

Redes LAN OSI – TCP-IP

IES San Clemente
Ver. 3 (11-10-05)

Profesor:
Carlos Carrión Álvarez
TCP / IP

OSI

Aplicación

Presentación

Sesión

Transporte

Rede

Enlace

Física

Aplicación

FTP

WEB

TELNET

...

Transporte (TCP / UDP)

Internet (IP)

Enlace / Interface de rede

Física / Hardware



Redes Área Local - OSI – TCP/IP

Acéptanse suxestións, corrección de erros, etc en carrion@edu.xunta.es.
Indicar no asunto o título do pdf e a versión.

Autorízase a reprodución total ou parcial deste documento, mencionando sempre a fonte.

1. Introducción

☞ Grande auxe na actualidade

Necesidades de intercomunicación (correo electrónico, bibliotecas información, etc)
Tecnoloxía a prezo asequible
Non ten senso o ordenador illado
No noso caso, redes instaladas pola consellería

1.1 Tipos de redes

☞ LAN (RAL) - Local Area Network

Comunican un conxunto de ordenadores ubicados nunha área xeográfica reducida (aulas, edificios, campus). Úsanse liñas propias.

☞ MAN - Metropolitan Area Network

Cubren un área xeográfica restrinxida a unha cidade. Xeralmente unen varias LANs mediante liñas públicas / dedicadas / privadas

☞ WAN - Wide Area Network

Abarcan áreas xeográficas tan grandes coma un país ou como o mundo enteiro (internet). Usan liñas dedicadas/públicas

1.2 Breve historia das comunicacións

☞ A arte da comunicación é tan antigo como a humanidade

Tan-Tan
Lume-fogo
Semáforos, etc.

☞ Ano 1834 S. Morse inventa o telégrafo

Código Morse (. e _)
Imposibilidade de automatizar debido á falta de sincronismo

☞ Ano 1874 Emil Baudot constrúe un código de lonxitude fixa

O número de elementos (bits) na sinal é o mesmo para cada carácter.
A lonxitude e a duración é a mesma para cada elemento.

☞ Ano 1876-1877 Invento e instalación da primeira liña de teléfono

☞ Dende 1928 ata 1970 Usáronse teleimpresores

Baseados no código de Baudot transmitían a 45 / 75 bps
Máis tarde baseados en código ASCII transmitían a 110 bps

☞ Ó final da Segunda guerra mundial comezou o desenvolvemento do ordenador

Orientados a procesos por lotes, non precisaban intercomunicarse

1.2 Breve historia das comunicacións

☞ Anos 50 – 60 desenvolvemento da informática financeira

Un gran ordenador o cal se interconectaban terminais moi rudimentarios “Tontos”
Usábase a conmutación de mensaxes

☞ Ano 1960 comézase a construír ARPANET

Rede militar americana
Na que se basea a archicoñecida rede Internet
Construcción do estándar TCP/IP

☞ Ano 1974 aparece as primeiras arquitecturas de IBM e DEC (SNA -System Networks Architecture, DNA – Digital Network Architecture)

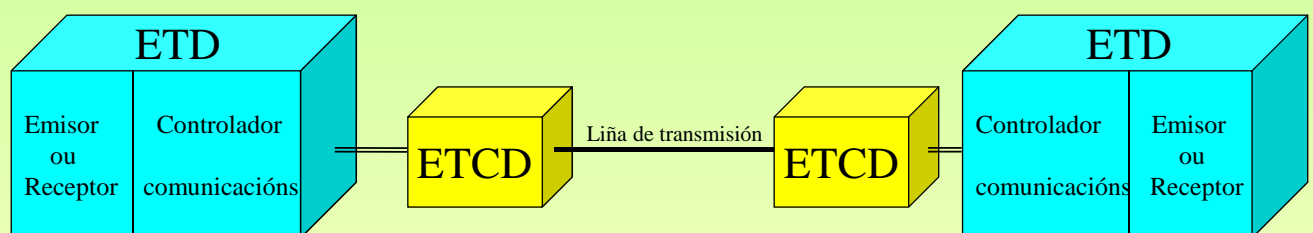
Tiñan estrutura de árbore.
Xurdiron para estandarizar as interconexións de tal cantidade de elementos dispares que ata ese momento tiñan.
A última versión de SNA saíu no 1985.
Foron as primeiras arquitecturas en abarcar tódolos niveis das comunicacións

☞ Ano 1984 aparece o modelo de referencia OSI (Open System Interconnection) de ISO

Trata de sentar as bases para que se poida desenvolver protocolos de comunicación que permitan a accesibilidade universal a información independentemente dos distintos produtos existentes e dos distintos fabricantes

2.- Medios de transmisión

☞ Modelo de un sistema de transmisión de datos



☞ ETD (Equipo terminal de datos)

Equipo fonte ou destino dos datos
Encargado de controlar as comunicacións

☞ ETCD (Equipo terminal do circuíto de datos)

Transforman os sinais dos ETD en outros que conteñan a mesma información, e en ocasións información de control, para poder ser transmitidos pola liña de transmisión

2.1- Perturbacións nas transmisións

☞ Perturbación

Conxunto de actuacións tanto externas como internas, sobre o sistema de transmisión, que provocan que o sinal recibido non sexa exactamente igual que o emitido polo emisor.

A Saber:

☞ Distorsión

Pódese producir tanto en amplitude como en frecuencia

☞ Intermodulación

O sinal emitido chega xunto con outras sinais a distintas frecuencias

☞ Ecos

Reflexión do sinal no receptor co cal volve ó emisor. Apreciable no receptor se o retardo é superior a 10ms.

☞ Diafonías

Prodúcese en liñas metálicas homoxéneas. Entre os dous ou varios cables dun mesmo conducto prodúcese acoplamentos.

☞ Ruído

Interferencias que recibe o medio de transmisión de distintos elementos externos. Térmicos (lámpada), impulsivos (ó acender un muíño)

☞ Atenuación

O sinal transmitido vai perdendo potencia a medida que aumenta a distancia de transmisión

2.2- Sistemas analóxicos e dixitais

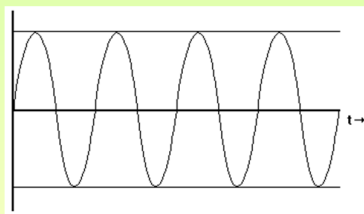
☞ Sistemas analóxicos

Sinal analóxica: aquela que pode tomar calquera valor dentro dun rango determinado.

A potencia do sinal analóxico recibido debe estar comprendido entre uns valores máximo e mínimo.

A calidade depende non só da potencia recibida, senón tamén do ruído que a acompaña.

Cando un sinal chega a un repetidor/amplificador este amplifica o sinal, co cal tamén amplifica o ruído que con ela chega.

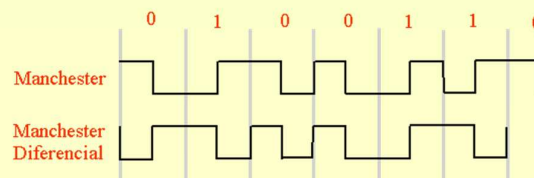


☞ Sistemas dixitais

Sinal discreta: aquela que só toma un número finito de valores dentro dun rango determinado.

A potencia do sinal discreto recibido debe estar comprendido entre uns valores máximo e mínimo.

Cando un sinal chega a un repetidor/amplificador este rexenera o sinal orixinal eliminando o ruído



2.3.- Modalidades de transmisión

Pódense clasificar atendendo a diversos parámetros

☞ Secuenciamento dos bit

SERIE: Os bits dunha palabra envíanse consecutivamente un tras outro.

PARALELA: Os bits dunha palabra envíanse por diferentes circuitos/cables.

☞ Simultaneidade na emisión-recepción

SIMPLEX (Simple): A transmisión realízase nun só sentido. TV, radio.

SEMI - DÚPLEX: A transmisión pódese realizar nos dous sentidos, pero non simultaneamente
Walkie-Talkie

DÚPLEX (Full-dúplex): A transmisión pódese realizar nos dous sentidos e simultaneamente.
Teléfono

☞ Sincronismo

Sincronismo: Proceso polo que o emisor informa ó receptor dos instantes en que comeza e finaliza un bloque de bits así como da duración de cada bit.

Sincronización de bit: recoñecemento do inicio e final de cada bit

Sincronización de palabra: recoñecemento do inicio e final dun conxunto de bits

Sincronización de bloques: recoñecemento do inicio e final dun conxunto de palabras

Transmisión ASINCRONA

Transmisión SINCRONA

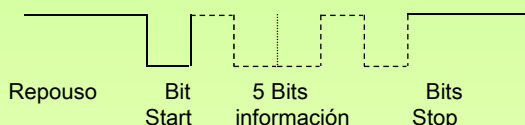
9

2.3.- Modalidades de transmisión

☞ Transmisión asíncrona

Foi a primeira en utilizarse. Un dos estándares é RS-232

O proceso de sincronización prodúcese para cada palabra que se transmite. Xunto cos bits da palabra a enviar envíanse outros que indican o inicio e o final da palabra.



Bit START: Marca o inicio dun novo carácter/palabra.

Bit STOP: Marca o final dun carácter/palabra. Sóense usar 1 ou 2 bits de STOP

Bits de información: depende do código usado: CCITT nº 2 (5 bits), CCITT nº5 (8 bits) e ASCII (8 bits)

Emisor e receptor deben traballar á mesma frecuencia e ter sincronizados os reloxos.

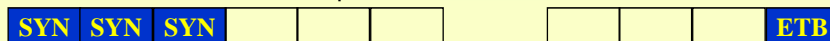
Eficiencia do código CCITT nº2: de cada 7 bits transmitidos 5 son de información, 71%

☞ Transmisión síncrona

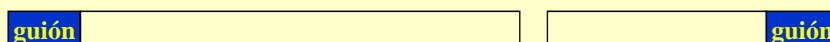
O sincronismo envíanse paralelamente cos datos.

Nos sinais dixitais realízase mediante determinados procedementos de codificación.

Tramas orientadas a carácter: o bloque de datos é tratado como unha secuencia de caracteres



Tramas orientadas a bit: o bloque de datos é tratado como unha secuencia de bits



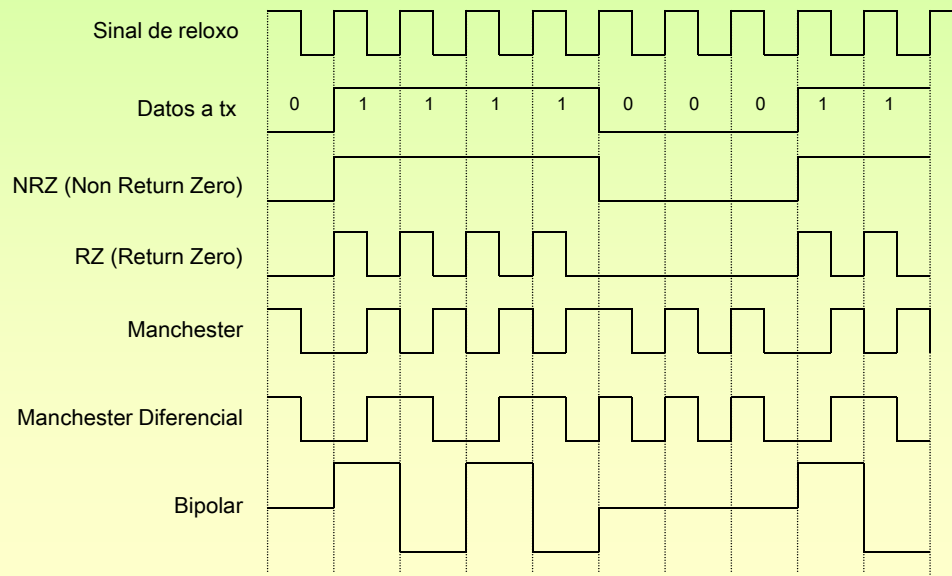
10

2.4.- Técnicas de Transmisión

Para transmitir os datos dixitais sobre as liñas de comunicación necesitanse determinados equipos: modems, tarxetas de rede, codificadores, decodificadores, etc.

☞ Transmisión de datos en Banda Base

Esta técnica define aquelas técnicas de transmisión nas que as frecuencias do medio (canle de transmisión) coinciden coas frecuencias do sinal que se desexa transmitir (información)



2.4.- Técnicas de Transmisión

☞ Transmisión de datos en Banda Ancha

Esta técnica define aquelas técnicas de transmisión nas que as frecuencias do medio (canle de transmisión) NON coinciden coas frecuencias do sinal que se desexa transmitir (información)

Portadora: sinal do medio, a que vai transportar a información.

Moduladora: sinal que modifica algún parámetro da portadora, é a información.

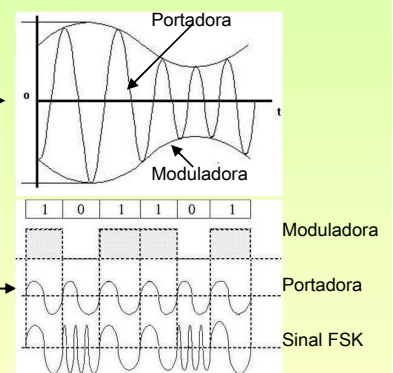
☞ Portadora Analóxica

Moduladora analóxica:

- Modulación en amplitude (AM)
- Modulación en frecuencia (FM)
- Modulación en fase (PM)

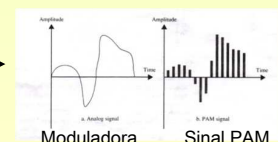
Moduladora dixital:

- Modulación por desprazamento de amplitude (ASK)
- Modulación por desprazamento de frecuencia (FSK)
- Modulación por desprazamento de fase (PSK)



☞ Portadora dixital e modulación analóxica

- Impulsos modulados en amplitude (PAM)
- Impulsos modulados en frecuencia (PPM)
- Impulsos modulados en duración (PDM)



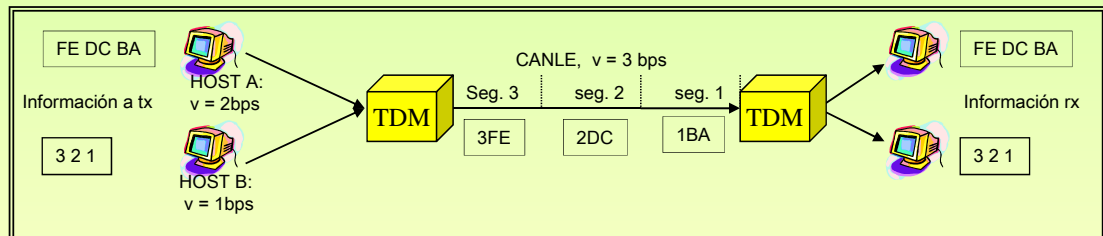
2.5.- Multiplexación

Definición

Transmitir por unha mesma canle información de distintas fontes. Existen dous tipos TDM e FDM

TDM (Multiplexación por división do tempo)

Úsase cando a velocidade do medio (canle) é superior a velocidade dos datos a ser transmitidos. Os emisores e receptores son máis lentos que a canle que transmite a información. A cada fonte de baixa velocidade asínaselle un fragmento de tempo da canle.



FDM (Multiplexación por división da frecuencia)

Os sistemas portadores son analóxicos con un amplo rango de frecuencias. Consiste en asignar a cada fonte (tx/rx) unha banda de frecuencias da canle. Doutro xeito, a canle divídese en bandas de frecuencia e estas son asignadas a cada unha fonte de datos. Por exemplo, o cable da TV, é un só cable polo cal se reciben moitas cadeas distintas.

2.6.- Medios de transmisión

Clasificación

Condutores metálicos

- Cable coaxial
- Cables de pares

Inalámbrica

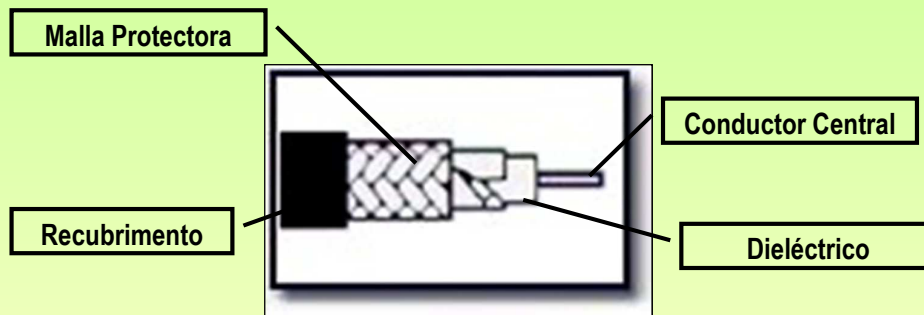
- Radio transmisión
- Microondas
- Infravermellos

Ópticos

- Ondas de luz
- Fibra óptica

2.6.- Medios de transmisión

☞ Conductores metálicos: CABLE COAXIAL



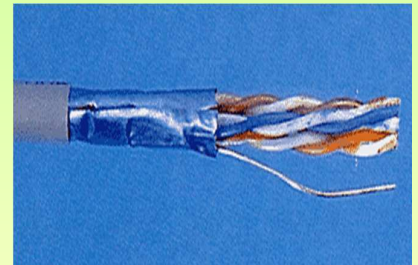
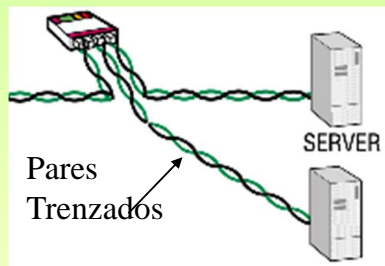
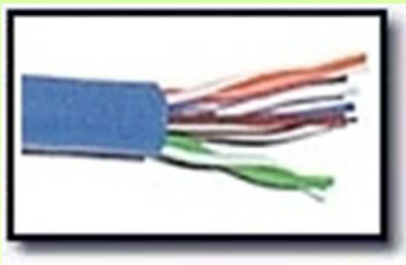
15

2.6.- Medios de transmisión

☞ Conductores metálicos: CABLE DE PARES

Plano / Sen trenzar: cable telefónico de 2 fíos

Trenzado: Cable de pares onde cada par de fíos vai trenzado sobre se mesmo.



☞ Cable de pares TRENZADO

UTP (Unshield Twisted Pair): cable de Pares Trenzado sen Apantallar

STP (Shield Twisted Pair): cable de Pares Trenzado Apantallado cunha cuberta de cobre

FTP (Foil Screened Twisted Pair): cable de Pares Trenzado Apantallado cunha cuberta de aluminio

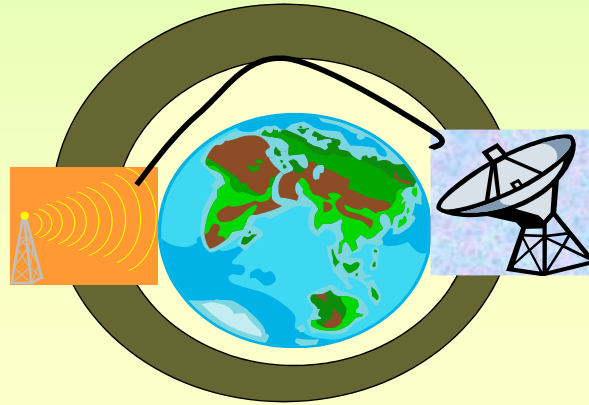
16

2.6.- Medios de transmisión

☞ Conductores AIRE / VACIO

Radio transmisión: Longas distancias, transmite en tódalas direccións
Antenas da Radio

Microondas: As ondas van en liña recta. Teñen problemas coa orografía.
Antenas Móviles
Comunicacións vía satélite / parabólicas



17

2.6.- Medios de transmisión

☞ Conductores ópticos

Ondas de Luz: Úsase en distancias curtas. Serve para unir edificios
Raios Láser

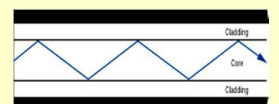
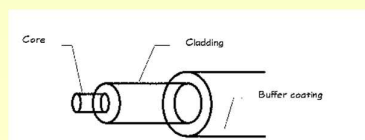
Infravermellos: Distancias curtas. Permítenos ter illadas as salas de comunicacións.
Calculadoras, Móviles
LANS inalámbricas

Fibra óptica: Conductor que transporta a información mediante haces de luz.
O núcleo está formado por un fio de vidro capaz de conducir no seu interior un raio óptico.

Monomodo: Transmite un só haz de luz. Permite altas velocidades e distancias.
Multimodo: Transmite varios raios de luz. Velocidades máis baixas e máis barata

Compoñentes: Emisor, transmisor, receptor

Vantaxes: Inmune ó ruído, baixa atenuación, non sofre interferencias
Inconvenientes: Cara, require especialistas



18

3.- Topoloxías de rede

☞ Tipos de Liñas

Punto a punto: Estas liñas unen **só dous** elementos de comunicación

Seguras contra roubo de información.
Caras (custe/nº elementos conectados)
Por exemplo:

Radio enlace.
Dous ordenadores

Multipunto / Broadcast: Estas liñas unen con un só medio varios elementos de comunicación

Inseguras contra roubo de información
Baratas (custe/ nº elementos conectados)
Por exemplo:

Bus de datos
Comunicacións vía satélite/parabólica

3.- Topoloxías de rede

☞ Propiedade das liñas

Privadas: As liñas que teñen un propietario definido. O mesmo propietario é quen fai uso delas.

LAN
Algunhas MANs (USC)

Públicas: Son de titularidade pública. Teñen ámbito nacional/supranacional

Os abonados fan uso das liñas mediante o pago dun aluguer/uso
Telefónica
Unión Fenosa

Dedicadas: Son liñas públicas pero de uso exclusivo de quen a aluga.

RECETGA (Liña dedicada de U. Fenosa Santiago-Lugo)

3.- Topologías de rede

☞ Topologías

Distintas formas de organizar unha rede.

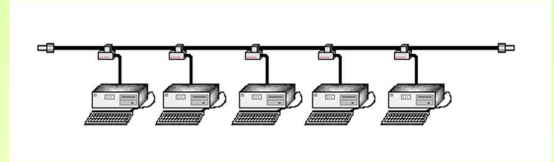
Bus
Anel
Estrela
Árbore

☞ BUS

Tódolos ordenadores conectados a un mesmo cable.

Fácil ampliación
Baixo custe de instalación

Facilidade de roubo de información
A rede queda inutilizada se se rompe un cable

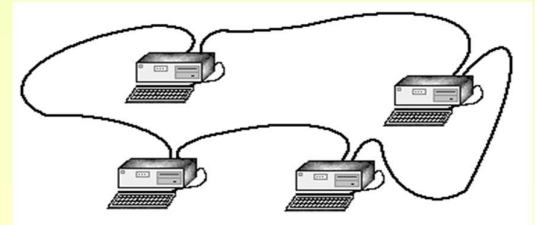


☞ Anel

Os nodos están enlazados entre si facendo un circulo.

Fácil ampliación
Custe moderado da instalación

Facilidade de roubo de información
Se rompe un cable non se comunicarán os ordenadores que enlazaba



21

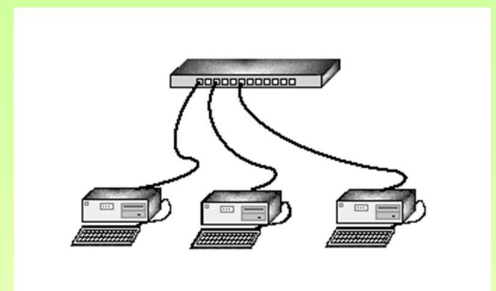
3.- Topologías de rede

☞ Estrela

Tódolos nodos están conectados a un nodo central.

Facilidade de ampliación
Custe medio/alto (un cable/nodo)

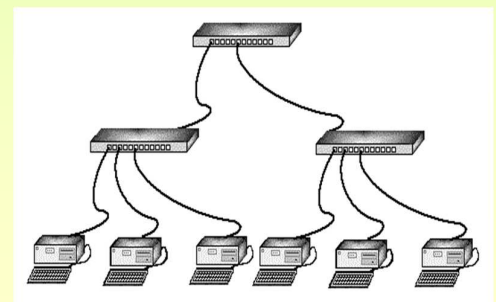
O problema é que se depende dun
nodo central.
O roubo de información pódese controlar



☞ Árbore

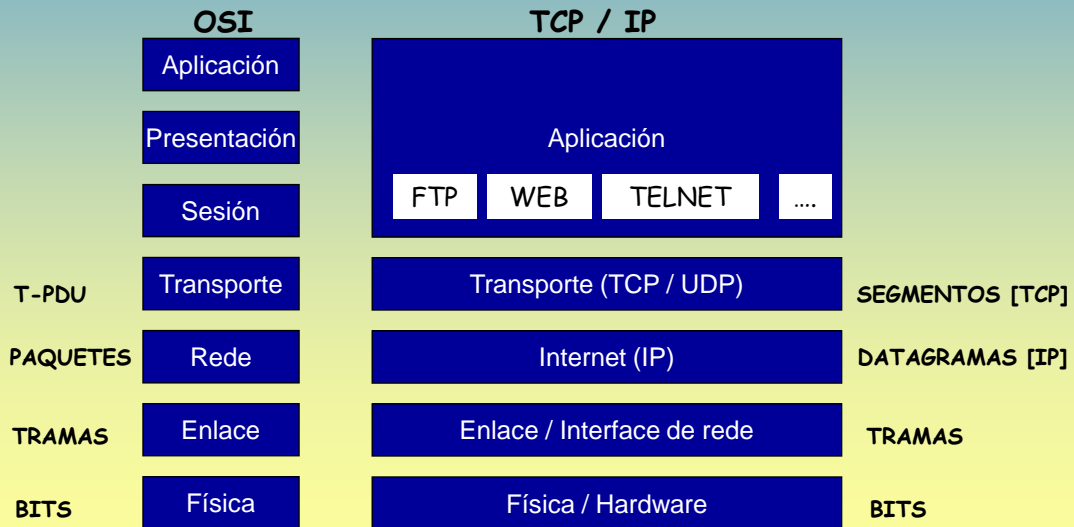
Interconexión de varias redes en estrela

Ten as vantaxes e inconvenientes anteriores



22

OSI – TCP/IP



Redes Área Local - OSI – TCP/IP

4.- Modelo de referencia OSI

☛ Dous amigos envíanse unha carta.

A imaxe que temos do proceso de envío é o seguinte.



A carta viaxa directamente dende o remitente ó destinatario



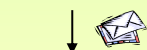
☛ A realidade.

A carta vai a través de diversos medios:

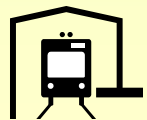
Oficinas de Correo
Estacións de tren, etc.

En cada un destes intermediarios engadiráselle información:

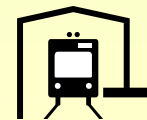
Certificada, (S/N)
Urxente (S/N), etc.



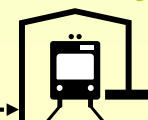
correos



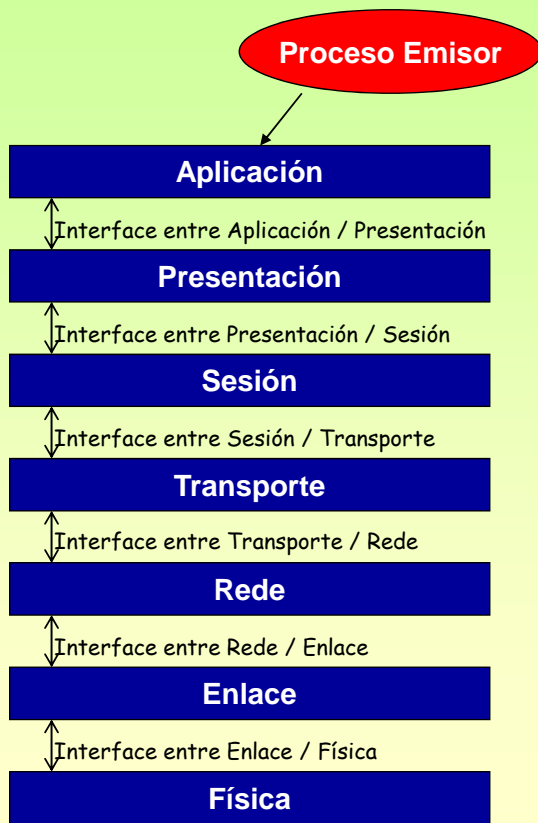
correos



correos



4. Modelo OSI de ISO (1984)



ISO: International Standard Organization (Organismo de estándares internacionais)

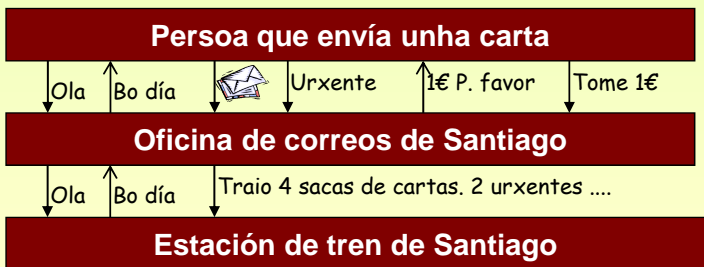
OSI: Open System Interconnection. (Interconexión de sistemas abiertos/heteroxéneos)

Arquitectura organizada en 7 capas/niveis
Cada unha con unha función clara e ben definida

INTERFACES

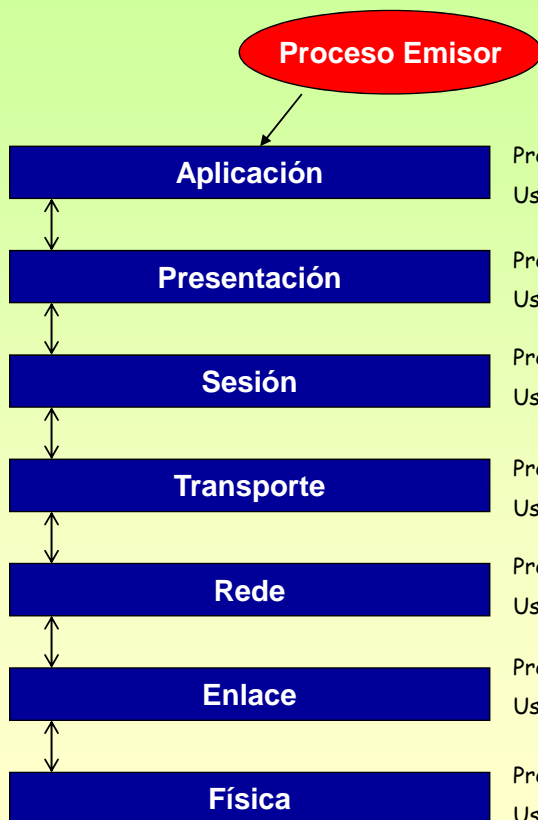
É o lugar polo que intercambian información dúas capas. Unha capa intercambia información coa súa superior/inferior inmediatas.

P. Ex.: Unha persoa en Santiago envía unha carta



A persoa non interactúa directamente coa estación

4.- Modelo de referencia OSI de ISO (1984)



SERVIZOS:

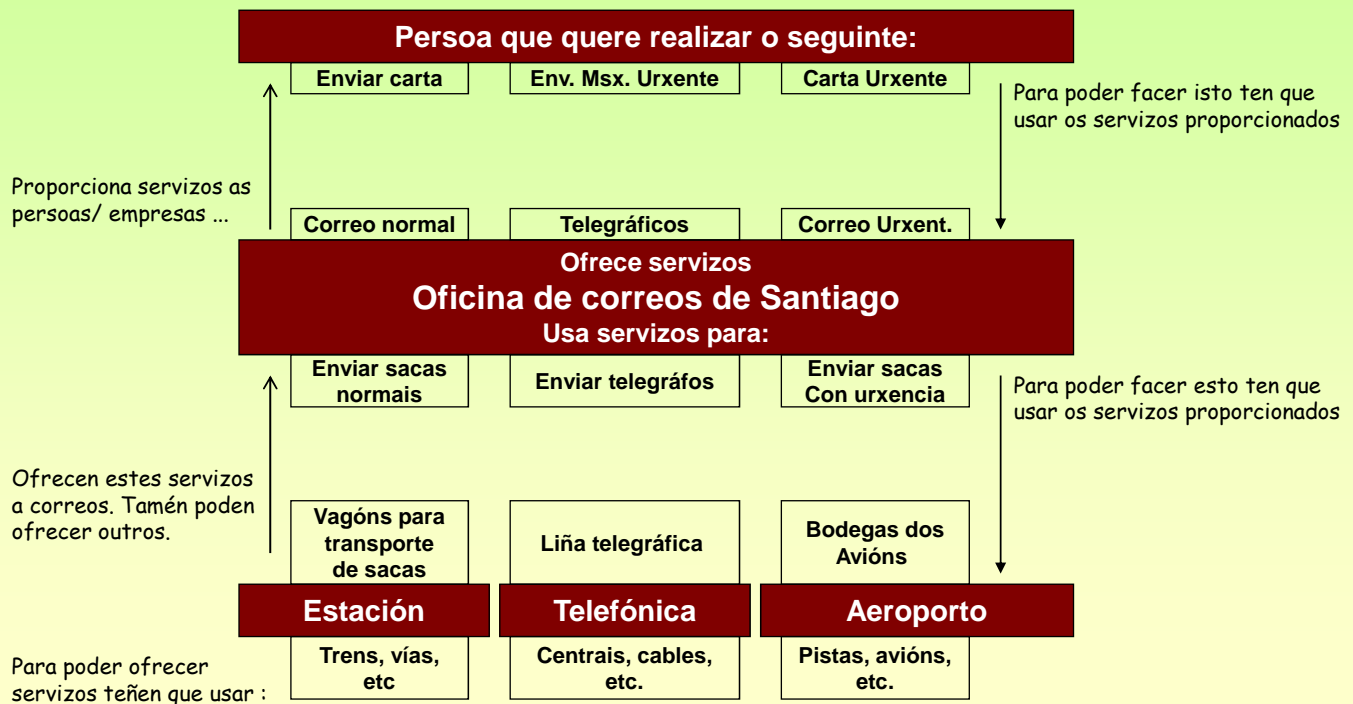
Para que unha capa poida levar a cabo as súas funcións usa os servizos que lle proporciona á capa inferior.

Aplicación	Presta servizos ó proceso emisor Usa servizos que ofrece presentación
Presentación	Presta servizos á capa Aplicación Usa servizos que ofrece sesión
Sesión	Presta servizos á capa Presentación Usa servizos que ofrece Transporte
Transporte	Presta ... Usa ...
Rede	Presta ... Usa ...
Enlace	Presta ... Usa ...
Física	Presta ... Usa os medios físicos...

4.- Modelo de referencia OSI de ISO (1984)

SERVIZOS - EJEMPLO

Unha persoa desexa enviar unha carta normal, outra urxente e unha mensaxe urxente.



27

4.- Modelo de referencia OSI de ISO (1984)

ENTIDADES

Os servizos que ofrece unha capa son en realidade ofertados por ENTIDADES desa capa. Cada capa ten un conxunto de entidades que son as que realizan e ofrecen os distintos servizos.

EJEMPLO

Nunha oficina de correo hai unha/s entidade/s que se encargan de correo normal, outras de xiros, outras de correo urxente...

Na realidade son as ENTIDADES as que ofrecen/usan servizos non toda a capa en si.

En informática imaxinar un ordenador que ten un servidor WEB e un servidor FTP, cada un deles é unha entidade/programa distinto. Non todo o ordenador é o servidor WEB, senón que dentro dese ordenador hai unha entidade/aplicación que realiza esa función.

SAP (Punto de acceso ó servizo)

As entidades ofrecen os seus servizos por un punto concreto, punto ó que se ten que dirixir a entidade da capa superior para poder usar ese servizo. En correos serían as xaneliñas (ventanillas).

Tipos de servizos que se poden ofertar

SERVIZO NON ORIENTADO Á CONEXIÓN:

Equivale ó **sistema postal**. Ó enviar varias cartas a un mesmo destino non se teñen garantías de que chegan todas nin na mesma orde en que saíron.

SERVIZO ORIENTADO Á CONEXIÓN:

Equivale ó **sistema Telefónico**. Para realizar unha comunicación:

- 1º Realízase unha chamada para establecer unha comunicación.
- 2º Realízase o intercambio de información. (A información recíbese na mesma orde na que se envía → imaxe TUBO)
- 3º Unha vez rematada a comunicación, libérase a conexión (cólgame ó teléfono)



28

4.- Modelo de referencia OSI de ISO (1984)

EXEMPLO DE ENTIDADES E SAP

Unha entidade da capa superior intercambiará información cunha entidade da capa inferior polo SAP



Puntos polos cales a Entidade usuario accede ós servizos que prestan as entidades de correos.

Un usuario non entra por dentro do mostrador e deposita el a súa carta onde desexe, senón que interactúa por unha xanela (SAP) coa entidade correspondente.

En síntese:

Unha capa ten **ENTIDADES** que realizan **funcións** e estas **ofrecen** os seus **servizos** ás entidades da capa superior polo **SAP**

Por outra banda, a oficina de correos intercambiará información coa Estación de Trens, Aeroporto, Telefónica, etc, polos SAPs que estes poñan a disposición da oficina de correos

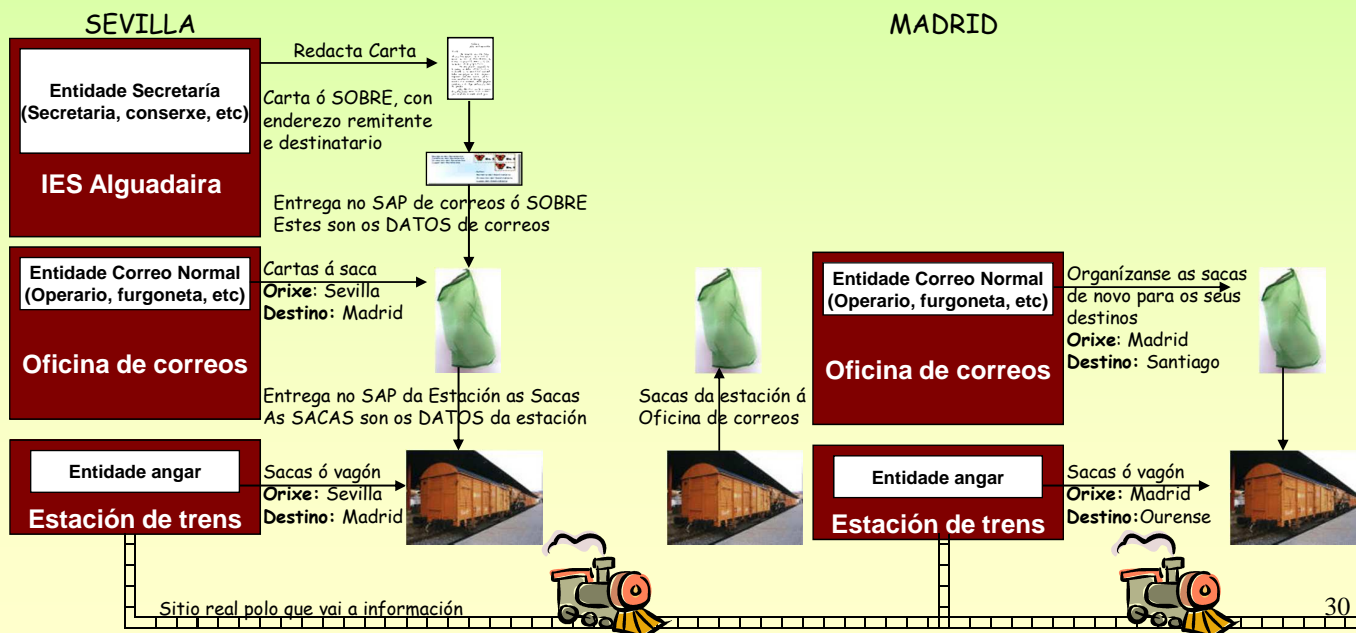
(No caso da estación e o aeroporto, podería ser a través dos angares, no caso de telefónica polo cable que e telégrafo que lles ten instalado na oficina).

4.- Modelo de referencia OSI de ISO (1984)

ENCAPSULACIÓN DA INFORMACIÓN

Un **REMITENTE / EMISOR** o único que desexa **transmitir/enviar** ó **DESTINATARIO / RECEPTOR** é unha **CARTA/MENSAXE** (entendida esta sen o sobre)

Pero a **CARTA** non pode viaxar pola rede de comunicación sen un **ENVOLTORIO/CABECEIRA** que lle permita a esta ser conducida ata o seu destino. Precísase un **SOBRE/CABECEIRA** no que transportar a carta.

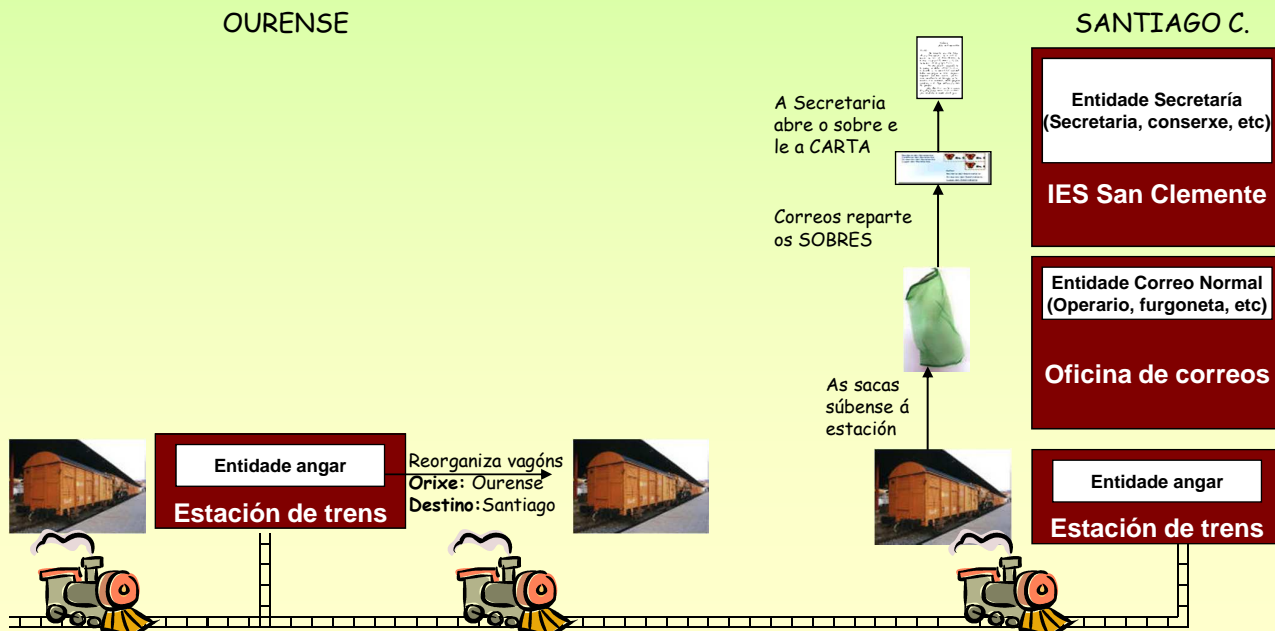


4.- Modelo de referencia OSI de ISO (1984)

ENCAPSULACIÓN DA INFORMACIÓN

Un **REMITENTE/EMISOR** o único que desexa **transmitir/enviar** co **DESTINATARIO/RECEPTOR** é unha **CARTA/MENSAXE** (entendida esta sen o sobre)

Pero a **CARTA** non pode viaxar pola rede de comunicación sen un **ENVOLTORIO/CABECEIRA** que lle permita a esta ser conducida ata o seu destino. Precísase un **SOBRE/CABECEIRA** no que transportar a carta.

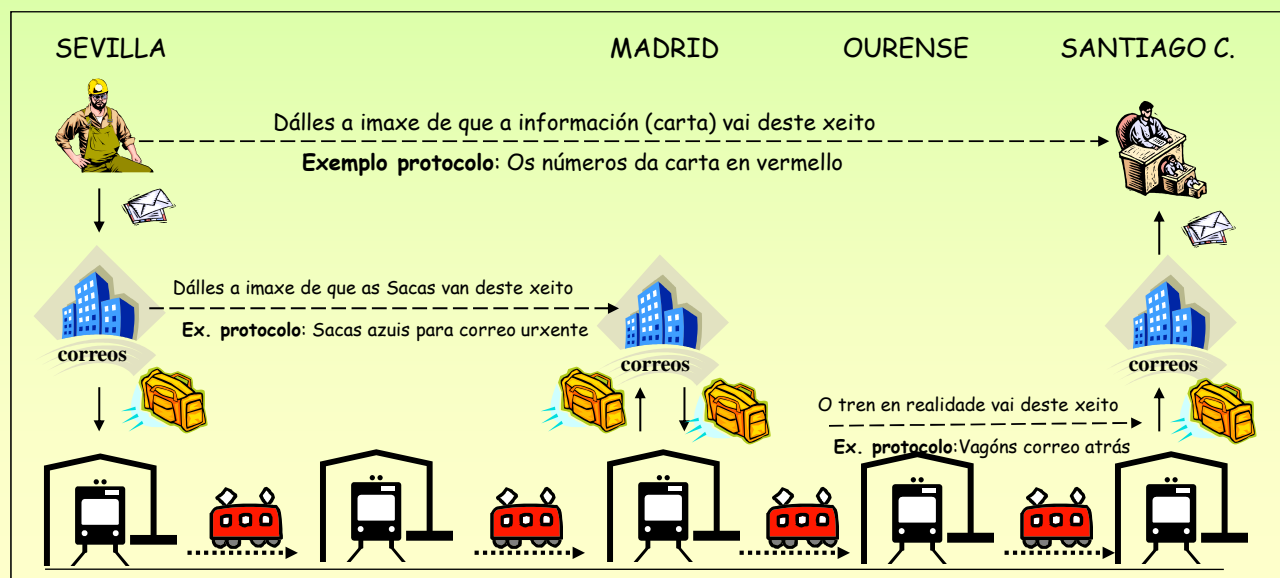


4.- Modelo de referencia OSI de ISO (1984)

SÍNTESE DO PROCESO DE TRANSMISIÓN, ENTIDADES PARES e PROTOCOLOS

Entidades PAR: son dúas entidades na mesma capa e en distinta máquina. (P.ex. Secretaría con Secretaría).

Protocolos: son as **normas/reglas** que establece cada **entidade par** para comunicarse entre elas.



Redes Área Local - OSI - TCP/IP

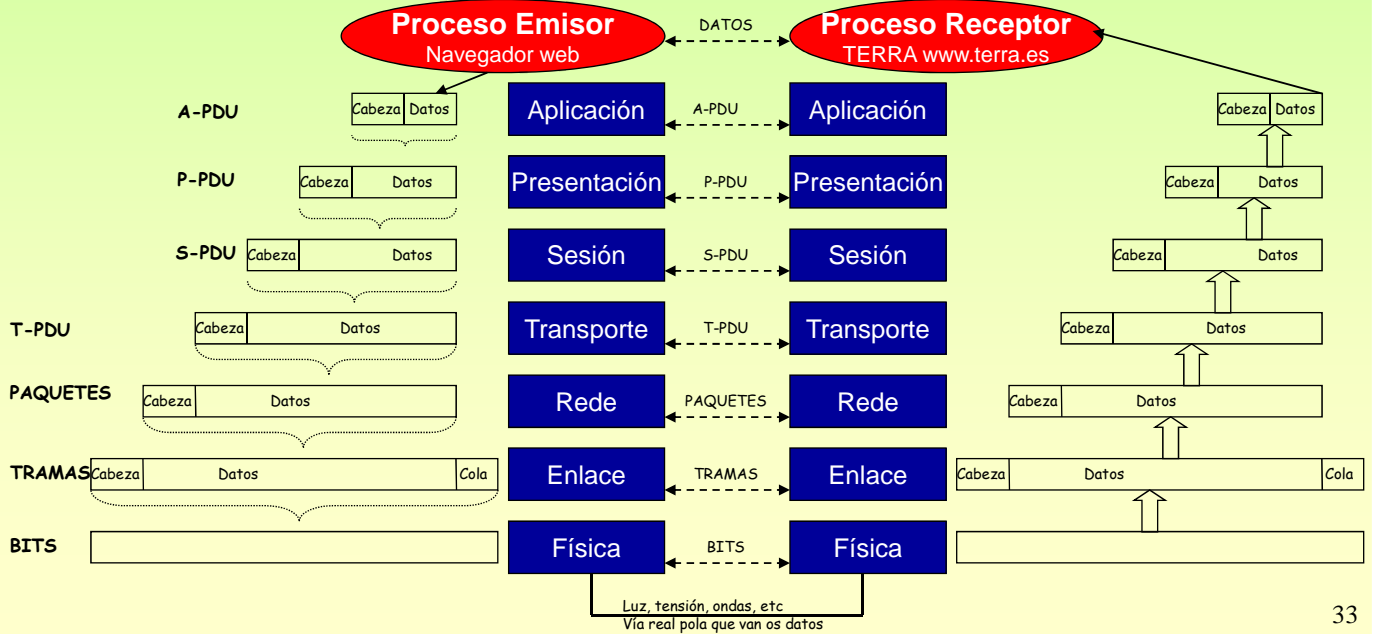
4.- Modelo de referencia OSI de ISO (1984)

INTERCAMBIO DE INFORMACIÓN EN OSI

LADO EMISOR: As entidades de cada capa reciben mensaxes das entidades da capa superior, engaden unha cabeceira e baixan a nova mensaxe á capa inferior.

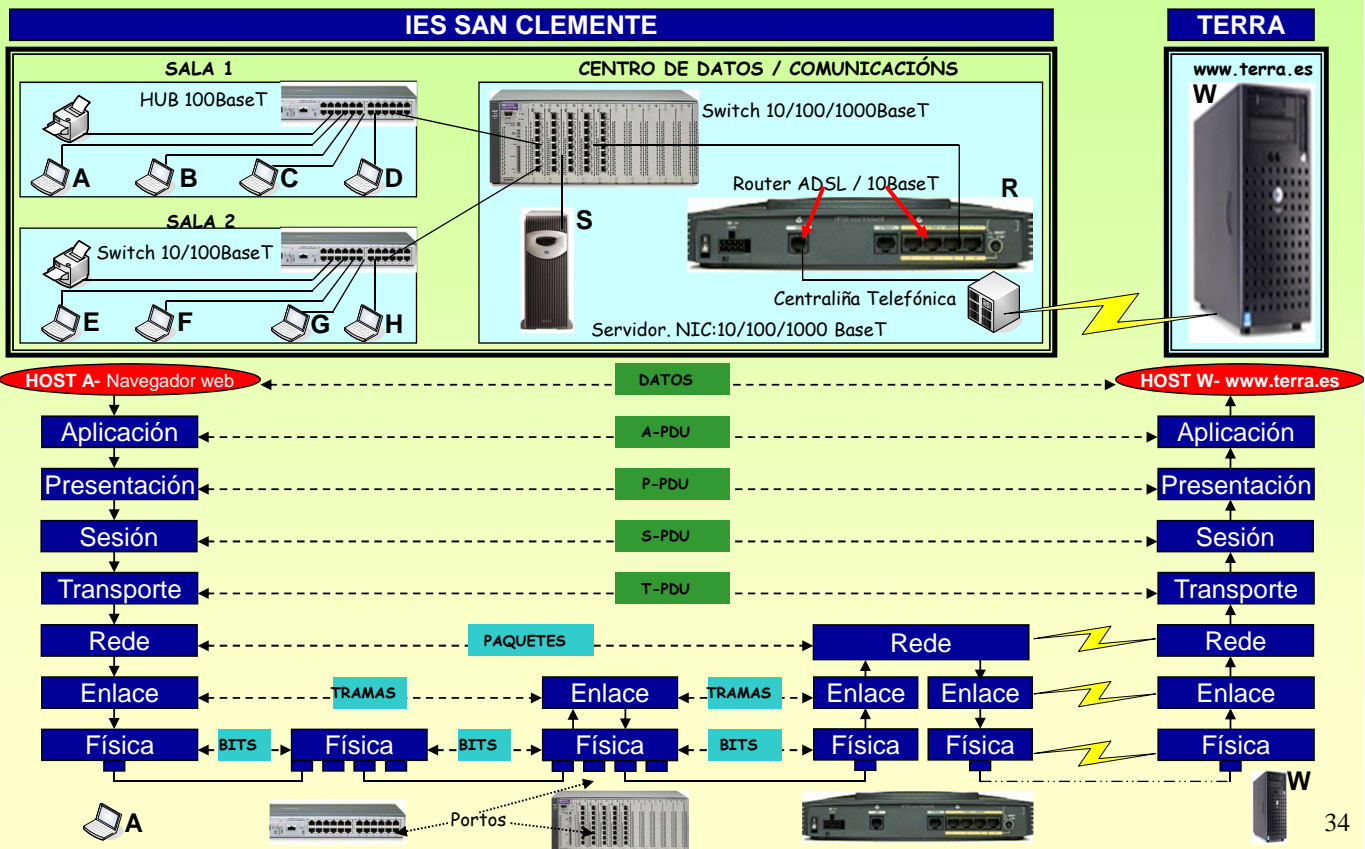
LADO RECEPTOR: As entidades de cada capa reciben das entidades da capa de abaixo as mensaxes, sacan a cabeceira e soben o campo de datos á capa superior.

PDU: (Unidade de datos do protocolo), é a mensaxe que intercambian as entidades pares.



Redes Área Local - OSI - TCP/IP

4.- Modelo de referencia OSI de ISO (1984)



4.- Modelo de referencia OSI de ISO (1984)

ALGUNHAS FUNCIONS DAS CAPAS / NIVEIS (Máis información na unidade de traballo 4)

Aplicación	<p>Constrúe e procesa A-PDUs. Neste nivel están as aplicacións como poderían ser o FTP, DNS, Servidor Web, Correo electrónico, etc</p>
Presentación	<p>Constrúe e procesa P-PDUs. Sintaxe e semántica (se unha máquina traballa en Complemento a 1 e outra en complemento a 2, haberá que traducir) Cifrado de datos (Encriptar/desencriptar a información que sae/chega a un host, P.ex. Chave simétrica, chave privada-pública) Compresión dos datos (Se se transmite un "que", no emisor podemos sacarlle o "u" e volverllo a poñer no receptor)</p>
Sesión	<p>Constrúe e procesa S-PDUs. Encárgase da xestión do diálogo entre dúas máquinas finais (Quen transmite primeiro, como nos pasamos a testemuña, etc)</p>
Transporte	<p>Constrúe e procesa T-PDUs. É o primeiro nivel extremo a extremo. (Para este nivel é como se non hai subrede, os protocolos son entre o emisor e receptor reais). Encárgase do control de fluxo entre hosts (Imaxinar un emisor real, que manda libros por correo cada día a un receptor real. O correo, a estación, etc, non son saturados, pero o receptor non ten tempo de ler tódolos libros, o receptor real está saturado)</p>
Rede	<p>Constrúe e procesa paquetes. Encamiña os paquetes. (Equivale a unha rotonda, xa que, ten sinais que indican que dirección coller para ir a un lugar). Interconexión de redes distintas (Pe: ADSL-Ethernet)(Unha rotonda tamén pode ser o nexo dunha autoestrada cunha estrada) Controla a congestión (Unha rotonda congestiónase se a suma de coches recibidos por tódalas liñas é maior que os que pode procesar)</p>
Enlace	<p>Constrúe e procesa tramas. Controla o fluxo (que un emisor non sature a receptor). Detección de erros, coa COLA. Emisor divide os datos entre un polinomio e o restoponse na cola. No receptor faise a mesma división e contrastase o resto resultante co que chegou na cola. Controla o acceso á canle: por loita (As estacións acceden cando queren), regulado (o acceso á canle faise de xeito ordenado)</p>
Física	<p>Encárgase da transmisión dos bits (luz, ondas, voltios) Define aspectos relacionados con aspectos mecánicos, procedimentais, (P.e. conector RJ 45, o seu formato, que cables se usan)</p>

35

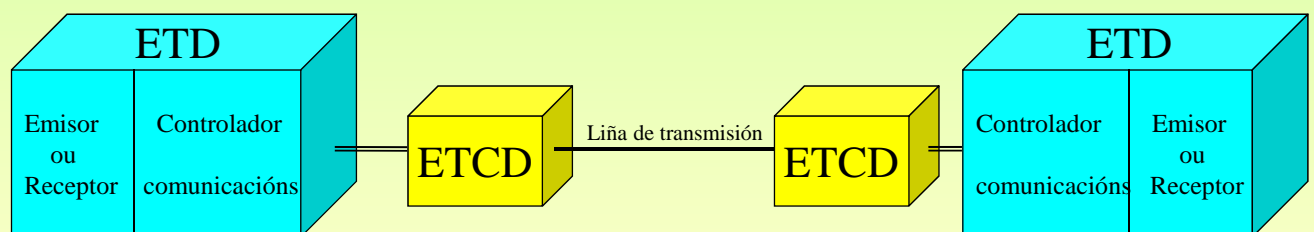
5.- Nivel físico

Función

Transmisión de bits ó longo da canle de comunicacións.

O seu deseño debe asegurar que cando se envía un bit con valor 1, este se reciba como un bit con valor 1 e non con valor 0.

Modelo de un sistema de transmisión de datos



ETD (Equipo terminal de datos)

Equipo fonte ou destino dos datos
Encargado de controlar as comunicacións

ETCD (Equipo terminal do circuíto de datos)

Transforman os sinais dos ETD en outros que conteñan a mesma información, e en ocasións información de control, para poder ser transmitidos por pola liña de transmisión

36

6.- Nivel de enlace

☞ Descripción

Trata de asegurar unha conexión libre de erros entre dous nodos adxacentes da mesma rede, isto é un ordenador con outro ordenador da LAN, un ordenador cunha impresora da LAN, un ordenador co Router da LAN, etc. Pero non un ordenador/impresora/etc con outro ordenador/impresora/etc separadas por un router.

Extremo emisor

Acepta os paquetes do nivel de rede e **troceaos** en tramas.
Constrúe os campos da trama.
Pasa as **tramas** ó nivel físico.

Extremo receptor

Compón a trama a partir dos bits que van subindo do nivel físico
Comprueba os erros
Se a trama é correcta **sube** a información ó nivel de rede.

☞ Subcapas

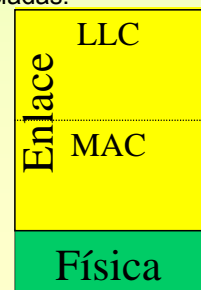
O nivel de enlace divídese en dúas subcapas con funcións claramente diferenciadas.

Subcapa LLC (Logic Link Control – Control de Enlace Lóxico)

Confección de tramas
Control de erros, ...

Subcapa MAC (Media Access Control – Control de Acceso ó Medio)

¿Cando está a canle libre?
Se está libre ¿Podo transmitir?



37

6.1- Subcapa LLC

☞ Funcións básicas

Confección da trama

Sincronización de trama

Determinar onde empeza e remata cada trama
Principio e conta
Principio e fin

Transparencia

Solucionar o problema: cando os datos do usuario conteñan un carácter semellante ó usado para determinar o comezo ou fin da trama, aquel non sexa entendido como tal.

Control de erros de transmisión

Determinar se a trama recibida ten ou non erros
Unidade de traballo 3

Control de fluxo e coordinación da comunicación

Determinar quen transmite dos dous interlocutores
Envío e espera
Ventá deslizante
Rexeite simple
Rexeite selectivo

Asentamentos en liñas bidireccionais

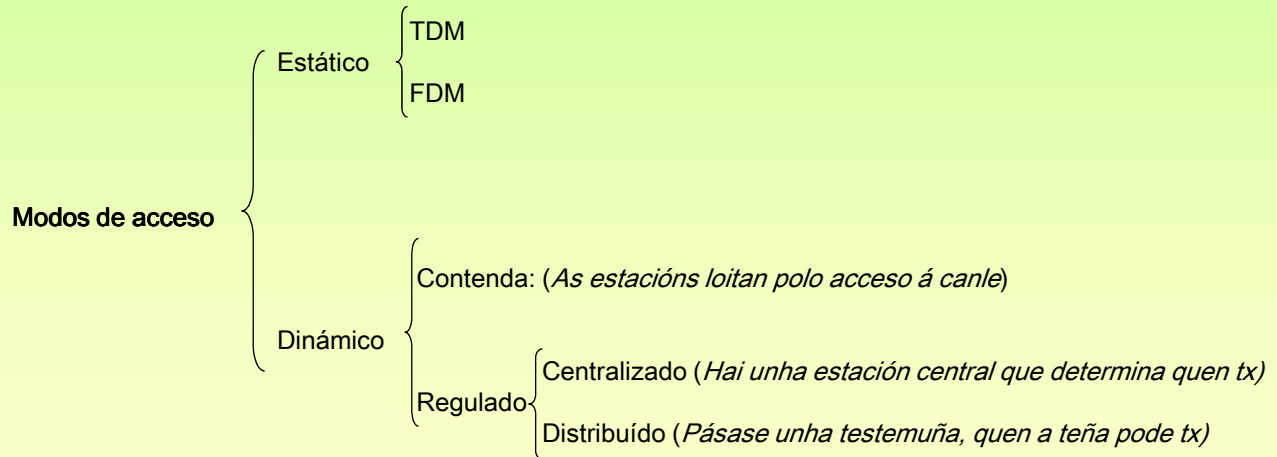
Os asentamentos van dentro dos mesmo datos (**piggy backing**).

38

6.2- Subcapa MAC

☞ Funcións básicas

Como se vai acceder ó medio físico



6.2- Subcapa MAC

☞ Acceso dinámico: Contenda

Varias estacións compiten pola canle.

Colisión: cando dúas tramas coinciden simultaneamente na mesma canle.
As tramas que interviron na colisión terán que ser retransmitidas.

Métodos para acceso por contenda

- Aloha puro
- Aloha rañurado
- CSMA / LBT
- CSMA – CD

☞ Aloha puro

Deixar ás estacións transmitir no momento en que teñan a información.

Pouco eficaz, pois o índice de colisións será moi elevado.

Unha mesma trama será rtx n veces e causará n-1 colisións.

Cando se producen colisións a estación emisora espera un tempo aleatorio antes de rtx.

☞ Aloha rañurado

O tempo divídese en slots (rañuras)

Cando unha estación teña datos para tx debe esperar ó comezo dun novo slot.

Reducense as colisións, pois se se está transmitindo unha trama e unha estación ten datos, esta debe esperar o comezo do novo slot.

As colisións produciranse ó comezo de cada slot.

O slot debe ser o suficientemente grande como para que se poida tx unha trama de extremo a extremo

6.2- Subcapa MAC

☞ **CSMA (Carrier Sense Multiple Access – Acceso Multiple con Detección de Portadora)**

☞ **LBT (Listen Before Talk – escoitar Antes de Falar)**

Cando unha estación desexa transmitir debe escoitar a canle para ver se está libre ou non

CSMA 1-persistente

Cando unha estación desexa tx, escoita a canle. Se está:

Ocupado: espera ata que estea libre e transmite a trama

Libre: transmite a súa trama

CSMA non-persistente

Cando unha estación desexa tx, escoita a canle. Se está:

Ocupado: reposa un tempo aleatorio antes de voltar a escoitar a canle

Libre: transmite a súa trama

CSMA p-persistente

Cando unha estación desexa tx, escoita a canle. Se está:

Ocupado: espera ata que estea libre.

Libre: transmite a súa trama cunha probabilidade p.

☞ **CSMA / CD (CSMA / Collision Detected – CSMA con detección de colisión)**

T: tempo que lle leva a unha trama ir de extremo a extremo.

Cando unha estación detecta unha colisión debe introducir un ruído na liña para que as demais se enteren.

Cando unha estación tx, debe esperar como máximo 2T para saber se a súa trama colisionou ou non. Pois se a colisión se produxo nun dos extremos e a estación está no outro, o aviso tardará 2T en chegar

41

7.- IEEE 802.x

☞ **Introducción**

A maioría das redes LAN (RAL) seguen os **estándares IEEE* 802**** para acceder ó medio compartido.

Nas LANs a información difúndese entre tódalas estacións, o que implica inseguridade na información

As especificacións 802.x definen tanto subcapa LLC (802.2) como a subcapa MAC e física (802.3, 802.4, 802.5, 802.6, 802.11, 802.12, FDDI)

E X E M P L O

LLC	IEEE 802.2			
MAC	IEEE	CSMA / CD 1-persistente	IEEE	Anel con paso de Testemuña
Físico	802.3	Coax: 10 BASE 2 UTP: 10/100 BASE T STP: 100 BASE T Fibra: 10/100 BASE F	802.5	STP: 4/16 Mbps UTP: 4 Mbps
	Ethernet		Token Ring	

*IEEE = Institute for Electrical and Electronics Engineers

**802.x: Comités dentro do IEEE que desenvolveron os estándares uso de medios compartidos (802.3, 802.4,...)

7.1.- Trama do IEEE 802.3

☞ Está baseado en CSMA / CD 1-persistente.

☞ A **trama MAC** está orientada a carácter (Principio e Conta). Esta ten o seguinte formato

Preámbulo	Inicio	Dir Destino	Dir Orixe	Lonxitude	Datos	Recheo	CRC
Bytes: 7	1	6	6	2	0 - 1500	0 – 46	4

Preámbulo: son 7 bytes: 10101010 Para que receptor e transmisor se sincronicen

Inicio: 1 byte: co patrón 10101011 Para indicar que comenza a trama

Dir Destino: é a dirección física (MAC) do destinatario da trama. A dirección física é única no mundo para cada adaptador (tarxeta).

Dir orixe: é a dirección física do transmisor. Hoxe en día nos dous campos de dirección úsanse 6 bytes e non 2. Estes bytes están expresados en Hexadecimal, cada 4 bits

Lonxitude: estes 2 bytes indican cantos bytes van no campo de datos ou de información

Datos: o campo de datos transporta a mensaxe do nivel superior. De 0 a 1500 bytes

Recheo: Unha trama ethernet debe ter como mínimo 64 bytes, se o campo de datos ten menos de 46 bytes, débese usar o campo de recheo para completar eses 64 bytes.

CRC: Código de redundancia cíclica

43

7.1.- Trama do IEEE 802.3

☞ **O ENDEREZO MAC: (Media Access Control address)**

☞ Definición informal: Sirve para identificara un compoñente hardware susceptible de ser conectado a unha rede.

☞ Tarxetas de rede.

☞ Periféricos (Impresoras, escáner, cámara IP, etc.).

☞ Electrodomésticos que se poidan conectar a unha LAN.

☞ Robots.

☞ Móviles, IPADs, PDAs, etc.

☞ Está composto por 48 bits (6 bytes), exprésase en formato hexadecimal: **B8-AC-6F-2F-84-0D**

☞ 24 primeiros bits (3 primeiros bytes) identifican ao **fabricante** do compoñente hardware.

☞ 24 últimos bits (3 últimos bytes) úsaos o fabricante para identificar cada un dos **dispositivos** que fábrica, de xeito que, cada un dos dispositivos vai ter un **endereço MAC único no mundo**.

☞ Resumo: cada endereço MAC, por exemplo **B8-AC-6F-2F-84-0D** ten 2 partes:

☞ **B8-AC-6F:** fabricante INTEL

☞ **2F-84-0D:** número que Intell lle deu a unha tarxeta de rede. Este número non se volverá a usar.

☞ Comandos para coñecer a MAC:

☞ Windows: **ipconfig /all** ou **getmac**

☞ Linux: **ifconfig**

44

7.2.- Capa física do IEEE 802.3

☞ O comité 802.3 foi o que definiu máis configuracións físicas alternativas.

- ❑ Ventaxa: Adaptarse as novas innovacións tecnolóxicas
- ❑ Inconvinte: Existencia de grande variedade de opcións
- ❑ Esta flexibilidade non implica que as distintas opcións non poidan estar integradas nun mesmo sistema

☞ O comité 802.3 desenvolveu unha notación concisa para distinguir as diversas opcións:

<Mbps> <senalización> <máxima lonxitude do segmento en hectómetros ou tipo de cable se non é coaxial>

EXEMPLO

10BASE5	Segmentos de 500m de cable coaxial a 10 Mbps. Codificación Banda Base
10BASET	Cable de pares Telefónico (T), codificación en Banda Base a 10 Mbps
100BASETX	Cable de pares Telefónico (T), codificación en Banda Base a 100 Mbps
10ANCHA36	Segmentos de 3600m de cable coaxial a 10 Mbps. Codificación Banda Ancha
100BASEF	Cable de Fibra óptica (F), codificación en Banda Base a 100 Mbps

45

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

☞ O comité 802.3 desenvolveu as seguintes alternativas a 10 Mbps.

10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F

NOTAR que a **T** significa par telefónico (STP,UTP,FTP) e que a **F** indica Fibra óptica.

Ademáis destas alternativas existen outras a 100 Mbps, combinación de ambas e a 1000 Mbps

46

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE2

10BASE-T

10ANCHA36

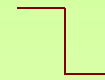
10BASE-F

☞ É a especificación do medio orixinal de 802.3

☞ Usa un cable coaxial grueso de 50 Ω

☞ Usa sinalización Manchester: +0,85 V

-0,85 V



☞ A lonxitude máxima de segmento é de 500 m.

☞ A lonxitude da rede pódese ampliar usando **REPETIDORES**

Un repetidor é un elemento de interconexión que ó único que fai e recibir o sinal por un lado e poñelo polo outro, pero amplificandoo. Non entende o senso da información que por el está pasando, para el todo son sinais eléctricos

Un repetidor é transparente a nivel MAC, é como un cable máis

☞ O número máximo de repetidores son 4.

☞ Lonxitude máxima do medio é de 2,5 Km (5 segmentos de 500m)

☞ As conexións fanse usando **Derivacións Vampiro** (Transceivir, Transceptor) para o cable e **conector AUI** para a tarxeta

☞ O número máximo de nodos por segmento é de 100

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

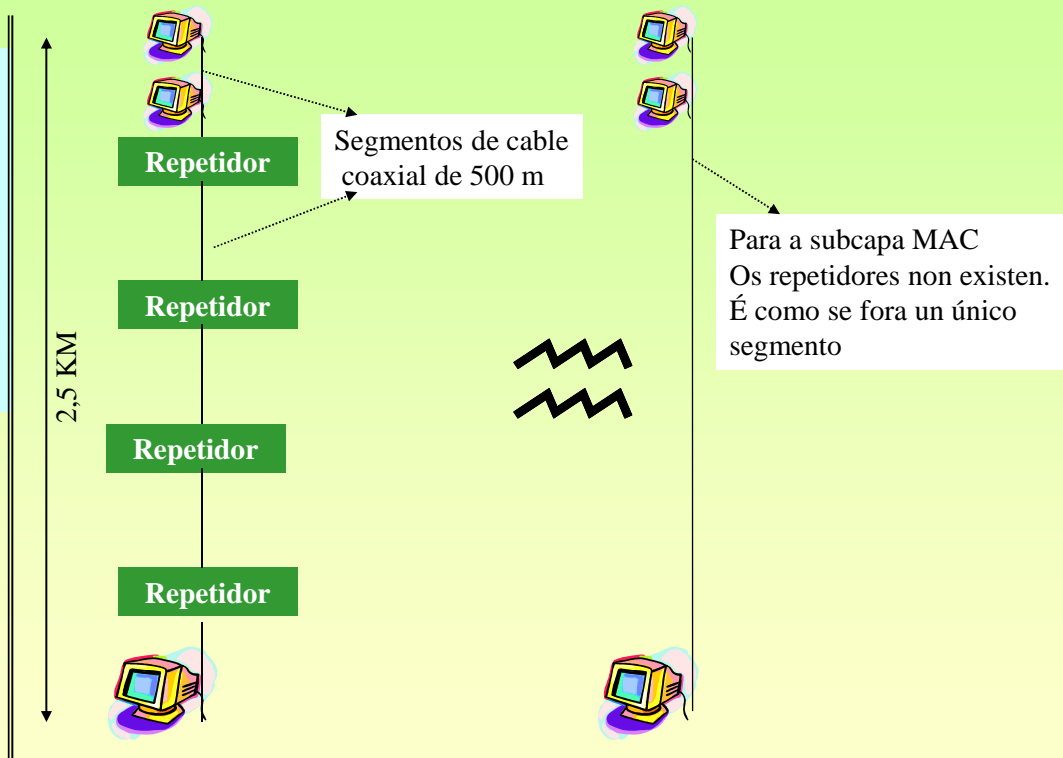
10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F



7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

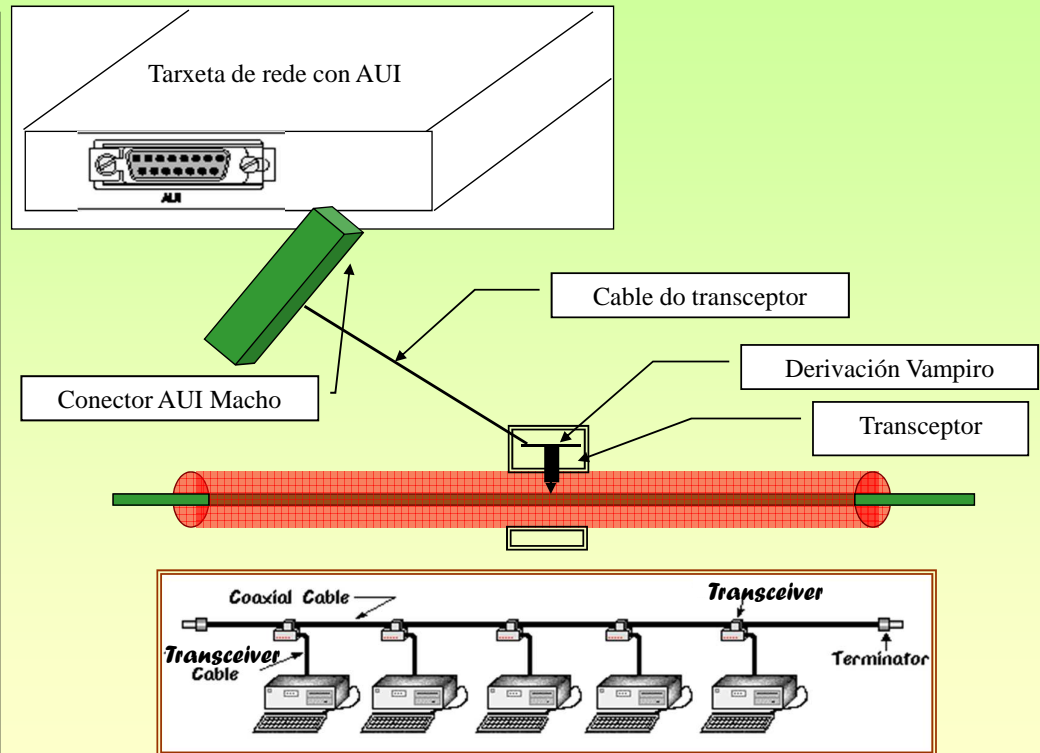
10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F



49

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F

☞ **Transceptor:** Contén a electrónica que detecta a **portadora** e as **colisións**. Ó detectar unha colisión pon unha sinal non válida para que os demais transceptores tamén se enteren.

Suxétase firmemente ó redor do cable

☞ **Cable do:** Une o transceptor á NIC (A Través do conector AUI)
Transceptor Pode ter ata 50m.

Conten 5 pares illados (10 fíos)

2 pares, un para Transmitir e outro para Recibir

2 pares, un transmite e outro recibe sinais de control

1 par, para que a NIC dea corrente ó transceptor

☞ **Tarxeta de rede:** Transmite e recibe tramas (marcos) ó/do transceptor

☞ **Terminador ou:** Conéctanse nos extremos do cable para
resistencia absorber o sinal eléctrico

50

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F

- ☞ Sistema menos custoso que 10BASE5
- ☞ Usa un cable **coaxial fino** de 50 Ω , que é máis barato que o grueso
- ☞ Posto que 10BASE5 e 10BASE2 presentan a mesma velocidade pódense intercalar segmentos de coaxial fino con coaxial grueso.
Para iso úsase un repetidor que se axusta a 10BASE2 por un extremo e a 10BASE5 polo outro.
- ☞ O resto das características son exactamente iguais a 10BASE5, salvo en:
 - ☞ As conexións fanse usando **Conectores BNC**
 - ☞ O número máximo de nodos por segmento é de 30
 - ☞ A lonxitude máxima de segmento é de 200m

51

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

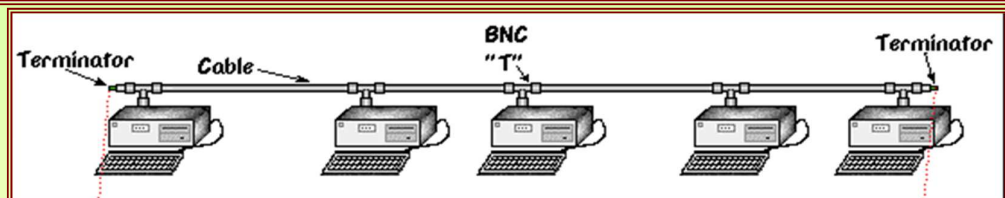
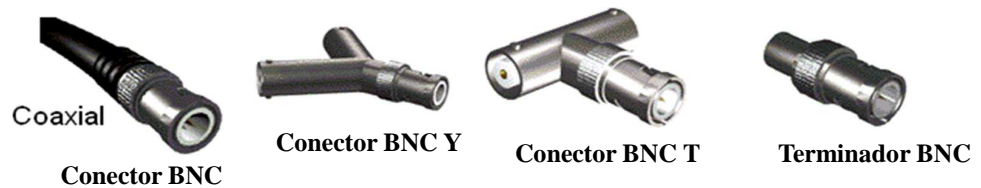
10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F



52

Redes Área Local - OSI – TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F

☞ **Conectores:** Cada trozo de cable coaxial termina nun conector BNC.

☞ Se se desexa unir varios segmentos débense usar os conectores BNC T ou Y .

☞ Por exemplo se desexamos unir un segmento que termina nun conector BNC a outro segmento que termina noutro conector BNC inserimos un conector T entre os dous e xa estarían unidos como se fora un único segmento.

☞ O outro extremo do conector T poderíase usar para unirlo ó conector BNC do adaptador de rede

☞ **Tarxeta de rede:** Transmite e recibe tramas (marcos). As funcións que fai o transceptor en 10BASE5 están implantadas en chips da propia tarxeta.

☞ **Terminador ou resistencia BNC :** Conéctanse nos extremos do cable para absorber o sinal eléctrico. Precísase un conector BNC T entre o segmento de cable e a resistencia.

53

Redes Área Local - OSI – TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

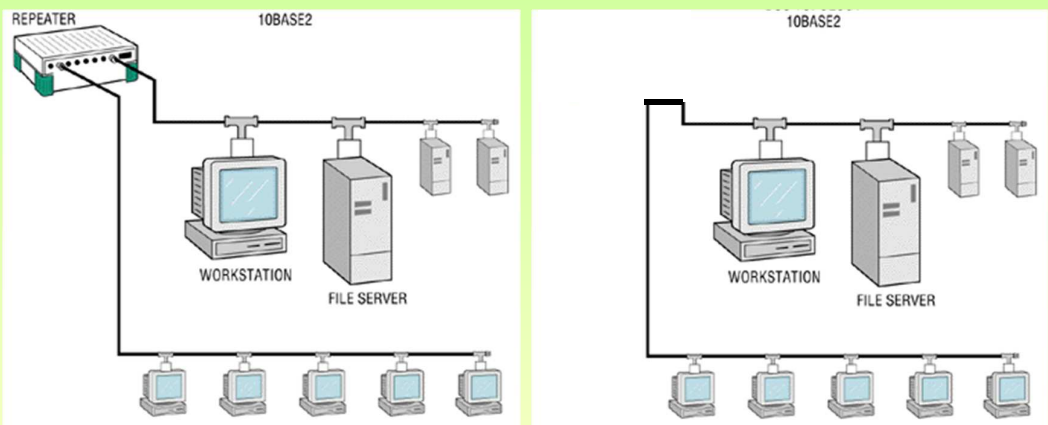
10BASE2

10BASE-T

10ANCHA36

10BASE-F

☞ A Continuación móstrase unha configuración 10 BASE 2 cun repetidor



☞ Para as estacións, en concreto para a subcapa MAC, é como se o repetidor non existira.

☞ Se o cable está estropeado, un conector funcionado mal, etc. A rede non funcionará, pois ó estar dividido o cable en dous trozos bos, estes non terían unha resistencia a cada extremo.

54

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASET

10ANCHA36

10BASE-F

☞ Topoloxía en estrela usando par telefónico

☞ Varias estacións están conectadas a un punto central, denominado:
REPETIDOR MULTIPORTO

HUB (lido /ghab/ non /jub/ nin /ub/)

CONCENTRADOR

☞ O hub recibe a información por un **porto**, amplifica o sinal e retransmíteo por tódolos demais portos.

☞ As estacións conéctanse ó hub mediante enlaces punto a punto.

A lonxitude dos enlaces é de 100m para cable UTP e 500m para fibra óptica

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

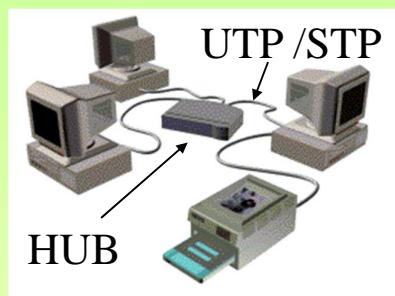
10BASE5

10BASE-2

10BASET

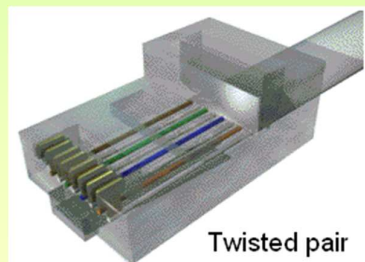
10ANCHA36

10BASE-F



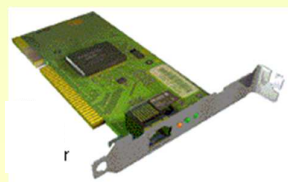
☞ Un Hub é un elemento do nivel físico que serve para conectar ordenadores.

☞ Úsase cable de 4 pares, 8 fios, para unir cada ordenador ó hub. (UTP, STP)



☞ Úsanse conectores RJ45 para realizar as conexións entre o cable e os elementos que interconecta (hub ou ordenador).

☞ Co cal cada trozo de cable ten 2 conectores RJ45 Machos



☞ As tarxetas son similares ás que teñen conectores BNC só que teñen un conector RJ45 femia

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

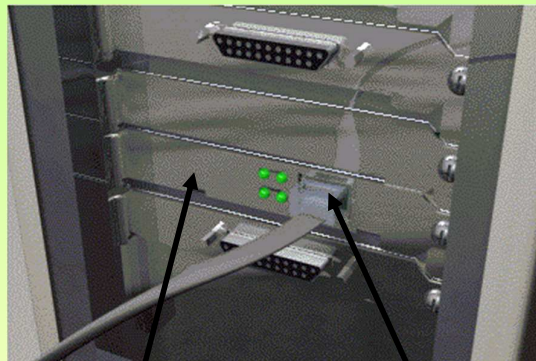
10BASE5

10BASE-2

10BASET

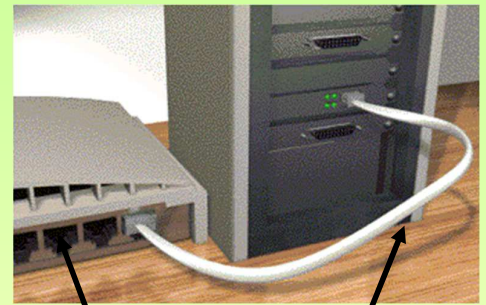
10ANCHA36

10BASE-F



Adaptador de rede

Conector RJ 45 Macho



Portos do hub

Cable UTP /STP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASET

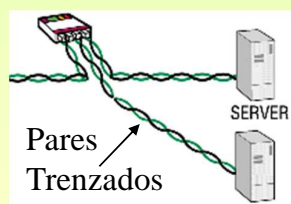
10ANCHA36

10BASE-F

CABLEADO UTP/STP

☞ O cable UTP/STP consta de 4 pares de fios trenzados, cada par de fios está trenzado sobre si mesmo.

☞ Canto máis trenzado estean os fios maior inmunidade ó ruído, pero pola contra menor lonxitude de cableado pois ó ter maior lonxitude de cable prodúcese maior atenuación



☞ Existen varias categorías de cable UTP, en función desta pódese transmitir a determinadas velocidades.

Categoría	Velocidade máxima de transmisión
3	16 Mbps
4	20 Mbps
5	100 Mbps
5e	1000 Mbps
6	1000 Mbps

Redes Área Local - OSI – TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASET

10ANCHA36

10BASE-F

CABLEADO

☞ A tarxeta de rede transmite e recibe a información polo conector RJ-45 femia. Os pins que se usan para tal fin son:



PIN/Patilla	Función
1	Tx
2	Tx
3	Rx
4	Non se usa
5	Non se usa
6	Rx
7	Non se usa
8	Non se usa



Cable Marrón trenzado con cable Blanco-Marrón

☞ Os cableciños do cable teñen unha cor que os identifica. Os pares que van trenzados son os de Cor con Branco-Cor:

Verde	trenzado con	Branco-Verde
Laranxa	trenzado con	Branco-Laranxa
Azul	trenzado con	Branco-Azul
Marrón	trenzado con	Branco-Marrón

59

Redes Área Local - OSI – TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASET

10ANCHA36

10BASE-F

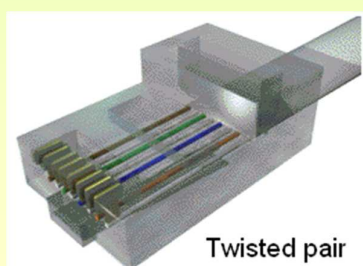
CABLEADO

☞ Polo que se veu antes os pins 1 e 2 transmiten e os 3 e 6 reciben.

☞ Se atendemos as consideracións de que os pares trenzados son máis inmunes ás interferencias, temos que:

☞ Se no pin 1 do conector RJ-45 macho poñemos un cabliño con cor Marrón no pin 2 teremos que poñer o cabliño con cor Branco-Marrón

☞ Existen dúas combinacións convencionais de cables. Non ten explicación técnica senón por convenio.



Twisted pair

PIN/Patilla	Código A	Código B
1	BV	BL
2	V	L
3	BL	BV
4	A	A
5	BA	BA
	L	V
7	BM	BM
8	M	M

60

Redes Área Local - OSI – TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASET

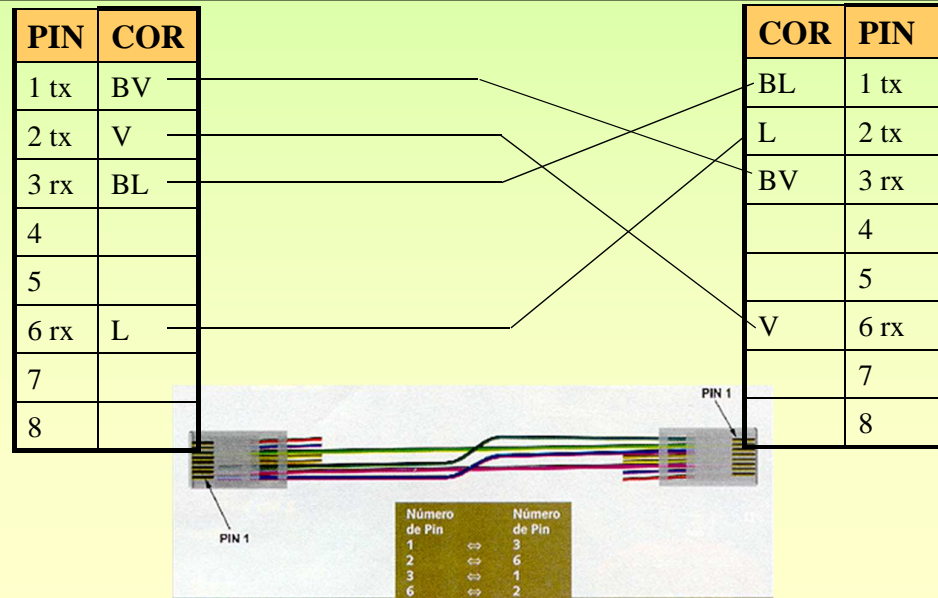
10ANCHA36

10BASE-F

INTERCONEXIÓN DE SÓ DOUS ORDENADORES

☞ Inserir unha tarxeta con conector RJ-45 en cada ordenador

☞ Coller un trozo de cable UTP e poñerlle dous conectores RJ-45 en cada extremo, da seguinte forma (cruzada):



61

Redes Área Local - OSI – TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

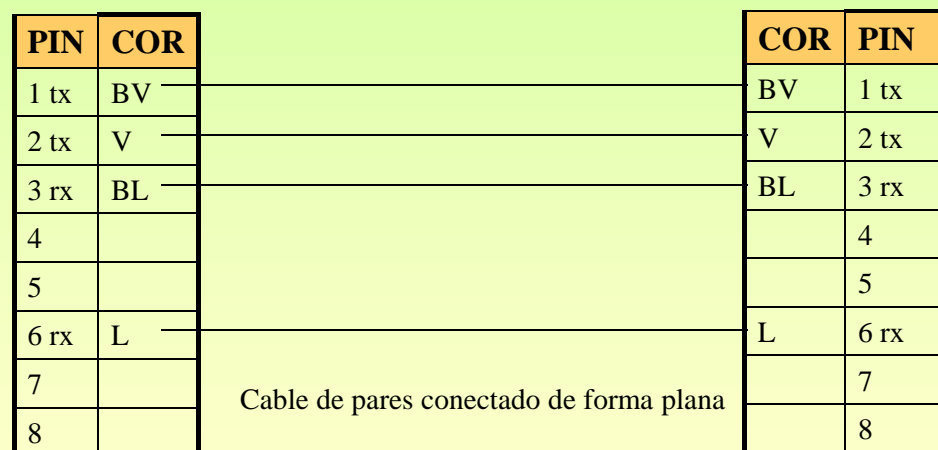
10BASET

10ANCHA36

10BASE-F

INTERCONEXIÓN DE ORDENADOR a HUB

☞ O hub o que recibe polos pins 1 e 2 dun porto trasmitelo polos pins 3 e 6 dos demais portos, co cal xa fai el o cruce. O cable é plano



Cable de pares conectado de forma plana

Conector RJ 45 ó ordenador

Conector RJ 45 ó hub

62

Redes Área Local - OSI - TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

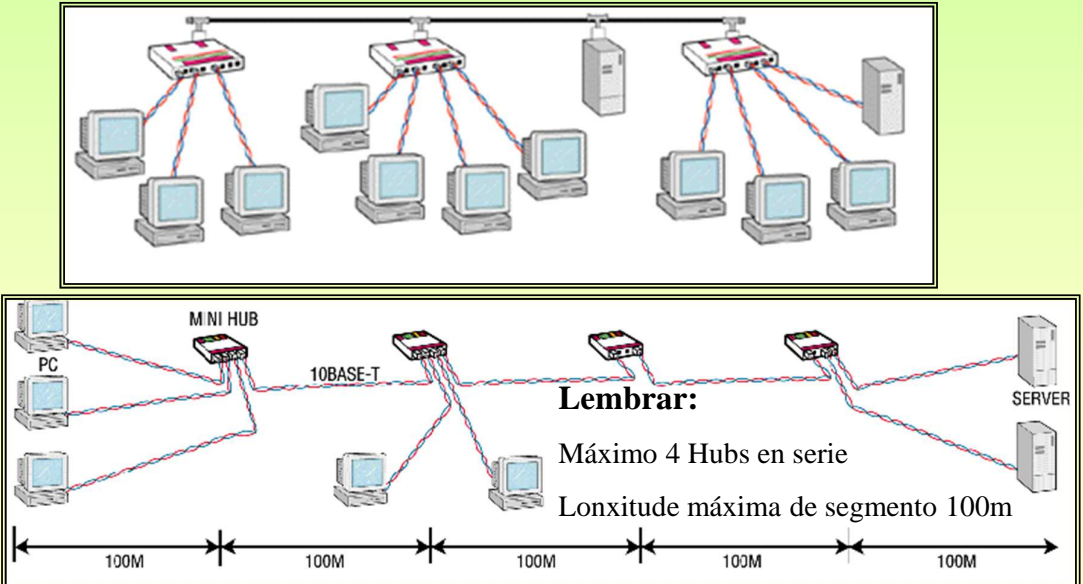
10BASET

10ANCHA36

10BASE-F

☞ As especificacións sobre hubs e interconexións destes veranse usando o manual do hub TP4COMBO de 3COM

☞ Por último, indicar que se poden ter unha mezcla das dúas topoloxías 10BASE2/5 con 10BASE - T



63

Redes Área Local - OSI - TCP/IP

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASET

10ANCHA36

10BASE-F

☞ É a única especificación para Banda Ancha

☞ Usa codificación PSK

☞ Usa cable coaxial CATV (Cable de TV) de 75 Ohmios

☞ A distancia máxima entre extremos é de 3.600 m

64

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

10BASE5

10BASE-2

10BASE-T

10ANCHA36

10BASEF

☞ É unha especificación similar a 10BASET que usa **Fibra Óptica**

7.2.1.- Capa física de IEEE 802.3 a 10 Mbps (ETHERNET)

Síntese das alternativas da capa física IEEE 802.3 a 10 Mbps

	10BASE5	10BASE2	10BASE T	10ANCHA36	10BASEFP
Medios de transmisión	Coax grueso (50Ω)	Coax fino (50Ω)	UTP /STP/FTP	Coax (75Ω)	Par de fibra óptica de 850 mm
Técnica de sinalización	Banda Base (Manchester)	Banda Base (Manchester)	Banda Base (Manchester)	Banda Ancha (PSK)	Manchester (si/non)
Topoloxía	Bus	Bus	Estrela / Árbore	Bus/árbore	Estrela / Árbore
Lonxitude máxima de segmento (m)	500	185	100	3.600	500
Nodos / segmento	100	30	-	-	33
Diámetro do cable (mm)	10	5	0,4-0,6	0,4-1	66,5/125 μm

7.2.2.- Capa física de IEEE 802.3 a 100 Mbps (FAST - ETHERNET)

Especificacións para LANs a alta velocidade a baixo custe e compatibles con Ethernet
 A designación global para estas LANs é de 100 BASE T, existindo diversas alternativas
 Notar que o nivel e trama MAC son iguais á de Ethernet

	100 BASE TX	100 BASE FX	100 BASE T4
Medio de transmisión	2 pares STP 2 pares UTP cat 5	2 fibras ópticas	4 pares UTP de Cat 3,4,5
Técnica de sinalización	4B 5B-NRZI	4B 5B-NRZI	8B6T-NRZ
Tasa de Datos	100 Mbps	100 Mbps	100 Mbps
Loxitude máxima de segmento	100 m	100 m	100 m
Expansión da rede	200 m	400 m	200 m

100 BASE T4, úsase para aproveitar as instalacións de cables de categoría 3 que existen nas instalacións para usos telefónicos.

Úsanse os 4 pares do cable, 3 pares para recibir e 3 para transmitir. As transmisións serán Half-Dúplex. Cada par tx a 33 Mbps.

Cando un NIC 100 BASE T4 ten que tx, este divide a trama en tres trozos e transmite cada trozo por cada un dos 3 pares

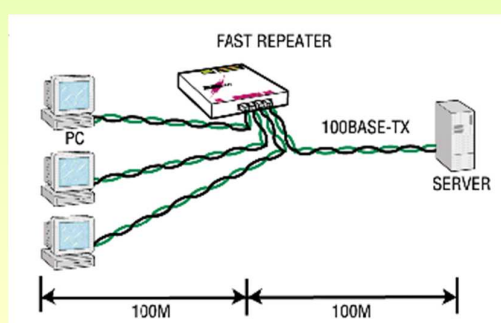
7.3.- Sistemas duales

Son aqueles que poden ir tanto a 10 Mbps como a 100 Mbps

Podense facer combinacións de ambos sistemas

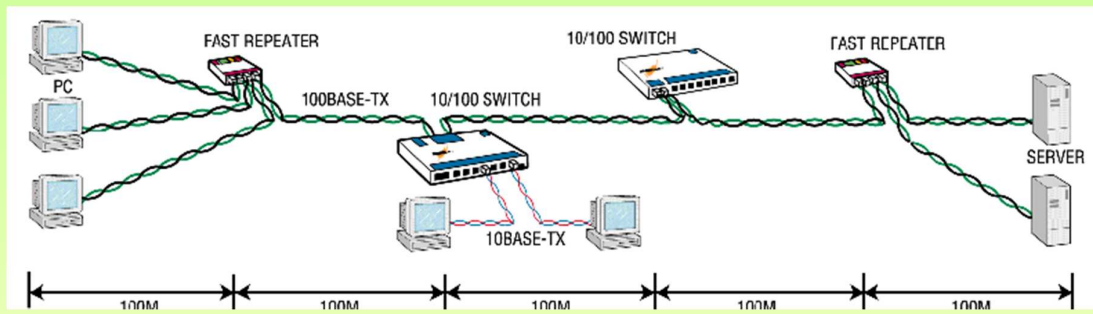
Un elemento dual tenta de ir sempre á máxima velocidade adaptándose ó que hai no outro extremo do cable.

Por exemplo un NIC 10/100 Base T conectado a un hub 10 BASE T iría a 10 Mbps, mentres que se está conectado a un hub a 100 BASE T ese mesmo NIC transmitiría a 100 Mbps.



Ollo que os sistemas a 100 Mbps so permiten 2 segmentos de 100 m

7.4.- Sistemas duales



7.5- Capa física de IEEE 802.3z a 1000 Mbps (Gigabit - Ethernet)

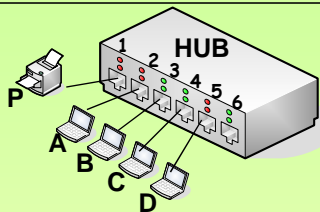
Especificación para LANs a 1000 Mbps

Notar que o funcionamento e trama son semellantes ós de Ethernet coa introducción de algunhas modificacións para as transmisións Half-Duplex

	1000 BASE SX	1000 BASE LX	1000 BASE T
Medio de transmisión	2 Fibras multimodo	2 Fibras multimodo	UTP Cat 5, 5e, 6
Técnica de sinalización	8B / 10B	8B / 10B	8B / 10B
Tipo de onda	Onda Curta (SW)	Onda Longa (LW)	
Loxitude máxima de segmento	550 m	3.000 m	25m Cat5 100m Cat 5e,6

7.6- HUBS e SWITCHES

CONCENTRADOR (HUB) vs. CONMUTADOR (SWITCH)



NIVEL DE TRABALLO:

Físico: só entende de electricidade e non do significado do que por el está a pasar. Dito dun xeito non científico é como un **arame**.

FUNCIONAMENTO:

Todo o que recibe o HUB por un porto é retransmitido polos demais portos

EXEMPLO:

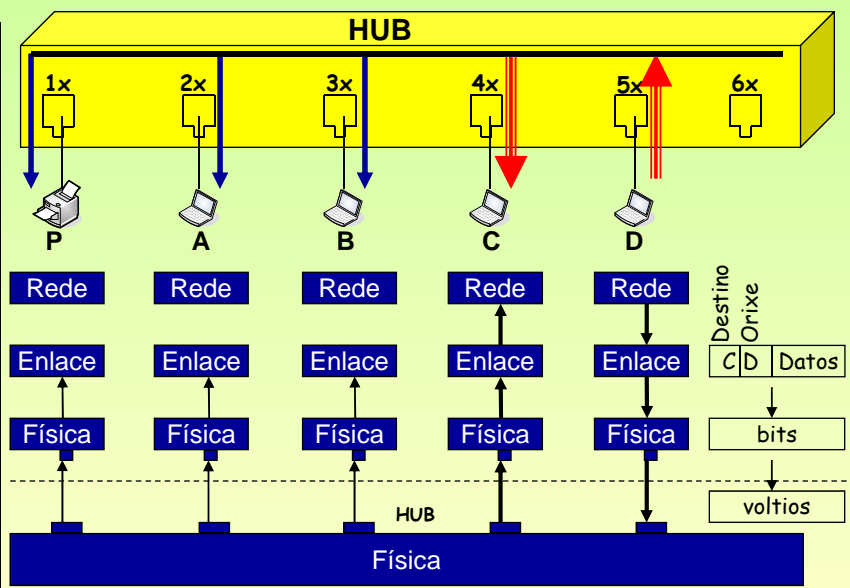
O HOST D desexa enviar unha **trama** ó HOST C. Supoñer que os enderezos **FÍSICOS/MAC** son as letras A,B,C,D e P

ACTIVIDADE NOS RECEPTORES

Tódolos equipos salvo o transmisor (host D) reciben no nivel de enlace a trama enviada.

C: procesa a trama, pois el é o destinatario

A, B e P: descartan a trama, pois eles non son os destinatarios

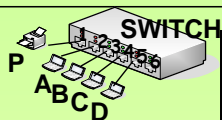


CONCLUSIÓNS:

- 1.- Cando transmite un equipo o hub **inunda** a rede molestado ós demais equipos, salvo ó receptor real.
- 2.- **Colisións:** cando tx dous ou máis equipos as tramas van chocar, pois por un mesmo porto envíanse varias tramas simultaneamente.
- 3.- **Fácil roubo** de información, pois todos están recibindo canto pasa polo hub
- 4.- Se no proceso de envío se **modificou algún bit** da trama o hub non o pode detectar pois non é capaz de interpretar campos de información

7.6- HUBS e SWITCHES

CONCENTRADOR (HUB) vs. CONMUTADOR (SWITCH)



NIVEL DE TRABALLO:

ENLACE: ó traballar neste nivel entende as tramas, está interesado nas direccións **MAC** orixe e destino e no CRC.

FUNCIONAMENTO:

Mantén unha **Táboa de MACs** co formato:

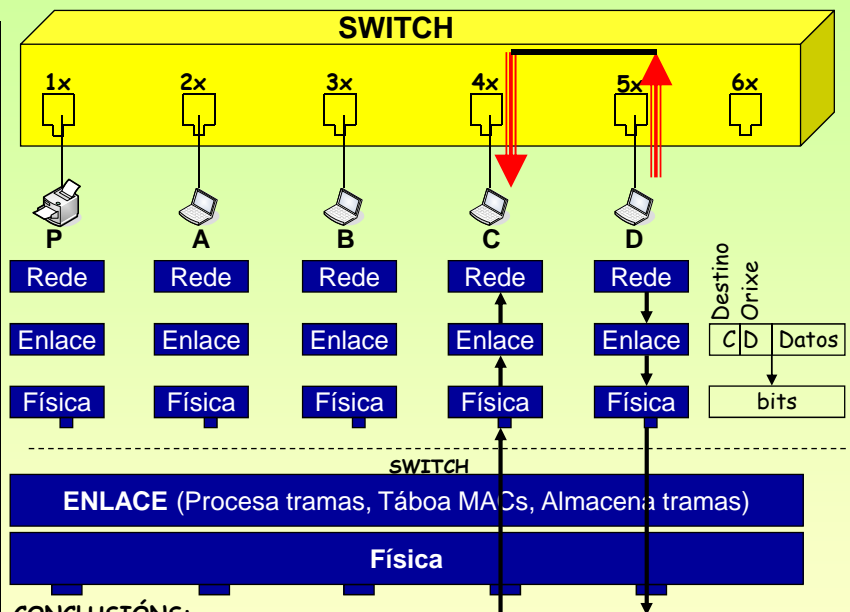
MAC	Porto	Tempo
P	1	10:00:12
B	3	10:00:13
D	5	10:00:27
A	2	10:01:05

Algoritmo de aprendizaxe cara atrás:

- 1.- Cando chega unha trama, apunta na táboa de MACs: **porto de entrada**, dirección **MAC** de quen a **envía** e o **hora** a que chegou.
- 2.- Mira o campo de **destino** da trama e consulta a táboa para saber porque porto está alcanzable esa dirección **MAC**.

Se non existe esa **MAC** (P.e. caso C) entón **inunda**, se existe envía polo porto axeitado.

- 3.- Borra as entradas da táboa cunha antigüidade superior a X segundos

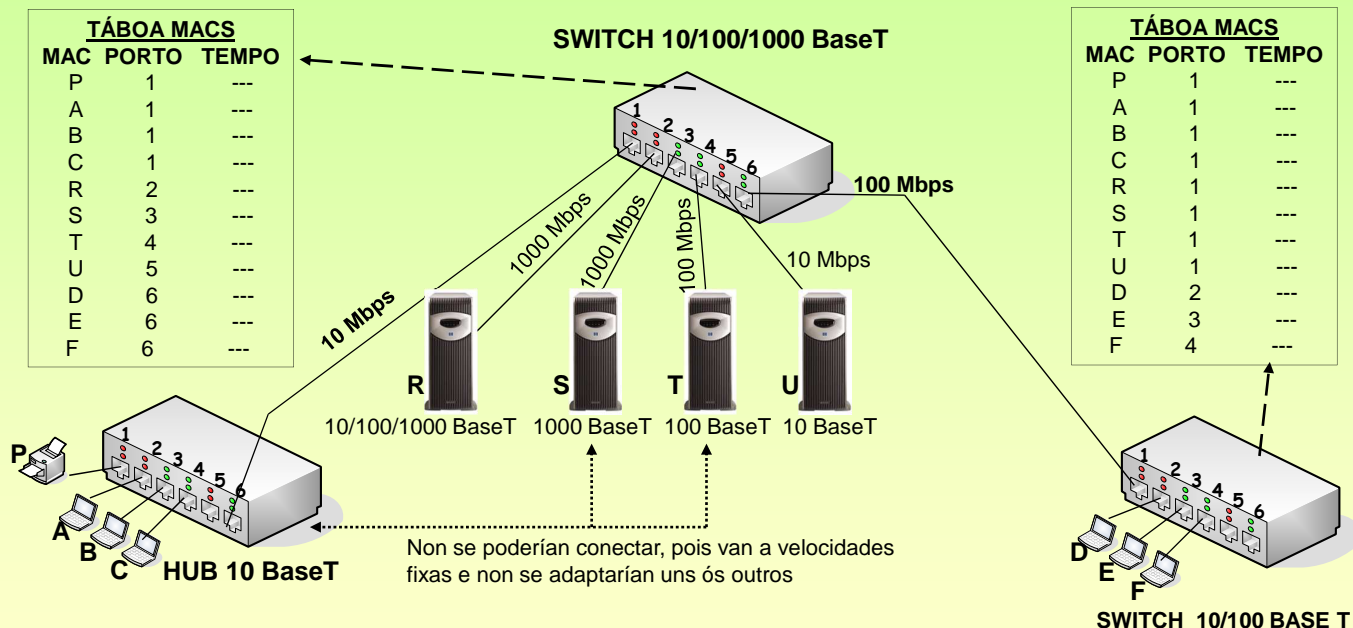


CONCLUSIÓNS:

- 1.- Cando un equipo tx, o switch recibe a trama e reenvía polo porto axeitado. Salvo que non estea o destino na táboa.
- 2.- **Colisións:** o switch almacena nunha memoria as tramas que chegan e logo procésaa. Dous hosts poderían estar enviando a outros dous sen molestarse.
- 3.- O **roubo** de información, precisa usar técnicas de hacker.
- 4.- O switch pode calcular o **CRC** da trama e comparalo co que ven na propia trama, se non coinciden descarta a trama

7.6- HUBS e SWITCHES

👉 ETHERNET (10 BASET) – FAST-ETHERNET (100BASET) – GIGABIT (1000BASET)



CONCLUSIÓN:

- 1.- Un equipo que funcione a 10/100/1000 Mbps pódese conectar con calquera outro elemento.
- 2.- Un equipo que funcione p.ex. a 10 Mbps pódese conectar a outro que vaia a 10 Mbps ou a 10/100 Mbps ou a 10/100/1000 Mbps
- 3.- Dous equipos que poidan ir a 2 ou máis velocidades tratarán de ir á velocidade máis alta.

8.- Introducción – TCP / IP

👉 **ORIXES**

O grupo de protocolos TCP/IP foi creado pola ARPA (Axencia de Proxectos de Investigación Avanzada) pertencente ó departamento de defensa de EE.UU.

👉 **OSI vs. TCP/IP**



8.- Introducción – TCP / IP

IETF (The Internet Engineering Task Force) www.ietf.org

É unha grande comunidade e aberta de deseñadores de rede, operadores, vendedores, investigadores, etc involucrados na evolución da Arquitectura e Funcionalidade do Internet. Está organizado en áreas (p.e. Ruteo, transporte, seguridade, etc)

☞ RFC (Request for comments, Petición de comentarios)

Son documentos que proporcionan información sobre a Arquitectura e a Funcionalidade de Internet. Algunhas son documentos oficiais do IETF, outros son borradores, propostas, tutoriais de aprendizaxe e finalmente outros son cómicos: RFC 2334 (HTCPCP) ou RFC 2549 (IP sobre pombas mensaxeiras con calidade de servizo)

Ademais do IETF estas pódense atopar en www.cse.ohio-state.edu/hypertext/information/rfc.html, www.rfc-editor.org. En español está www.rfc-es.org onde se atopan as RFCs máis importantes traducidas.

☞ Algunhas RFCs

RFC Obxectivo

768 UDP
791 IP
792 ICMP
793 TCP
821 SMTP
959 FTP
1034 DNS
1035 DNS
2131 DHCP
2136 DDNS
Etc.

8.1.- Enderezos IP

☞ ENDEREZOS IP (Internet Protocol) - TIPOS

Cada equipo da rede que chegue ata o nivel 3 de OSI (nivel de rede) vai ter un enderezo IP.

Está composto por 32 bits (4 bytes) que se representan con 4 números enteiros separados por puntos.

Exemplo: 0000 1010 . 0000 0011 . 0000 0101 . 0000 0110 (binario) → 10.3.5.6 (decimal)

Os 32 bits divídense en dúas partes: **Identificador de rede (net id)**: indica o número de rede IP.

Identificador de equipo (host id): indica o número de equipo dentro da rede IP.

Valores característicos na parte de identificador de equipo:

- Poñer todo **ceros** na parte de equipo é para referirse á rede en se mesma (úsase par enrotar / encamiñar)

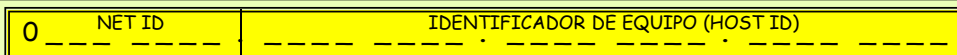
10.0.0.0 (0000 1010 . 0000 0000 . 0000 0000 . 0000 0000) Fai referencia a toda a rede 10 (tódolos equipos da rede 10)

- Poñer todo **uns** na parte de equipo – Multidifusión (Posto nunha dirección destino, ese paquete envíase a todos os equipos da mesma **rede IP**).

10.255.255.255 (0000 1010 . 1111 1111 . 1111 1111 . 1111 1111) Para transmitir a todos os equipos da rede 10.0.0.0

DOUS equipos poderanse comunicar directamente entre se, **se están na mesma rede IP**, senón terán que usar intermediarios: **routers**

☞ TIPO A



1º ÍTEM: 0 - 127

REDES: $2^7 = 128$

EQUIPOS: $2^{24} - 2 = 16.777.214$

REDE PARA USO PRIVADO: 10.0.0.0 - 10.255.255.255 (1 sóa rede clase A - RFC 1989)

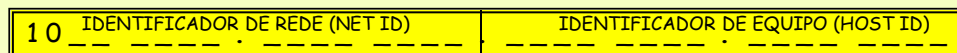
EXEMPLO: 95.3.20.2

REDE: 95.0.0.0

EQUIPO: 3.20.2

MULTIDIFUSIÓN: 95.255.255.255

☞ TIPO B



1º ÍTEM: 128 - 191

REDES: $2^{14} = 16.384$

EQUIPOS: $2^{16} - 2 = 65.534$

REDE PARA USO PRIVADO: 172.16.0.0 - 172.31.255.255 (16 redes clase B - RFC 1989)

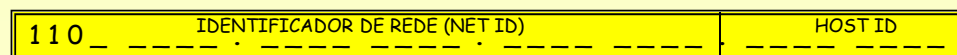
EXEMPLO: 150.3.20.2

REDE: 150.3.0.0

EQUIPO: 20.2

MULTIDIFUSIÓN: 150.3.255.255

☞ TIPO C



1º ÍTEM: 192 - 223

REDES: $2^{21} = 2.097.152$

EQUIPOS: $2^8 - 2 = 254$

REDE PARA USO PRIVADO: 192.168.0.0 - 192.168.255.255 (256 redes clase C - RFC 1989)

EXEMPLO: 192.3.20.2

REDE: 192.3.20.0

EQUIPO: 2

MULTIDIFUSIÓN: 192.3.20.255

8.1.- Enderezos IP

TIPOS ESPECIAIS DE IPs

As IPs privadas de cada clase úsanse para fogares, cibers, institucións, etc, que non queiran ter equipos con IPs reais en internet.

A rede 127.0.0.0 non se usa para asignar ós equipos. En concreto a IP 127.0.0.1 úsase para **loopback** (é o propio equipo). Un equipo aínda que non teña tarxeta de rede sempre ten un IP asignada: 127.0.0.1
Tamén se coñece co nome de "**localhost**" (Explicado máis adiante)

DIFUSIÓN LIMITADA: IP de destino: 255.255.255.255. Úsase para difusión local, cando un equipo desexa enviar a tódolos equipos da súa rede. Úsana os clientes DHCP cando un equipo trata de obter unha dirección IP. (Explicado máis adiante)

DIFUSIÓN: Supoñer esta IP de destino: 10.255.255.255. Se é enviada, por exemplo, por 10.0.3.2 é o mesmo que o caso anterior. Se é enviada, por exemplo, por 11.0.3.4, ese paquete atravesará routers ata alcanzar a rede 10.0.0.0

En www.iana.org (Internet Assigned Numbers Authority) pódense atopar as distintas restricións sobre o uso de IPs.

TIPO D 1 1 1 0 | ----- ENDEREZO DE MULTIDIFUSIÓN -----

1º ÍTEM: 224 - 239

ÚSASE XERALMENTE PARA A DIFUSIÓN DE VÍDEO (UN ÚNICO EMISOR E VARIOS RECEPTORES).

TRÁTASE DE QUE O EMISOR SÓ EMITA UNHA SÓA VEZ E NON TANTAS COMO RECPTORES HAXA.

TIPO E 1 1 1 1 1 0 | ----- RESERVADO PARA USO FUTURO -----

1º ÍTEM: 240 - 247

8.1.- Enderezos IP

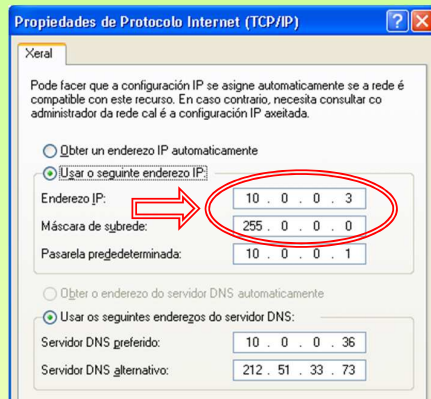
MÁSCARAS

Para determinar nunha dirección IP: que parte é **rede?** e que parte é **equipo?** úsase á **máscara**.

Está formada por 32 bits, que se organizan en 4 números enteiros, ao igual que en un enderezo IP.

A parte da máscara na que hai **uns (1s)** corresponde coa parte de **rede IP** do enderezo IP.

Unha máscara é como a sombra dun enderezo IP. Se non se ten a máscara que acompaña a unha IP non se poderá determinar a parte de rede e a parte de equipo.



MÁSCARA -----
 1º ÍTEM: 0 - 255 2º ÍTEM: 0 - 255 3º ÍTEM: 0 - 255 4º ÍTEM: 0 - 255

MÁSCARA TIPO - A 1111 1111 . 0000 0000 . 0000 0000 . 0000 0000
 255 . 0 . 0 . 0

MÁSCARA TIPO - B 1111 1111 . 1111 1111 . 0000 0000 . 0000 0000
 255 . 255 . 0 . 0

MÁSCARA TIPO - C 1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
 255 . 255 . 255 . 0

8.1.- Enderezos IP

☞ MÁIS SOBRE MÁSCARAS

Outra forma de representar as máscaras é indicando o número de **1s** que posúe esta, sempre contando dende a esquerda.

Exemplo: 10.4.5.6 / 8 (Indica que os 8 primeiros bits da máscara son **1s** e os 24 bits restantes **0s**)
A máscara equivalente en formato de octetos separados por puntos é 255.0.0.0

Como sabe un equipo cal é a súa **rede-IP**? ó facer un AND BINARIO do seu enderezo IP coa súa máscara.

Exemplo: 10 . 4.5.6	0000 1010 . 0000 0100 . 0000 0101 . 0000 0110	
255.0.0.0	1111 1111 . 0000 0000 . 0000 0000 . 0000 0000	AND BINARIO
10 . 0.0.0	0000 1010 . 0000 0000 . 0000 0000 . 0000 0000	

Este ordenador está na **rede-IP** 10.0.0.0 e do **equipo** 4.5.6 dentro desa rede - IP.

☞ IMPORTANCIA DA MÁSCARA

En función da máscara unha, dirección IP pode estar nunha rede IP ou noutra distinta.

EXEMPLO:

10.3.2.1 / 8= 10. 3. 2. 1 255.0.0.0	10.3.2.1 / 16= 10.3.2.1 255.255.0.0	10.3.2.1 / 24 = 10.3.2.1 255.255.255.0
REDE: 10.0.0.0	REDE:10.3.0.0	REDE:10.3.2.0
EQUIPO: 3.2.1	EQUIPO: 2.1	EQUIPO:1

☞ SUBREDES

O exemplo anterior é un claro exemplo de subrede, converteuse unha dirección de tipo A noutras de tipo B e tipo C.

Se unha empresa ten 20 departamentos e está interesada en que cada un deles estea nunha rede – IP distinta,
A empresa merca a IANA a rede IP de tipo B: **130.6.0.0**.
Se lle pon a tódolos equipos a máscara **255.255.0.0** tódolos equipos estarían na mesma rede-IP.

A solución pasa por facer subredes, pasar a IP anterior a outra de **tipo C**, iso conséguese coa máscara.
Se poñen a un departamento IPs na subrede **130.6.1.0 / 24** e a outro **130.6.2.0 / 24**, xa estarían en redes - IP distintas.

79

8.1.- Enderezos IP

☞ E REMATAMOS COAS MÁSCARAS

Desafortunadamente, non tódalas máscaras son /8, /16 ou /24 (isto é 255.0.0.0, 255.255.0.0, 255.255.255.0)
O seguinte exemplo mostra que os valores da máscara van dende /0 ata /32 (Estes 2 casos, en concreto, son casos especiais)

Exemplo: Tres equipos coas seguintes IPs: 10.1.4.6 / 23 (Máscara 255.255.254.0)
Comprobar se están na mesma 10.1.5.6 / 23 (Máscara 255.255.254.0)
rede ip? 10.1.6.6 / 23 (Máscara 255.255.254.0)

Faise o paso a binario:

10.1.4.6 /23	0000 1010 . 0000 0001 . 0000 010	0 . 0000 0110	
Máscara	1111 1111 . 1111 1111 . 1111 111	0 . 0000 0000	AND BINARIO
	0000 1010 . 0000 0001 . 0000 010	0 . 0000 0000	
10.1.5.6 /23	0000 1010 . 0000 0001 . 0000 010	1 . 0000 0110	
Máscara	1111 1111 . 1111 1111 . 1111 111	0 . 0000 0000	AND BINARIO
	0000 1010 . 0000 0001 . 0000 010	0 . 0000 0000	
10.1.6.6 /23	0000 1010 . 0000 0001 . 0000 011	0 . 0000 0110	
Máscara	1111 1111 . 1111 1111 . 1111 111	0 . 0000 0000	AND BINARIO
	0000 1010 . 0000 0001 . 0000 011	0 . 0000 0000	
	NET ID : 23 bits	HOST ID : 9 bits	

Os dous primeiros equipos pódense comunicar entre sei, pois **están na mesma rede –IP**. Os primeiros 23 bits do resultado do AND son iguais.

O terceiro equipo non se pode comunicar cos outros. Está nunha rede-IP distinta. Non coinciden os 23 primeiros bits do resultado do AND cos demais resultados dos 2 primeiros enderezos IP.

Ollo co seguinte exemplo:

10.1.4.4 /30	0000 1010 . 0000 0001 . 0000 0100 . 0000 01	00	Esta IP ten 0s na parte de equipo. Refírese á rede-IP
10.1.4.5 /30	0000 1010 . 0000 0001 . 0000 0100 . 0000 01	01	Esta IP pódesele poñer a un equipo.
10.1.4.6 /30	0000 1010 . 0000 0001 . 0000 0100 . 0000 01	10	Esta IP pódesele poñer a un equipo.
10.1.4.7 /30	0000 1010 . 0000 0001 . 0000 0100 . 0000 01	11	Esta IP ten 1s na parte de equipo. Multidifusión
Máscara	1111 1111 . 1111 1111 . 1111 1111 . 1111 11	00	
	NET ID : 30 bits	HOST ID : 2 bits	

80

8.2.- Routers IP

ENRUTAMENTO IP - AS ROTONDAS

As rotondas de tráfico serven para:

- encamiñar o tráfico. Grazas ás sinais que indican cara a onde están os destinos.
- unir estradas de distintos tipos e velocidades. Por exemplo, unha vía rápida cunha estrada corrente.

Un condutor ó chegar a unha rotonda encamiña o seu coche en función das sinais de dirección.



ROUTERS / ENCAMIÑADORES / PORTA DE ENLACE / PASARELA

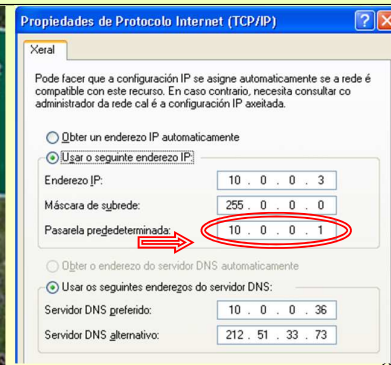
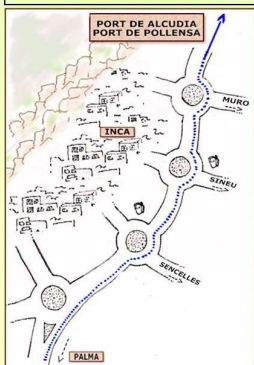
Un **router** actúa coma unha rotonda. A el chegan paquetes que serán encamiñados por unha ou outra liña en función da **táboa de encamiñamento**.

Un condutor para acadar o seu destino pode atravesar moitas rotondas.

Un datagrama / paquete para acadar o seu destino pode atravesar moitos routers.

Un ordenador que desexe enviar un datagrama a outro que non está na mesma rede-IP ca el, debe enviar ese paquete ó router.

Esta é a razón pola que se configura unha porta de enlace no propio equipo. **A porta de enlace estará na mesma rede que o Equipo.**



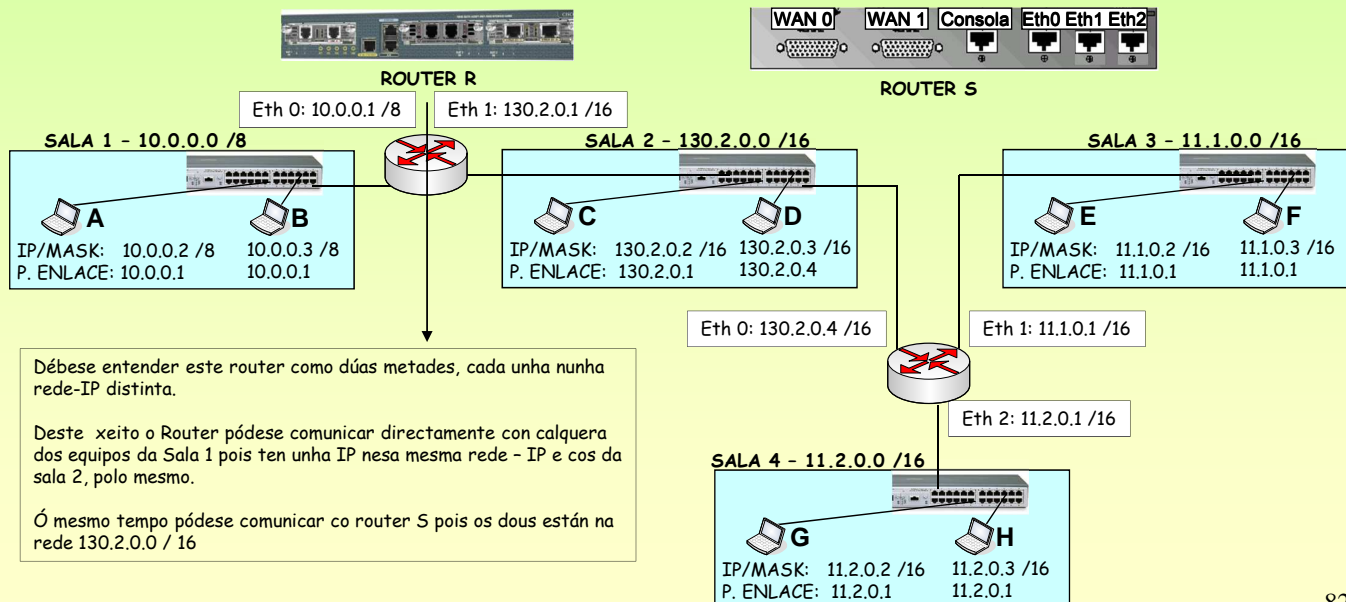
8.2.- Routers IP

CONFIGURAR UN ROUTER: IPs

Obsérvese o seguinte exemplo:

- 4 Redes – IP . Dúas delas en subredes (Sala 3 e Sala 4)
- 2 Routers: **Router R**: une dúas redes IP.
Router S: une tres redes IP.

Cada ordenador debe ter configurada unha porta de enlace á que enviar os paquetes que non vaian para a súa REDE – IP. Ollar como **C e D** teñen configurada unha porta de enlace distinta, pero correctas. Poderían os dous ter a mesma



Débese entender este router como dúas metades, cada unha nunha rede-IP distinta.

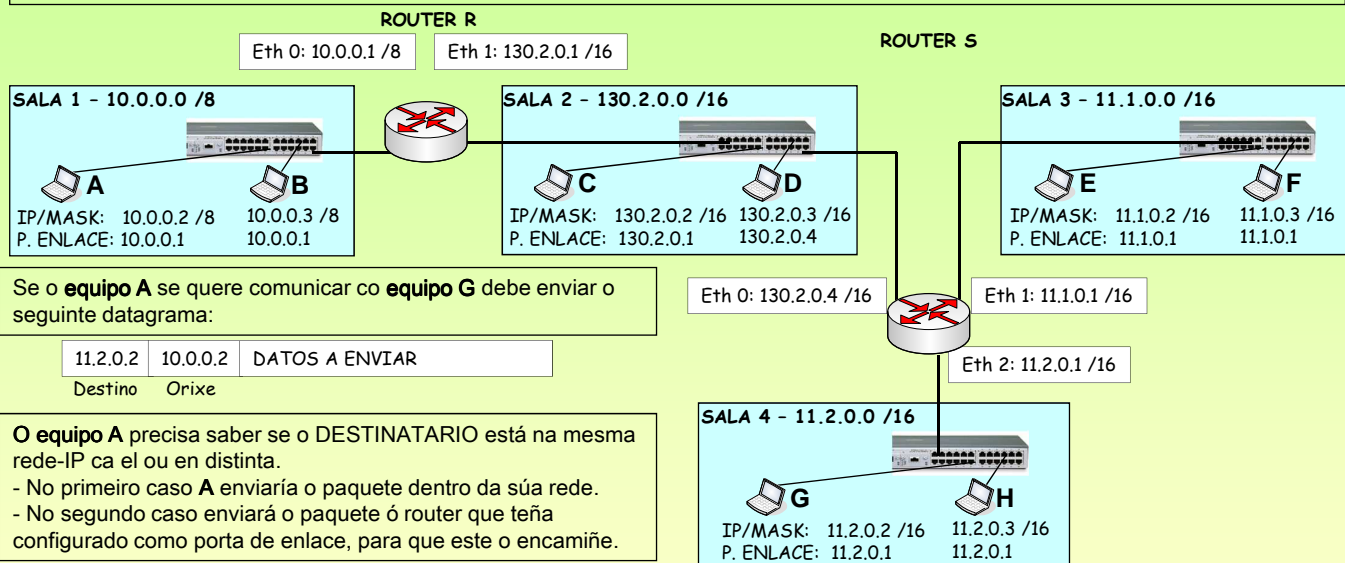
Deste xeito o Router pódese comunicar directamente con calquera dos equipos da Sala 1 pois ten unha IP nesa mesma rede - IP e cos da sala 2, polo mesmo.

Ó mesmo tempo pódese comunicar co router S pois os dous están na rede 130.2.0.0 / 16

Redes Área Local - OSI - TCP/IP

8.2.- Routers IP

CONFIGURAR UN ROUTER: O equipo A va a enviar un paquete ó equipo G



O equipo **A** fai un AND da **súa** máscara coas IPs ORIXE e DESTINO do paquete, deste xeito **A** saberá se destino e orixe están na mesma rede IP:

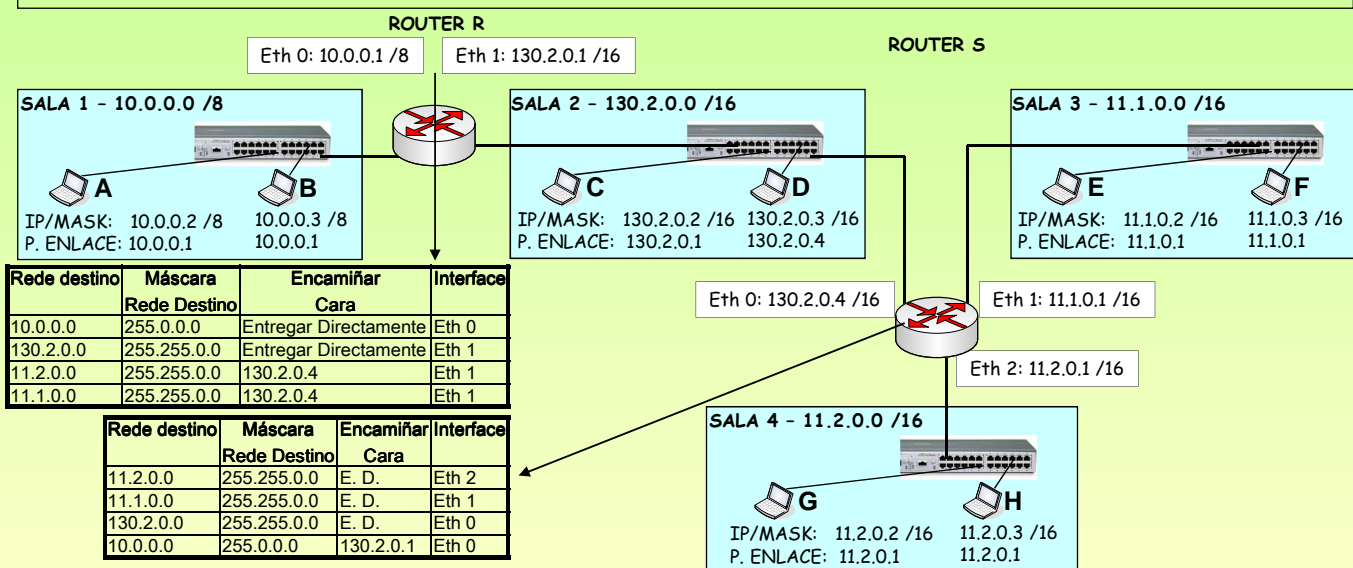
	11	.2.0.2	10	.0.0.2
Máscara do orixe (A)	255	.0.0.0	255	.0.0.0 &
	11	.0.0.0	10	.0.0.0

O **equipo A** chega á conclusión de que o **DESTINATARIO** non está na mesma rede ca el, senón terían que coincidir os resultados.
 O **equipo A** decide, entón, enviar o paquete á súa porta de enlace que é 10.0.0.1 (Router R) e que el o **encamiñe**.
 O **equipo A** pode comunicarse co **Router R** porque, este por un dos lados está na mesma rede ca el.

Redes Área Local - OSI - TCP/IP

8.2.- Routers IP

CONFIGURAR UN ROUTER: TÁBOAS DE ENCAMIÑAMENTO (I)



O **equipo A** decidiu enviar o anterior paquete ó router. Este fará o que fai un carteiro, mirará a dirección de destino. Neste caso: 11.2.0.2
 O router realiza una AND da IP DESTINO coa primeira máscara da táboa de ruteo e mira se coincide coa columna **Rede Destino**.

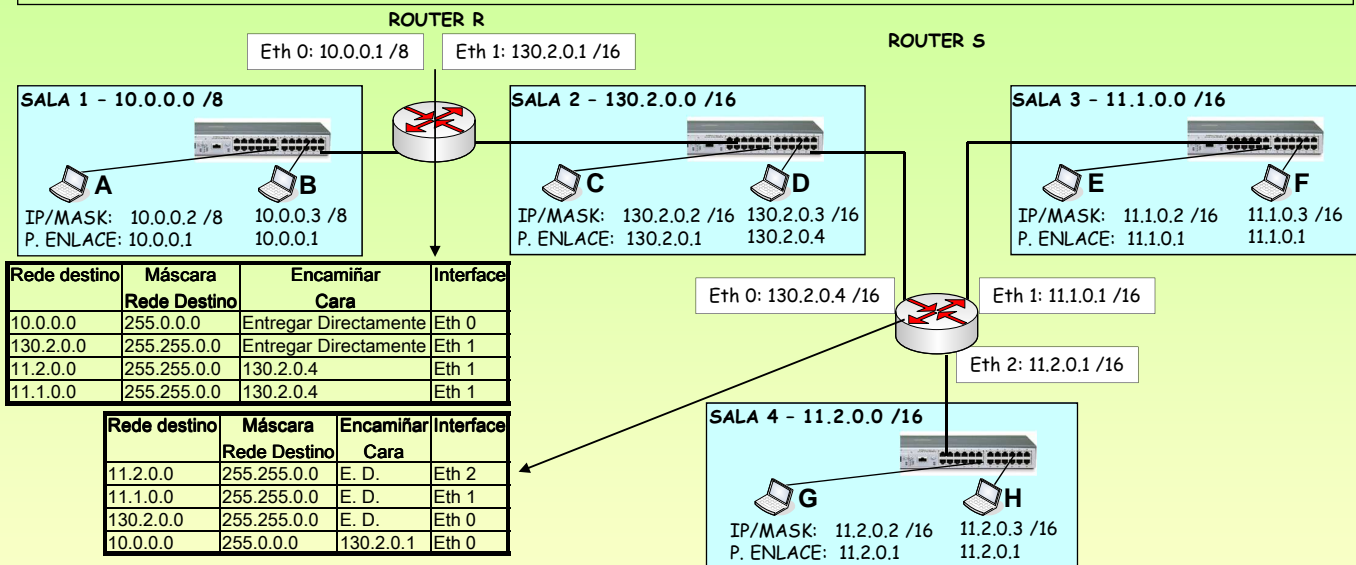
- **SE COINCIDE:** envía o paquete a onde indique a columna **Encamiñar CARA**, polo **interface** indicado.
- **SE NON COINCIDE:** realiza a mesma operación do AND coa segunda entrada da táboa. E así ata coincidir ou rematar.

NESTE CASO: (Destino) 11.2.0.2 & (1ª Máscara) 255.0.0.0 = 11.0.0.0 non coincide con 10.0.0.0 (da primeira fila)
 11.2.0.2 & 255.255.0.0 = 11.2.0.0 non coincide con 130.2.0.0 (da segunda fila)
 11.2.0.2 & 255.255.0.0 = 11.2.0.0 **SI** coincide con 11.2.0.0. Enviar paquete a : 130.2.0.4

Redes Área Local - OSI - TCP/IP

8.2.- Routers IP

CONFIGURAR UN ROUTER: TÁBOAS DE ENCAMIÑAMENTO (II)



Un router está interesado no DESTINO dos paquetes que lle chegan, ó igual que as oficinas de correos.

Seguindo co exemplo anterior, agora, o paquete teno o Router S. Este realizará o mesmo proceso que o router R. Neste caso a primeira entrada da táboa xa lle indica que ese paquete teno que **entregar directamente** polo interface Eth 2.

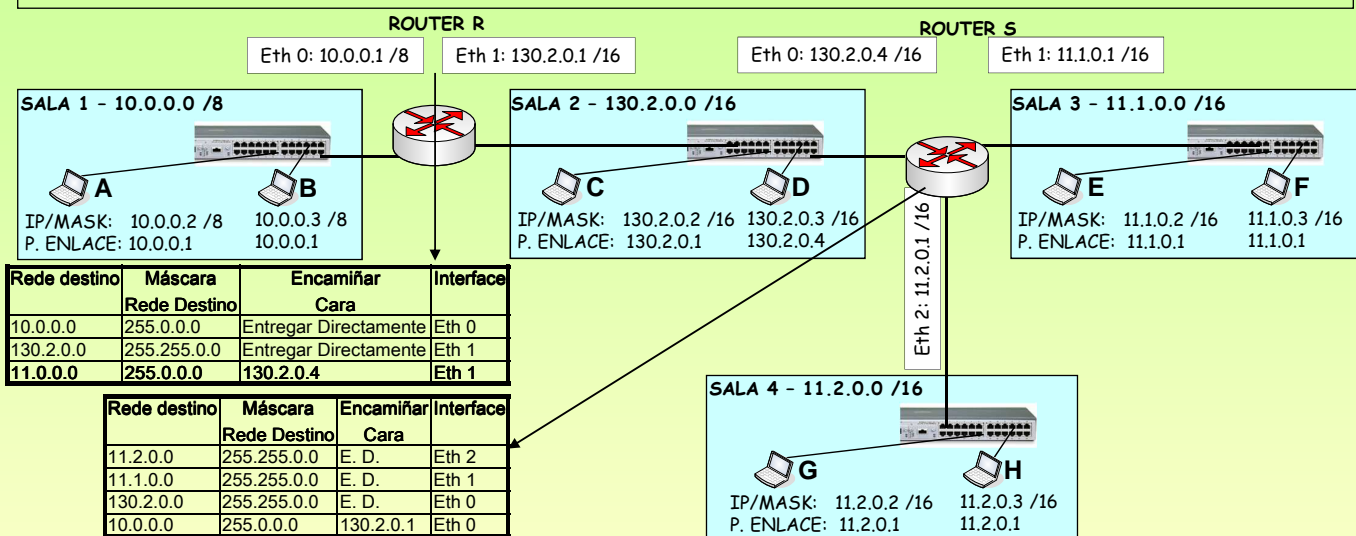
ENTREGAR DIRECTAMENTE: cando unha carta chega á última oficina de correos, só resta que o carteiro colla a Vespa e leve a carta ó seu destinatario real.

Neste caso igual, ó router só lle resta mandarlle ó seu destinatario final.

Redes Área Local - OSI - TCP/IP

8.2.- Routers IP

CONFIGURAR UN ROUTER: TÁBOAS DE ENCAMIÑAMENTO (II)



Débase desprender que a dirección IP Destino do paquete non se modifica, ó igual que non se modifica nunha carta, senón non se podería encamiñar ata o seu destino final.

Se a rede 11.0.0.0 é toda da empresa. E se esta é a configuración final da rede, obsérvase como se podería modificar a táboa de encamiñamento do ROUTER R.

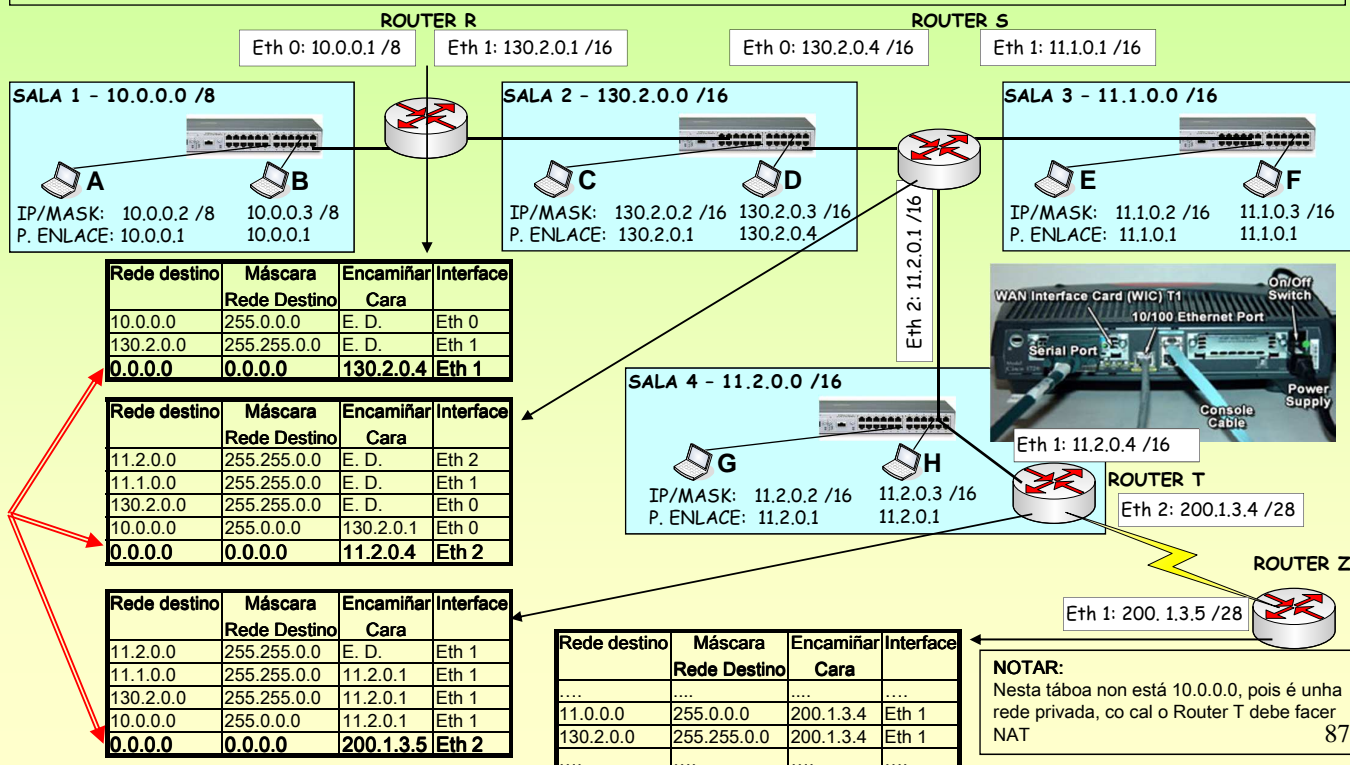
Sácanse as dúas entradas 11.2.0.0/16 e 11.1.0.0/16 e substitúese por unha soa entrada 11.0.0.0/8. Pois tanto a subrede 11.1.0.0 como a 11.2.0.0 teñen en común rede 11.0.0.0 na súa totalidade.

Será o router S quen faga as distincións entre unha subrede e a outra.

Redes Área Local - OSI - TCP/IP

8.2.- Routers IP

CONFIGURAR UN ROUTER: TÁBOAS DE ENCAMIÑAMENTO (III) Conectados a INTERNET



Redes Área Local - OSI - TCP/IP

8.2.- Routers IP

ROUTER R:

O router R pode entregar paquetes para a SALA 1 e a SALA 2, se os paquetes van para calquera outro sitio terá que enviarllo ó router S e que el se encargue de encamiñalos.

A última entrada da Táboa de Encamiñamento é a que indica que cando chegue un paquete que non vaia para unha desas salas llo envíe ó router S.

Deste xeito non se teñen que contemplar nunha táboa de encamiñamento tódolos posibles destinos (tanto da intranet como de internet, que sería imposible).

EXEMPLO: pénsese que ó router R chegaron tres paquetes cos seguintes destinos:

11.1.0.2 (Sala 3)
213.4.130.210 (www.terra.es)

En calquera dos dous casos terá que enviar ese paquete ó router S. Realicemos a proceso do router coa segunda IP.

IP DESTINO	MÁSCARA	RESULTAO	1ª COLUMNA	
213.4.130.210	& 255.0.0.0	= 213.0.0.0	!= 10.0.0.0	→ Seguir co proceso e operar coa 2ª entrada
213.4.130.210	& 255.255.0.0	= 213.4.0.0	!= 130.2.0.0	→ Seguir co proceso e operar coa 3ª entrada
213.4.130.210	& 0.0.0.0	= 0.0.0.0	= 0.0.0.0	→ Encamiñar cara 130.2.0.4

CONCLUSIÓN: como calquera IP AND 0.0.0.0 vai dar 0.0.0.0 esa entrada sempre se debe poñer ó final da táboa. Os demais routers tamén deben ter a entrada 0.0.0.0.

ROUTER T: o router da empresa para saír a internet a través dun ISP

Este router une dúas entidades. Cada unha encárgase de configurar a súa "metade". A empresa non pode condicionar a IP polo lado do Proveedor de Servizos de Internet (ISP). Esa función correspóndelle ó ISP para adaptalo á súa rede IP.

ROUTER Z: o router do ISP que encamiña cara á empresa.

Este router configúrao totalmente o ISP, pero nel ten que ter entradas que axuden ós paquetes a chegar ata as dúas redes-IP da empresa.

Díñese dúas redes pois a empresa mercou a 130.2.0.0 /16 e a 11.0.0.0/8 aínda que esta última estea convertida en subredes. Neste caso as subredes son algo interno da empresa que no exterior non o van saber. No exterior todo é 11.0.0.0 /8

8.2.- Routers IP

ALGORITMOS DE ENCAMIÑAMENTO

Indican a forma en que se constrúe a táboa de encamiñamento dun router

NON ADAPTATIVOS (ESTÁTICOS)

Non se adaptan ás situacións cambiantes da rede (unha liña saturada, unha liña que cae, etc). Cando chegen varios paquetes para o mesmo destino sempre os vai encamiñar polo mesmo sitio.

Hai que configuralos manualmente.

Equivalen a unha rotonda na que só hai sinais indicativas e que non sabe en que situación se atopan cada unha das saídas.

ADAPTATIVOS

Os routers que usan algoritmos adaptativos adaptáanse ós cambios e situacións da rede. Existen tres tipos:

CENTRALIZADO:

Equivale á sala de control de tráfico dunha cidade onde teñen a información do que está a pasar en cada unha das rotondas, que rúas están saturadas, cales cortadas, etc. Con toda esa información elaboran as accións que deben levar a cabo cada un dos Gardas que están nas rotondas.

Existe un nó central ó que cada router lle envía información (cal é a liña máis solicitada, de onde lle veñen paquetes devoltos, se ten enlace cos demais routers, etc). Con esa información o nó elabora a táboa de cada router e logo envíallaa. Existen problemas: uns routers terán as táboas antes que outros, esas táboas son paquetes competindo con outros na rede.

ILLADOS:

Equivale a poñer un GARDA en cada rotonda e que este dirixa o tráfico como lle apeteza sen ter en conta nada de nada, nin se está saturada unha saída, se hai un incidente, etc.

Exemplo: PATACA QUENTE: Chega un paquete, desfai del tan pronto como poida e por calquera liña.

DISTRIBUÍDOS:

Equivale a ter Gardas nas rotondas pero cada un comunicase cos GARDAS das rotondas próximas a el, deste xeito trata de tomar as decisións adaptándose ó que pasa ó seu arredor.

8.2.- Routers IP

COMANDOS

Windows: ROUTE

```
C:\WINDOWS\System32\CMD.exe
L:\>ROUTE
Manipula tablas de enrutamiento de red.
ROUTE [-f] [-p] [comando [destino] [MASK]
[METRIC métrica] [IF interfaz]
-f Borra las tablas de enrutamiento de puerta de enlace.
-p Cuando se usa con el comando ADD, hace una ruta persistente en los inicios del sistema. De manera predeterminada, las rutas no se conservan cuando se reinicia el sistema. Se pasa por alto para todos los demás comandos, que siempre afectan a las rutas persistentes apropiadas. Esta opción no puede utilizarse en Windows 95.
comando Uno de los siguientes:
        PRINT Imprime una ruta
        ADD Agrega una ruta
        DELETE Elimina una ruta
        CHANGE Modifica una ruta existente
destino Especifica el host.
MASK Especifica que el siguiente parámetro es el valor de "máscara_red".
máscara_red Especifica un valor de máscara de subred para esta entrada de ruta. Si no se especifica, se usa de forma predeterminada el valor 255.255.255.255.
puerta_enlace Especifica la puerta de enlace.
interfaz El número de interfaz para la ruta especificada.
METRIC Especifica la métrica; por ejemplo, costo para el destino.
```

```
C:\WINDOWS\System32\CMD.exe
L:\>route print
=====
Lista de interfaces
0x1 ..... MS TCP Loopback interface
0x4 ...00 0b 6a 2a 74 9a ..... UIA UT6102 Rhine II Fast Ethernet Adapter - Mini puerto del administrador de paquetes
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de acceso      Interfaz      Métrica
10.0.0.0            0.0.0.0             10.0.0.1              10.0.0.5      20
10.0.0.0            255.0.0.0           10.0.0.5              10.0.0.5      20
10.0.0.5            255.255.255.255    127.0.0.1             127.0.0.1     20
10.255.255.255     255.255.255.255    10.0.0.5              10.0.0.5      20
127.0.0.0          255.0.0.0           127.0.0.1             127.0.0.1     1
224.0.0.0          240.0.0.0           10.0.0.5              10.0.0.5      20
255.255.255.255   255.255.255.255    10.0.0.5              10.0.0.5      1
Puerta de enlace predeterminada: 10.0.0.1
=====
Rutas persistentes:
ninguno
```

8.2.- Routers IP

```

root@linuxp: /root - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[root@linuxp root]# route --help
Usage: route [-nNvee] [-FC] [<AF>]
       route [-v] [-FC] {add|del|flush} ...
       route {-h|--help} [<AF>]
       route {-V|--version}

       -v, --verbose          be verbose
       -n, --numeric          don't resolve names
       -e, --extend           display other/more information
       -F, --fib              display Forwarding Information Base (default)
       -C, --cache            display routing cache instead of FIB

<AF>=Use '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
inet (DARPA Internet) inet6 (IPv6) ar25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
[root@linuxp root]#
    
```

COMANDOS
Linux: route

```

root@linuxp: /root - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[root@linuxp root]# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0       *               255.0.0.0      U        0      0      0 eth0
127.0.0.0      *               255.0.0.0      U        0      0      0 lo
default        10.0.0.1        0.0.0.0        UG       0      0      0 eth0
[root@linuxp root]#
    
```

8.3.- ARP (Address Resolution Protocol)

MÁS TÁBOAS - CACHE ARP (I) (a ligazón do nivel IP co nivel de enlace)

EXEMPLO: O HOST A desexa enviar un paquete ó HOST B. (No gráfico débense seguir os números. Supoñer que as letras A, B, J son as MACs dos Hosts)

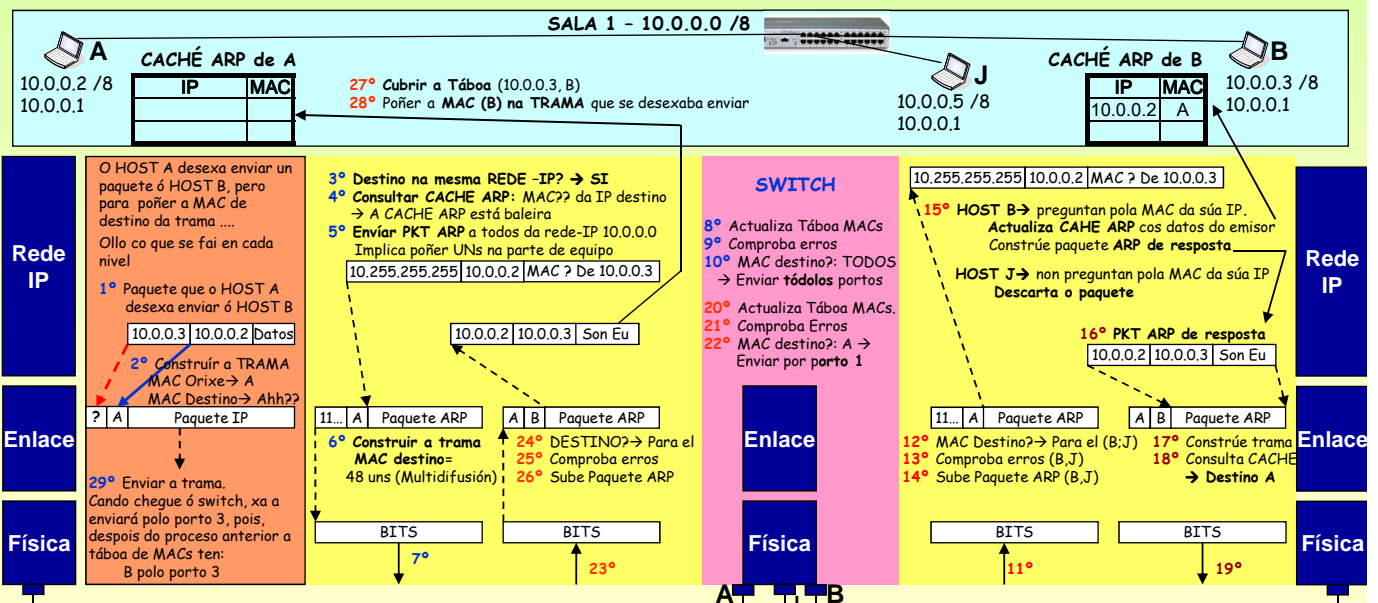
NIVEL IP: constrúe o datagrama cos enderezos orixe (10.0.0.2) e destino (10.0.0.3) e o campo de datos. Comproba se o destino está na mesma rede IP → A CACHE ARP está baleira

NIVEL ENLACE: constrúe á trama, pero ¿Cal é a dirección MAC do destino?. Para achala usa o **Address Resolution Protocol (ARP)**

ARP: Cada equipo almacena en memoria unha táboa (CACHE ARP) que asocia IPs con MACs. Para construír esa táboa usa o Protocolo de Resolución de Enderezos (ARP). O protocolo ARP está na capa de REDE, no nivel 3.

Consiste en enviar a tódolos equipos da LAN a seguinte pregunta: **¿Pódeme dicir o ordenador con IP X.Y.Z.T cal é a súa MAC?**

Esta pregunta recibiríana tódolos equipos da LAN e só responderá o afectado, coa resposta imos cubrindo os campos da táboa para futuras ocasións. Ó mesmo tempo o ordenador afectado rexistra na súa CACHE ARP a IP e MAC de que fixo a petición.



Redes Área Local - OSI - TCP/IP

8.3.- ARP (Address Resolution Protocol)

MÁS TÁBOAS - CACHE ARP (II)

EXEMPLO: Agora o HOST A desexa enviar un paquete ó HOST D. Pero para chegar ó HOST D temos que pasar antes polo Router R.

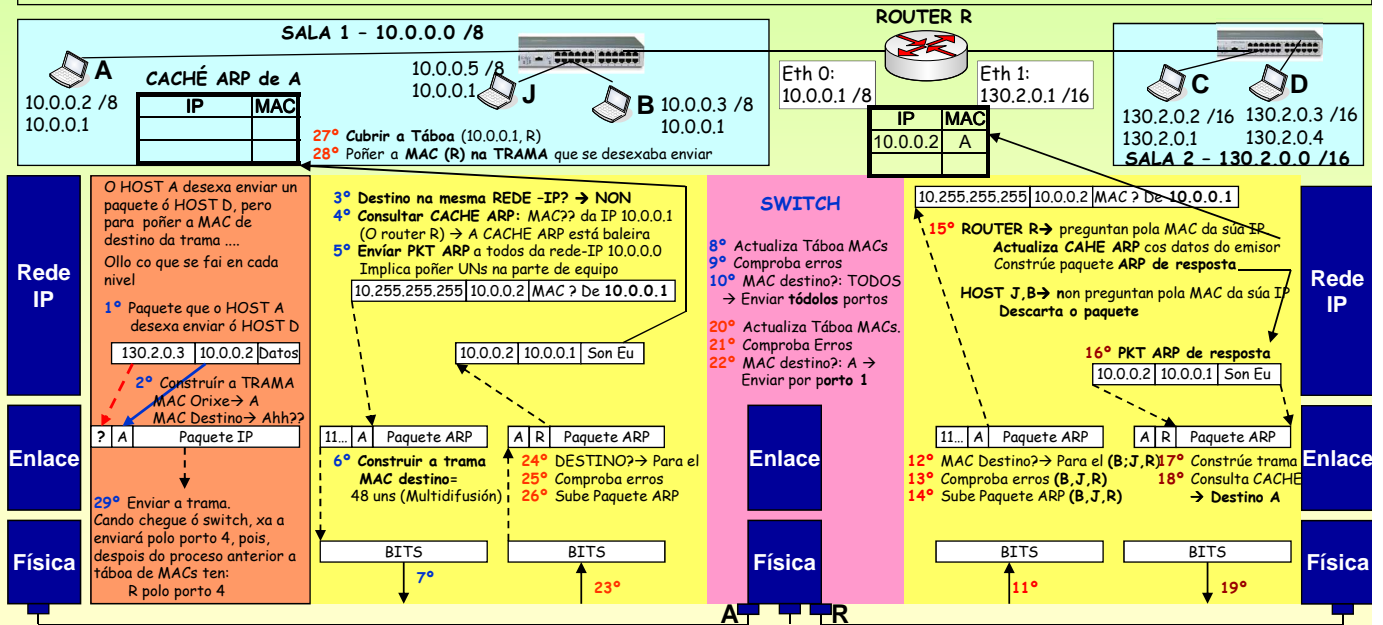
NIVEL IP: constrúe o datagrama cos enderezos orixe (10.0.0.2) e destino (130.2.0.3) e o campo de datos. Comproba se o destino está na mesma rede IP É AQUI, onde radica a diferenza co caso anterior. O host A tenlle que enviar o paquete ó Router para que el o encamiñe, co cal no nivel 2 a MAC que ten que achar é a do ROUTER R e non a do host D. **OBSERVAR OS PASO 1,3,4,5,27 O RESTO E SEMELLANTE.**

NIVEL ENLACE: constrúe a trama, pero ¿Cal é a dirección MAC do ROUTER R (10.0.0.1), NON do DESTINO REAL?.

ARP: Os routers tamén teñen a táboa CACHE ARP, pero neste caso terá IPs e MACs das redes que una por cada interface.

O host A realizará o mesmo proceso que no caso anterior só que a MAC que ten que calcular é a da porta de enlace.

Unha vez que o HOST A averigüe a MAC do router R enviaralle a trama a este. Logo, o router terá que facer todo o proceso pero cara á SALA 2.

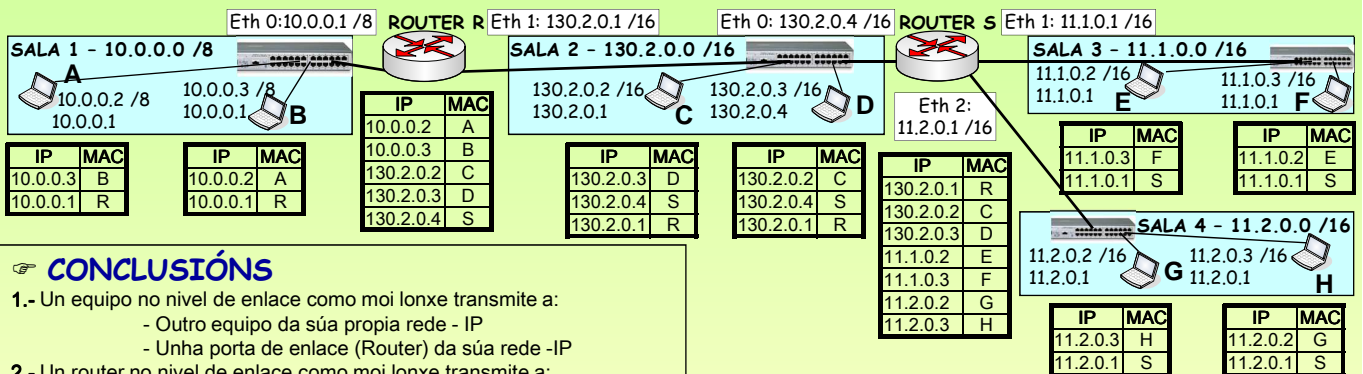


Redes Área Local - OSI - TCP/IP

8.3.- ARP (Address Resolution Protocol)

EXEMPLO - TÁBOAS CACHE ARP (III)

As táboas constrúense dinamicamente. Aquelas entradas na táboa que pasado un tempo non se usen vanse borrando. No seguinte exemplo suponse que tódolos equipos se comunicaron con todos. As súas táboas serían:



CONCLUSIÓNS

- Un equipo no nivel de enlace como moi lonxe transmite a:
 - Outro equipo da súa propia rede - IP
 - Unha porta de enlace (Router) da súa rede -IP
- Un router no nivel de enlace como moi lonxe transmite a:
 - Outro router da súa mesma rede-IP.
 - Un equipo de calquera das redes-IP que interconecta.

COMANDOS

COMANDOS: co comando **arp** (Linux / Windows) podemos traballar coa táboa CACHE ARP

```
C:\WINDOWS\System32\cmd.exe
L:\>arp -a

Interfaz: 10.0.0.5 --- 0x4
Dirección IP      Dirección física      Tipo
10.0.0.1          00-60-67-02-1f-4a    dinámico
10.0.0.35         00-0a-5e-1a-35-cf    dinámico
10.0.0.45         00-0d-61-1c-10-5b    dinámico
10.0.0.51         00-00-e2-13-0e-fd    dinámico
```

```
root@linuxp:/root - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[root@linuxp root]# arp
Address           HWtype  HWaddress           Flags
10.0.0.38         ether   00:05:5D:D2:E4:0F   C
10.0.0.5          ether   00:0E:6A:2A:74:9A   C
10.0.0.35         ether   00:0A:5E:1A:35:CF   C
10.0.0.35         ether   00:0A:5E:1A:35:CF   C
```

Redes Área Local - OSI – TCP/IP

8.3.- ARP (Address Resolution Protocol)

☞ IP (Internet Protocol)

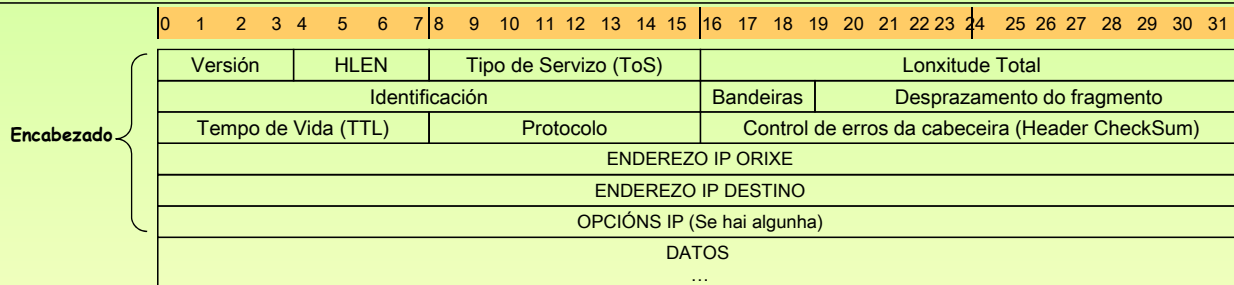
DATAGRAMAS: paquetes nos que se divide unha mensaxe e que se envían usando un **servizo non orientado á conexión**.

O nivel IP especifica o formato dos paquetes do nivel de rede, chamados **datagramas**.

Supón unha subrede (elementos de comunicacións entre orixe e destino reais) moi fiable pois fíase de que os paquetes van chegar ó destino.

O datagrama pode fragmentarse noutros máis pequenos se ten que atravesar redes con MTU (Campo de datos da trama) máis pequena.

O tamaño máximo do datagrama é de 64 KBytes. Este divídese en dúas partes CABECEIRA e DATOS



VERSION:	Versión do protocolo IP coa que se creou o datagrama. Versións actuais (IPv4 para enderezos de 32 bits)
HLEN:	Lonxitude da cabeceira medida en palabras de 32 bits (1 palabra de 32 bits é igual a unha fila do debuxo) O encabezado común, sen opcións mide 5 (5 filas, 5 palabras de 32 bits). Isto é 5x4= 20 bytes.
LONGITUDE TOTAL:	Medido en Bytes, inclúe os bytes da cabeceira e dos datos. O campo ten 16 bits → 2 ¹⁶ =65.536 octetos (64 KB)
TIPO DE SERVIZO:	Para especificar a prioridade do datagrama, fiabilidade , retardo ... Os routers non fan moito caso a este campo.
TEMPO DE VIDA:	(Time to live) Especifica o tempo en segundos que o datagrama pode estar na rede. Ó pasar polos routers, estes van decrecendo este valor. Se o seu tempo concluíu e non chegou ó destino os routers elimínanos.
PROTOCOLO:	Que protocolo de alto nivel creou o datagrama . (TCP ou UDP).
CHECKSUM:	Realiza unha serie de complementos a un coa cabeceira e o resultado pono neste campo, para no receptor comprobar que a cabeceira chegou correctamente.
ENDERZOS IP:	Conteñen as direccións IP orixe do paquete e destino do paquete.
OPCIÓNS:	Úsase para probas de rede e depuración (Rexistrar rutas, etc). Como máximo poden ser 10 palabras de 32 b=40B
DATOS:	Contén bytes que se corresponden a un segmento (Unidade de datos que intercambian entidades de transporte)

Redes Área Local - OSI – TCP/IP

8.4.- Datagrama IP

☞ IP (Internet Protocol) – A fragmentación: (Maximun Transfer Unit) (I)

Un emisor debe pasar un datagrama do nivel 3 ó nivel 2. Isto é, debe meter o datagrama no campo de datos dunha TRAMA.

Pero dependendo da especificación que se use no nivel 2 o campo de datos terá un tamaño ou outro, este tamaño coñécese como **MTU**.

Ethernet (IEEE 802.3):	1.500 Bytes	Token Bus (IEEE 802.4):	8.174 Bytes
Token Ring (IEEE 802.5):	ilimitado	FDDI:	ilimitado
ATM (ATM sobre ADSL):	48 bytes	FRAME RELAY:	ilimitado

Co cal se se ten un datagrama de tamaño maior que o campo de datos da trama, terase que fragmentar o datagrama noutros máis pequenos.

IDENTIFICACIÓN:	identifica o número de paquete, se este se fragmenta, cada fragmento levará a mesma IDENTIFICACIÓN. Así o receptor saberá que fragmentos se corresponden a cada paquete orixinal.
BANDEIRAS (FLAGS):	indica se o paquete se pode ou non fragmentar. No caso de que se poida, indica se é un fragmento intermedio ou último
DESPRAZAMENTO:	Cando se fragmenta un paquete, cada fragmento leva un anaco do datagrama orixinal. Este campo indica que posición ocupan os bytes, que leva un fragmento, no datagrama orixinal. (Enténdase como se fose a numeración de cada fragmento).
ONDE SE FRAGMENTA?:	Un datagrama pódese fragmentar no extremo emisor ou en calquera dos routers intermedios, sempre e cando o esixa a MTU da rede a atravesar.
ONDE SE REENSAMBLA?:	Só, só, só no EXTREMO RECEPTOR FINAL . Pois cada fragmento puido ir por camiños distintos ata chegar ó receptor final, así pois será o que reciba tódolos anacos nos que se dividiron os fragmentos.



8.4.- Datagrama IP

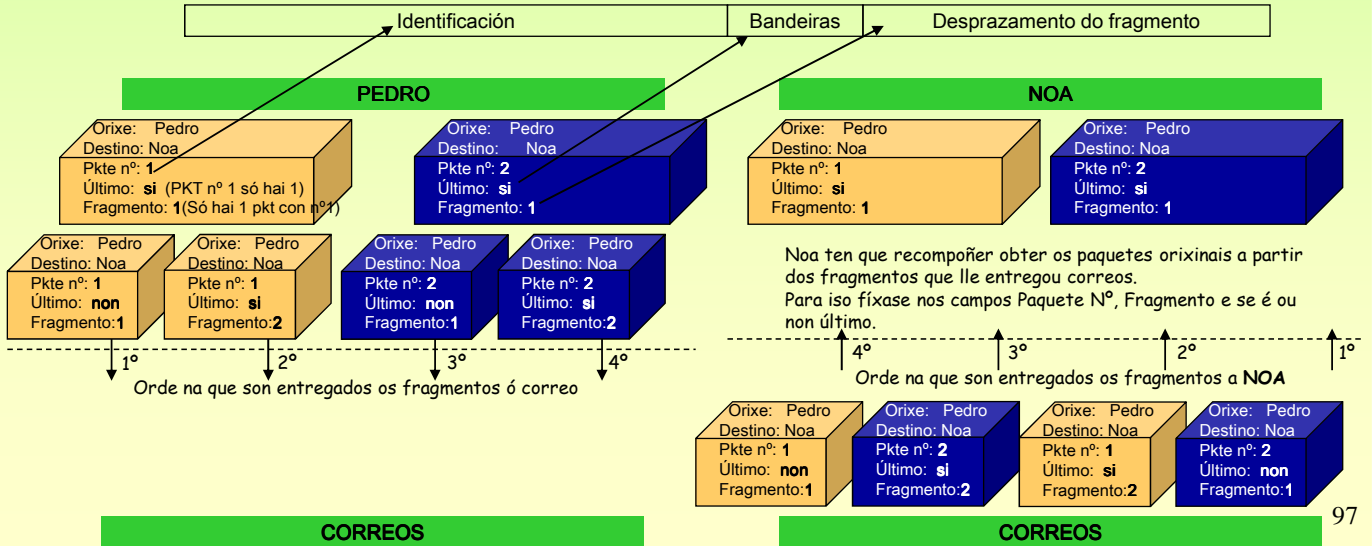
☞ IP (Internet Protocol) - A fragmentación: Exemplo de correos (II)

Obsérvese o seguinte exemplo no que PEDRO desexa enviar dous paquetes a NOA.

Os paquetes a enviar son moi grandes para mandar por correos. Este obrígaos a fragmentalos.

Pedro fragmenta cada paquete en 2 anacos, e copia nos anacos a información común do paquete: identificación, destino, orixe, ... Logo numera cada un dos fragmentos dentro do paquete orixinal para que o receptor ó recibilos poida recompoñer o paquete.

Obsérvese que Pedro envía os fragmentos nunha orde e que correos llos entrega a Noa noutra orde distinta. É Noa quen, coa información que ven en cada fragmento ten que recompoñer os paquetes orixinais.



8.4.- Datagrama IP

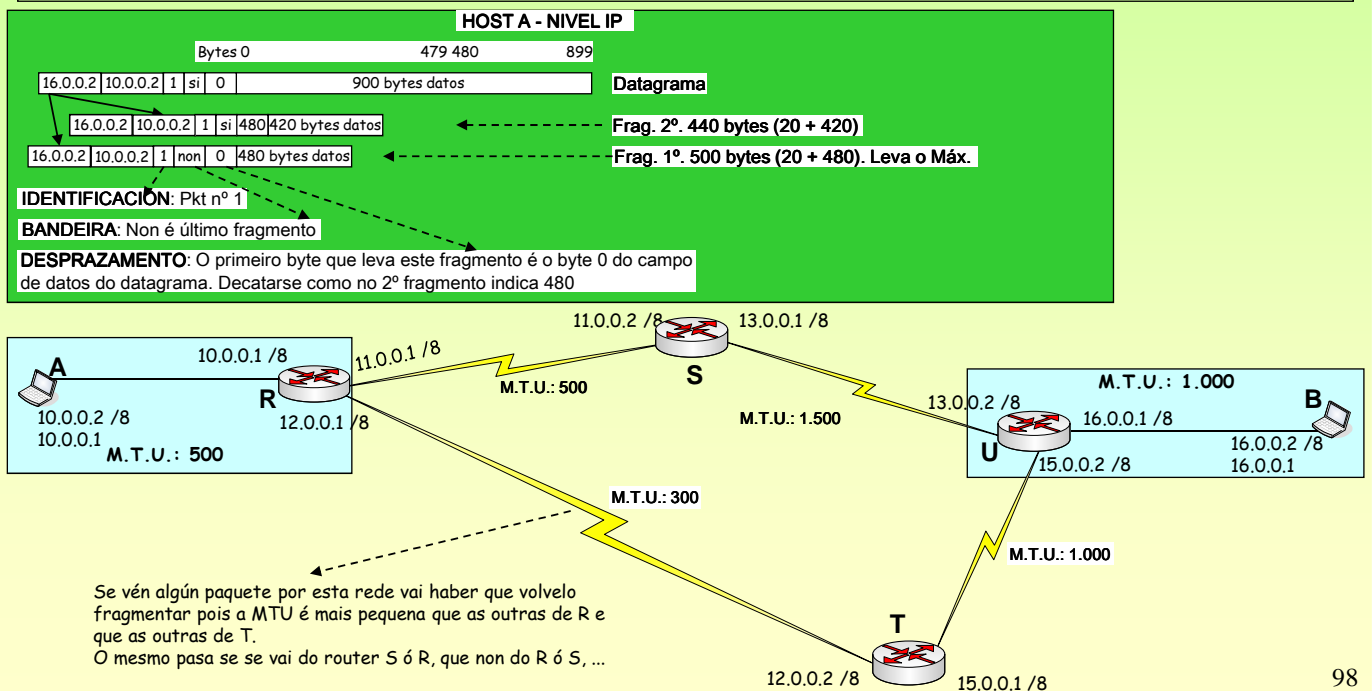
☞ IP (Internet Protocol) - A fragmentación: Exemplo informático (III)

O HOST A desexa enviar un paquete ó HOST B. Existen diferentes MTUs, comprobar no debuxo.

O paquete a enviar mide 920 bytes (900 datos, 20 bytes cabeza sen opcións) e a MTU=500, implica que A vai ter que fragmentar en 2 anacos.

Os routers son dinámicos, isto é, varios paquetes para un mesmo destino, poden ser encamiñados por distintas rutas.

NOTA: O enderezo de máis a esquerda é o destino e o outro é a orixe. Non coincide coa realidade.

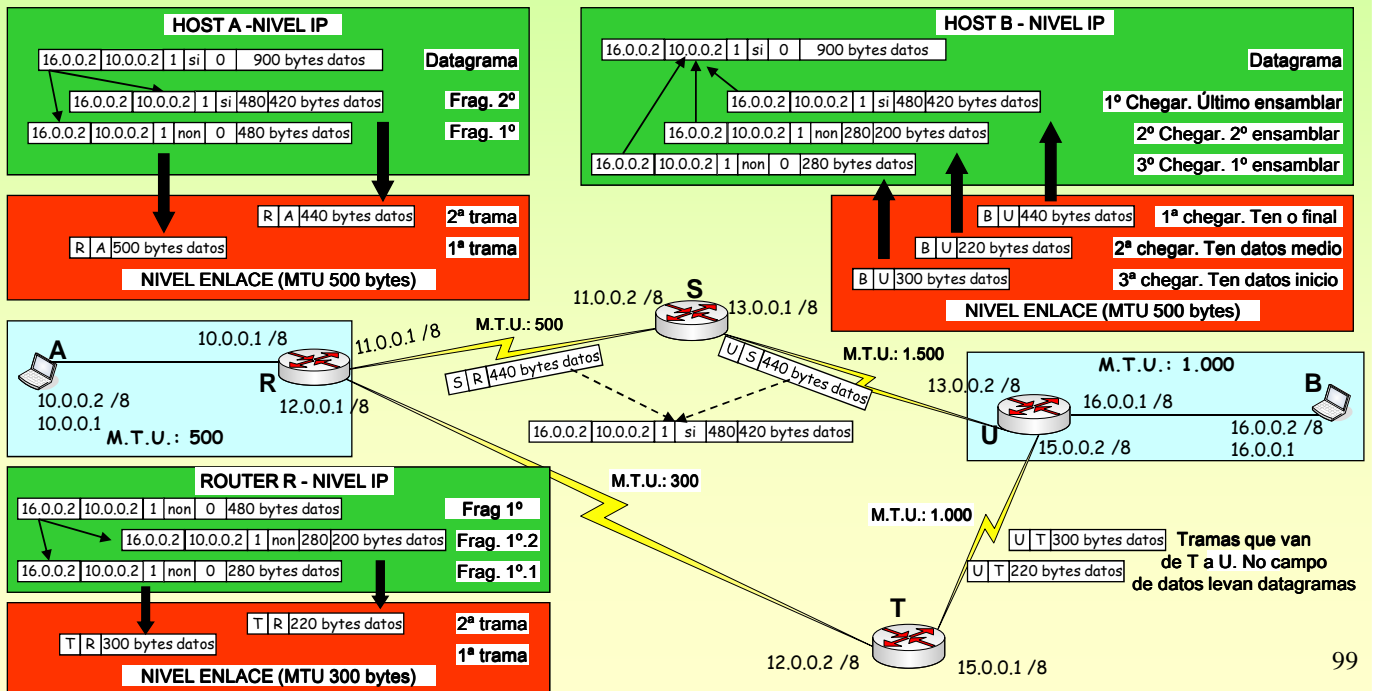


Redes Área Local - OSI - TCP/IP

8.4.- Datagrama IP

☞ IP (Internet Protocol) - A fragmentación: Exemplo informático (IV)

O router R envía o fragmento 2º pola liña superior e o outro pola inferior, que ten MTU=300, co cal ten que volver a fragmentar o fragmento 1º. No HOST B recibense os 3 fragmentos desordenados, é responsabilidade do NIVEL IP ordenalos e ensamlalos na orde correcta. Se non chegou un fragmento, ou a cabeceira chegou con erros (CHEKSUM) descártanse todos os fragmentos coa mesma IDENTIFICACIÓN. Serán os protocolos da capa de transporte (TCP) os que se encarguen de solucionar eses incidentes.

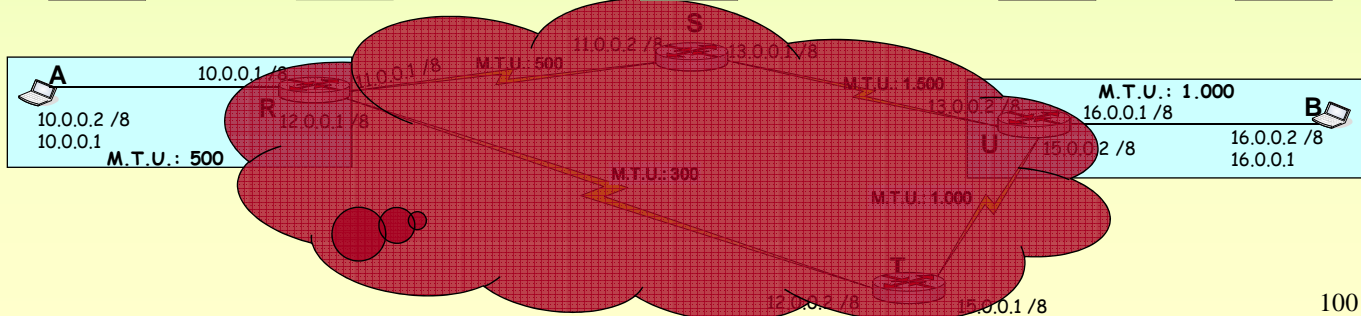
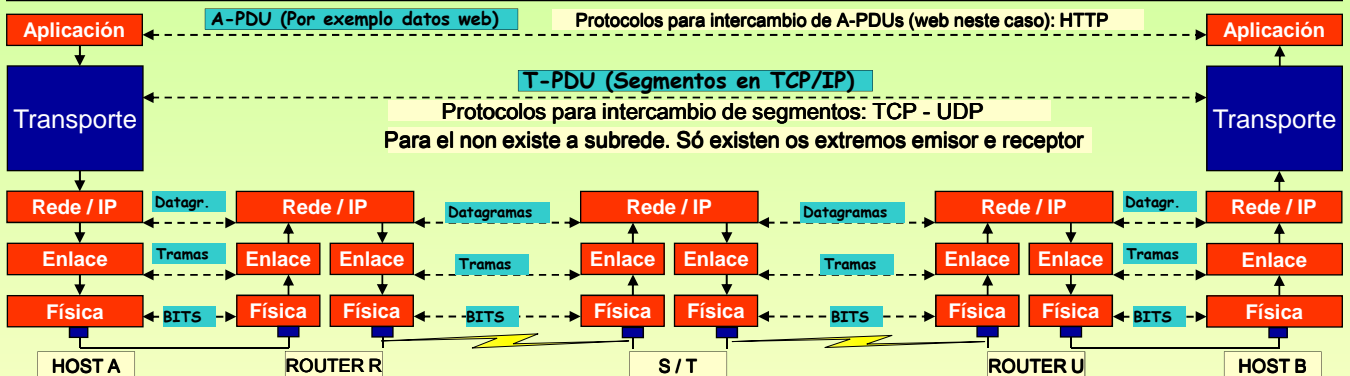


Redes Área Local - OSI - TCP/IP

8.5.- TCP (Transmission Control Protocol)

☞ CAPA DE TRANSPORTE en TCP/IP (TCP - UDP)

É a primeira capa extremo a extremo. Isto é, os protocolos que se establecen nesta capa son entre o extremo EMISOR real e o extremo RECEPTOR real, non entre elementos intermediarios, chamada **Subrede** (routers, switches, hubs, cables, etc.). O nivel de transporte illa a capa de APLICACIÓN da subrede (nivel IP, enlace, fisico). Para o nivel de transporte é como se só existiran os HOSTS extremos (A e B neste caso), non sabe nada de fragmentación, routers, MTU, hubs...



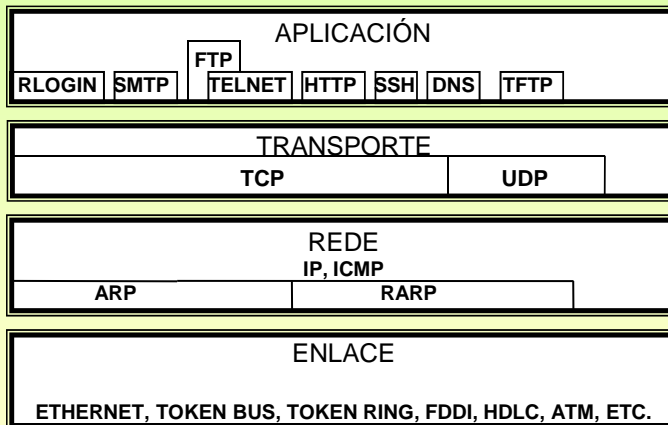
Redes Área Local - OSI – TCP/IP

8.5.- TCP (Transmission Control Protocol)

CAPA DE TRANSPORTE en TCP/IP (TCP - UDP)

No seguinte modelo de capas amósase unha síntese dos protocolos que hai en cada nivel. Obsérvese como hai protocolos de aplicación que só usan TCP, outros UDP e outros os 2. Pode haber aplicacións que se salten a capa de transporte, por exemplo o comando **Ping**. A capa de transporte "*transporta*" os datos independentemente das redes subxacentes.

TCP: Transmission Control Protocol, é un protocolo orientado á conexión. (Sistema telefónico)
UDP: User Data Protocol, é un protocolo non orientado á conexión. (Sistema postal)



Redes Área Local - OSI – TCP/IP

8.5.- TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) (I)

PORTO: Son os enderezos do nivel de transporte. Son os SAP (Puntos de acceso ó servizo) entre as aplicacións e o TCP/UDP. Cada porto está asociado a unha aplicación. Os portos pódense asignar de dous xeitos:

APLICACIÓN CLIENTE: Cando se abre unha aplicación o SO asínalles un porto dos que teña libres. (Exemplo: navegador web, cliente ftp, etc)
APLICACIÓN SERVIDOR: As aplicacións servidor están sempre escoitando nun porto chamado **BEN COÑECIDO**. Este porto é configurado manualmente. Exemplos **PORTOS BEN COÑECIDOS:**

- | | | | |
|-----------------|-----------------|-----------------|----------------------|
| 80 Servidor Web | 21 Servidor FTP | 23 Telnet | 22 SSH |
| 13 Hora / Día | 25 SMTP | 53 Servidor DNS | 3389 Terminal Server |

EXEMPLO: Un usuario fai dobre clic sobre o navegador web, nese intre o Sistema Operativo (SO) asínalles un porto a esa aplicación (1500). A aplicación cliente sabe en que porto está escoitando a **Aplicación Servidor** as peticións (neste caso no 80). Se a aplicación servidor está escoitando nun porto distinto ó que lle corresponde, o usuario debe expresar cal é ese porto. (ex. :81)

PUNTO EXTREMO: o par formado por (IP, PORTO), por exemplo: (20.0.0.3, 1500)
CONEXIÓN: circuito virtual entre dous programas, isto é, un par de puntos extremos. Así podemos abrir varias aplic. nun HOST
Conexión 1: (20.0.0.3, 1500) – (213.4.130.50, 80) **Conexión 2:** (20.0.0.3, 1501) – (213.4.130.50, 80)



8.5.- TCP (Transmission Control Protocol)

☞ TCP (Transmission Control Protocol) (II)

ORIENTADO A CONEXIÓN: Para realizar unha comunicación entre dous puntos extremos, débese:

- 1º **Establecer** a conexión (O cliente solicita ó servidor que quere comunicarse con el)
- 2º Unha vez establecida a conexión realízase o **intercambio** de información.
- 3º Finalizado ó intercambio, **libérase** a conexión.

- ASENTIMIENTO:** **Acuse de recibo**, segmento que envía o receptor ó emisor para informalo de se recibiu correcta (ACK) ou incorrectamente (NACK) o que o emisor enviou.
- FULL-DÚPLEX:** Permite os dous extremos enviar información nos dous sentidos simultaneamente. Usa para iso o protocolo de ventá deslizante que se verá máis adiante.
- PIGGY BACKING:** Os segmentos con asentimentos que envía o receptor poden levar ademais datos do receptor cara ó emisor.
- FIABLE:** Proporciona comunicación extremo a extremo de tal xeito que lle ofrece ás aplicacións unha conexión libre de erros. Para iso úsase o protocolo de ventá deslizante. Lémbrese que o nivel IP non garante que cheguen os datagrama, nin que cheguen ordenados. É o TCP que se encarga de solucionar estes problemas.
- CONTROL DE FLUXO:** O emisor debe enviar datos adaptándose á velocidade do receptor para procesalos/aceptalos. Unha das funcións do nivel 2 (enlace) do modelo de referencia OSI é o Control de Fluxo, pero nese caso ese control dáse entre os elementos que compoñen a subrede, non entre o emisor e o receptor real. No nivel de transporte tamén se realiza este control, pero entre o emisor e o receptor real. No caso do TCP úsase o protocolo de ventá deslizante para levar a cabo esta función.
- TEMPORIZADORES:** O emisor habilita temporizadores para cada segmento que envía se non recibe unha confirmación do receptor antes de que remate o temporizador volve a retransmitir o mesmo segmento.
- MSS:** **Maximun Segment Size:** (Tamaño do campo de datos do segmento). Cando se establece a conexión entre dous extremos négóciase o tamaño do segmento. O tamaño do segmento deberá ser aquel, que cando se pase este ó nivel de rede, para ir no campo de datos dun datagrama, non provocara a fragmentación do datagrama.
- Isto é, debería ir en relación á MTU da rede, co cal, cando se establece a conexión, o nivel TCP trata de averiguar a MTU da rede, e deste xeito calcula o MSS (restar cabeceira segmento e cabeceira datagrama, como mínimo 40 bytes, 20 de cada cabeza). Distínguense dous casos:
- **OS EXTREMOS ESTÁN NUNHA LAN:** a MTU pódese averiguar facilmente pois é a mesma de orixe a destino.
 - **OS EXTREMOS ESTÁN EN REDES DISTINTAS:** a MTU é difícil de averiguar, pois no nivel 3 existen routers que poden realizar encamiñamentos dinámicos, o que implica que unhas rotas terán unha MTU e outras terán outra.

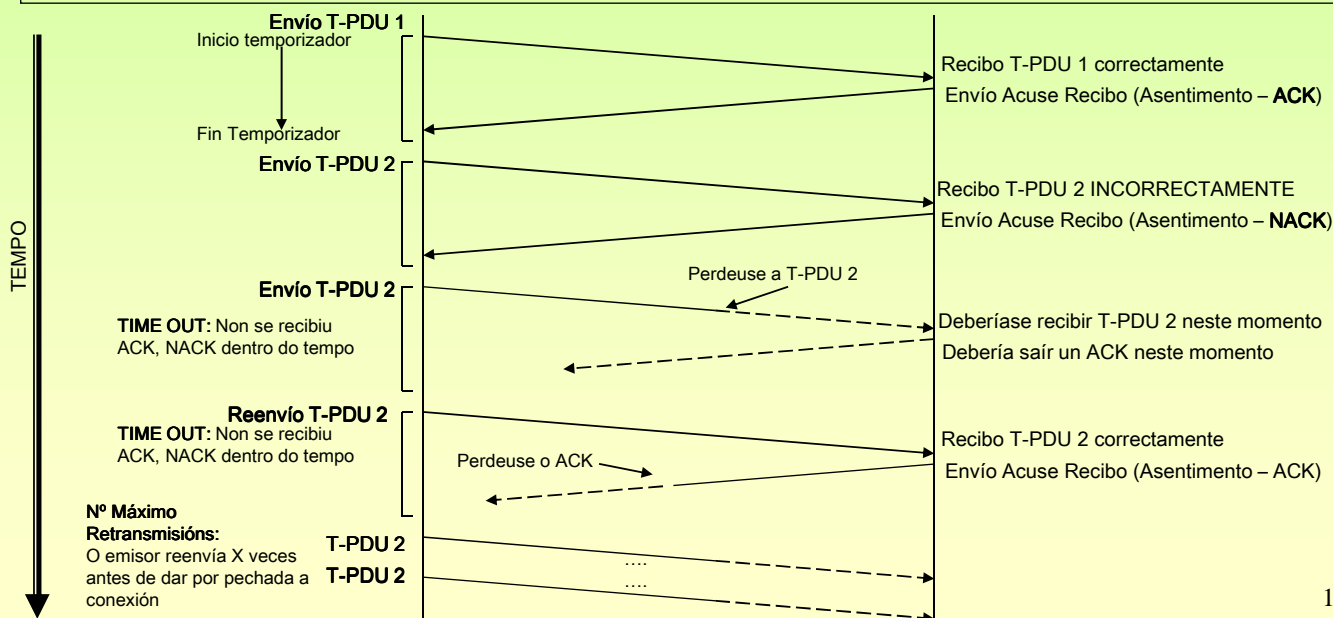
8.6.- TCP – Control de fluxo

☞ CONTROL DE FLUXO – Técnica: Envío - Espera

Tanto no envío de Tramas (nivel 2) como no envío de segmentos, realízase o control de fluxo. No primeiro caso entre os IPMs que compoñen a subrede e no segundo entre o emisor e o receptor finais.

A técnica de **ENVÍO E ESPERA** consiste en enviar un bloque de información e esperar a que o receptor envíe un acuse de recibo. Mentres non se reciba ese acuse de recibo positivo non se enviará o seguinte bloque de información.

- TEMPORIZADOR:** o emisor ó enviar un bloque de información abre un temporizador dentro do cal debe recibir un acuse de recibo. indica que expirou o temporizador. Cando se trata de conectar a unha páxina e pasado un tempo dá erro.
- TIME OUT:** Non se recibiu ACK, NACK dentro do tempo
- Nº MAX. RETRANSMIS.:** o emisor envía un mesmo bloque de información nun número máximo de X veces. Se se acaba péchase a conexión



8.6.- TCP – Control de fluxo

CONTROL DE FLUXO - Técnica: VENTÁ ESVARADÍA (DESLIZANTE)

O protocolo usa a TÉCNICA DE VENTÁ DESLIZANTE CON REXEITE SELECTIVO.

O protocolo de ventá deslizante consiste en establecer límite no números de bloques de información que o emisor pode enviar sen recibir acuse de recibo deles.

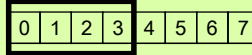
Cada bloque de información ten o seguinte formato: I XY

I= Información X: Número de bloque que se envía

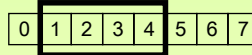
Y: N° de bloque que se espera, co cal recibiu os Y-1 bloques OK.

EXEMPLO: un emisor ten que enviar 8 bloques de información (0-7) e establécese unha ventá de tamaño 4 bloques.

Pode enviar os bloques 0, 1, 2 e 3 sen esperar por asentimento



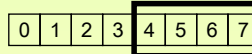
Ó recibir o asentimento do bloque 0, desliza a ventá



Non pode enviar máis bloques pois chegou ó limite da ventá



Recibe o asentimento dos bloques 1,2,3 → desliza a ventá

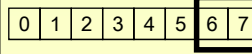


Recibe o asentimento dos bloques 4 e 5 → deslízase a ventá
Pero xa se enviarán 6 e 7. O receptor informa que os bloques anteriores o 6 foron recibidos correctamente.

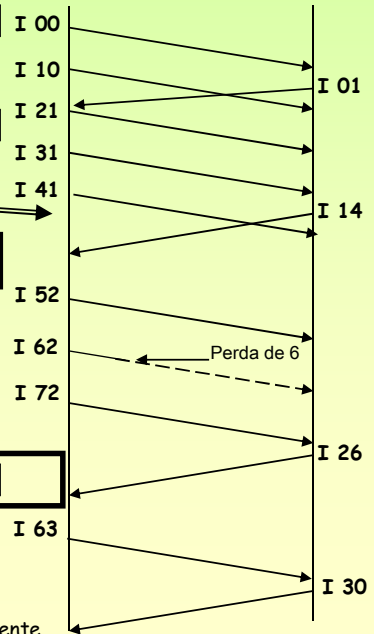
O emisor á vista do problema pode usar:

REXEITE SIMPLE: enviar todo dende o bloque errado. (6 e 7)

REXEITE SELECTIVO: enviar só o bloque errado (6)



O emisor dáse por avisado de que todo o enviado foi recibido correctamente



8.6.- TCP – Control de fluxo

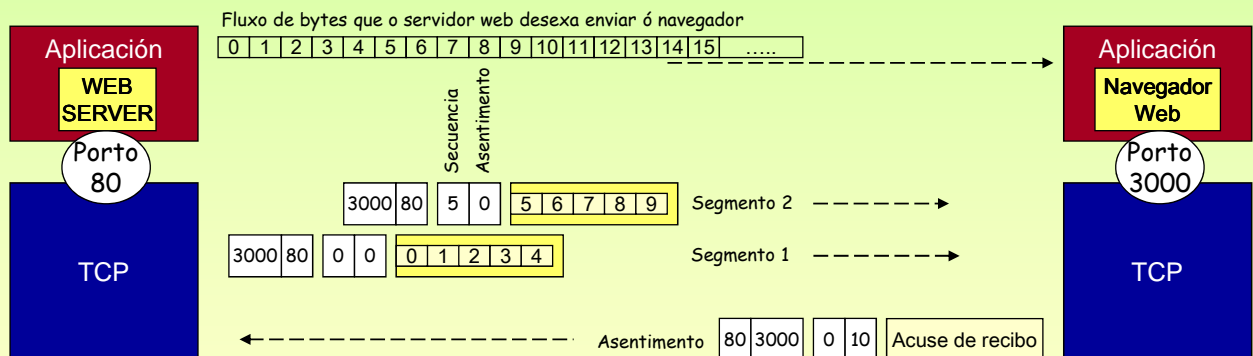
TCP e a Ventá deslizante

O tamaño da ventá deslizante en TCP mídese en bytes, isto é, cantos bytes se van poder enviar sen estar pendente do acuse de recibo.

Cando se envía un segmento o primeiro byte do campo de datos correspóndese cun número de byte do fluxo de bytes que se desexa intercambiar co receptor no nivel de aplicación.

EXEMPLO: Datos: MSS → 5, TAMAÑO DA VENTÁ → 10 bytes.

Construír os segmentos necesarios ata o primeiro acuse de recibo.



FIABILIDADE

O software TCP emisor non se desfai dos bytes enviados ata que reciba o asentimento do receptor.

O emisor xestiona temporizadores para cada segmento enviado. No caso de que se perda algún segmento ou se perda un acuse de recibo o temporizador expirará e volverá a retransmitir o segmento errado.

Se o receptor recibe segmentos duplicados vaise decatar, pois cada segmento vai numerado.

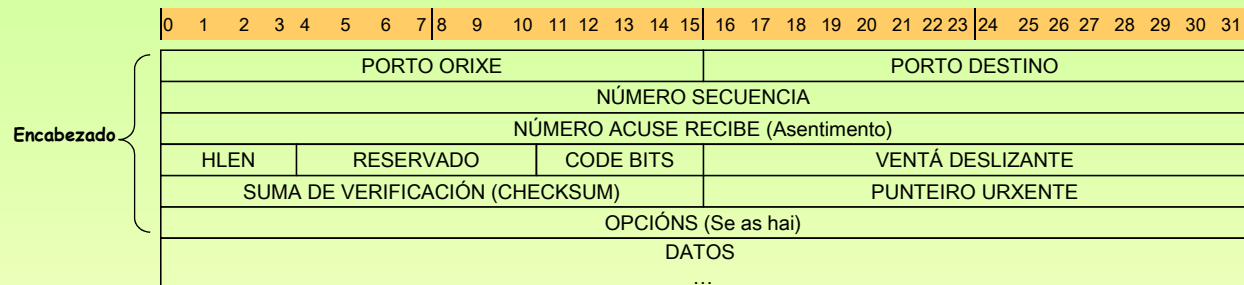
Deste xeito o nivel TCP é independente do IP, pois se este perde fragmentos, datagramas enteiros ou estes chegan con erros, ó non subir nada ó nivel TCP, este vaise decatar de que algo anormal está a pasar.

8.6.- TCP – Segmento

☞ TCP (Transmission Control Protocol) Formato do segmento (I)

Os segmentos intercámbianse para establecer conexións, transferir datos, enviar acusos de recibo (asentimentos), indicar o tamaño da ventá deslizable e pechar as conexións:

Un acuse de recibo que vaia do HOST A ó B, pode levar datos de A a B.



☞ Algúns campos do segmento.

PORTO: Contéñen os números de porto TCP que identifican as dúas aplicacións dunha conexión.

HLEN: Número enteiro que indica o tamaño da cabeceira medida en palabras de 32 bits (1 liña). Sen opcións: HLEN =5 → 20 bytes.

RESERV.: Reservado para uso futuro

CODE BITS: Pode tomar varios valores, entre eles destacamos:

FIN: indica que é o último segmento dunha restra.

URG: indica que o campo punteiro urxente é válido.

RST: iniciación da conexión.

CHECKSUM.: úsase para o control de erros en TCP, para o seu cálculo inclúese a cabeceira e os datos.

P. URXENTE: Aínda que a información debe ser procesada no receptor na mesma orde na que saíu, ás veces é preciso que o programa dun extremo envíe datos *fora de banda* sen esperar a que o programa do outro lado procese tódolos bytes que aínda están en fluxo. Supóñase que dende un extremo se desexa abortar ou interromper a execución do programa do outro lado. Esa sinal debe saltar todo o fluxo de datos. Exemplo: cando visitamos unha páxina prememos STOP antes de que se remate de cargala.

OPCIÓN: cando se establece unha conexión entre dous extremos négóciase o MSS (tamaño do segmento). O software TCP usa este campo para realizar esta negociación.

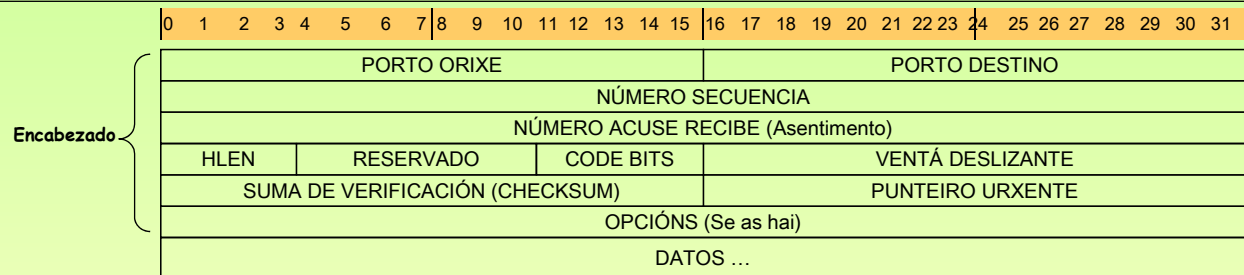
107

8.6.- TCP – Segmento

☞ TCP (Transmission Control Protocol) Formato do segmento (II)

Os segmentos intercámbianse para establecer conexións, transferir datos, enviar acusos de recibo (asentimentos), indicar o tamaño da ventá deslizable e pechar as conexións:

Un acuse de recibo que vaia do HOST A ó B, pode levar datos de A a B.



☞ Os restantes campos do segmento.

VENTÁ: En cada acuse de recibo que o receptor lle envía ó emisor, infórmao de cantos bytes máis está disposto a recibir, co cal o tamaño da ventá é dinámico e vaise adaptando á dispoñibilidade de memoria do receptor.

Cando o receptor envía este campo cun valor 0, estalle indicando ó emisor que se deteña ata nova orde.

Nº SECUENCIA: O emisor informa ó receptor que byte ocupa o primeiro byte do campo de datos dentro do fluxo de datos que está enviando unha aplicación a outra.

ORDE: ó ir tódolos segmentos numerados, pódese entregar a información á aplicación do HOST receptor na mesma orde en que foron enviados pola aplicación do HOST emisor, aínda que estes foran entregados polo nivel IP do receptor en desorde.

Hai que ter en conta que eses segmentos que chegaron ó TCP receptor puideron ir no nivel IP por rotas distintas, xa que no nivel IP os datagramas son encamiñados dinamicamente.

Nº ASENTIMENTO: O receptor informa ó emisor cal é o seguinte byte polo que está a esperar, confirmándolle así o emisor, que todo o enviado ata ese byte - 1 foi recibido correctamente.

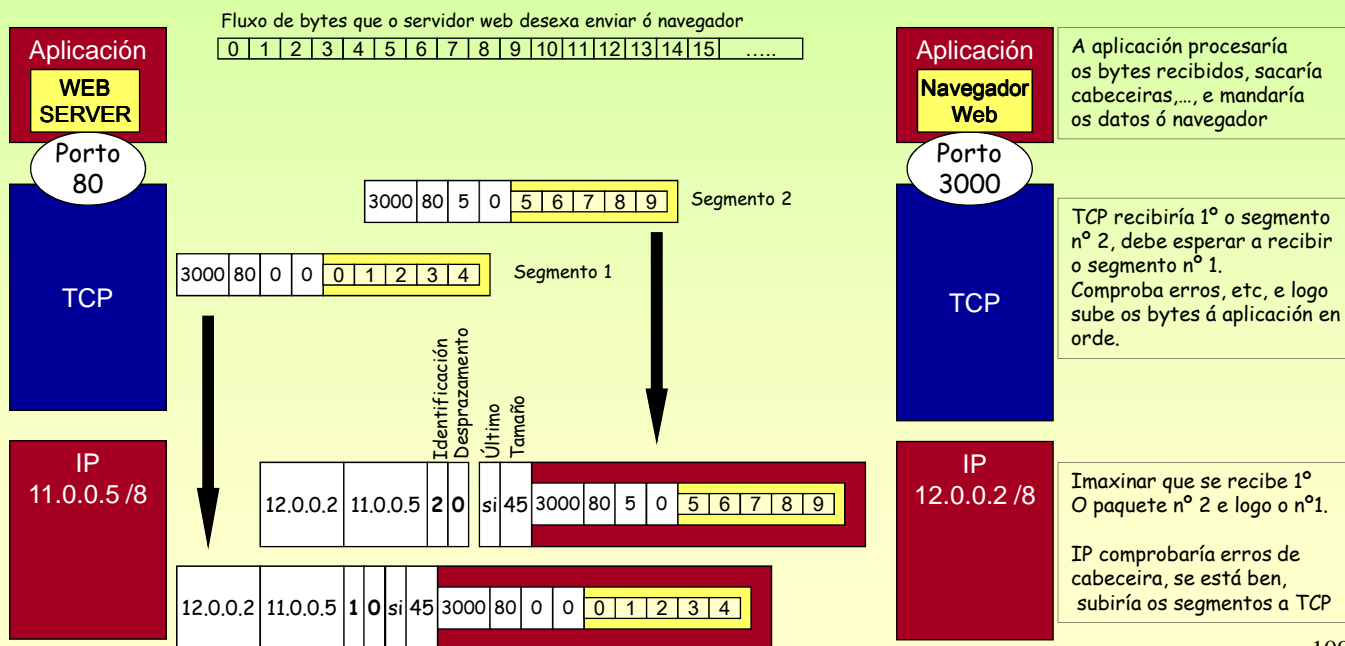
108

8.7.- Relación entre TCP/IP

☞ **A relación entre as tres capas: Aplicación, TCP, IP**

EXEMPLO: Dados: MSS → 5, TAMAÑO DA VENTÁ → 10 bytes.

Construír os segmentos e datagramas necesarios ata o primeiro acuse de recibo. Fixarse no campo identificación do datagrama.
 NOTA: Os enderezos están: 1º o destino e logo a orixe.



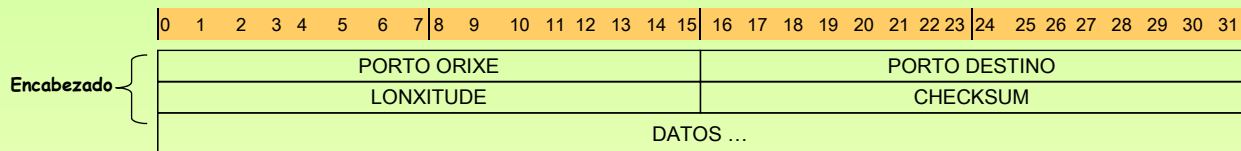
8.8.- UDP (Unit Data of Protocol)

☞ **UDP (Unidade de Datos do Protocolo).**

É o protocolo da capa de transporte NON ORIENTADO Á CONEXIÓN.

A diferenza do TCP non é fiable, non garante que os datos se entreguen en orde nin que se recupere de erros.

En consecuencia, é rápido pero inseguro.



8.9.- Comandos TCP

```

C:\WINDOWS\System32\cmd.exe
L:\>netstat -?

Muestra estadísticas del protocolo y conexiones TCP/IP actuales.

NETSTAT [-al [-e] [-n] [-o] [-s] [-p proto] [-r] [intervalo]

-a Muestra todas las conexiones y puertos de escucha.
  <Normalmente, el extremo servidor de las conexiones no se muestra>.
-e Muestra estadísticas Ethernet. Se puede combinar con la opción -s.
-n Muestra números de puertos y direcciones en formato numérico.
-o Muestra la Id. de proceso asociado con cada conexión.
-p proto Muestra conexiones de protocolo que puede ser TCP, UDP,
  -s para mostrar estadísticas de protocolo que puede ser TCP, UDP,
  TCPv6 o UDPv6.
-r Muestra el contenido de la tabla de enrutamiento.
-s Muestra estadísticas de protocolo.
    
```



```

C:\WINDOWS\System32\cmd.exe
L:\>netstat -n

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP BARRIOESAMO:4446 10.0.0.35:microsoft-ds ESTABLISHED
TCP BARRIOESAMO:4691 10.0.0.6:microsoft-ds ESTABLISHED
TCP BARRIOESAMO:4944 www.terra.es:http TIME_WAIT
TCP BARRIOESAMO:4945 www.terra.es:http TIME_WAIT
TCP BARRIOESAMO:4955 10.0.0.35:microsoft-ds TIME_WAIT
    
```



```

C:\WINDOWS\System32\cmd.exe
L:\>netstat -n

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 10.0.0.5:4446 10.0.0.35:445 ESTABLISHED
TCP 10.0.0.5:4691 10.0.0.6:445 ESTABLISHED
TCP 10.0.0.5:4958 213.4.130.50:80 ESTABLISHED
TCP 10.0.0.5:4959 213.4.130.210:80 TIME_WAIT
TCP 10.0.0.5:4960 213.4.130.210:80 ESTABLISHED
TCP 10.0.0.5:4961 195.22.198.32:80 ESTABLISHED
TCP 10.0.0.5:4962 209.202.249.250:80 ESTABLISHED
TCP 10.0.0.5:4963 213.4.130.210:80 ESTABLISHED
TCP 10.0.0.5:4964 213.4.130.210:80 TIME_WAIT
TCP 10.0.0.5:4965 213.4.130.50:80 ESTABLISHED
TCP 10.0.0.5:4966 213.4.130.50:80 ESTABLISHED
TCP 10.0.0.5:4967 213.4.130.50:80 ESTABLISHED
TCP 10.0.0.5:4968 213.86.246.154:80 ESTABLISHED
TCP 10.0.0.5:4971 213.86.246.154:80 ESTABLISHED
TCP 10.0.0.5:4972 64.237.51.161:80 ESTABLISHED
TCP 10.0.0.5:4973 213.4.130.210:80 ESTABLISHED
TCP 10.0.0.5:4974 213.4.130.210:80 ESTABLISHED
TCP 10.0.0.5:4975 200.16.144.230:80 ESTABLISHED
TCP 10.0.0.5:4976 213.4.130.210:80 ESTABLISHED
TCP 10.0.0.5:4977 213.4.130.210:80 ESTABLISHED
    
```

COMANDOS
Windows: netstat

8.9.- Comandos TCP

```

[root@linuxp root]# netstat --help
usage: netstat [-veenNcCF] [{<Af>}] -r netstat {-V|--version|-h|--help}
netstat [-vnNcaeoI] [{<Socket>} ...]
netstat { [-veenNac] -i | [-cnNe] -M | -s }

-r, --route display routing table
-i, --interfaces display interface table
-g, --groups display multicast group memberships
-s, --statistics display networking statistics (like SNMP)
-M, --masquerade display masqueraded connections

-v, --verbose be verbose
-n, --numeric don't resolve names
--numeric-hosts don't resolve host names
--numeric-ports don't resolve port names
--numeric-users don't resolve user names
-N, --symbolic resolve hardware names
-e, --extend display other/more information
-p, --programs display PID/Program name for sockets
-c, --continuous continuous listing

-l, --listening display listening server sockets
-a, --all, --listening display all sockets (default: connected)
-o, --timers display timers
-F, --fib display Forwarding Information Base (default)
-C, --cache display routing cache instead of FIB

<Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
<AF>=Use -A <af> or --<af>; default: inet
List of possible address families (which support routing):
inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
    
```

COMANDOS
Linux: netstat

Como se pode observar este comando serve para máis cousas que para ver as conexións TCP.

8.9.- Comandos TCP

```

Sesión  Editar  Vista  Marcadores  Preferencias  Ayuda
[root@linuxp root]# netstat Socket -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 linuxp:postgres        linuxp:34324            ESTABLISHED
tcp        0      0 linuxp:postgres        linuxp:34323            ESTABLISHED
tcp        351    0 linuxp:37063            10.0.0.35:netbios-ssn  ESTABLISHED
tcp        0      0 linuxp:37085            10.0.0.35:microsoft-ds ESTABLISHED
tcp        0      0 linuxp:33431            10.0.0.35:microsoft-ds ESTABLISHED
tcp        0      0 linuxp:32769            10.0.0.35:microsoft-ds ESTABLISHED
tcp        0      0 linuxp:37304            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37305            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37297            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37298            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37299            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37300            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37301            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37302            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:37303            carpanta, rede, usc. :http TIME_WAIT
tcp        0      0 linuxp:34323            linuxp:postgres        ESTABLISHED
tcp        0      0 linuxp:34324            linuxp:postgres        ESTABLISHED
tcp        0      0 linuxp:37204            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37202            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37200            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37201            10.0.0.5:x11           ESTABLISHED
tcp        0      1204 linuxp:37198            10.0.0.5:x11           ESTABLISHED
tcp        64     0 linuxp:37199            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37196            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37197            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37195            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37192            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37193            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37189            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37187            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:37167            10.0.0.5:x11           ESTABLISHED
tcp        0      0 linuxp:33251            10.0.0.38:netbios-ssn  ESTABLISHED
tcp        0      0 linuxp:37285            prscl2.40.xunta.es:http TIME_WAIT

```

COMANDOS

Linux: netstat

Os estados das conexións tanto en Linux como en Windows, poden ser, entre outros:

```

CLOSE_WAIT
CLOSED
ESTABLISHED
FIN_WAIT_1
FIN_WAIT_2
LAST_ACK
LISTEN
SYN_RECEIVED
SYN_SEND
TIME_WAIT

```

Para coñecer o seu significado recoméndase consultar o:

RFC 793

Onde se especifica o TCP.
www.ietf.org

9.- DNS (Domain Name Service)

SISTEMA DE NOMES DE DOMINIOS (DNS).

Pero, ¡¡¡¡Os humanos non traballan directamente con IPs!!!!

DNS deseñouse a comezos dos 80 en 1984 escolleuse como estándar **para asociar IPs a Nomes**.

Antes de que Internet cambiase a DNS existía un único arquivo (Hosts) que se enviaba a través de FTP a quen quixese converter IPs a nomes. Cada cambio implicaba a modificación do arquivo e volvelo a distribuír.

DNS mantén unha base de datos nun servidor ó cal preguntan aqueles que desexen achar a IP asociada a un nome de dominio.

Espacio de nomes.

Describe a estrutura en forma de árbore de todos os dominios dende a raíz (“.”, punto) ata o nivel inferior da estrutura. A estrutura é xerárquica e cada nivel sepárase do superior por un punto “.”

Dominios de primeiro nivel.

Son os dominios que se atopan xusto debaixo do dominio raíz “.”. Estes divídense en dous tipos:

Dominios Organizativos: Creados inicialmente para organizar o Internet en EE.UU.

- .COM: inicialmente era para empresas, hoxe está aberto a calquera cousa.
- .NET: inicialmente era para empresas e organismos relacionados coa Rede, hoxe ...
- .ORG: inicialmente era para organismos de EE.UU. sen ánimo de lucro, hoxe ...
- .MIL: inicialmente era para organismos militares de EE.UU. e hoxe séguese sendo.
- .EDU: inicialmente era para universidades de EE.UU. e hoxe séguese sendo.
- .GOV: é para organismos relacionados co goberno de EE.UU. e hoxe séguese sendo.
- .INT: é para organismos internacionais, p.e. www.eu.int (Portal da Unión Europea)

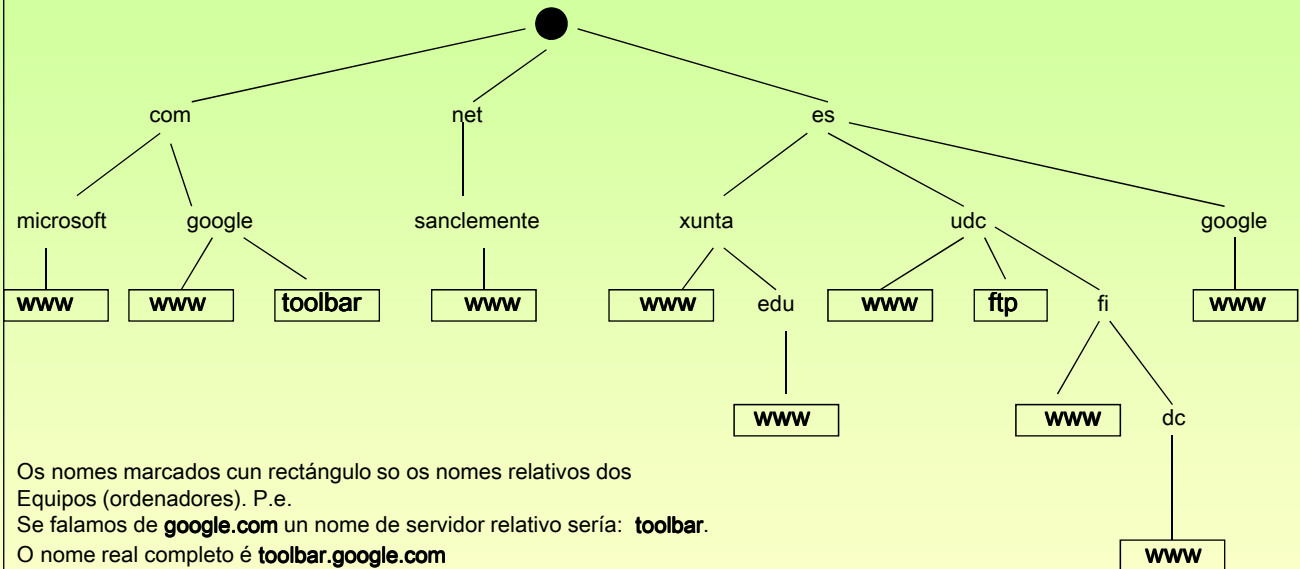
Dominios xeográficos: xurdiron cando o Internet se expandiu alén dos EE.UU.

- .ES España. Non fixo control sobre os dominios secundarios.
- .UK Reino Unido. Fixo control sobre os dominios secundarios. P.e. co.uk, gov.uk, org.uk
- .BR Brasil. Fixo o mesmo que os ingleses
- .DE Alemaña
- .PT Portugal

Dominios de recente creación: .tv, .mail, .info, .museum. En www.internic.net ou en www.icann.org están todos.

9.- DNS (Domain Name Service)

SISTEMA DE NOMES DE DOMINIOS (DNS). Estructura.



Os nomes marcados cun rectángulo so os nomes relativos dos Equipos (ordenadores). P.e.
 Se falamos de **google.com** un nome de servidor relativo sería: **toolbar**.
 O nome real completo é **toolbar.google.com**

Consideracións p.e. do dominio da xunta.

- xunta.es → é un dominio, e ó mesmo tempo **xunta** é un subdominio de **.es**
- edu.xunta.es → é un dominio, e ó mesmo tempo **edu** é un subdominio de **xunta.es**
- www.xunta.es → é o equipo **www** dentro do dominio **xunta.es**
- www.edu.xunta.es → é o equipo **www** dentro do dominio **edu.xunta.es**
- Toolbar.google.com → é o equipo **toolbar** dentro do dominio **google.com**

9.- DNS (Domain Name Service)

Configuración DNS (Domain Name System)

Pero, ¡!!!Os humanos non traballan directamente con IPs!!!!

Ese problema resólvese con nomes de dominio do estilo www.iessanclemente.net, www.terra.es, www.edu.xunta.es

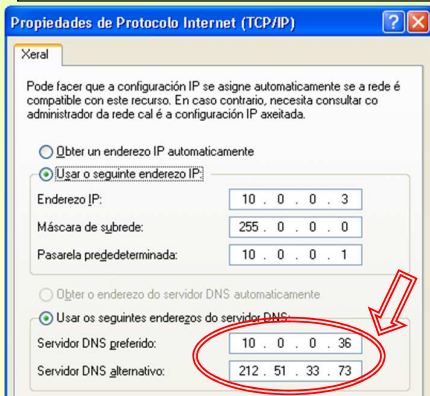
Anoxía con sistema telefónico: Unha persoa pode saber uns cantos números de teléfono, pero se descoñece algún pode chamar ó 11811 para preguntar polo número dun abonado, pero se este número non funciona ou está ocupado podes chamar a outro 11824.

En TCP/IP existe o Servidor de Nomes de Dominio (DNS) que ten unha IP á cal os clientes DNS poden preguntarlle cal é a IP asignada a un nome de dominio.

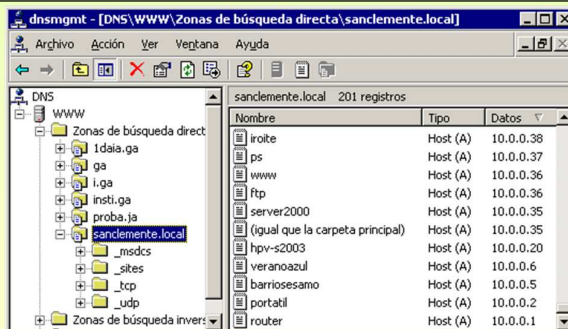
Os clientes configúranse indicando a IP do servidor de DNS que pode resolver as súas consultas.

- Servidor DNS primario, preferido, etc:** É ó 1º servidor ó que se lle vai consultar se fallase consultaríase a:
- Servidor DNS secundario, alternativo:** Este servidor é consultado no caso de que falle o primeiro.

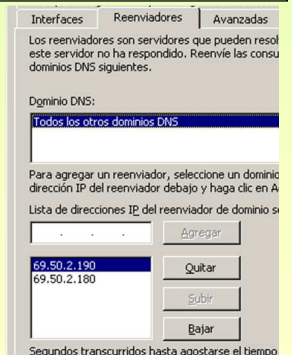
Os servidores DNS non saben tódalas IPs e nomes de dominio existentes. Estes organizanse en forma de árbore, de tal xeito que se un servidor de DNS non é capaz de resolver un nome de dominio este **REENVÍA** a pregunta a outro servidor de DNS ou usa **RECURSIVIDADE** ata atopar o nome de dominio ou obter unha resposta negativa.



Configuración cliente DNS



10.0.0.36. Configuración server DNS. Zonas e equipos



Configuración server DNS. Reenviador

9.- DNS (Domain Name Service)

PING (ICMP)

Comando que axuda a comprobar a conectividade no nivel IP, esto é, comprobar que dous HOSTs se poidan conectar. Para elo precisa coñecer a IP do destinatario.

Se se especifica un nome de dominio o ping encárgase de averiguar a IP usando o proceso de consultas DNS. Obsérvese os seguintes exemplos:

```

C:\>ping

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
        [-r cuenta] [-s cuenta] [-j lista-host] [-k lista-host]
        [-w tiempo de espera] [-R] [-S srcaddr] [-4] [-6] nombre-destino

Opciones:
-t          Ping el host especificado hasta que se pare.
            Para ver estadísticas y continuar - presionar
            Control-Interr.
-a          Parar - presionar Control-C.
            Resolver direcciones en nombres de host.
-n cuenta  Número de peticiones eco para enviar.
-l tamaño  Enviar tamaño del hufer.
-f         Establece No Fragmentar el indicador en paquetes
            (sólo IPv4).
-i TTL     Tiempo de vida.
-v TOS     Tipo de servicio (sólo IPv4).
-r cuenta  Ruta del registro para la cuenta de saltos (sólo IPv4).
-s cuenta  Sello de hora para la cuenta de saltos (sólo IPv4).
-j lista-host  Øloja la ruta de origen a lo largo de la lista-host
            (sólo IPv4).
-k lista-host  Restringir la ruta de origen a lo largo de la
            lista-host (sólo IPv4).
-w tiempo de espera  Tiempo de espera en milisegundos para esperar cada
            respuesta.
-R         Seguir la ruta de retorno (sólo IPv6).
-S srcaddr  Dirección de origen para utilizar (sólo IPv4).
-4         Forzar usando IPv4.
-6         Forzar usando IPv6.
    
```

```

C:\>ping 10.0.0.1

Haciendo ping a 10.0.0.1 con 32 bytes de datos:
Respuesta desde 10.0.0.1: bytes=32 tiempo=19ms TTL=255
Respuesta desde 10.0.0.1: bytes=32 tiempo=15ms TTL=255
Respuesta desde 10.0.0.1: bytes=32 tiempo=3ms TTL=255
Respuesta desde 10.0.0.1: bytes=32 tiempo=7ms TTL=255

Estadísticas de ping para 10.0.0.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempo aproximados de ida y vuelta en milisegundos:
Mínimo = 3ms, Máximo = 19ms, Media = 11ms
    
```

```

C:\>ping www.terra.es

Haciendo ping a www.terra.es [213.4.130.210] con 32 bytes de
datos:
Respuesta desde 213.4.130.210: bytes=32 tiempo=59ms TTL=118
Respuesta desde 213.4.130.210: bytes=32 tiempo=52ms TTL=118
Respuesta desde 213.4.130.210: bytes=32 tiempo=47ms TTL=118
Respuesta desde 213.4.130.210: bytes=32 tiempo=48ms TTL=118

Estadísticas de ping para 213.4.130.210:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempo aproximados de ida y vuelta en milisegundos:
Mínimo = 47ms, Máximo = 59ms, Media = 51ms
    
```

```

C:\>ping www.microsoft.com

Haciendo ping a www.microsoft.com.nsatc.net [207.46.245.156]
con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 207.46.245.156:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),
    
```

Ping a unha IP que coñecemos. O respondernos indicanos canto tempo tarda en chegar un PKT. Deste xeito sabemos que 10.0.0.1 is alive

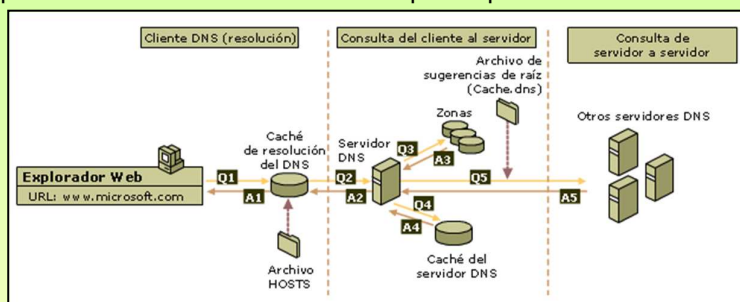
O programa debe averiguar a IP de www.terra.es [está entre corchetes] e logo realiza o "ping". Terra está acendido, respondendo e polos tempos máis lonxe que 10.0.0.1.

O programa averigua a IP e logo realiza o "ping". O host non responde:
A.- Pode ser que estea apagado, ou non que non se pode chegar a el.
B.- Pode estar acendido pero deshabilitada a resposta a pings.

9.- DNS (Domain Name Service)

DNS (Domain Name System)

No seguinte exemplo móstrase como funcionan as consultas DNS. (Tomado da axuda de Windows)
 O proceso de averiguar a IP asociada a un nome de dominio coñéceselle co nome: **Resolución DNS**
 Un ordenador do IES (cliente) fai un ping a **www.microsoft.com**. Para elo débese averiguar a súa IP.
 Neste exemplo só nos interesa que se resolva a consulta DNS non que resposte o servidor.



O cliente DNS dispón de:

Caché DNS: onde se almacena resultados de resolucións previas, incluso as de resultado negativo.

Arquivo HOSTS: está (...system32\drivers\etc\). Mantén asociacións estáticas de Nomes con IPs.

Q1: Cliente DNS consulta a súa cache DNS (xa inclúe os datos do arquivo HOSTS automaticamente) pregunta pola IP de www.microsoft.com.

A1: Se existe entrada devolve a IP senón segue o proceso:

Q2: Pregunta ó servidor de DNS configurado como preferido:

Q3: O servidor de DNS consulta ás súas zonas (Os dominios que xestiona el) (Arquivos *.dns de windows\dns\ do server)

A3: Se Xestiona ese dominio (microsoft.com) e ten ese host (www) devolve a IP ó cliente, senón segue o proceso.

Q4: O servidor de DNS ten almacenada na Caché do Servidor de DNS as resolucións que resolveu previamente.

A4: Se o servidor ten esa entrada na caché devolve a IP ó cliente, senón segue co proceso.

Q5: Se o server DNS non puido resolver, preguntará a outros servidores DNS.

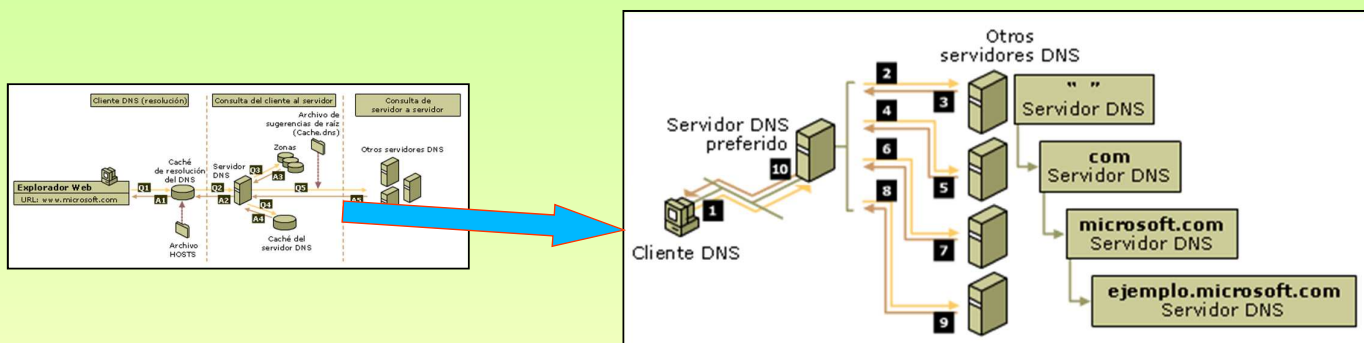
A5: Eses servidores devolverán ó SERVER DNS anterior a IP ou o fallo DNS. O server DNS anterior almacenará na caché o resultado para as futuras peticións que reciba.

A2: Devolve ó cliente o resultado da busca (IP ou Fallo). O cliente almacenará na súa caché o resultado para futuras consultas.

9.- DNS (Domain Name Service)

☞ DNS (Domain Name System) – PROCESO DE RECURSIVIDADE

Cando o **Servidor de DNS preferido** non atopa información nas súas bases de datos locais nin na caché DNS é cando pregunta a outros servidores. Por defecto o servidor de DNS ven configurado cunha lista de servidores raíz (root) os que preguntar para estes casos. Tamén ven, por defecto, activado para usar o **proceso de recursividade**:



- 1.- O cliente desexa comunicarse con **ftp.ejemplo.microsoft.com**. Tras consultar a súa caché pregunta o servidor DNS preferido. O servidor DNS preferido consulta as súas zonas e a súa caché e non pode resolver.

PROCESO DE RECURSIVIDADE.

- 2.- O servidor pregunta a un dos seus servidores raíz(root), ¿Quen é o servidor DNS que xestiona os dominios .COM?
- 3.- O servidor root dálle unha **referencia (IP)** ó servidor DNS que xestiona os .COM. O servidor preferido almacena na caché esa **referencia (IP)** para futuras consultas a un .COM.
- 4.- O servidor preferido pregunta ó servidor de DNS que xestiona as .COM ¿Sabes algo de **MICROSOFT.COM**?
- 5.- O xestor DNS do dominio .COM devólvelle unha **referencia (IP)** ó servidor que xestiona o dominio **MICROSOFT.COM**.
- 6,7.- 8,- Semellante ós pasos anteriores.
- 9.- O servidor DNS **ejemplo.microsoft.com** trata de resolver a IP do host **FTP**. Ben resolva **positivamente** ou **negativamente** informará ó servidor de DNS que fixo a petición do resultado e este almacenarao na súa cache DNS de servidor.
- 10.- Fin da recursividade. O servidor informa ó cliente do resultado e este almacena na cache e actúa en consecuencia.

9.- DNS (Domain Name Service)

☞ DNS (Domain Name System) – REENVÍO – REENVÍO CONDICIONAL

Cando se configura un servidor de DNS pode interesar que este pregunte a outro/s servidor/es de DNS **concreto/s** antes de usar o Proceso de Recursividade.

Observar o seguinte caso:

A Xunta é a Provedora de Servicios de Internet (**ISP**) dos IES. Como tal, ofrécelles dous servidores de DNS os que os clientes dos centros poden facer as súa peticións de Resolución DNS. Estes servidores xestionan o dominio **xunta.es**

Agora ben, o centro ten a súa propia intranet local (p.e. **sanclemente.local**) co seu servidor de DNS local (10.0.0.36). Os clientes do centro preguntan a ese servidor de DNS.

Se o servidor de DNS local está configurado para reenviar as consultas que non poida resolver a eses dous reenviadores.

Deste xeito, un cliente desexa conectarse a **ola.xunta.es** e a **www.microsoft.com**. O proceso é como segue.

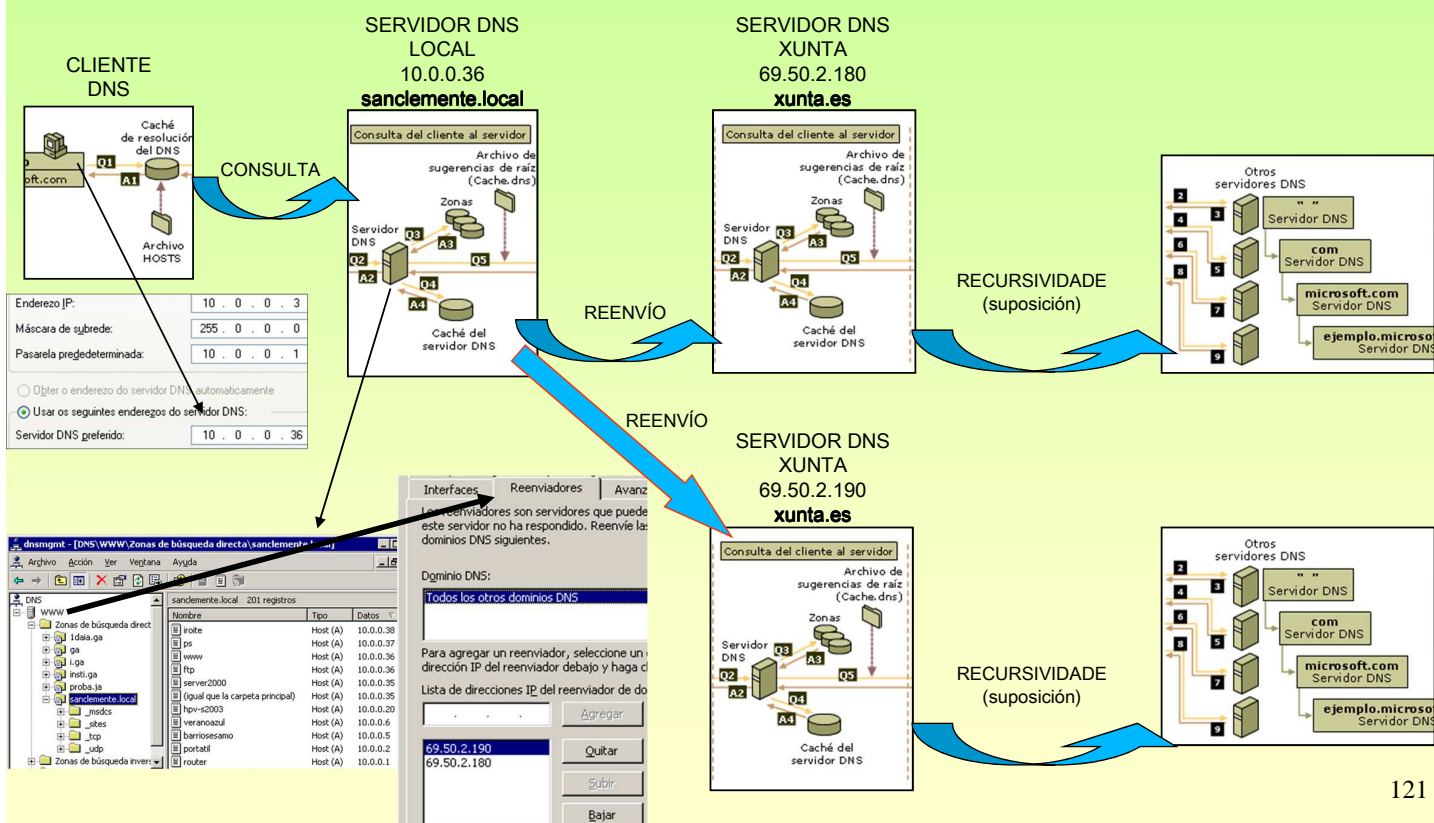
- 1.- O cliente consulta a súa cache local, se non atopa nada reenvía a pregunta o server DNS preferido local.
- 2.- O servidor DNS preferido local, trata de resolver usando as súas bases de datos e a súa cache se non atopa nada preguntará a un servidor DNS da XUNTA.
- 3.- Se o servidor DNS da XUNTA non resposta no tempo establecido preguntárase ó outro reenviador , neste caso tamén da XUNTA.
 - 4.- Cada un deles consultará a súa base de datos (para **ola.xunta.es**), a caché (para **www.microsoft.com**)
 - 4.a.- No caso de **ola.xunta.es** o server da XUNTA devolve ó local que non existe ola.xunta.es.
 - 4.b.- No caso de microsoft se non atopa nada na caché usará reenvío ou recursividade en función de como estea configurado. Unha vez que teña unha resposta almacenaraa na caché e respostaralle ó servidor local
- 5.- O servidor DNS local almacenará na caché as respostas e enviaraas ó cliente.
- 6.- Finalmente o cliente almacenará na cache as respostas e actuará en consecuencia.

REENVÍO CONDICIONAL.

Permite que uns dominios sexan consultados por un reenviador e outros por outro.

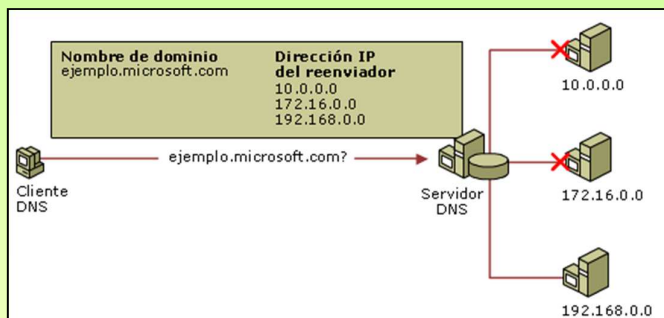
9.- DNS (Domain Name Service)

DNS (Domain Name System) - REENVÍO - REENVÍO CONDICIONAL (II) EJEMPLOS

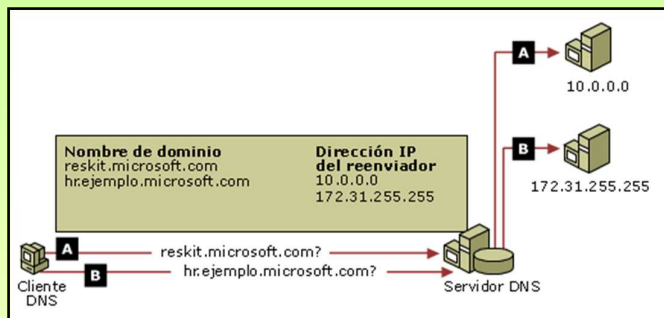


9.- DNS (Domain Name Service)

DNS (Domain Name System) - REENVÍO - REENVÍO CONDICIONAL (III) EJEMPLOS



A este servidor DNS non lle responderon no tempo establecido os dous primeiros reenviadores

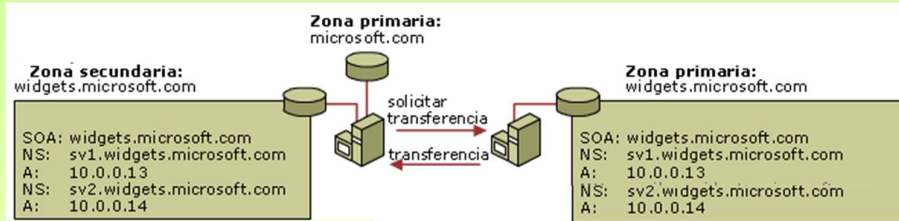


Servidor de reenvío condicional. Un dominio (A) é consultado a un reenviador e o outro dominio (B) a outro reenviador.

9.- DNS (Domain Name Service)

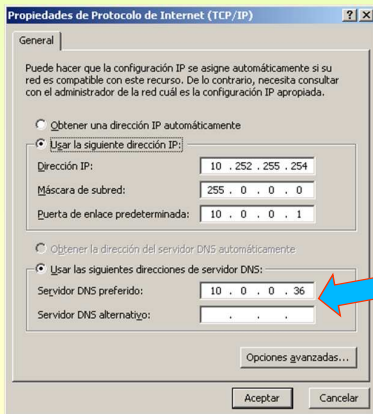
ZONAS SECUNDARIAS

Son copias de respaldo da información que ten unha zona principal. Como no caso anterior da XUNTA que ofertaba dous servidores DNS (primario e secundario)



ACTUALIZACIÓN DUNHA ZONA SECUNDARIA

O servidor secundario envía unha petición principal para pedir permiso par actualizarse, logo pídelles actualización completa (transferir todo de principal a secundario AXFR) ou incremental (IXFR).



Configuración cliente DNS

Pódense especificar varios DNS ós que preguntar.

Se o 1º non responde Pregúntaselle ó segundo, e así sucesivamente.

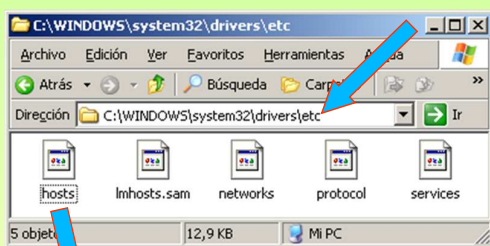
Ata que un deles dea unha resposta ben positiva ben negativa



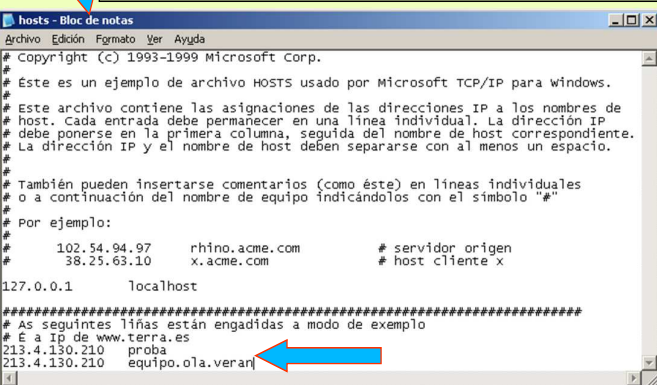
9.- DNS (Domain Name Service)

ARQUIVO HOSTS

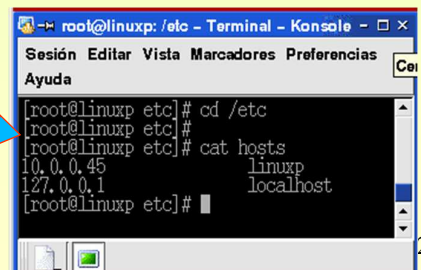
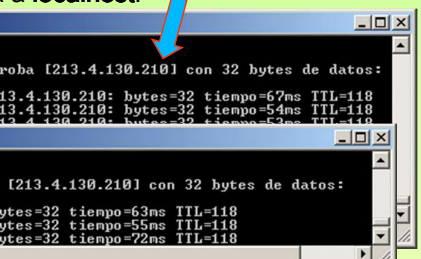
Todo cliente DNS ten un arquivo HOSTS, onde se almacena estaticamente asociacións de de nomes de equipos (con ou sen o dominio) e as súas IPs. Sempre ten a entrada de loopback 127.0.0.1 asociada a localhost.



Engadíronselle dúas entradas o final a modo de exemplo. O resultado é o da dereita. Só modificable por administradores



En Linux /etc/hosts



9.- DNS (Domain Name Service)

COMANDOS: IPCONFIG (WINDOWS) (I)

Mostra os valores da configuración TCP/IP. E actualiza a configuración de DHCP (Dynamic Host Configuration Protocol, que se verá máis adiante) e de DNS.

```

C:\>ipconfig /?

USO:
ipconfig [/? ! /all ! /renew [adapter] ! /release [adapter] !
        /flushdns ! /displaydns ! /registerdns !
        /showclassid adapter !
        /setclassid adapter [classid] ]

donde
adaptador      nombre de conexión
                (se permiten caracteres comodines * y ?, vea los ejemplos)

Opciones:
/?            muestra la ayuda
/all         muestra toda la información de configuración.
/release    libera la dirección IP para el adaptador específico.
/renew      renueva la dirección IP para el adaptador específico.
/flushdns   purga la caché de resolución de DNS.
/registerdns actualiza todas las concesiones y vuelve a registrar los
            nombres DNS.
/displaydns muestra el contenido de la caché de resolución DNS.
/showclassid muestra todas las id. de clase dhcp permitidas para
            este adaptador.
/setclassid modifica la id. de clase dhcp.

De manera predeterminada se muestra solamente la dirección IP, la máscara de
subred y la puerta de enlace para cada adaptador enlazado con TCP/IP.

Para Release y Renew, si no hay ningún nombre de adaptador especificado, se
liberan o renuevan las concesiones de dirección IP enlazadas con TCP/IP.

Para Setclassid, si no hay Classid especificada, se quita Classid.

Ejemplos:
> ipconfig                ... muestra información
> ipconfig /all           ... muestra información detallada
> ipconfig /renew         ... renueva todos los adaptadores
> ipconfig /renew EL*     ... renueva cualquier conexión cuyo nombre
                        comience con EL
> ipconfig /release *Con* ... libera todas las conexiones que coincidan
                        por ejemplo:
                        "Conexión de área local 1" o
                        "Conexión de área local 2"
    
```

```

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /displaydns

Configuración IP de Windows

equipo.ola.veran
-----
Nombre de registro . . : equipo.ola.veran
Tipo de registro . . . : 1
Tiempo de vida . . . . : 565197
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Un registro (host) . . : 213.4.130.210

proba
-----
Nombre de registro . . : proba
Tipo de registro . . . : 1
Tiempo de vida . . . . : 565197
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Un registro (host) . . : 213.4.130.210

localhost
-----
Nombre de registro . . : localhost
Tipo de registro . . . : 1
Tiempo de vida . . . . : 565197
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Un registro (host) . . : 127.0.0.1

www.usc.es
-----
Nombre de registro . . : www.usc.es
Tipo de registro . . . : 5
Tiempo de vida . . . . : 6256
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Registro CNAME. . . . : carpanta.rede.usc.es

www.terra.es
-----
Nombre de registro . . : www.terra.es
Tipo de registro . . . : 1
Tiempo de vida . . . . : 5710
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Un registro (host) . . : 213.4.130.210
    
```

125

9.- DNS (Domain Name Service)

COMANDOS: IPCONFIG (WINDOWS) (II) – BORRADO DA CACHÉ DNS DO CLIENTE

Mostra os valores da configuración TCP/IP. E actualiza a configuración de DHCP (Dynamic Host Configuration Protocol, que se verá máis adiante) e de DNS.

1º Se os datos están no arquivo HOSTS borrando as entradas as dúas entradas anteriores xa non estarán na caché local para a próxima ocasión que se pregunte por elas.

```

hosts - Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-1999 Microsoft Corp.
# Este es un ejemplo de archivo HOSTS usado por Microsoft TCP/IP para windows.
# Este archivo contiene las asignaciones de las direcciones IP a los nombres de
# host. Cada entrada debe permanecer en una línea individual. La dirección IP
# debe ponerse en la primera columna, seguida del nombre de host correspondiente.
# La dirección IP y el nombre de host deben separarse con al menos un espacio.
#
# También pueden insertarse comentarios (como éste) en líneas individuales
# o a continuación del nombre de equipo indicándolos con el símbolo "#"
# Por ejemplo:
#
# 102.54.94.97   rhino.acme.com   # servidor origen
# 38.25.63.10   x.acme.com           # host cliente x
127.0.0.1       localhost
    
```

2º As entradas na caché DNS que proceden do Servidor DNS preferido bórranse co comando `ipconfig /flushdns`

Tras o borrado e actualización do arquivo HOSTS, a caché DNS cliente está como segue.

```

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /flushdns

Configuración IP de Windows

Se vació con éxito la caché de resolución de DNS.

C:\>ipconfig /displaydns

Configuración IP de Windows

1.0.0.127.in-addr.arpa
-----
Nombre de registro . . : 1.0.0.127.in-addr.arpa.
Tipo de registro . . . : 12
Tiempo de vida . . . . : 564086
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Registro PTR. . . . . : localhost

localhost
-----
Nombre de registro . . : localhost
Tipo de registro . . . : 1
Tiempo de vida . . . . : 564086
Longitud de datos . . . : 4
Sección. . . . . : respuesta
Un registro (host) . . : 127.0.0.1
    
```

26

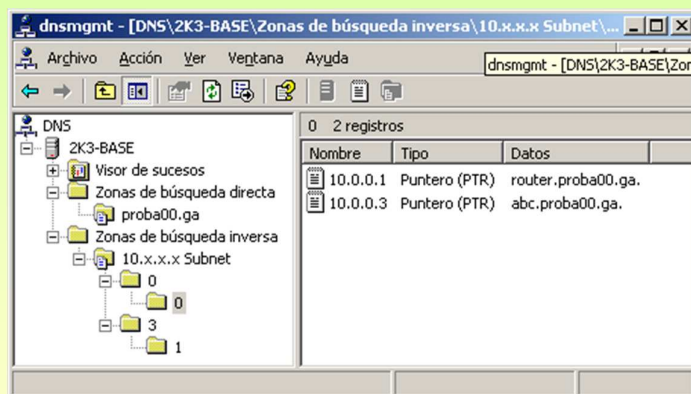
9.- DNS (Domain Name Service)

☞ DNS (Domain Name System) – Zonas de busca INVERSA

Ás veces é interesante dada unha IP averiguar cal é nome de dominio que ten asignado.

Esto é útil cando se ten un conflito IP (máis dunha máquina coa mesma IP) e se desexa averiguar quen é o causante. Pódese desconectar un dos implicados, faise un ping -a <IP en conflito> e saberase o nome douto dos afectados.

Para elo é preciso dar de alta unha Zoa de Busca Inversa no servidor DNS que teña asociadas IPs a Nomes.



9.- DNS (Domain Name Service)

☞ DNS (Domain Name System) – NSLOOKUP

Mostra información sobre a infraestrutura dun servidor DNS

Iniciamos a aplicación Nome e IP do servidor DNS que vai realizar as resolucións .	→	C:\WINDOWS\system32\cmd.exe - nslookup C:\>nslookup Servidor predeterminado: www.sanclemente.local Address: 10.0.0.36
IP? De quen xestiona a zona xunta.es Observar que amosa o nome e a IP do servidor que resolve Neste caso www.sanclemente.local 10.0.0.36	→	> xunta.es Servidor: www.sanclemente.local Address: 10.0.0.36
IP? do equipo www.xunta.es .	→	Nombre: xunta.es Address: 69.50.12.40
Observar o alias Fixarse que servidor DNS e web están na mesma IP	→	> www.xunta.es Servidor: www.sanclemente.local Address: 10.0.0.36 Nombre: PRSC12_40.xunta.es Address: 69.50.12.40 Alias: www.xunta.es
IP? De que xestiona a zona edu.xunta.es	→	> edu.xunta.es Servidor: www.sanclemente.local Address: 10.0.0.36 Nombre: edu.xunta.es Address: 69.50.22.2
IP? Do equipo www dentro do dominio edu.xunta.es	→	> www.edu.xunta.es Servidor: www.sanclemente.local Address: 10.0.0.36 Nombre: www.edu.xunta.es Address: 69.50.22.8
IP? Do equipo smtp (Correo) dentro do dominio edu.xunta.es	→	> smtp.edu.xunta.es Servidor: www.sanclemente.local Address: 10.0.0.36 Nombre: smtp.edu.xunta.es Address: 69.50.22.242
Sáimos	→	> exit

Redes Área Local - OSI - TCP/IP

9.- DNS (Domain Name Service)

☞ DNS (Domain Name System) – Un mesmo nome de dominio con varias IPs

Imaxínese un servidor web (p.e. www.google.es) distribuído en 3 hosts distintos para balancear a carga. Ó mesmo tempo desexase que todos eles respondan ó mesmo nome de dominio (www.google.es).

A solución é simple: so hai que dar de alta na zona google.es 3 hosts de alta co mesmo nome (www) e con distintas IPs. Deste xeito ó servidor DNS ó ser consultado dará unha IP distinta cada vez.

OLLO os SO windows almacenan na caché DNS a IP dunha resolución previa, para comprobar o cambio de IP cada vez que se solicita unha conexión a www.google.es é preciso baleira-la caché.

En linux esto último non é preciso, pois os hosts non teñen caché DNS

```
C:\WINDOWS\system32\cmd.exe
C:\>nslookup www.google.es
Servidor: www.sanclemente.local
Address: 10.0.0.36

Respuesta no autoritativa:
Nombre: www.l.google.com
Addresses: 66.102.9.104, 66.102.9.147, 66.102.9.99
Aliases: www.google.es, www.google.com
```

Obsérvense as 3 IPs asignadas a www.google.es e os distintos alias

```
Archivo Edición Formato Ver Ayuda
C:\>ping www.google.es
Haciendo ping a www.l.google.com [66.102.9.147] con 32 bytes de datos:

Respuesta desde 66.102.9.147: bytes=32 tiempo=704ms TTL=240

C:\>ipconfig /flushdns
Configuración IP de Windows
Se vació con éxito la caché de resolución de DNS.

C:\>ping www.google.es
Haciendo ping a www.l.google.com [66.102.9.99] con 32 bytes de datos:

Respuesta desde 66.102.9.99: bytes=32 tiempo=808ms TTL=239

C:\>ipconfig /flushdns
Configuración IP de Windows
Se vació con éxito la caché de resolución de DNS.

C:\>ping www.google.es
Haciendo ping a www.l.google.com [66.102.9.104] con 32 bytes de datos:

Respuesta desde 66.102.9.104: bytes=32 tiempo=489ms TTL=240
```

Redes Área Local - OSI - TCP/IP

10.- DHCP (Dynamic Host Configuration Protocol)

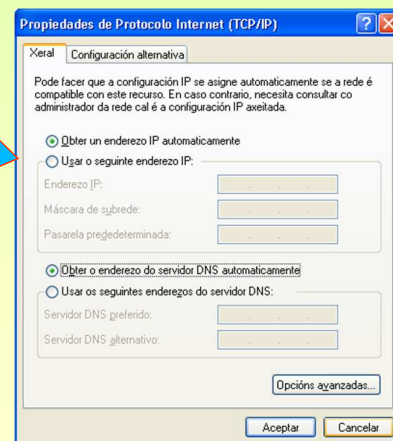
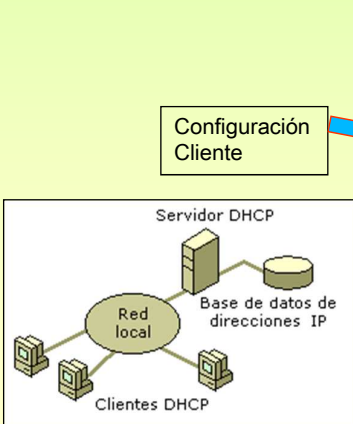
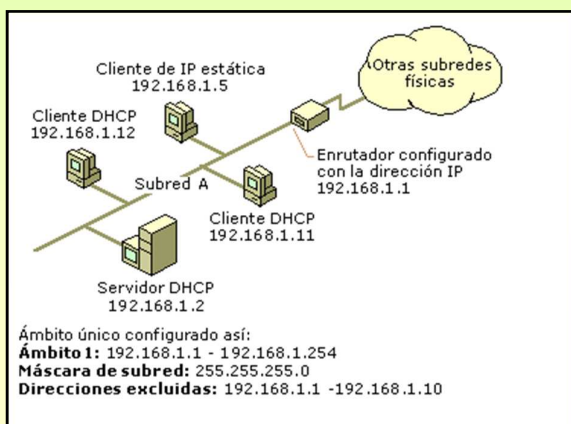
☞ DHCP (Dynamic Host Configuration Protocol).

Hai veces nas que é interesante que os usuarios con ordenadores portátiles poidan chegar a un IES (p.e.), conectarse fisicamente á rede (por cable ou por wi-fi) e que o usuario nin o administrador teñan que estar a configurar as propiedades do protocolo de Internet.

Pois ben, débese configurar un servidor de DHCP que ofrezca un rango de IPs coa súa máscara, porta de enlace e DNS.

Ó acenderse un equipo que teña configurado **Obter automaticamente unha IP** este preguntará á toda a rede se hai alguén que lle poida dar unha IP, o servidor DHCP escoitará a petición e será el quen lla ofrezca. O mesmo co DNS.

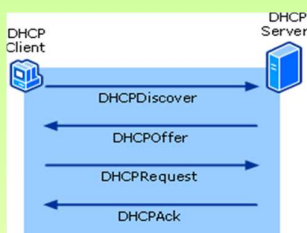
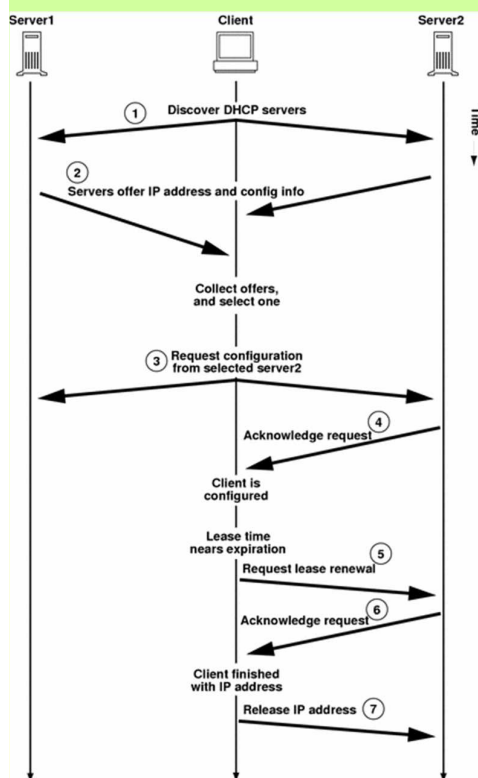
O servidor DHCP leva un control das IPs que leva asignadas



Redes Área Local - OSI - TCP/IP

10.- DHCP (Dynamic Host Configuration Protocol)

FUNCIONAMENTO do DHCP (Dynamic Host Configuration Protocol).



APIPA

```
C:\>ipconfig /all
Configuración IP de Windows
Nombre del host . . . . . : xp
Sufijo DNS principal . . . . . : proba00.ga
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No

Adaptador Ethernet Conexión de área local :
Descripción. . . . . : Adaptador Fast Etherne
n Intel 21140 (Genérico) . . . . . :
Dirección física. . . . . : 00-03-FF-6D-72-0A
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . . . : Si
Dirección IP de autoconfiguración : 169.254.202.52
Máscara de subred . . . . . : 255.255.0.0
Puerta de enlace predeterminada :

```

APIPA

- 1.- O cliente solicita unha IP difundindo unha mensaxe DHCP DISCOVER á subrede local
- 2.- Os servidores ofrecen unha dirección IP (DHCP OFFER) e demais configuración (DNS, dominio, etc) se esta está configurada para ser entregada. Se ningún servidor DHCP responde ó cliente, este envía DHCP DISCOVER cada 0,4,8,16 e 32 seg e logo un intervalo aleatorio ate un minuto. Se pasado1 minuto e non recibe resposta:
A.- Se o cliente usa APIPA (Automatic Private IP addressing), o cliente autoconfigúrase cunha IP (no caso de Microsoft será un IP da rede 169.254.0.0/24)
B.- O interface do cliente non se inicializa (IP 0.0.0.0 /0)

En ambos casos comeza cun novo ciclo DHCP DISCOVER cada 5 mn.
- 3.- O cliente ó recibir DHCP OFFER indica a un dos oferentes que acepta a IP recibida (DHCP REQUEST)
- 4.- O servidor envía unha confirmación DHCP ACK ó cliente indicándolle os termos do arrendamento. A partir de agora o cliente xa pode usas a IP asignada.
- 5.- O cliente solicita renovación da IP cando pase a metade do tempo da concesión.
- 6.- O servidor concédelle a renovación.
- 7.- O Cliente libera a IP

Redes Área Local - OSI - TCP/IP

11.- PKI (Public Key Infrastructure)

PKI (Public Key Infrastructure, Infraestructura de Chave Pública) (I)

A PKI encárgase de procesos relacionados co cifrado de información (Criptografía ven do grego **Krytos** = esconder e **graphos**= grafía, escritura).

PROBLEMAS A RESOLVER (PIANO = CIANO)

Privacidade / Confidencialidade: Un emisor envía unha información cifrada que só o receptor pode entender, ó descifrala. Se a mensaxe é interceptada por un terceiro, este non a entenderá

Integridade: fai referencia a que a información que envía un emisor a un receptor non chegue alterada por un terceiro. Non importa que o terceiro entenda a mensaxe, interesa que non a modifique e se isto ocorre, que o receptor se decate.

Autenticidade: os participantes dunha conversa deben ser quen din ser e non estar suplantados (algo semellante a presentación do DNI por parte dun alumno nun exame, para non suplantar a outra persoa).

Non Repudio: o emisor dunha información nunca pode negar que el foi o remitente.

Lectura recomendada

Para comprender os conceptos asociados a PKI como:

- Chave simétrica,
- Chave pública,
- Resumo,
- Firma dixital,
- Certificados, etc.

Recoméndase a lectura do documento extraído do CERES (Autoridade Pública de Certificación Española). www.cert.fnmt.es

11.- PKI (Public Key Infrastructure)

☞ PKI (Public Key Infrastructure, Infraestructura de Chave Pública) (II)

Unha vez lido o documento, extráese:

Chave simétrica: serve para intercambiar información cifrada entre interlocutores. Estes deben coñecer a chave de cifrado:

- Ventaxa: é rápido.
- Inconvinte: ¿como intercambiar a chave entre o emisor e o receptor?

Chave pública: cada interlocutor xenera dúas chaves (unha inversa da outra); Privada (quédase o usuario con ela), Pública (distribúea entre os demais usuarios).

- Ventaxa: aínda que alguén intercepte unha mensaxe cifrado coa pública e teña a chave pública non poderá descifrar nin a mensaxe nin a chave privada.
- Inconvinte: os algoritmos de cifrados son lentos e xeran mensaxes cifrados moitísimo máis grandes que os orixinais.

- **Resumo:** a través dun algoritmo obtense unha síntese dos datos orixinais. O emisor enviará a mensaxe orixinal e o resumo. O receptor realiza a mesma función sobre a mensaxe orixinal e compara o resumo obtido co recibido. Deste xeito comproba se a mensaxe foi modificada polo camiño.

- Ventaxa: Permite ó receptor asegurarse que a mensaxe non sufriu mudas dende a orixe.

- **Certificado:** é unha garantía emitida por un “notario” asegurando que a chave pública dun usuario é certamente dese usuario.

- Ventaxa: Un usuario A non poderá pasarse polo usuario B dicíndolle a C que lle envía a chave pública B.

Verase máis adiante un estudio máis profundo dos certificados.

11.- PKI (Public Key Infrastructure)

☞ PKI (Public Key Infrastructure, Infraestructura de Chave Pública) (IV)

☞ Resolución dos problemas:

Problemas	Solucións
Privacidade / Confidencialidade: (Que un terceiro non entenda)	1.- Chave simétrica: (Problema intercambio da chave) 2.- Chave asimétrica: (Problema de lentitude) 3.- Combinación de ambas: Cifrar mensaxe con simétrica e intercambiar a simétrica cifrándoa coa pública do destinatario da mensaxe.
Integridade: (que un terceiro non modifique)	1.- Os tres anteriores. 2.- Obter un resumo da mensaxe e enviar este xunto coa mensaxe. (ten o problema de que un terceiro, sabendo a función de hash, podería modificar a mensaxe e o resumo) 3.- Obter un resumo da mensaxe e cifralo coa chave pública do receptor (non habería firma dixital nin privacidade). 4.- Obter un resumo da mensaxe e cifralo coa chave privada do emisor (a mensaxe estaría firmada pero non habería confidencialidade)
Autenticidade: (Emisor sexa quen di ser)	1.- Cifrar a mensaxe coa privada do emisor, só el ten a privada: (Lento). 2.- Realizar un resumo da mensaxe e cifralo coa privada do emisor: (rápido)
Non repudio: (Emisor non negue a paternidade da mensaxe)	1.- Cifrar a mensaxe coa privada do emisor: (Lento). 2.- Realizar un resumo da mensaxe e cifralo coa privada do emisor: (rápido) En calquera dos dous casos só o emisor ten a súa chave privada, co cal non pode negar a paternidade da mensaxe

11.- PKI (Public Key Infrastructure)

☞ PKI (Public Key Infrastructure, Infraestructura de Chave Pública) (V)

☞ Certificados:

Un certificado divídese en tres partes cada unha delas cos seus campos:

- Identidade do solicitante do certificado (persoa, empresa, organismo, etc)
- A chave pública que hai que certificar
- A firma da entidade certificadora.

Os datos dos dous primeiros son proporcionados polo usuario, mentres que o último é xerado pola entidade certificador (CE) tamén chamada Autoridade Certificadora (CA).

Unha CA non é máis que unha especie de notario que certifica que a chave pública contida no certificado pertence a o usuario que identificado, tamén, no certificado. Para elo a CA o que fai e facer un resumo das dúas primeiras partes e logo cifralo coa súa chave privada.

Cada entidade certificadora tamén ten dúas chaves (privada e simétrica). A privada quédase ela con ela e a pública é distribuída mediante un certificado da CA.

Pénsese nun usuario A que recibiu un certificado dun usuario B, para que o usuario A poida comprobar que o certificado é correcto ten que obter o resumo das dúas primeiras partes e logo contrastalo co que ven no certificado (3ª parte). Pero para iso precisa descifralo, e é aquí, cando o usuario A precisa a chave pública (certificado) da CA para poder descifrar esa firma da CA.

11.- PKI (Public Key Infrastructure)

☞ PKI (Public Key Infrastructure, Infraestructura de Chave Pública) (VI)

☞ Certificados: X.509 v3

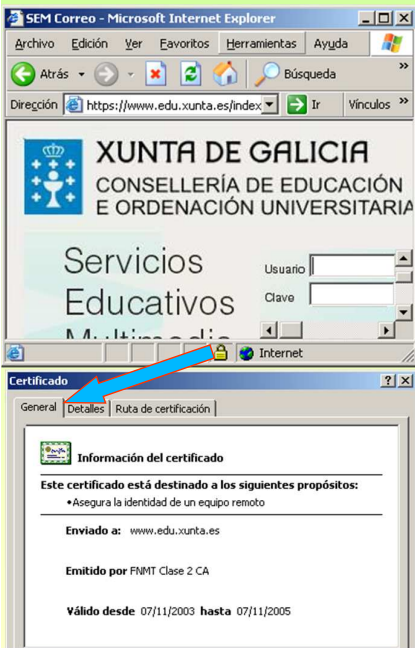
O estándar X.509 define o formato e contido dos campos dun certificado. Actualmente vai na versión 3, esta permite definir campos a parte dos xa establecidos.

Campos	Descrición
Versión	Versión do estándar X.509 (1, 2 ou 3)
Nº Serie	A AC a cada certificado que emite pónlle un nº. Este tamén serve para comprobar se o certificado está na lista dos revocados (CRL).
Emisor Certificado	Quen emite o certificado, esto é quen o firma. Por exemplo, FNMT, Verisign, etc.
Algoritmo de firma	Cal foi o algoritmo usado para obter o resumo (firma)
Período de validez	Dende (data) ate (data)
Usuario	Indentificación do dono do certificado, a quen se lle está certificando a súa chave pública
Chave pública	A chave pública que vai compartir cos demais usuarios. Lonxitude desta, con que algoritmo se xerou, etc.
Datos opcionais	Datos extras que desexe incluír o usuario.
Firma	Resumo do resto dos campos obtido co algoritmo de firma e cifrado coa chave privada da CA

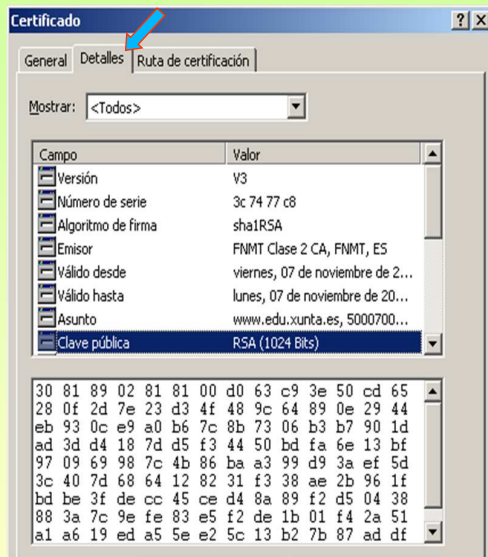
11.- PKI (Public Key Infraestructure)

PKI (Public Key Infraestructure, Infraestructura de Chave Pública) (VII)

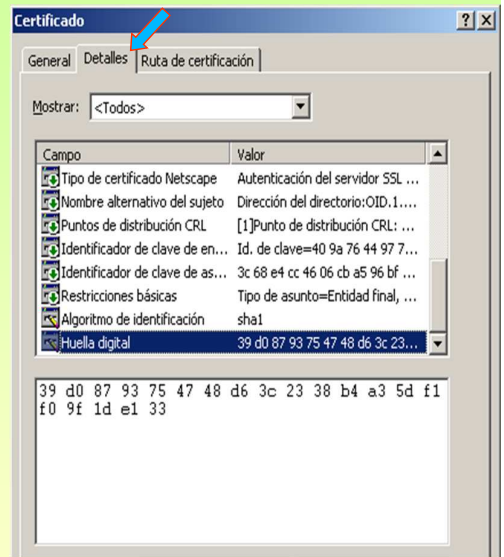
Exemplo de certificado: correo web de www.edu.xunta.es



Nunha páxina https facendo dobre clic sobre o candado inferior vese o certificado SSL. Certificado emitido pola FNMT



Obsérvase:
Os campos antes indicados.
Quen o emite.
Para quen o emite, etc.
A chave pública do dono do certificado



Obsérvase:
A firma dixital, obtida co algoritmo sha1RSA

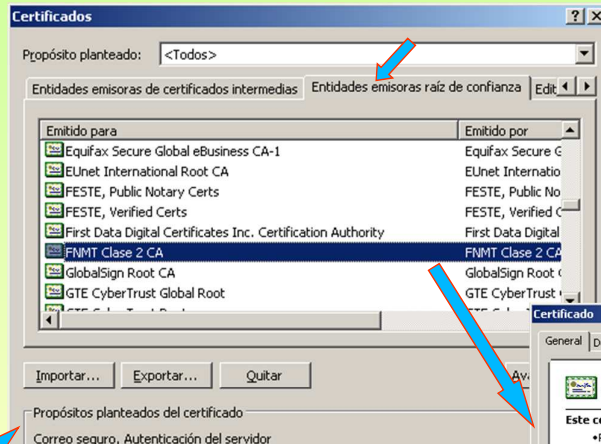
11.- PKI (Public Key Infraestructure)

PKI (Public Key Infraestructure, Infraestructura de Chave Pública) (VII)

Certificados raíz instalados nos clientes (certificados de emitidos da CA para a propia CA)

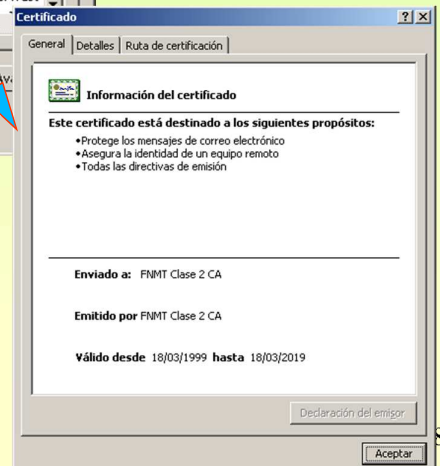


Neste caso trabalarase co Internet Explorer de MS



O certificado anterior foi emitido pol Fábbrica Nacional de Moeda e Timbre (FNMT). Para comprobar se está correcto precisase a chave pública da CA, ou sexa o seu certificado. Como se ve está instalado nas CA raíz.

Obsérvase como o emite a FNMT para a FNMT

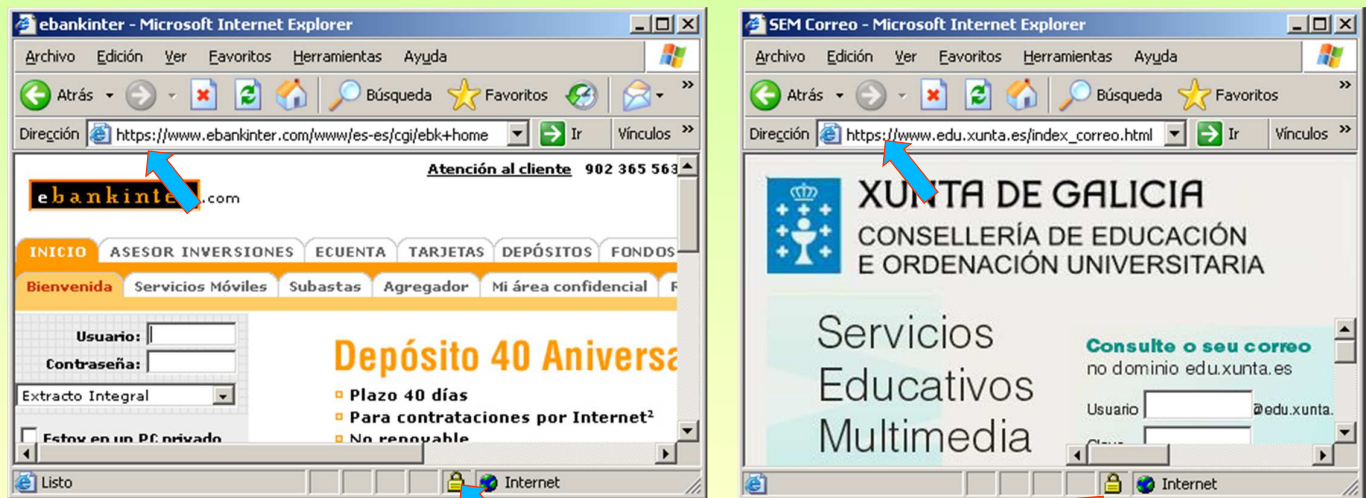


11.- PKI (Public Key Infraestructure)

SSL (Secure Socket Layer, Capa de Sockets Seguros) (II)

-O porto ben coñecido dunha conexión que use httpS (SSL) é o 443.

-Nun cliente web (navegador) sábese cando está en modo seguro cando na súa parte inferior aparece un candado e na url Https:



Conexións SSL.
Realizando dobre clic sobre o candado vense as propiedades do certificado.

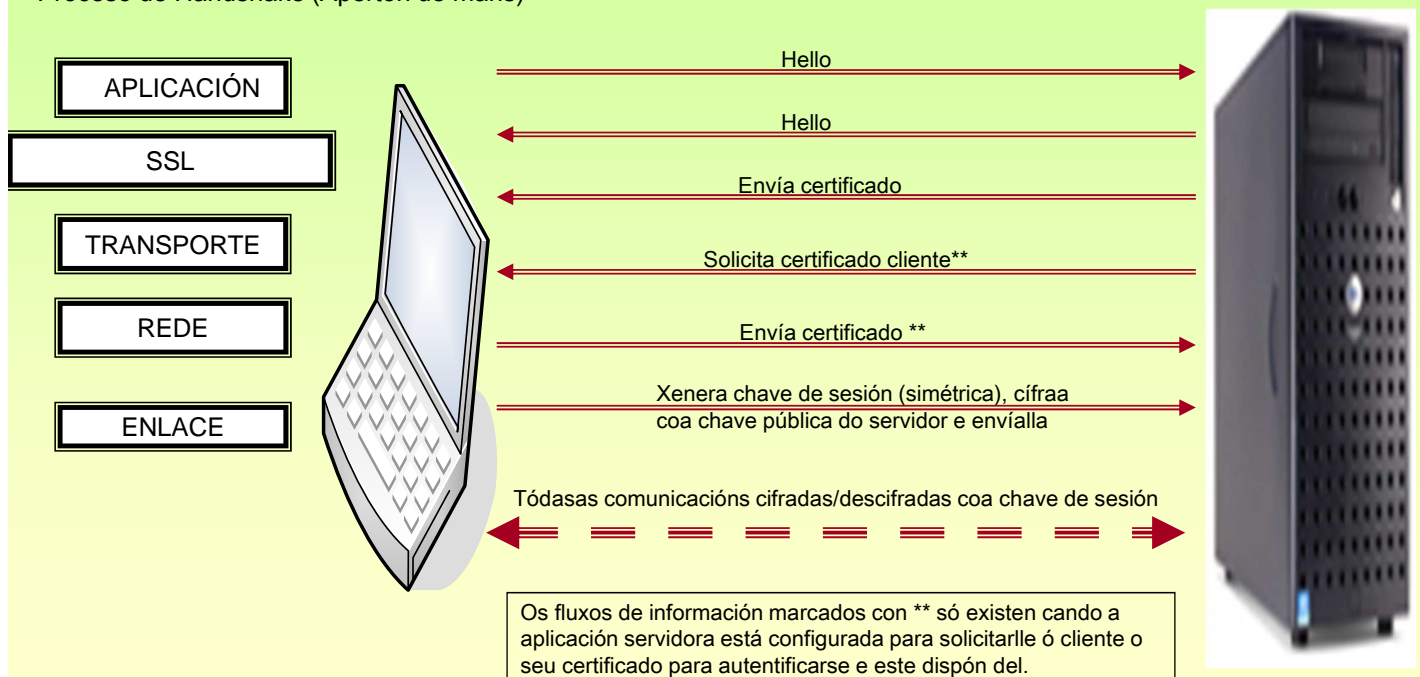
139

11.- PKI (Public Key Infraestructure)

SSL (Secure Socket Layer, Capa de Sockets Seguros) (I)

-Creado no 1994 por Netscape. Permite crear túneles seguros entre unha aplicación cliente e a aplicación servidor

- Proceso de Handshake (Apertón de mans)



140

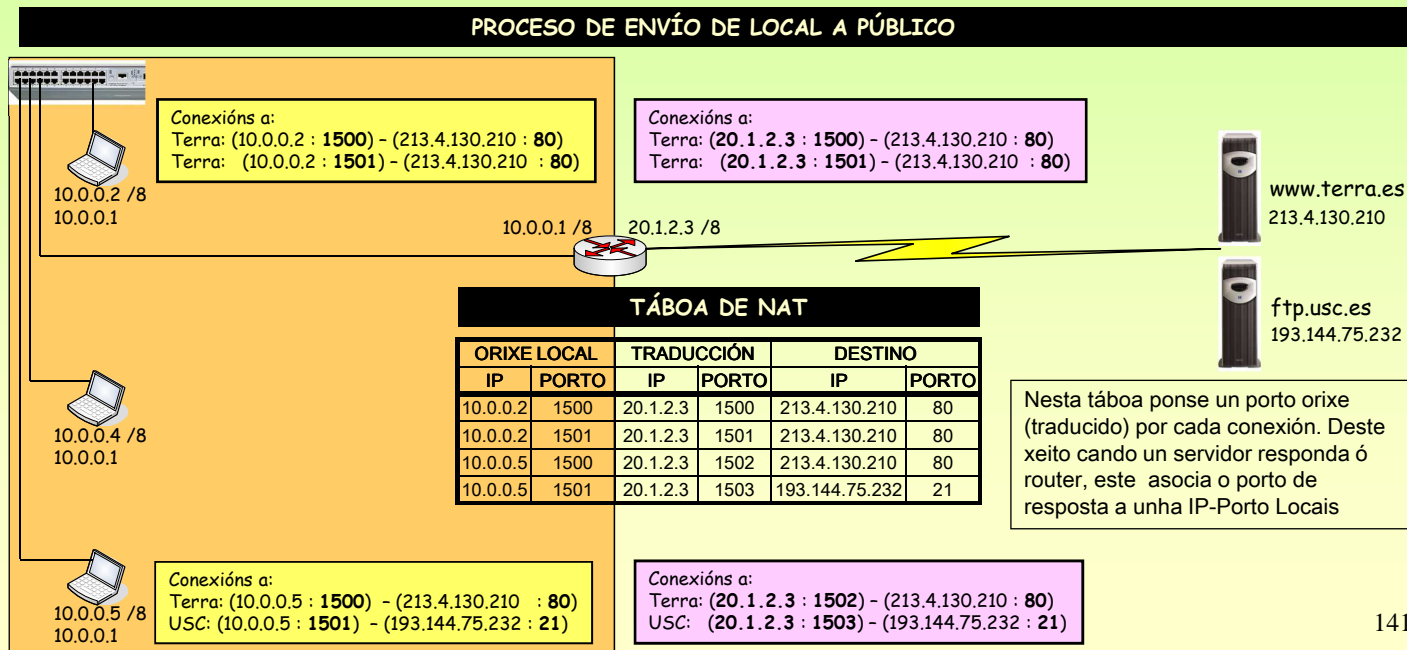
Redes Área Local - OSI - TCP/IP

12.-NAT (Network Address Translation)

NAT (Network Address Translation - Tradución de enderezos de rede) (I - Consulta)

Un host cunha IP privada establece unha conexión cun Host cunha IP pública. Pero o host coa IP pública non sabe como chegar o host coa IP privada.

Solución: O router realiza NAT, isto é, el pon a súa IP pública como orixe do paquete, e modifica o porto orixe. Esta táboa constrúese dinamicamente a medida que os hosts locais inician conexións co exterior.



Redes Área Local - OSI - TCP/IP

12.-NAT (Network Address Translation)

NAT (Network Address Translation - Tradución de enderezos de rede) (II - Resposta)

Agora o equipo PÚBLICO respóndelle a quen lle fixo a solicitude que foi o Router coa súa IP PÚBLICA,

O Router mira a que porto lle están respondendo, consulta a táboa de NAT e envíalle o paquete-IP ao ordenador da LAN que iniciou a conexión co exterior. Este pensa que quen lle está respondendo é o ordenador PÚBLICO directamente.

