Redes y Seguridad Perimetral

Introducción a la seguridad - Sesión 1/4

Luis Dominguez
ldominguez@tamps.cinvestav.mx

Octubre 26 de 2012

Objetivos

Se dará una introducción a los conceptos básicos de redes y se sentarán las bases para el diseño de redes seguras.

Outline

Outline for section 1

Modelo OSI


Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Físico

Físico

- La capa física es la encargada de la transmisión de los bits sobre un canal de comunicación. Los detalles de diseño tienen que ver con asegurarse de cuando un lado envía un bit en 1, el otro reciba un bit en 1, y no en 0.
- Dependiendo del medio de comunicación, sea hace necesario que se definan cuántos voltios son un bit en 1 y cuántos en 0, o si son impulsos luminosos, u ondas de radio frecuencia, hay que definir los niveles, además de el tiempo de duración de un bit.
- Si la transmisión puede ser simultáneamente en ambos sentidos; cómo se inicia la transmisión y cuándo ya no se están transmitiendo bits; si el conector usa pines, cuántos son y para qué se utilizan

Enlace

- La Capa de enlace brinda brinda conexión nodo a nodo dentro de un dominio único de red.

- Transforma el nivel fisico en un medio confiable, proporcionando un servicio a la capa de red al enlazar de nodo a nodo fraccionando, verificando, y corrigiendo o solicitando retransmisión de los datos y administrando la transmisión de datos.

Red

- Es responsable de dirigir los paquetes por el camino correcto y óptimo al destino. Puede pasar a través de muchas redes, por lo que es necesario que se agregue información de encaminamiento.

Transporte

- Se asegura de la entrega extremo a extremo de todo el mensaje. Lleva un control de cómo fueron entregados (orden, cantidad y tiempo) por lo que además presenta un esquema de control de calidad del servicio de comunicación como un todo.

Sesión

- Supervisa la interacción entre los extremos, de tal forma que únicamente se transporten los mensajes correspondientes al conjunto de actividades actual, en términos de validez de destino, tiempo, contenido y pertenencia.

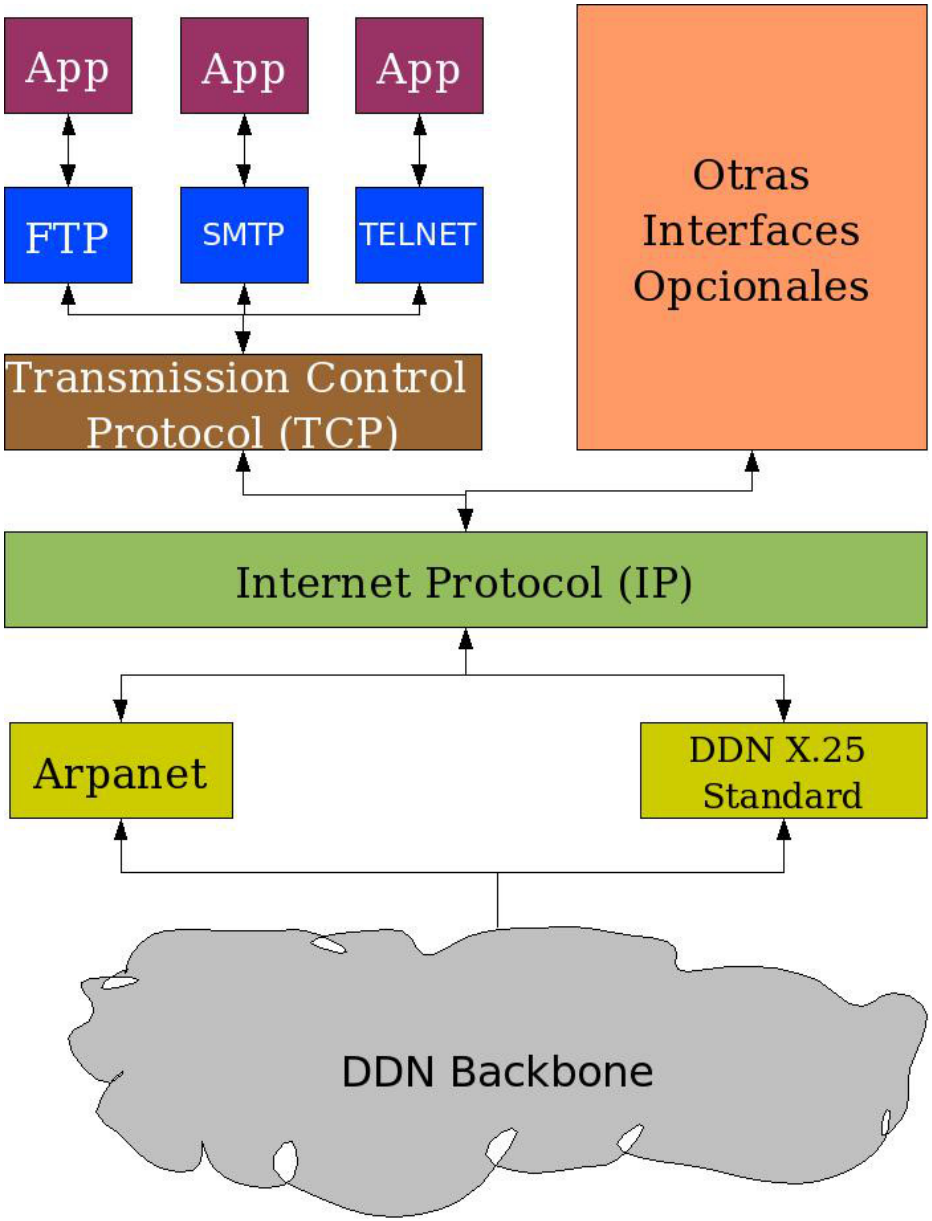
Presentación

- Traduce el mensaje a la semántica y lenguaje (sintaxis) correspondientes para los extremos. Como traducir a un juego de caracteres adecuado, cifrar y comprimir la información.

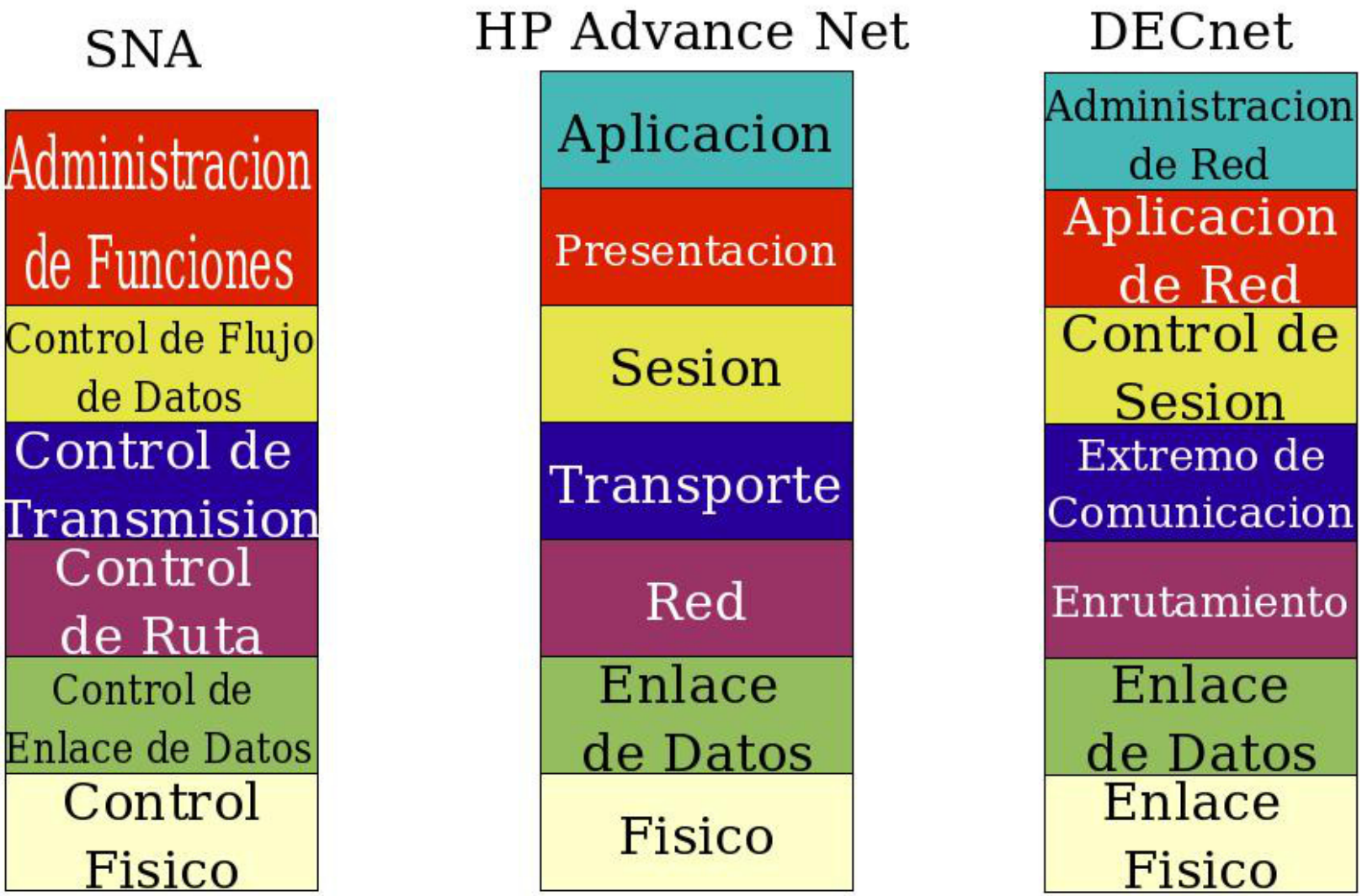
Aplicación

- Es la capa por la cual el usuario, humano o no, se comunica con el otro extremo, es decir, está formada por programas, tales como protocolos de internet, o programas de segundo plano.

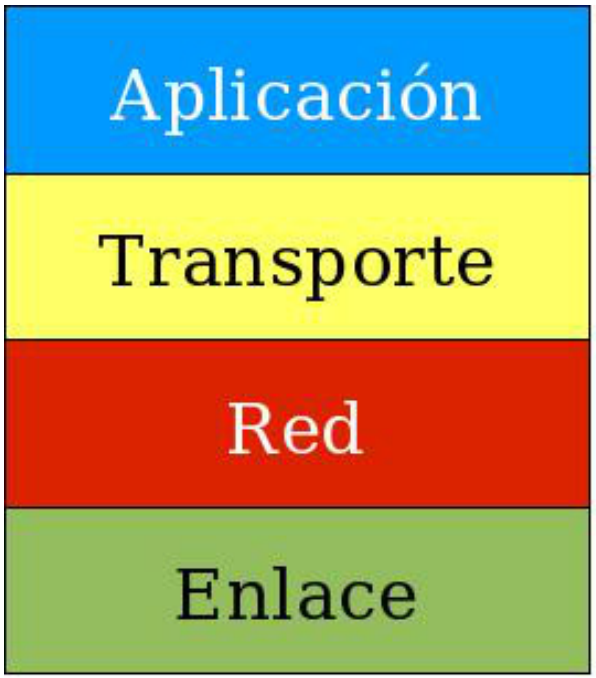
Modelo del Departamento de Defensa de los EEUU



Otros modelos



Modelo TCP/IP



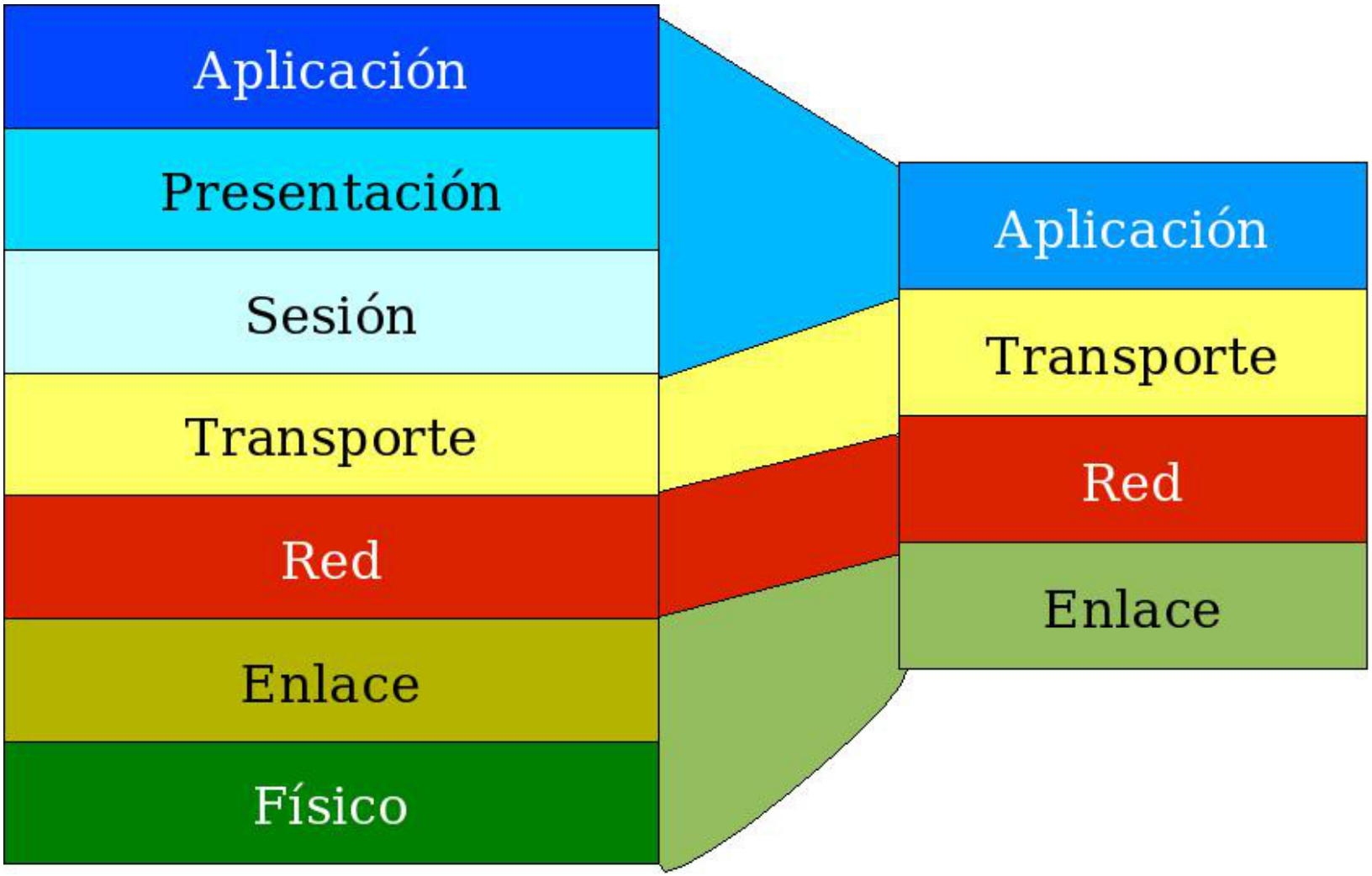
Web, email, chat

TCP, UDP

IP, ICMP, IGMP

Controladores y NIC

Modelo OSI vs TCP/IP



Organizaciones

Crean estándares de carácter general

- International Standards Organization (ISO)
- American National Standard Institute (ANSI)
- British Standard Institute (BSI)
- Association Française de Normatisation (AFNOR)
- Deutsches Intitut für Normung (DIN)

Organizaciones

Crean estándares especializados

- Telecomunications Industries Association (TIA)
- Electronic Industries Association (EIA)
- Institute of Electrical and Electronic Engineers (IEEE)
- International Telecommunication Union (ITU, antes CCITT)
- Internet Engineering Task Force (IETF)

Outline for section 2

Direcciones MAC

Consta de 6 bytes:

- 3 del proveedor, 3 del número de serie consecutivo, se expresa en hexadecimal

Ejemplos:

- 00:01:02:64:f8:90 corresponde a 3Com Corporation 3c905B
- d0:67:e5:f3:f5:7f corresponde a Broadcom Corporation NetXtreme BCM5722 (Dell)
- d4:9a:20:5c:ce:10 corresponde a Apple AirPort Extreme (0x168C, 0x8F) (Atheros)

http://www.base64online.com/mac_address.php

- A través del icono de conexión de red
- Comando ipconfig, ifconfig, o ip desde la consola

```
Last login: Fri Oct 12 16:13:47 on ttys000
ldominguez:~ ldominguez$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:23:df:fd:99:98
        inet6 fe80::223:dfff:fefd:9998%en0 prefixlen 64 scopeid 0x4
        inet 148.247.201.98 netmask 0xffffff00 broadcast 148.247.201.255
        media: autoselect (1000baseT <full-duplex,flow-control>)
        status: active
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr d4:9a:20:ff:fe:cb:17:cc
        media: autoselect <full-duplex>
        status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:1c:c0:12:c8:20
        media: autoselect (<unknown type>)
        status: inactive
en2: flags=8822<BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
        ether 64:b9:e8:e0:22:4d
        media: autoselect
        status: inactive
ldominguez:~ ldominguez$
```

Dirección IP

- Compuesta por 32 bits separadas de 4 octetos numéricos del 0 al 255.
- Separados por puntos decimales: 1.2.3.4
- Ejemplos:
  - 192.168.1.10
  - 128.0.1.30
  - 148.235.3.97
  - 200.78.231.34

- A través del icono de conexión de red
- Comando ipconfig, ifconfig, o ip desde la consola

```
Last login: Fri Oct 12 16:13:47 on ttys000
ldominguez:~ ldominguez$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:23:df:fd:99:98
        inet6 fe80::223:dfff:fefd:9998%en0 prefixlen 64 scopeid 0x4
        inet 148.247.201.98 netmask 0xffffff00 broadcast 148.247.201.255
        media: autoselect (1000baseT <full-duplex,flow-control>)
        status: active
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr d4:9a:20:ff:fe:cb:17:cc
        media: autoselect <full-duplex>
        status: inactive
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:1c:c0:12:c8:20
        media: autoselect (<unknown type>)
        status: inactive
en2: flags=8822<BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
        ether 64:b9:e8:e0:22:4d
        media: autoselect
        status: inactive
ldominguez:~ ldominguez$
```

Buscando al dueño de la IP

LACNIC, ARIN, y otros brindan el servicio de WHOIS.

REGISTRATION SERVICES

SEARCH

```
% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2012-10-15 15:28:03 (BRT -03:00)

inetnum:     148.247/16
status:      assigned
aut-num:     N/A
owner:       Centro de Investigacion y de Estudios Avanzados de
ownerid:     MX-CIYE6-LACNIC
responsible: Manuel Mendez Nonell
address:     Edificio de Computacion AV. Instituto Politecnico Nacion
```

Clases

- Las redes IP se clasifican en 5 grandes clases: A, B, C, D y E:

Clase	Rango		
A	0.0.0.0	–	127.255.255.255
B	128.0.0.0	–	191.255.255.255
C	192.0.0.0	–	223.255.255.255
D	224.0.0.0	–	239.255.255.255
E	240.0.0.0	–	255.255.255.255

Clases de uso interno

- Existe una clase de uso interno a los dispositivos de comunicación:
  - 127.0.0.0 – 127.255.255.255
    RFC: 1700

- Existen 3 clases de uso reservado para las organizaciones:
  - 172.16.1.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255
  - 10.0.0.0 – 10.255.255.255
    RFC: 1918

Clases de uso especial

Rango			Descripción
0.0.0.0	–	0.255.255.255	Dirección cero
169.254.0.0	–	169.254.255.255	Configuración cero
192.0.2.0	–	192.0.2.255	Documentación y ejemplos
192.88.99.0	–	192.88.99.255	IPv6 a IPv4 relay y anycast
192.18.0.0	–	192.19.255.255	Network Device Benchmark

- RFC 1700
- RFC 2544
- RFC 3068
- RFC 3330

Capacidad de las direcciones

- 32 bits de direccionamiento, sirven para especificar hasta 4294967296 equipos.
- Sin embargo:
  - La primera dirección de una clase (ej. 192.168.1.0) sirve de identificador de red. No se puede asignar a un dispositivo.
  - La última dirección de una clase (ej. 192.168.1.255) sirve para llamar a toda la red. No se puede asignar a un dispositivo.

Máscara de subred

- Operación Lógica AND con la dirección IP para diferenciar la subred:
  - IP: 192.168.1.15
  - Máscara: 255.255.255.0
  - IP: 11000000.10101000.00000001.00001111
  - Máscara: 11111111.11111111.11111111.00000000
  - Resultado: 11000000.10101000.00000001.00000000

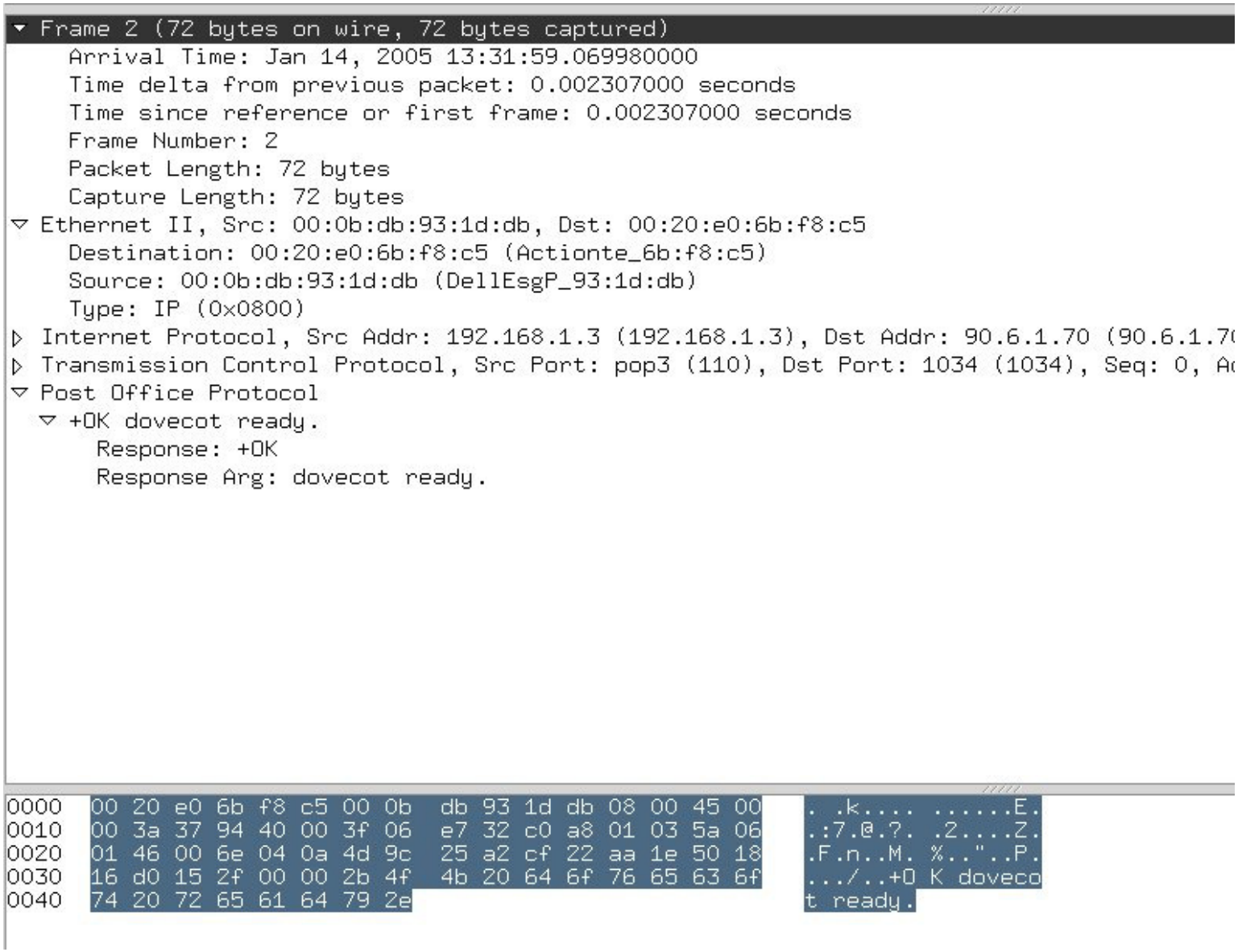
Subredes

Addr	Bits	Prefijo	Notación	Máscara	Hexadecimal
1	0	/32		255.255.255.255	ffffffff
2	1	/31		255.255.255.254	fffffffe
4	2	/30		255.255.255.252	fffffffc
8	3	/29		255.255.255.248	fffffff8
16	4	/28		255.255.255.240	fffffff0
32	5	/27		255.255.255.224	ffffffe0
64	6	/26		255.255.255.192	ffffffc0
128	7	/25		255.255.255.128	ffffff80
256	8	/24	1 C	255.255.255.0	ffffff00
512	9	/23	2 C	255.255.254.0	fffffe00
1 K	10	/22	4 C	255.255.252.0	fffffc00
2 K	11	/21	8 C	255.255.248.0	fffff800
4 K	12	/20	16 C	255.255.240.0	fffff000
8 K	13	/19	32 C	255.255.224.0	ffffe000
16 K	14	/18	64 C	255.255.192.0	ffffc000
32 K	15	/17	128 C	255.255.128.0	ffff8000

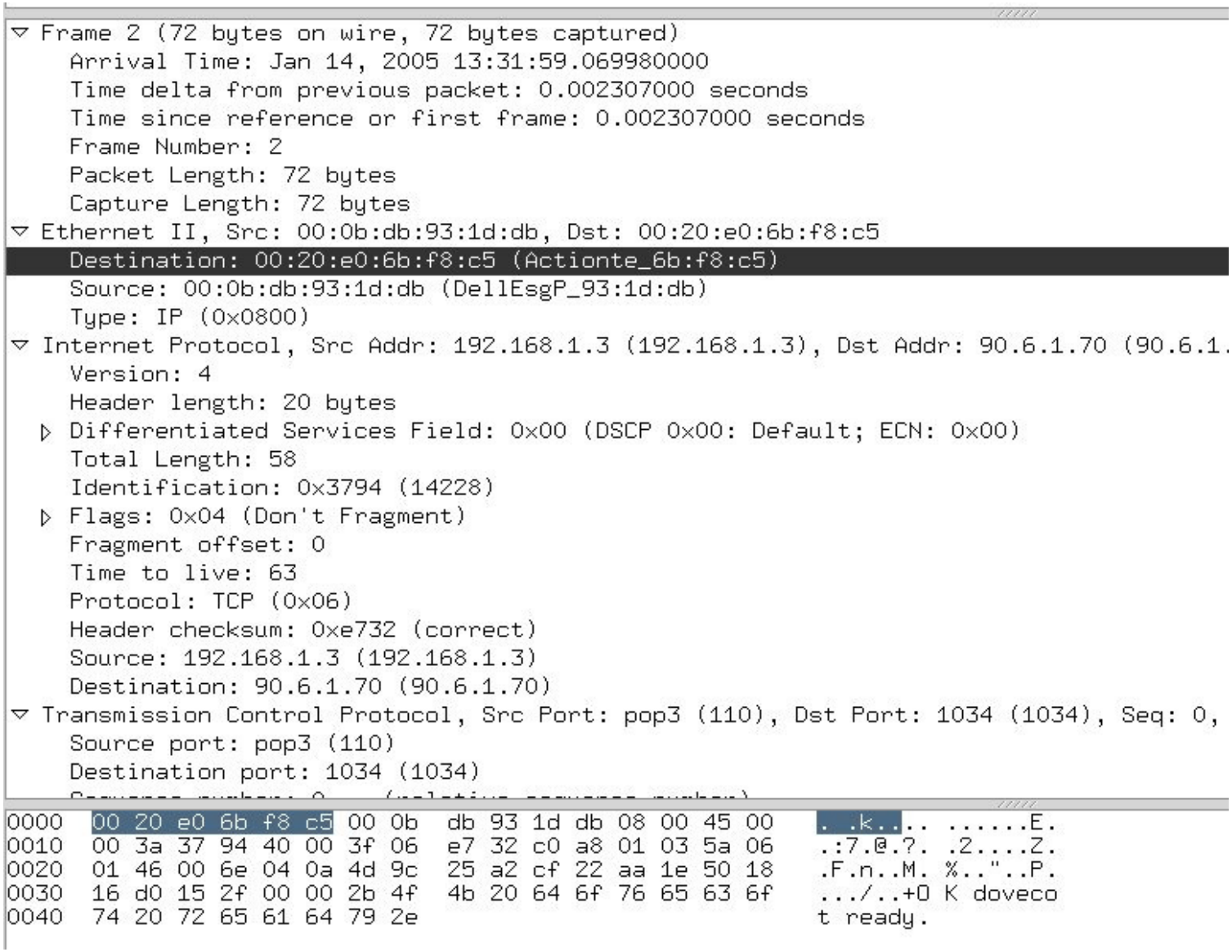
Subredes

Addr	Bits	Prefijo	Notación	Máscara	Hexadecimal
64 K	16	/16	1 B	255.255.0.0	ffff0000
128 K	17	/15	2 B	255.254.0.0	fffe0000
256 K	18	/14	4 B	255.252.0.0	fffc0000
512 K	19	/13	8 B	255.248.0.0	fff80000
1 M	20	/12	16 B	255.240.0.0	fff00000
2 M	21	/11	32 B	255.224.0.0	ffe0000
4 M	22	/10	64 B	255.192.0.0	ffc00000
8 M	23	/9	128 B	255.128.0.0	ff800000
16 M	24	/8	1 A	255.0.0.0	ff000000
32 M	25	/7	2 A	254.0.0.0	fe000000
64 M	26	/6	4 A	252.0.0.0	fc000000
128 M	27	/5	8 A	248.0.0.0	f8000000
256 M	28	/4	16 A	240.0.0.0	f0000000
512 M	29	/3	32 A	224.0.0.0	e0000000
1024 M	30	/2	64 A	192.0.0.0	c0000000

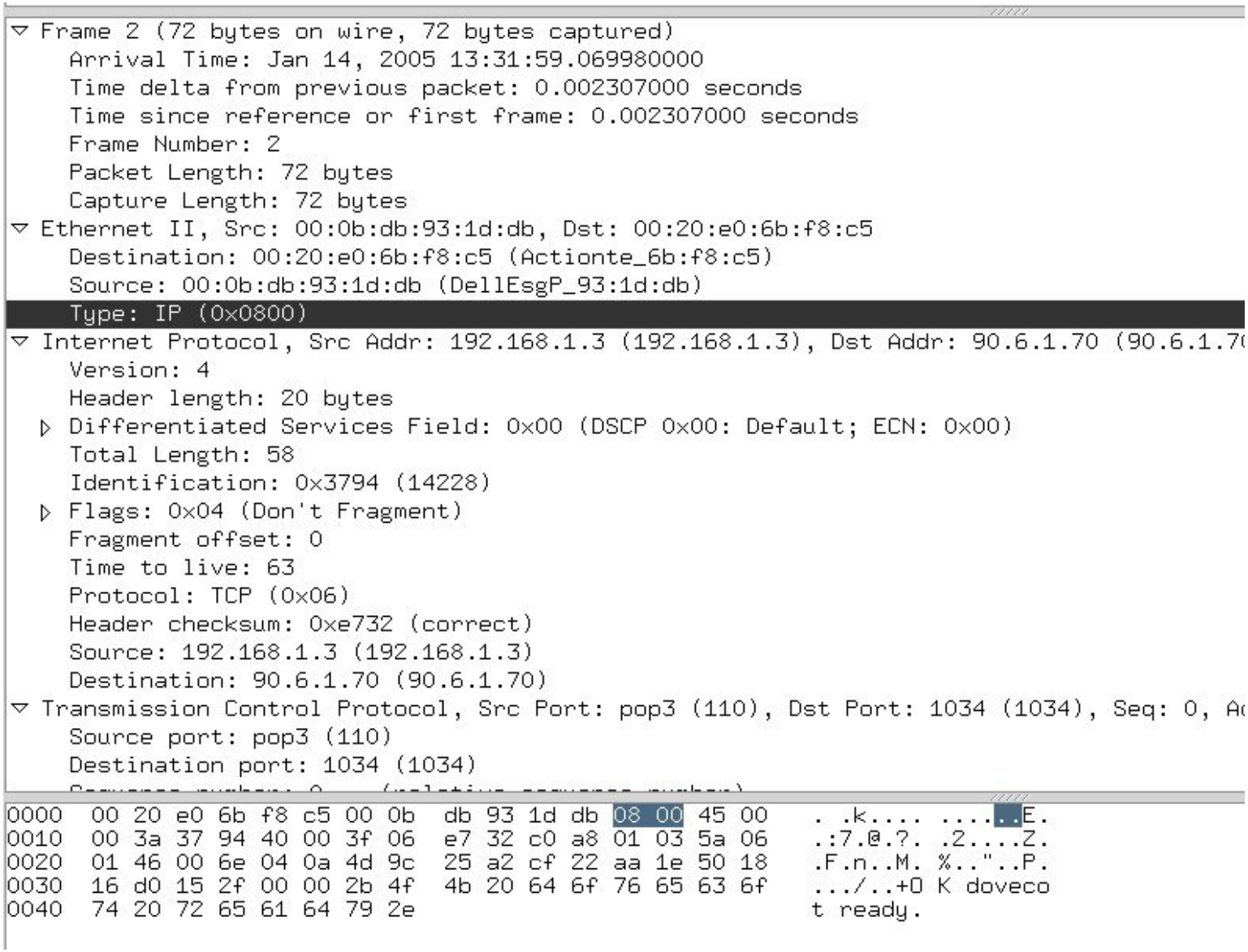
Bit stream


Frame 2 (72 bytes on wire, 72 bytes captured)
Arrival Time: Jan 14, 2005 13:31:59.069980000
Time delta from previous packet: 0.002307000 seconds
Time since reference or first frame: 0.002307000 seconds
Frame Number: 2
Packet Length: 72 bytes
Capture Length: 72 bytes
Ethernet II, Src: 00:0b:db:93:1d:db, Dst: 00:20:e0:6b:f8:c5
Destination: 00:20:e0:6b:f8:c5 (Actionte_6b:f8:c5)
Source: 00:0b:db:93:1d:db (DellEsgP_93:1d:db)
Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.1.3 (192.168.1.3), Dst Addr: 90.6.1.70 (90.6.1.7
Transmission Control Protocol, Src Port: pop3 (110), Dst Port: 1034 (1034), Seq: 0, A
Post Office Protocol
+OK dovecot ready.
Response: +OK
Response Arg: dovecot ready.
0000 00 20 e0 6b f8 c5 00 0b db 93 1d db 08 00 45 00 . .k.... ......E.
0010 00 3a 37 94 40 00 3f 06 e7 32 c0 a8 01 03 5a 06 .:7.@.?. .2....Z.
0020 01 46 00 6e 04 0a 4d 9c 25 a2 cf 22 aa 1e 50 18 .F.n..M. %.."..P.
0030 16 d0 15 2f 00 00 2b 4f 4b 20 64 6f 76 65 63 6f .../..+O K doveco
0040 74 20 72 65 61 64 79 2e t ready.

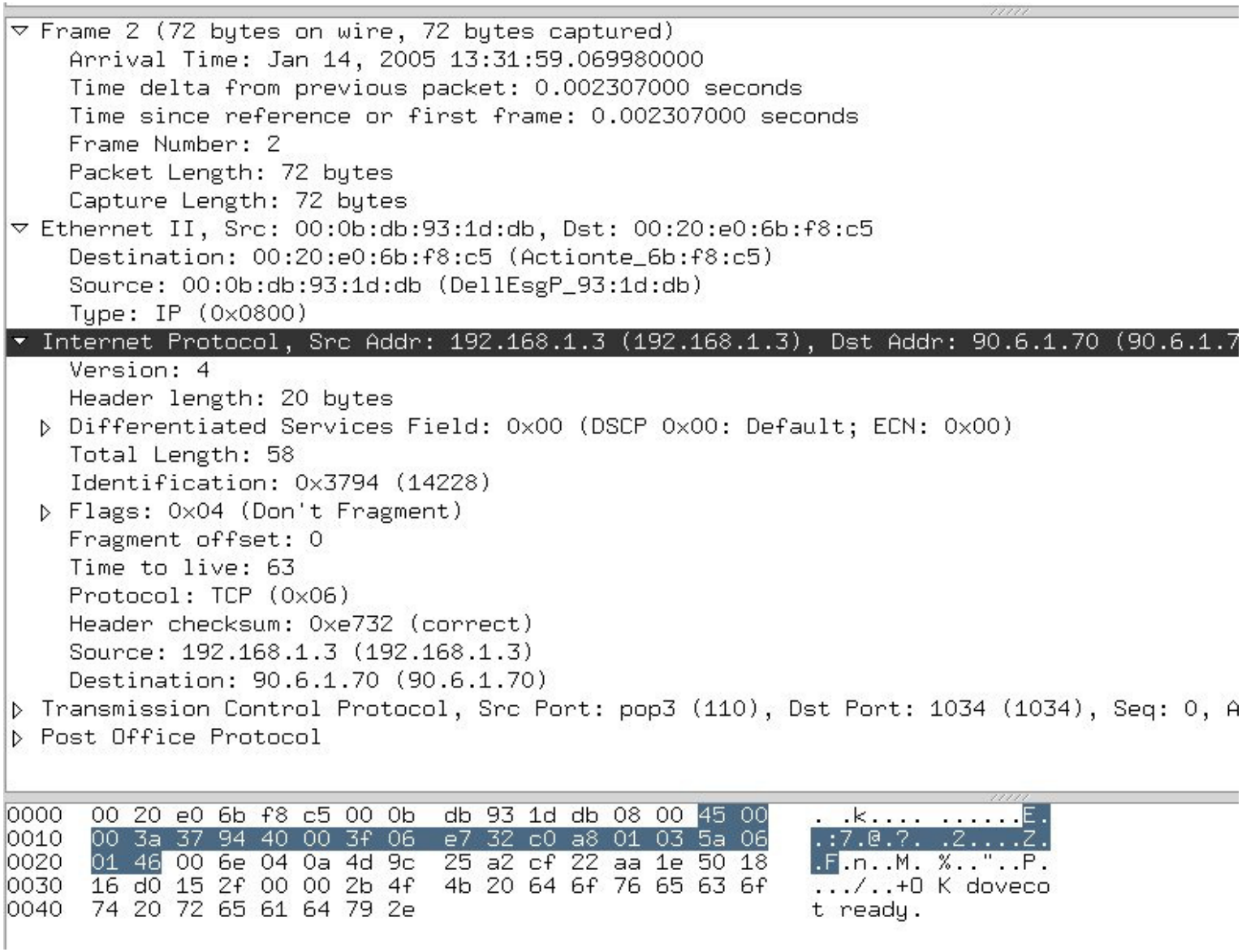
Frame


Frame 2 (72 bytes on wire, 72 bytes captured)
Arrival Time: Jan 14, 2005 13:31:59.069980000
Time delta from previous packet: 0.002307000 seconds
Time since reference or first frame: 0.002307000 seconds
Frame Number: 2
Packet Length: 72 bytes
Capture Length: 72 bytes
Ethernet II, Src: 00:0b:db:93:1d:db, Dst: 00:20:e0:6b:f8:c5
Destination: 00:20:e0:6b:f8:c5 (Actionte_6b:f8:c5)
Source: 00:0b:db:93:1d:db (DellEsgP_93:1d:db)
Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.1.3 (192.168.1.3), Dst Addr: 90.6.1.70 (90.6.1.
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 58
Identification: 0x3794 (14228)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 63
Protocol: TCP (0x06)
Header checksum: 0xe732 (correct)
Source: 192.168.1.3 (192.168.1.3)
Destination: 90.6.1.70 (90.6.1.70)
Transmission Control Protocol, Src Port: pop3 (110), Dst Port: 1034 (1034), Seq: 0,
Source port: pop3 (110)
Destination port: 1034 (1034)
0000 00 20 e0 6b f8 c5 00 0b db 93 1d db 08 00 45 00 . .k.. ....E.
0010 00 3a 37 94 40 00 3f 06 e7 32 c0 a8 01 03 5a 06 .:7.@.?. .2....Z.
0020 01 46 00 6e 04 0a 4d 9c 25 a2 cf 22 aa 1e 50 18 .F.n..M. %.."..P.
0030 16 d0 15 2f 00 00 2b 4f 4b 20 64 6f 76 65 63 6f .../..+O K doveco
0040 74 20 72 65 61 64 79 2e t ready.

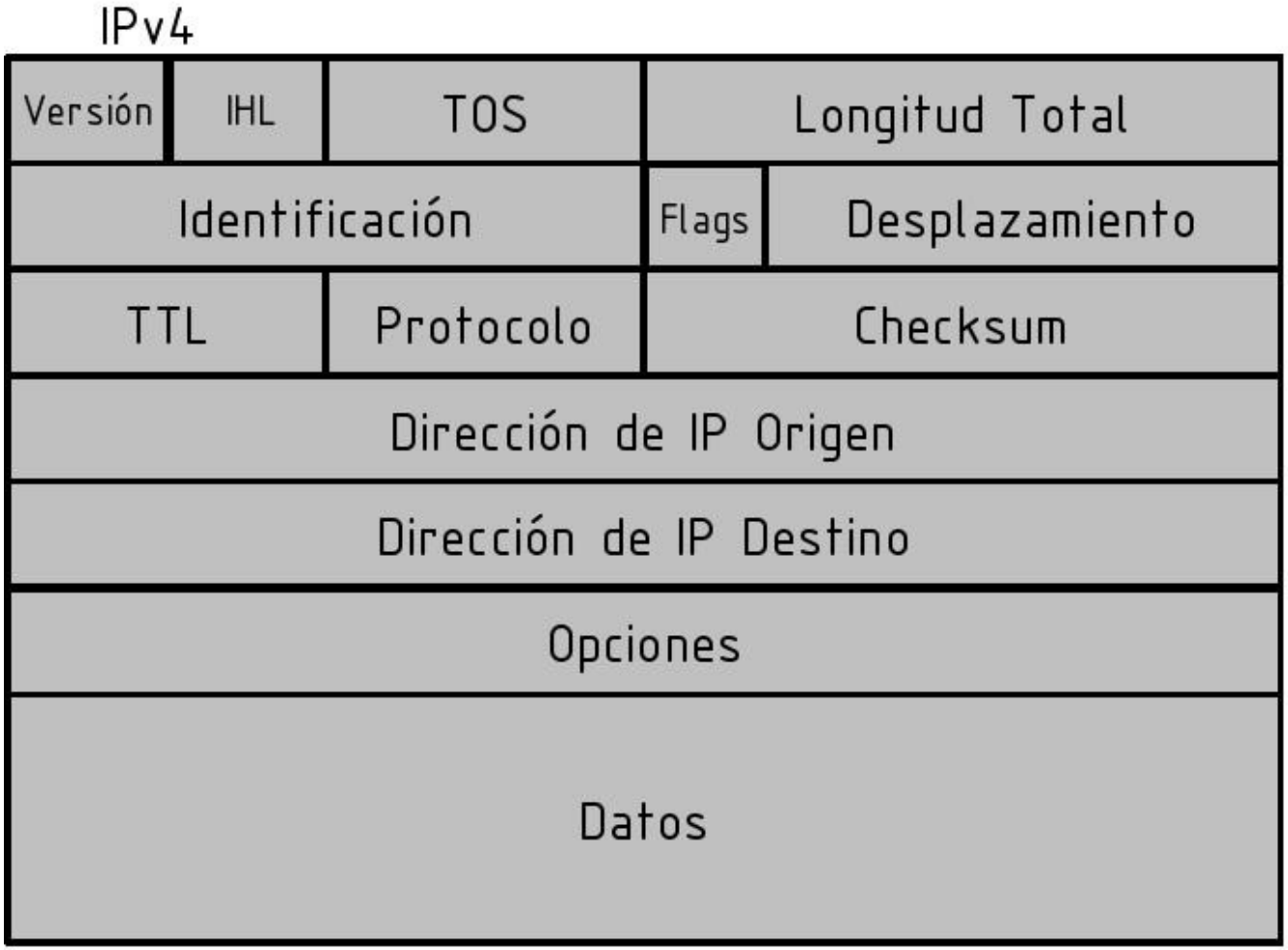
Segmento


Frame 2 (72 bytes on wire, 72 bytes captured)
Arrival Time: Jan 14, 2005 13:31:59.069980000
Time delta from previous packet: 0.002307000 seconds
Time since reference or first frame: 0.002307000 seconds
Frame Number: 2
Packet Length: 72 bytes
Capture Length: 72 bytes
Ethernet II, Src: 00:0b:db:93:1d:db, Dst: 00:20:e0:6b:f8:c5
Destination: 00:20:e0:6b:f8:c5 (Actionte_6b:f8:c5)
Source: 00:0b:db:93:1d:db (DellEsgP_93:1d:db)
Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.1.3 (192.168.1.3), Dst Addr: 90.6.1.70 (90.6.1.7
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 58
Identification: 0x3794 (14228)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 63
Protocol: TCP (0x06)
Header checksum: 0xe732 (correct)
Source: 192.168.1.3 (192.168.1.3)
Destination: 90.6.1.70 (90.6.1.70)
Transmission Control Protocol, Src Port: pop3 (110), Dst Port: 1034 (1034), Seq: 0, A
Source port: pop3 (110)
Destination port: 1034 (1034)
0000 00 20 e0 6b f8 c5 00 0b db 93 1d db 08 00 45 00 . .k.... ......E.
0010 00 3a 37 94 40 00 3f 06 e7 32 c0 a8 01 03 5a 06 .:7.@.?. .2....Z.
0020 01 46 00 6e 04 0a 4d 9c 25 a2 cf 22 aa 1e 50 18 .F.n..M. %.."..P.
0030 16 d0 15 2f 00 00 2b 4f 4b 20 64 6f 76 65 63 6f .../..+O K doveco
0040 74 20 72 65 61 64 79 2e t ready.

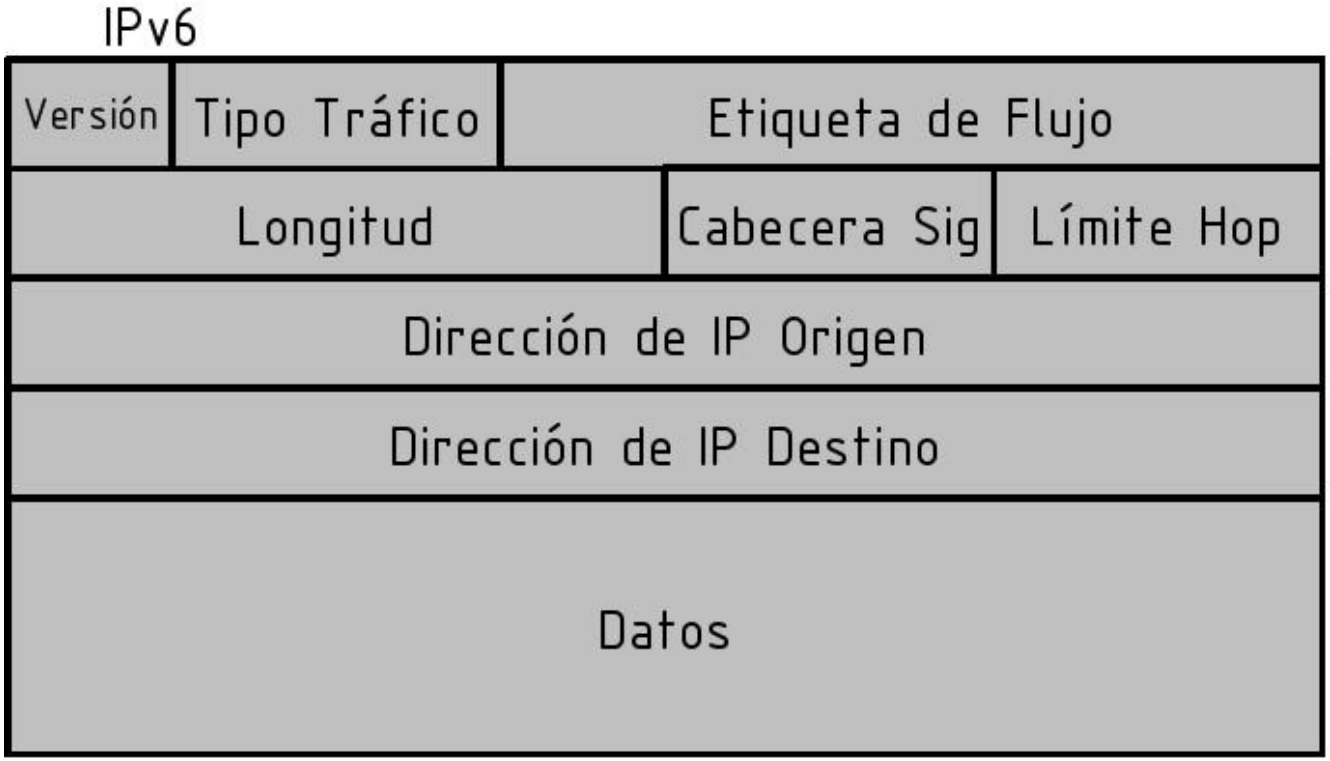
Dirección de IP



Paquete IPv4



Dirección de IPv6



Formato de una dirección de IPv6

Formato IPv6:

- Son de 128 bits de largo
- se escriben en hexadecimal
- se forman ocho grupos de 16 bits
- el separador es el ":"
- los ceros consecutivos se omiten 1 sola ocasión

Ejemplos:

- 3ffe:1900:4545:3:200:f8ff:fe21:67cf
- fe80:0:0:0:200:f8ff:fe21:67cf → fe80::200:f8ff:fe21:67cf

Migración a IPv6

- Escasez de direcciones de IPv4

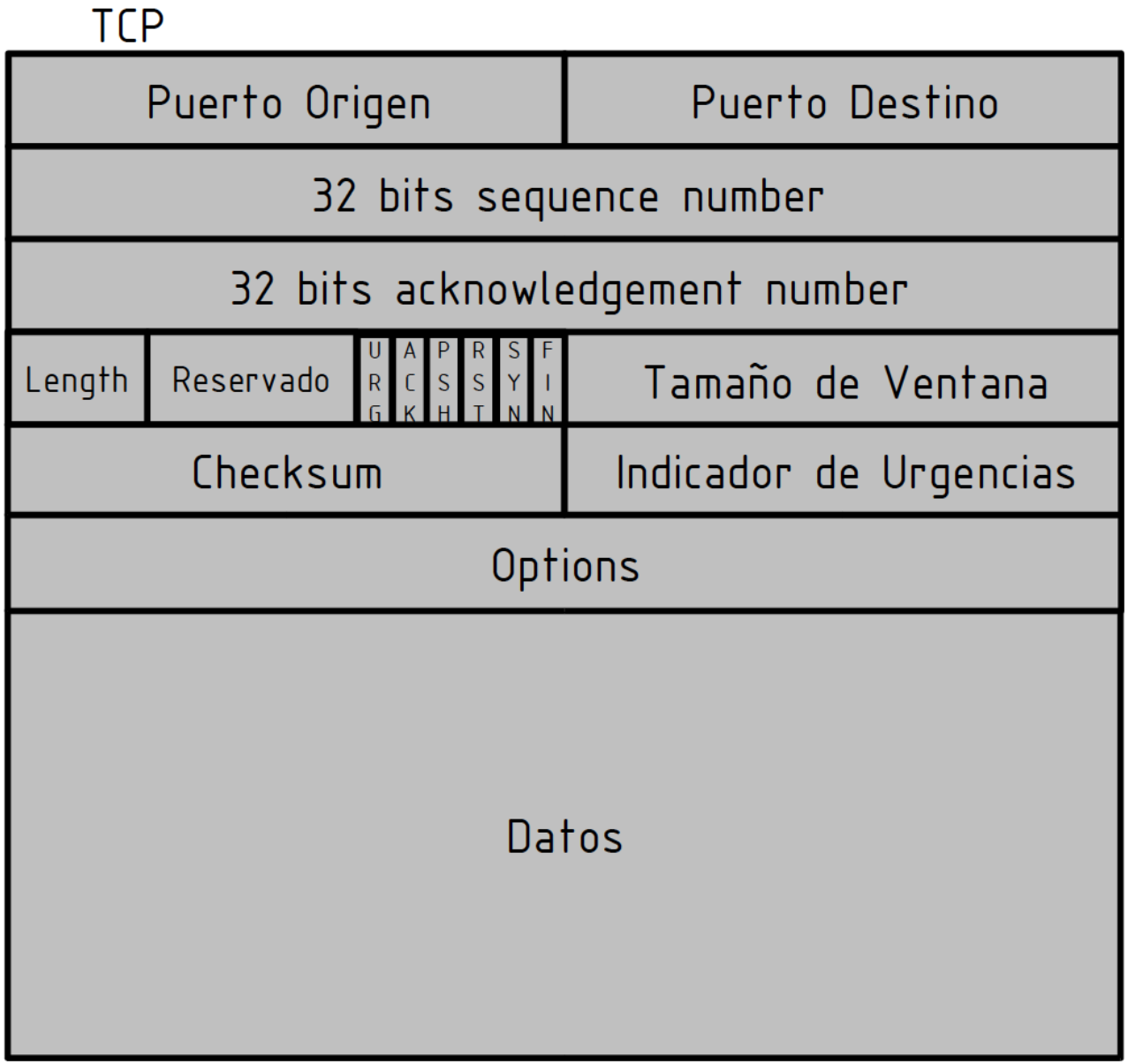
Outline for section 3

Capa de transporte

La capa de transporte tiene los siguientes objetivos

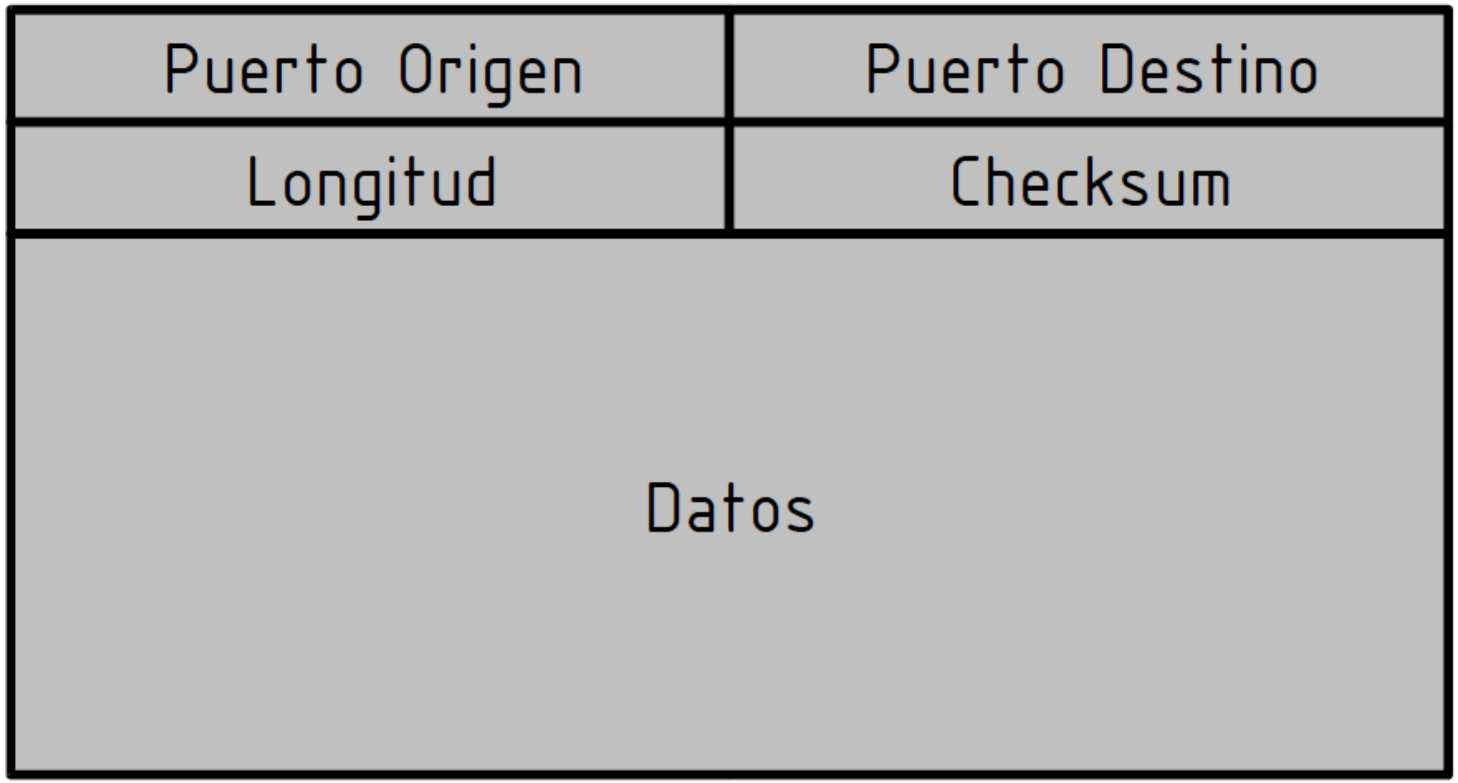
- Asegurarse que los segmentos de datos enviados sean reconocidos por el receptor
- Proveer la retransmisión de todos los segmentos de datos que no sean reconocidos
- Ordenar los segmentos de datos recibidos
- Proveer control y evasión de congestión de red

Paquete TCP

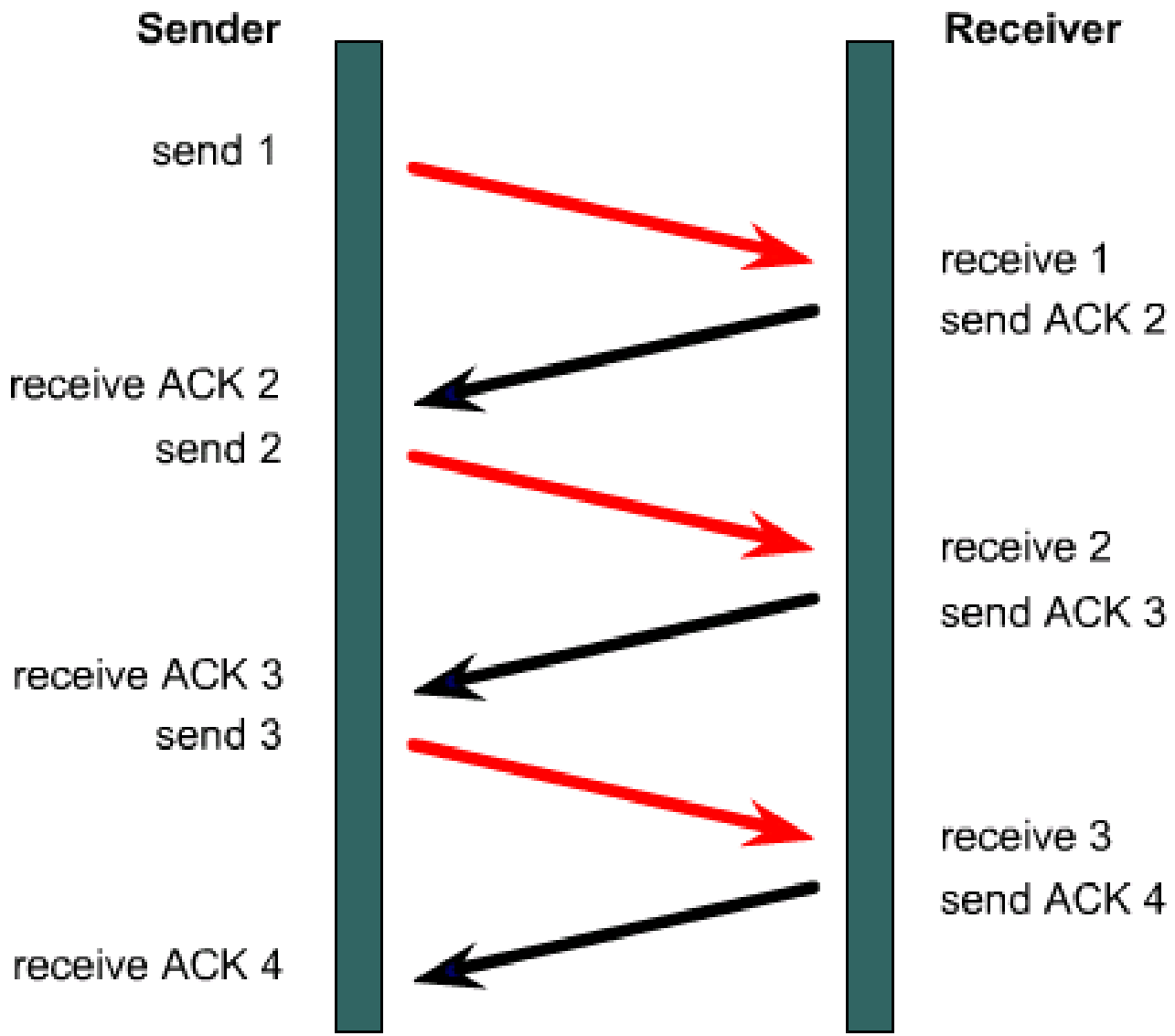

TCP
Puerto Origen
Puerto Destino
32 bits sequence number
32 bits acknowledgement number
Length
Reservado
URG
ACK
PSH
RST
SYN
FIN
Tamaño de Ventana
Checksum
Indicador de Urgencias
Options
Datos

Paquete UDP

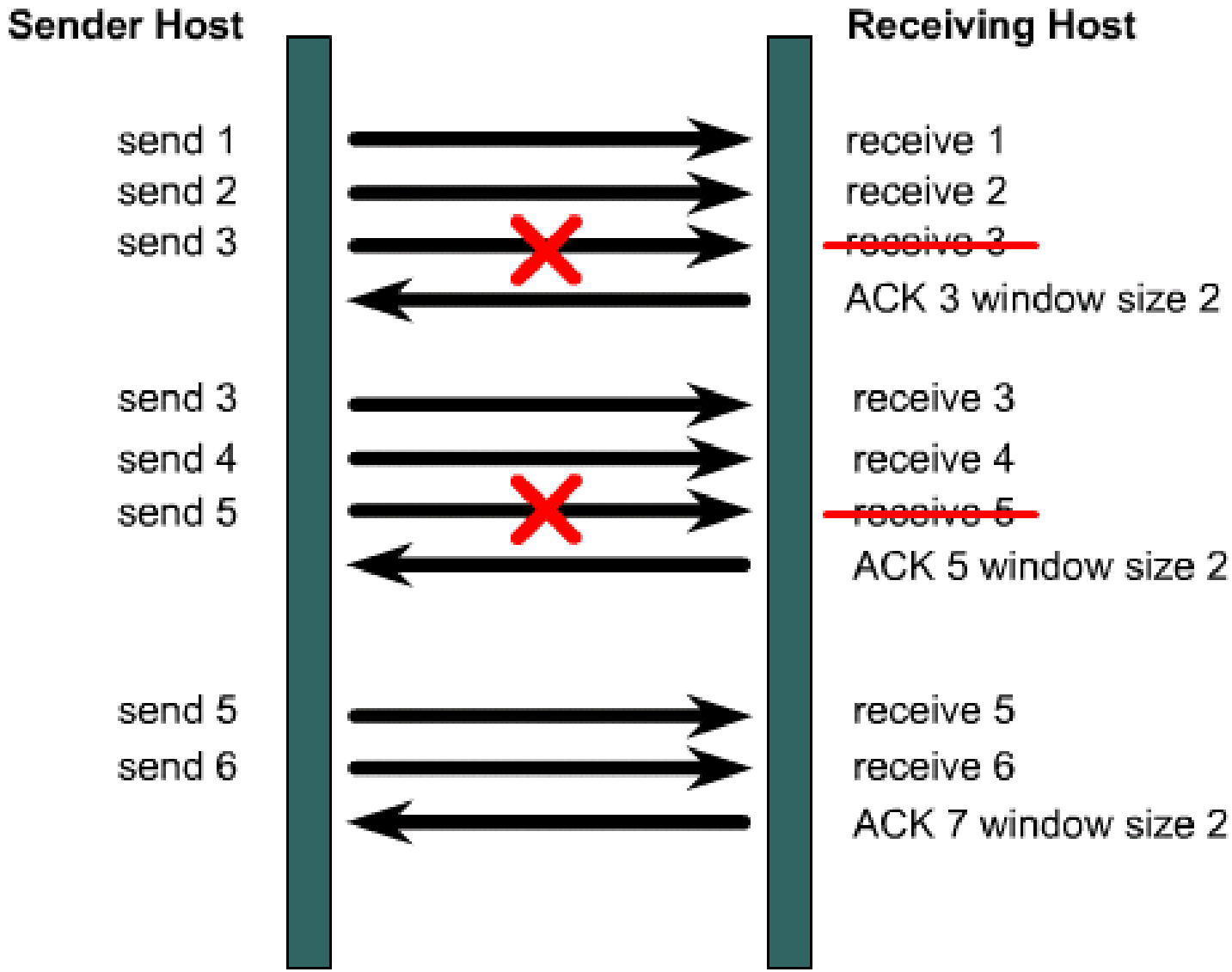
UDP



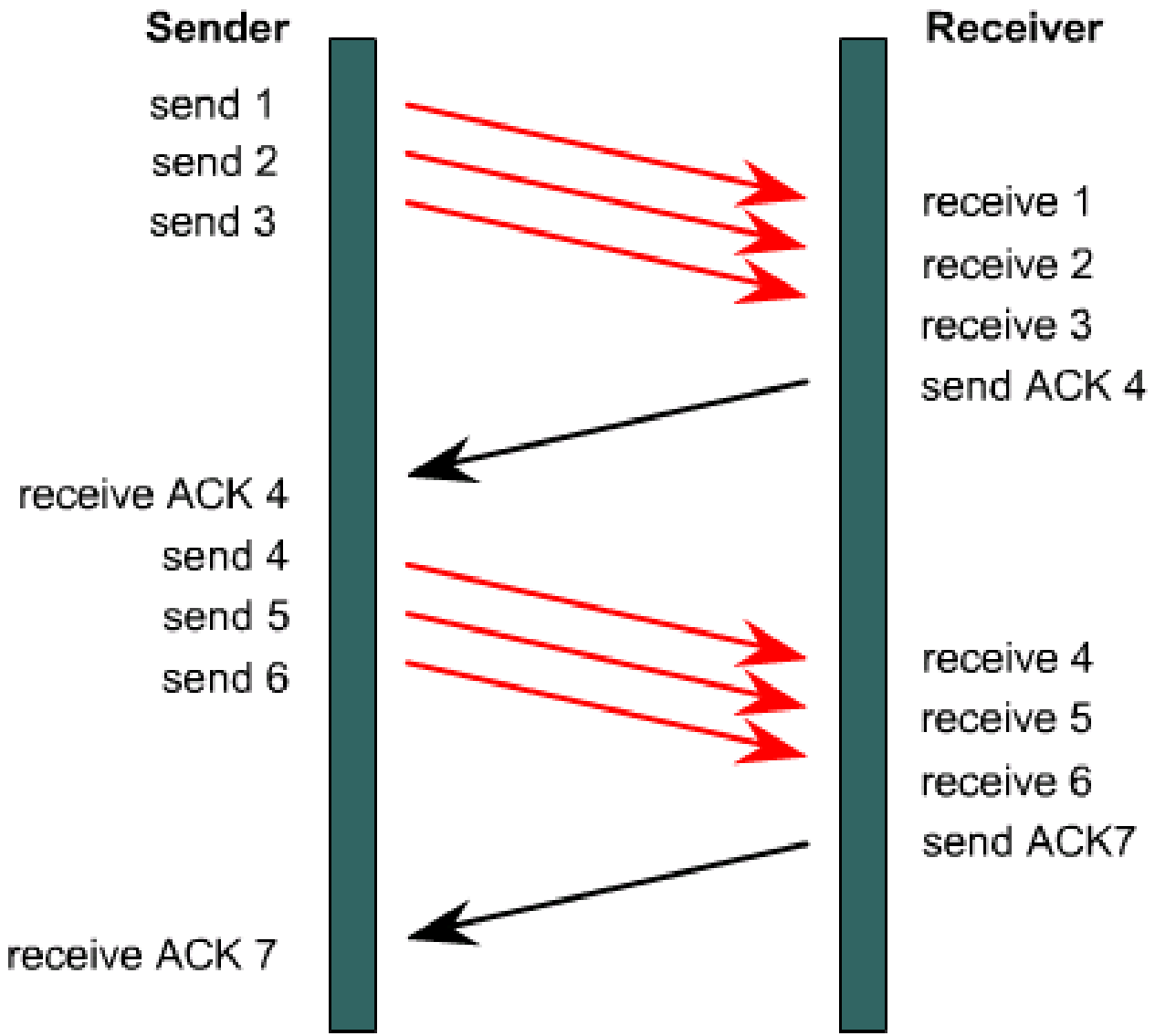
Inicialización TCP



Ventanas deslizantes 1/2

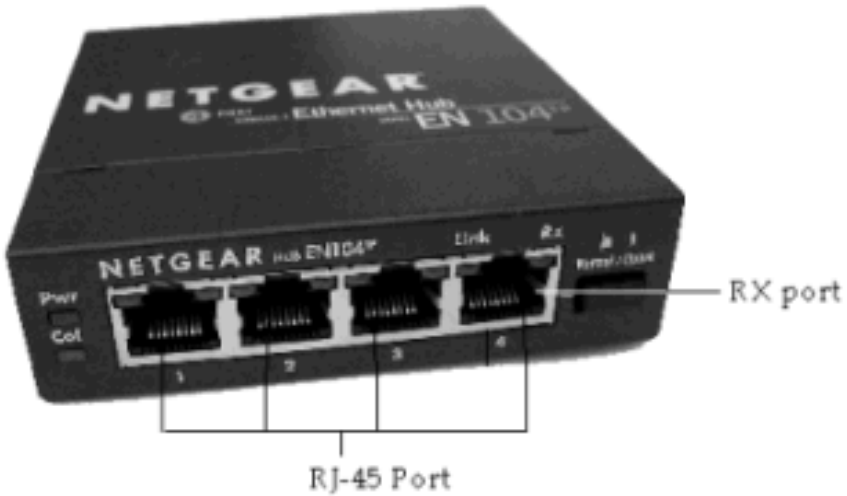


Ventanas deslizantes 2/2



Outline for section 4

Concentrador

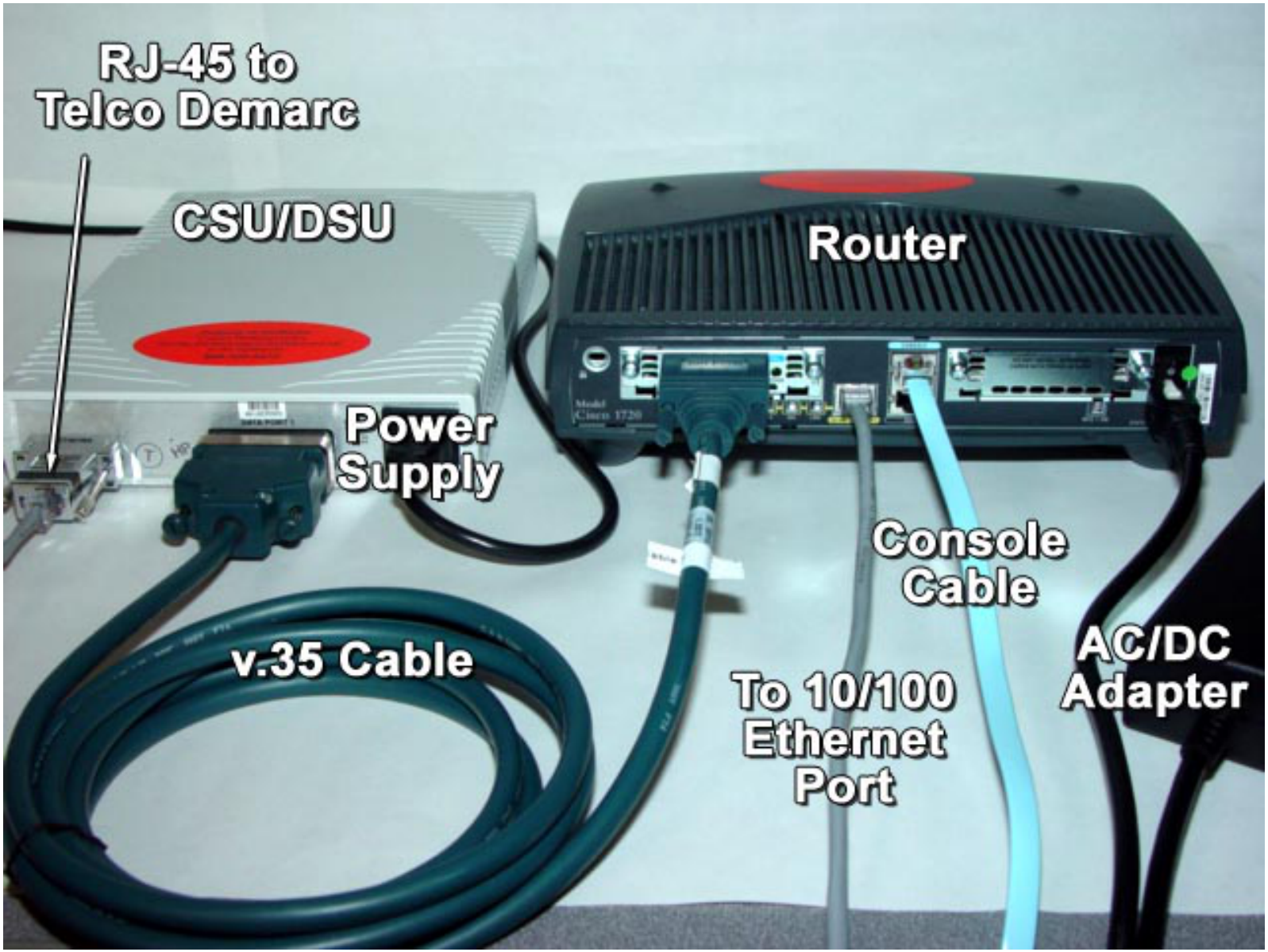


Puente

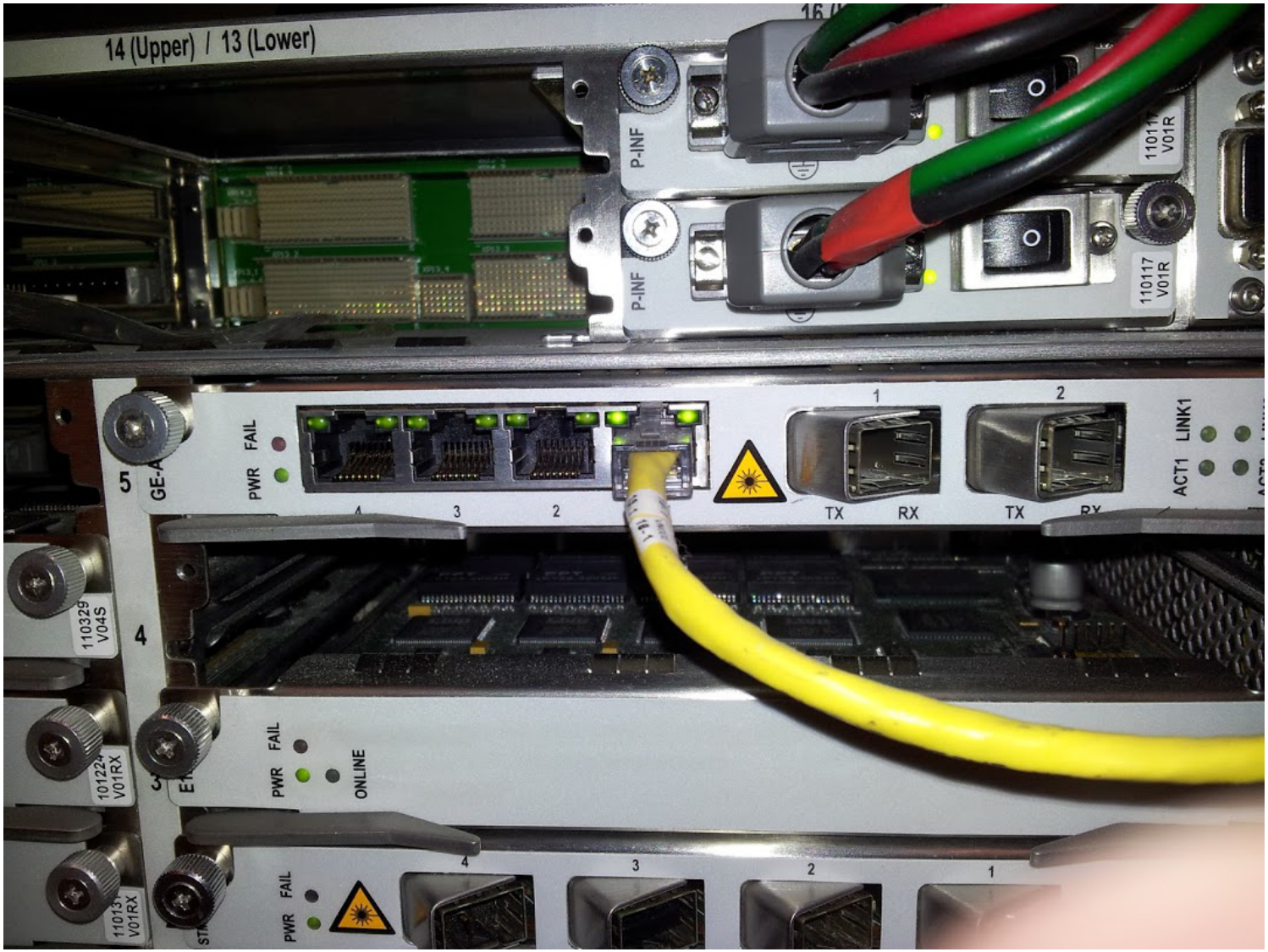
Conmutador

Enruteador

Enruteador de internet (viejo)

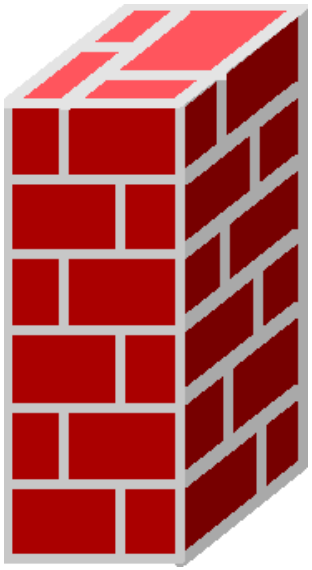


Enruteador de internet (hoy)

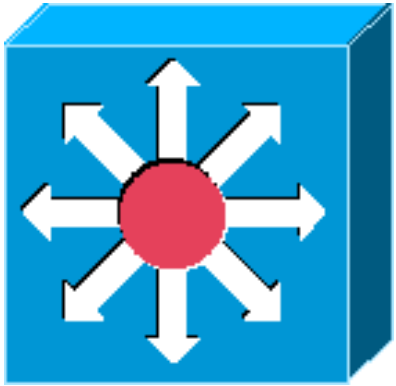


Punto de acceso

Cortafuegos / Firewall



Conmutador multicapa



Outline for section 5

Redes desmilitarizadas

Red demilitarizada. También conocida como red DMZ o red perimetral, es la sección o delimitación en donde un incidente de seguridad tendría un impacto mayor en la infraestructura de red.

Sus orígenes vienen en las zonas neutrales entre países en conflictos bélicos. Son estas zonas precisamente las más peligrosas (a pesar del nombre).

En esta sección de la red de datos, se encuentran los servicios e información de la empresa, por lo que cualquier intrusión se debe de considerar como un ataque.

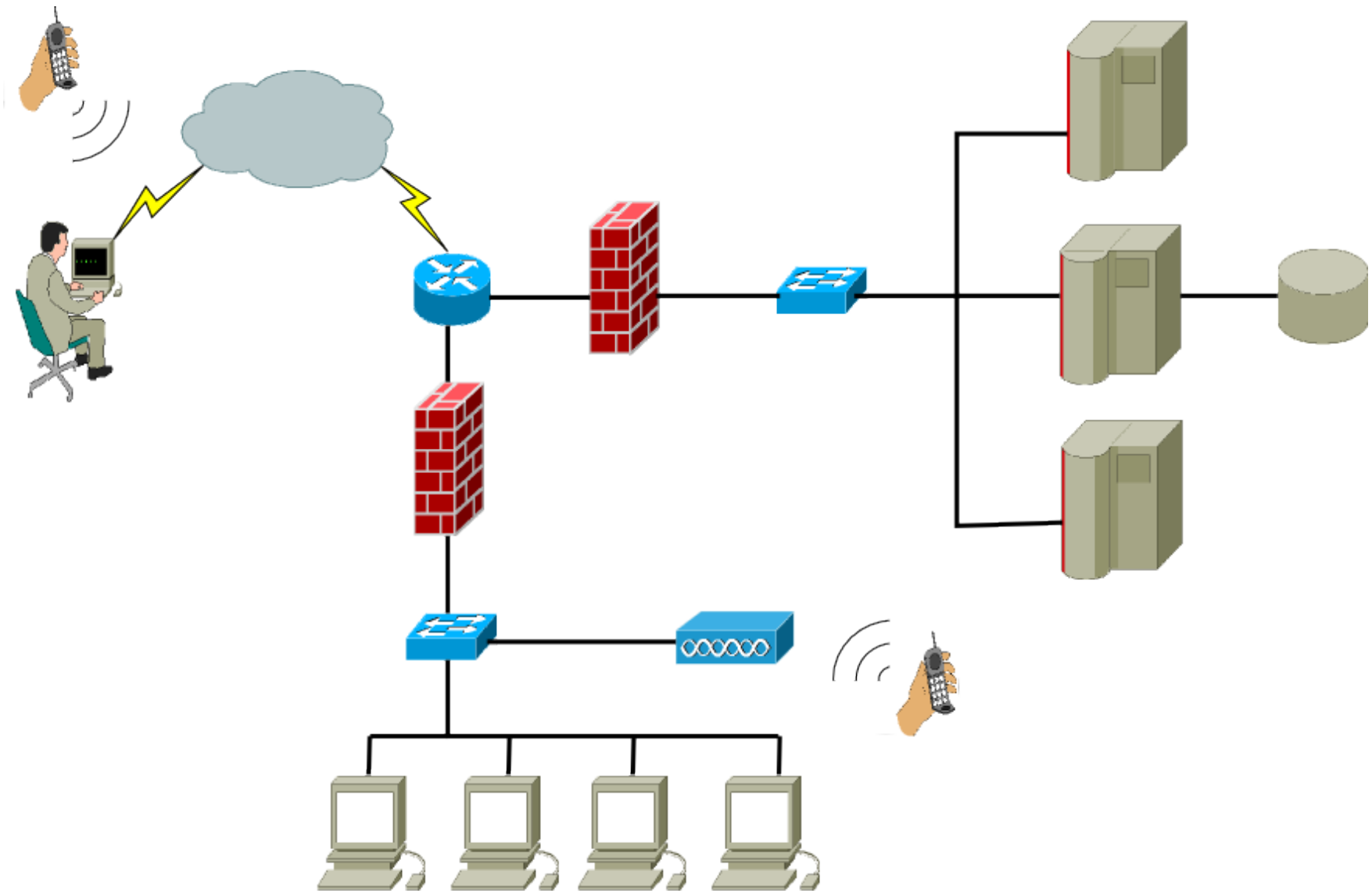
Redes desmilitarizadas

En la **DMZ** de la red de datos, se encuentran los servicios e información de la empresa, por lo que cualquier intrusión se debe de considerar como un ataque.

Esta red se encuentra normalmente detrás de un firewall y a partir de este, sólo se permite tráfico específico a los servidores, esto es: tráfico web sólo al servidor web, correo al servidor correspodiente, etc.

Si se tienen recursos, las labores de administración se realizan desde una red física aparte, de otra forma, se brinda acceso especial al administrador.

Red "Básica"



Intranet, extranet e internet

Intranet. Es la red interna a una corporación en una o varias sucursales. Algunas organizaciones se refieren a los recursos web únicamente accesibles desde la red interna.

Extranet. Es una red que permite accesso controlado desde el exterior a ciertos recursos internos. Utilizado por proveedores que requieren acceso a recursos propios de una intranet.

Internet. Es un sistema global de redes interconectadas. Se utiliza para obtener acceso a recursos públicos o información privada que necesita ser consultada desde cualquier punto en la red. Muchas empresas la utilizan como una extranet con ayuda de mecanismos de autenticación.

Outline for section 6

Redes virtuales

Dominio de difusión. Es un espacio lógico en el cual todos los nodos pueden contactarte al mismo nivel de la capa de enlace.

VLAN (Red virtual) Un grupo de puertos en el mismo dominio de difusión. Se pueden clasificar en:

- Puerto físico
- Dirección MAC
- Protocolo de red
- Aplicación

Redes virtuales

Dominio de difusión. Es un espacio lógico en el cual todos los nodos pueden contactarte al mismo nivel de la capa de enlace.

VLAN (Red virtual) Un grupo de puertos en el mismo dominio de difusión. Se pueden clasificar en:

- Puerto físico **Nivel Físico**
- Dirección MAC
- Protocolo de red
- Aplicación

Redes virtuales

Dominio de difusión. Es un espacio lógico en el cual todos los nodos pueden contactarte al mismo nivel de la capa de enlace.

VLAN (Red virtual) Un grupo de puertos en el mismo dominio de difusión. Se pueden clasificar en:

- Puerto físico **Nivel Físico**
- Dirección MAC **Nivel Enlace**
- Protocolo de red
- Aplicación

Redes virtuales

Dominio de difusión. Es un espacio lógico en el cual todos los nodos pueden contactarte al mismo nivel de la capa de enlace.

VLAN (Red virtual) Un grupo de puertos en el mismo dominio de difusión. Se pueden clasificar en:

- Puerto físico **Nivel Físico**
- Dirección MAC **Nivel Enlace**
- Protocolo de red **Nivel Red (IP/IGMP)**
- Aplicación

Redes virtuales

Dominio de difusión. Es un espacio lógico en el cual todos los nodos pueden contactarte al mismo nivel de la capa de enlace.

VLAN (Red virtual) Un grupo de puertos en el mismo dominio de difusión. Se pueden clasificar en:

- Puerto físico **Nivel Físico**
- Dirección MAC **Nivel Enlace**
- Protocolo de red **Nivel Red (IP/IGMP)**
- Aplicación **Nivel Transporte (TCP/UDP)**

Configuración

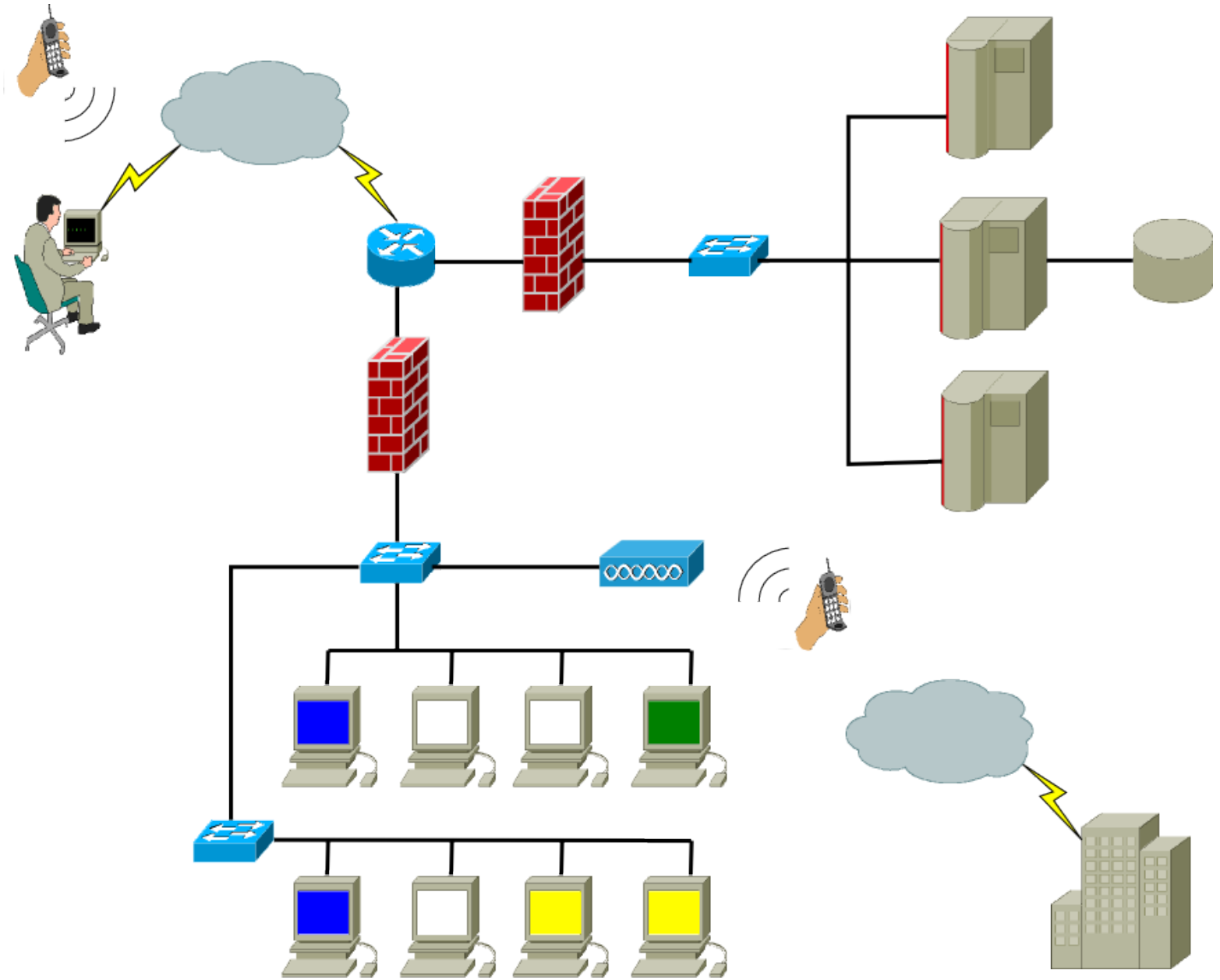
La configuración de las VLANs normalmente se hace a mano en archivos de texto y la sintaxis depende de la marca de los dispositivos. Algunos son incompatibles, estos normalmente se envían a donde no afecte.

Dependiendo de las características de nuestros equipos, tenemos las siguientes opciones:

- Configuración gráfica
- Configuración desde consola (o archivo)
- Distribución automática de las reglas (etiquetado de tramas de red)
- Configuración manual

Conmutador versus Conmutador multicapa.

Red "Básica"



Outline for section 7

Redes privadas virtuales

Las redes privadas virtuales (VPN) permiten a usuarios conectarse a recursos internos de la organización desde lugares externos como hoteles, el domicilio de los trabajadores, un café, entre otros.

Encapsulan el tráfico de red entre las partes en un paquete cifrado que es enviado a través de un medio inseguro. Dicho paquete se enruta como un paquete normal dentro de la red a la que están conectados los equipos.

Elementos involucrados

Los tipos de conectividad de las VPNs son:

- Punto a punto.
- Punto a multipunto.
- Multipunto a multipunto.

Elementos involucrados

Los tipos de conectividad de las VPNs son:

- Punto a punto. **Equipo a equipo**
- Punto a multipunto.
- Multipunto a multipunto.

Elementos involucrados

Los tipos de conectividad de las VPNs son:

- Punto a punto. **Equipo a equipo**
- Punto a multipunto. **Equipo a red empresarial**
- Multipunto a multipunto.

Elementos involucrados

Los tipos de conectividad de las VPNs son:

- Punto a punto. **Equipo a equipo**
- Punto a multipunto. **Equipo a red empresarial**
- Multipunto a multipunto. **Entre sucursales**

Elementos involucrados

Los tipos de conectividad de las VPNs son:

- Punto a punto. **Equipo a equipo**
- Punto a multipunto. **Equipo a red empresarial**
- Multipunto a multipunto. **Entre sucursales**

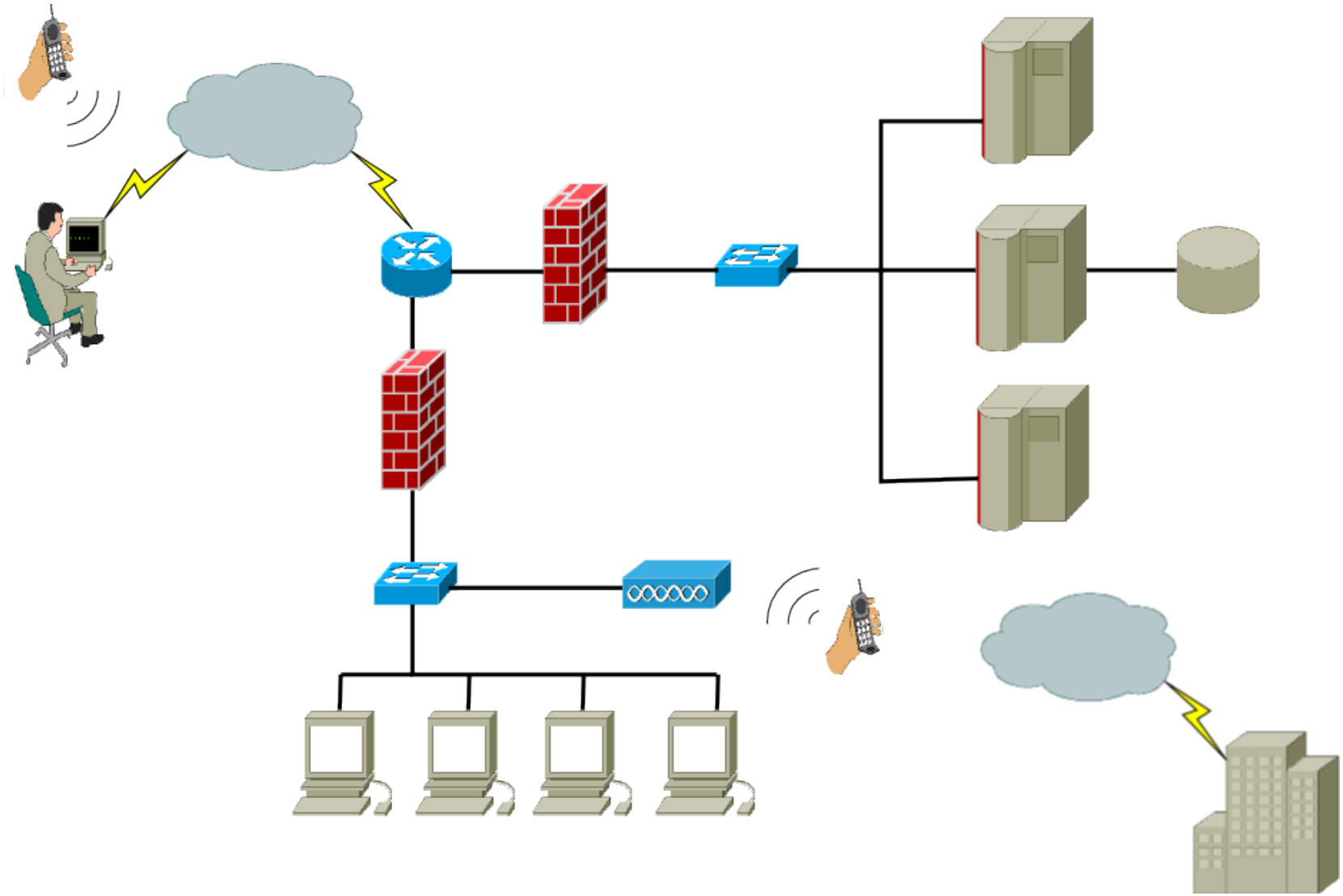
Cuando es de equipo a equipo o a una red, el equipo tiene un software en su computadora, el cual puede llegar a ser costoso. En el caso de conexiones entre redes, se prefiere equipo especializado.

Tipos de VPN

Para que una VPN sea efectiva, se requiere que esta sea en el nivel más abajo posible, esto es, existen soluciones comerciales de VPN a nivel de software, sin embargo, estas no siempre garantizan que las capas inferiores fueron comprometidas en su seguridad.

Actualmente, las VPNs seguras son las basadas en IPSec. Aún así, una mala configuración o descuido de las partes puede resultar catastrófico.

Red "Básica"



IPSec

IP Security, RFC 2401

- Seguridad en la capa de red.
- Proporciona servicios de cifrado y autenticación
- Es independiente de la aplicación a utilizar
- Soporta diversos esquemas de seguridad (algunos ya obsoletos)
- Provee un mecanismo para el intercambio de llaves (cifrado/descifrado)
- Provee protección de la identidad de las partes (al autenticar)

Su único problema es que es costoso en cuanto a la administración, además, los vendedores tienden a dar altos costos. Como opción para proteger la información, las empresas utilizan TLS (aka SSL).

Outline for section 8

Nivel o capa de aplicación

Recordemos que en un paquete TCP tenemos que establecer a qué puerto TCP/UDP se va a destinar la información recibida.

A nivel de software, cuando se programa una aplicación de red, se establece el puerto TCP/UDP al cual se va a escuchar. De esta manera el compilar genera código, que al ejecutarse, instruye al sistema operativo a redirigir el tráfico del puerto seleccionado a la aplicación (y viceversa).

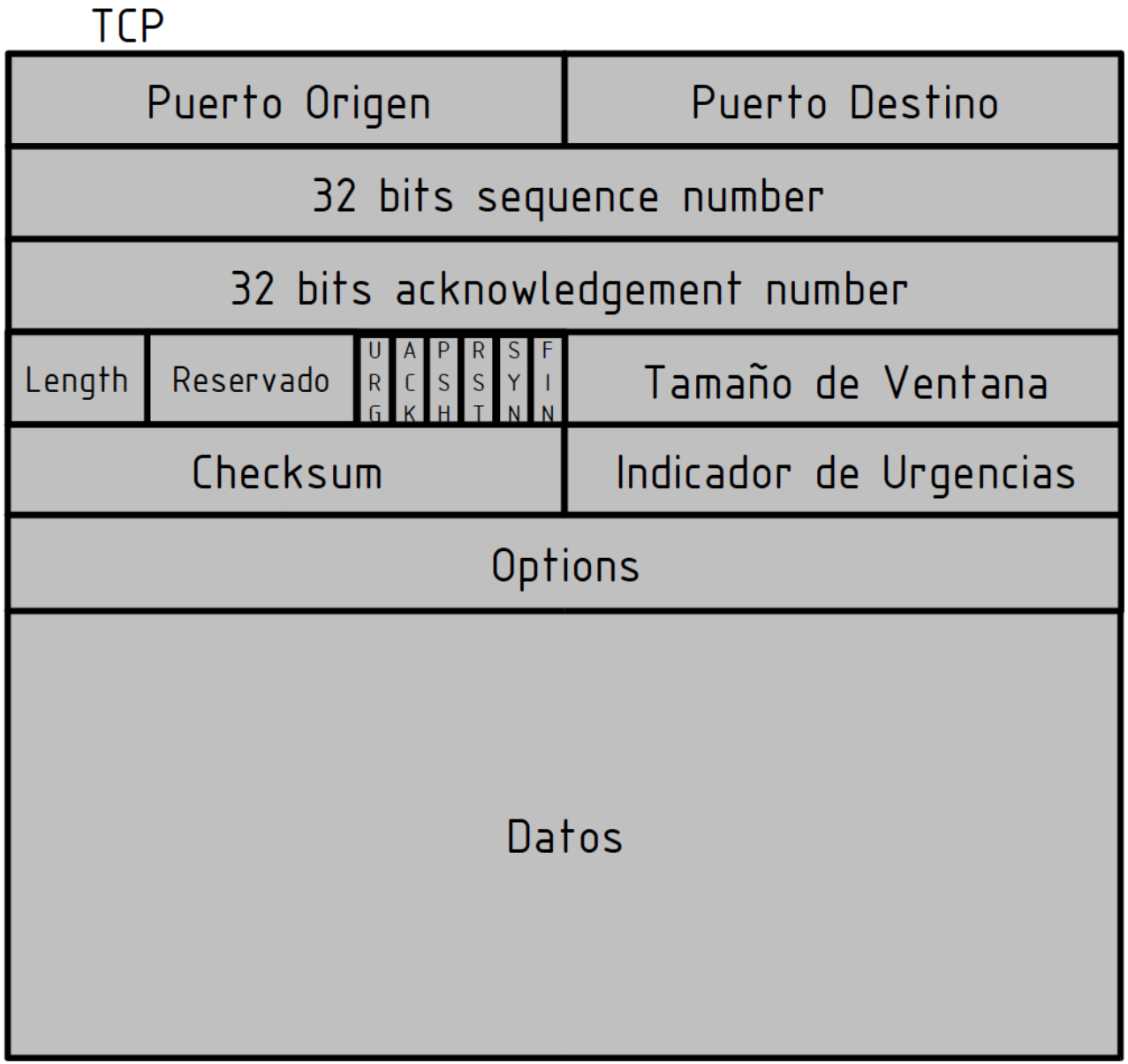
Nivel o capa de aplicación

Recordemos que en un paquete TCP tenemos que establecer a qué puerto TCP/UDP se va a destinar la información recibida.

A nivel de software, cuando se programa una aplicación de red, se establece el puerto TCP/UDP al cual se va a escuchar. De esta manera el compilar genera código, que al ejecutarse, instruye al sistema operativo a redirigir el tráfico del puerto seleccionado a la aplicación (y viceversa).

Ver diagrama anexo:

Paquete TCP


TCP
Puerto Origen
Puerto Destino
32 bits sequence number
32 bits acknowledgement number
Length
Reservado
URG
ACK
PSH
RST
SYN
FIN
Tamaño de Ventana
Checksum
Indicador de Urgencias
Options
Datos

Puertos TCP/UDP estándar 1/2

Para facilitar el intercamvio de datos, se estandarizaron números de puertos TCP/UDP de acuerdo a ciertas funcionalidades estándar en internet.

Los primeros 1024 puertos están reservados para aplicaciones de internet estándares y utilizadas de “siempre”

El resto de los puertos (del 1024 al 65535) son libres, aunque en algunos casos, las empresas loos utilizan para sus aplicaciones. El número de puertos está asociado al paquete TCP/UDP, por lo que no se pueden agregar más.

Puertos TCP/UDP estándar 2/2

Algunos de los servicios estándar son:

HTTP	80	Páginas web
FTP	21	Transferencia de archivos
Telnet	23	Terminal remota
SMTP	25	Envío de correo
DNS	53	Resolución de nombres de dominio
SSH	22	Terminal remota segura
POP3	110	Oficina postal
IMAP	143	Acceso a mensajes de internet

Existen además las versiones seguras de estos protocolos: https (443), pop3s (995), imaps (993), etc.

Outline for section 9

Ataques de red

Existen muchos tipos de ataques en la red.

- Denegación de servicio
- Man-in-the-middle
- XSS
- Overflow
- Mail relay
- DNS hijacking
- IP spoofing
- Eavesdropping
- Sniffing
- Modificación de datos
- Destrucción de infraestructura
- etc.

Razones

Los ataques en la red vienen dados por diferentes razones:

- Errores de diseño de los protocolos de red
- Errores de implementación de los protocolos de red
- Errores de diseño de la arquitectura de red
- Falta de presupuesto
- Descuidos en la configuración de los equipos
- Factores externos

Mecanismos de contensión 1/2

Salvo que se tenga una importante suma de dinero en infraestructura, la mayoría de los ataques podrían ser efectivos. Sin embargo, un ataque se puede evitar si existen suficientes factores que lo desmotiven.

Esto es, no existe una fórmula 100% efectiva, y salvo que se trate de un ataque específico contra la compañía, se pueden activar prácticas adecuadas para que un ataque automatizado, o de un amateur desista.

Mecanismos de contensión 2/2

Además de prácticas seguras, existen mecanismos palpables a instalar en la red:

- Firewall
- Detector de intrusiones
- Prevensor de intrusiones
- Pasarela de aplicación

Firewall 1/3

El firewall es el mecanismo básico de protección perimetral en una red. Tanto así, que ya fue cubierto como parte básica en una red.

Un firewall es un programa que dependiendo la flexibilidad del producto, puede distinguir usuarios o conexiones de red en diversas capas del modelo tcp/ip.

Es como un portero que deja entrar al personal a las diferentes áreas del edificio, verificando su ID. En algunos casos, nos deja pasar si ya hemos estado en el inmueble. Solo hace una verificación general de los datos al entrar.

Firewall 2/3

Un firewall restringir el acceso a la red al distinguir entre:

- Aplicaciones
- Puertos TCP
- Puertos UDP
- Direcciones de IP
- Tráfico de red
- Redes
- Direcciones de enlace

Firewall 3/3

Opcionalmente, verifica si:

- Si ha entrado recientemente
- Si se ha autenticado a la red
- Si ha hecho una secuencia de acceso

Finalmente, lleva un registro de entradas y salidas.

Detector de intrusiones

El detector de intrusiones (IDS) es un programa que verifica la autenticidad de los paseantes en la red, así como sus intenciones.

Esto es, verifica que:

- las direcciones de IP correspondan a quien dicen ser
- los puertos TCP/UDP correspondan al tipo de tráfico correspondiente (en algunos casos).
- los permisos de uso de red estén vigentes
- que no se esté realizando un ataque

Además de llevar un ataque, un IDS emite alertas de red de acuerdo a las políticas definidas dentro de la empresa. Las alertas pueden ser: correo electrónico, pager, llamada telefónica automatizada, etc. En todos los casos, se lleva una bitácora de los incidentes.

Prevensión de intrusiones

El prevensor de intrusiones (IPS), es un programa que además de realizar las labores de detección de instrusiones, o en conjunto con un IDS, intenta detener el ataque, o realiza aciones correctivas dependiendo de las capacidades de la red, por ejemplo:

- Avisar al firewall sobre alguna conexión maliciosa
- Enviar una señal al servidor para bloquear el acceso
- Alterar la comunicación para que no lleguen los datos
- Lanzar un ataque en respuesta.

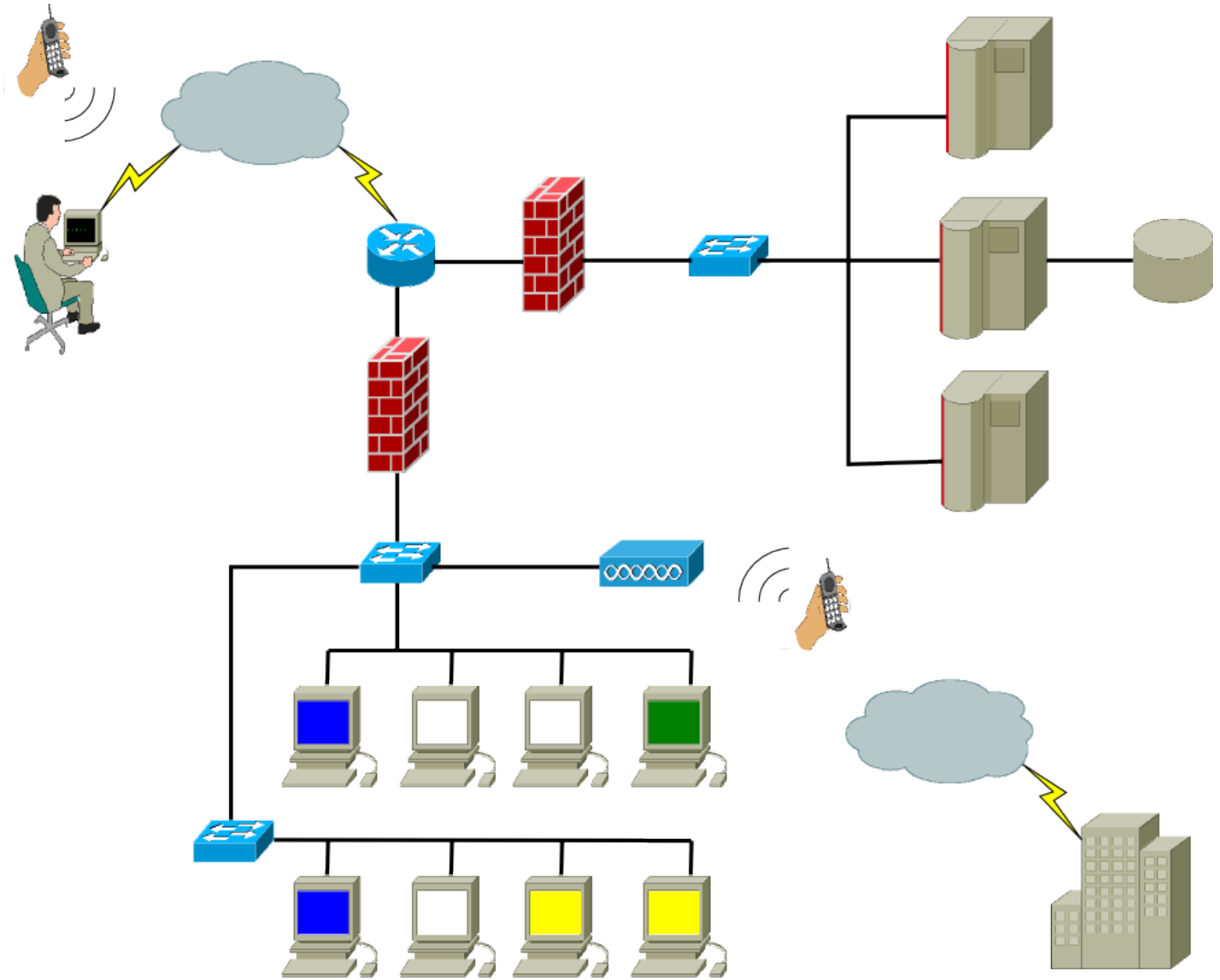
Pasarela de aplicación

Una pasarela de aplicación puede ser cualquier programa que intercepte legítimamente la comunicación entre pares y realice labores de análisis en busca de amenazas.

El tipo más común de pasarelas de aplicación es el antivirus gateway. Este tipo de programas responde a las peticiones de algún servicio, actuando como tal, y de no tener virus o trojanos conocidos, redirecciona el tráfico a su destino, por ejemplo: el servidor de correo, un servidor de archivos, o un servicio de mensajería instantánea.

Estos equipos son intrusivos, es decir, provocan latencia en la transmisión y pueden crear problemas a ciertas aplicaciones.

Red "Básica"



Outline for section 10

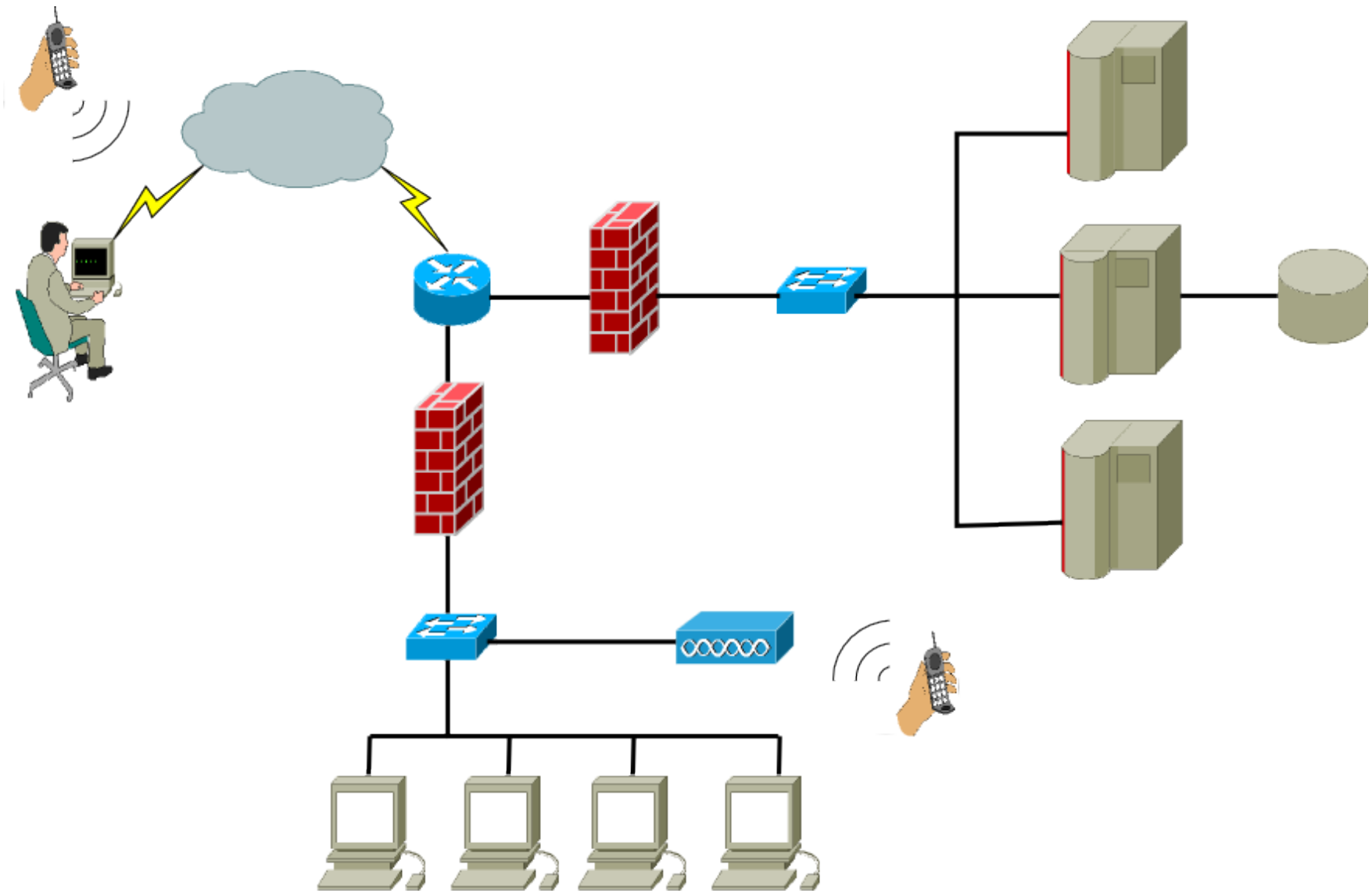
Práctica

Diseñar un esquema de red de su empresa, detallando las zonas desmilitarizadas, zonas de intranet, internet y extranet. Incluir diseño de redes virtuales (VLAN), y direccionamiento interno.

Opciones:

- Se presentará el diagrama actual general de red de la empresa y se discutirán sus partes. Se podrán hacer propuestas de mejora de ser necesario.
- Se realizará una propuesta de la red general de datos de la empresa, tomando en cuenta los puntos anteriormente mencionados.
- Se realizará una propuesta de una red de datos de una empresa tercera a la que se tenga conocimiento los participantes.

Red "Básica"



Redes y Seguridad Perimetral

Introducción a la seguridad - Sesión 1/4

Luis Dominguez
ldominguez@tamps.cinvestav.mx

Octubre 26 de 2012