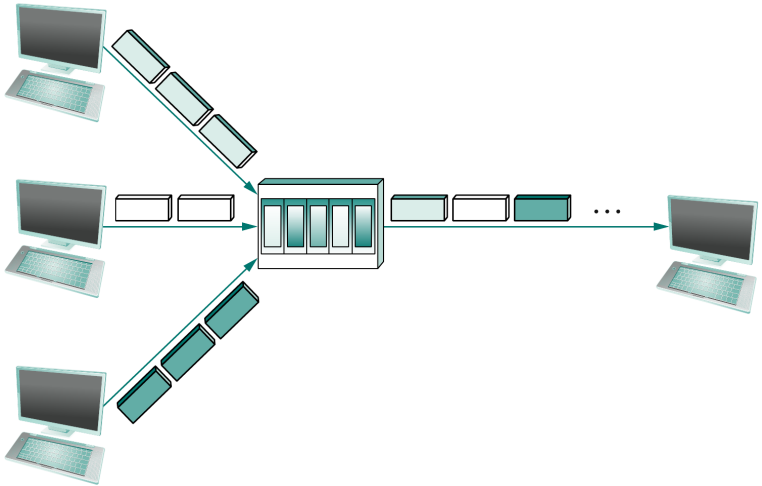
- El tiempo de propagación del medio, es 0,65 veces en los cables de par de cobre trenzado.
- Una estación que necesita transmitir, lo hará siempre que haya detectado ausencia de portadora. Sin embargo, no puede conocer el estado de encolamiento de frames para transmitir en las restantes estaciones.
- Este pequeño delay, es suficiente como para que las estaciones que en un instante t_0 sensan presencia de portadora no lleguen a recibir, el dato que una estación pone en el medio para iniciar su transmisión en ese mismo instante t_0. El mismo será recibido por estas en $t_0 + \delta$, en donde δ es un tiempo proporcional a la distancia en metros de cada estación.
- Por lo tanto y a pesar del Sensado de Portadora antes de transmitir..., ocurren colisiones

Frame Ethernet

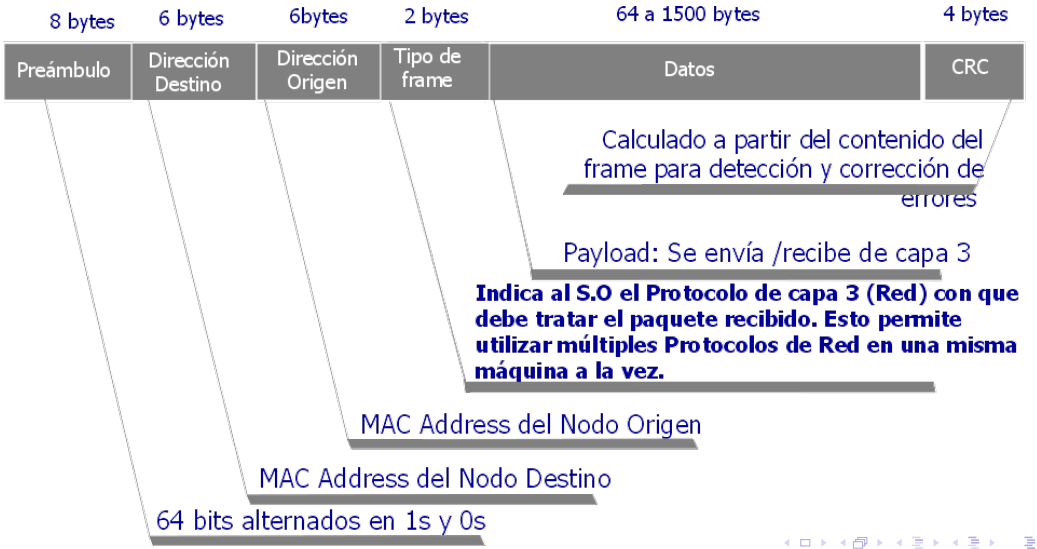


Topología Moderna

Objetivo: Eliminar las colisiones

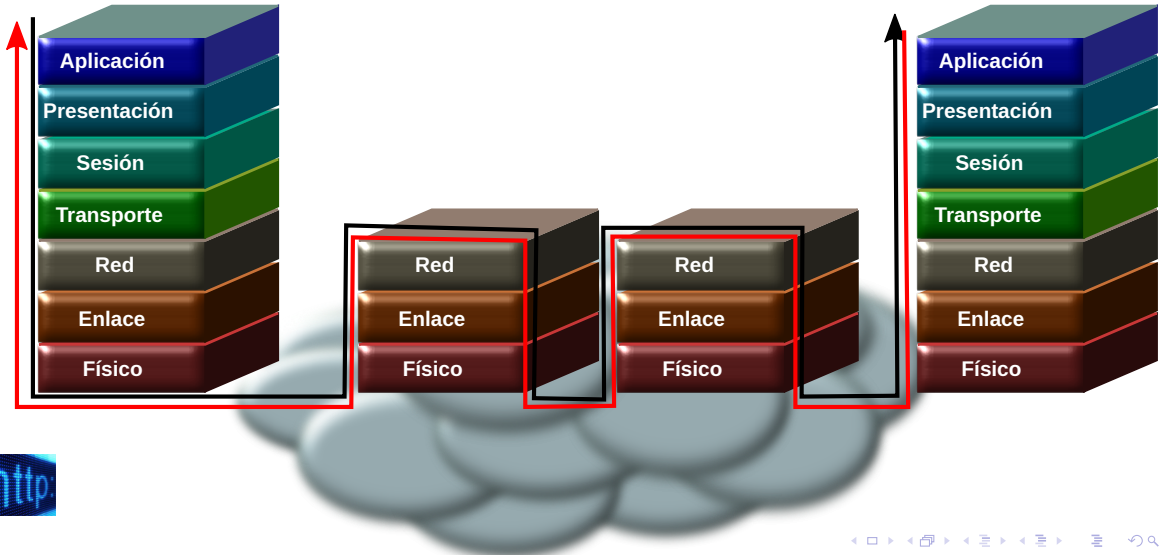


Frame Ethernet

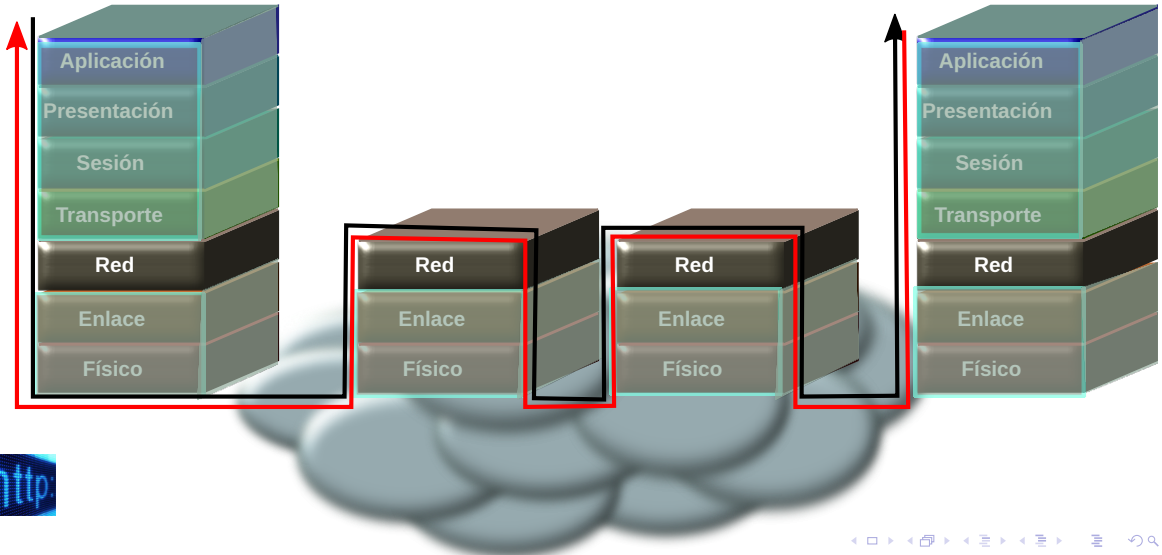


Temario

Modelo de capas



Modelo de capas



Características fundamentales

- Para identificar unívocamente a cada nodo en una red el sistema de comunicaciones le asigna a cada nodo una dirección.

Características fundamentales

- Para identificar unívocamente a cada nodo en una red el sistema de comunicaciones le asigna a cada nodo una dirección.
- En el layer 3 del modelo OSI una dirección de red permite identificar a un nodo en una internet (en una red de redes).

Características fundamentales

- Para identificar unívocamente a cada nodo en una red el sistema de comunicaciones le asigna a cada nodo una dirección.
- En el layer 3 del modelo OSI una dirección de red permite identificar a un nodo en una internet (en una red de redes).
- Cada red que conforma la internet tiene un rango de direcciones, de modo que estas no se repitan a lo largo de la internet (unívoca!!).

Características fundamentales

- Para identificar unívocamente a cada nodo en una red el sistema de comunicaciones le asigna a cada nodo una dirección.
- En el layer 3 del modelo OSI una dirección de red permite identificar a un nodo en una internet (en una red de redes).
- Cada red que conforma la internet tiene un rango de direcciones, de modo que estas no se repitan a lo largo de la internet (unívoca!!).
- La dirección es un número. Por ejemplo, en el caso del protocolo IPv4 (Internet Protocol versión 4), una dirección de red es, como veremos, un número de 32 bits.

TCP/IP

Antecedentes

La suite de protocolos TCP/IP permite comunicar computadores de cualquier tamaño, fabricante, tecnología, aún si son administradas por diferentes sistemas operativos.
Desarrollado por DARPA (Defense Advanced Research Project Agency) a fines de 1960, se convierte en los años 90 en el protocolo por excelencia al sostener el desarrollo de Internet

Protocolo IP

La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.

Formato de la dirección IP

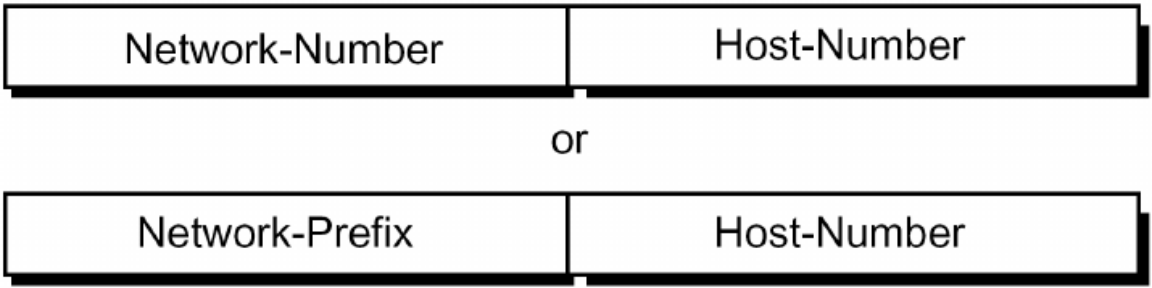
- Notación “punto”: Representa a la dirección IP mediante los cuatro números entre 0 y 255, separados por el punto decimal. Ej 200.35.144.21.

Formato de la dirección IP

- Notación “punto”: Representa a la dirección IP mediante los cuatro números entre 0 y 255, separados por el punto decimal. Ej 200.35.144.21.
- Esta dirección IP de cuatro números se subdividen en dos campos.

Formato de la dirección IP

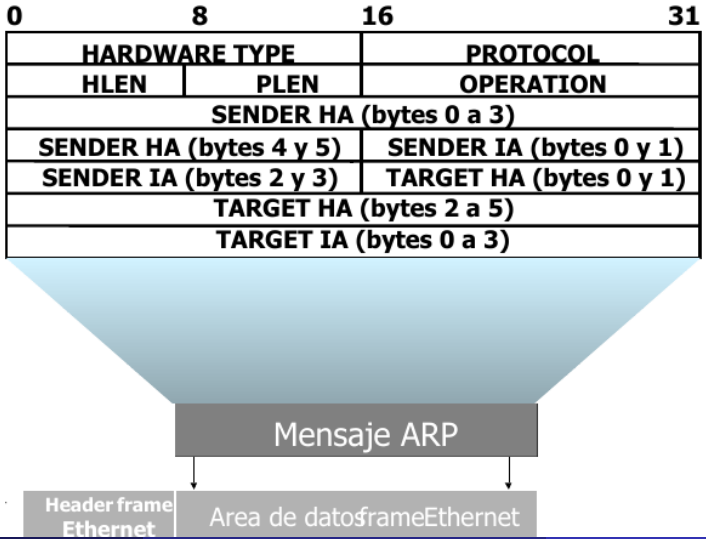
- Notación “punto”: Representa a la dirección IP mediante los cuatro números entre 0 y 255, separados por el punto decimal. Ej 200.35.144.21.
- Esta dirección IP de cuatro números se subdividen en dos campos.



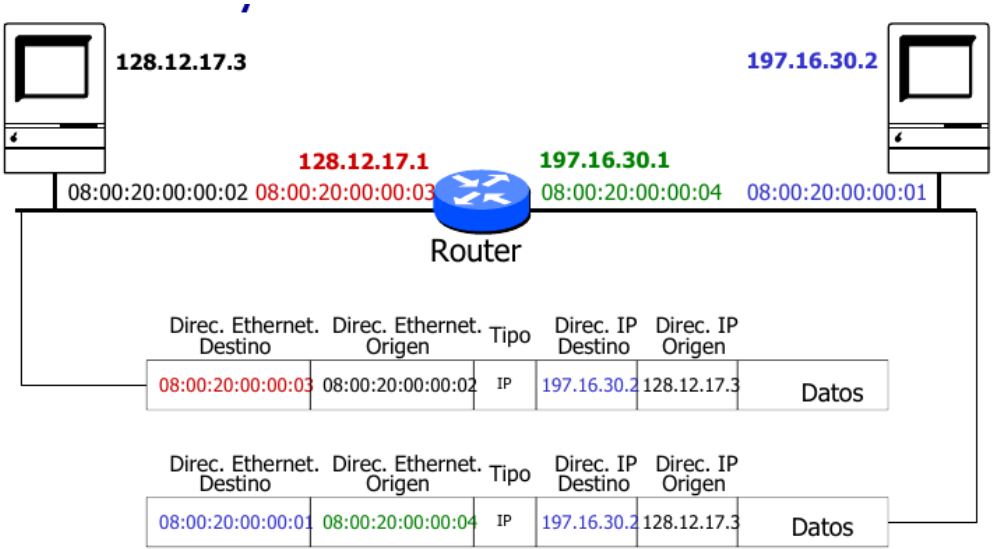
Aunque estemos en capa 3 se necesita la MAC Address

- Se trata de conectar máquinas a nivel de una red en la capa, 2.
- Pero la búsqueda parte de una aplicación.
- Es relativamente fácil determinar la IP del nodo destino. Ya que en una internet el esquema de addressing de capa 3 está muy bien organizado. Es lógico tratándose de un esquema homogéneo de direccionamiento.
- No obstante en las diferentes redes por las que viaje el paquete es necesario que se pueda conocer la MAC destino.
- Una internet se puede componer de redes de diferente tecnología de capa 2.
- ¿Entonces?

Protocolo ARP



Uso de ARP. Ejemplo con router incluido



Protocolo IP

- La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.

Protocolo IP

- La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.
- En TCP/IP este servicio es brindado por el protocolo IP. Es un servicio de tipo Best Effort

Protocolo IP

- La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.
- En TCP/IP este servicio es brindado por el protocolo IP. Es un servicio de tipo Best Effort
- No garantiza que la información llegue a destino.

Protocolo IP

- La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.
- En TCP/IP este servicio es brindado por el protocolo IP. Es un servicio de tipo Best Effort
- No garantiza que la información llegue a destino.
- Los paquetes podrían ser descartados por congestión en la red o corrupción de los datos.

Protocolo IP

- La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.
- En TCP/IP este servicio es brindado por el protocolo IP. Es un servicio de tipo Best Effort
- No garantiza que la información llegue a destino.
- Los paquetes podrían ser descartados por congestión en la red o corrupción de los datos.
- La capa 3 (Red) se encarga entonces, de permitir a los paquetes llegar a destino salvando por ejemplo, las diferencias de tecnolo de redes intermedias que deban atravesar.

Protocolo IP

- La Capa 3 definida en los modelos OSI y DARPA permite a un nodo origen, alcanzar a un nodo destino, conociendo su dirección de red.
- En TCP/IP este servicio es brindado por el protocolo IP. Es un servicio de tipo Best Effort
- No garantiza que la información llegue a destino.
- Los paquetes podrían ser descartados por congestión en la red o corrupción de los datos.
- La capa 3 (Red) se encarga entonces, de permitir a los paquetes llegar a destino salvando por ejemplo, las diferencias de tecnolo de redes intermedias que deban atravesar.
- Sobre el datagrama IP, ya en la capa 4, veremos que se montan diferentes tipos de servicios.

Organización de direcciones IP

- Internic es el organismo internacional encargado de administrar la asignación de direcciones IP públicas para Internet.

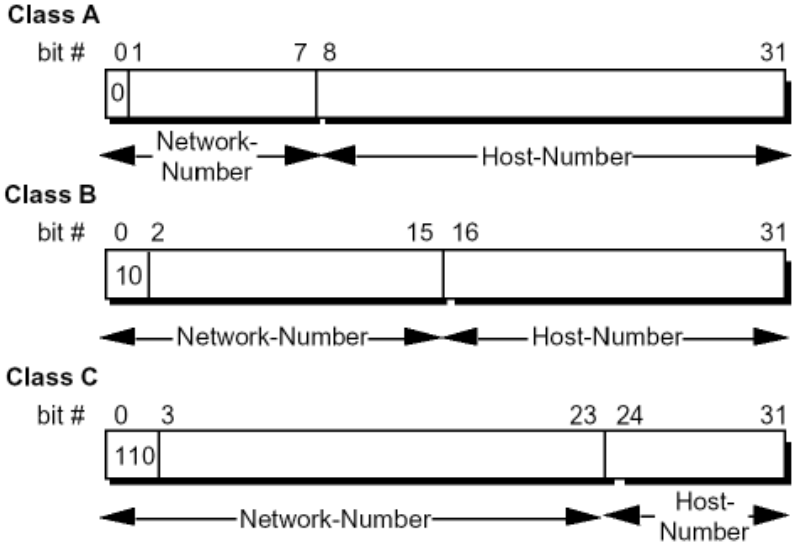
Organización de direcciones IP

- Internic es el organismo internacional encargado de administrar la asignación de direcciones IP públicas para Internet.
- Internic dividió el espacio de direcciones en **clases** de acuerdo a los tamaños de los campos Network Number y Host Number

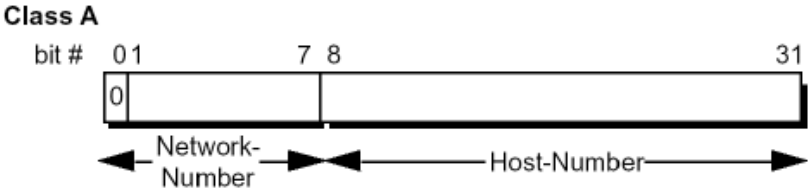
Organización de direcciones IP

- Internic es el organismo internacional encargado de administrar la asignación de direcciones IP públicas para Internet.
- Internic dividió el espacio de direcciones en **clases** de acuerdo a los tamaños de los campos Network Number y Host Number
- Los operadores compran estas direcciones (redes completas) para su propio uso o para asignarlas a sus clientes.

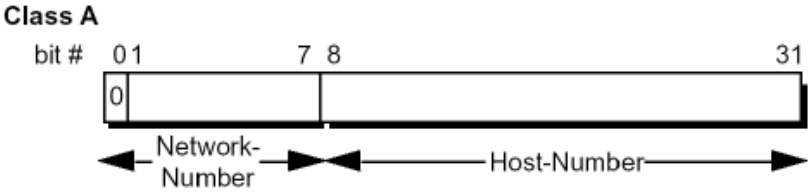
Esquema de direccionamiento



Redes clase A

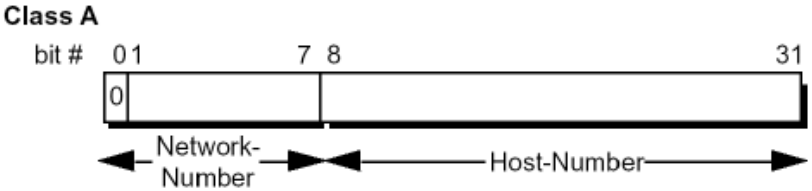


Redes clase A



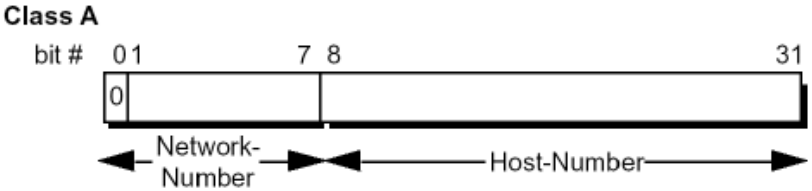
- Comienzan con un bit en ’0’.

Redes clase A



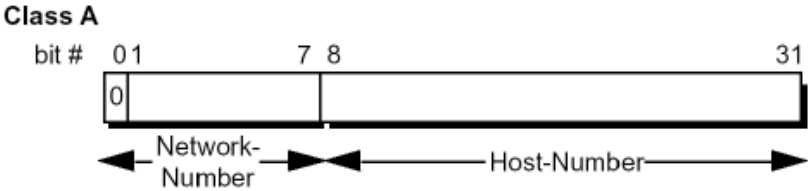
- Comienzan con un bit en '0'.
- Como el ***Network Prefix*** es de 8 bits (el mas significativo en 0), se las nombre en forma reducida como /8, y solo hay 126 redes Clase A (La red 127 no se utiliza ya que se asigna a la dirección localhost 127.0.0.1). Rango: 1.xxx.xxx.xxx a 126.xxx.xxx.xxx

Redes clase A



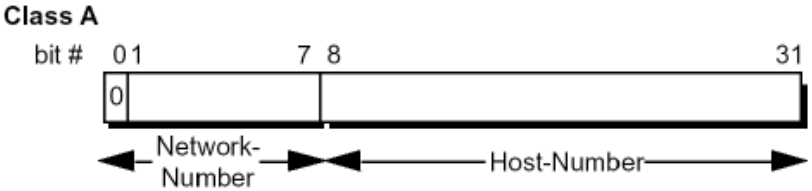
- Comienzan con un bit en '0'.
- Como el ***Network Prefix*** es de 8 bits (el mas significativo en 0), se las nombre en forma reducida como /8, y solo hay 126 redes Clase A (La red 127 no se utiliza ya que se asigna a la dirección localhost 127.0.0.1). Rango: 1.xxx.xxx.xxx a 126.xxx.xxx.xxx
- Cada red puede alojar hasta $2^{24} - 2$ hosts.

Redes clase A



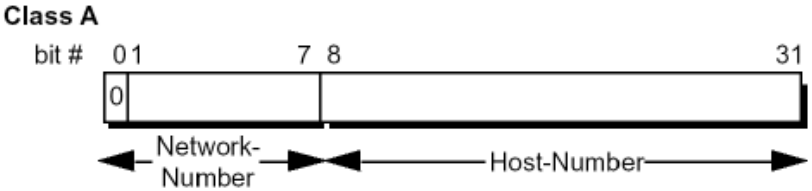
- Comienzan con un bit en '0'.
- Como el ***Network Prefix*** es de 8 bits (el mas significativo en 0), se las nombre en forma reducida como /8, y solo hay 126 redes Clase A (La red 127 no se utiliza ya que se asigna a la dirección localhost 127.0.0.1). Rango: 1.xxx.xxx.xxx a 126.xxx.xxx.xxx
- Cada red puede alojar hasta $2^{24} - 2$ hosts.
  - la dirección X.0.0.0 corresponde a la dirección de la Red.

Redes clase A



- Comienzan con un bit en '0'.
- Como el ***Network Prefix*** es de 8 bits (el mas significativo en 0), se las nombre en forma reducida como /8, y solo hay 126 redes Clase A (La red 127 no se utiliza ya que se asigna a la dirección localhost 127.0.0.1). Rango: 1.xxx.xxx.xxx a 126.xxx.xxx.xxx
- Cada red puede alojar hasta $2^{24} - 2$ hosts.
  - la dirección X.0.0.0 corresponde a la dirección de la Red.
  - la dirección X.255.255.255 es la broadcast (permite enviar un solo mensaje y que lo reciban todos los nodos

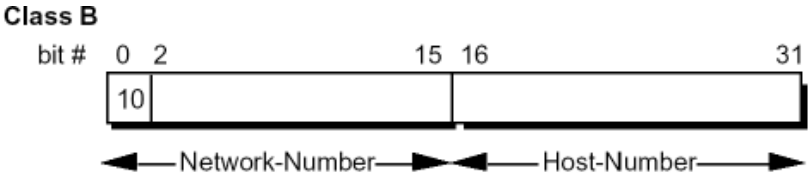
Redes clase A



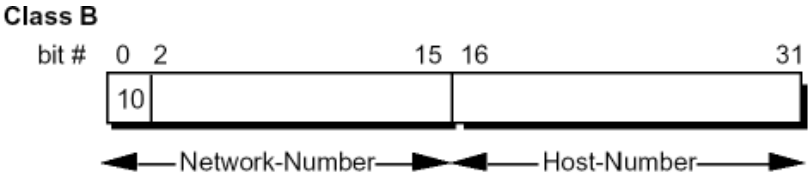
- Comienzan con un bit en '0'.
- Como el ***Network Prefix*** es de 8 bits (el mas significativo en 0), se las nombre en forma reducida como /8, y solo hay 126 redes Clase A (La red 127 no se utiliza ya que se asigna a la dirección localhost 127.0.0.1). Rango: 1.xxx.xxx.xxx a 126.xxx.xxx.xxx
- Cada red puede alojar hasta $2^{24} - 2$ hosts.
  - la dirección X.0.0.0 corresponde a la dirección de la Red.
  - la dirección X.255.255.255 es la broadcast (permite enviar un solo mensaje y que lo reciban todos los nodos

- 126 redes consumen la mitad del rango de direcciones.

Redes clase B

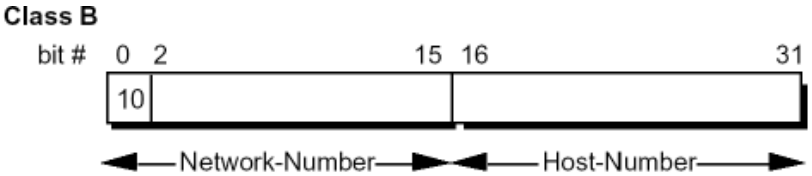


Redes clase B



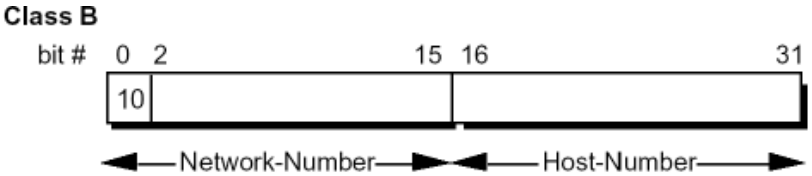
- Comienzan con ’10’.

Redes clase B



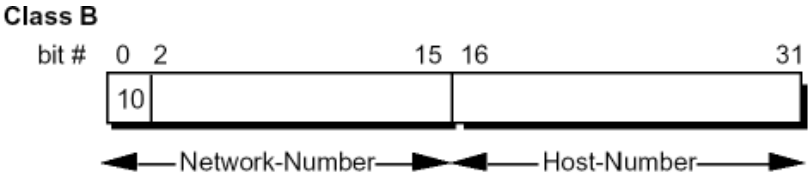
- Comienzan con ’10’.
- Como el ***Network Prefix*** es de 16 bits, se las nombre en forma reducida como /16, y hay 16.384 redes Clase B (los dos mas significativos siempre valen ’10’). Rango 128.0.xxx.xxx a 191.255.xxx.xxx

Redes clase B



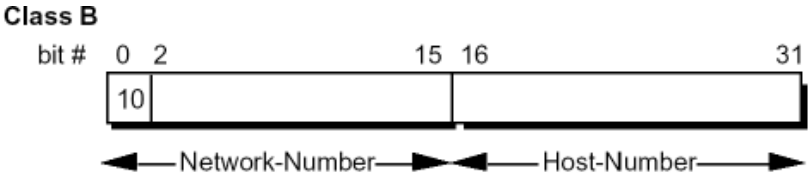
- Comienzan con ’10’.
- Como el ***Network Prefix*** es de 16 bits, se las nombre en forma reducida como /16, y hay 16.384 redes Clase B (los dos mas significativos siempre valen ’10’). Rango 128.0.xxx.xxx a 191.255.xxx.xxx
- Cada red puede alojar hasta $2^{16} - 2$ hosts.

Redes clase B



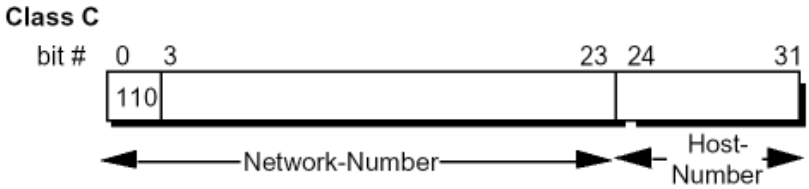
- Comienzan con ’10’.
- Como el ***Network Prefix*** es de 16 bits, se las nombre en forma reducida como /16, y hay 16.384 redes Clase B (los dos mas significativos siempre valen ’10’). Rango 128.0.xxx.xxx a 191.255.xxx.xxx
- Cada red puede alojar hasta $2^{16} - 2$ hosts.
  - la dirección X.X.0.0 corresponde a la dirección de la Red.

Redes clase B

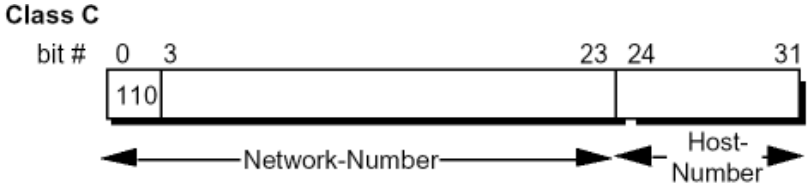


- Comienzan con ’10’.
- Como el ***Network Prefix*** es de 16 bits, se las nombre en forma reducida como /16, y hay 16.384 redes Clase B (los dos mas significativos siempre valen ’10’). Rango 128.0.xxx.xxx a 191.255.xxx.xxx
- Cada red puede alojar hasta $2^{16} - 2$ hosts.
  - la dirección X.X.0.0 corresponde a la dirección de la Red.
  - la dirección X.X.255.255 es la broadcast (permite enviar un solo mensaje y que lo reciban todos los nodos

Redes clase C

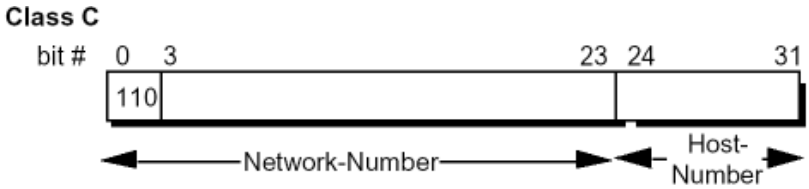


Redes clase C



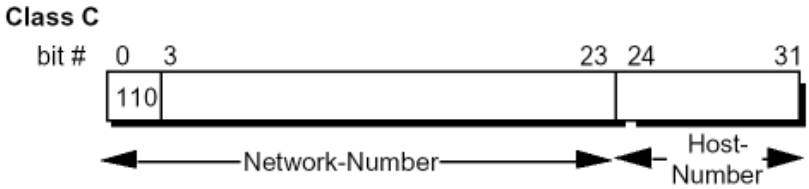
- Comienzan con ’110’.

Redes clase C



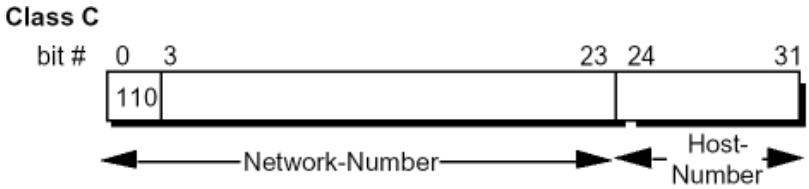
- Comienzan con ’110’.
- Como el ***Network Prefix*** es de 24 bits, se las nombre en forma reducida como /24, y hay 2.097.152 redes Clase C (los tres mas significativos siempre valen ’110’). –Rango: 192.0.0.xxx a 223.255.255.xxx

Redes clase C



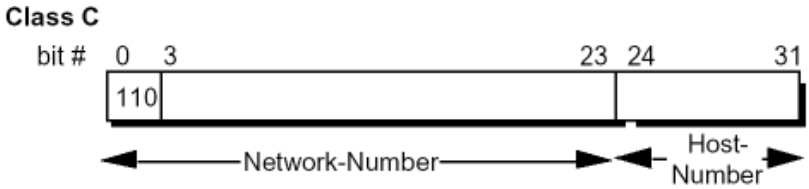
- Comienzan con ’110’.
- Como el ***Network Prefix*** es de 24 bits, se las nombre en forma reducida como /24, y hay 2.097.152 redes Clase C (los tres mas significativos siempre valen ’110’). –Rango: 192.0.0.xxx a 223.255.255.xxx
- Cada red puede alojar hasta $2^8 - 2$ hosts.

Redes clase C



- Comienzan con ’110’.
- Como el ***Network Prefix*** es de 24 bits, se las nombre en forma reducida como /24, y hay 2.097.152 redes Clase C (los tres mas significativos siempre valen ’110’). –Rango: 192.0.0.xxx a 223.255.255.xxx
- Cada red puede alojar hasta $2^8 - 2$ hosts.
  - la dirección X.X.X.0 corresponde a la dirección de la Red.

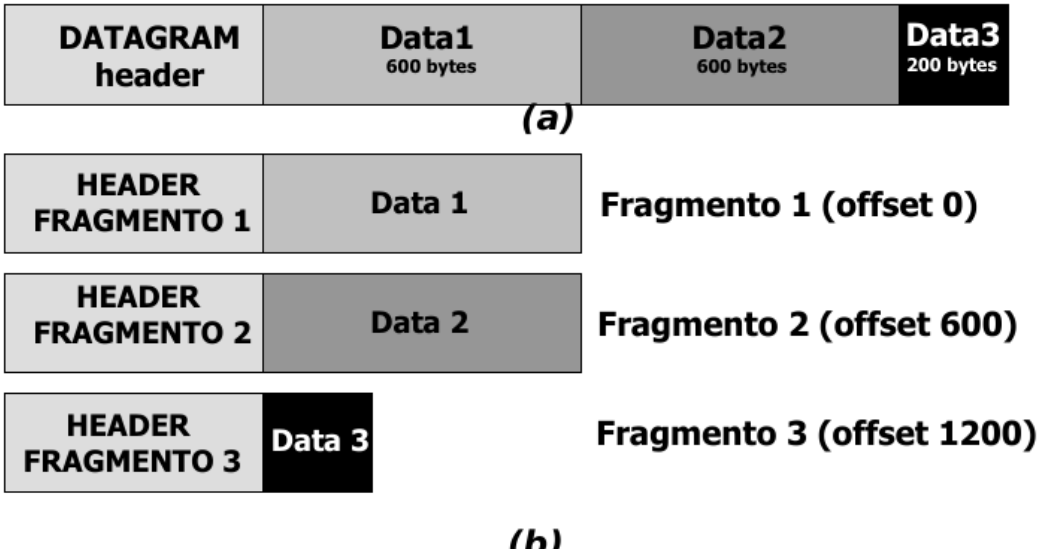
Redes clase C



- Comienzan con ’110’.
- Como el ***Network Prefix*** es de 24 bits, se las nombre en forma reducida como /24, y hay 2.097.152 redes Clase C (los tres mas significativos siempre valen ’110’). –Rango: 192.0.0.xxx a 223.255.255.xxx
- Cada red puede alojar hasta $2^8 - 2$ hosts.
  - la dirección X.X.X.0 corresponde a la dirección de la Red.
  - la dirección X.X.X.255 es la broadcast (permite enviar un solo mensaje y que lo reciban todos los nodos

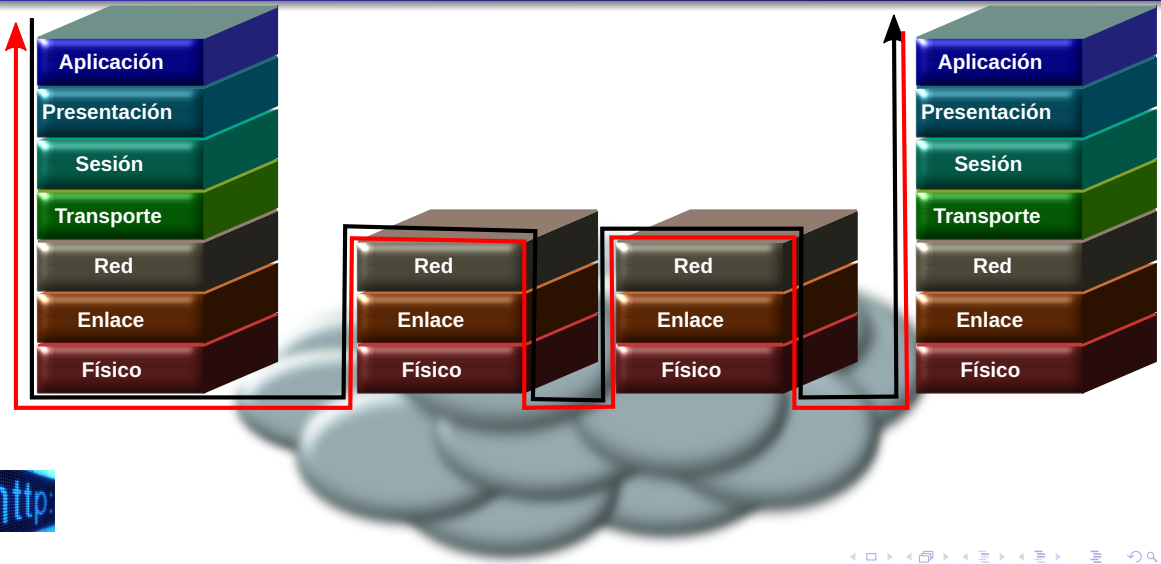
Formato del Header IP

Fragmentación de un paquete

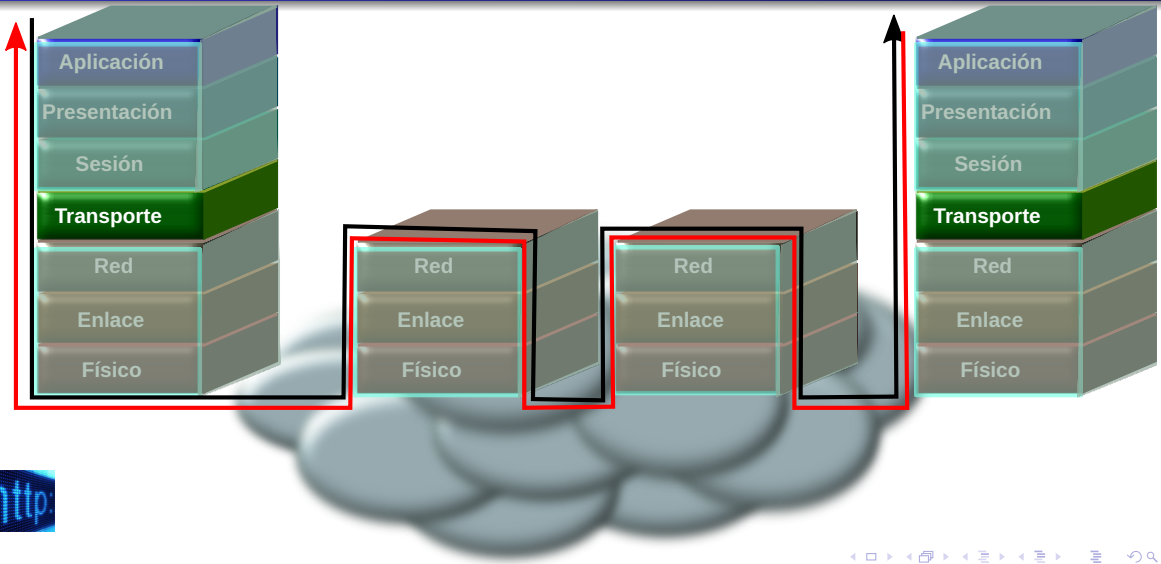


Temario

Modelo de capas



Nos concentraremos en la capa de Transporte



Problemática de la capa de Transporte

Comunicación proceso-proceso

Problemática de la capa de Transporte

Comunicación proceso-proceso

- Las capas 1 a 3 del modelo de comunicaciones se ocuparon de asegurar conexión host-host, libre de errores.

Problemática de la capa de Transporte

Comunicación proceso-proceso

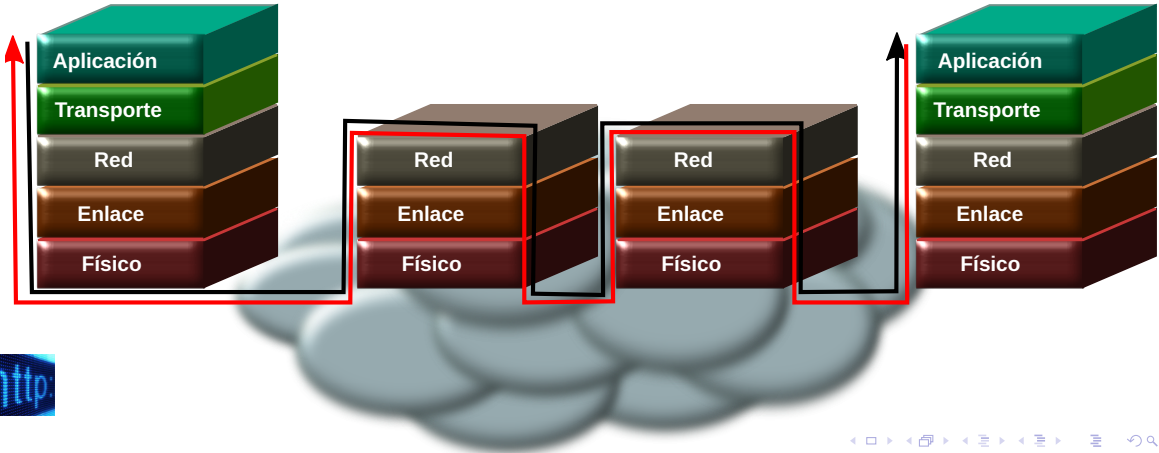
- Las capas 1 a 3 del modelo de comunicaciones se ocuparon de asegurar conexión host-host, libre de errores.
- Rol la capa de Transporte: asegurar la comunicación proceso - proceso.

Problemática de la capa de Transporte

Comunicación proceso-proceso

- Las capas 1 a 3 del modelo de comunicaciones se ocuparon de asegurar conexión host-host, libre de errores.
- Rol la capa de Transporte: asegurar la comunicación proceso - proceso.
- Provee un canal de comunicaciones entre los procesos extremo de la comunicación $=>$ *Protocolos End To End*.

Modelo de capas



Temario

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.
- Los sistemas operativos proveen un ID a cada proceso. Típicamente se denomina PID (por Process ID).

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.
- Los sistemas operativos proveen un ID a cada proceso. Típicamente se denomina PID (por Process ID).
- Para independizarse del Sistema Operativo en el que trabaje cada extremo de la comunicación, en TCP/IP se ha definido en la capa de Transporte una entidad abstracta denominada ***port***, que permitirá identificar de manera indirecta un proceso.

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.
- Los sistemas operativos proveen un ID a cada proceso. Típicamente se denomina PID (por Process ID).
- Para independizarse del Sistema Operativo en el que trabaje cada extremo de la comunicación, en TCP/IP se ha definido en la capa de Transporte una entidad abstracta denominada ***port***, que permitirá identificar de manera indirecta un proceso.
- Identificar procesos con independencia del S.O.: $\rightarrow$ ***port***

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.
- Los sistemas operativos proveen un ID a cada proceso. Típicamente se denomina PID (por Process ID).
- Para independizarse del Sistema Operativo en el que trabaje cada extremo de la comunicación, en TCP/IP se ha definido en la capa de Transporte una entidad abstracta denominada ***port***, que permitirá identificar de manera indirecta un proceso.
- Identificar procesos con independencia del S.O.: $\rightarrow$ ***port***
- Existe una relación biunívoca ***port*** $<->$ proceso.

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.
- Los sistemas operativos proveen un ID a cada proceso. Típicamente se denomina PID (por Process ID).
- Para independizarse del Sistema Operativo en el que trabaje cada extremo de la comunicación, en TCP/IP se ha definido en la capa de Transporte una entidad abstracta denominada ***port***, que permitirá identificar de manera indirecta un proceso.
- Identificar procesos con independencia del S.O.: $\rightarrow$ ***port***
- Existe una relación biunívoca ***port*** $<->$ proceso.
- Para relacionar ***port*** con proceso, cada Sistema Operativo tiene por lo general un archivo de configuración llamado `services` (en Linux este archivo está en el directorio `/etc`).

Intercomunicando procesos

- Se requiere un mecanismo que permita identificar a los procesos en cada nodo.
- Los sistemas operativos proveen un ID a cada proceso. Típicamente se denomina PID (por Process ID).
- Para independizarse del Sistema Operativo en el que trabaje cada extremo de la comunicación, en TCP/IP se ha definido en la capa de Transporte una entidad abstracta denominada ***port***, que permitirá identificar de manera indirecta un proceso.
- Identificar procesos con independencia del S.O.: $\rightarrow$ ***port***
- Existe una relación biunívoca ***port*** $<->$ proceso.
- Para relacionar ***port*** con proceso, cada Sistema Operativo tiene por lo general un archivo de configuración llamado `services` (en Linux este archivo está en el directorio `/etc`).

Un proceso origen envía mensajes a un ***port***, y el proceso destino recoge sus mensajes de un ***port***.

Relación entre port y proceso: /etc/services

Formato:

```
service name  port/protocol  [aliases]
```

Relación entre port y proceso: /etc/services

Formato:

```
service name  port/protocol  [aliases]
```

```
ftp             21/tcp
ssh             22/tcp                  # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
nameserver      42/tcp          name    # IEN 116
whois           43/tcp          nicname
domain          53/tcp                  # Domain Name Server
domain          53/udp
http            80/tcp          www     # WorldWideWeb HTTP
http            80/udp                  # HyperText Transfer Protocol
pop3            110/tcp         pop-3   # POP version 3
pop3            110/udp         pop-3
https           443/tcp                 # http protocol over TLS/SSL
https           443/udp
```

Ports

- Un ***port*** se implementa en un host en internet. No es una entidad dispersa a través de la red.

Ports

- Un ***port*** se implementa en un host en internet. No es una entidad dispersa a través de la red.
- Un servicio se identifica entonces mediante el par (host,port).

Ports

- Un ***port*** se implementa en un host en internet. No es una entidad dispersa a través de la red.
- Un servicio se identifica entonces mediante el par (host,port).
- ***iana*** (Internet Asigned Numbers Authority), es la entidad encargada de estandarizar entre otros, los números de ***port***, asignados.

Ports

- Un ***port*** se implementa en un host en internet. No es una entidad dispersa a través de la red.
- Un servicio se identifica entonces mediante el par (host,port).
- ***iana*** (Internet Asigned Numbers Authority), es la entidad encargada de estandarizar entre otros, los números de ***port***, asignados.
- En: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt, se encuentran los ***ports*** que se han definido para uso standard por el S.O. (*well known ports*) y los que van ganando un uso aceptado en internet.

Temario

Características Principales

- Servicio de byte streaming orientado a conexión y confiable.

Características Principales

- Servicio de byte streaming orientado a conexión y confiable.
- Asegura a la aplicación transmisión libre de errores y en orden.

Características Principales

- Servicio de byte streaming orientado a conexión y confiable.
- Asegura a la aplicación transmisión libre de errores y en orden.
- Comunicación full duplex: un byte stream en cada dirección por conexión.

Características Principales

- Servicio de byte streaming orientado a conexión y confiable.
- Asegura a la aplicación transmisión libre de errores y en orden.
- Comunicación full duplex: un byte stream en cada dirección por conexión.
- Control de flujo: permite en cada momento al receptor, limitar la cantidad de información que un transmisor puede enviarle.

Características Principales

- Servicio de byte streaming orientado a conexión y confiable.
- Asegura a la aplicación transmisión libre de errores y en orden.
- Comunicación full duplex: un byte stream en cada dirección por conexión.
- Control de flujo: permite en cada momento al receptor, limitar la cantidad de información que un transmisor puede enviarle.
- Mecanismo de demultiplexación: diferentes aplicaciones en un mismo host pueden establecer conexiones simultáneamente con sus pares (peers)

Transmisión confiable

Se basa en los siguientes atributos:

Transmisión confiable

Se basa en los siguientes atributos:

- Control de errores

Transmisión confiable

Se basa en los siguientes atributos:

- Control de errores
- Acknowlegement

Transmisión confiable

Se basa en los siguientes atributos:

- Control de errores
- Acknowlegement
- Timeout

End to end issues

1. TCP necesita un mecanismo de establecimiento de conexión para que ambos nodos acepten intercambiar datos entre si.

End to end issues

1. TCP necesita un mecanismo de establecimiento de conexión para que ambos nodos acepten intercambiar datos entre si.
2. El tiempo de loop es altamente variable en una internet.

End to end issues

1. TCP necesita un mecanismo de establecimiento de conexión para que ambos nodos acepten intercambiar datos entre si.
2. El tiempo de loop es altamente variable en una internet.
3. Los paquetes en una internet se desordenan, y en ocasiones se pierden por expiración del TTL especificado en el datagrama IP.

End to end issues

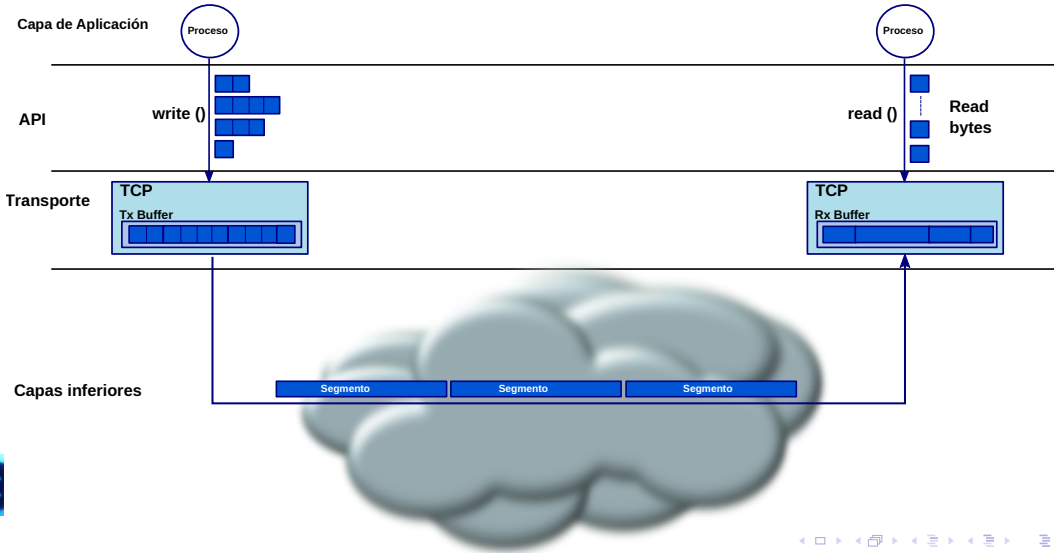
1. TCP necesita un mecanismo de establecimiento de conexión para que ambos nodos acepten intercambiar datos entre si.
2. El tiempo de loop es altamente variable en una internet.
3. Los paquetes en una internet se desordenan, y en ocasiones se pierden por expiración del TTL especificado en el datagrama IP.
4. La cantidad de aplicaciones que utilicen TCP en un nodo, puede variar fuertemente de un momento a otro, afectando los recursos disponibles en un enlace compartido en internet.

End to end issues

1. TCP necesita un mecanismo de establecimiento de conexión para que ambos nodos acepten intercambiar datos entre si.
2. El tiempo de loop es altamente variable en una internet.
3. Los paquetes en una internet se desordenan, y en ocasiones se pierden por expiración del TTL especificado en el datagrama IP.
4. La cantidad de aplicaciones que utilicen TCP en un nodo, puede variar fuertemente de un momento a otro, afectando los recursos disponibles en un enlace compartido en internet.
5. Todo enlace en internet es compartido. Puede congestionarse con cierta facilidad.

Temario

Manejo del byte-stream



Segmentos

- El proceso transmisor, escribe cadenas de bytes de longitud variable acorde con la entrada de datos de la aplicación, en un buffer.

Segmentos

- El proceso transmisor, escribe cadenas de bytes de longitud variable acorde con la entrada de datos de la aplicación, en un buffer.
- El buffer de Transmisión contiene el byte-stream de salida.

Segmentos

- El proceso transmisor, escribe cadenas de bytes de longitud variable acorde con la entrada de datos de la aplicación, en un buffer.
- El buffer de Transmisión contiene el byte-stream de salida.
- TCP divide el byte-stream en segmentos de tamaño fijo.

Segmentos

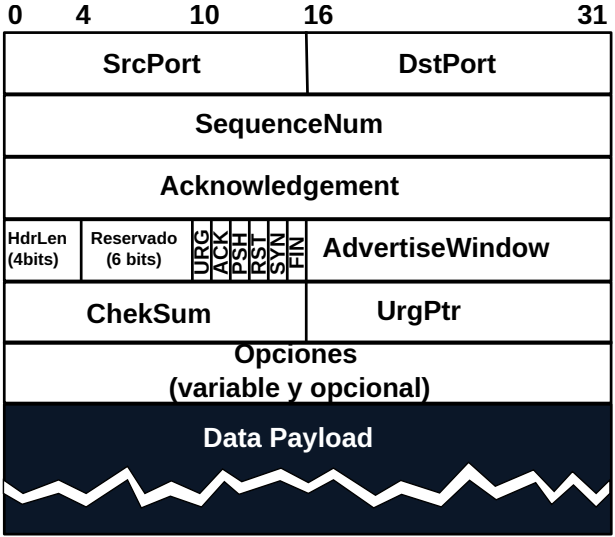
- El proceso transmisor, escribe cadenas de bytes de longitud variable acorde con la entrada de datos de la aplicación, en un buffer.
- El buffer de Transmisión contiene el byte-stream de salida.
- TCP divide el byte-stream en segmentos de tamaño fijo.
- Cada segmento se empaqueta con un encabezado y se envía por la red.

Segmentos

- El proceso transmisor, escribe cadenas de bytes de longitud variable acorde con la entrada de datos de la aplicación, en un buffer.
- El buffer de Transmisión contiene el byte-stream de salida.
- TCP divide el byte-stream en segmentos de tamaño fijo.
- Cada segmento se empaqueta con un encabezado y se envía por la red.
- El lado receptor recibe el contenido del segmento en un Buffer de recepción y el proceso lo lee como un byte stream.

Temario

Encabezamiento



Encabezamiento: Ports

SrcPort Identifica el Port de origen

DstPort Identifica el Port de destino

Coordenadas de una conexión

SrcPort y ***DstPort*** junto con las direcciones IP del nodo origen y del nodo destino, que viajan en el encabezado de la capa 3, identifican una conexión TCP.
Una conexión TCP se puede demultiplexar en cada nodo mediante la tupla (SrcPort, SrcIPAddr, DstPort, DstIPAddr)

Encabezamiento: Números de secuencia

SequenceNum Identifica la posición del primer byte del segmento enviado por el transmisor, dentro del byte-stream total a enviar como sucesión de segmentos. Lo pone el endpoint transmisor en cada paquete que envía.

Encabezamiento: Números de secuencia

SequenceNum Identifica la posición del primer byte del segmento enviado por el transmisor, dentro del byte-stream total a enviar como sucesión de segmentos. Lo pone el endpoint transmisor en cada paquete que envía.

Acknowledgment Identifica la posición del próximo byte que se espera recibir. Es devuelto por el receptor en cada paquete de acknowldge.

Encabezamiento: Números de secuencia

SequenceNum Identifica la posición del primer byte del segmento enviado por el transmisor, dentro del byte-stream total a enviar como sucesión de segmentos. Lo pone el endpoint transmisor en cada paquete que envía.

Acknowledgment Identifica la posición del próximo byte que se espera recibir. Es devuelto por el receptor en cada paquete de acknowldge.

AdvertisedWindow Número de bytes a partir del especificado en Acknowledgment que el receptor aceptará. Por default es 4096. Es anunciado por ambos extremos (endpoints) en el momento de la conexión.

Encabezamiento: Flags

RST Indica que la conexión se ha deteriorado (por ejemplo si se recibe un paquete que no se espera recibir). Su resultado es un reset de la conexión.

Encabezamiento: Flags

RST Indica que la conexión se ha deteriorado (por ejemplo si se recibe un paquete que no se espera recibir). Su resultado es un reset de la conexión.

PUSH EL transmisor invocó una función PUSH la cual debe ser informada al proceso del lado receptor.

Encabezamiento: Flags

RST Indica que la conexión se ha deteriorado (por ejemplo si se recibe un paquete que no se espera recibir). Su resultado es un reset de la conexión.

PUSH EL transmisor invocó una función PUSH la cual debe ser informada al proceso del lado receptor.

URG Indica que el segmento recibido contiene datos urgentes. Estos se ubican al inicio del paquete de datos El campo UrgPtr es válido, e indica donde comienza el bloque de datos no urgentes.

Encabezamiento: Flags

RST Indica que la conexión se ha deteriorado (por ejemplo si se recibe un paquete que no se espera recibir). Su resultado es un reset de la conexión.

PUSH EL transmisor invocó una función PUSH la cual debe ser informada al proceso del lado receptor.

URG Indica que el segmento recibido contiene datos urgentes. Estos se ubican al inicio del paquete de datos El campo UrgPtr es válido, e indica donde comienza el bloque de datos no urgentes.

SYN Inicia una conexión (three way handshake)

Encabezamiento: Flags

RST Indica que la conexión se ha deteriorado (por ejemplo si se recibe un paquete que no se espera recibir). Su resultado es un reset de la conexión.

PUSH EL transmisor invocó una función PUSH la cual debe ser informada al proceso del lado receptor.

URG Indica que el segmento recibido contiene datos urgentes. Estos se ubican al inicio del paquete de datos El campo UrgPtr es válido, e indica donde comienza el bloque de datos no urgentes.

SYN Inicia una conexión (three way handshake)

FIN Finaliza una conexión

Encabezamiento: Flags

RST Indica que la conexión se ha deteriorado (por ejemplo si se recibe un paquete que no se espera recibir). Su resultado es un reset de la conexión.

PUSH EL transmisor invocó una función PUSH la cual debe ser informada al proceso del lado receptor.

URG Indica que el segmento recibido contiene datos urgentes. Estos se ubican al inicio del paquete de datos El campo UrgPtr es válido, e indica donde comienza el bloque de datos no urgentes.

SYN Inicia una conexión (three way handshake)

FIN Finaliza una conexión

ACK Indica que el campo **Acknowledgment** es válido. El receptor deberá prestarle atención.

Encabezamiento: Campos de Control de integridad

HdrLen Es un nibble que contiene la cantidad de palabras de 32 bits que ocupa el encabezado. Vale 5, a menos que el campo opciones tenga información válida.

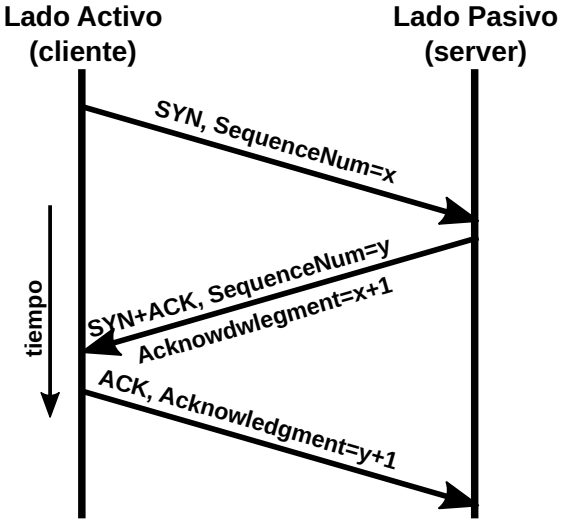
Encabezamiento: Campos de Control de integridad

HdrLen Es un nibble que contiene la cantidad de palabras de 32 bits que ocupa el encabezado. Vale 5, a menos que el campo opciones tenga información válida.

Checksum Contiene el checksum del paquete completo (Header + Datos)

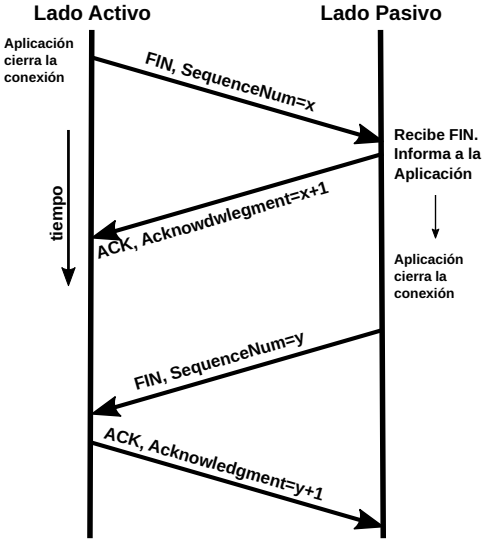
Temario

Establecimiento de una conexión



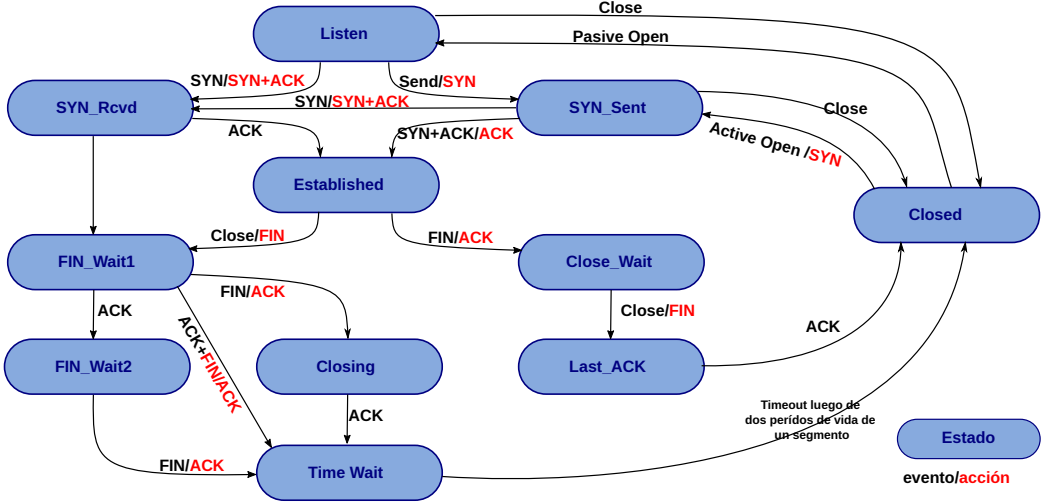
Temario

Cierre de una conexión



Temario

Establecimiento de una conexión



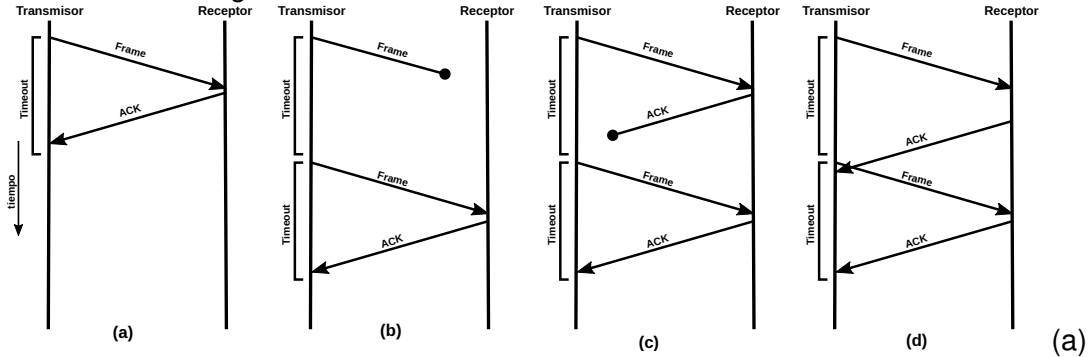
Implementación de Transmisión Confiable

Estado Established

Este estado en el diagrama del slide previo engloba Todo el funcionamiento del protocolo TCP en régimen, es decir, una vez establecida la conexión.
Aquí es donde se ponen de manifiesto en cada transacción los dos parámetros a los que nos referimos previamente al plantear los requisito para lograr una Transmisión confiable.

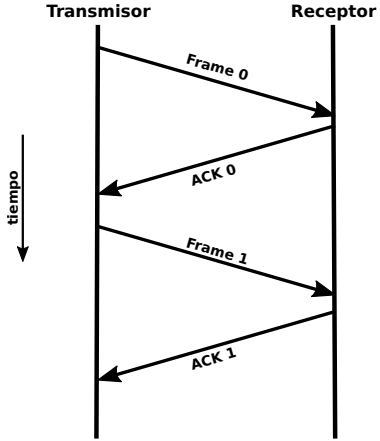
Stop and Wait

La idea es transmitir un frame una vez recibido el ACK del frame previo. Se distinguen los cuatro escenarios siguientes.

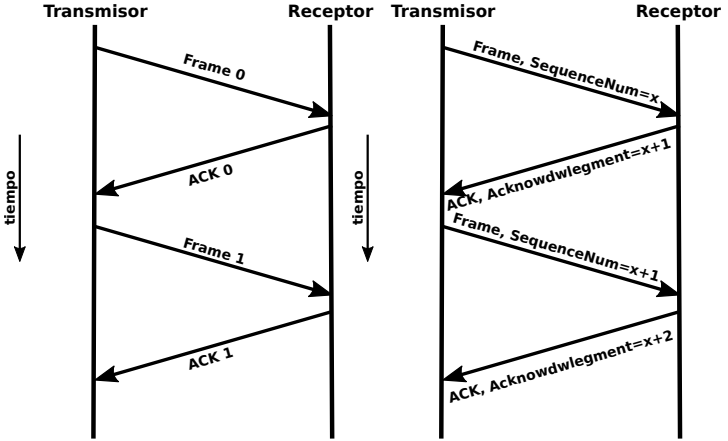


(a) Escenario esperable. (b) Frame dropped. Retransmisión. (c) y (d) Receptor recibe Frame. Transmisor no recibe ACK. Retransmisión. Se necesita identificar paquete.

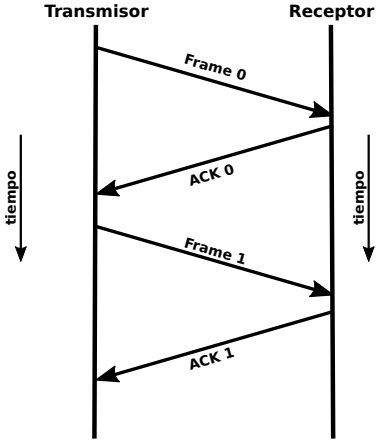
Stop and Wait

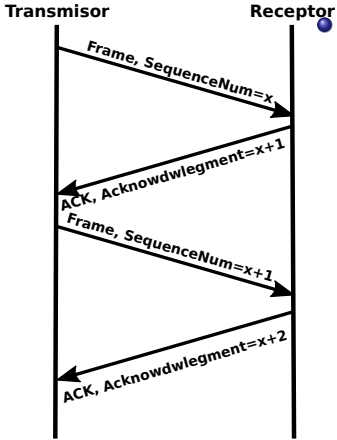


Stop and Wait



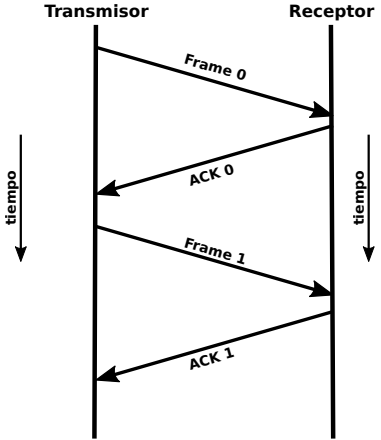
Stop and Wait

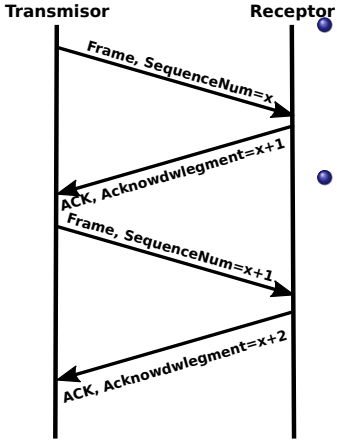




- Los escenarios (c) y (d) del slide de anterior se resuelven identificando al frame y su ACK asociado.

Stop and Wait





- Los escenarios (c) y (d) del slide de anterior se resuelven identificando al frame y su ACK asociado.
- En el caso de un enlace dedicado con un bit alcanza ya que los parámetros eléctricos son constantes. En el caso de Internet este supuesto deja de ser válido.

Consideraciones de ancho de banda

- Stop and Wait, permite un único frame viajando por el enlace.
- Un enlace ADSL de 3 Mbps tiene RTT (Round Trip Time) promedio de 45 mseg.
- El producto Ancho de banda x delay de este enlace es:

$$\frac{3000000 bit/seg}{8 bit/byte} * 0{,}045 seg. = 16,875 kbytes$$

Consideraciones de ancho de banda

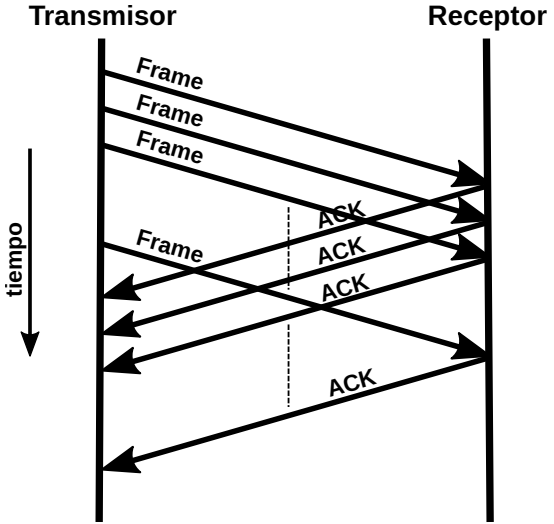
- El tamaño de un paquete TCP es 1514 bytes.
- La velocidad máxima a la que se puede transmitir un frame con RTT = 45 mseg. es:

$$\frac{1514 bytes * 8 bits/byte}{0{,}045 seg} = 269155,56 bps$$

- Desaprovechamos el BW del enlace
- Se puede transmitir:

$$\frac{3000000}{269155} = 11 paquetes$$

Sliding Window



Sliding Window - Algoritmo

- El transmisor y el receptor mantienen tres variables, y vigilan porque satisfagan estas relaciones

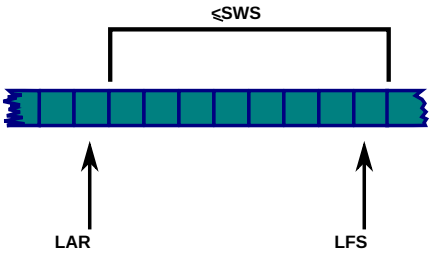
$$SWS \geq LFS - LAR$$

$$RWS \geq LAF - LFR$$

SWS Sender Window Size
LFS Last Frame Sent
LAR Last Acknowdlegment Received

RWS Receiver Window Size
LAF Last Acknowdlegment Forwarded
LFR Last Frame Received

Sliding Window - Algoritmos



Sliding Window - Algoritmo simple

- Cuando recibe un frame el receptor, examina el campo **`SequenceNum`** del header.
- Si ($LFR \geq SequenceNum > LAF$) el paquete se descarta.
- Si ($LFR < SequenceNum \leq LAF$) el paquete está dentro de la ventana del receptor. Es aceptado.
- Si llegan paquetes fuera de orden, no se envía ACK de los mismos sino hasta que llegue el paquete cuyo SequenceNum corresponda a LFR + 1.
- Cuando arribe ese paquete se lo reconoce junto con los consecutivos en secuencia que llegaron antes y se ajustan LFR y LAF.

Preguntas ???.