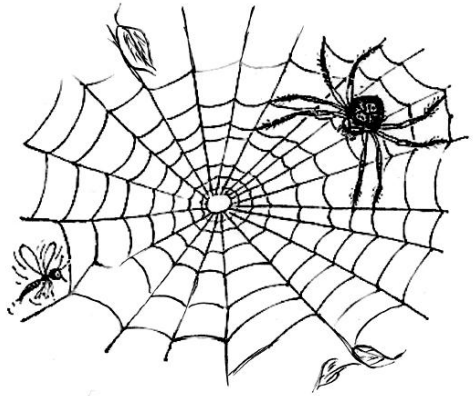
Repaso Control 1

Inter
Net
Working



Agenda

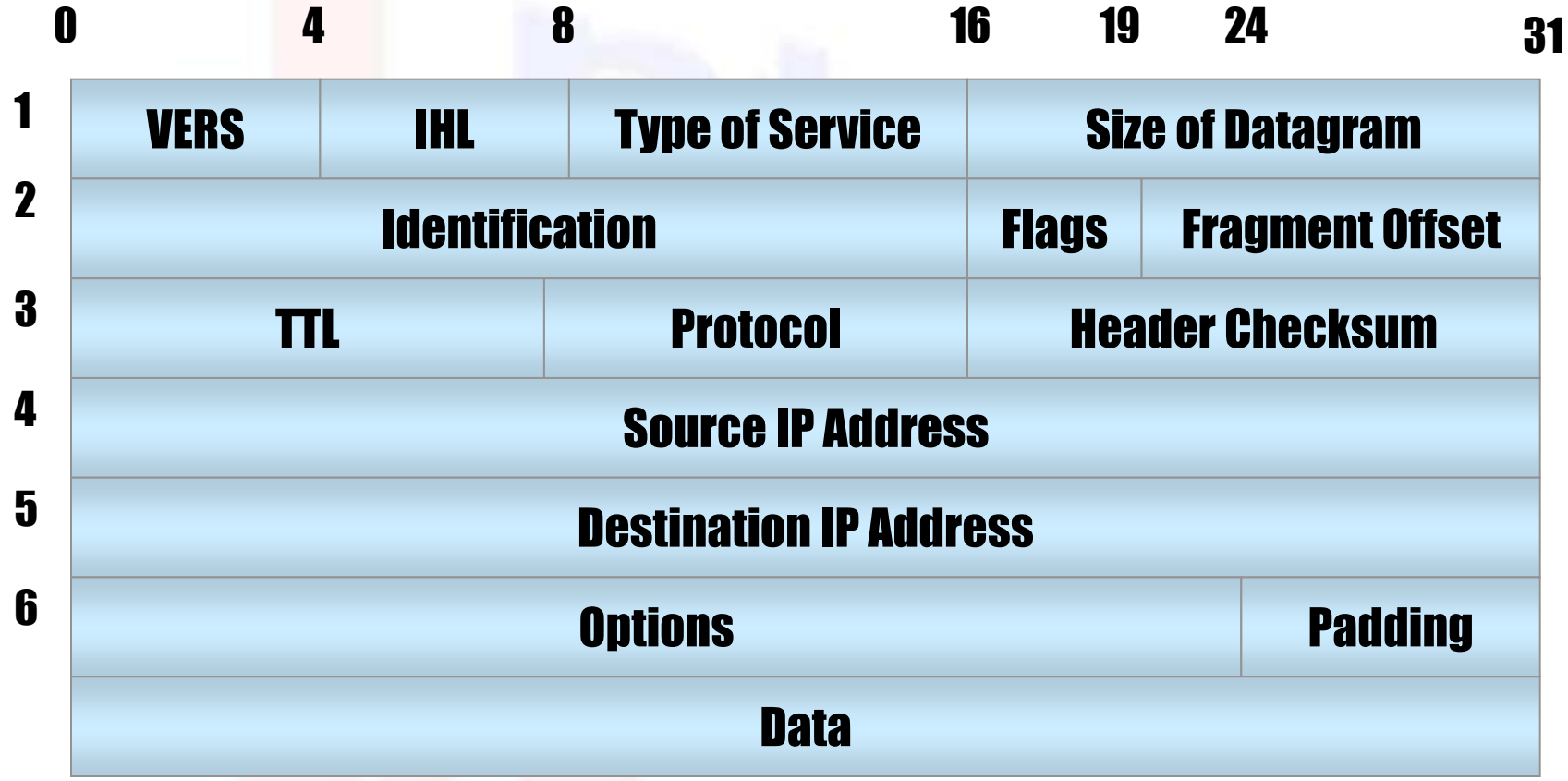
- Network Discovery
- Direccionamiento IP
- TCP
- Lan Switching

Network Discovery

IP - Internet Protocol

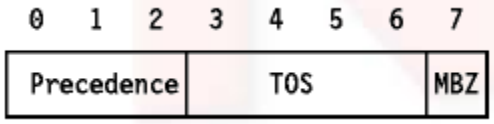
- Protocolo no orientado a la conexión.
- No transmite información de control.
- No establece una conexión end-to-end. antes de transmitir los datos.
- No es confiable.

Header del Datagrama IP



Descripción de Campos 1

- Vers. Version de IP.
- IHL. IP Header Length. Número de palabras de 32 bits que forman el header. Usualmente 5.
- Type of Service. Ahora conocido como Differentiated Services Code Point (DSCP) (usualmente 0, pero puede indicar una Calidad de Servicios solicitada a la red, DSCP define uno de los tipos de Clase de Servicio)



- Precedencia : Es una medida de la naturaleza y prioridad de este datagrama.
  - 000 Rutina
  - 001 Prioridad
  - 010 Imediato
  - 011 "Flash"
  - 100 "Flash override"
  - 101 Crítico
  - 110 Control de red("Internetwork control")
  - 111 Control de red("Network control")

- TOS "*type of service*":
  - 1000 Minimizar retardo
  - 0100 Maximizar la densidad de flujo
  - 0010 Maximizar la fiabilidad
  - 0001 Minimizar el coste monetario
  - 0000 Servicio normal
- MBZ
  - Reservado para uso futuro(debe ser cero, a menos que participe en un experimento con IP que haga uso de este bit)
  - Una descripción detallada del TOS se puede encontrar en el RFC 1349.

Descripción de Campos 2

- Identification. Número de 16 bit number que junto con la dirección fuente identifica en forma única al paquete. Se utiliza especialmente para reensamblar datagamas fragmentados.
- Flags. Secuencia de tres flags usados para control si los routers tienen permitido fragmentar paquetes e indicar las partes de un paquete que reciben.

- **0** Reservado, debe ser cero
- **DF** No fragmentar("Don't Fragment")
  - 0 permite la fragmentación
  - 1 no.
- **MF** Más fragmentos("More fragments")
  - 0 significa que se trata del último fragmento del datagrama.
  - 1 que no es el último.

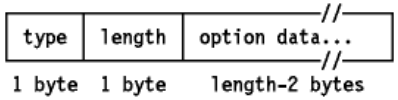
Descripción de Campos 3

- Fragmentation Offset. Contador de bytes desde el comienzo del paquete original enviado enviando por un router que realizó una fragmentación.
- TTL. Time To Live. Número de saltos o links que los paquetes puedes ser ruteados, el valor es decrementado al pasar por los routers. Es usado para prevenir loops de ruteo accidentales.
- Size of Datagram. Largo del datagrama IP incluye largo del header + data.
- Protocol. Indica el tipo de transporte empaquetado
  - 1 = ICMP
  - 2 = IGMP
  - 4 = IP encapsulation
  - 6 = TCP
  - 17 = UDP
  - 89 = OSPF
- Header Checksum. Chequeo de Errores del encabezado utilizado para detectar errores de procesamiento en los routers.
- Source/Destination IP Address. Dirección IP de la fuente original o del destino final del paquete.

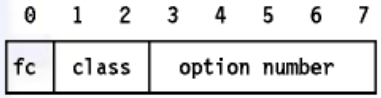
Descripción de Campos 4

- Options. Este campo tiene longitud variable. Puede haber cero o más opciones. Hay dos formatos para estas. El formato usado depende del valor del número de opción hallado en el primer byte.

  - Un byte de de tipo (“type byte”).
  - Un byte de tipo, un byte de longitud y uno o más bytes de opciones



- Estructura del “type byte”
  - fc "Flag copy", que indica si el campo se ha de copiar(1) o no(0) cuando el datagrama está fragmentado.
  - class Un entero sin signo de 2 bits:
    - 0 control
    - 1 reservado
    - 2 depurado y mediciones
    - 3 reservado



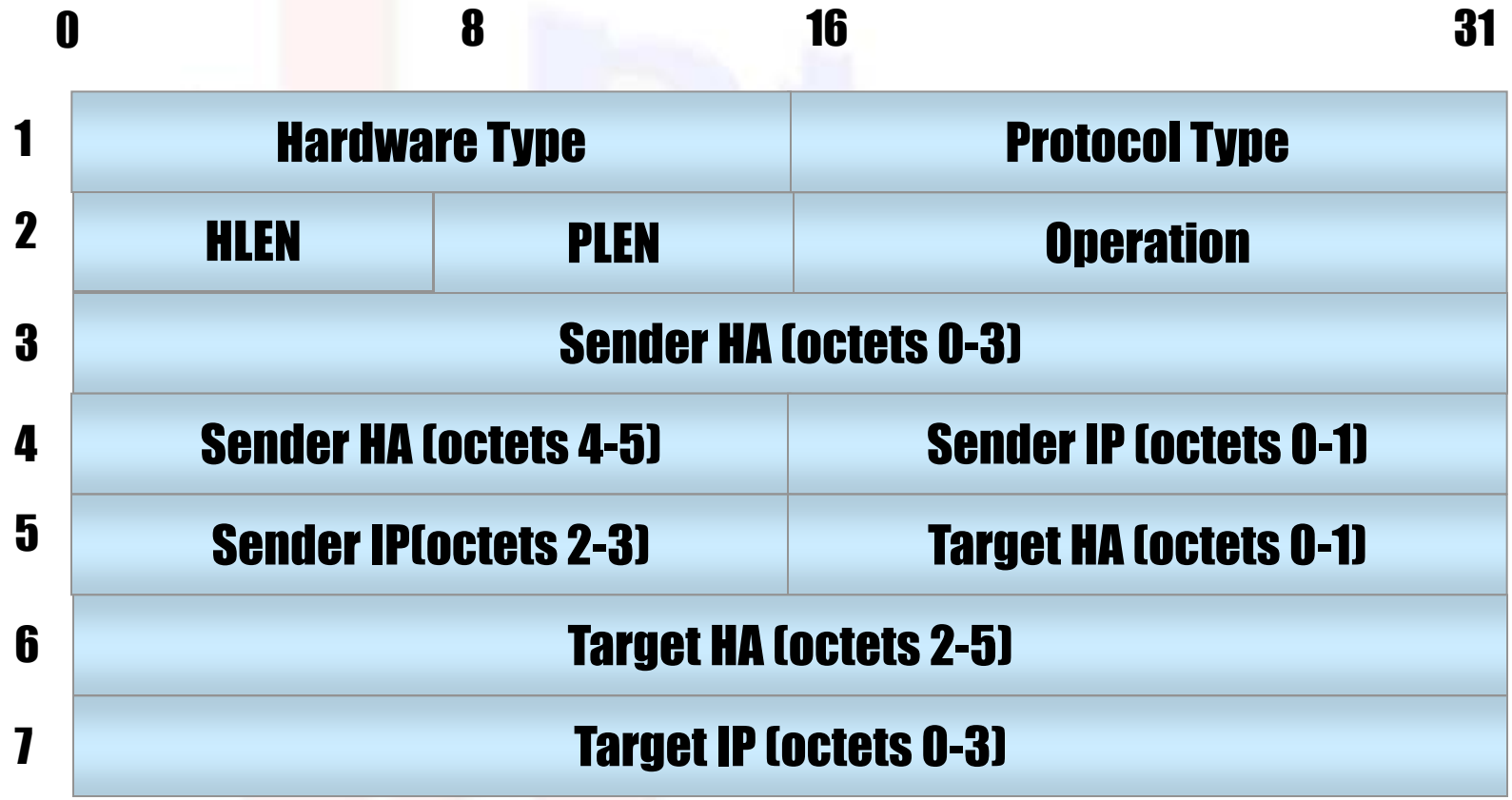
- option number Entero sin signo de 5 bits.
  - 0 Fin de la lista de opciones, con "class" a cero, fc a cero, y sin byte de longitud o de datos. Es decir, la lista termina con el byte X'00'. Sólo se requiere si la longitud de la cabecera IP(que es un múltiplo de 4 bytes) no se corresponde con la longitud real de las opciones.
  - 1 No operación. Tiene "class" a cero, fc a cero y no hay byte de longitud ni de datagramas. Es decir, un byte X'01' es NOP("no operation"). Se puede usar para alinear campos en el datagrama.
  - 2 Securidad. Tiene "class" a cero, fc a uno y el byte de longitud a 11 y el de datos a 8. Se usa para la info de seguridad que necesitan las especificaciones del depto de defensa de US.
  - 3 LSR("Loose Source Routing"). Tiene "class" a cero, fc a uno y hay un campo de datos de longitud variable.
  - 4 IT("Internet Timestamp"). Tiene "class" a 2, fc a cero y hay un campo de datos de longitud variable.
  - 7 RR("Record Route"). Tiene "class" a 0, fc a cero y hay un campo de datos de longitud variable.
  - 8 SID("Stream ID", o identificador de flujo). Tiene "class" a 0, fc a uno y hay un byte de longitud a 4 y un byte de datos. Se usa con el sistema SATNET.
  - 9 SSS("Strict Source Routing"). Tiene "class" a 0, fc a uno y hay un campo de datos de longitud variable.

ARP

ARP Address Resolution Protocol

- Es un protocolo utilizado por IP para asociar una dirección IP a una dirección física y de este modo establecer una comunicación.
- El protocolo envía un broadcast preguntando por una dirección IP determinada y la estación que la posee responde indicando de este modo su dirección física.
- Para optimizar la consulta continua los equipos poseen una tabla cache con las últimas interrogaciones solicitadas.
- RARP. Corresponde a la consulta inversa es decir cuando se requiere saber la dirección IP de un dispositivo con dirección MAC conocida.

Formato del Mensaje ARP



Tipos de Mensajes

- ARP request
- ARP reply
- RARP request
- RARP reply

Tablas ARP

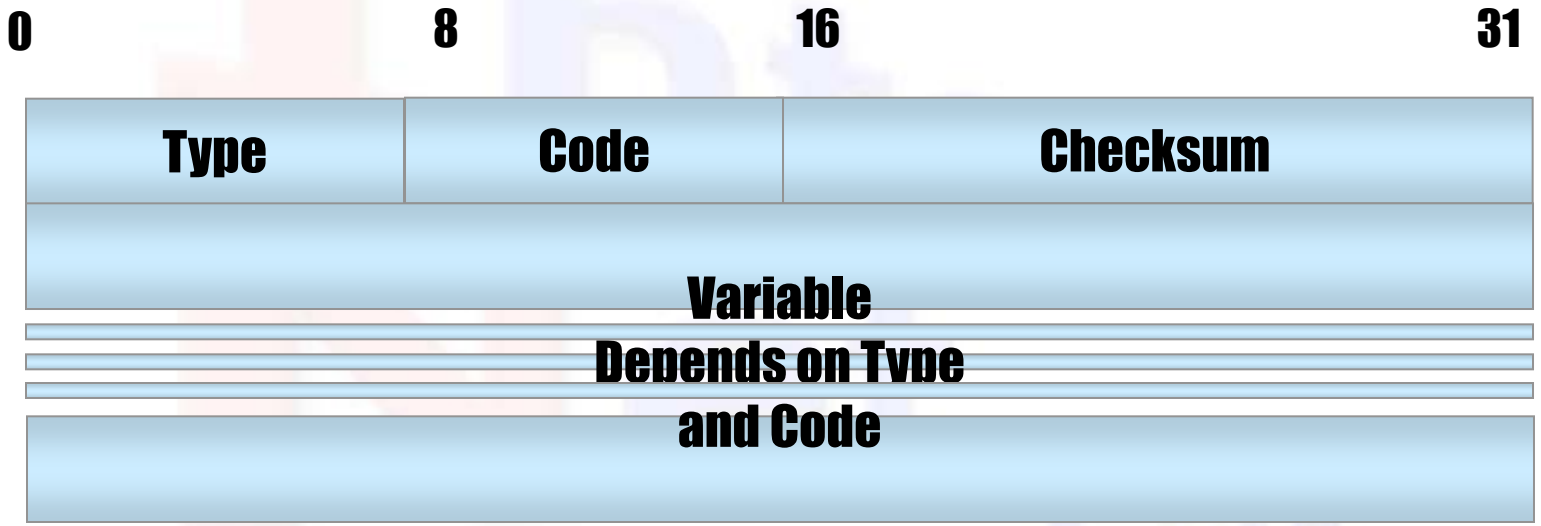
```
matrix% arp
Usage: arp hostname
       arp -a
       arp -d hostname
       arp -s hostname ether_addr [temp] [pub] [trail]
       arp -f filename
matrix% arp -a

Net to Media Table: IPv4
Device   IP Address               Mask      Flags   Phys Addr
------ -------------------- -------------- ----- ---------------
hme0   172.16.231.90        255.255.255.255      00:05:5d:5f:af:c2
hme0   172.16.231.83        255.255.255.255      00:02:3f:22:af:24
hme0   172.16.231.77        255.255.255.255      00:10:b5:f5:ce:8e
hme0   jsandova.tmovil.cl   255.255.255.255      00:02:3f:22:a3:0b
hme0   172.16.231.121       255.255.255.255      00:08:02:8f:c8:2f
```

ICMP

ICMP- Internet Control Mensaje Protocol

- RFC 792
- Control de flujo.
  - ICMP source quench message.
- Detecta destino inaccequible.
  - Destination unreacheable message
- Redirecciona rutas.
  - ICMP redirect message.
- Chequea host remotos (PING)
  - ICMP echo message.

Formato del Mensaje ICMP



Tipos de Mensajes

- Type Especifica el tipo del mensaje:
  - 0 Echo reply
  - 3 Destination unreachable
  - 4 Source quench
  - 5 Redirect
  - 8 Echo
  - 9 Router Advertisement
  - 10 Router Solicitation
  - 11 Time exceeded
  - 12 Parameter Problem
  - 13 Timestamp request
  - 14 Timestamp reply
  - 15 Information request(obsolete)
  - 16 Information reply(obsolete)
  - 17 Adress mask request
  - 18 Adress mask reply

Tipos de Mensajes 1

- Destination Unreachable Message.
  - Indica que de acuerdo a la tabla de ruteo la red es inalcanzable por el host origen.
- Time Exceeded Message
  - Indica que el TTL ha llegado a Cero y que el paquete ha sido descartado.
- Parameter Problem Message
  - Indica que se ha detectado un problema con los parámetros del header y no puede seguir procesándose el datagrama por lo que se descartará.
- Source Quench Message
  - Indica que no tiene espacio en el buffer para enviarlo a la próxima red.

Tipos de Mensajes 2

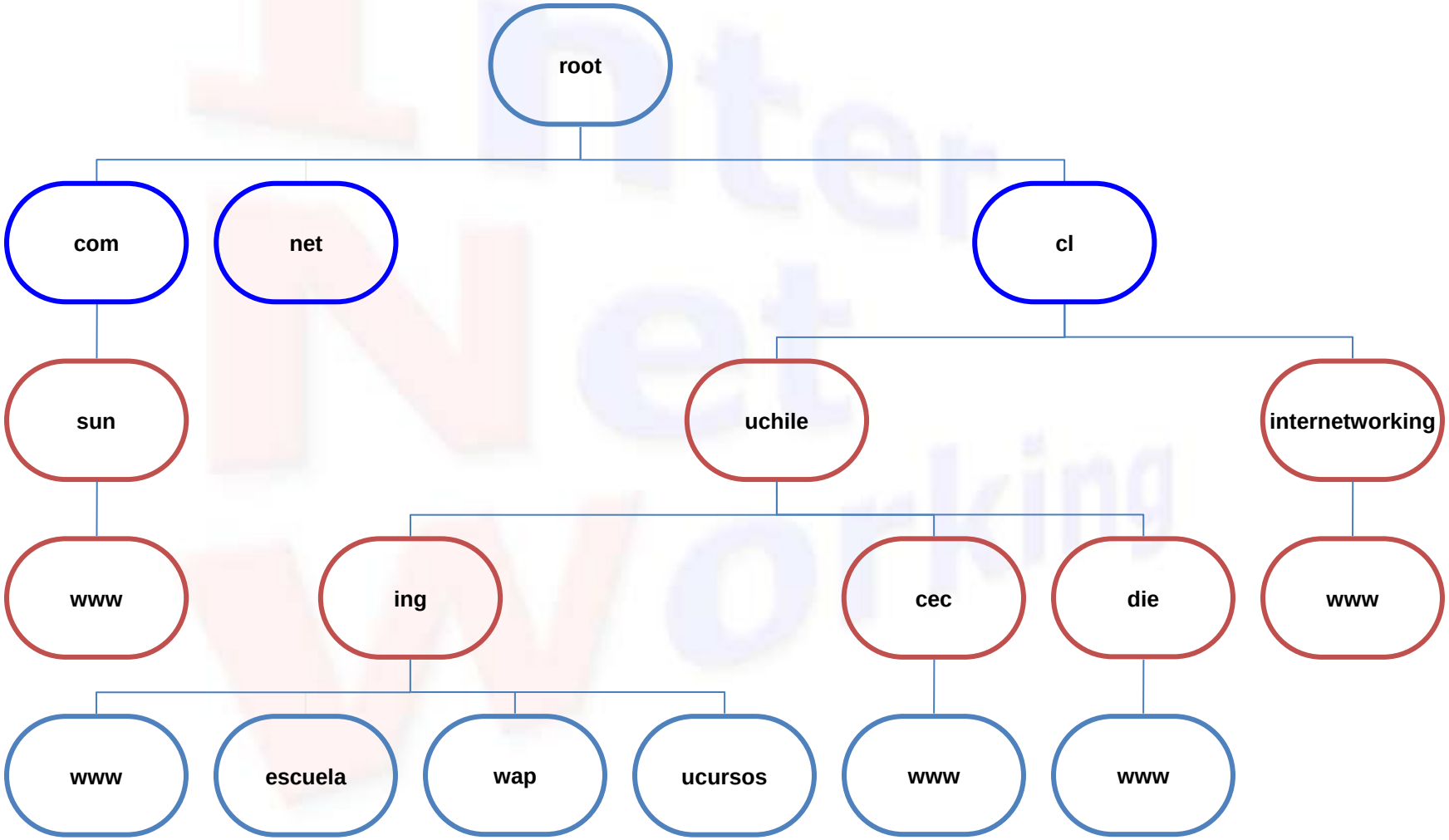
- Redirect Message
  - El router detecta que el próximo salto es un router dentro de la misma red del equipo que recibio el datagrama por lo que le informa que es mejor que se lo envie al otro router.
- Echo or Echo Reply Message.
  - La información recibida en un mensaje echo debe ser devuelta en un mensaje echo reply. Usualmente utilizado para medir Round Trip y perdida de paquetes
- Timestamp or Timestamp Reply Message
  - Usado pora identificar tiempos de vieje y de procesamiento del mensaje contine: Originate Timestamp, Receive Timestamp y Transmit Timestamp.
- Information Request or Information Reply Message
  - Utilizado para determinar las redes a las que se encuentra conectado un host.

DNS

DNS

- Aplicación distribuida que permite asociar un nombre a una dirección IP.
- Posee una estructura jerárquica.
- Delegación de autoridad
- BIND. Berkeley Internet Name Domain
- Conceptos:
  - Servidor Primario. Actualiza
  - Servidor Secundario. Informa
  - Servidor Cache. Informa sin autoridad

Estructura jerárquica



Delegación de Autoridad

- Se delegan a subdominios definiendo un record NS.
- Las preguntas sobre hosts de un subdominio son derivadas al DNS del subdominio

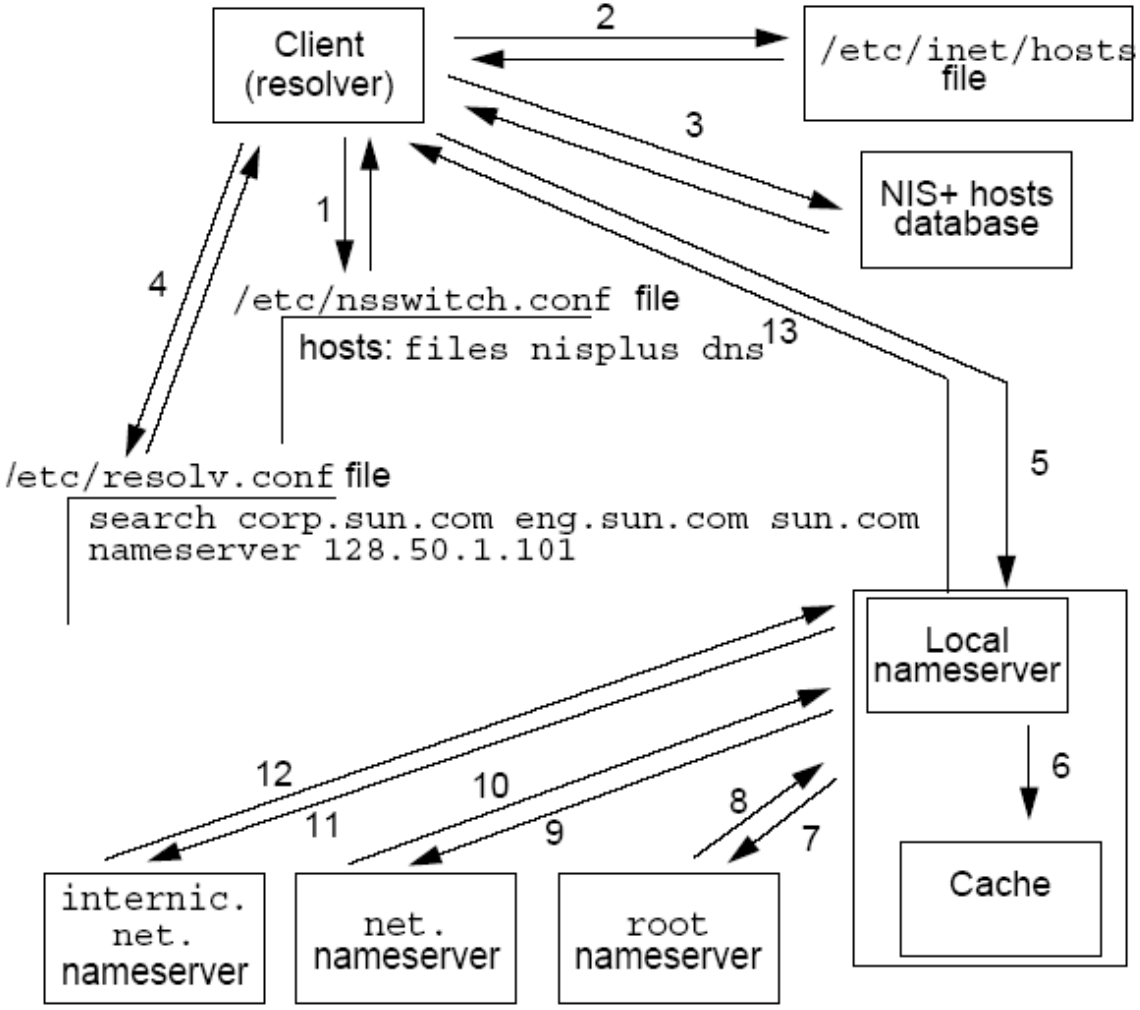
Tipos de Registros

- **A** Address Record. Para definir un host
- **CNAME** Canonical Name. Usado para definir una alias de un host.
- **NS** Name Service. Para definir un DNS
- **MX** Mail Exchange. Para definir un servidor SMTP
- **PTR** para definir un dominio inverso
- **SOA** Start of Authority

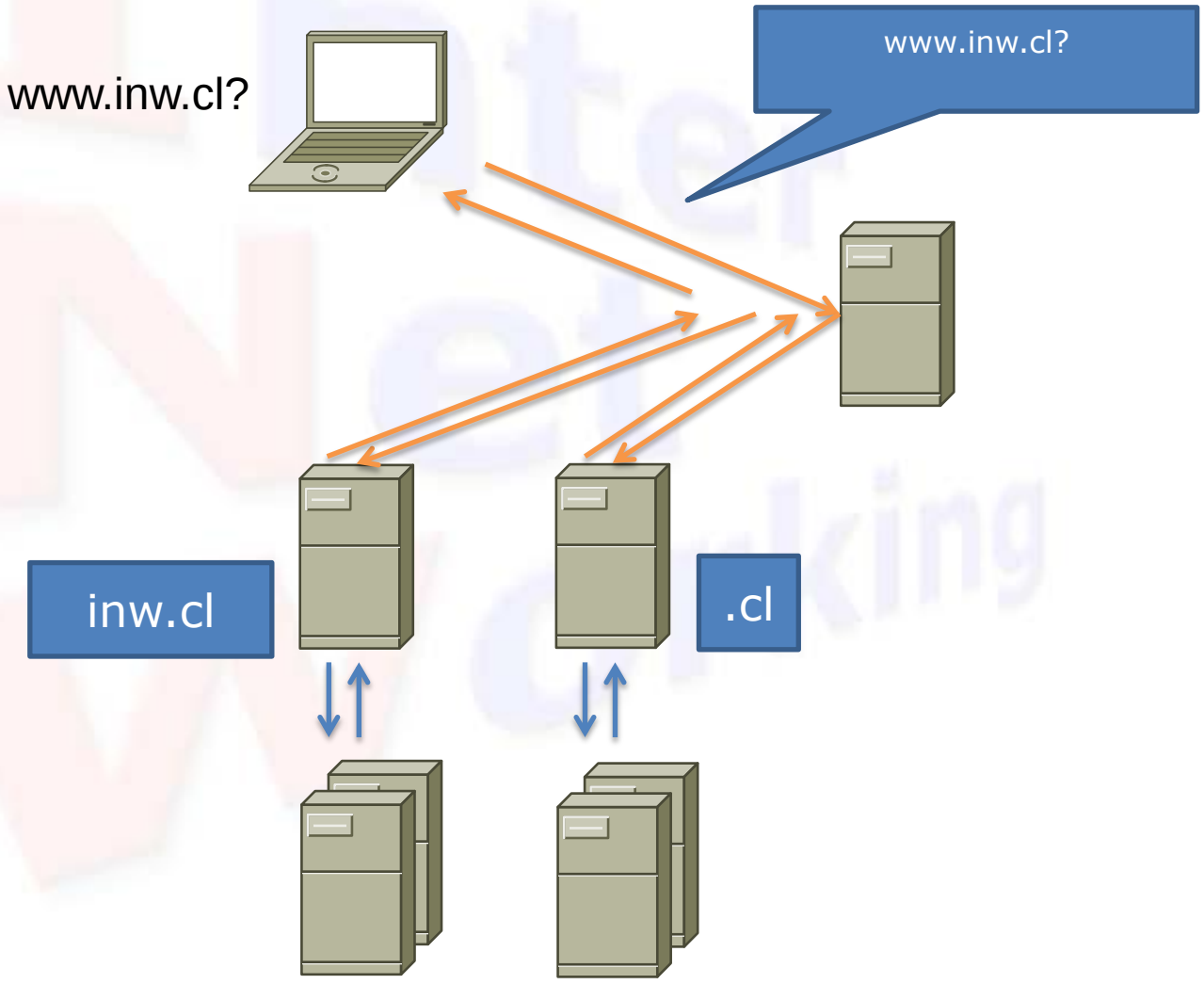
SOA Start of Authority

- **Serial Number**. Habitualmente en formato yyyymmddhh para indicar modificación. Se asume una nueva versión si este número se incrementa.
- **Refresh**. Cada cuanto tiempo el secundario refresca.
- **Retry**. Cada cuanto tiempo reintenta si la actualización del secundario fracaza.
- **Expire**. Indica cuanto tiempo puede estar la copia en el secundario sin refrescar.
- **TTL**. Tiempo que permanecerán los registros en los caches de los DNSs.

Ejemplo de resolución de nombres



Tipos de Servidores de Nombres



named.conf

- Servidor Maestro

```
zone "example.com" IN {
 type master;
 file "example.com.zone";
 allow-update { none; };
 };
```

- Servidor Esclavo

```
zone "example.com" {
 type slave;
 file "example.com.zone";
 masters { 192.168.0.1; };
 };
```

Archivo de Zona

```
$ORIGIN example.com.
$TTL 86400
@ IN SOA dns1.example.com. hostmaster.example.com. (
                              2001062501 ; serial
                              21600 ; refresh after 6 hours
                              3600 ; retry after 1 hour
                              604800 ; expire after 1 week
                              86400 ) ; minimum TTL of 1 day
          IN       NS       dns1.example.com.
          IN       NS       dns2.example.com.
          IN       MX       10 mail.example.com.
          IN       MX       20 mail2.example.com.
          IN       A        10.0.1.5
server1   IN       A        10.0.1.5
server2   IN       A        10.0.1.7
dns1      IN       A        10.0.1.2
dns2      IN       A        10.0.1.3
ftp       IN       CNAME    server1
mail      IN       CNAME    server1
mail2     IN       CNAME    server2
www       IN       CNAME    server2
```

Resolución Inversa

```
zone "1.0.10.in-addr.arpa" IN {
 type master;
 file "example.com.rr.zone";
 allow-update { none; };
};
```

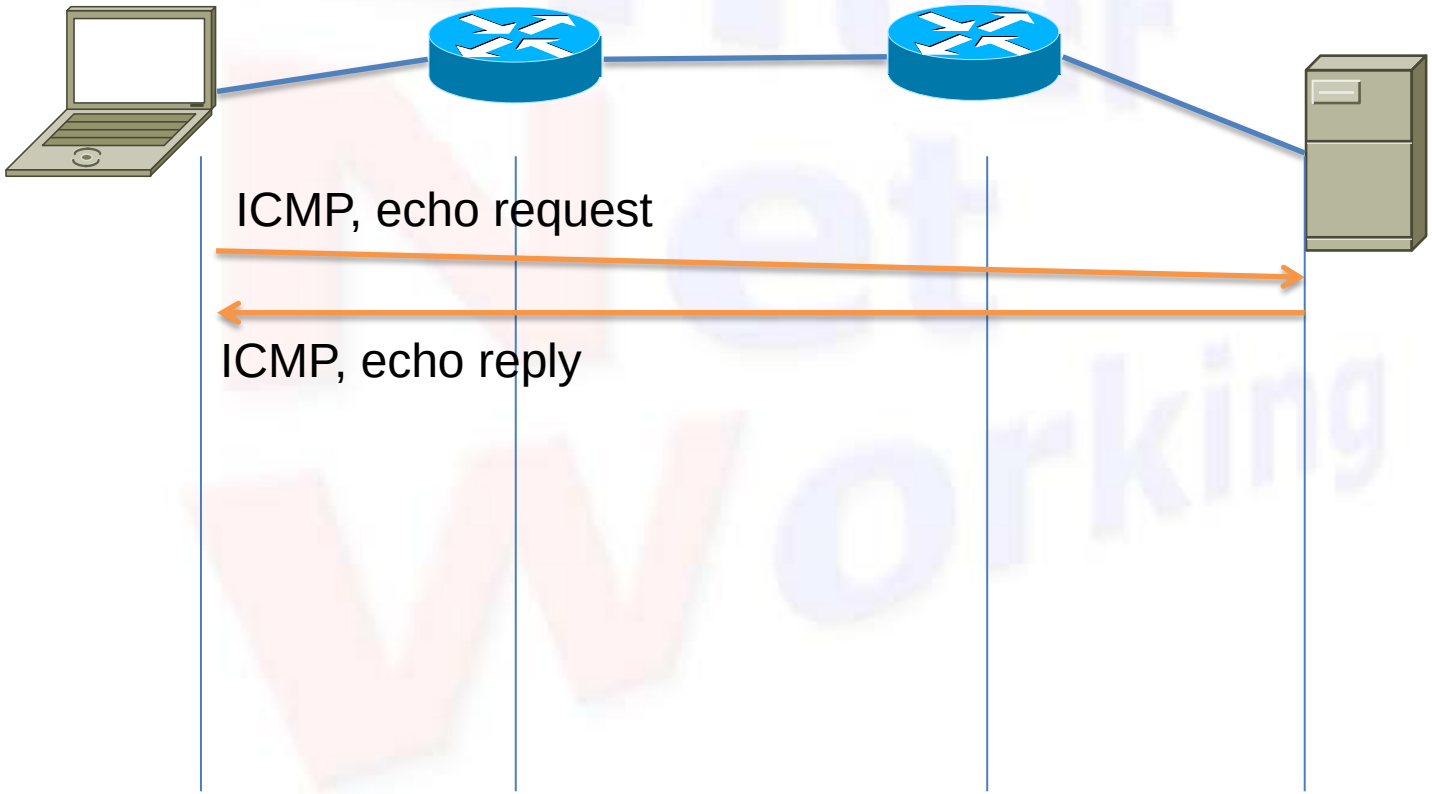
```
$ORIGIN 1.0.10.in-addr.arpa.
$TTL 86400
@ IN SOA dns1.example.com. hostmaster.example.com. (
                            2001062501 ; serial
                            21600 ; refresh after 6 hours
                            3600 ; retry after 1 hour
                            604800 ; expire after 1 week
                            86400 ) ; minimum TTL of 1 day
          IN       NS dns1.example.com.
          IN       NS dns2.example.com.
20        IN       PTR alice.example.com.
21        IN       PTR betty.example.com.
22        IN       PTR charlie.example.com.
23        IN       PTR doug.example.com.
24        IN       PTR ernest.example.com.
25        IN       PTR fanny.example.com.
```

Herramientas

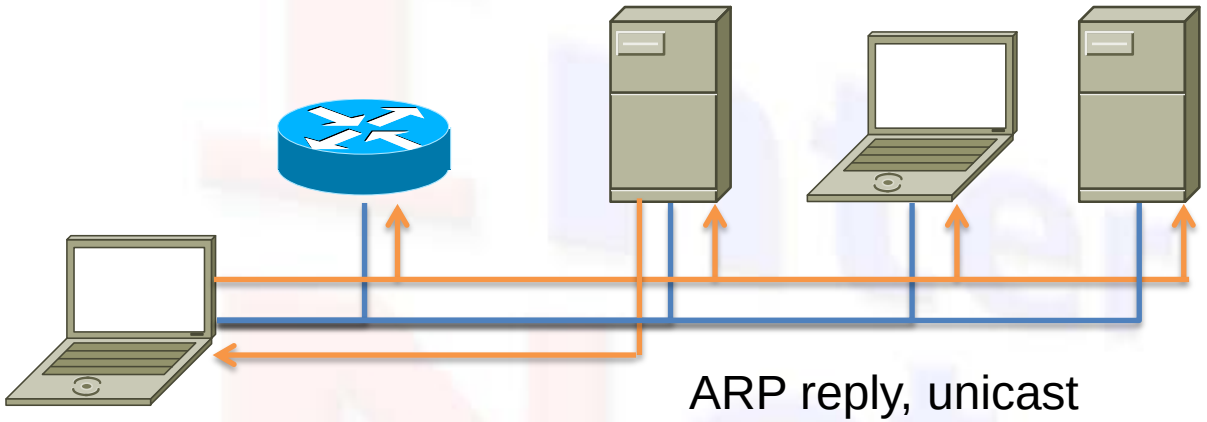
Herramientas nativas

- Ping
- Traceroute (tracert)
- Arp
- netstat
- Snoop
- Tcpdump

Ping



Tablas ARP

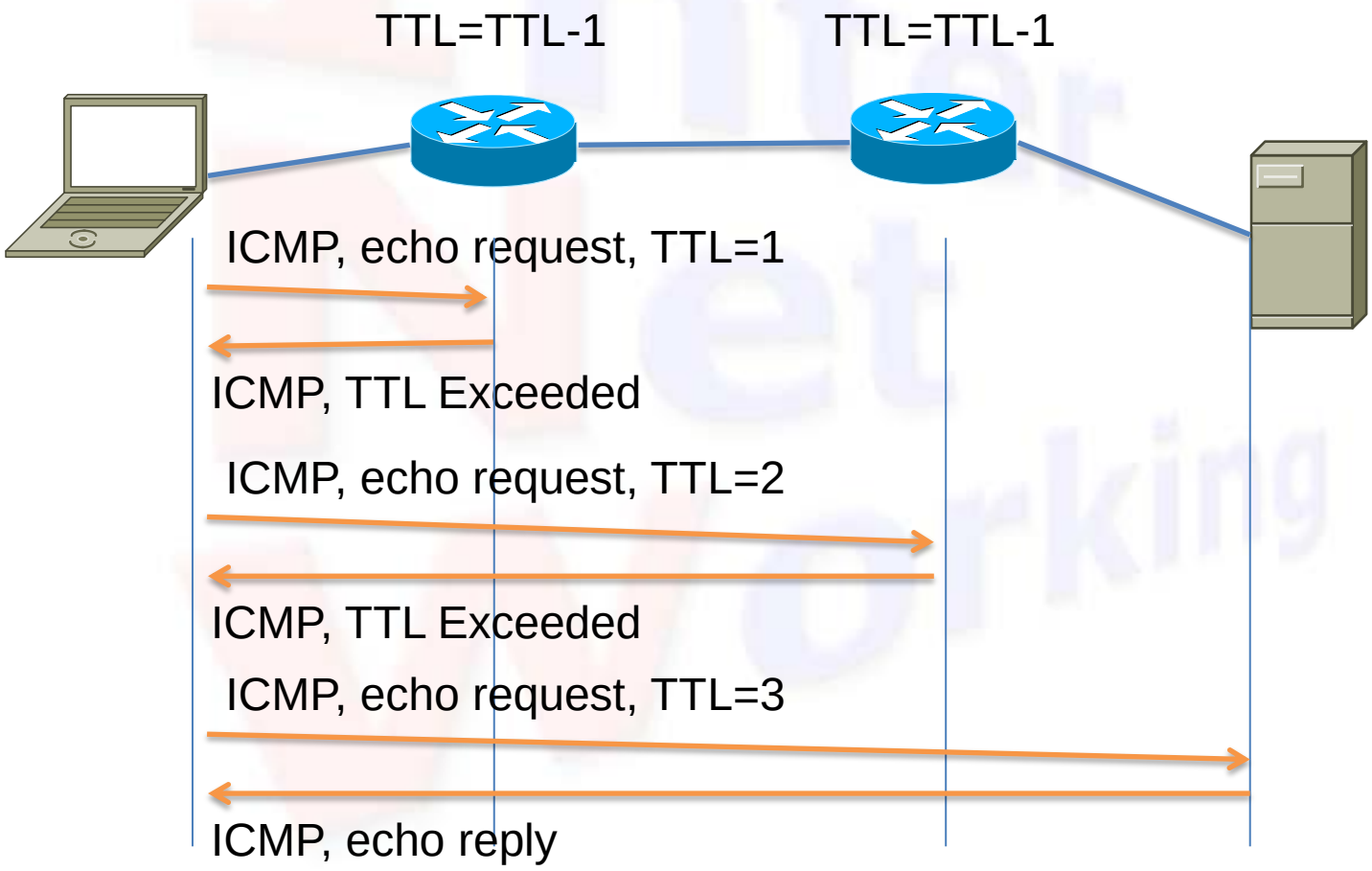


ARP request, broadcast

ARP reply, unicast

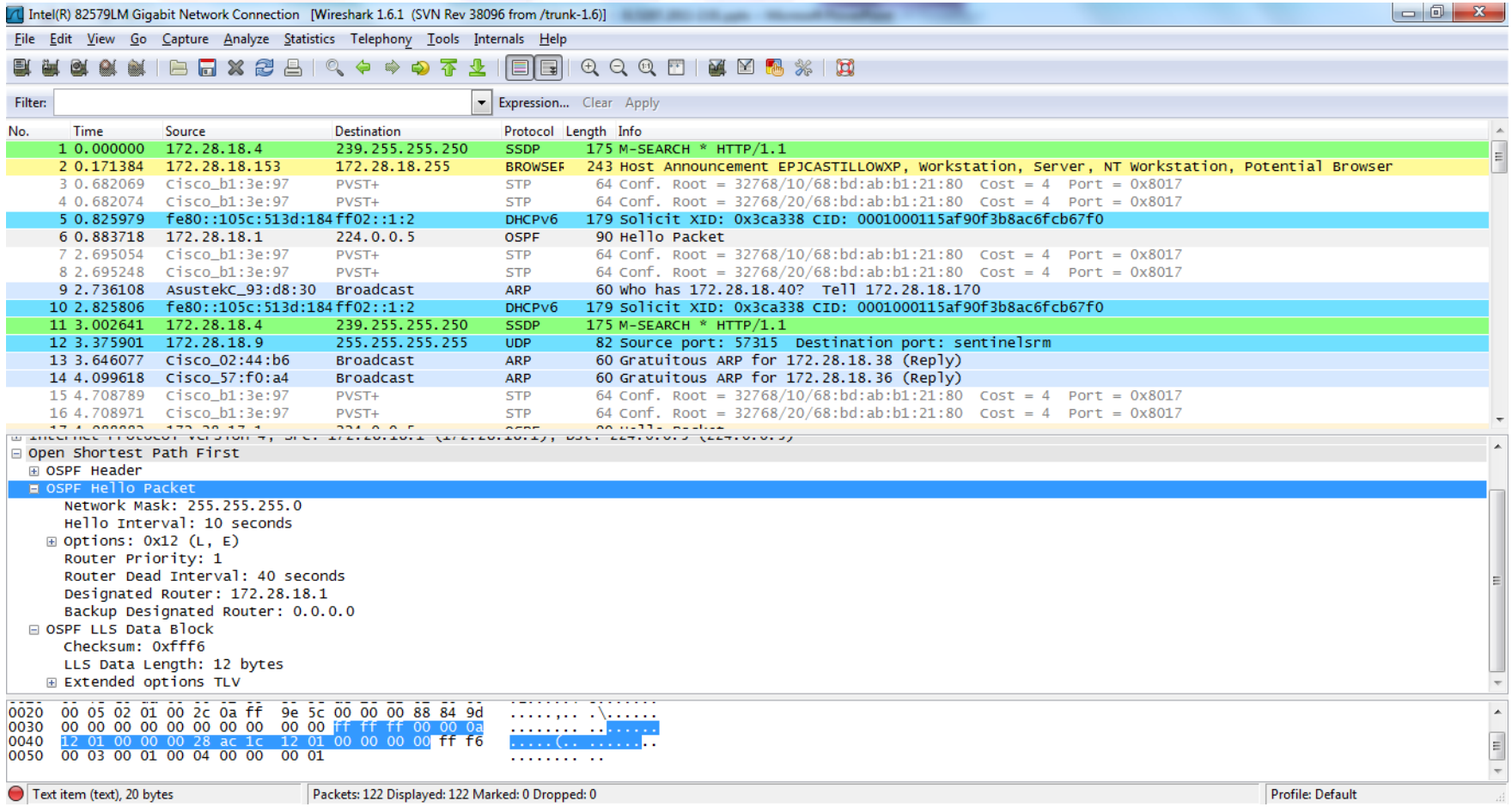
```
C:\Users\jsandoval>arp -a

Interfaz: 192.168.1.115 --- 0xf
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           68-7f-74-ba-d1-40     dinámico
  192.168.1.10          00-90-a9-81-de-e6     dinámico
  192.168.1.124         e8-39-df-b2-ed-9f     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  224.0.0.253           01-00-5e-00-00-fd     estático
  224.0.1.60            01-00-5e-00-01-3c     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

C:\Users\jsandoval>
```

Traceroute


TTL=TTL-1
TTL=TTL-1
ICMP, echo request, TTL=1
ICMP, TTL Exceeded
ICMP, echo request, TTL=2
ICMP, TTL Exceeded
ICMP, echo request, TTL=3
ICMP, echo reply

wireshark

- www.wireshark.org

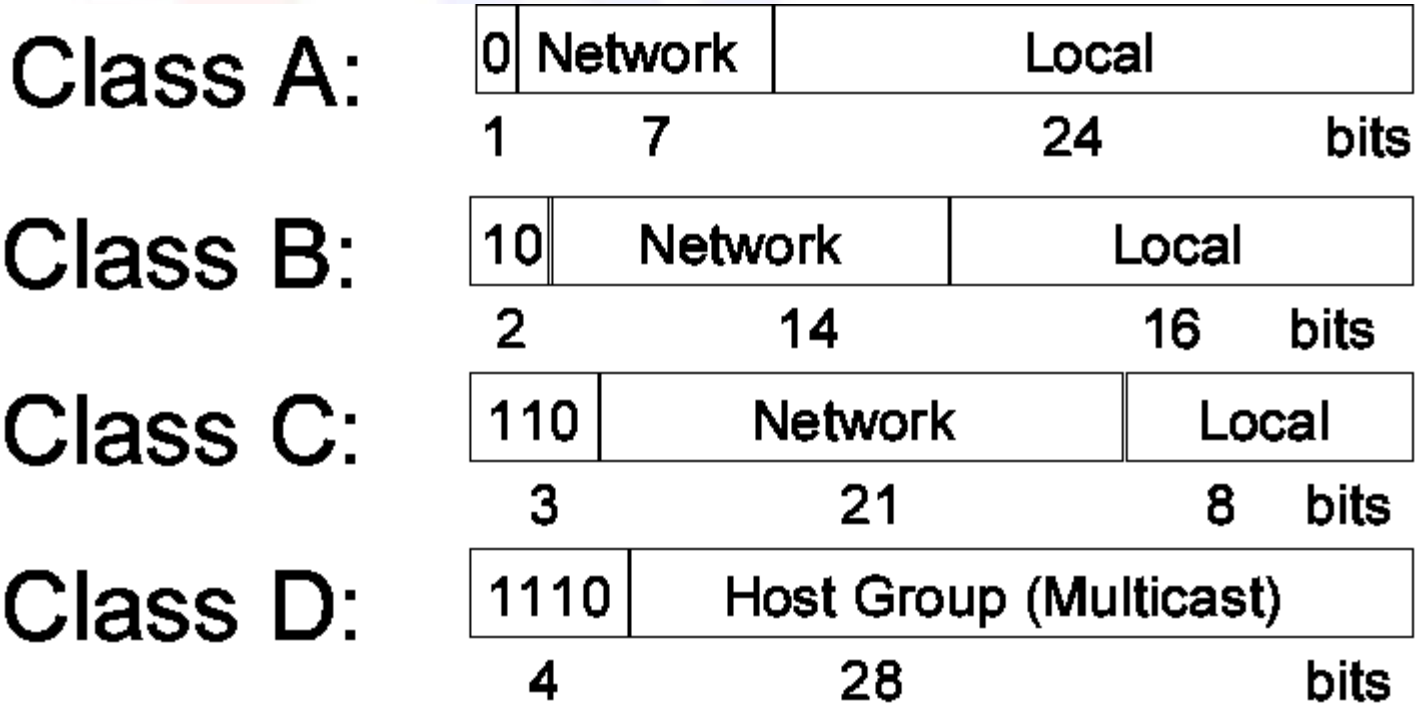


Direccionamiento

¿Qué es un dirección IP?

- Una dirección IP es el identificador único de un host en una red IP.
- Está compuesto por 32 bit que usualmente se representa en cuatro decimales y cada uno de ellos representa 8 bit.
- Ejemplo:
  - 146.83.12.32
  - 1001 0010. 0101 0011. 0000 1100. 0010 0000

Clases de Direcciones IP



Clases de Direcciones

- Rangos de Direcciones
  - A 0.10.0.0-126.0.0.0
  - B 128.0.0.0-191.255.0.0
  - C 192.0.1.0-223.255.255.255
  - D 224.0.0.0-239.255.255.255 multicast
  - E 240.0.0.0-254.255.255.255 experimentación

- La encargada de la administración de las direcciones ip es la IANA (Internet Assigned Numbres Authority). LACNIC para latinoamérica y El Caribe

Direcciones IP Privadas

- Direcciones IP privadas (RFC 1597):
  - 10.0.0.0 1 clase A
  - 172.16.0.0 a la 172.31.0.0 16 clases B
  - 192.168.0.0 256 clases C
  - Las puede usar quien quiera. NO son ruteables en Internet

Subnetting

Mascara por defecto 1

- La clase determina la máscara por defecto que tendrá la red y la cantidad de IPs que se pueden asignar a los host.
  - Clase A: AAAAAAAA.xxxxxxxx.xxxxxxxx.xxxxxxxx
    - 126 Redes
    - 2^24 - 2=16.777.214 direcciones
  - Clase B: BBBBBBBB.BBBBBBBB.xxxxxxxx.xxxxxxxx
    - 16.382 Redes
    - 2^16 - 2=65.534 direcciones
  - Clase C: CCCCCCCC.CCCCCCCC.CCCCCCCC.xxxxxxxx
    - 2.097.150 Redes
    - 2^8 - 2=254 direcciones

Mascara por defecto 2

- La mascara de red se utiliza para determinar el nombre de la red.
- Realizando la operación “and” lógico obtenemos el nombre de red.
  - Ejm.
  - Dirección IP: 146.83.12.32
  - Mascara Def: 255.255.0.0
  - Red: 146.83.0.0

Problemática

- Las clases de red determinan redes muy dispares.
  - Muy pocas redes con muchas direcciones para hosts.
  - Muchas redes con pocas direcciones para hosts.
- Solución Subdividir las redes.
  - Subnetting

Subnetting 1

- Si movemos mascara de red podemos generar subredes con un número de host adecuado a las necesidades de la Red.

Subnetting 2

- Ejemplo:
  - Red: 146.83.0.0
  - Mascara Def: 255.255.0.0
  - 1111 1111.1111 1111.0000 0000.0000 0000
  - Nueva Mascara: 255.255.224.0
  - 1111 1111.1111 1111.1110 0000.0000 0000
  - Número de Subredes: 2^3-2 = 6
  - Número de Hosts: 2^13-2 = 8190
  - Número de host útiles sin subnetting: 65.534
  - Número de Hosts útiles CON subnetting: 8190*6=49.140

Ejemplo

- IP address: 192.169.49.35
- Subnet Mask: 255.255.255.224
- No Subredes: 23-2=6
- No Nodos/subred: 25-2=30
- Subnet address: 192.169.49.32
- Direcciones válidas: 192.169.49.33-62
- Subnet broadcast: 192.169.49.63

Ejemplo (cont.)

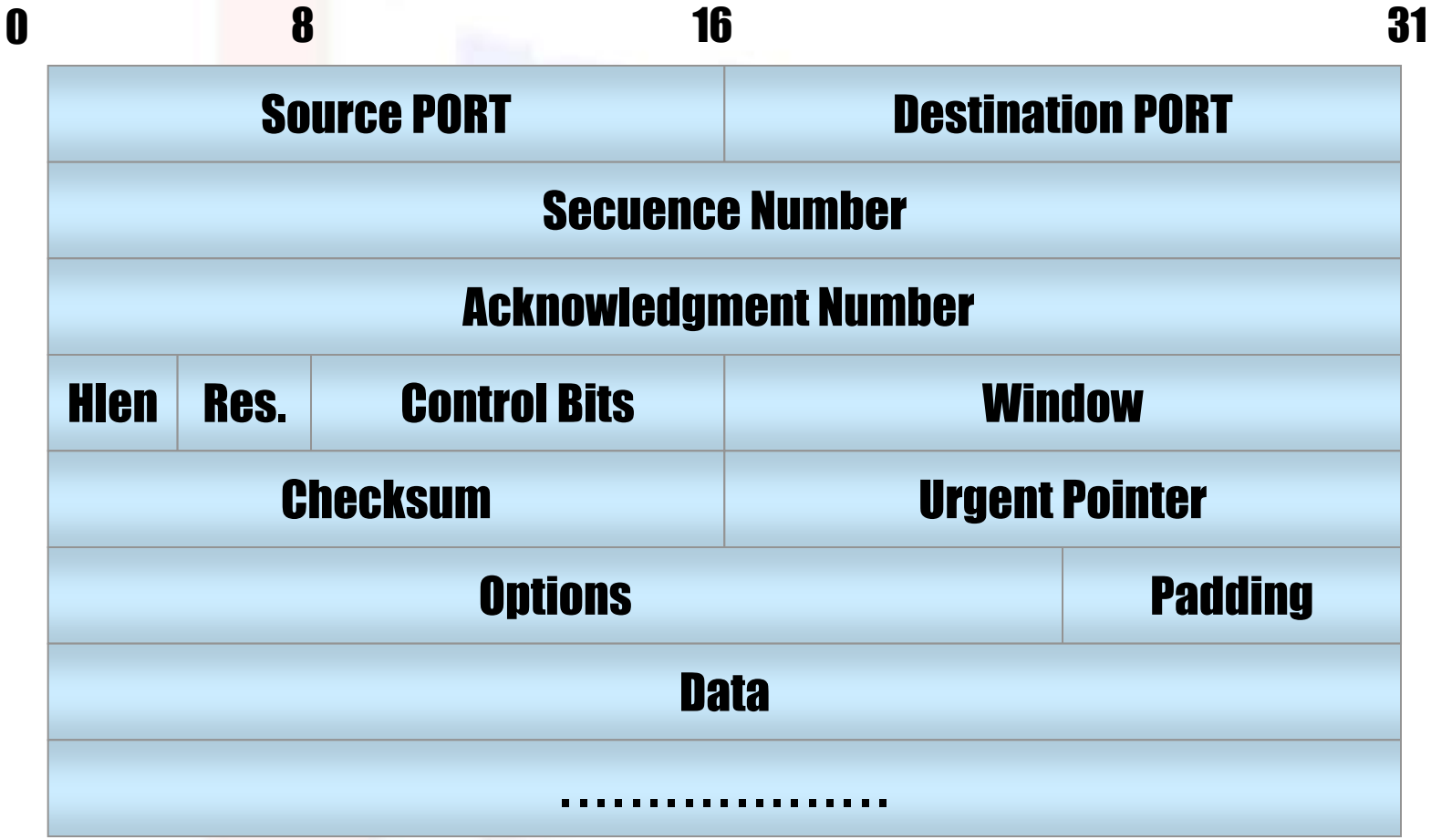
Numero de Red	Direcciones para Nodos	Dirección de Broadcast
192.169.49.0	Reservado	NA
192.169.49.32	.33 al .62	192.169.49.63
192.169.49.64	.65 al .94	192.169.49.95
192.169.49.96	.97 al .126	192.169.49.127
192.169.49.128	.129 al .158	192.169.49.159
192.169.49.160	.161 al 190	192.169.49.191
192.169.49.192	.193 al .222	192.169.49.223
192.169.49.224	Reservado	NA

TCP

TCP - Trasport Control Protocol

- Orientado a la Conexión.
- Permite el flujo bidireccional de datos libre de errores.
- Permite Control de Congestión de la Conexión.
- Servicio de Flujo de Datos entre aplicaciones corriendo en diferentes maquinas.
- Permite múltiples conexiones simultáneas
- Confiable, asegura integridad de los datos

Header TCP


0
8
16
31
Source PORT
Destination PORT
Secuence Number
Acknowledgment Number
Hlen
Res.
Control Bits
Window
Checksum
Urgent Pointer
Options
Padding
Data
.....

Descripción de Campos 1

- Source / Destination PORT. Numero de puerto Origen/Destino. 16 bit.
- Secuence number. Número de secuencia del primer byte de la data en este segmento (excepto en SYN). Cuando SYN está presente SN es el ISN (Initial Secuence Number y el primer byte es ISN+1
- Acknowledgment Number. Si el bit ACK está presente indica el próximo SN que se espera recibir.
- HLEN. Largo del header TCP en palabras de 32 bit.

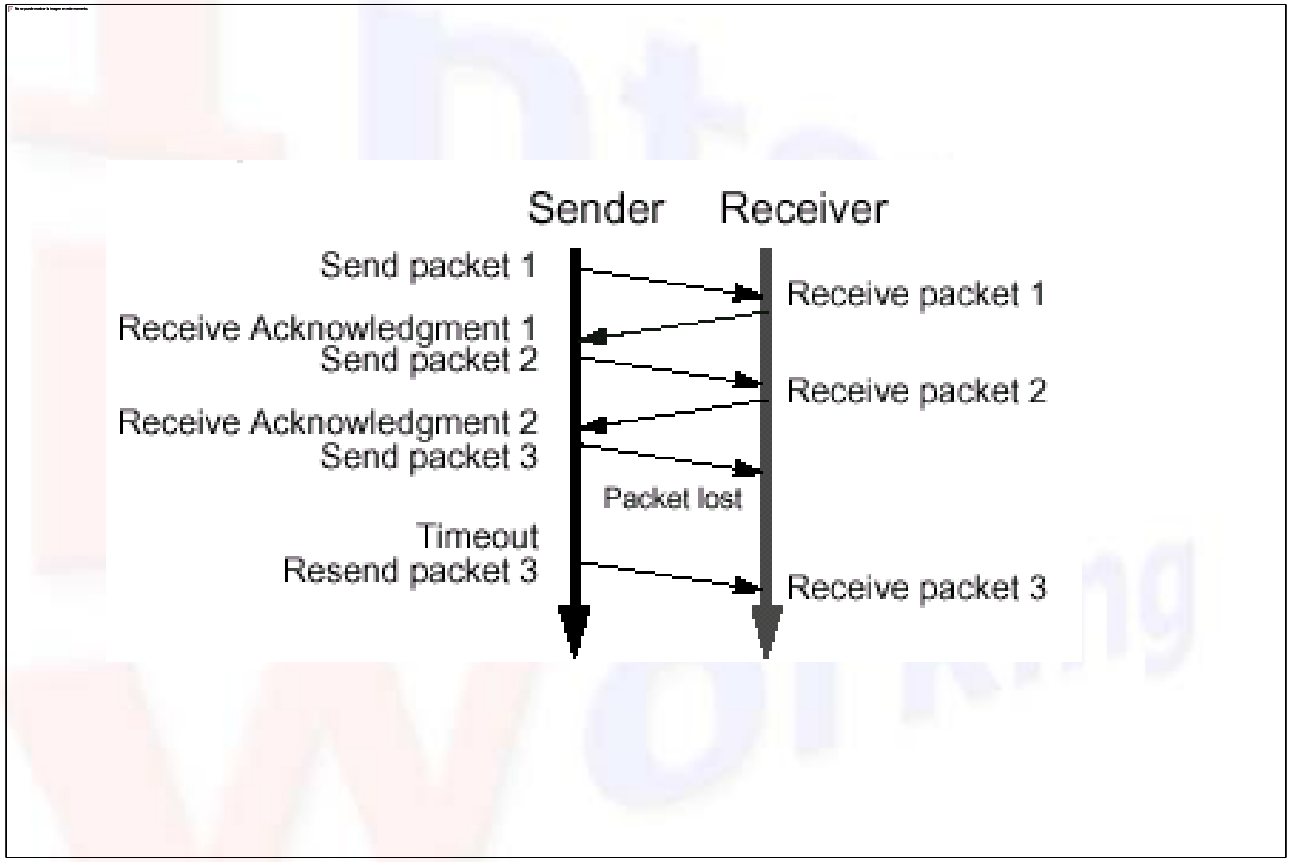
Descripción de Campos 2

- Control Bits. Bits de Control.
  - URG: Urgent Pointer field significant
  - ACK: Acknowledgment field significant
  - PSH: Push Function
  - RST: Reset the connection
  - SYN: Synchronize sequence numbers
  - FIN: No more data from sender
- Window. Número bytes que están en el aire esperando ser aceptados.
- Urgent Pointer. Largo del header TCP en palabras de 32 bit.

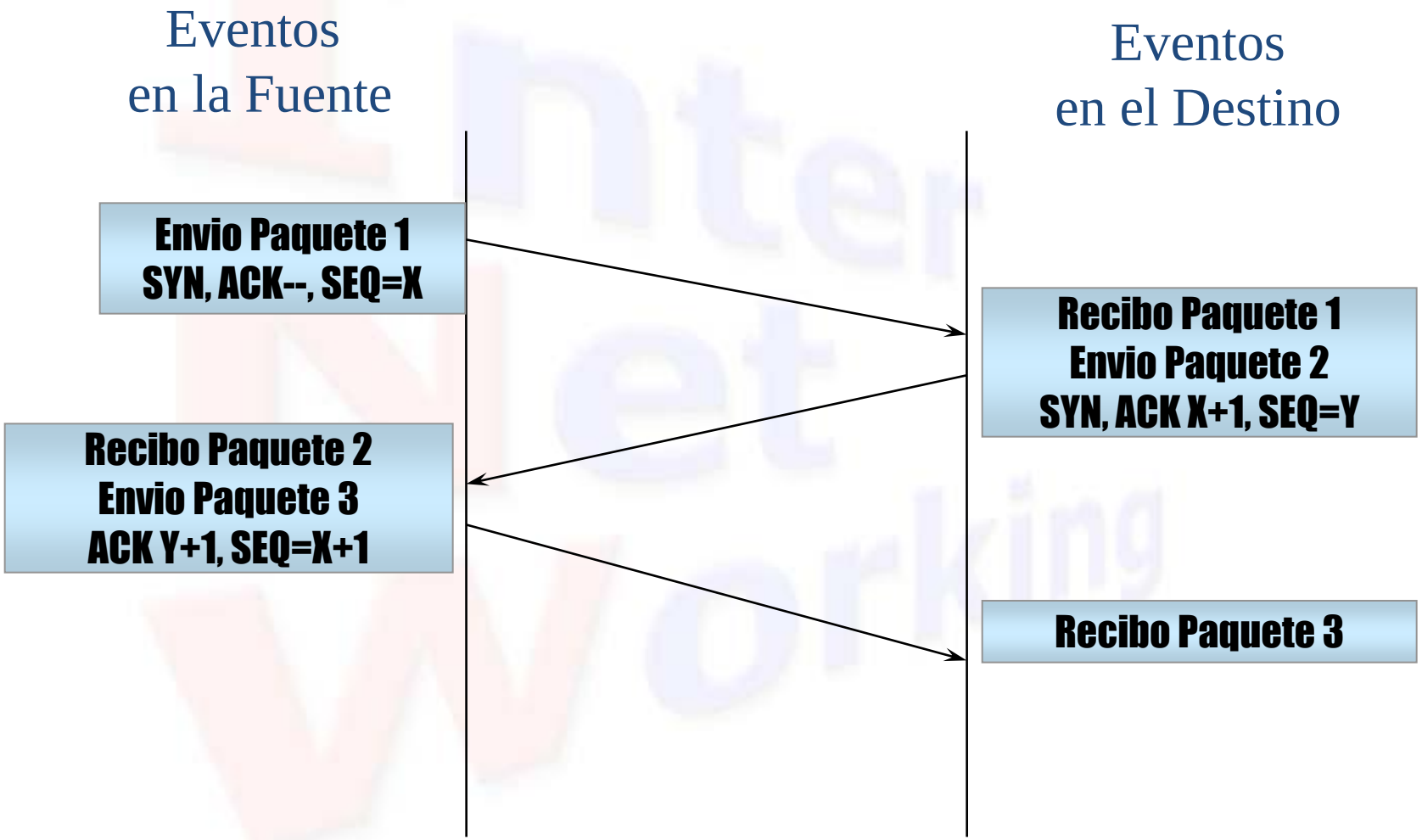
Control de Flujo y Congestión

- ACK con retransmisión.
- Control de flujo
  - Sliding Windows protocols.
  - Stop-and-wait protocols.
- Control de congestión
  - Ventana de Congestión.

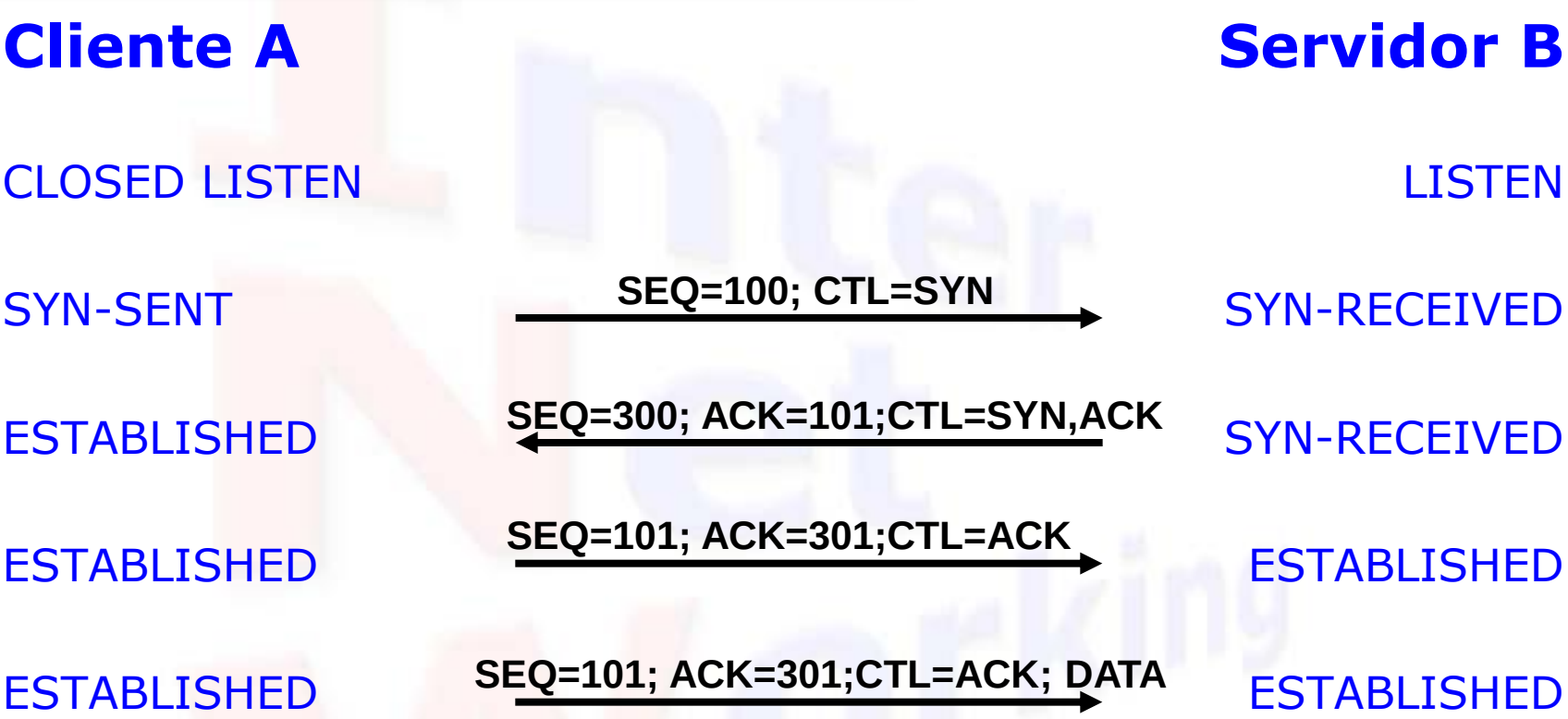
Confiabilidad



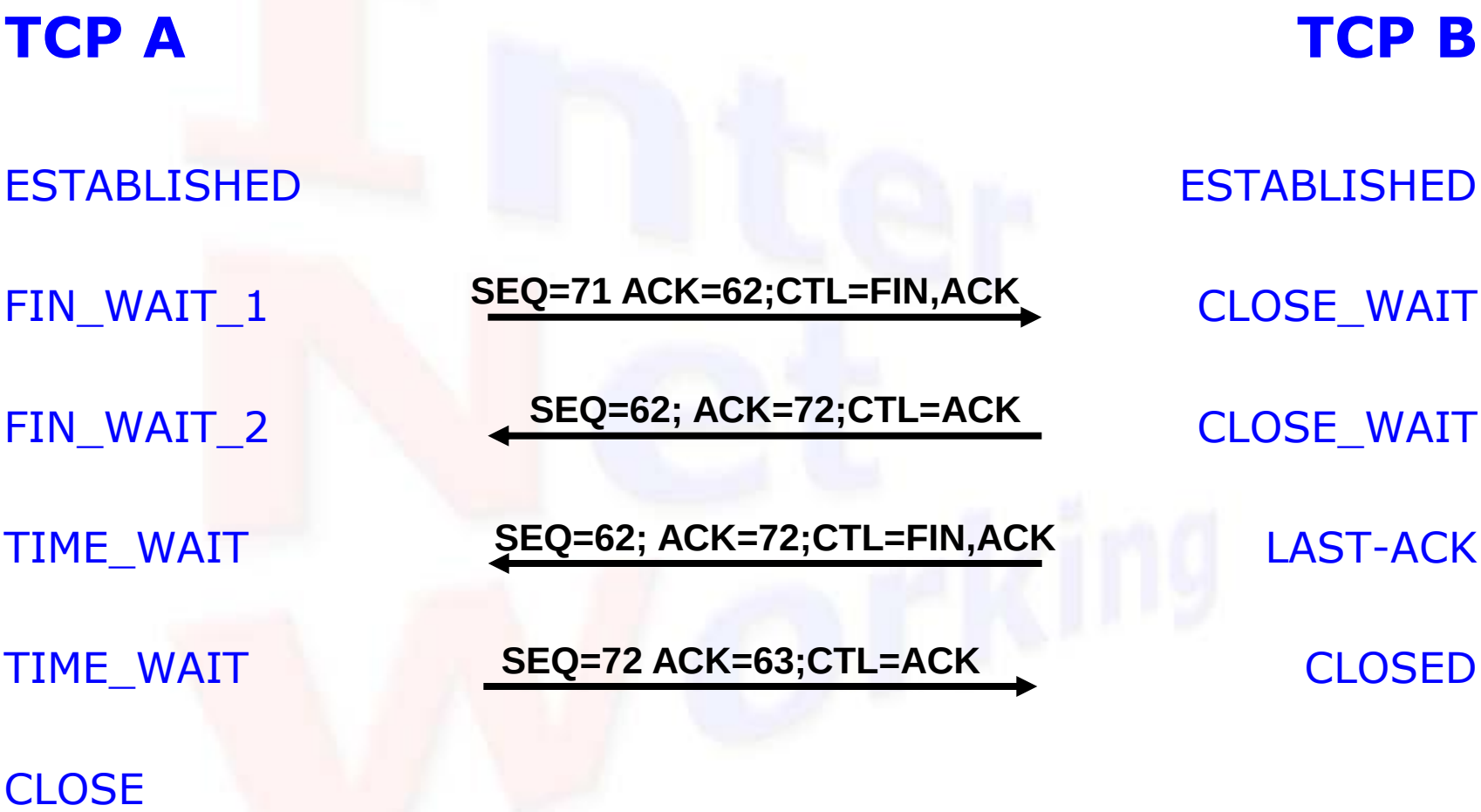
Inicio Conexión TCP: 3 way handshake



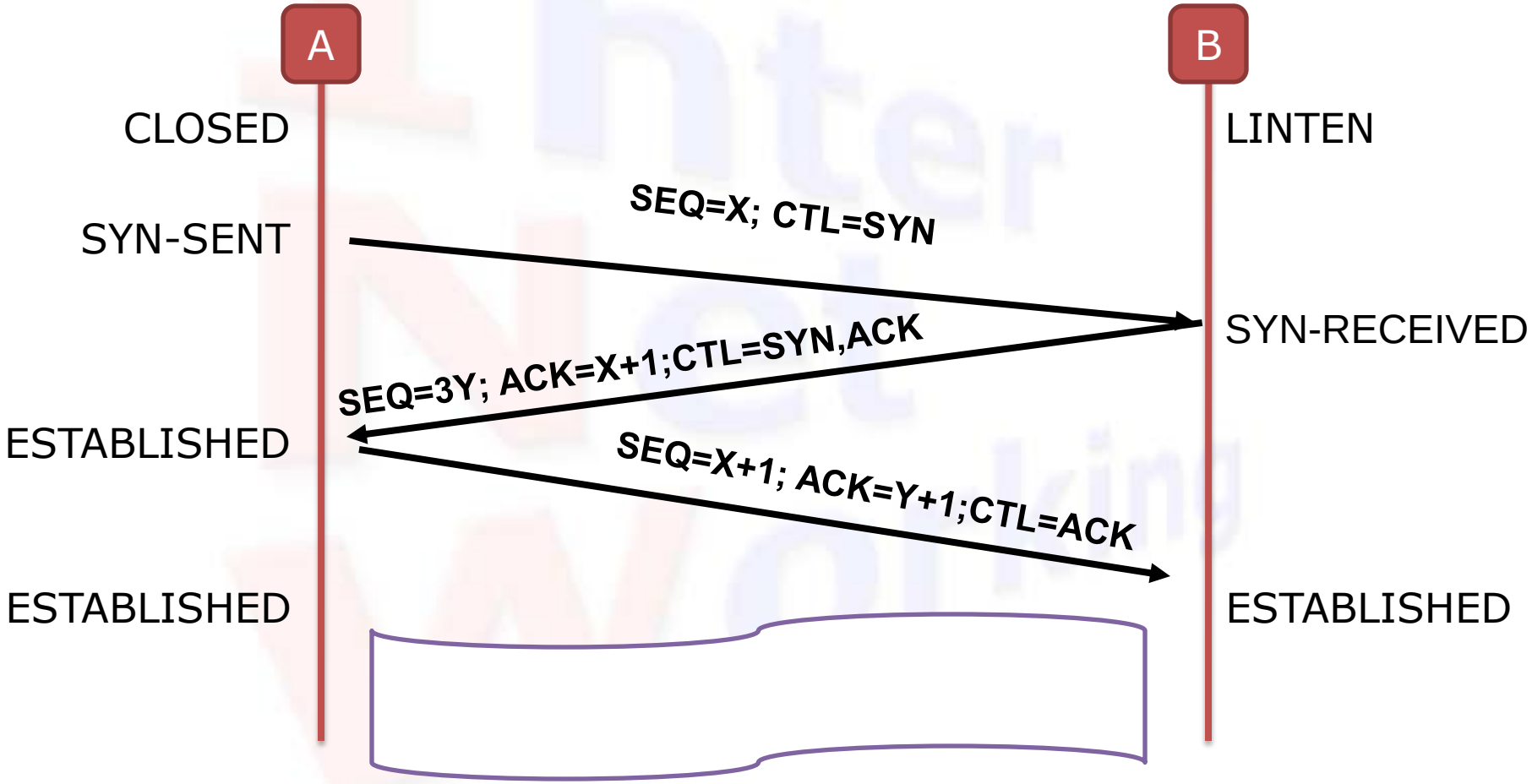
Secuencia Normal SYN



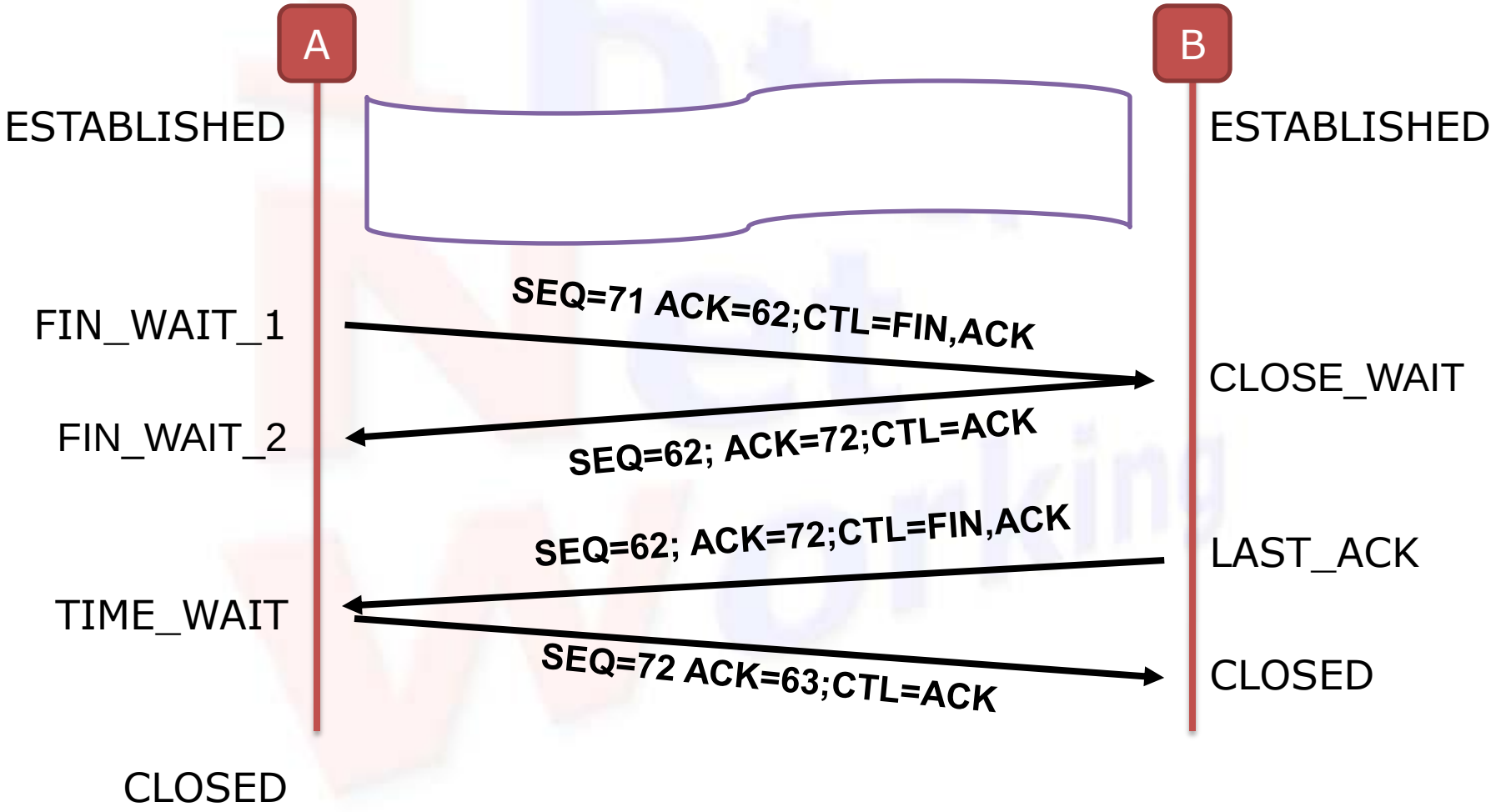
Secuencia Normal de FIN



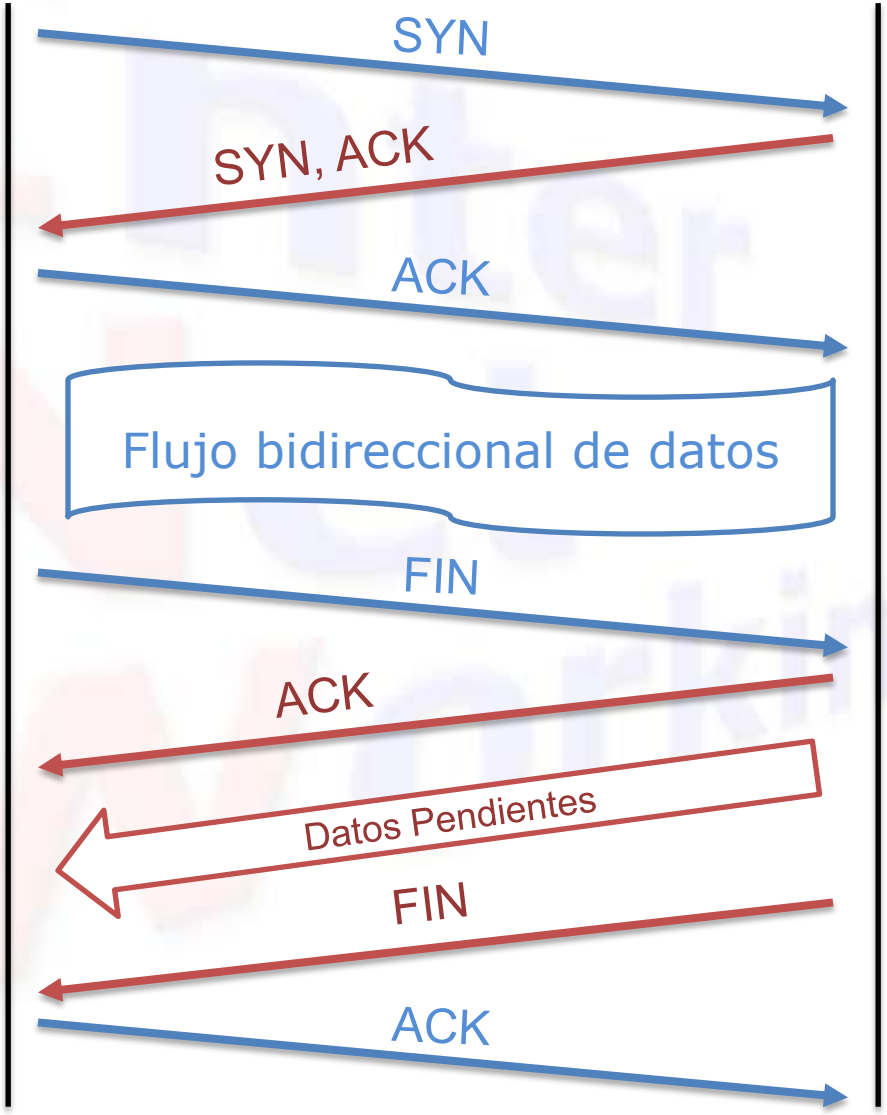
3 way handshake



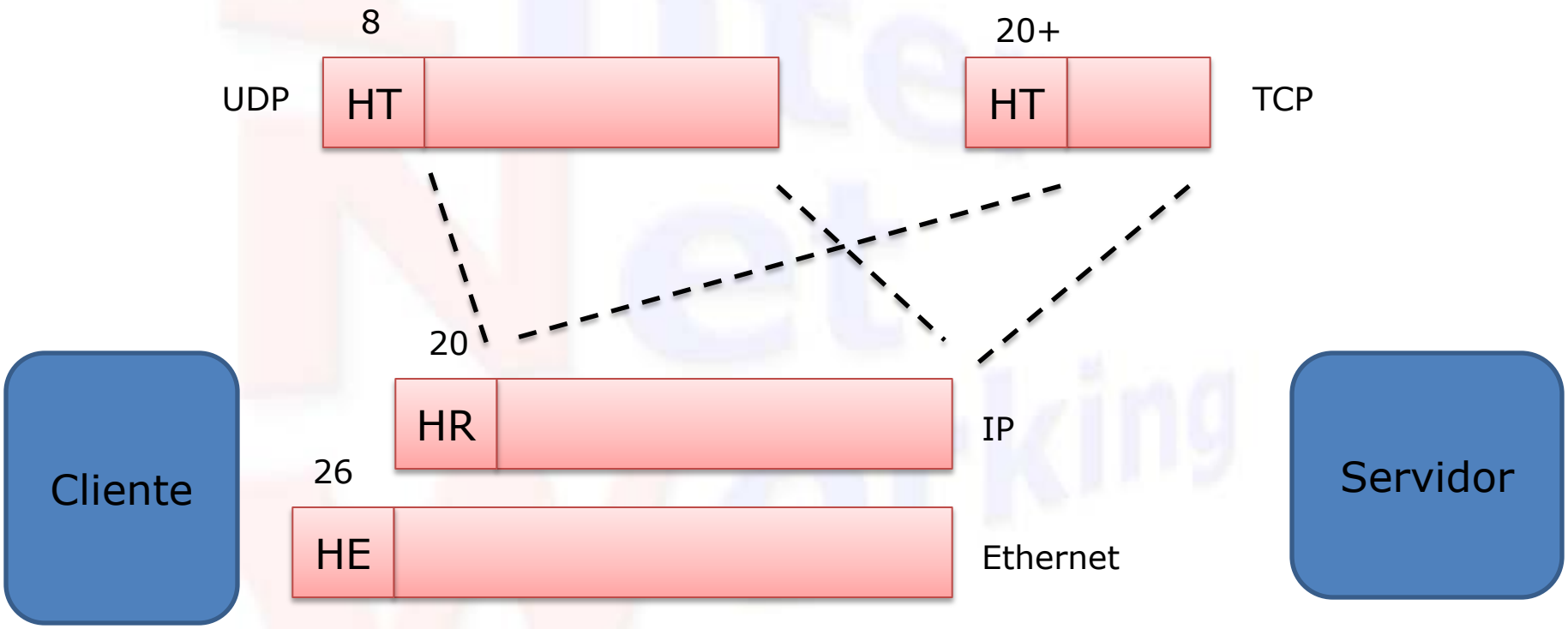
Secuencia Normal de FIN



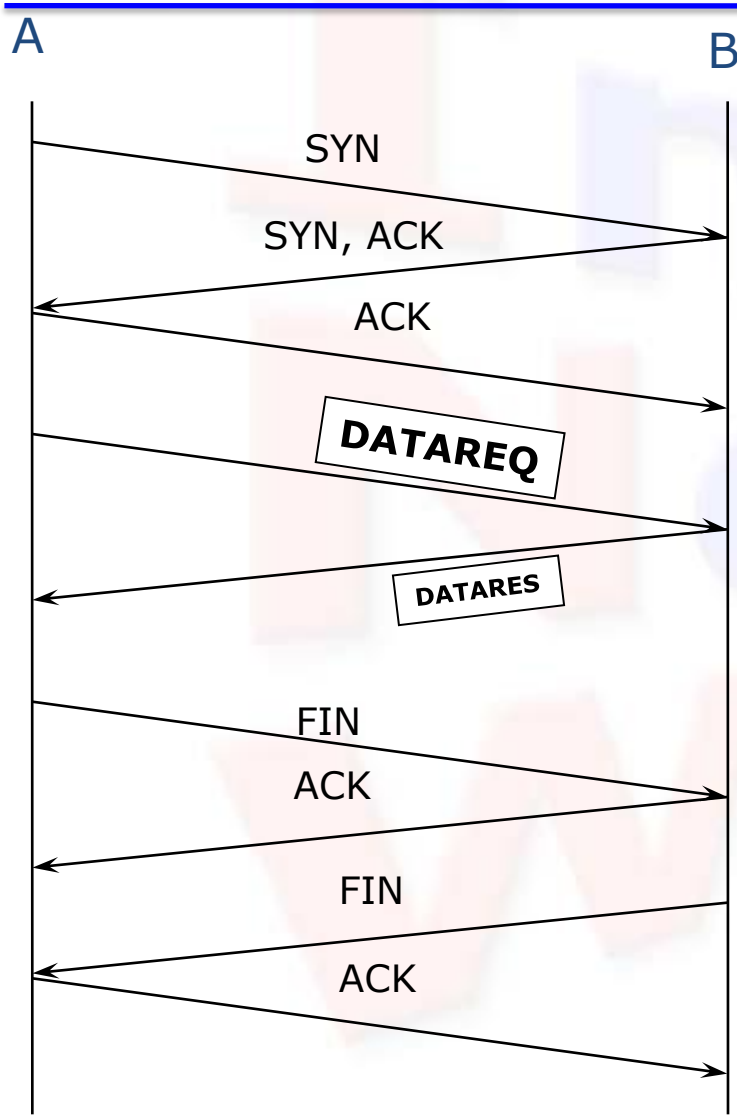
Inicio y Fin


SYN
SYN, ACK
ACK
Flujo bidireccional de datos
FIN
ACK
Datos Pendientes
FIN
ACK

Ejemplo Encapsulamiento



Conexión TCP Caso Estándar



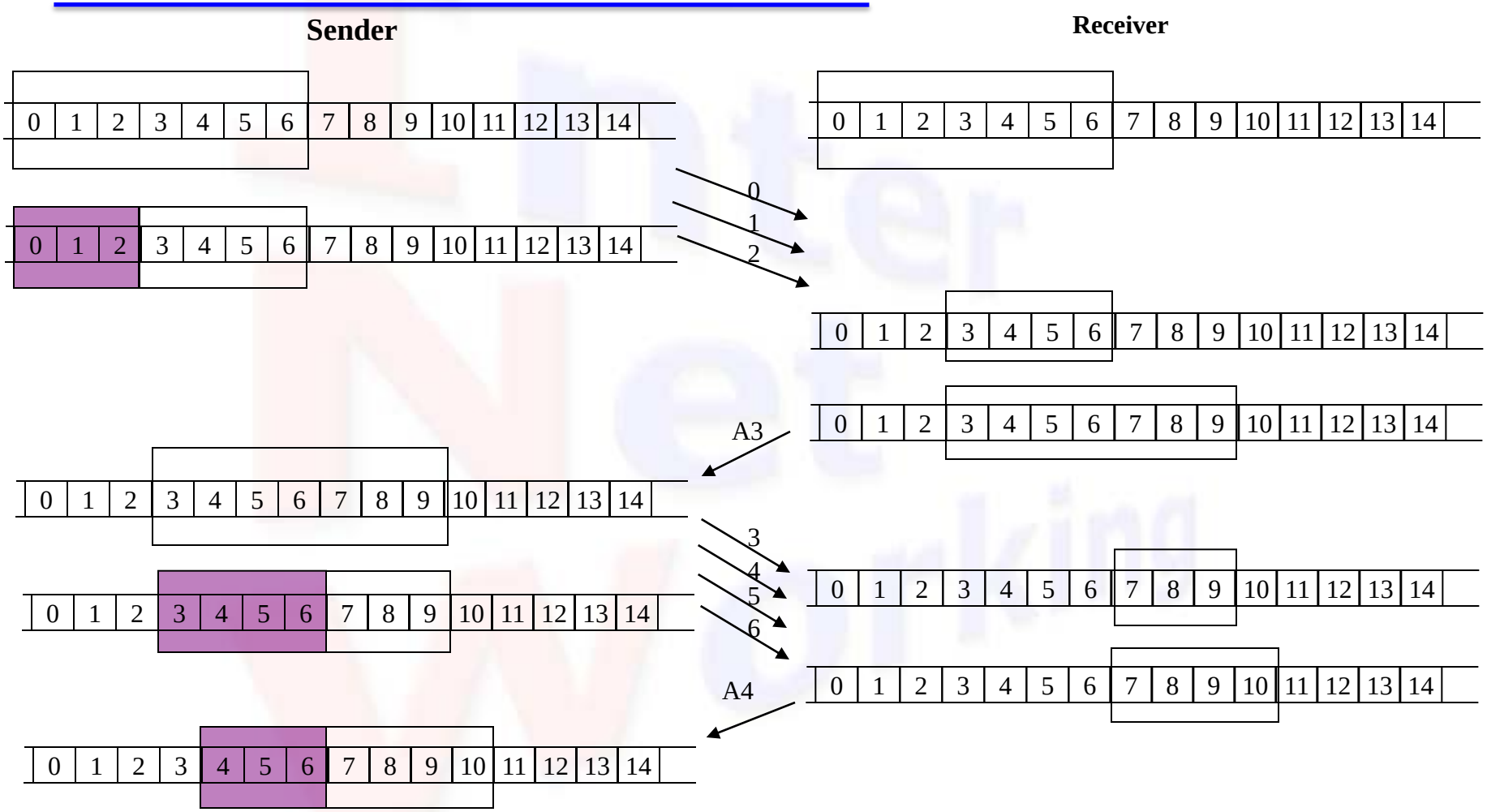
Inicio Conexión (132 Bytes):
IP:20 Bytes + TCP:28 Bytes
IP:20 Bytes + TCP:24 Bytes
IP:20 Bytes + TCP:20 Bytes

TRF Datos (132 Bytes):
IP:20 Bytes + TCP:20 Bytes+DATAREQ
IP:20 Bytes + TCP:20 Bytes+DATARES

Fin Conexión (160 Bytes):
IP:20 Bytes + TCP:20 Bytes
IP:20 Bytes + TCP:20 Bytes
IP:20 Bytes + TCP:20 Bytes
IP:20 Bytes + TCP:20 Bytes

TOTAL: 292+n*(80+DATAREQ+DATARES)

Ejemplo de ventana deslizante



Ventana óptima=RTT*BW

Control de Congestión

- RFC 2581
- Slow Start
  - Initial Window

$$IW = \min\left(4 * MMS, \max\left(2 * MSS, 4380\right)\right)$$

  - Control Window

$$CWND+ = MSS \qquad \left(CWND+ = 2 * MSS\right)$$

  - Slow Start Threshold

$$\text{ssthresh}_{\text{incial}} \approx\leq WINDOW$$

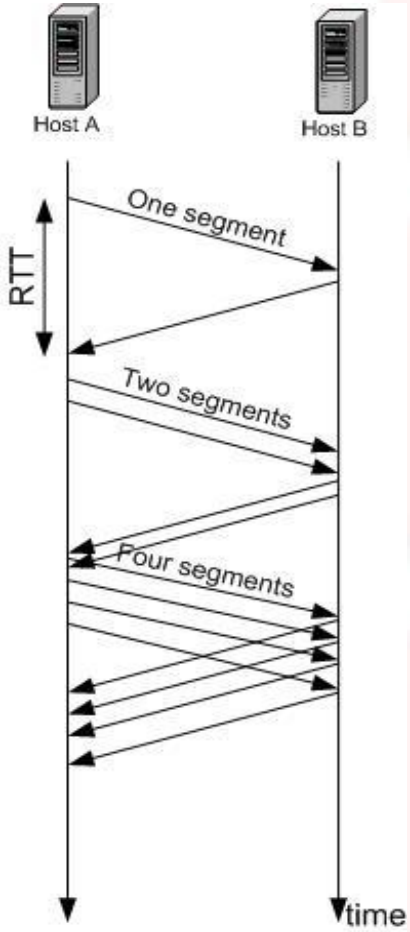
- Congestion Avoidance

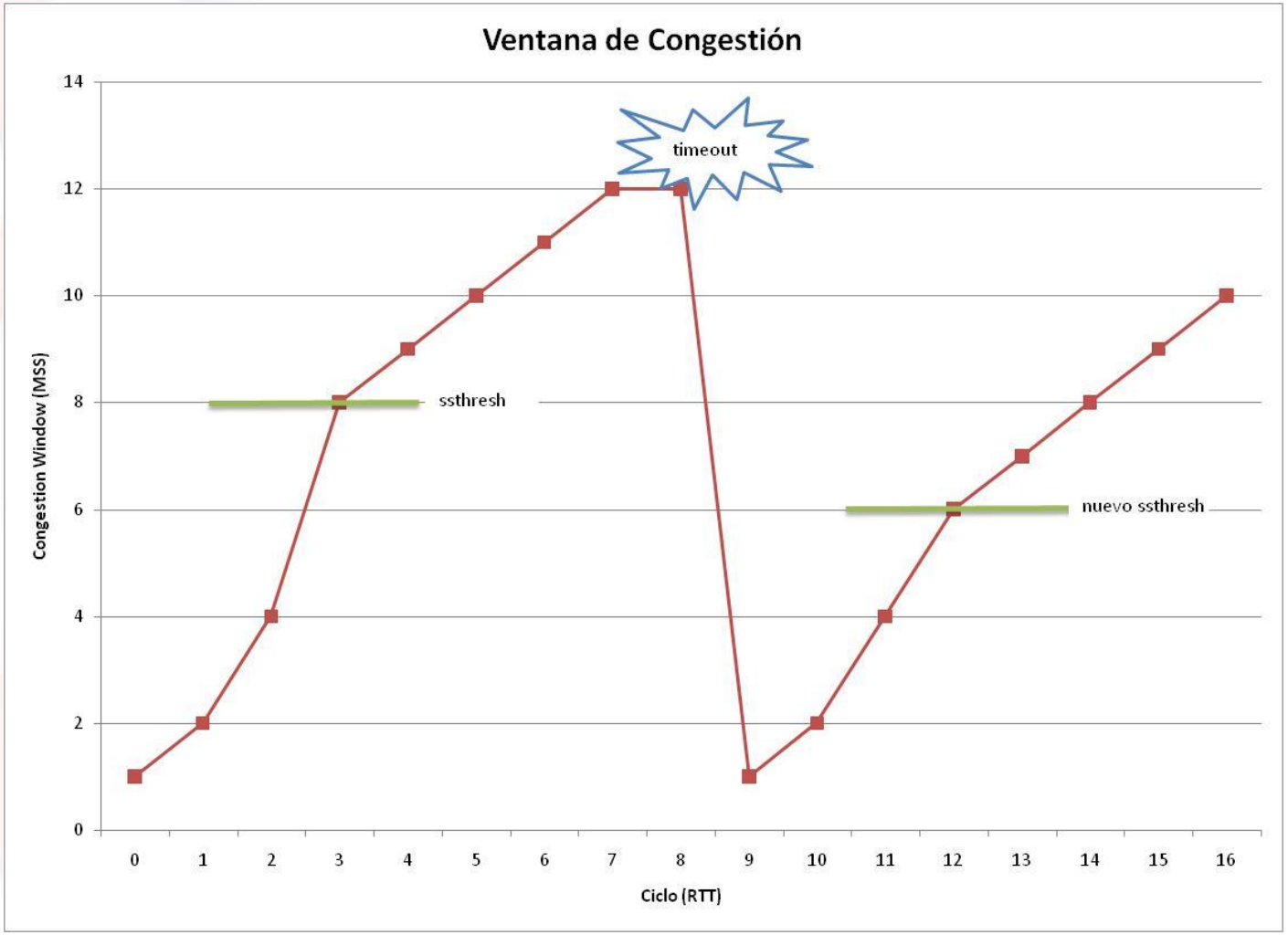
$$CWND+ = MSS * \frac{MSS}{CWND}$$

- Segment Loss

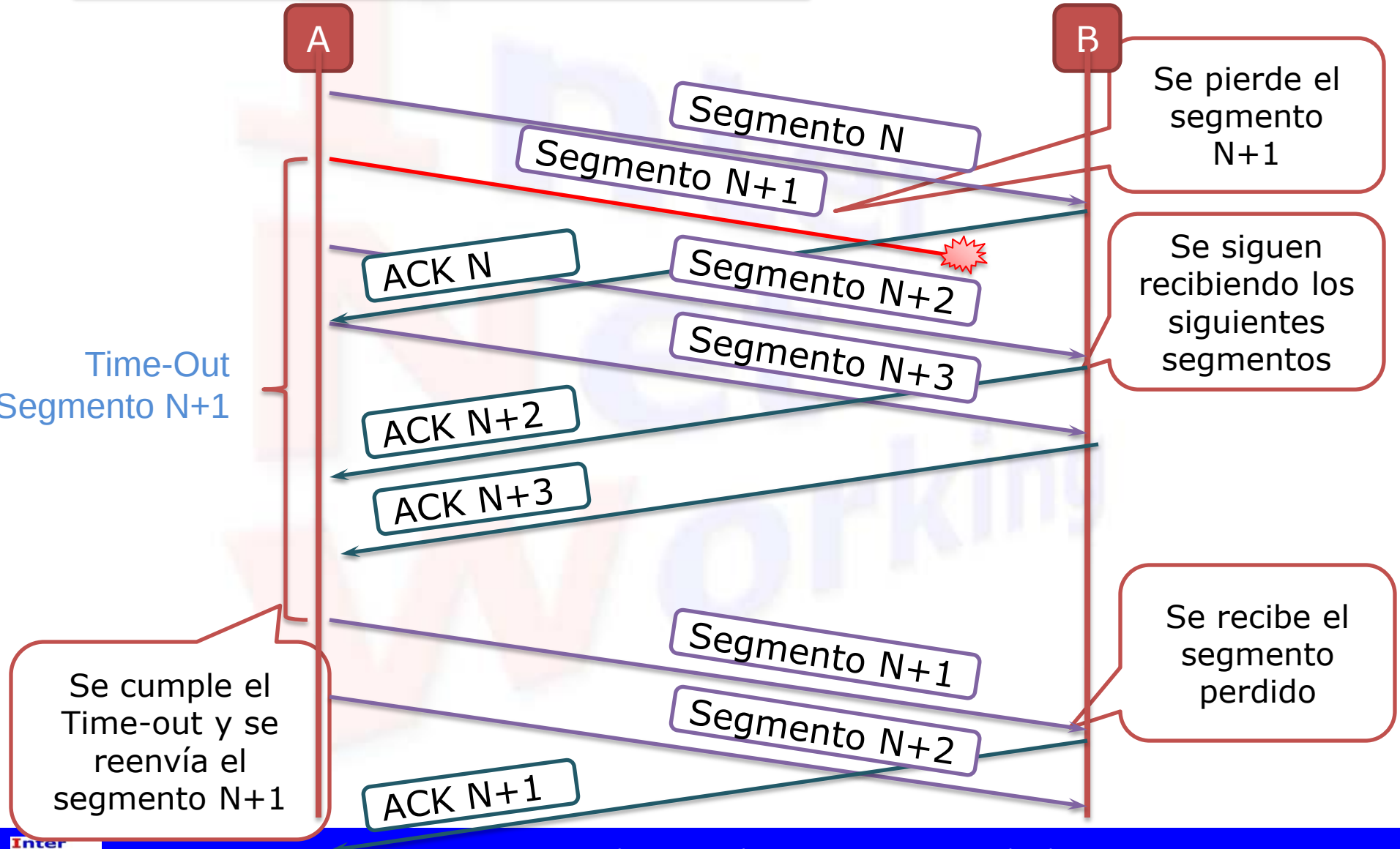
$$\text{ssthresh} = \max\left(\frac{\text{FlightSize}}{2}, 2 * MSS\right) \qquad CWND = MSS$$

Control de Congestión

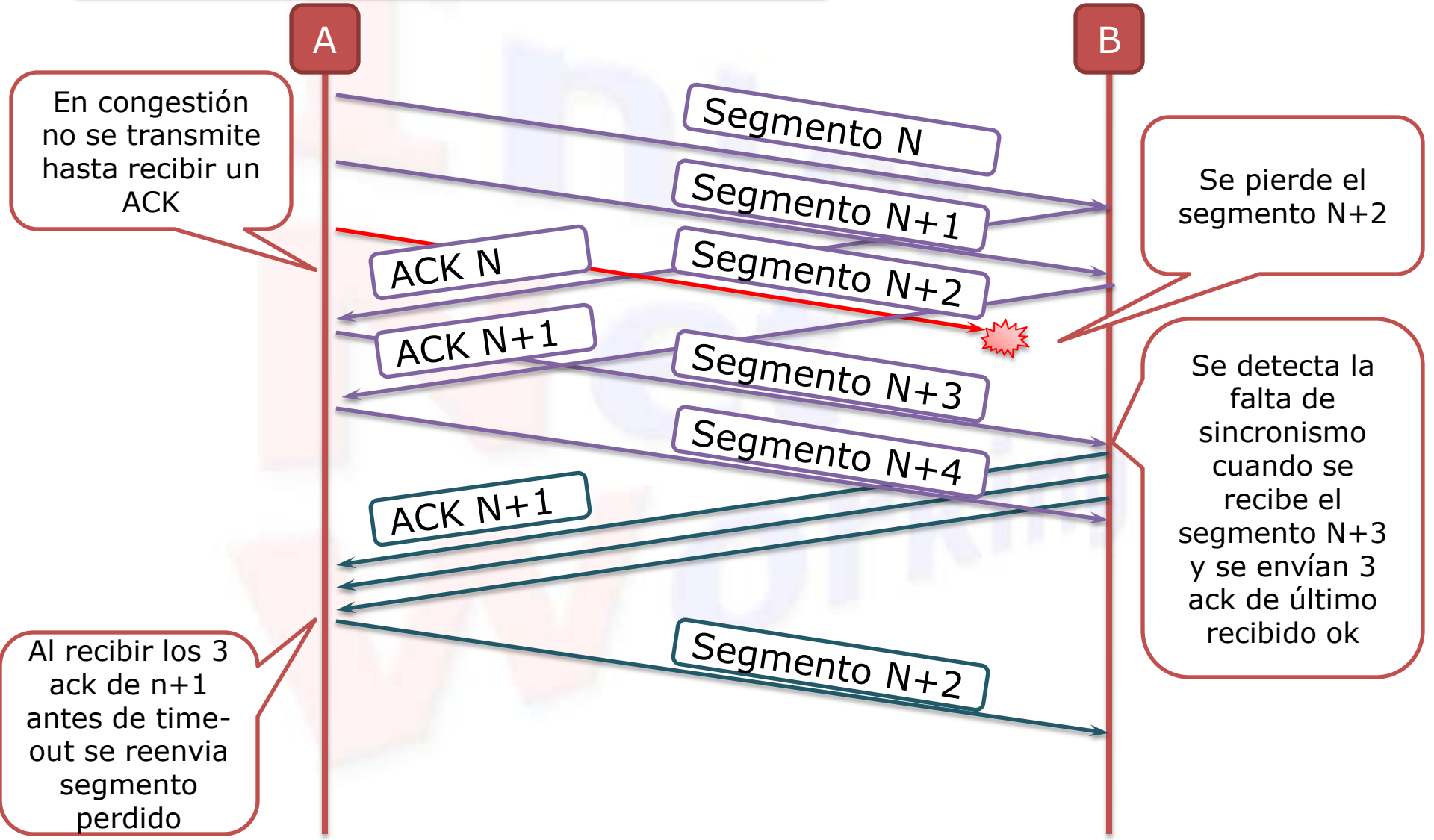




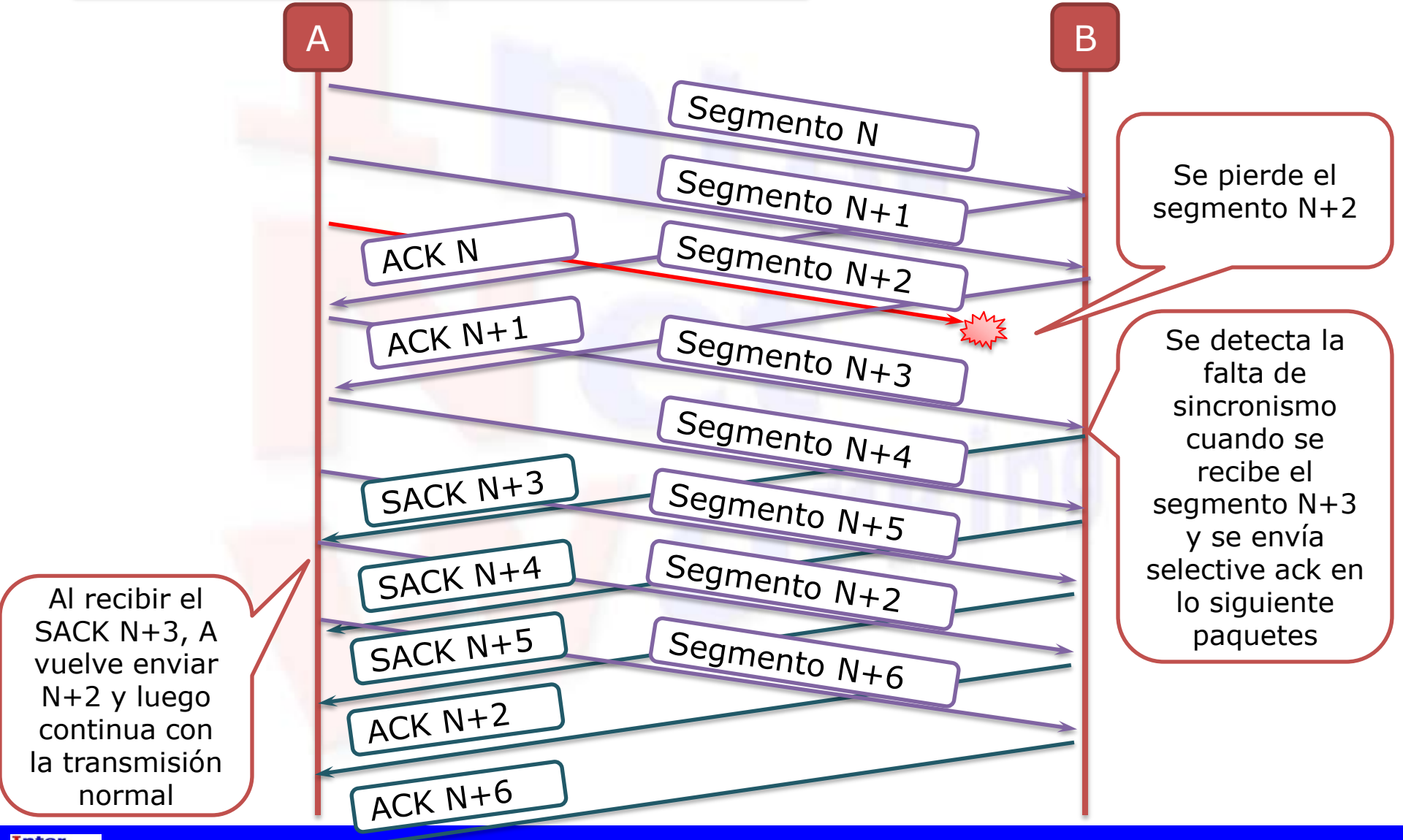
Pérdida y retransmisión por TimeOut



Pérdida y Fast Retransmit



Pérdida y Selective ACK



Fast Recovery

- Luego de Fast Retransmit se asume lo siguiente:
  - Slow Start Threshold

$$ssthresh = \max\left(\frac{FlightSize}{2}, 2 * MSS\right)$$

  - Control Window

$$CWND = ssthresh + 3 * MSS$$

Sincronización

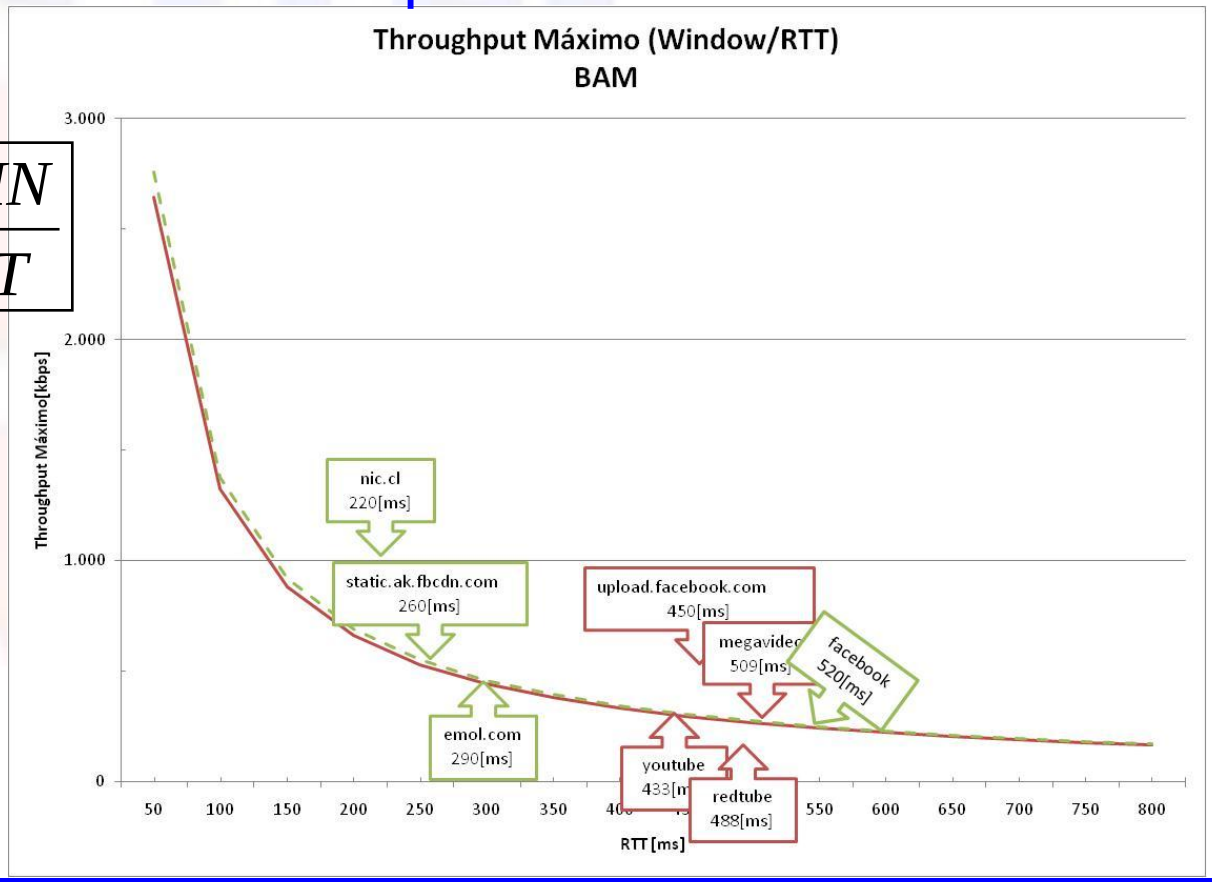
- Durante este proceso se establece:
  - MSS: Maximum Segment Size (MSS=MTU-H3-H4)
  - Window Scale: factor de escalamiento (2^x)
  - TCP Timestamps: permite medir el tiempo de viaje RTTM

Throughput

Throughput

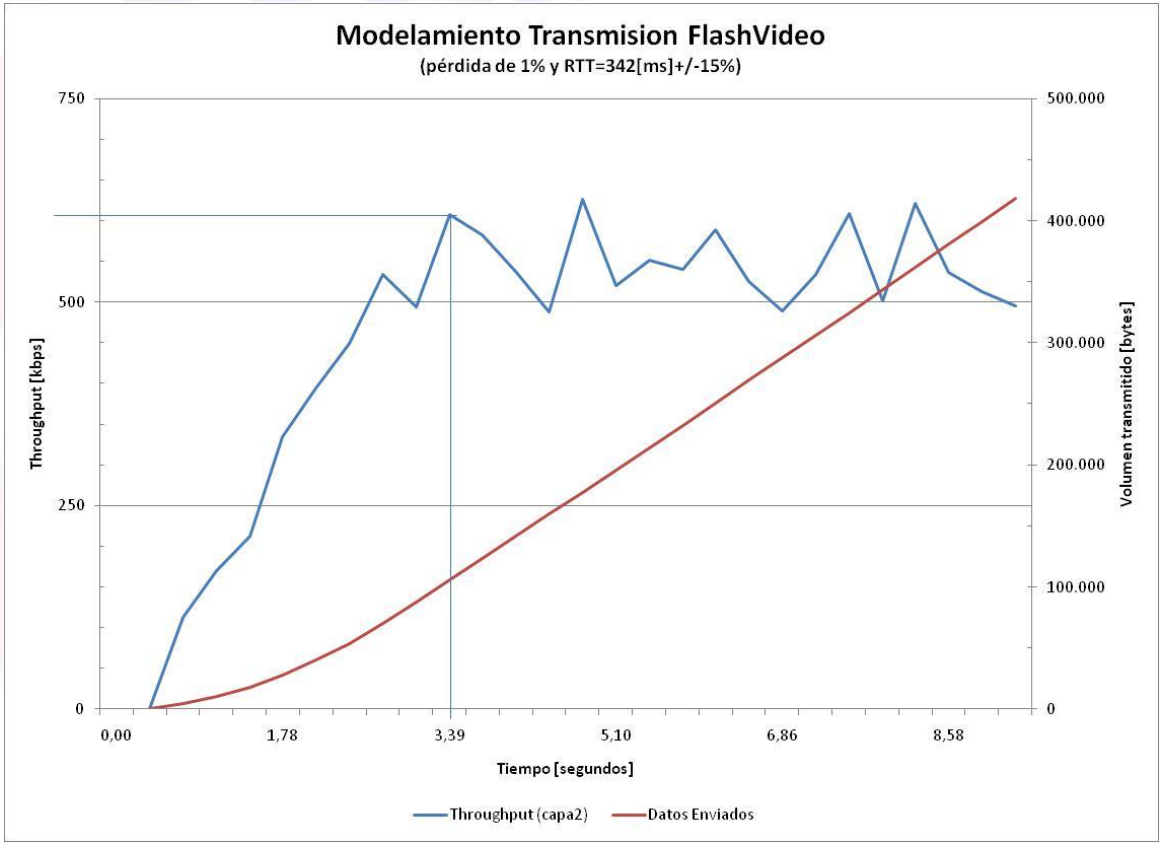
- El throughput de una conexión son los bytes enviados en un intervalos de tiempo. Si consideramos la forma de operar de TCP tenemos:

$$Throughput \leq \frac{RWIN}{RTT}$$



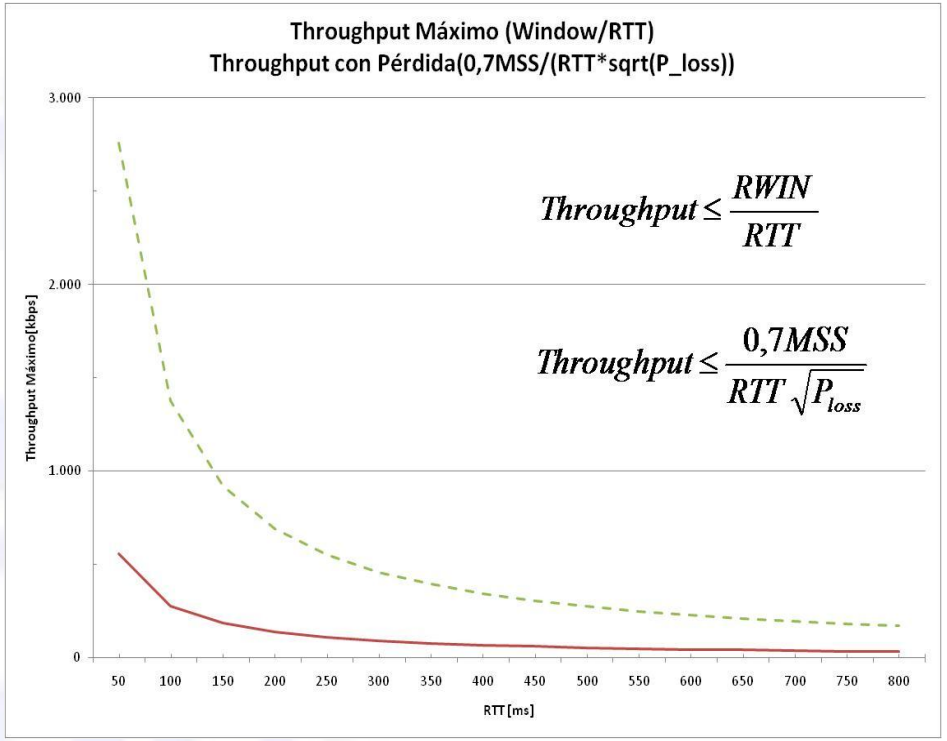
Throughput Máximo

- El throughput máximo no se alcanza inmediatamente sino al menos 10-12 ciclos luego de la conexión, ie, 10*RTT [s] y 124*MSS[Bytes] (3,42 segundos y 150KBytes)



Rendimiento: throughput

- Errores (Segment loss)
  - El tiempo de recuperación y la disminución del Slow Start Threshold afectan considerablemente el throughput.



$$throughput = \frac{tamaño\_paquete}{RTT\sqrt{\frac{2bp}{3}}}$$

RTT : round trip time
b : # de paquetes ack'ed por ACK (cuando se usa Selective ACK)
p : razón de pérdida=paquetes pérdidos/total

LAN Switching

Ethernet IEEE 802.3

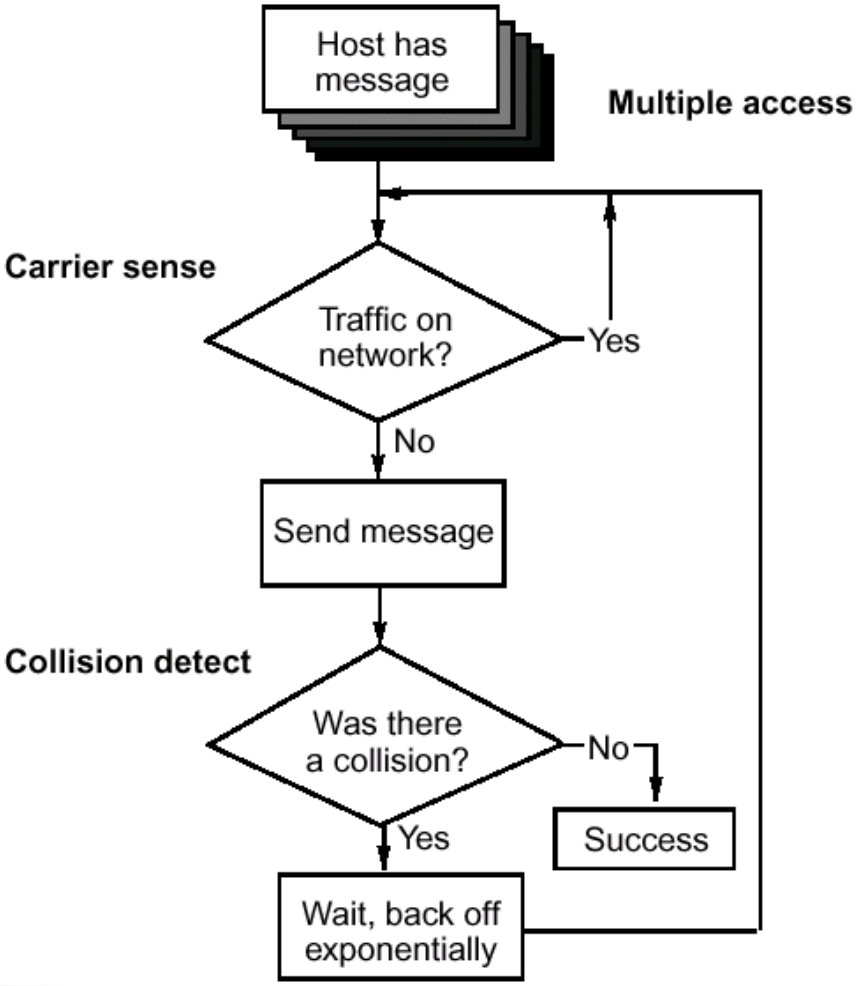
Características

- Desarrollado por DEC, Intel y Xerox
- Fue estandarizado en IEEE 802.3
- Utiliza CSMA/CD
- Codificación Manchester
- Medio físico compartido
- Transmisión asíncrona
- Cada nodo es Tx y RX
- Cada nodo tiene su reloj
- Tamaño de frame mínimo y máximo
- Distancia máxima (en un dominio de colisión)

CSMA/CD

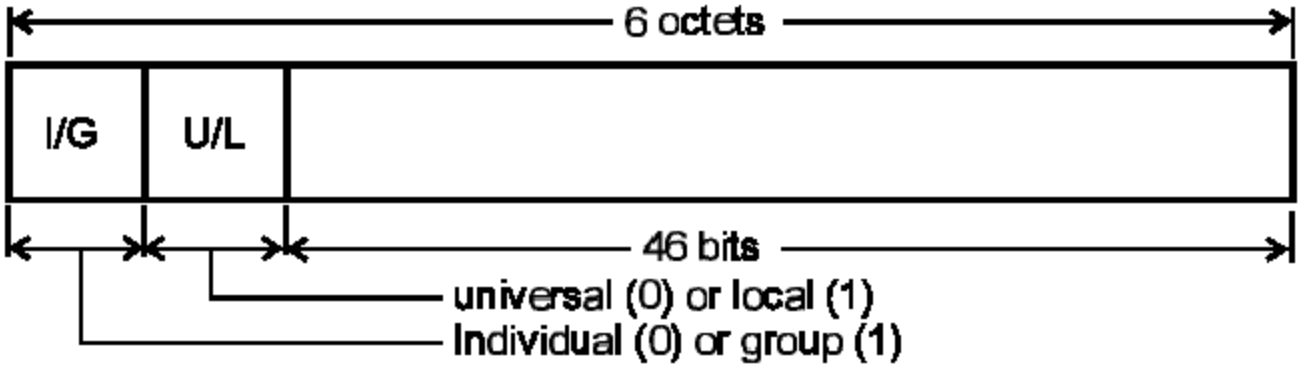
- Carrier Sense Multiple Access Collision Detection
- Evolución
  - Aloha Puro
  - Slotted Aloha
  - CSMA (Carrier Sense Multiple Access)
  - CSMA/CD (Collision Detection)
- Funcionamiento
  1. Escucha si el medio esta siendo utilizado por algún sistema.
  2. Espera a que el medio esté libre
  3. Si hay colisión espero tiempo aleatorio y reintento (Algoritmo Backoff)

Diagrama de Flujo CSMA/CD

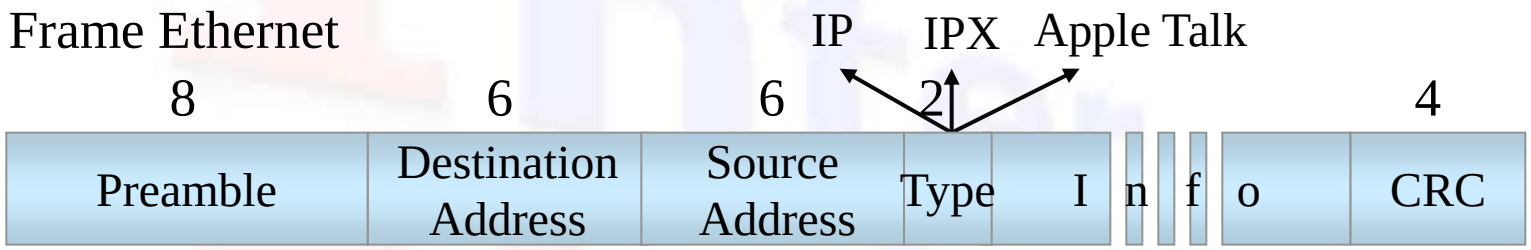


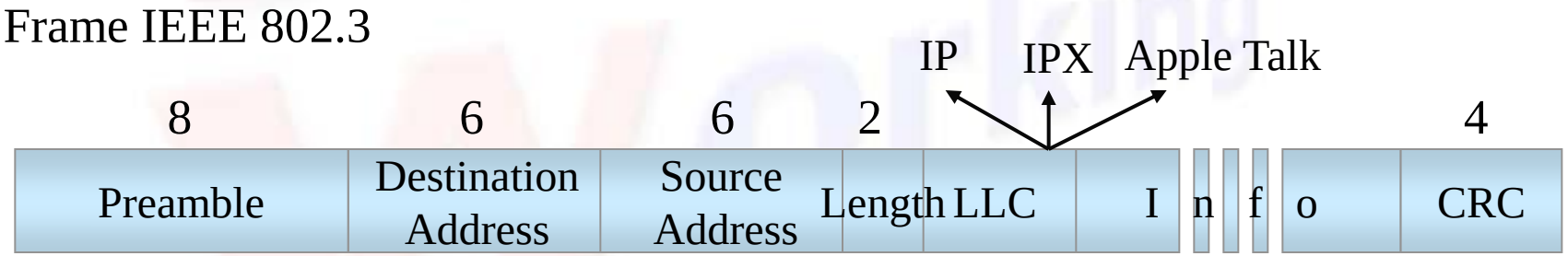
Direccionamiento Ethernet

- Los host poseen una dirección de interfaz de red única de 48 bit (12 digitos Hexadecimales)
- Primero 3 octetos representan al vendor y los restantes a la interfaz de red
- Tipos de Direcciones:
  - Unicast (08:0:20:77:dc:7b)
  - Broadcast (FF:FF:FF:FF:FF:FF)
  - Multicast (01:00:5E:xx:xx:xx)



Frame Ethernet y IEEE 802.3

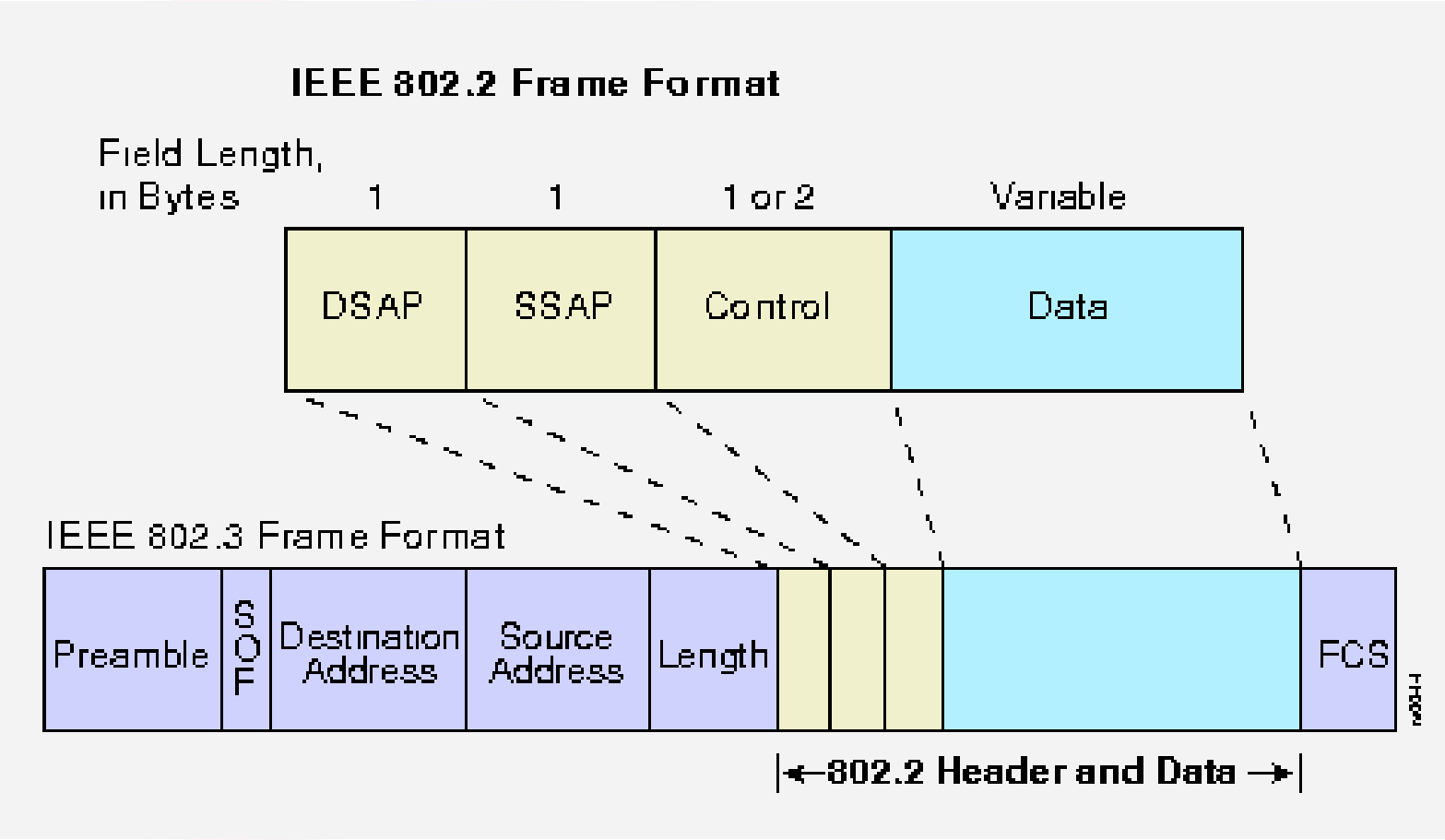




Descripción de Campos del Frame

- Preamble
  - Compuesto de unos y ceros es usado para la sincronización y determinar cuando un frame comienza.
- Destination address
  - Dirección Ethernet del host destino.
- Source address
  - Dirección Ethernet del host origen.
- Type
  - Describe el tipo de datos que se está encapsulando (como IP, ICMP, ARP, o RARP).
- Data
  - Información que envia la aplicación.
- CRC
  - Se usa para la detección de errores.

Frame IEEE 802.3 con IEEE 802.2



Distancia Máxima v/s Frame mínimo

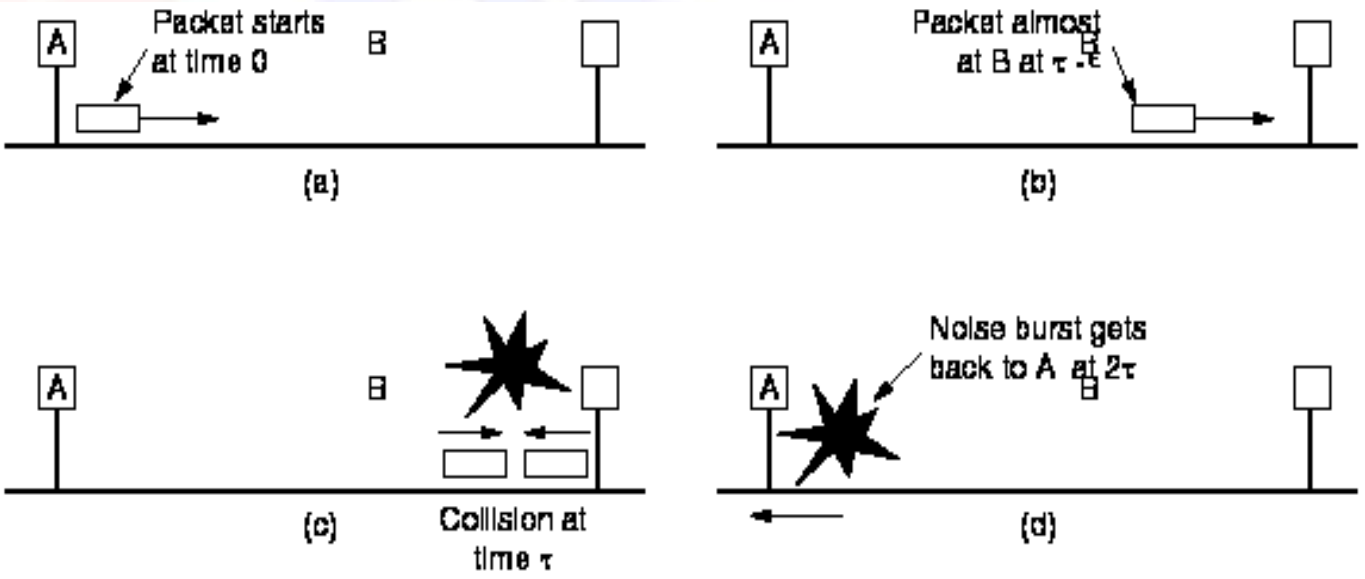


Fig. 4-22. Collision detection can take as long as 2τ.

Spanning Tree Protocol

Descripción

- Spanning Tree Protocol – STP
  - Protocolo que previene loops de capa 2.
  - Se implementa por interfaz.
  - Se crea un árbol identificando un nodo raíz.
  - Es implementado tanto en switch como en bridges.

Estados de las Interfaces

ESTADO	Reenvia Frames	Aprende MAC	Tipo de Estado
Blocking	NO	NO	Estable
Listerning	NO	NO	Transitorio
Learning	NO	SI	Transitorio
Forwarding	SI	SI	Estable

- Listening y learning son estados transitorios cuando cambia de root el árbol.
- En el estado learning las direcciones MAC pueden ser aprendidas basadas en frames entrantes.

Tiempos entre estados

- Tiempos entre estados.
  - Max-Age : 6 a 20 seg. (20 seg)
    - Blocking →Listening
    - Lifetime de una BPDU
  - Forward Delay: 4 a 30 sec. (15 seg.)
    - Listening → Learning
    - Learning → Forwarding
  - Hello Interval : 2 sec, min 1 sec
    - intervalo de transmición de BPDUs desde el root).

Operación

- Todas las interfaces del árbol están en modo forwarding
- Cada bridge que no es root considera una de sus puertas para tener menor distancia administrativa entre el mismo y el bridge root. Esta interfaz llamada puerta de bridge root es puesta en estado forwarding.
- Existen los mensajes BPDU (Bridge Protocol Data Unit) que se utilizan para controlar el protocolo

Operación 2

- Los bridges intercambian el Bridge ID (MAC) y eligen al root (MAC menor). Todas las interfaces están inicialmente en estado forwarding
- Cada bridge recibe BPDU desde el root. La puerta por la cual recibe el BPDU con menor costo es llamado la puerta al bridge root, esta puerta es puesta en estado forwarding.
- Las otras interfaces son puestas en estado blocking.
- El root envía BPDU cada "Hello time" segundos. Los otros bridges escuchan los BPDU y saben que nada ha cambiado. El Hello time es definido por el BPDU.
- Si el bridge no recibe el BPDU por un tiempo determinado es causa que el spanning tree ha cambiado y se debe elegir otro root.
- Algunas interfaces cambian a forwarding desde blocking o viceversa.
- Pueden ocurrir loops temporales dentro de los cambios.

Operación 3

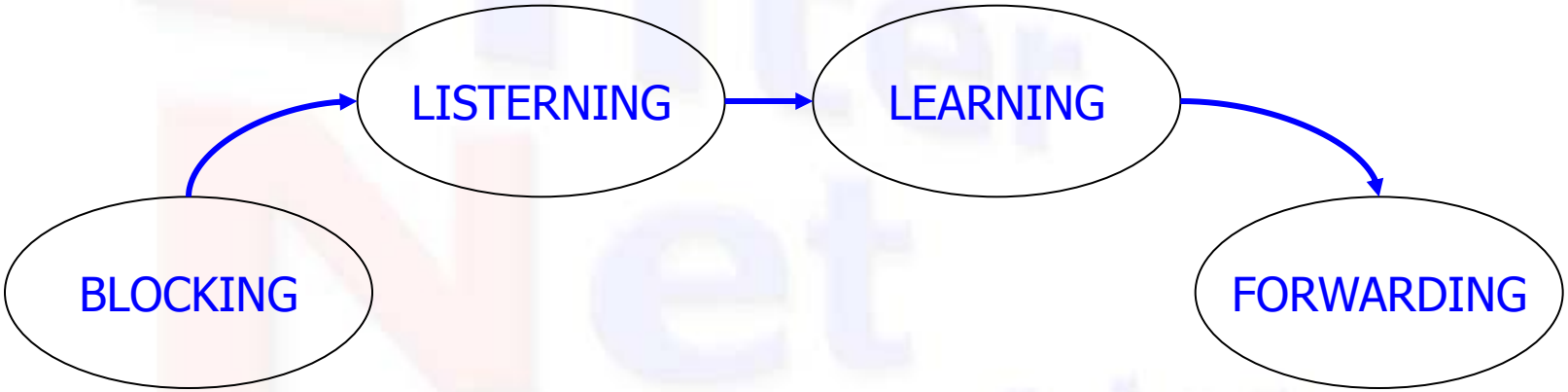


Diagrama de Funcionamiento 1

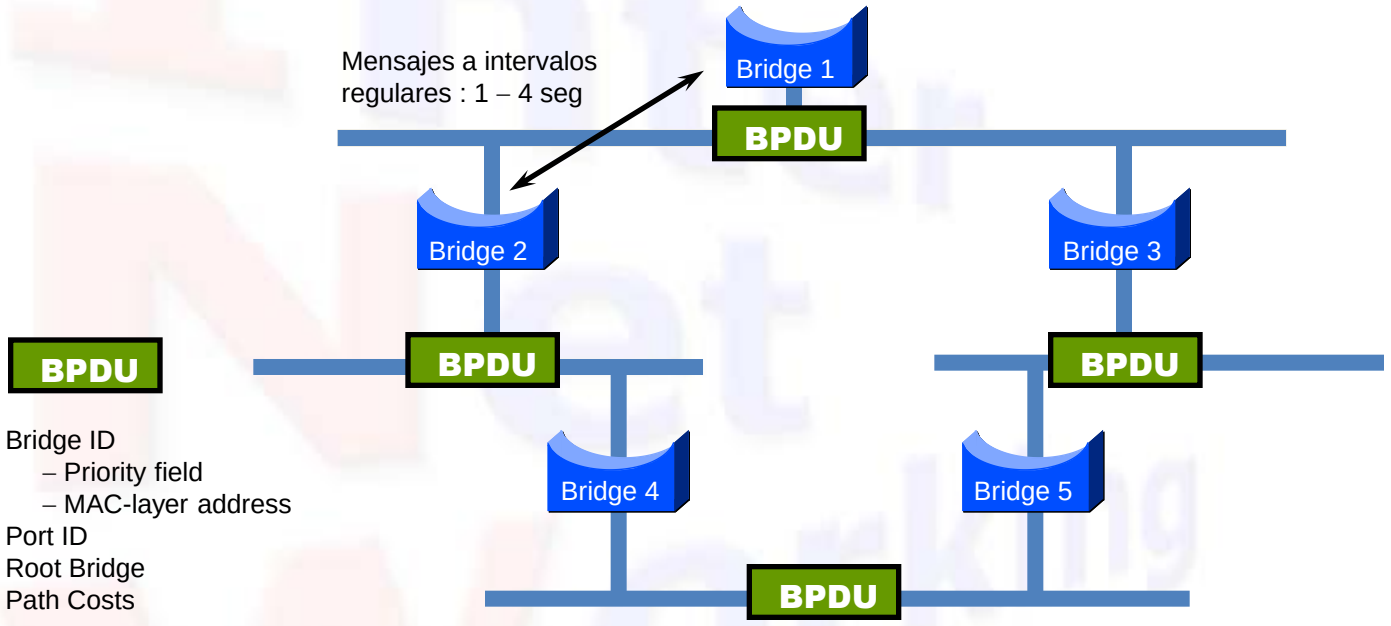
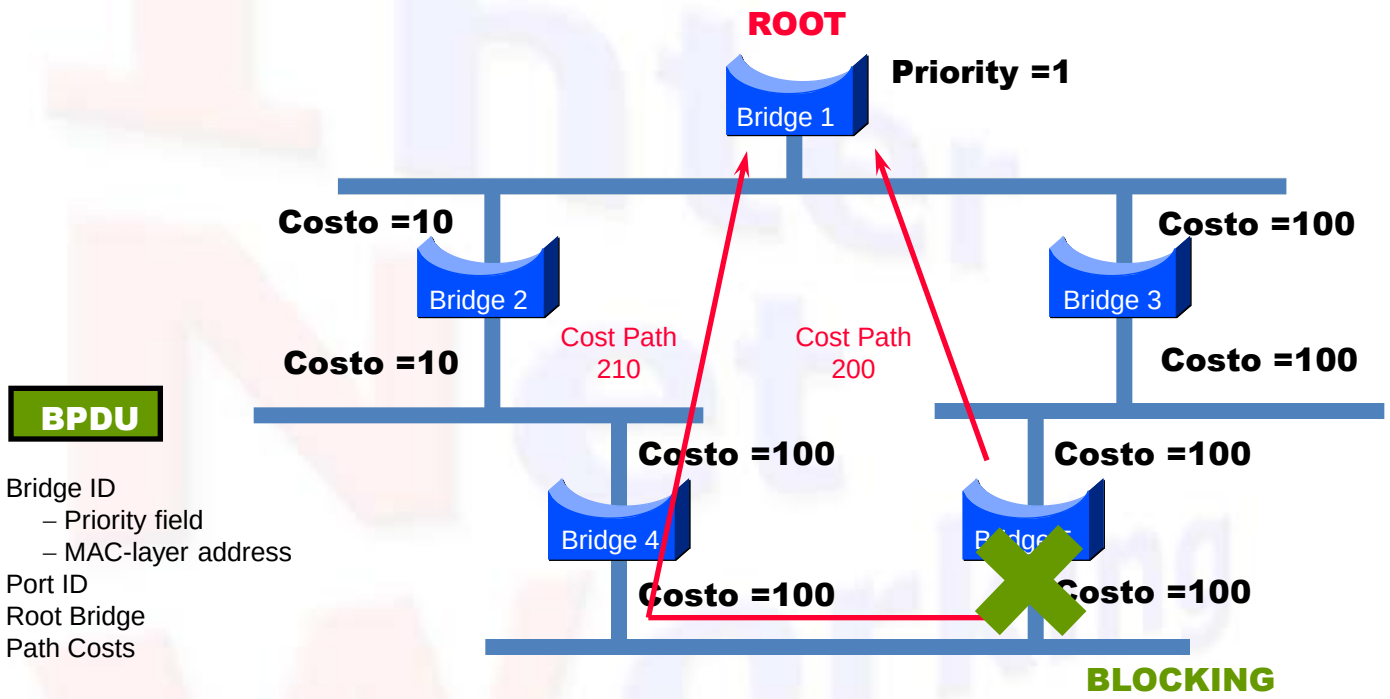


Diagrama de Funcionamiento 2

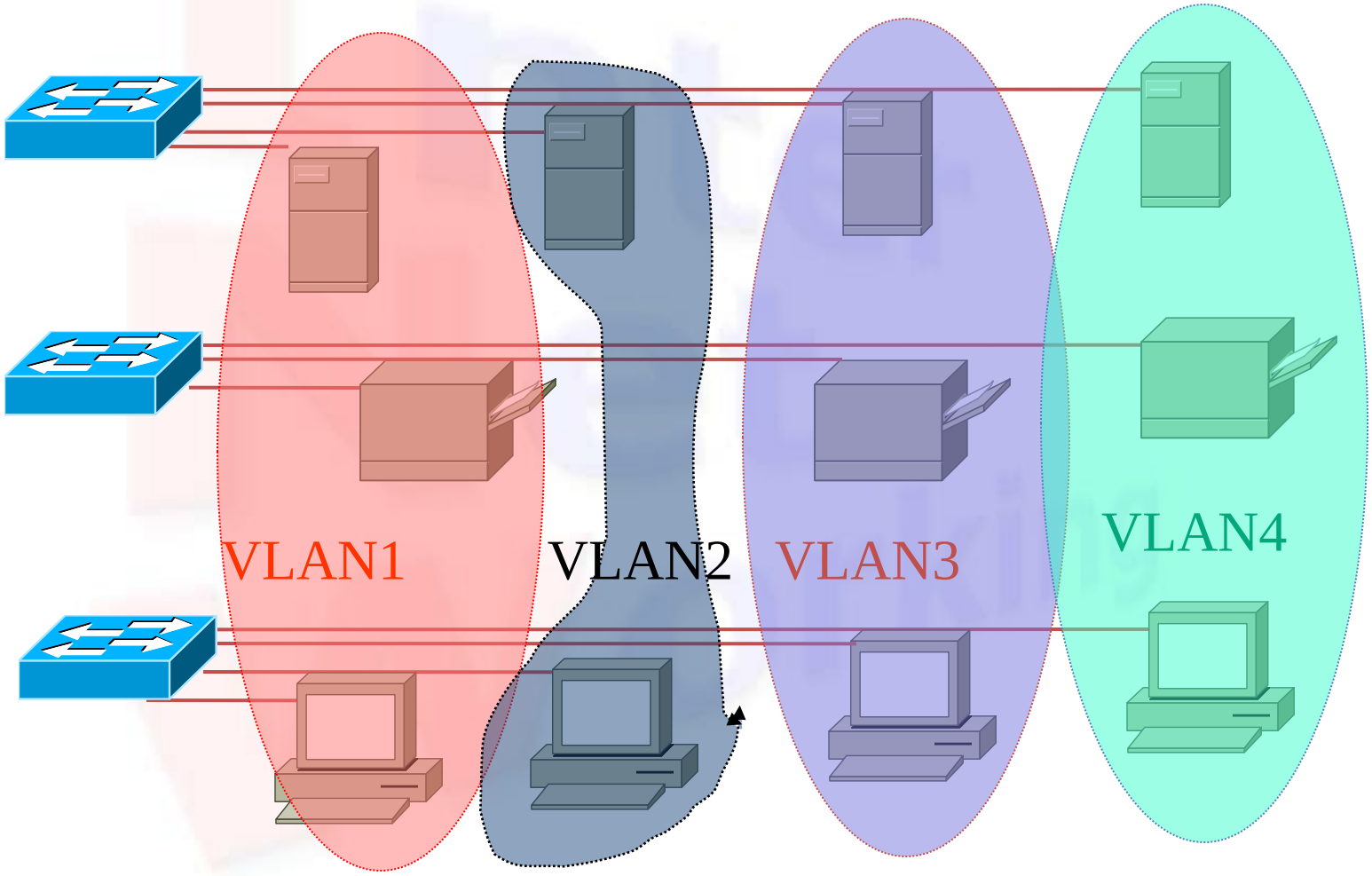


Variaciones de STP

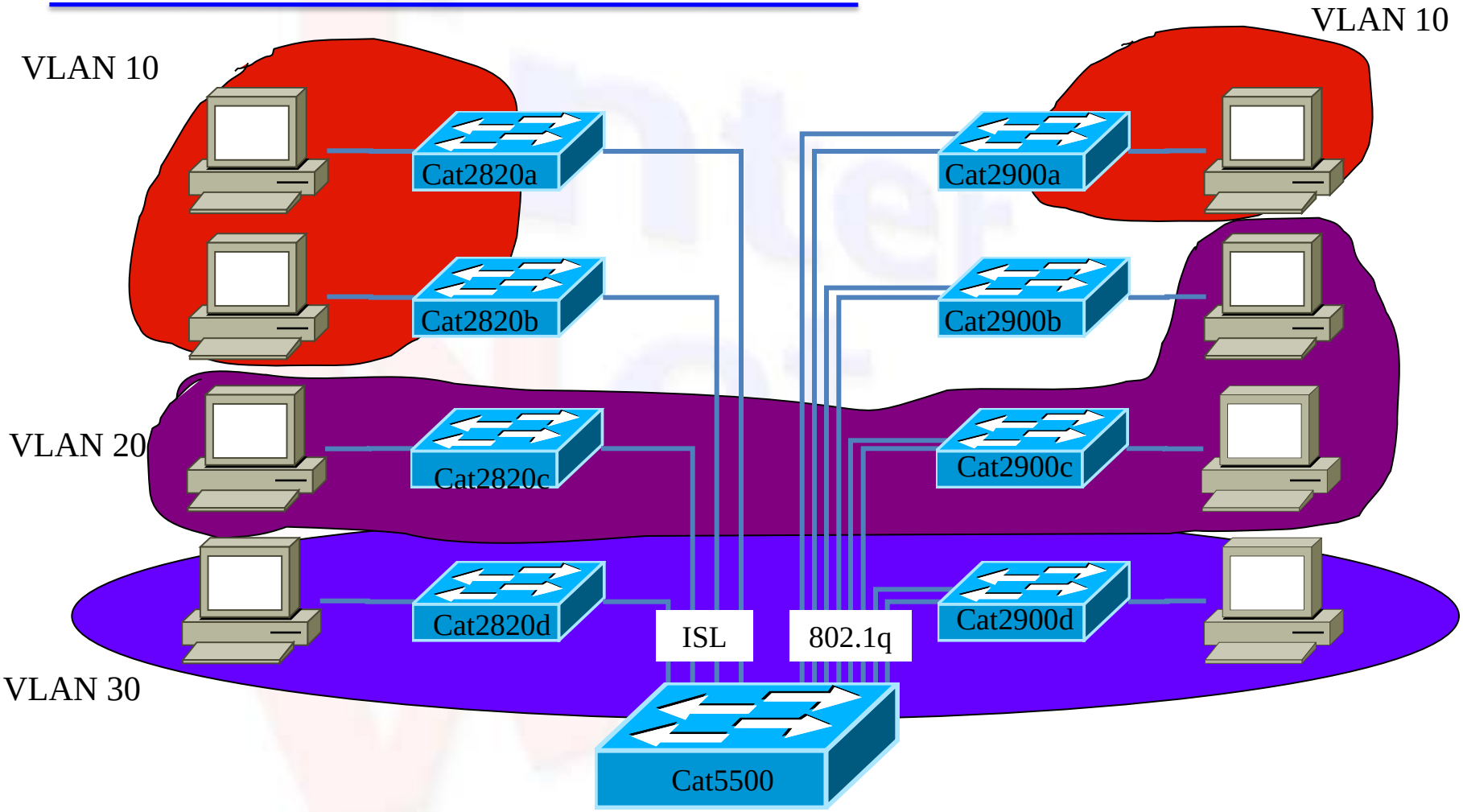
- CST : Common STP (802.1Q)
- PVSP : STP por VLANs. (ISL)
- PVST+ : Propietario de Cisco que permite pasar información CST hacia PVST.

VLAN: Virtual LAN

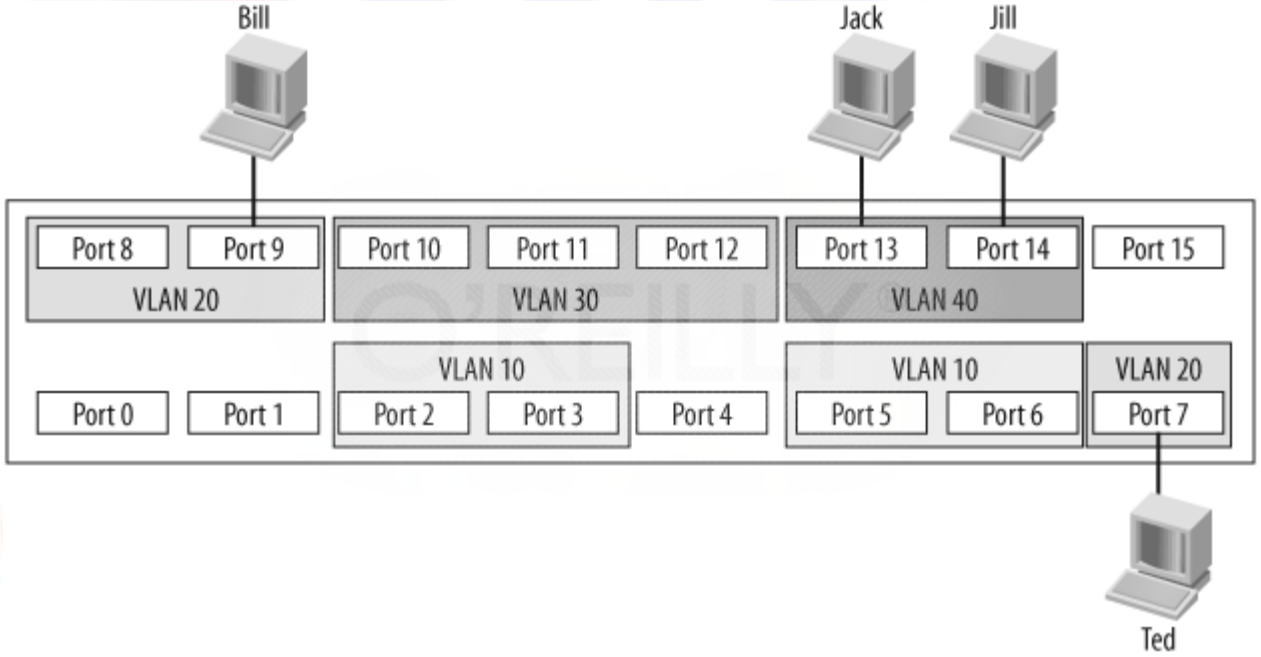
VLAN



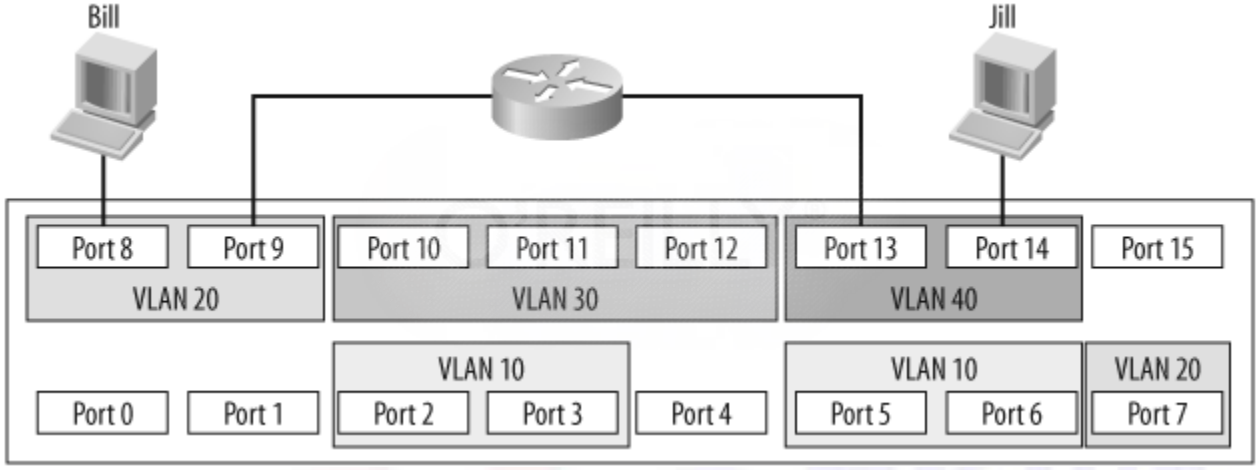
Independiente de la Topología y Tecnología usada



Configuración en Equipos



Comunicación entre VLAN



VTP: Virtual Trunk Protocol

Trunking

- Tecnología que permiten identificar tráfico de diferentes VLANs
  - Inter-Switch Link (ISL).
  - IEEE 802.1Q
  - LAN Emulation (LANE)
  - 802.10
- Una troncal es una conexión punto a punto entre dos Switches que permite transportar tráfico de diferentes VLANs.

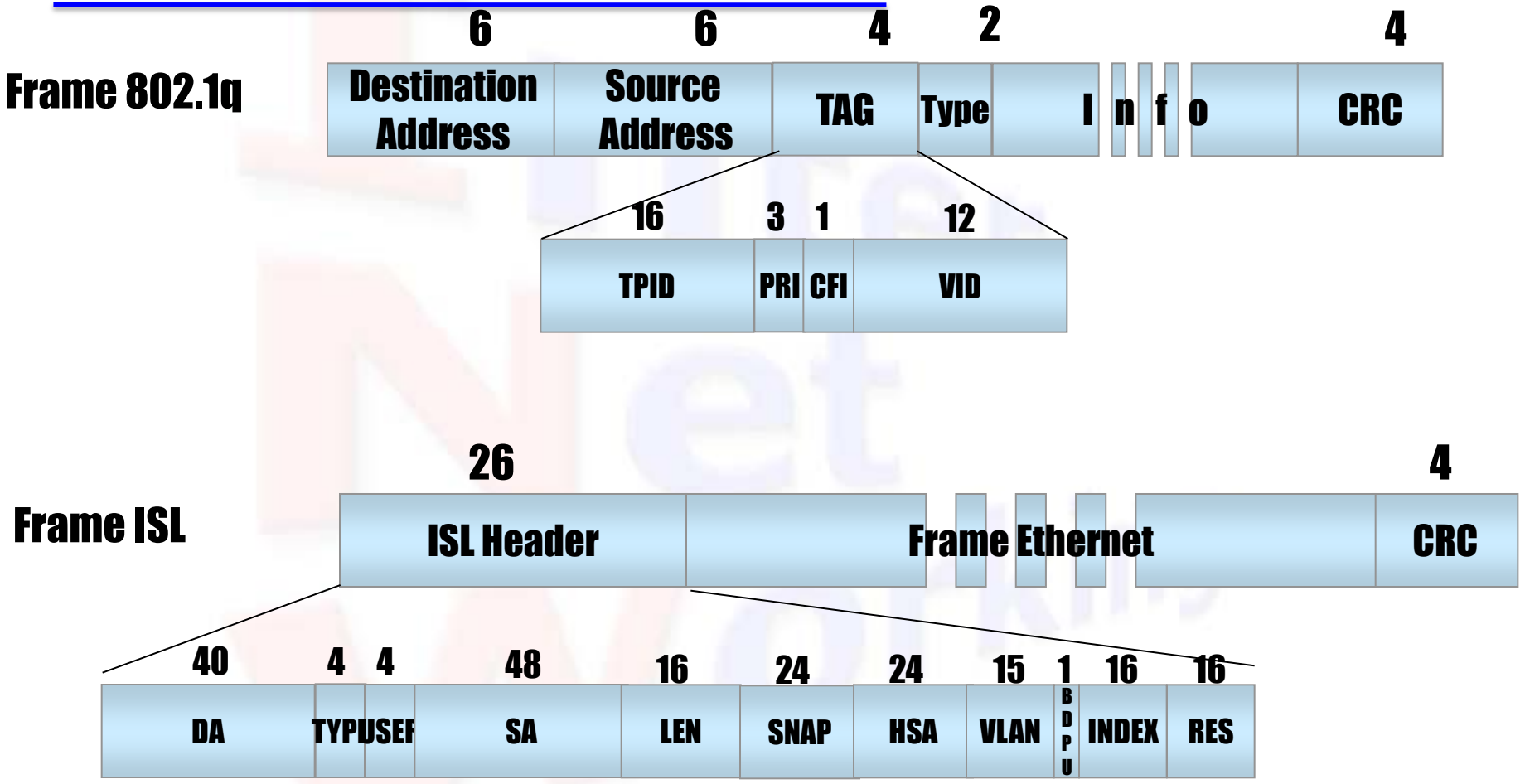
IEEE 802.1Q

- TPID: (Tag Protocol Identifier) 0x8100 indica 802.1q/802.1p
- TCI : Tag Control Information
  - 3 bits Prioridad del usuario.
  - 1 bit canonical format (CFI Indicator).
  - 12 bit VLAN ID (4096 VLANs).
- Al usar 802.1Q los frames Ethernet exceden los 1518 bytes originales, (1518 + 4 tag 802.1q = 1522 bytes).
- Standar adoptado por la industria.
- Medio Ethernet

ISL - Inter-Swicth Link Protocol

- Header ISL contiene 10 bits de VLAN ID. (1024 VLANs).
- Encapsulación
- Propietario de Cisco
- Medio Ethernet

Frame IEEE 802.1Q



802.10

- VLANs sobre Backbones FDDI.
- Propietario de Cisco.
- Transporta VLAN dentro de frames 802.10 FDDI.
- SAID Security Association Identifier

Dynamic Trunk Protocol (DTP)

- Protocolo que negocia automáticamente el tipo de troncal.
- Modos.
  - On
  - Off
  - Desirable
  - Auto
  - Nonegotiate
- DTP es un protocolo punto a punto.
- Durante la negociación de la troncal el puerto no participa en el STP.

Vlan Trunk Protocol - VTP

- Protocolo Propietario de Cisco.
- Maneja la consistencia de las VLANs a traves de la red de Swicthes.
- VTP Domain.
- Modos de Operación VTP.
  - Server: Capacidades de crear, modificar y borrar VLANs; configurar VTP domain, VTP version, VTP pruning y otros parametros. Es el modo por defecto.
  - Client: Recive la información desde los VTP Servers.
  - Transparent: No participa en VTP. Forward VTP advertisements, pero no sincroniza sus VLANs con los VTP advertisements de los otros switches.
- VTP Prunning.

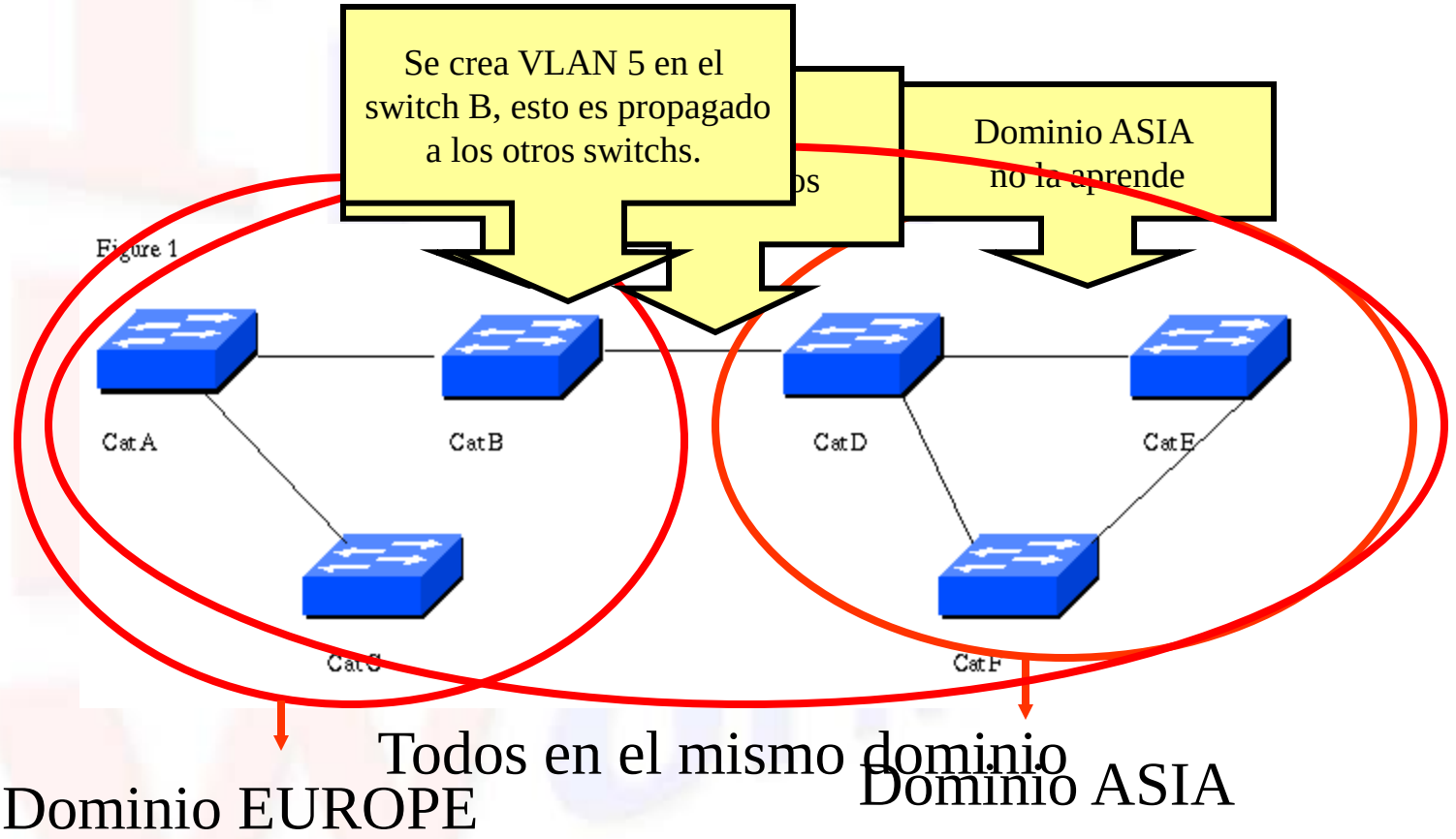
Modos de Operación

- Server.
  - Capacidades de crear, modificar y borrar VLANs.
  - Configurar VTP domain, VTP version, VTP pruning y otros parametros. Es el modo por defecto.
- Client
  - Recive la información desde los VTP Servers.
- Transparent
  - No participa en VTP.
  - Reenvia los VTP advertisements, pero no sincroniza sus VLANs con los VTP advertisements de los otros swicthes.

VTP: Operación

- VTP opera a través de mensajes (multicast) enviados a una MAC particular. Note que los avisos VTP sólo viajan por las puertas de trunk.
- Se asigna un dominio VTP, para ello se asigna un nombre de dominio a cada switch. La información VTP viaja sólo dentro de este dominio.
- Para ello deben cumplirse las siguientes condiciones:
  - El switch en un dominio debe estar asigando al dominio VTP
  - Los switches deben ser adyacentes.
  - Trunking debe estar habilitado entre todos los switches.

VTP: Operación



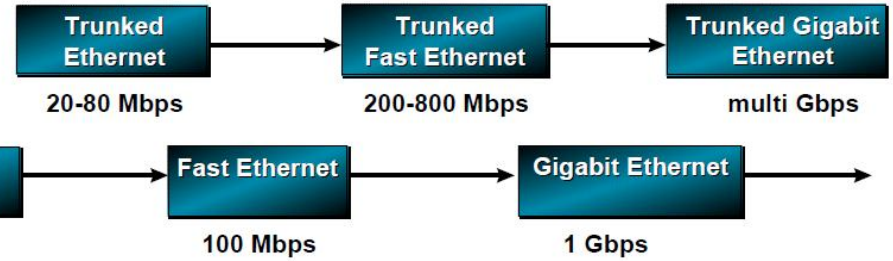
Si se limpia la VLAN 4 en el switch D, esto se refleja en el E y F, pero nunca se aprende en el switch A, B y C.

Fast EtherChannel FEC

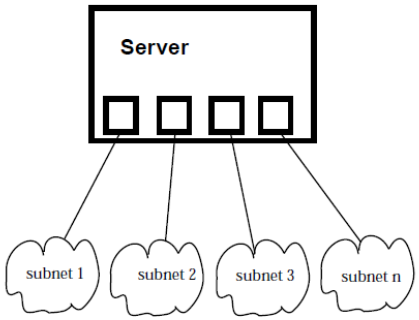
- Permite agrupar puertas Fastethernet.
- Link paralelos tratados como un único Link.
- Un STP.
- Redundancia.
- Compartir tráfico.
- PAgP (Port Aggregation Protocol).
- Ahorro de costos ya que no es necesario aumentar en 10x con altos precios

Link Aggegation Protocol

- Link aggregation está estandarizado bajo IEEE 802.1AX-2008

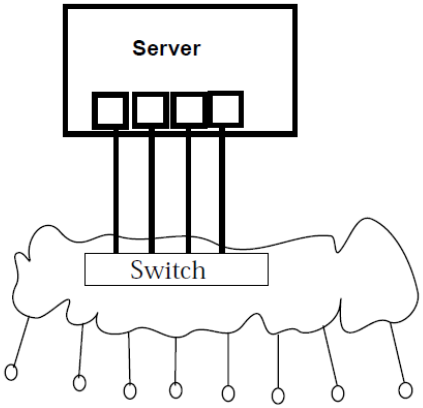


Before



Multiple Server identities

After



Single server identity:

One IP address
One MAC address