Seguretat en xarxes

Seguretat en xarxes informàtiques.

Autor: Lluís Pérez Vidal

Seguretat en xarxes

Autors:

Aquest capítol de transparències és adaptat i traduït del curs sobre "Seguretat a l'Internet" dels professors Engin Kirda i Christopher Kruegel que podeu trobar a http://www.seclab.tuwien.ac.at/inetsec

Autor: Lluís Pérez Vidal

Seguretat en xarxes

Objectiu inicial d'aquest capítol

Fer-nos conscients de la importància de la seguretat

Veure les vulnerabilitats dels sistemes

Justificació

Els plans d'estudis d'Informàtica es centren molt en els aspectes de programació, enginyeria de programari, gestió, etc. i no tracten prou bé els temes de seguretat

Petites errades de seguretat ==> greus problemes

El nombre d'incidents de seguretat creix exponencialment

Autor: Lluís Pérez Vidal

Seguretat en xarxes

Contingut d'aquest capítol

Introducció i motivació

Amenaces a la seguretat

Model de referència OSI(Open Systems Interconnection).

comparació amb els protocols TCP/IP

Protocol d'Internet

estructura, atributs

IP sobre xarxes locals

atacs de fragmentació a una LAN

Autor: Lluís Pérez Vidal

Nombre d'incidents

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Autor: Lluís Pérez Vidal

Terminologia

Alguns noms especials

Hacker.

Persona a la que li agrada “remenar” dins dels sistemes, propis o d'altri. El terme no comporta qualificació negativa.

Cracker

Persona que s'introdueix dins de sistemes d'altri amb intencions malicioses.

Script kiddie (“niñato” que fa scripts)

Nen sense gaire coneixement ni experiència, però capaç de causar greus problemes.

Autor: Lluís Pérez Vidal

Seguretat en xarxes

Per què una persona remena ("hackeja") un sistema?

Reconeixement

Admiració

Curiositat

Poder i guanys

Venjança

Autor: Lluís Pérez Vidal

Tenim un greu problema

Els administradors de sistemes i de xarxes no estan (no estem) preparats

Manca de mitjans suficients

Manca de preparació i entrenament

Els intrusos cada dia coneixen millor i aprofiten les possibilitats de les connexions de banda ampla

Moltes computadores domèstiques connectades a la xarxa són vulnerables

Un conjunt gran de computadores domèstiques "controlades" són un arma potent (p.ex. per atacs DDOS)

Autor: Lluís Pérez Vidal

Nombre de vulnerabilitats

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

2004-2008

Year	2004	2005	2006	2007	2008
Vulnerabilities	3,780	5,990	8,064	7,236	6,058

www.cert.or

Autor: Lluís Pérez Vidal

Una mica d'història

Fa segles que es practica el “hacking”

A la dècada del 1870, els joves ja trastejaven amb el nou sistema de telefonia

A la dècada del 1960, apareixen els primers hackers al Artificial Intelligence Lab del MIT. Hackers és una denominació molt positiva.

Dècada dels 1970: Els hackers comencen a remenar els telèfons. Apareixen els phreaks=phone hackers.

Començaments dels 1980: Apareix la paraula “ciberespai” a la pel·lícula *Neuromancer.* Apareixen dos grups de hackers: Legion of Doom (USA) i Chaos Computer Club (RFA)

Autor: Lluís Pérez Vidal

Més història

Finals dels 80, als USA: Llei contra l'abús i el frau en l'ús de les computadores. Es forma el CERT (Computer Emergency Response Team). Kevin Mitnick és detingut.

Començament dels 90: Cauen els serveis de llarga distància de ATT. Redades de hackers als USA. Entrada dins la Base Griffith USAF, dins la NASA, etc.

Finals dels 90: Els hackers canvien planes web del govern i les computadores de Defense reben 250,000 atacs en un any.

Anys 2000 i escaig: Més atacs, phishing, etc.

Autor: Lluís Pérez Vidal

Els atacs canvien

Els intrusos estan més preparats i organitzats.

Els atacs des de Internet són fàcils, són una amenaça de baixa intensitat i molt difícils de detectar i de rastrejar.

Les eines dels intrusos cada cop són: a) més sofisticades; b) més fàcils d'usar.

No cal conèixer el codi font per trobar vulnerabilitats

Augmenta la complexitat de les aplicacions i els protocols en Internet i augmenta la nostra depndència d'ells.

Autor: Lluís Pérez Vidal

Amenaces a la seguretat

En el domini de l'informació

Espionatge de dades.

Adquisició d'informació per persones no autoritzades.
Exemple: “password sniffing”= Ensumar contrasenyes.

Manipulació de dades.

Creació o alteració no autoritzada d'informacions. Incloent-hi programes.

Exemples: Canvi d'una ordre de pagament electrònica, instal·lació d'un rootkit.

Autor: Lluís Pérez Vidal

Amenaces a la seguretat

En el domini de les operacions

Robatori de recursos.

Ús i abús de maquinari sense autorització.

Vandalisme.

Interferència en el funcionament correcte d'un sistema sense extreure'n profit.

Autor: Lluís Pérez Vidal

Alguns mètodes d'atac

"Punxar" una línia (eavesdropping).

Obtenir còpies d'informació sense tenir-ne permís.

Emmascarament.

Fer-se passar per un altre. P.ex., en l'enviament d'un missatge.

Manipulació de missatge

Alterar el contingut d'un missatge.

Autor: Lluís Pérez Vidal

Més mètodes d'atac

Repetició de la jugada (replaying).

Guardar còpia d'un missatge i enviar la còpia més tard. P.ex. reenviar un ordre de pagament

Aprofitar-se (exploiting).

Usar errors de programari per aconseguir entrar sense permís a un computador.

Combinacions.

Home al mig (man in the middle)

Emular les comunicacions de l'emisor i el receptor d'un missatge.

Autor: Lluís Pérez Vidal

Enginyeria social

Abans d'entrar en qüestions tècniques, veiem una tàctica d'atac molt extesa.

S'il·lustra a la pel·lícula “Intrusos”(sneakers).

“L'art i la ciència de fer que algú compleixi els teus desitjos”.

La seguretat pivota sobre la confiança. Intenten crear-li confiança a l'usuari final, que és l'element més feble de la cadena.

Trucades telefòniques.

Phishing.

Remenar a les papereres.

Autor: Lluís Pérez Vidal

La contrasenya

Cal preservar el propi password.

MAI no donis el teu password.

Pensa un password que puguis recordar de memòria.

A qualsevol altra persona li ha de resultar molt difícil d'endevinar el teu password.

MAI no canviïs el teu password perquè t'ho ordeni o t'ho recomani un e-mail.

Autor: Lluís Pérez Vidal

Criteris per escollir contrasenya

Un password de vuit caràcters.

Amb una barreja de majúscules, minúscules, alguna xifra i algún caràcter especial ($).

Pensar una frase i comprimir-la fins a vuit caràcters. “No hi han bolets” es pot transformar en Nhhnblts.

Quelcom que només tu puguis pensar. Fes servir l'imaginació!

MAI no canviïs el teu password perquè t'ho ordeni o t'ho recomani un e-mail.

Autor: Lluís Pérez Vidal

Exemples de contrasenya

Passwords dolents:

Montseny.

JoanPere

bermudas

Passwords bons:

QZ1hx2=/

2(xwk#0z

lu=)”5rH

Autor: Lluís Pérez Vidal

Trencament de contrasenya

Tàctiques conegudes per “trencar” el password:

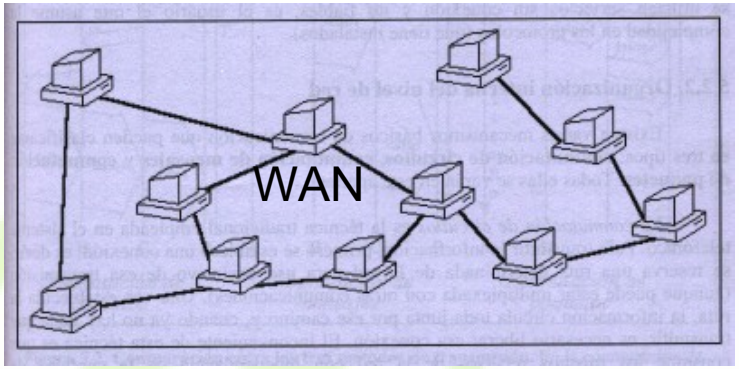
Qualsevol paraula que aparegui en un diccionari.

El teu username, el teu nom, nom d'algú que coneixes, canviar algún caràcter (0 per o, 1 per i).

Autor: Lluís Pérez Vidal

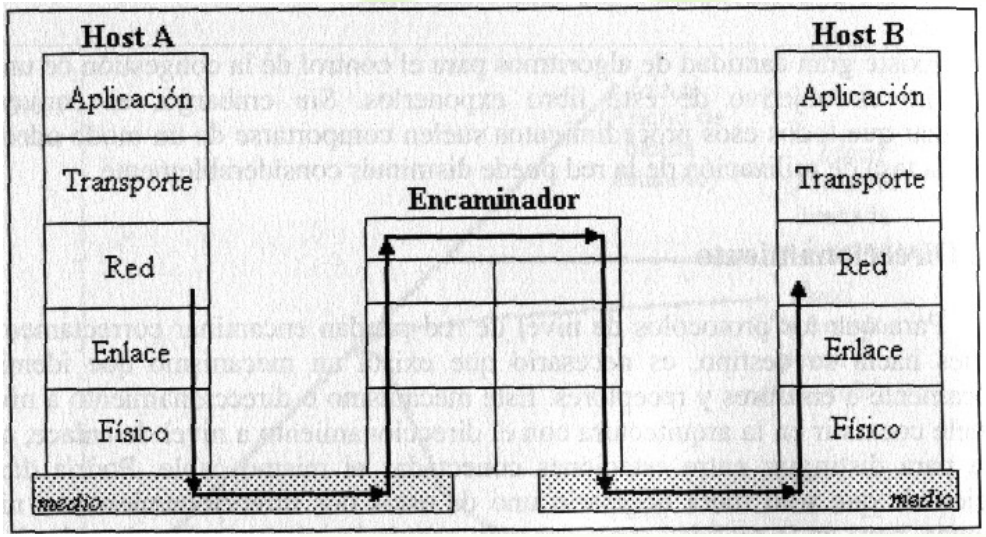
Model de referència OSI

Típic de les xarxes WAN



Aquest és el model OSI de set capes

Tot i que aquí només ensenyem cinc

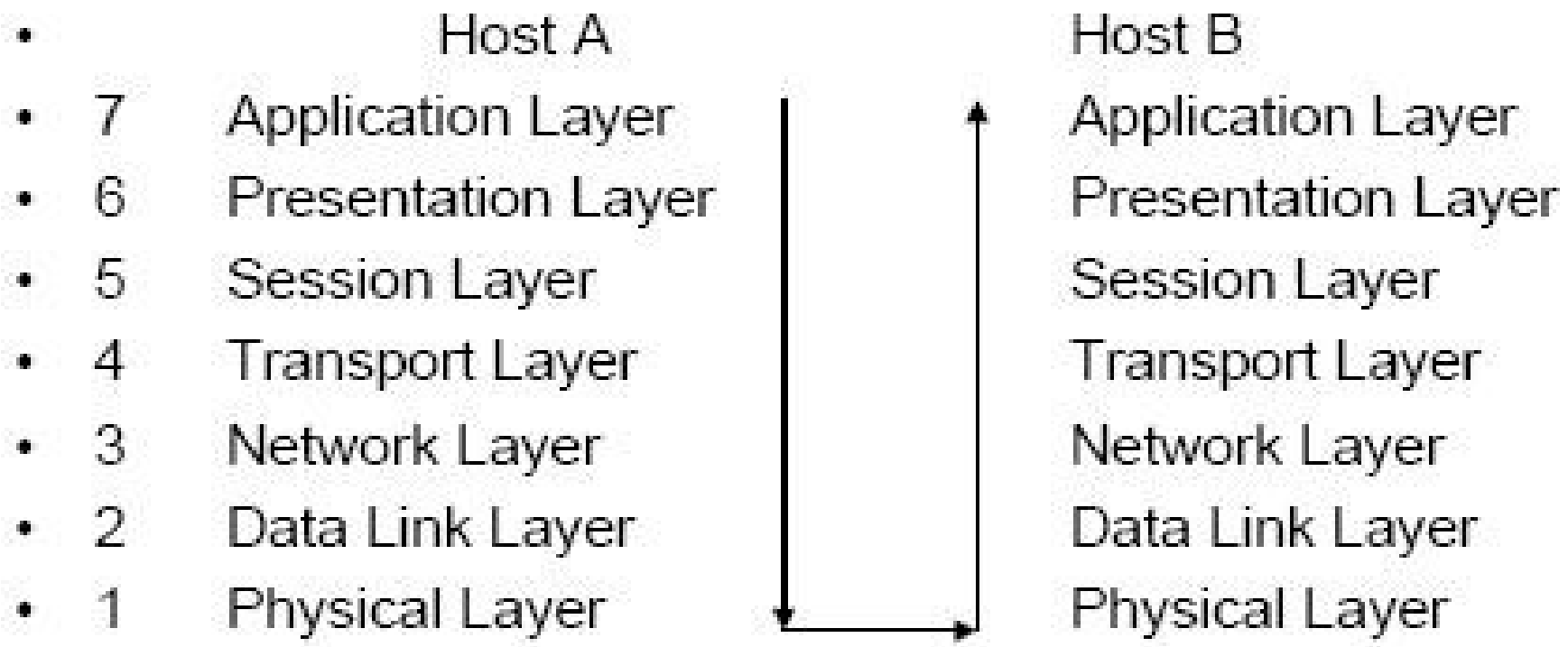


Autor: Lluís Pérez Vidal

Model de referència OSI

Desenvelopat per ISO per suportar l'interconnexió entre sistemes oberts

Arquitectura de capes: capa n usa els serveis de la n-1.



Autor: Lluís Pérez Vidal

Model de referència OSI

Nivell físic:

Connectat al canal. Transmet bytes (cable de xarxa).

Nivell d'enllaç de dades:

Control d'errades entre nodes adjacents.

Nivell de xarxa:

Transmissió i enrutament a través de subxarxes

Nivell de transport

Ordenació.

Multiplexat

Correcció

Autor: Lluís Pérez Vidal

Model de referència OSI

Nivell de sessió:

Suport per interacció basada en la sessió.

P.Ex. Paràmetres de la comunicació. Estat de la comunicació.

Nivell de presentació:

Representació estàndard de dades.

Nivell d'aplicació:

Protocols específics de l'aplicació.

Autor: Lluís Pérez Vidal

Per què capes?

Model obert:

Les capes superiors poden interactuar encara que les xarxes que hi han per sota siguin diferents.

Possibilita la compatibilitat de sistemes.

Permet maquinaris de diferents fabricants.

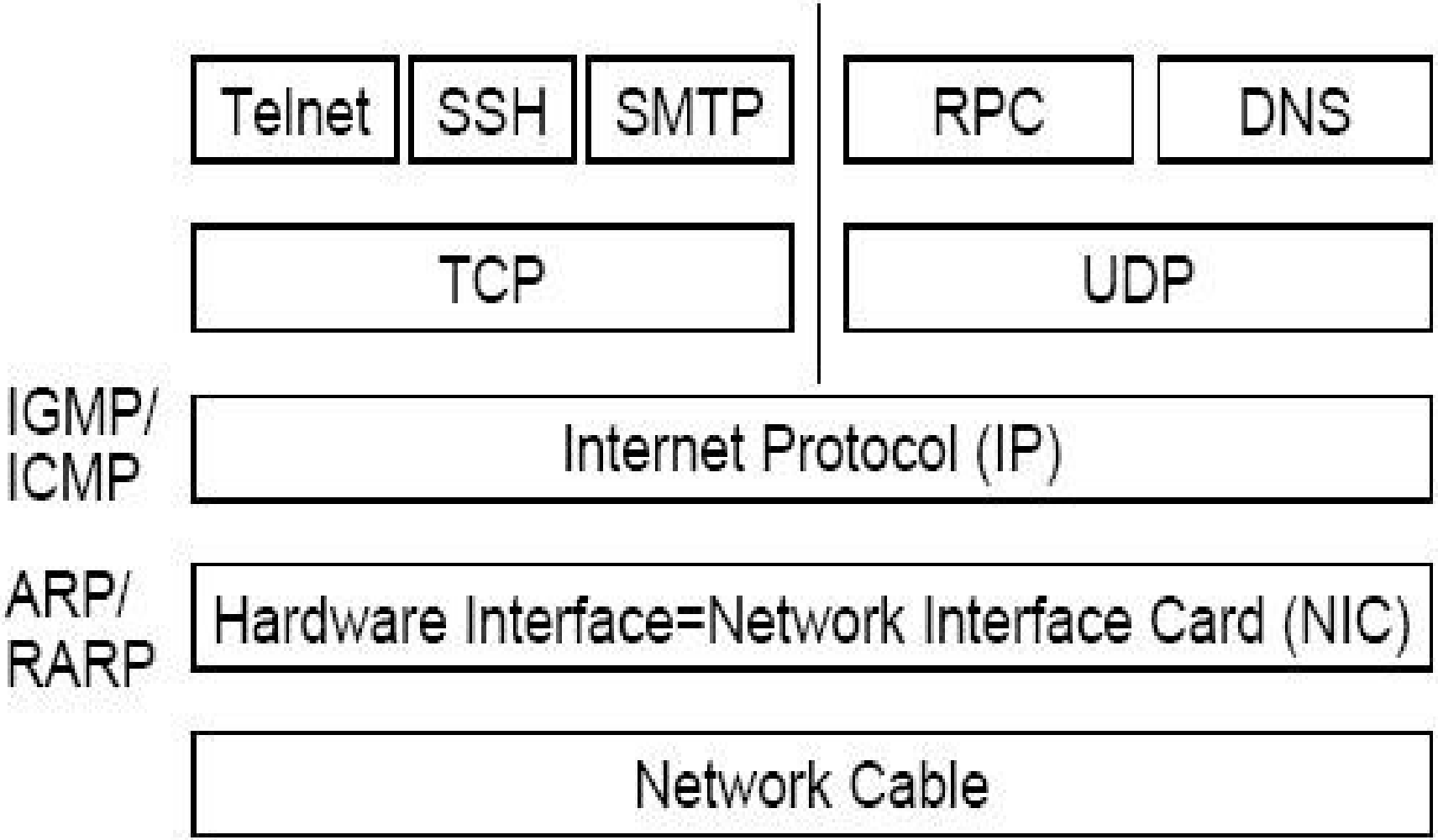
Permet protocols de diferents procedències.

Permet independència del fabricant.

Implementació OSI: MAP (Manufacturing Automation Protocol-GM, Token-Ring)

Autor: Lluís Pérez Vidal

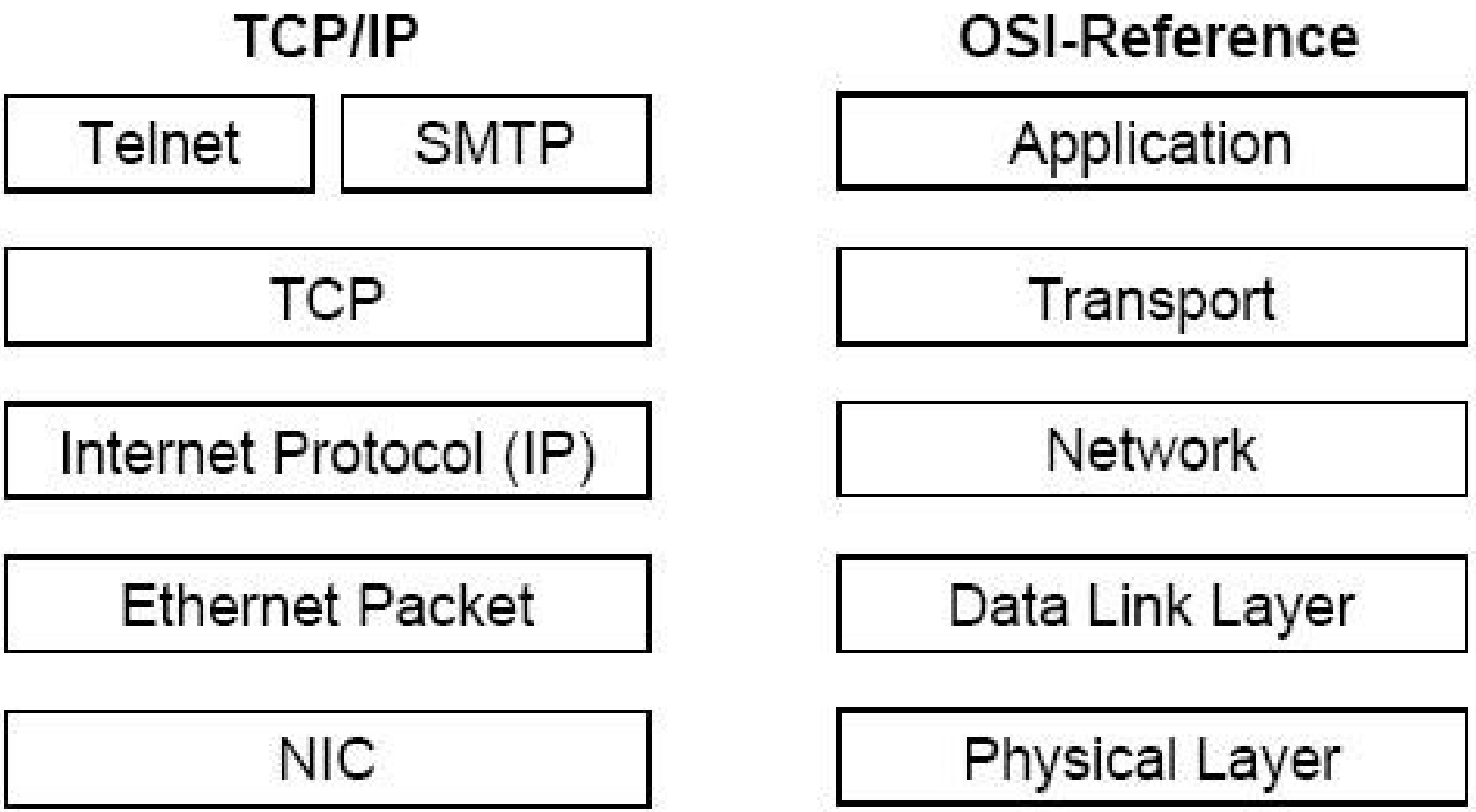
Capes TCP-IP



Autor: Lluís Pérez Vidal

Corespondència

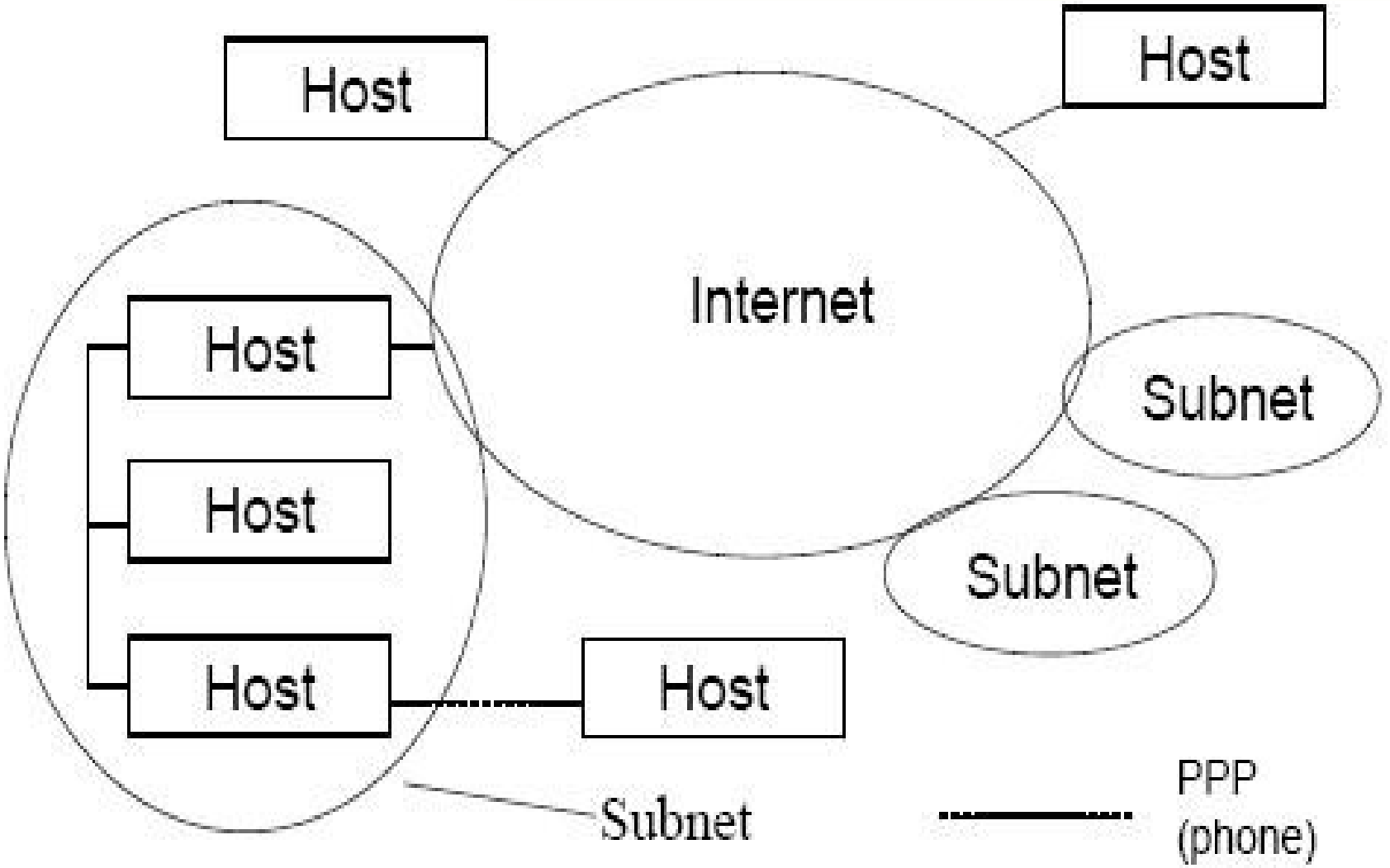
Mapping Correspondència



Autor: Lluís Pérez Vidal

L'internet

La xarxa:



Autor: Lluís Pérez Vidal

Apunts

A partir d'aqui:

http://www.

aboutdebian.com/network.htm

Apunts MOLT entenedors sobre el que segueix

Autor: Lluís Pérez Vidal

Adreces IP

Les adreces IP són de 32 bits

Permeten adreçar una mica menys de 4300 milions de màquines.

El format més comú és el decimal amb punts.

207.142.131.235 correspòn als 32 bits:
11001111.10001110.10000011.11101011

Altres notacions

Notation	Value	Conversion from dot-decimal
Dot-decimal notation	207.142.131.235	N/A
Dotted Hexadecimal	0xCF.0x8E.0x83.0xEB	Each octet is individually converted to hex
Dotted Octal	0317.0216.0203.0353	Each octet is individually converted into octal
Hexadecimal	0xCF8E83EB	Concatenation of the octets from the dotted hexadecimal
Decimal	3482223595	The hexadecimal form converted to decimal
Octal	031743501753	The hexadecimal form converted to octal

Autor: Lluís Pérez Vidal

Adreces IP

Adreces de 32 bits en IPv4:

(classe + xarxa + identificacio de màquina(“host”).

Cada host té una adreça única IP per cada NIC.

Ara executeu aquestes comandes, assabenteu-vos de que és cada part de les respostes, i comenteu-les.

/sbin/ifconfig
sudo ifconfig

cat /etc/resolv.conf

Autor: Lluís Pérez Vidal

Adreces IP

Suposem que hem de canviar algún paràmetre:

Suposem que la identificacio de màquina("host"), la seva IP sigui 147.83.29.11. I que el nom és "canyella".

Ara executeu aquestes comandes:

```
/sbin/ifconfig lo down
/sbin/ifconfig eth0 down
/sbin/ifconfig lo 127.0.0.1
/sbin/ifconfig eth0 147.83.29.11 broadcast 147.83.29.255 netmask 255.255.255.0
/sbin/route add -net 127.0.0.0 netmask 255.0.0.0 lo
/sbin/route add -net 147.83.29.0 netmask 255.255.255.0 eth0
/sbin/route add default gw 147.83.29.1 eth0
hostname canyella.lsi.upc.edu
rm /etc/resolv.conf
echo "search lsi.upc.edu" > /etc/resolv.conf
echo "nameserver  147.83.29.75" > /etc/resolv.conf
echo "nameserver  147.83.2.3" > /etc/resolv.conf
```


Autor: Lluís Pérez Vidal

Adreces IP

Adreces de 32 bits en Ipv4:

Les classes: [#: nombre de possibles hosts]

<comencen amb><bits de xarxa><bits de host><#>

Classe A: <0><7><24><16,777,216>

Classe B:<10><14><16><65,536>

Classe C:<110><21><8><256>

Classe D:<1110> Especial:28 bits d'adreça “multicast”

Classe E:<1111> reservat per futurs usos

Autor: Lluís Pérez Vidal

Subxarxes IP

No és realista tenir una xarxa amb tants hosts:

Què fem?: Dividir el camp de bits de host entre identificació de subxarxa i identificació de host.

Avantatge: Estalvi d'espai en les adreces.

Autor: Lluís Pérez Vidal

Subxarxes

La màscara determina quins bits estan reservats a la xarxa i quins bits a les màquines.

Depenent de les necessitats de xarxa (nombre de subxarxes i nombre de màquines per xarxa) s'escull la classe més adequada.

Els routers connecten subxarxes.

Autor: Lluís Pérez Vidal

Subxarxes IP

Exemple: La classe C normalment té 3 bits de xarxa

subxarxa classe C amb subnet mask 255.255.255.240

240 = 1111 0000

| identificació de host : 16 hosts per subxarxa

identificació de subxarxa : 16 subxarxes dins la xarxa

Autor: Lluís Pérez Vidal

Subxarxes IP

Exemple 2: La classe C normalment té 3 bits de xarxa

subxarxa classe C amb subnet mask 255.255.255.248

248 = 1111 1000

| identificació de host : 8 hosts per subxarxa

identificació de subxarxa : 32 subxarxes dins la xarxa

Autor: Lluís Pérez Vidal

Adreces IP especials

Com a adreça orígen i adreça destinació:

Interfície “loopback”.

Com a adreça de destinació:

Tots els bits a 1: “broadcast” local

Identificació de xarxa <> només 1s;identificació de host només 1s: “broadcast” cap al host per tota la xarxa.

Autor: Lluís Pérez Vidal

Adreces IP especials

Adreces reservades-no transmissibles (RFC 1597)

10.0.0.0 <-> 10.255.255.255

172.16.0.0 <-> 172.131.255.255

192.168.0.0<->192.168.255.255

Autor: Lluís Pérez Vidal

Protocol d'Internet IP

És la llengua en que es parlen els hosts.

Estàndard establert per l'RFC 791.

Atributs de l'entrega:

Sense connexió.

El datagrama és el millor possible però no és fiable:

NO es garanteix ni l'entrega, ni la integritat, ni l'ordre ni la no-duplicació.

Els paquets IP (datagrames) poden ser intercanviats entre qualsevol parella de nodes que estiguin configurats com a nodes IP.

Autor: Lluís Pérez Vidal

Protocol d'Internet IP

Per la comunicació directa, l'IP es vehicula mitjançant

protocols de més baix nivell:

Ethernet,

Token Ring

FDDI,PPP, etc

Ordenació estàndar de les dades (ordre a la xarxa)

S'explicita a la capçalera (“header”).

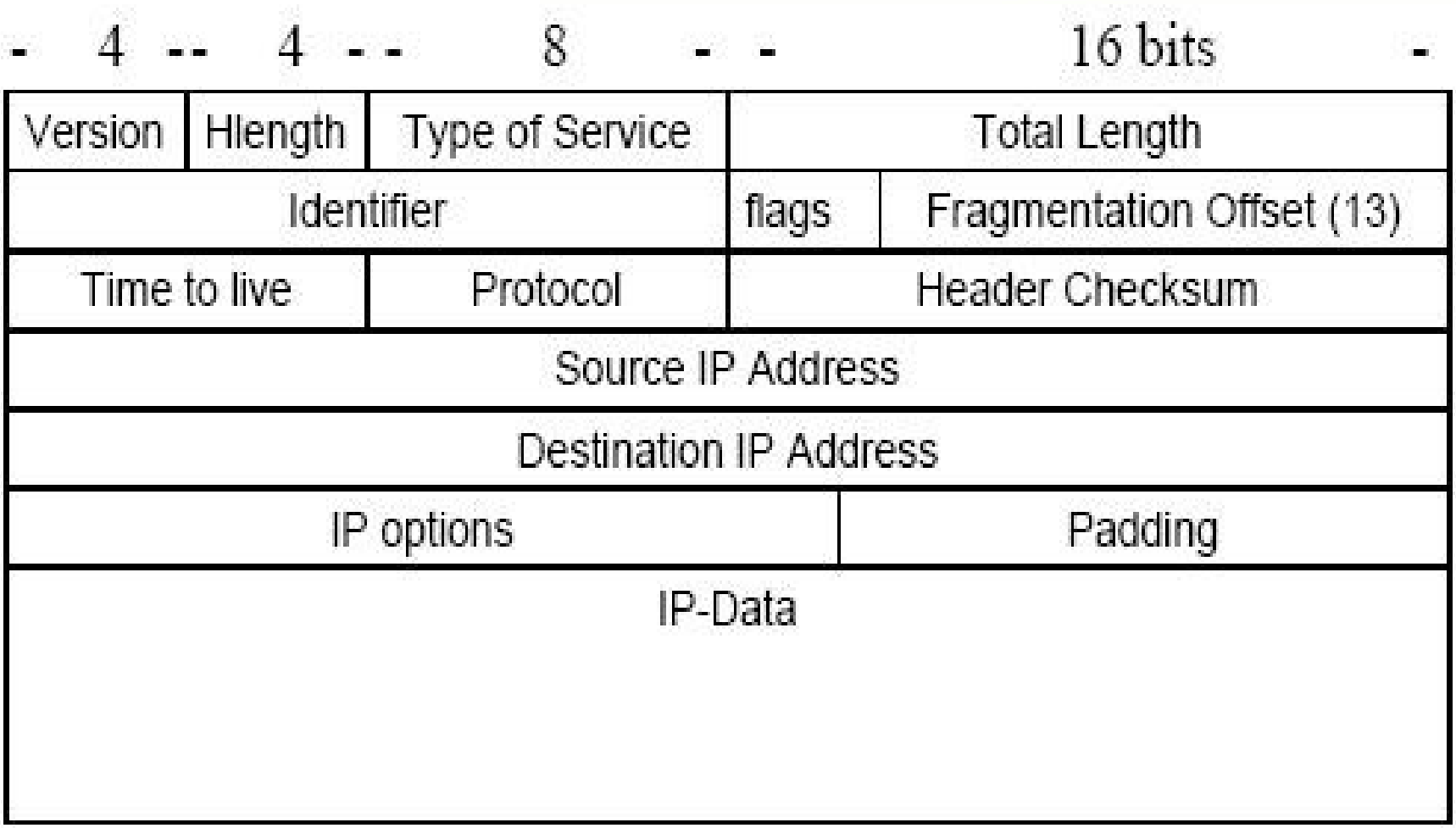
Ordre a la xarxa : big endian (a Linux0x86: littleendian)

El byte de menys pes es guarda a l'adreça més alta.

Autor: Lluís Pérez Vidal

Datagrama IP

Esquema funcional:



Autor: Lluís Pérez Vidal

Capçalera IP

Tamany normal : 20 bytes.

Versió 4 bits: Valor actual 4 bits (Ipv4)

Llargada de la capçalera: 4 bits

Nombre de paraules de 32 bits a la capçalera, incloent-hi les opcions IP.

Tipus de servei:

Prioritat (3 bits);QOS(4); 1 bit no utilizat.

Llargada total: Tamany total de capçalera i dades IP

Identificador del datagrama(16): incrementat +1

Autor: Lluís Pérez Vidal

Capçalera IP

Flags (3) i offset(13 bits)

usats per la fragmentació del datagrama.

Temps de vida (8 bits)

Nombre de salts permès per l'entrega.

Protocol(8 bits)

Detalla amb quin protocol és encapsul·lat el datagrama (TCP, UDP).

Checksum de la capçalera (16).

Adreces (32 + 32 bits):

Especifiquen origen i destinació.

Autor: Lluís Pérez Vidal

Opcions IP

Llargada variable.

Identificada pel primer byte:

Seguretat i restriccions de manipulació:

Registre de ruta:Es guarden les adreces ip dels routers.

Segell de temps: Cada router hi posa el seu.

Ruta de l'orígen:

S'especifica una llista d'adreces IP que el datagrama ha de travessar:

Laxes: Convé preferir aquests hosts.

Estrictes: Usar només els hosts donats (ruta).

Autor: Lluís Pérez Vidal

Rutes IP

Per examinar el camí (la ruta):

Us dona tots els “salts”.

Cal que l'atureu amb Ctrl-C.

mtr www.debian.org
mtr www.caliu.cat

Autor: Lluís Pérez Vidal

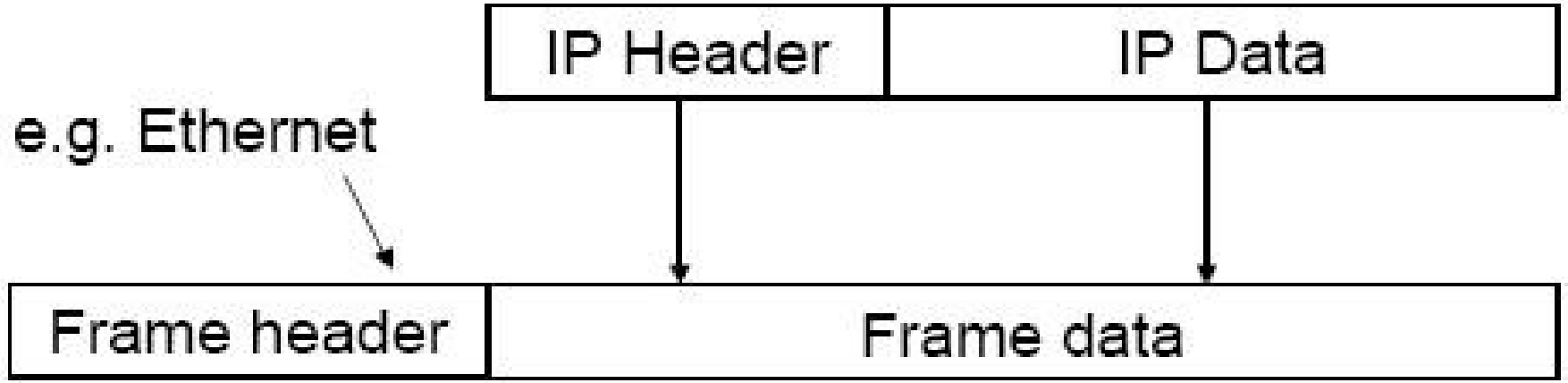
Encapsulament d'IP

Com es transmet un datagrama IP sobre una LAN?

No es pot fer directament a causa de la diferència de formats.

Les normes RFC 894 i 826 expliquen com fer-ho sobre Ethernet.

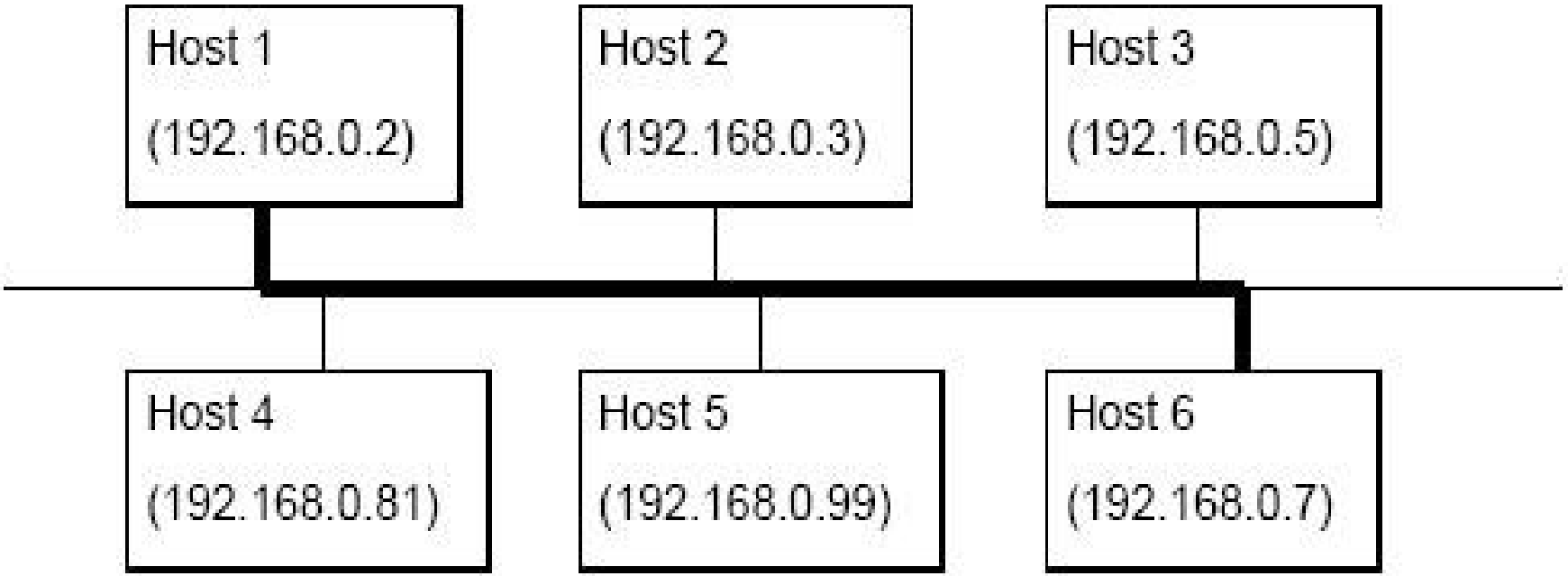
Solució: Encapsulament i transmissió directa.



Autor: Lluís Pérez Vidal

Entrega directa IP

Si dos hosts són a la mateixa xarxa física, el datagrama IP s'encapsula i s'entrega directament



Autor: Lluís Pérez Vidal

Ping senzill

Per fer una verificació ràpida:

Ping a màquina molt propera

Cada host té una adreça única IP per cada NIC.

Ara executeu aquesta comanda, assabenteu-vos de que és cada part de la resposta, i comenteu-la.

```
ping www.upc.edu -c 3
ping 147.83.2.135 -c 3
ping 147.83.155.1 -c 3
```


Autor: Lluís Pérez Vidal

Fragmentació

S'utilitza si l'encapsulament en un protocol de nivell inferior implica trocejar el datagrama en porcions de menor grandària.

Quan la grandària excedeix del MTU (Maximum Transmission Unit).

Es fa al host d'origen o en algun d'intermedi.

La reconstrucció del paquet IP només es fa al host de destinació.

Cada fragment s'entrega com un datagrama separat.

Autor: Lluís Pérez Vidal

Fragmentació

Amb cada fragment s'envia una capçalera IP adaptada.

Controlat usant 3 bits de flags IP i 13 bits d'offset

1er. bit : reservat.

bit de no-fragmentació: No es pot trocejar el datagrama.

bit de “més fragments”: Si aquest no és el darrer fragment d'un datagrama IP.

Autor: Lluís Pérez Vidal

Fragmentació

Si cal fragmentar però el bit de no-fragmentació és a CERT, s'envia un missatge d'error (ICMP) cap al remitent del missatge.

Si un fragment és distorsionat o perdut, es descarta completament tot el datagrama.

Autor: Lluís Pérez Vidal

Atacs de fragmentació

Antiga tàctica: El ping de la mort:

Cal ultrapassar el tamany màxim de datagrama IP.

El ping és un servei basat en l'IP: ¿els hosts són en marxa i són “visibles”?

Normalment la càrrega útil és de 64 bytes.

Amb fragmentació, es podria enviar un paquet IP amb grandària > 65535.

Autor: Lluís Pérez Vidal

Atacs de fragmentació

L'offset del darrer segment és tal que la grandària total del datagrama reconstruit supera la grandària màxima permesa--> es causa un sobreeiximent (overflow) al buffer estàtic de kernel que provoca un kernel panic (Ha funcionat amb Windows, Mac i Linux 2.0.x).

Autor: Lluís Pérez Vidal

Atacs de fragmentació

Antiga tàctica: Sobreescriptura de TCP. Enganyar el tallafocs (firewall).

Es fragmenta el datagrama IP que conté el tràfic TCP.

La capçalera TCP conté el port permés (p.ex. el 80).

El tallafocs deixa passar aquest paquet.

Les dades s'envien fragmentades.

Un paquet conté l'offset de fragment(1):

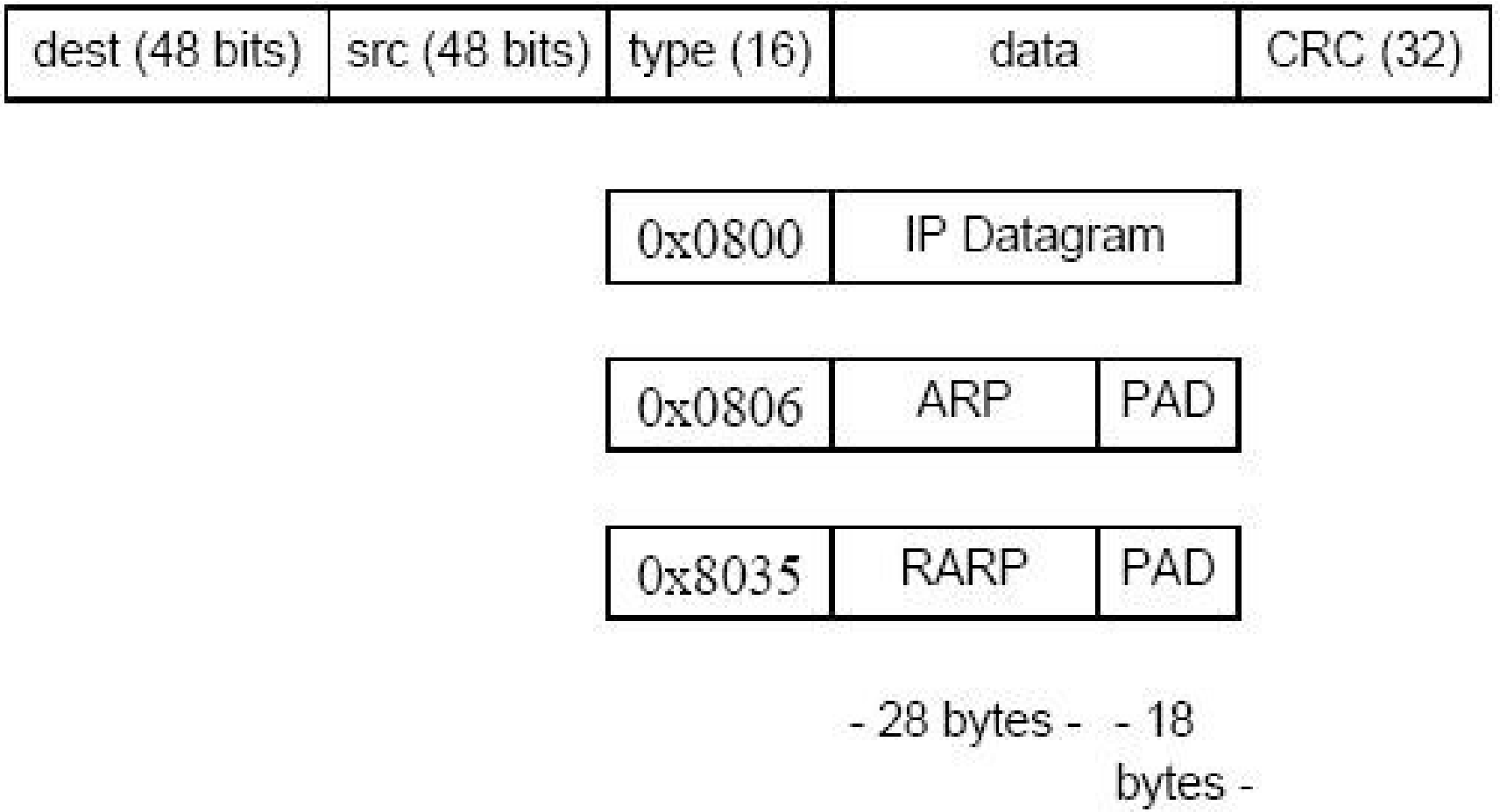
Es sobreescriuen els ports (p.ex. port nou 23).

Després de que s'hagi reconstruït completament el paquet, serà lliurat al nou port.

Autor: Lluís Pérez Vidal

Ethernet

Esquema



Autor: Lluís Pérez Vidal

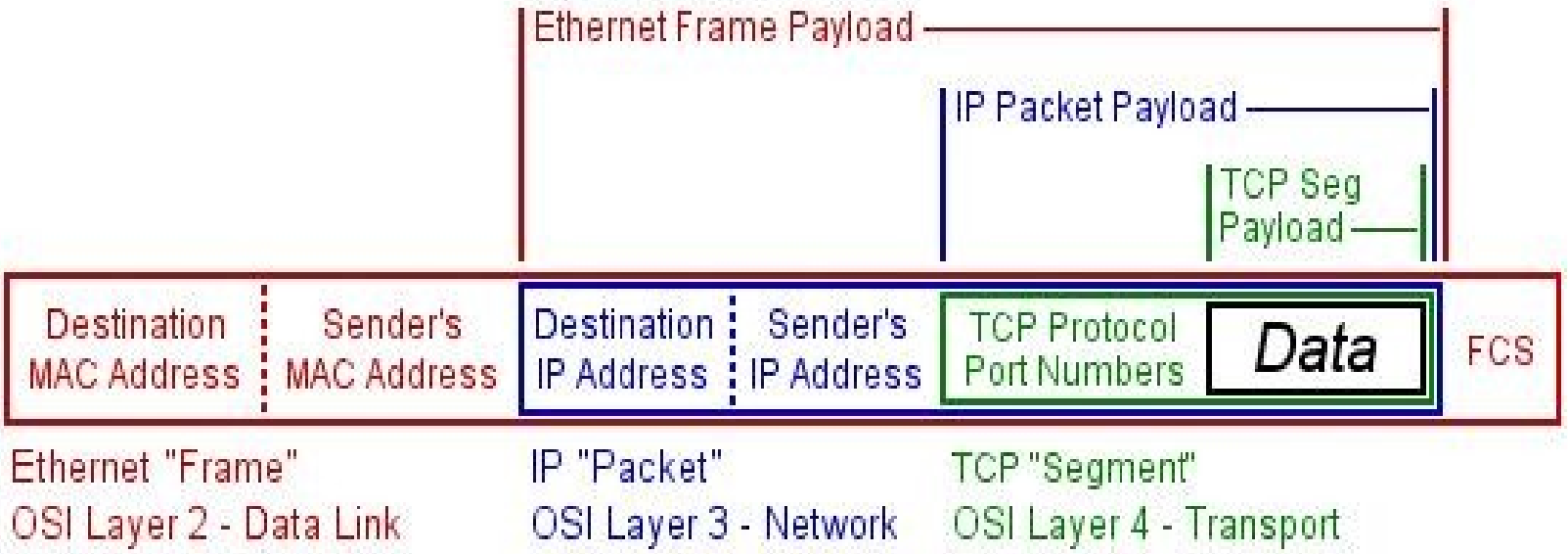
Ethernet

Esquema

Autor: Lluís Pérez Vidal

Ethernet

Esquema



Autor: Lluís Pérez Vidal

Ethernet

Protocol per capes molt utilitzat.

Carrier Sense, Multiple Access, Collision Detection (Escoltar la línia, accès multiple, detecció de col·lisions)

Adreces: 48 bits (p. ex.: c0:ad:fe:3c:ac:d2)

La majoria cablejada pel fabricant.

Autor: Lluís Pérez Vidal

Ethernet

Tipus: 2 bytes, diu quin protocol (IP,ARP,RARP).

Dades:

Mínim càrrega útil 46 bytes (possible “relleno”). Màxim 1550 bytes.

CRC : 4 bytes.

Autor: Lluís Pérez Vidal

Manipulació de la caché de ARP

Per veure la taula de caché de ARP:

I podeu esborrar alguna fila. Però alerta que no sigui important; o sigui, feu primer un ping a una màquina propera. I després l'esborreu de la taula ARP

Cada host té una adreça única IP per cada NIC.

Ara executeu aquesta comanda, assabenteu-vos de que és cada part de la resposta, i comenteu-la.

```
sudo arp
sudo arp -d 123.111.222.111
```


Autor: Lluís Pérez Vidal

La taula d'encaminament

Per veure la taula de caché de route

I podeu examinar les files.

```
route -C
route -Cvee
```


Autor: Lluís Pérez Vidal

Atacs a la xarxa local (LAN)

Objectius:

Capturar informació.

Suplantar un host.

Alterar mecanismes d'entrega.

Mètodes:

Ensumar (sniffing).

Spoofing d'IP.

Atacs d'ARP.

Autor: Lluís Pérez Vidal

Ensumar la xarxa (sniffing)

És la base de molt atacs:

L'atacant posa la NIC en mode “promiscu”.

La NIC passa tots el paquets entrants cap a la capa IP.

La NIC pot accedir tots els paquest que passen pel fil.

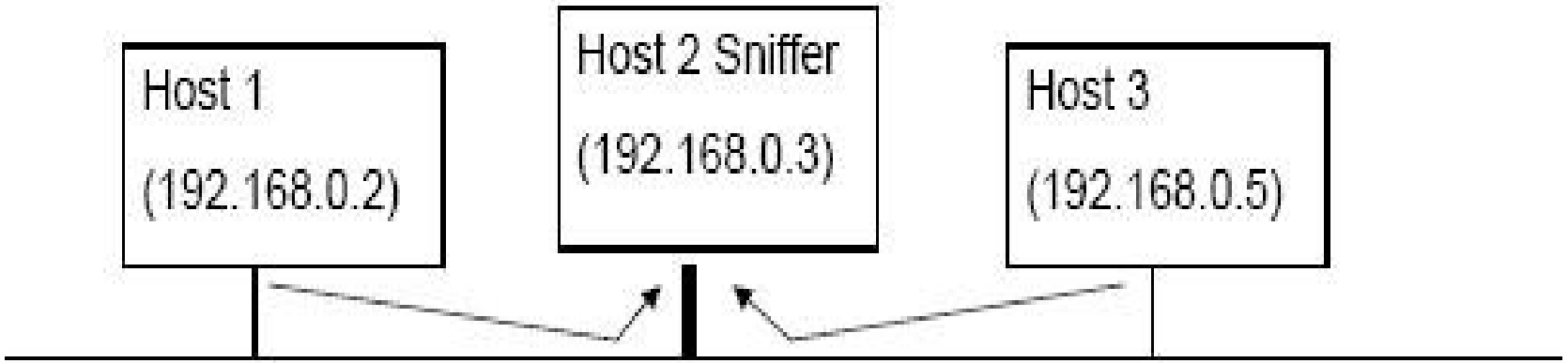
Molts protocols envien l'informació d'autenticació en text clar i planer -> capturar username, passwd.

Moltes eines disponibles: tcpdump -x, dsniff, etc.

Autor: Lluís Pérez Vidal

Ensumar la xarxa (sniffing)

Diagrama



Autor: Lluís Pérez Vidal

Ensumar la xarxa (sniffing)

¿Es pot ensumar una xarxa commutada, ón el switch només reenvia els paquets correctes cap el nostre host? SI

Inundació de MAC:

El switch té una taula amb el “mapping” adreça MAC-port.

Inundar el switch amb adreces MAC falses provoca un sobreeiximent de la taula.

El switch cau cap a mode hub.

Duplicació o clonat de MAC:

Hom pot comprar NICs amb adreces MAC reconfigurables.

El switch guardará això a la taula i m'enviarà el tràfic a mi.

Autor: Lluís Pérez Vidal

Detecció d'ensumadors (sniffers)

Es posa l'interfície en mode “promiscu”.

usar programes com /sbin/ifconfig per averiguar l'estat de la NIC.

Lectures del DNS sospitoses.

L'”sniffer” intenta resoldre noms associats a adreces IP.

Parany: Generar connexió des d'una IP impostora -> detectar el tràfic de DNS.

Autor: Lluís Pérez Vidal

Detecció d'ensumadors (sniffers)

Enviar un paquet IP a un servei que respongui (DNS, Telnet)

Posar l'adreça IP de destinació a aquell host.

Posar una adreça MAC inexistent.

Respostes del host->Tots els paquets a la pila TCP/IP.

Autor: Lluís Pérez Vidal

Detecció d'ensumadors (sniffers)

Latència.

Usar el ping per veure el temps de resposta del host A.

Generar enorme tràfic a d'altres hosts.

Veure el temps de resposta del host A.

Si mode promiscu: temps de resposta més llarg, pq s'analitzen tots els paquets.

Autor: Lluís Pérez Vidal

Conclusió

En aquesta sessió hem vist qüestions bàsiques de seguretat i xarxes

Reptes de seguretat.

Enginyeria social.

Model de referència OSI i protocol TCP/IP.

Ethernet, IP.

Atacs de fragmentació i a les LAN.

Autor: Lluís Pérez Vidal

creative commons

COMMONS DEED

Reconeixement-CompartirIgual 2.5

Sou lliure de:

- copiar, distribuir i comunicar públicament l'obra
- fer-ne obres derivades
- fer un ús comercial de l'obra

Amb les condicions següents:

Reconeixement. Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador.

Compartir amb la mateixa llicència. Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.

- Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.
- Alguna d'aquestes condicions pot no aplicar-se si obteniu el permís del titular dels drets d'autor.

Els drets derivats d'usos legítims o altres limitacions reconegudes per llei no queden afectats per l'anterior

Això és un resum fàcilment llegible del text legal (la llicència completa).

Advertiment

Autor: Lluís Pérez Vidal