APUNTES

(SIMR)

SISTEMAS INFORMÁTICOS MULTIUSUARIO E EN REDE

1º DE DAI

REDES

(OSI - TCP/IP - SERVIZOS)

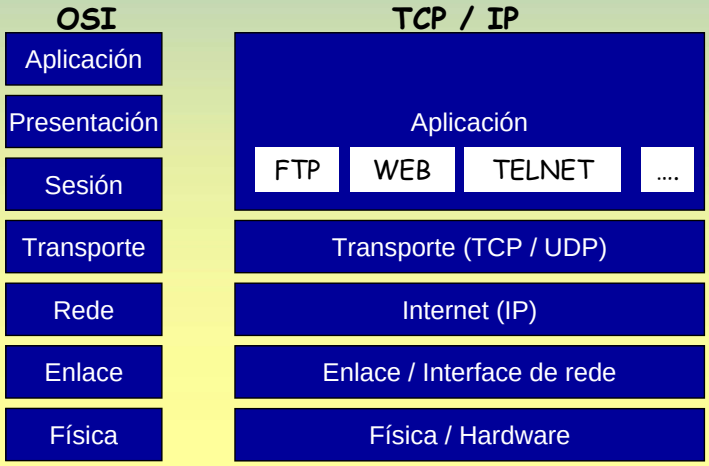
CURSO 06-07
IES SAN CLEMENTE
SANTIAGO DE COMPOSTELA

Profesor:
Carlos Carrión Álvarez

Redes LAN
OSI – TCP-IP

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

Profesor:
Carlos Carrión Álvarez



Redes Área Local - OSI – TCP/IP

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 pais ou como o mundo enteiro (internet).
  - Usan liñas dedicadas/públicas

1.2 Breve historia das comunicacións

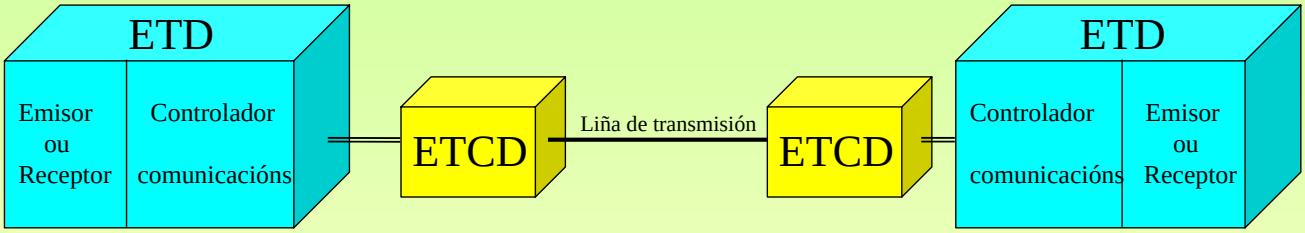
- A arte da comunicación é tan antigo como a humanidade
  - Tan-Tan
  - Lume-fogo
  - Semáforos, etc.
- Ano 1834 S. Morse inventa o telégrafo
  - Código Morse (. e _)
  - Imposibilidade de automatizar debido á falta de sincronismo
- Ano 1874 Emil Baudot constrúe un código de lonxitude fixa
  - O número 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 Archiquecture, DNA – Digital Network Arquitecture)
  - Tiñan estructura 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 productos 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**

    Prodúcense en liñas metálicas homoxéneas. Entre os dous ou varios cables dun mesmo conducto prodúcense 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

7

Redes Área Local - OSI – TCP/IP

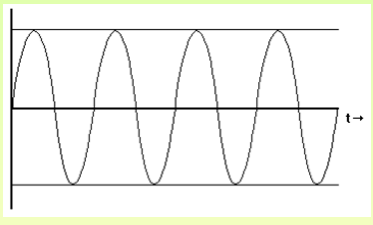
2.2- Sistemas analóxicos e dixitais

- **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.

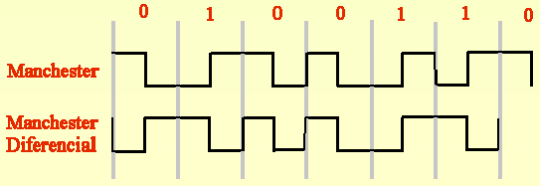
  Cando un sinal chega a un repetidor/amplificador este amplifica o sinal, co cal tamén amplifica o ruído que con ela chega.



- **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



8

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 circuítos/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

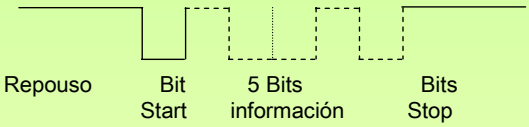
  Transmisión SINCRONA

Redes Área Local - OSI – TCP/IP

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.



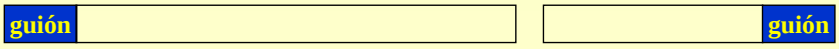
  Bit START: Marca o inicio dun novo carácter/palabra.
  Bit STOP: Marca o final dun carácter/palabra. Sóense usar 1 ou 2 bits de STOP
  Bits de información: depende do código usado: CCITT nº 2 (5 bits), CCITT nº5 (8 bits) e ASCII (8 bits)
  Emisor e receptor deben traballar á mesma frecuencia e ter sincronizados os reloxos.
  Eficiencia do código CCITT nº2: de cada 7 bits transmitidos 5 son de información, 71%

- Transmisión síncrona

  O sincronismo envíase 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

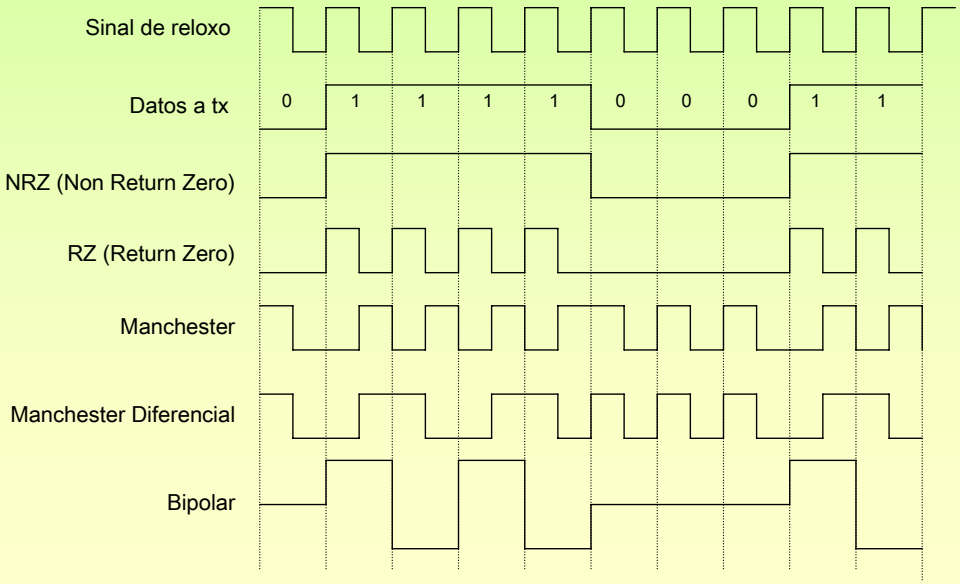


2.4.- Técnicas de Transmisión

Para transmitir os datos dixitais sobre as liñas de comunicación necesítanse 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)



Redes Área Local - OSI – TCP/IP

2.4.- Técnicas de Transmisión

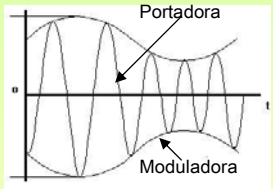
☞ **Transmisión de datos en Banda Ancha**

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)

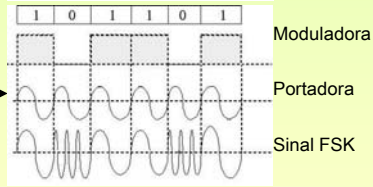
Portadora: sinal do medio, a que vai transportar a información.
Moduladora: sinal que modifica algún parámetro da portadora, é a información.

☞ **Portadora Analóxica**

Moduladora analóxica:
- Modulación en amplitude (AM)
- Modulación en frecuencia (FM)
- Modulación en fase (PM)

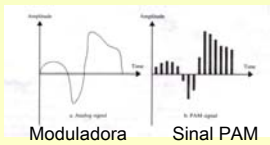


Moduladora dixital:
- Modulación por desprazamento de amplitude (ASK)
- Modulación por desprazamento de frecuencia (FSK)
- Modulación por desprazamento de fase (PSK)



☞ **Portadora dixital e modulación analóxica**

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



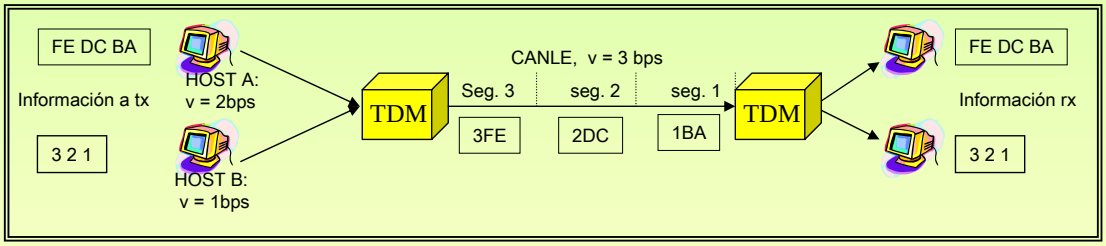
2.5.- Multiplexación

- **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**

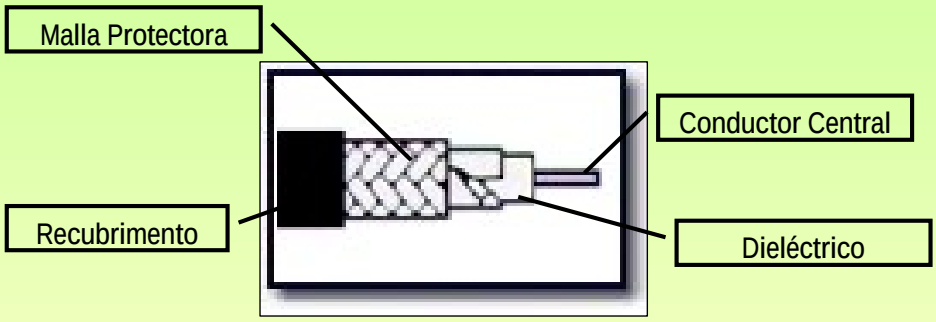
  Conductores metálicos
  - Cable coaxial
  - Cables de pares

  Inalámbrica
  - Radio transmisión
  - Microondas
  - Infravermellos

  Ópticos
  - Ondas de luz
  - Fibra óptica

2.6.- Medios de transmisión

- Conductores metálicos: CABLE COAXIAL



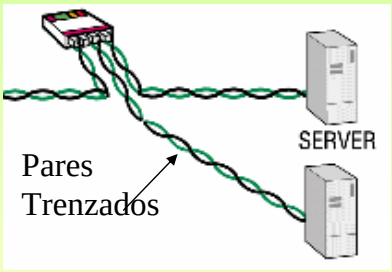
Redes Área Local - OSI – TCP/IP

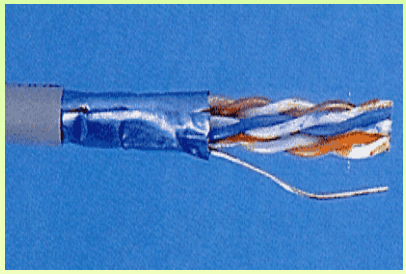
2.6.- Medios de transmisión

- 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

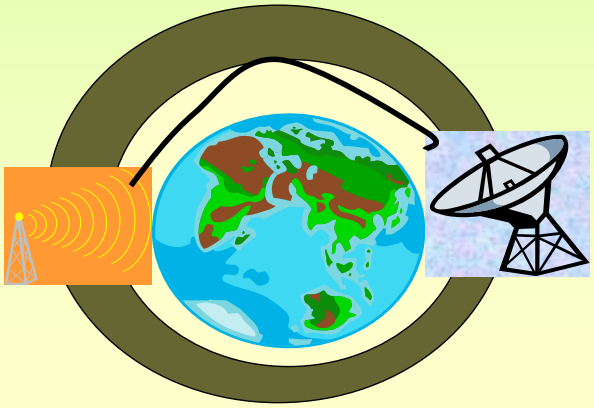
FTP (Foil Screnned Twisted Pair): cable de Pares Trenzado Apantallado cunha cuberta de aluminio

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 Móbiles
Comunicacións vía satélite / parabólicas



Redes Área Local - OSI – TCP/IP

2.6.- Medios de transmisión

☞ Conductores ópticos

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

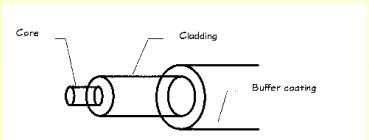
Infravermellos: Distancias curtas. Permítenos ter illadas as salas de comunicacións.
Calculadoras, Móbiles
LANS inalámbricas

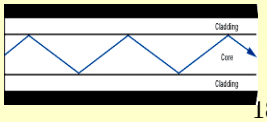
Fibra óptica: Conductor que transporta a información mediante haces de luz.
O núcleo está formado por un fío de vidro capaz de conducir no seu interior un raio óptico.

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





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

Redes Área Local - OSI – TCP/IP

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.- Topoloxías de rede

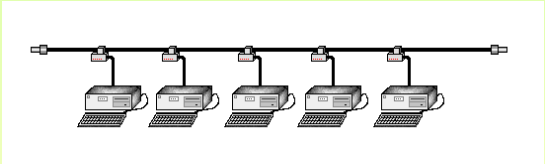
☞ **Topoloxías**

Distintas formas de organizar unha rede.

Bus
Anel
Estrela
Árbore

☞ **BUS**

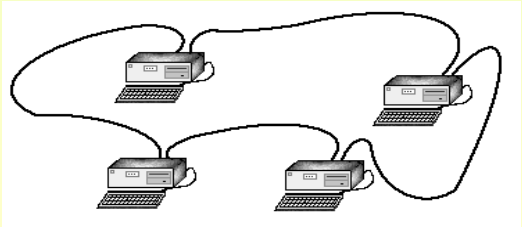
Tódolos ordenadores conectados a un mesmo cable.
Fácil ampliación
Baixo custe de instalación



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

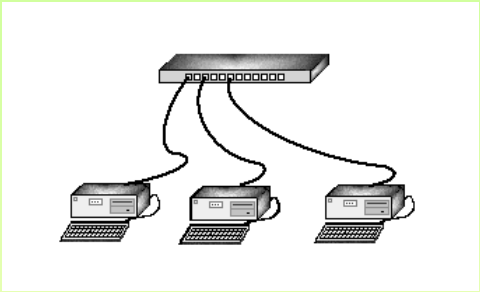
21

Redes Área Local - OSI – TCP/IP

3.- Topoloxías de rede

☞ **Estrela**

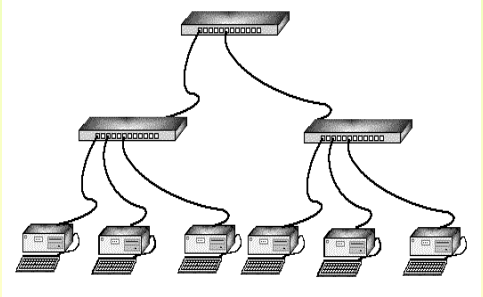
Tódolos nodos están conectados a un nodo central.
Facilidade de ampliación
Custe medio/alto (un cable/nodo)



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

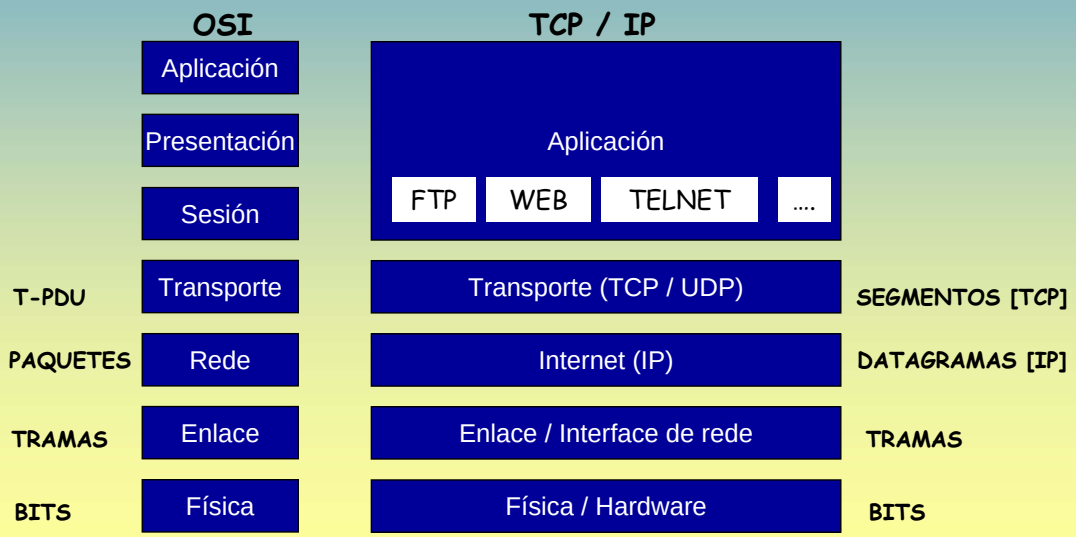
☞ **Árbore**

Interconexión de varias redes en estrela
Ten as vantaxes e inconvenientes anteriores



22

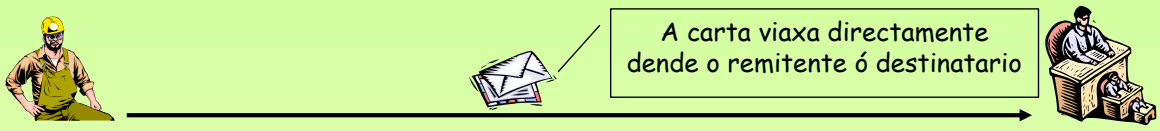
OSI – TCP/IP



4.- Modelo de referencia OSI

☞ Dous amigos envíanse unha carta.

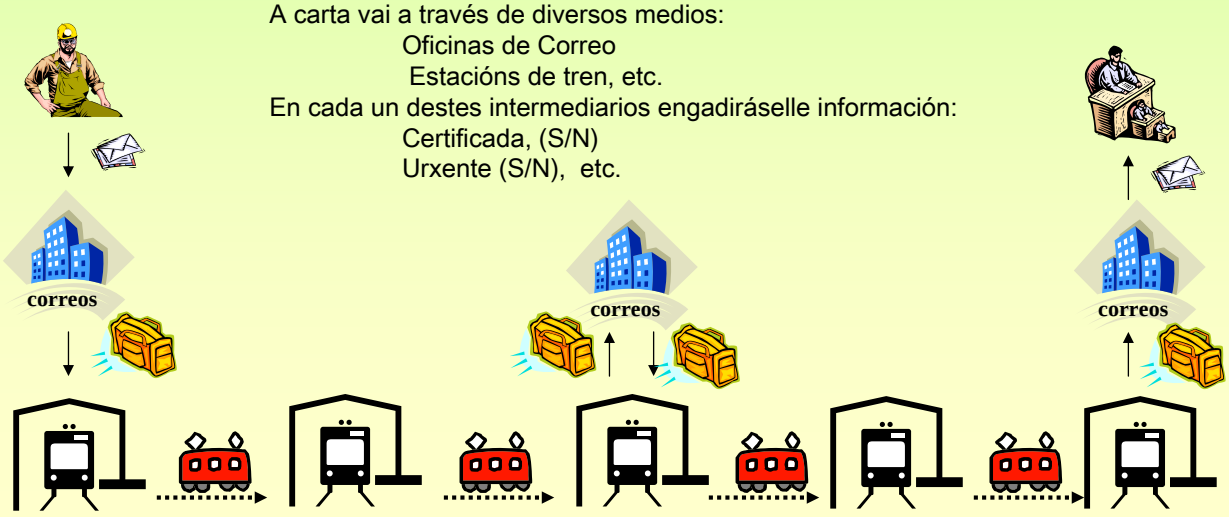
A imaxe que temos do proceso de envío é o seguinte.



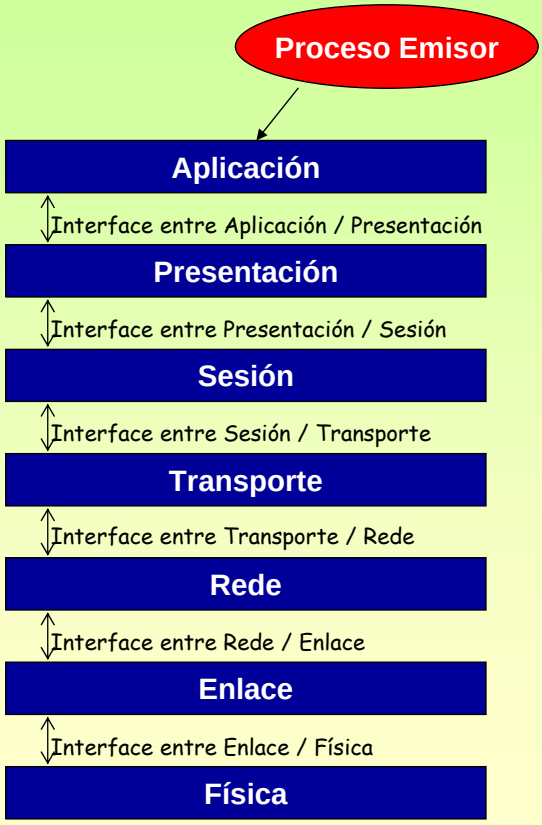
☞ A realidade.

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.



4. Modelo OSI de ISO (1984)

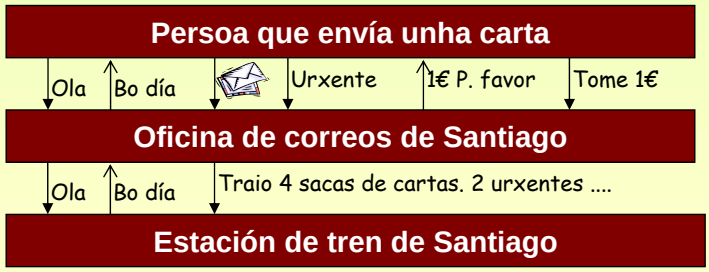


- ISO: International Standard Organization
  (Organismo de estándares internacionais)
- OSI: Open System Interconection.
  (Interconexión de sistemas abertos/heteroxéneos)
- Arquitectura organizada en 7 capas/niveis
  Cada unha con unha función clara e ben definida

- INTERFACES

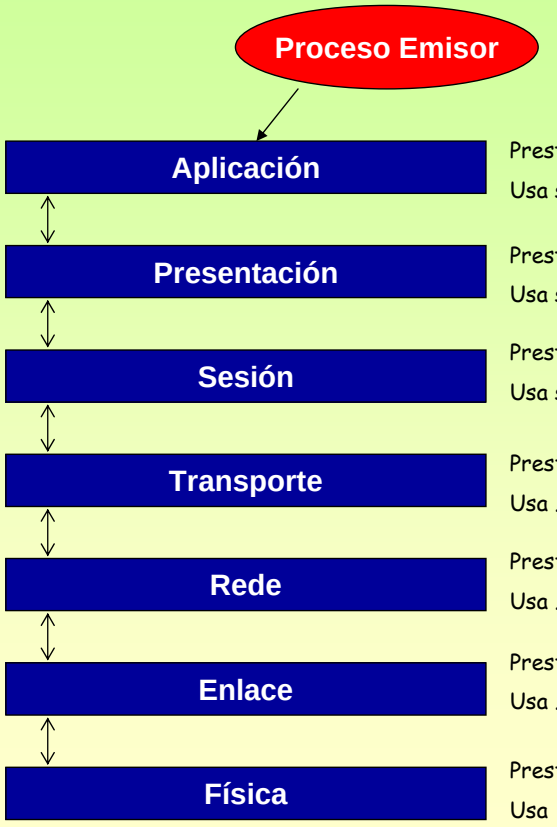
É o lugar polo que intercambian infomación dúas capas. Unha capa intercambia información coa súa superior/inferior inmediatas.

- 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 súa 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 ...

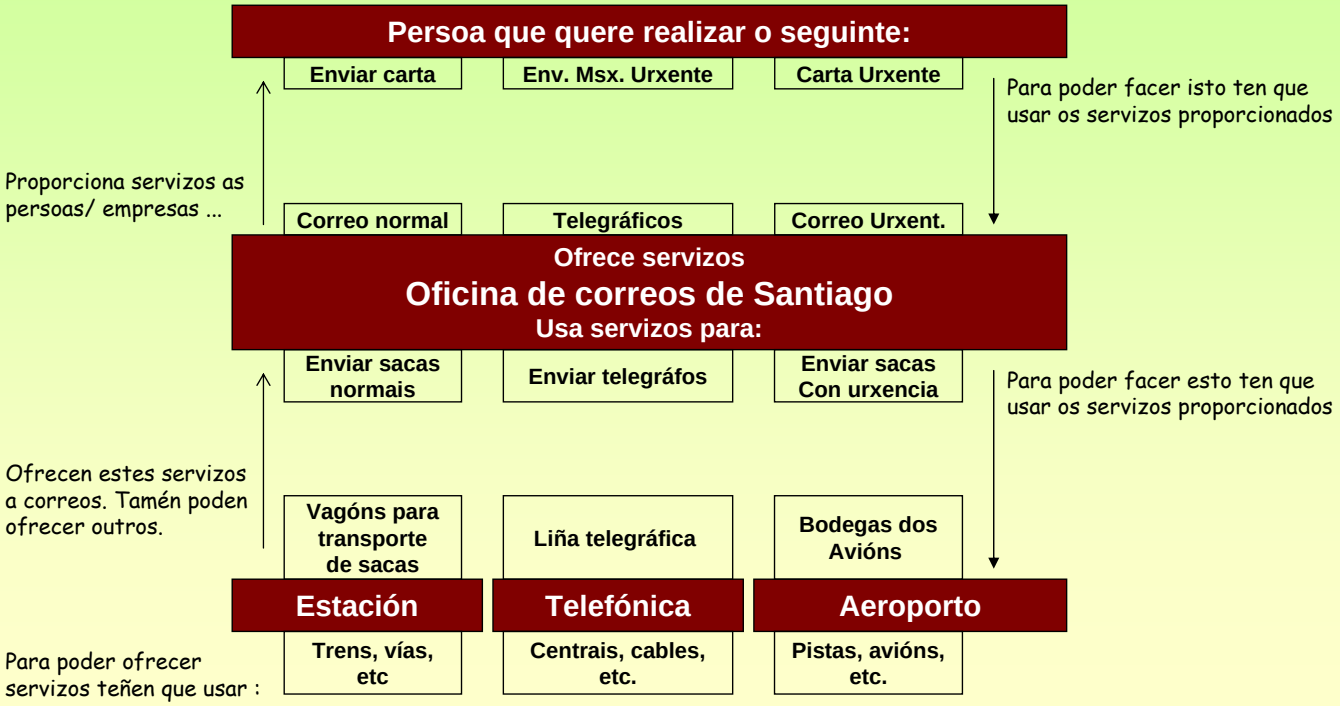
Enlace
Presta ...
Usa ...

Física
Presta ...
Usa os medios físicos...

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

☞ SERVIZOS - EXEMPLO

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



Redes Área Local - OSI – TCP/IP

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.

☞ EXEMPLO

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 chegen todas nin na mesma orde en que saíron.

SERVIZO ORIENTADO Á CONEXIÓN:

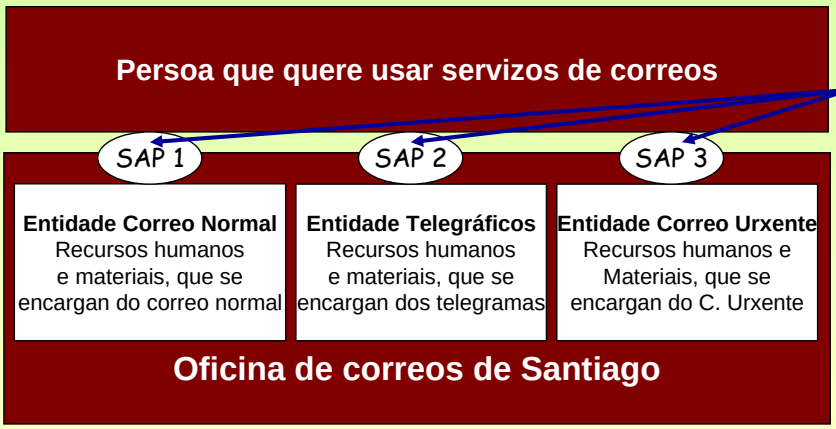
Equivale ó **sistema Telefónico**. Para realizar unha comunicación:

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 (cólgase ó teléfono)

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**

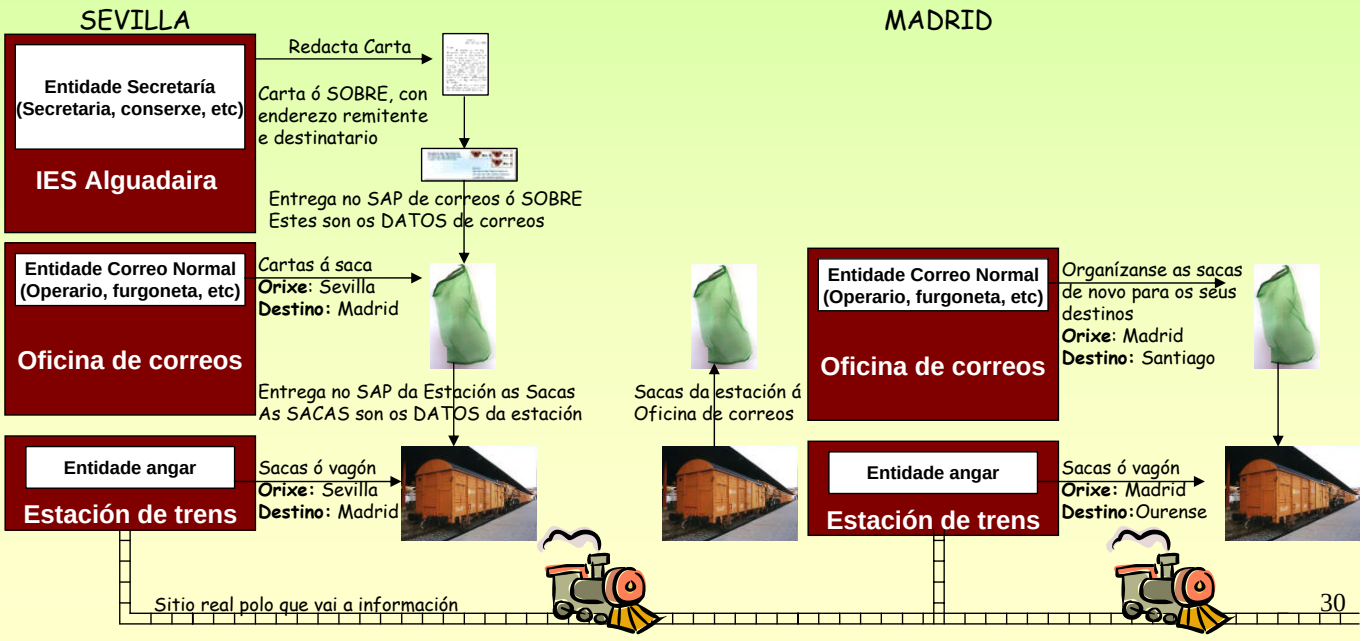
Por outra banda, a oficina de correos intercambiará información coa Estación de Trens, Aeroporto, Telefónica, etc, polos SAPs que estes poñan a disposición da oficina de correos

(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

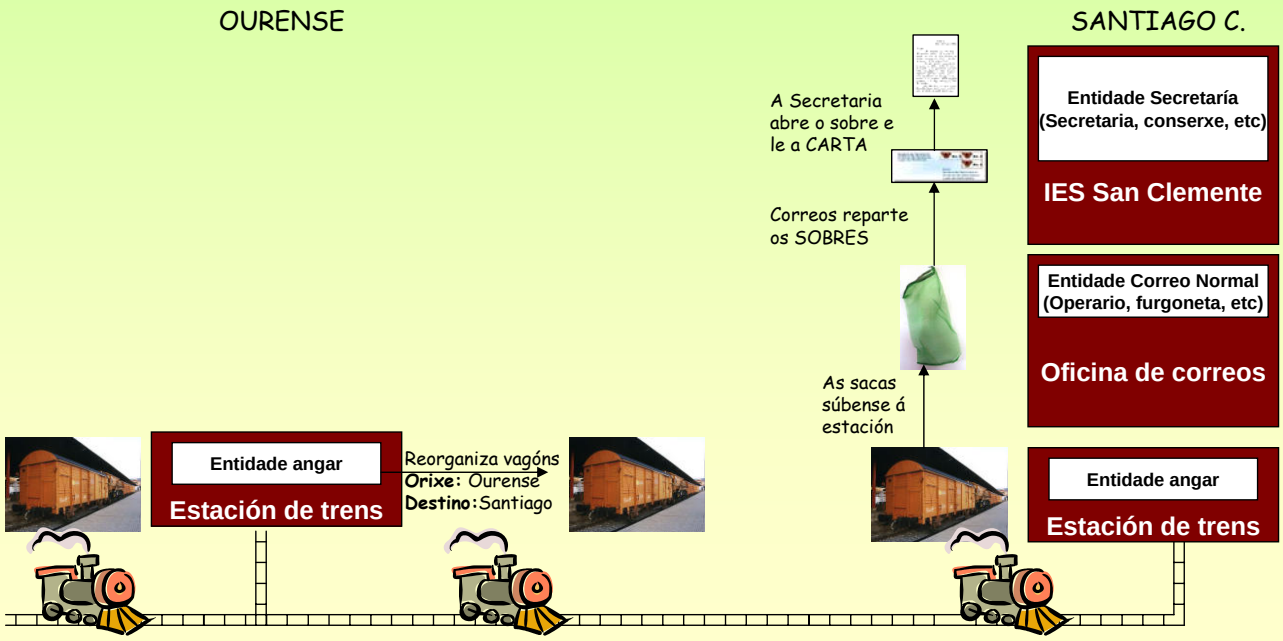
Un **REMITENTE / EMISOR** o único que desexa **transmitir/enviar** ó **DESTINATARIO / RECEPTOR** é unha **CARTA/MENSAXE** (entendida esta sen o sobre)
Pero a CARTA non pode viaxar pola rede de comunicación sen un **ENVOLTORIO/CABECEIRA** que lle permita a esta ser conducida ata o seu destino. Precísase 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.



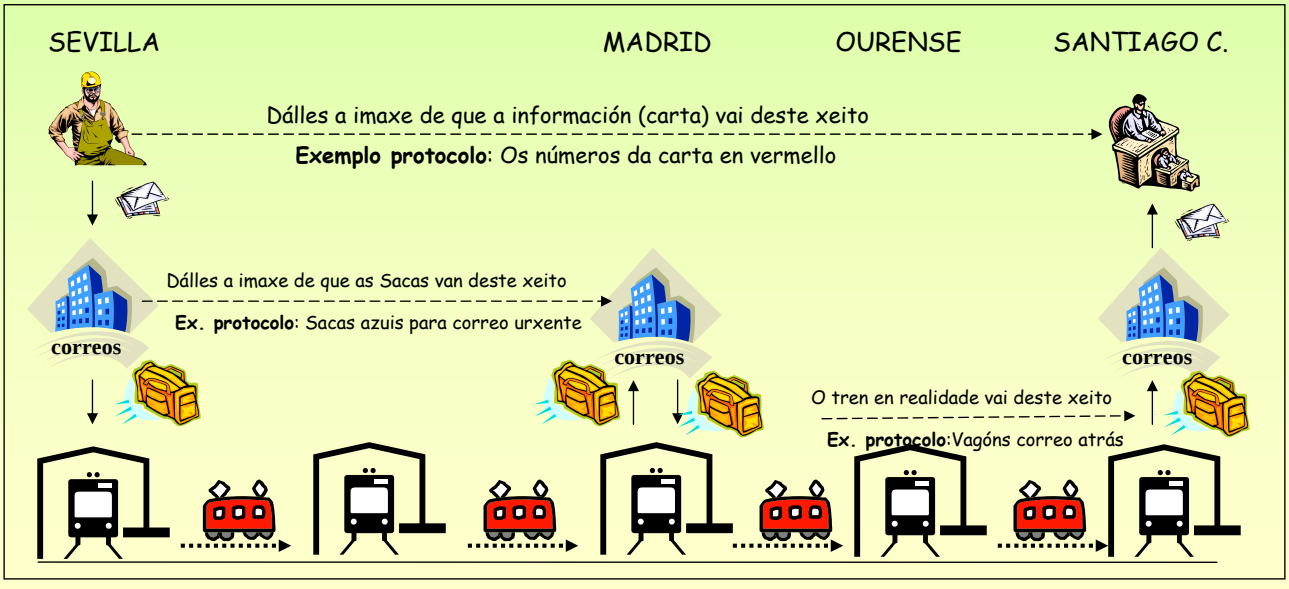
Redes Área Local - OSI – TCP/IP

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/regras** que establece cada **entidade par** para comunicarse entre elas.



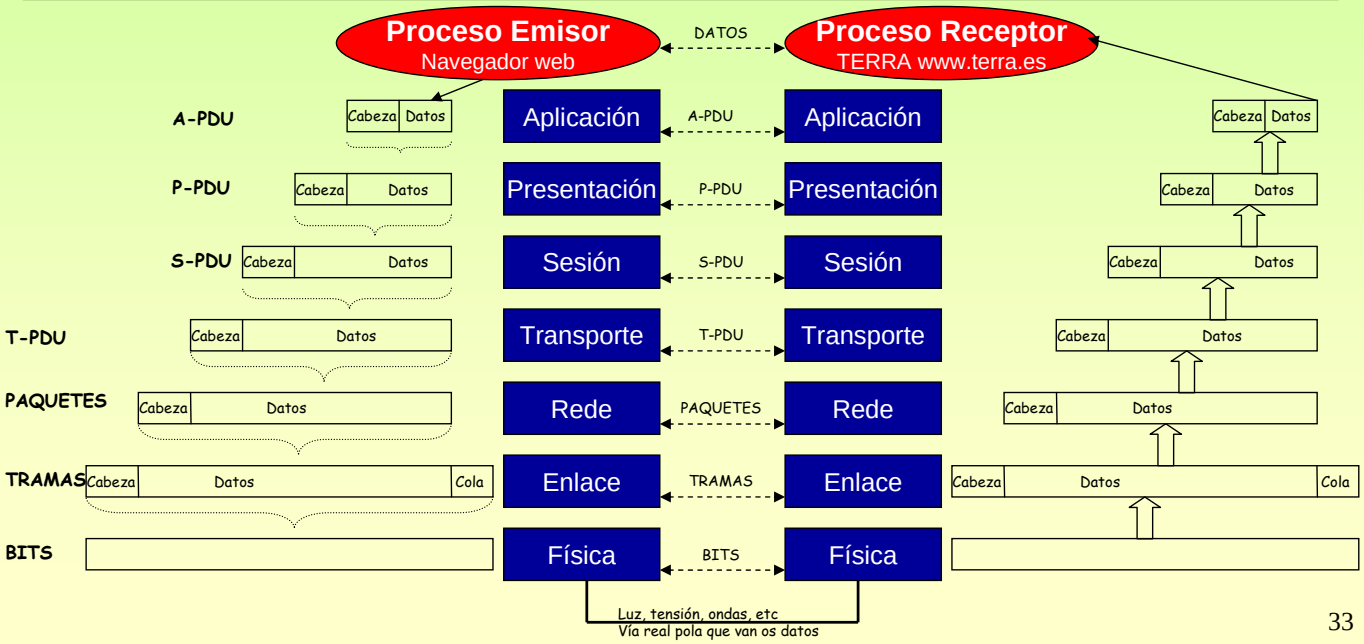
4.- Modelo de referencia OSI de ISO (1984)

☞ **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.

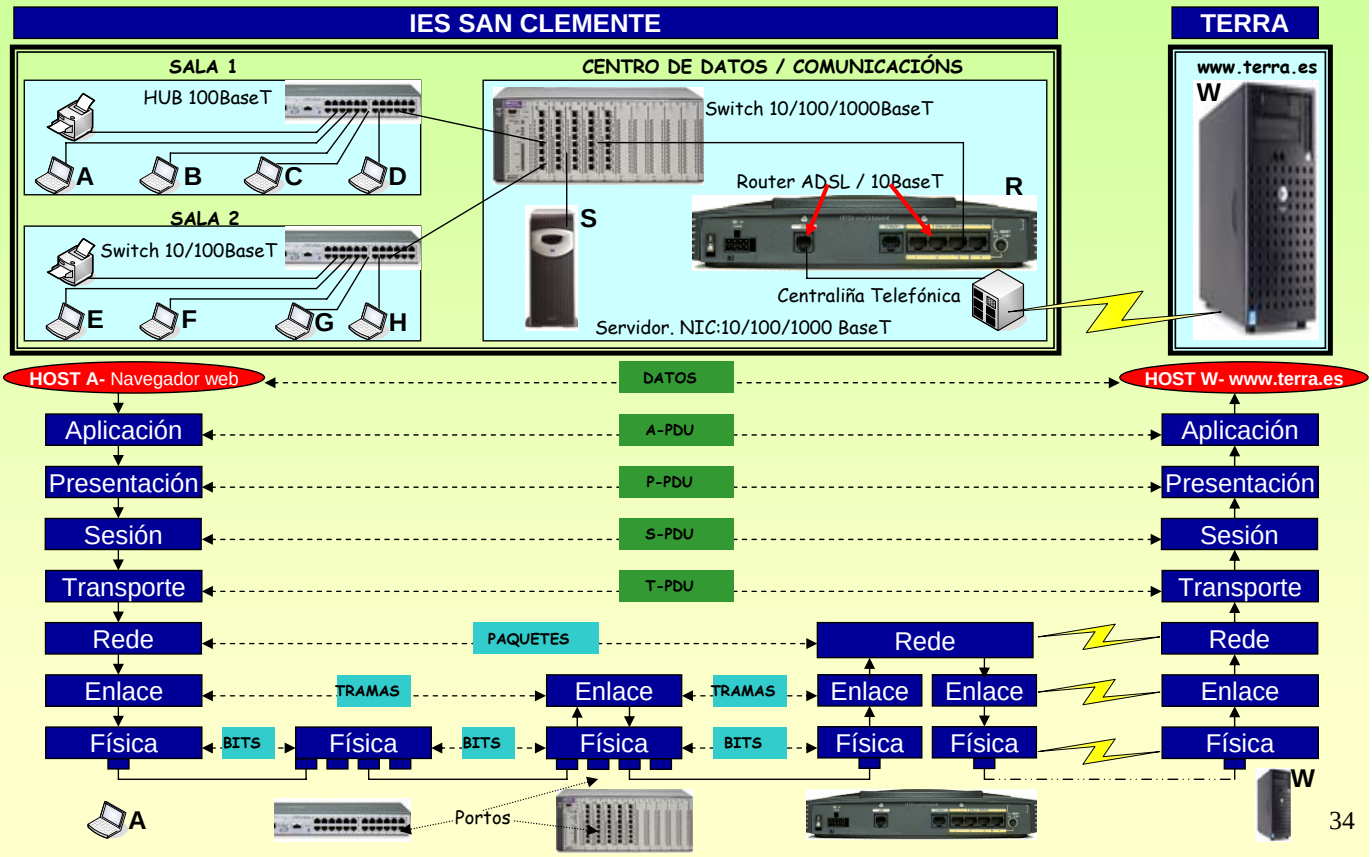
LADO RECEPTOR: As entidades de cada capa reciben das entidades da capa de abaixo as mensaxes, sacan a cabeceira e soben o campo de datos á capa superior.

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

Aplicación

Constrúe e procesa **A-PDUs**.
Neste nivel están as aplicacións como poderían ser o **FTP**, **DNS**, Servidor **Web**, **Correo electrónico**, etc

Presentación

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 trasmite un "**que**", no emisor podemos sacarlle o "**u**" e volverllo a poñer no receptor)

Sesión

Constrúe e procesa **S-PDUs**.
Encárgase da **xestión do diálogo** entre dúas máquinas finais (Quen transmite primeiro, como nos pasamos a testemuña, etc)

Transporte

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)

Rede

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 conxestión (Unha rotonda conxestiónase se a suma de coches recibidos por tódalas liñas é maior que os que pode procesar)

Enlace

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 resto ponse na cola. No receptor faise a mesma división e contrástase 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)

Física

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)

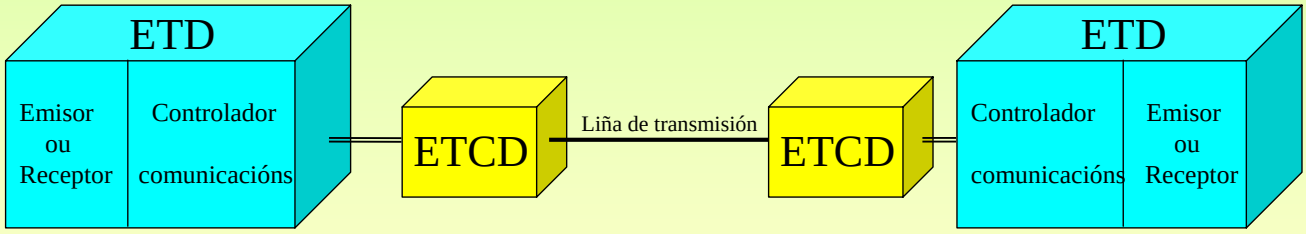
5.- Nivel físico

☞ **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

6.- Nivel de enlace

☞ Descrición

Trata de asegurar unha conexión libre de erros entre dous nodos da mesma rede.

Extremo emisor

- Acepta os paquetes do nivel de rede e **troceaos** en tramas.
- **Construe** 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
- **Comproba** os erros
- Se a trama é correcta **sube** a información ó nivel de rede.

☞ Subcapas

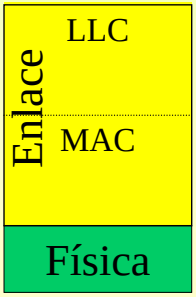
O nivel de enlace divídese en dúas subcapas con funcións claramente diferenciadas.

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

- Confección de tramas
- Control de erros, ...

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

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



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 simpre
    - Rexeite selectivo

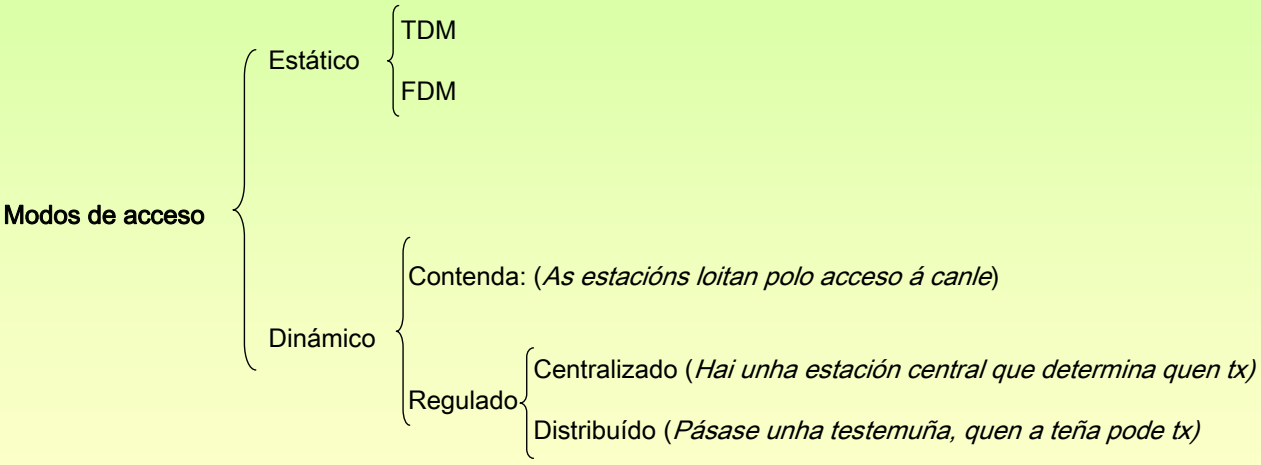
Asentementos en liñas bidireccionais

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

6.2- Subcapa MAC

- **Funcións básicas**

  Como se vai acceder ó medio físico



Redes Área Local - OSI – TCP/IP

6.2- Subcapa MAC

- **Acceso dinámico: Contenda**

  Varias estacións compiten pola canle.

  Colisión: cando dúas tramas coiciden 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 Medium Access – Acceso ó Medio 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

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)

EXEMPLO

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

*IEEE = Institute for Electrical and Electronics Engeneers

**802.x: Comités dentro do IEEE que desenvolveron os estandares 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	2 ou 6	2 ou 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

7.2.- Capa física do IEEE 802.3

- O comité 802.3 foi o que defineu 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> <sinalización> <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

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

Redes Área Local - OSI – TCP/IP

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

10BASE5

10BASE2

10BASE-T

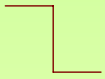
10ANCHA36

10BASE-F

☞ 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 e 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 (Transceiveir, 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)

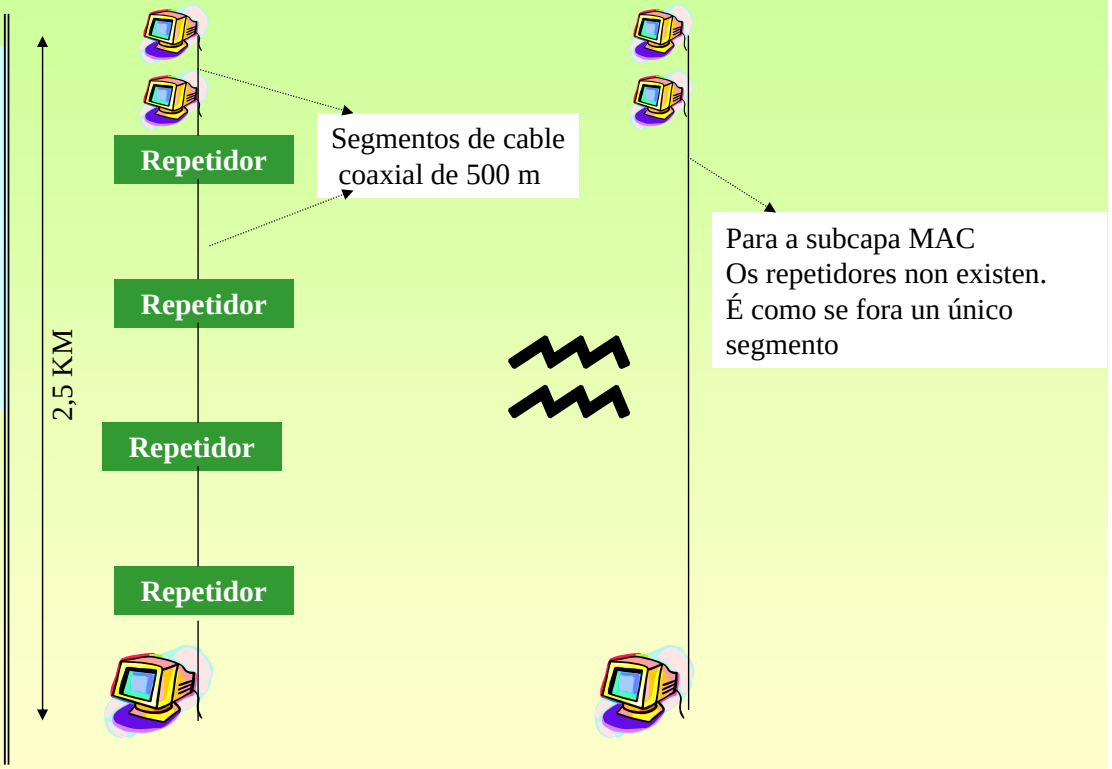
10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F



Redes Área Local - OSI – TCP/IP

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

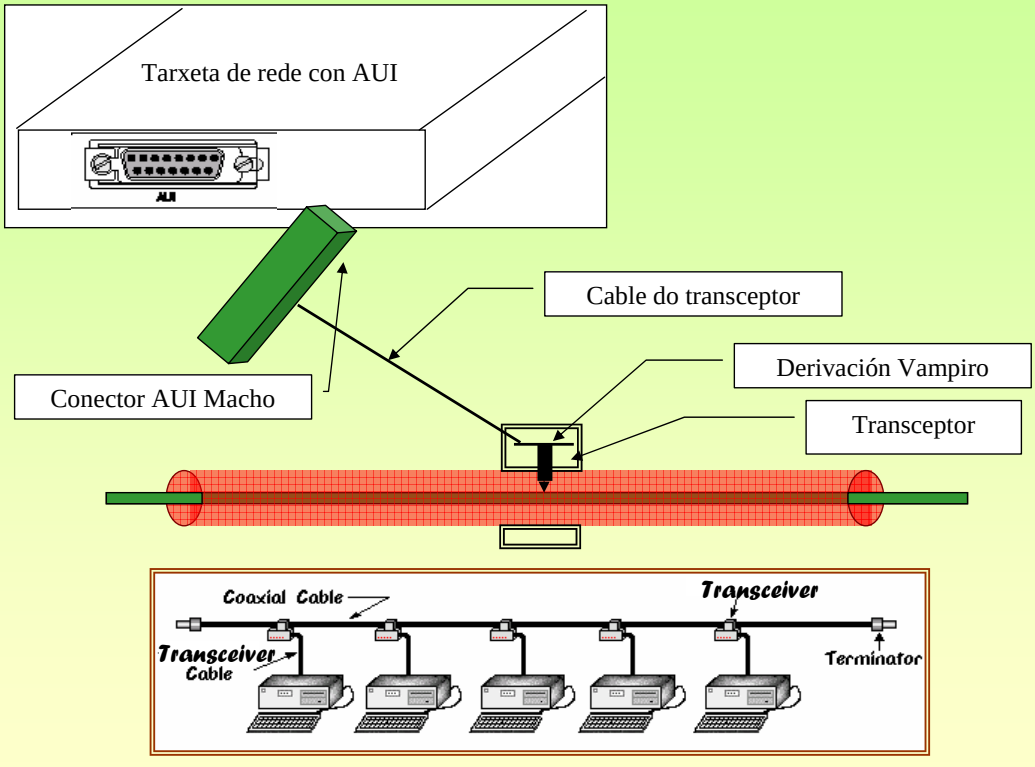
10BASE5

10BASE2

10BASE-T

10ANCHA36

10BASE-F



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 demáis transceptores tamén se enteren.

Suxétase firmemente ó redor do cable

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

Conten 5 pares illados (10 fios)

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 resistencia: Conéctanse nos extremos do cable para absorver o sinal eléctrico

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

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

10BASE5

10BASE2

10BASE-T

10ANCHA36

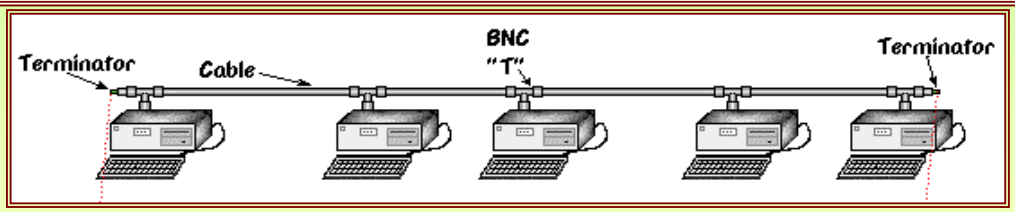
10BASE-F

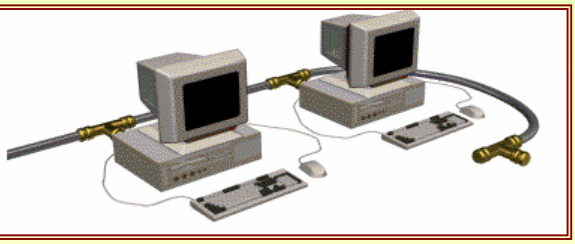
Conector BNC

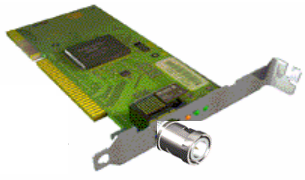
Conector BNC Y

Conector BNC T

Terminador BNC







NIC con conector BNC

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 conecto 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 unilo 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 absorver o sinal eléctrico. Precísase un conector BNC T entre o segmento de cable e a resitencia.

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

10BASE5

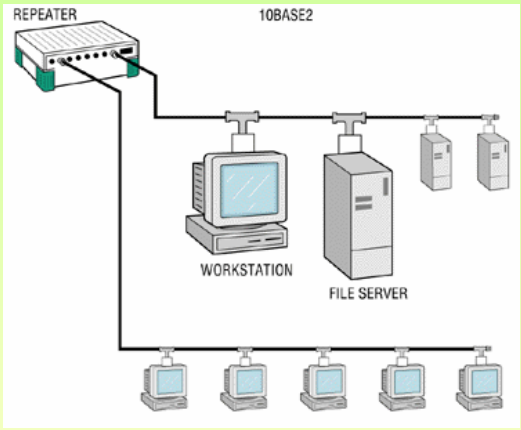
10BASE2

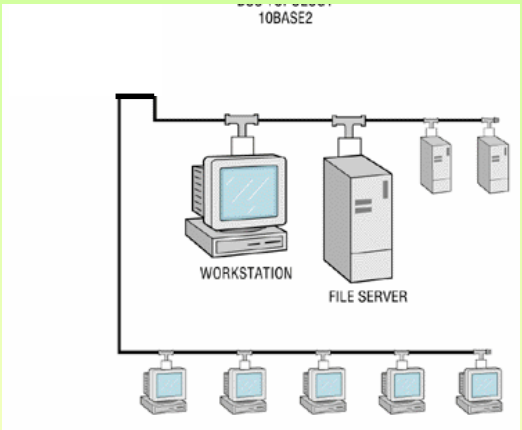
10BASE-T

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.

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

☞ 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 demáis 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)

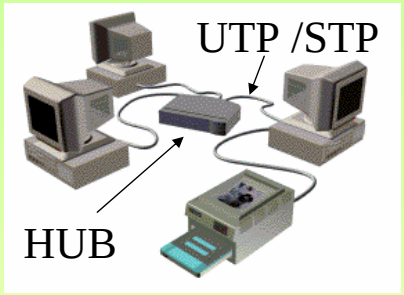
10BASE5

10BASE-2

10BASET

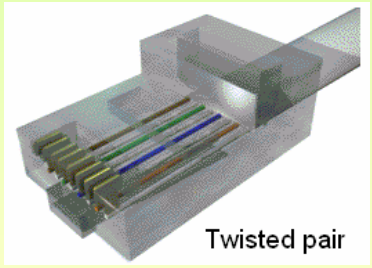
10ANCHA36

10BASE-F



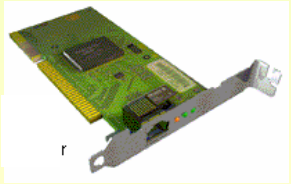
☞ Un Hub é un elemento do nivel físico que serve para conectar ordenadores.

☞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

Redes Área Local - OSI – TCP/IP

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

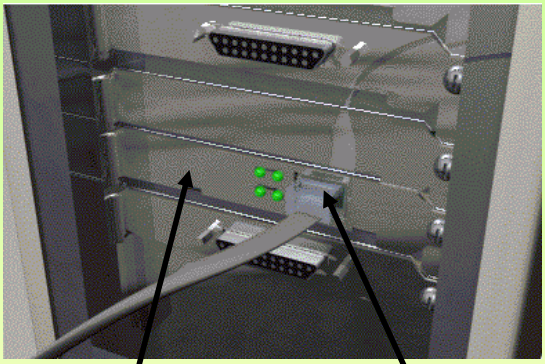
10BASE5

10BASE-2

10BASET

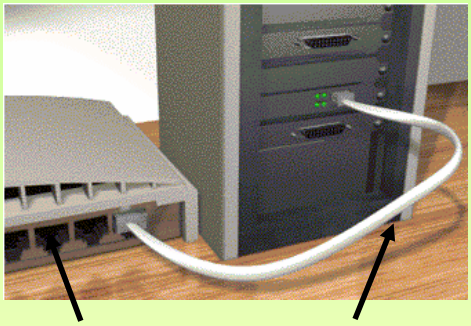
10ANCHA36

10BASE-F



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

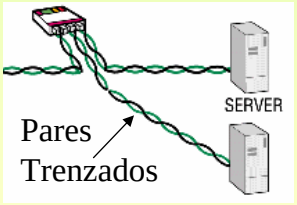
10BASET

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

☞ 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

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

10BASE5

10BASE-2

10BASET

10ANCHA36

10BASE-F

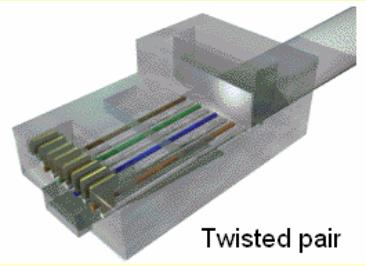
CABLEADO

☞ 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.



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

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

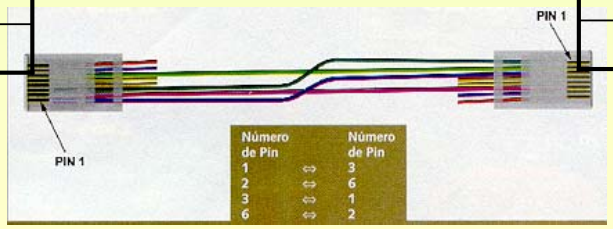
INTERCONEXIÓN DE SÓ DOUS ORDENADORES

☞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):

PIN	COR
1 tx	BV
2 tx	V
3 rx	BL
4	
5	
6 rx	L
7	
8	

COR	PIN
BL	1 tx
L	2 tx
BV	3 rx
	4
	5
V	6 rx
	7
	8



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 trasmiteo polos pins 3 e 6 dos demais portos, co cal xa fai el o cruce. O cable é plano

PIN	COR
1 tx	BV
2 tx	V
3 rx	BL
4	
5	
6 rx	L
7	
8	

Conector RJ 45 ó ordenador

Cable de pares conectado de forma plana

COR	PIN
BV	1 tx
V	2 tx
BL	3 rx
	4
	5
L	6 rx
	7
	8

Conector RJ 45 ó hub

61

Redes Área Local - OSI – TCP/IP

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

10BASE5

10BASE-2

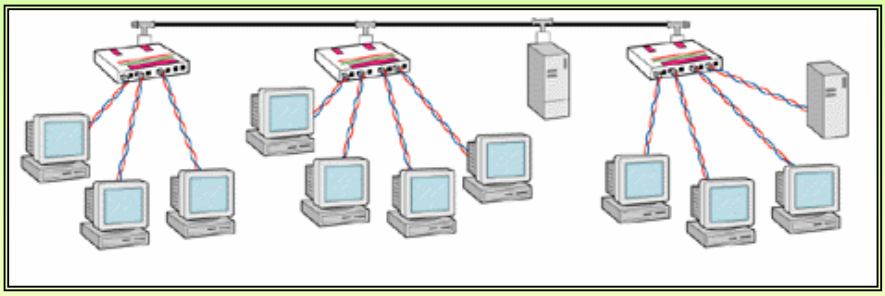
10BASET

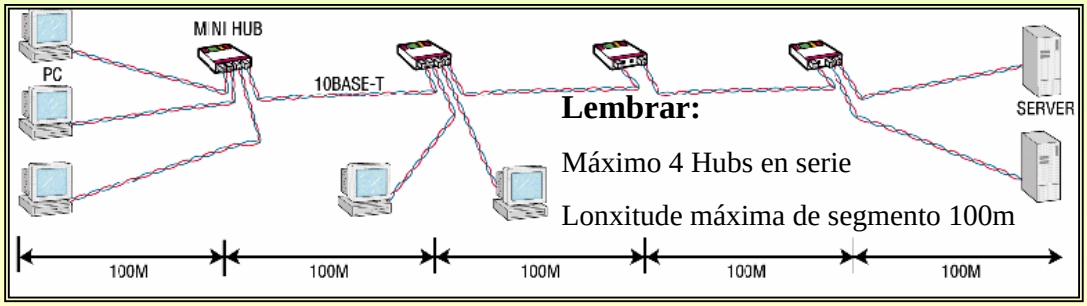
10ANCHA36

10BASE-F

☞**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**





62

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

10BASE5
10BASE-2
10BASET
10ANCHA36
10BASE-F

- E a única especificación para Banda Ancha
- Usa codificación PSK
- Usa cable coxial CATV (Cable de TV) de 75 Ohmios
- A distancia máxima entre extremos é de 3.600 m

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

10BASE5
10BASE-2
10BASE-T
10ANCHA36
10BASEF

- E 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 IEE 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 teléfónicos.

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

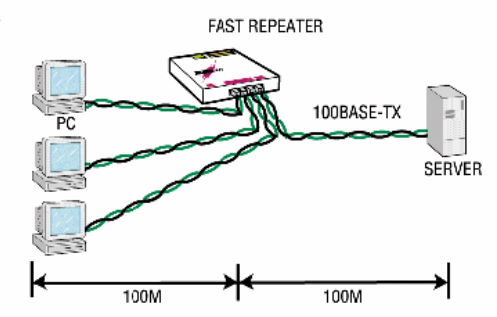
7.3.- Sistemas duales

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

Podense facer combinacións de ambos sistemas

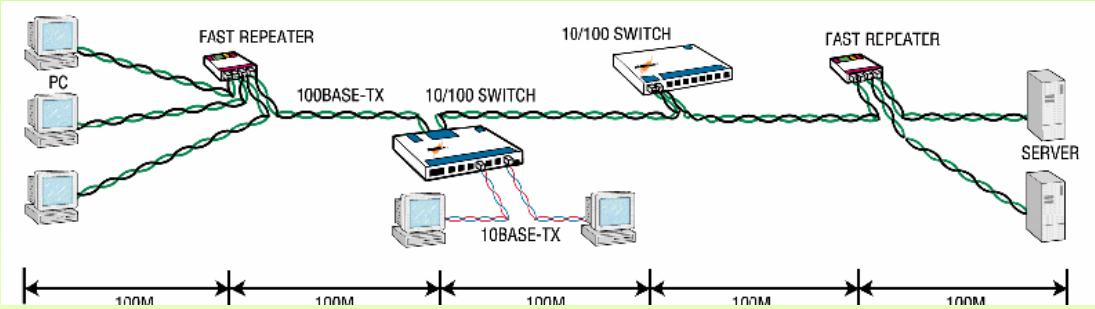
Un elemento dual tenta de ir sempre á máxima velocidade adaptandose ó que hai no outro extremo do cable.

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)

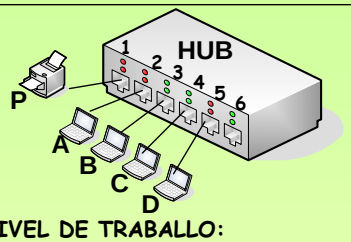
Especificacións para LANs a 1000 Mbps

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**.

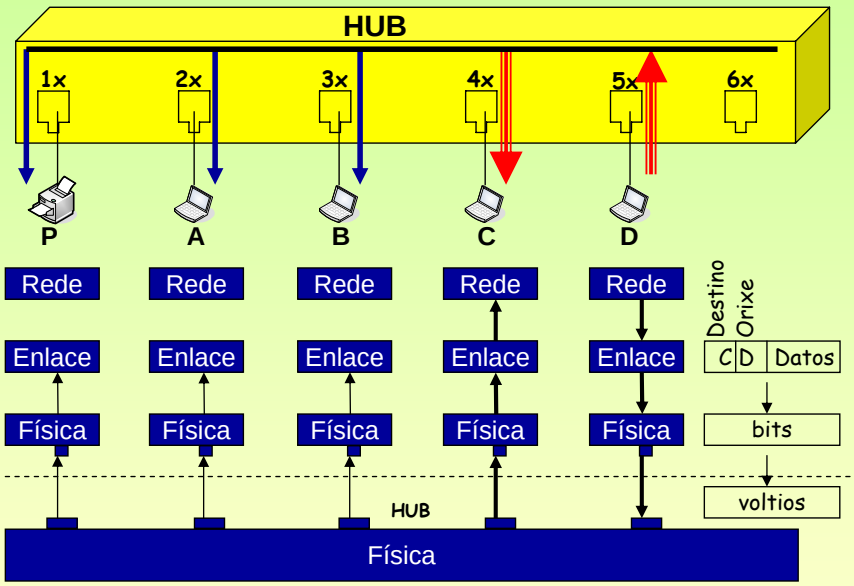
FUNCIONAMENTO:
Todo o que recibe o HUB por un porto é retransmitido polos demais portos

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

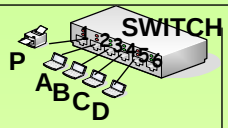
A, B e P: descartan a trama, pois eles non son os destinatarios



CONCLUSIÓNS:
1.- Cando transmite un equipo o hub **inunda** a rede molestando ós demais equipos, salvo ó receptor real.
2.- **Colisións:** cando tx dous ou máis equipos as tramas van chocar, pois por un mesmo porto enviaranse 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:

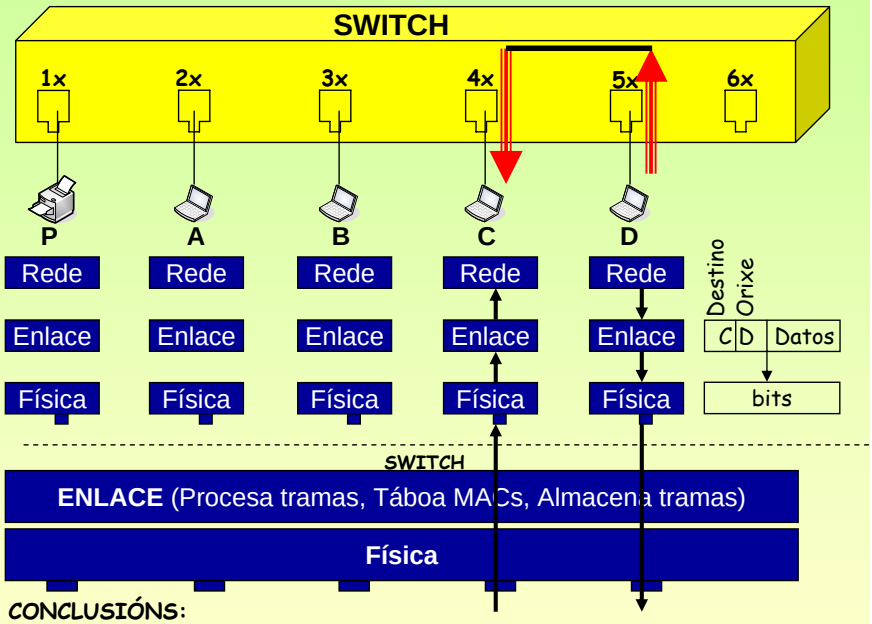
MAC	Porto	Tempo
P	1	10:00:12
B	3	10:00:13
D	5	10:00:27
A	2	10:01:05

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.

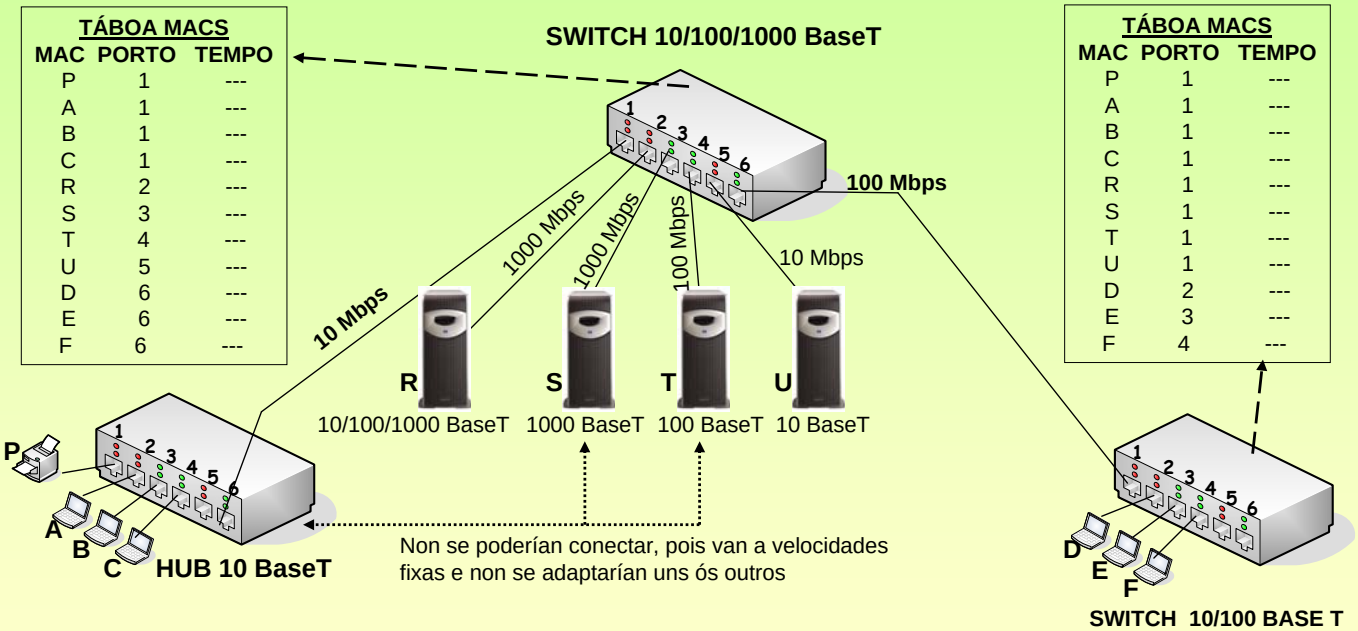
3.- Borra as entradas da táboa cunha antigüidade superior a X segundos



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 procésaas. 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)



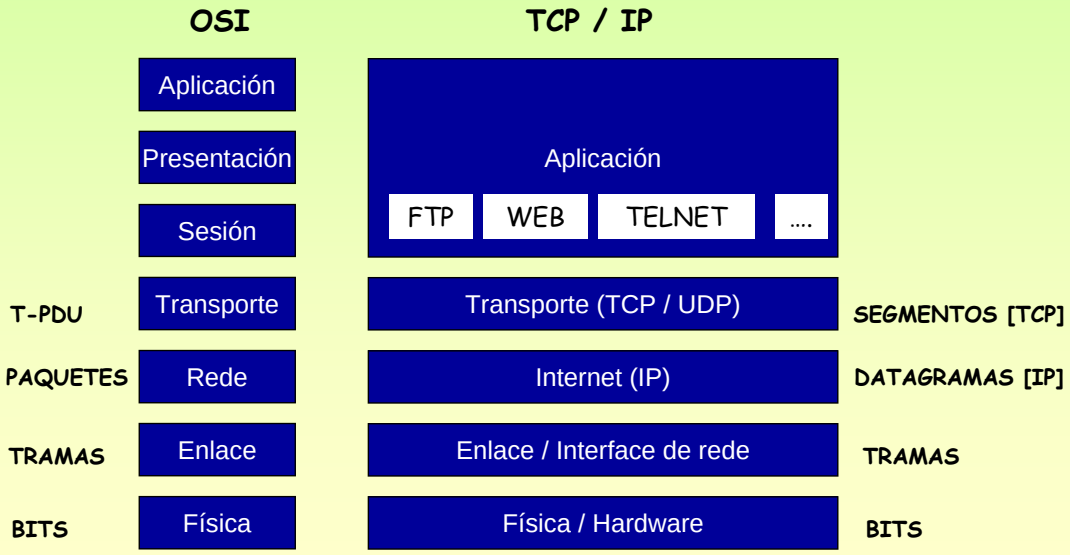
CONCLUSIÓNS:
1.- Un equipo que funcione a 10/100/1000 Mbps pódese conectar con calquera outro elemento.
2.- Un equipo que funcione p.ex. a 10 Mbps pódese conectar a outro que vaia a 10 Mbps ou a 10/100 Mbps ou a 10/100/1000 Mbps
3.- Dous equipos que poidan ir a 2 ou máis velocidades tratarán de ir á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



Redes Área Local - OSI – 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 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 (rede) vai ter un enderezo IP.
Está composto po 32 bits (4 bytes) que se representan con 4 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.

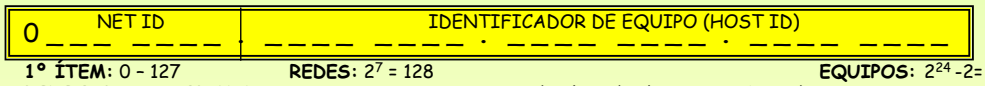
Valores característicos na parte de identificador de equipo:

- Poñer todo **ceros** na parte de equipo é para referirse á rede en si mesma (úsase par enrutar / encamiñar)
  10.0.0.0 (0000 1010 . 0000 0000 . 0000 0000 . 0000 0000) Fai referencia a toda a rede 10

- Poñer todo **uns** na parte de equipo – Multidifusión (Posto nunha dirección destino é para enviar a todos os da mesma rede IP)
  10.255.255.255 (0000 1010 . 1111 1111 . 1111 1111 . 1111 1111) Para transmitir a todos os da rede 10.0.0.0

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

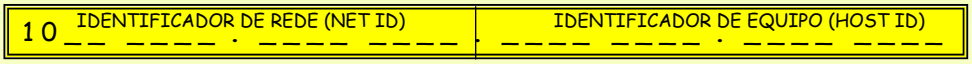
TIPO A



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

Redes Área Local - OSI – TCP/IP

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 restriccións sobre o uso de IPs.

TIPO D

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

1º ÍTEM: 240 – 247

8.1.- Enderezos IP

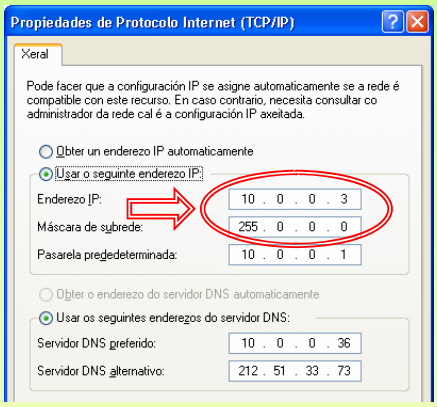
☞ MÁSCARAS

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

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

Redes Área Local - OSI – TCP/IP

8.1.- Enderezos IP

☞ MÁIS SOBRE MÁSCARAS

Outra forma de representar as máscaras é indicando o número de **1s** que posúe.

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 é 255.0.0.0

O equipo sabe cal é a súa **rede-IP** ó facer un AND BINARIO do 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

Estaríamos a falar da 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.

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.

8.1.- Enderezos IP

☞ E REMATAMOS COAS MÁSCARAS

Desafortunadamente, non tódalas máscaras son /8, /16 ou /24 (esto 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)
10.1.5.6 / 23 (Máscara 255.255.254.0)
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 si, pois **están na mesma rede –IP**. Os primeiros 23 bits son iguais.
O terceiro equipo non se pode comunicar cos outros. Está nunha rede-IP distinta. Non coinciden os 23 primeiros bits.

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 pódeselle poñer a un equipo.**
10.1.4.6 /30	0000 1010 . 0000 0001 . 0000 0100 .	0000 01	10 **Esta IP pódeselle 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

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.

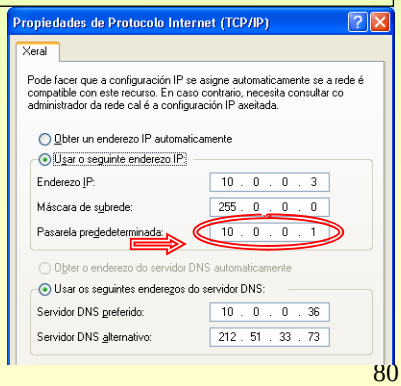
Un conductor ó chegar a unha rotonda encamiña o seu coche en función das sinais de dirección.

☞ 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 conductor 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

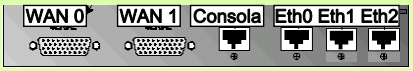
☞ CONFIGURAR UN ROUTER: IPs

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

ROUTER R



ROUTER S

Eth 0: 10.0.0.1 /8 | Eth 1: 130.2.0.1 /16

SALA 1 – 10.0.0.0 /8

A — IP/MASK: 10.0.0.2 /8 — P. ENLACE: 10.0.0.1
B — 10.0.0.3 /8 — 10.0.0.1

SALA 2 – 130.2.0.0 /16

C — IP/MASK: 130.2.0.2 /16 — P. ENLACE: 130.2.0.1
D — 130.2.0.3 /16 — 130.2.0.4

SALA 3 – 11.1.0.0 /16

E — IP/MASK: 11.1.0.2 /16 — P. ENLACE: 11.1.0.1
F — 11.1.0.3 /16 — 11.1.0.1

Eth 0: 130.2.0.4 /16 | Eth 1: 11.1.0.1 /16

Eth 2: 11.2.0.1 /16

SALA 4 – 11.2.0.0 /16

G — IP/MASK: 11.2.0.2 /16 — P. ENLACE: 11.2.0.1
H — 11.2.0.3 /16 — 11.2.0.1

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 vaille enviar un paquete ó equipo G

ROUTER R
Eth 0: 10.0.0.1 /8 | Eth 1: 130.2.0.1 /16
ROUTER S
SALA 1 – 10.0.0.0 /8
A — IP/MASK: 10.0.0.2 /8 — P. ENLACE: 10.0.0.1
B — 10.0.0.3 /8 — 10.0.0.1
SALA 2 – 130.2.0.0 /16
C — IP/MASK: 130.2.0.2 /16 — P. ENLACE: 130.2.0.1
D — 130.2.0.3 /16 — 130.2.0.4
SALA 3 – 11.1.0.0 /16
E — IP/MASK: 11.1.0.2 /16 — P. ENLACE: 11.1.0.1
F — 11.1.0.3 /16 — 11.1.0.1
Eth 0: 130.2.0.4 /16 | Eth 1: 11.1.0.1 /16
Eth 2: 11.2.0.1 /16
SALA 4 – 11.2.0.0 /16
G — IP/MASK: 11.2.0.2 /16 — P. ENLACE: 11.2.0.1
H — 11.2.0.3 /16 — 11.2.0.1

Se o **equipo A** se quere comunicar co **equipo G** debe enviar o seguinte datagrama:

11.2.0.2	10.0.0.2	DATOS A ENVIAR
Destino	Orixe	

O equipo A precisa saber se o DESTINATARIO está na mesma rede-IP ca el ou en distinta.
- No primeiro caso **A** enviaría o paquete dentro da súa rede.
- No segundo caso enviará o paquete ó router que teña configurado como porta de enlace, para que este o encamiñe.

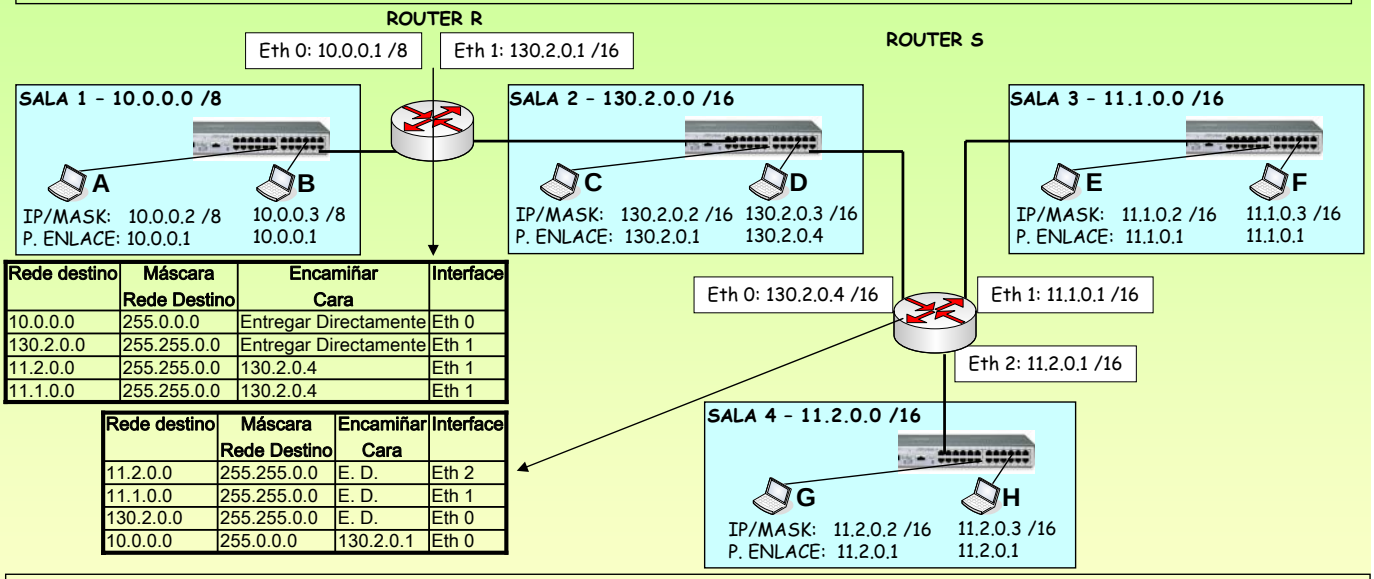
O equipo **A** fai un AND da **súa** máscara coas IPs ORIXE e DESTINO do paquete, deste xeito **A** saberá se destino e orixe están na mesma rede IP:

	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.

8.2.- Routers IP

☞ CONFIGURAR UN ROUTER: TÁBOAS DE ENCAMIÑAMENTO (I)



Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
10.0.0.0	255.0.0.0	Entregar Directamente	Eth 0
130.2.0.0	255.255.0.0	Entregar Directamente	Eth 1
11.2.0.0	255.255.0.0	130.2.0.4	Eth 1
11.1.0.0	255.255.0.0	130.2.0.4	Eth 1

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 2
11.1.0.0	255.255.0.0	E. D.	Eth 1
130.2.0.0	255.255.0.0	E. D.	Eth 0
10.0.0.0	255.0.0.0	130.2.0.1	Eth 0

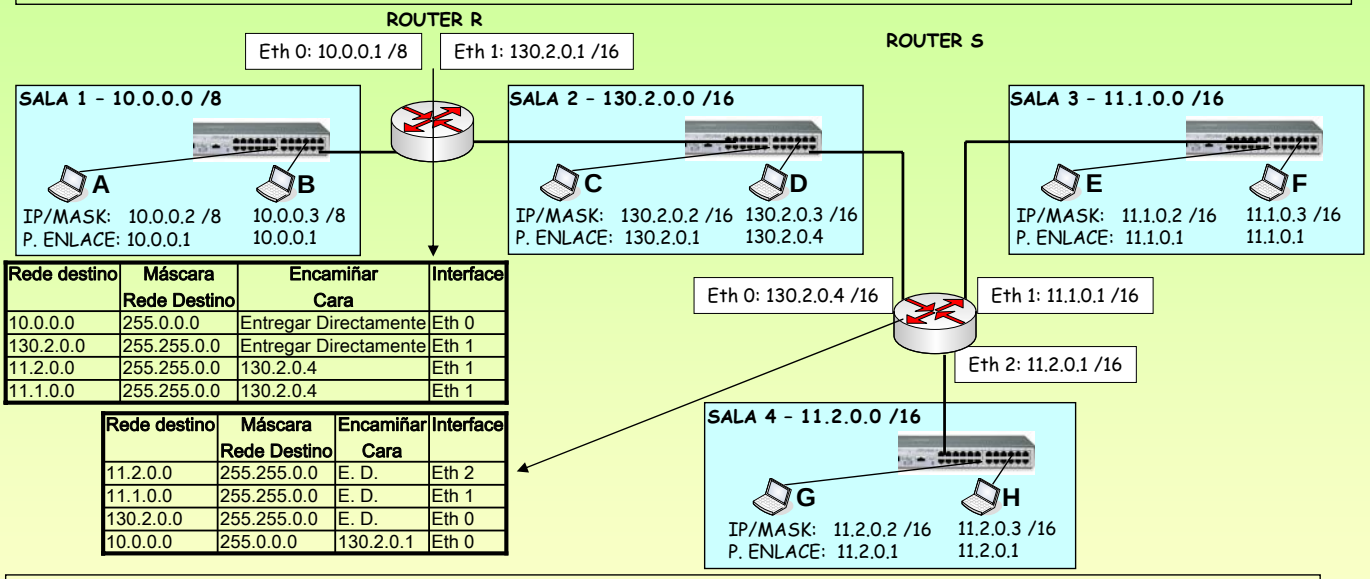
O **equipo A** decidiu enviar o anterior paquete ó router. Este fará o que fai un carteiro, mirará a dirección de destino. Neste caso: 11.2.0.2
O router realiza una AND da IP DESTINO coa primeira máscara da táboa de ruteo e mira se coincide coa columna **Rede Destino.**
- **SE COINCIDE:** envía o paquete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



Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
10.0.0.0	255.0.0.0	Entregar Directamente	Eth 0
130.2.0.0	255.255.0.0	Entregar Directamente	Eth 1
11.2.0.0	255.255.0.0	130.2.0.4	Eth 1
11.1.0.0	255.255.0.0	130.2.0.4	Eth 1

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 2
11.1.0.0	255.255.0.0	E. D.	Eth 1
130.2.0.0	255.255.0.0	E. D.	Eth 0
10.0.0.0	255.0.0.0	130.2.0.1	Eth 0

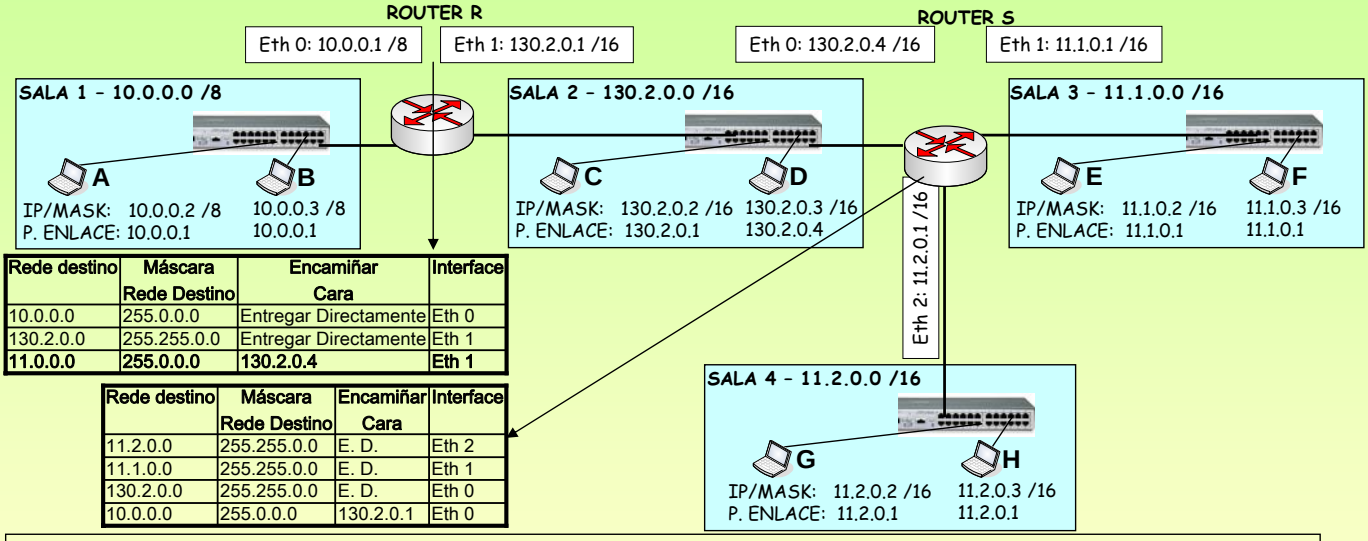
Un router está interesado no DESTINO dos paquetes que lle chegan, ó igual que as oficinas de correos.

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 mandarlla ó seu destinatario final.

8.2.- Routers IP

☞ CONFIGURAR UN ROUTER: TÁBOAS DE ENCAMIÑAMENTO (II)



Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
10.0.0.0	255.0.0.0	Entregar Directamente	Eth 0
130.2.0.0	255.255.0.0	Entregar Directamente	Eth 1
11.0.0.0	**255.0.0.0**	**130.2.0.4**	**Eth 1**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 2
11.1.0.0	255.255.0.0	E. D.	Eth 1
130.2.0.0	255.255.0.0	E. D.	Eth 0
10.0.0.0	255.0.0.0	130.2.0.1	Eth 0

Débese 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.

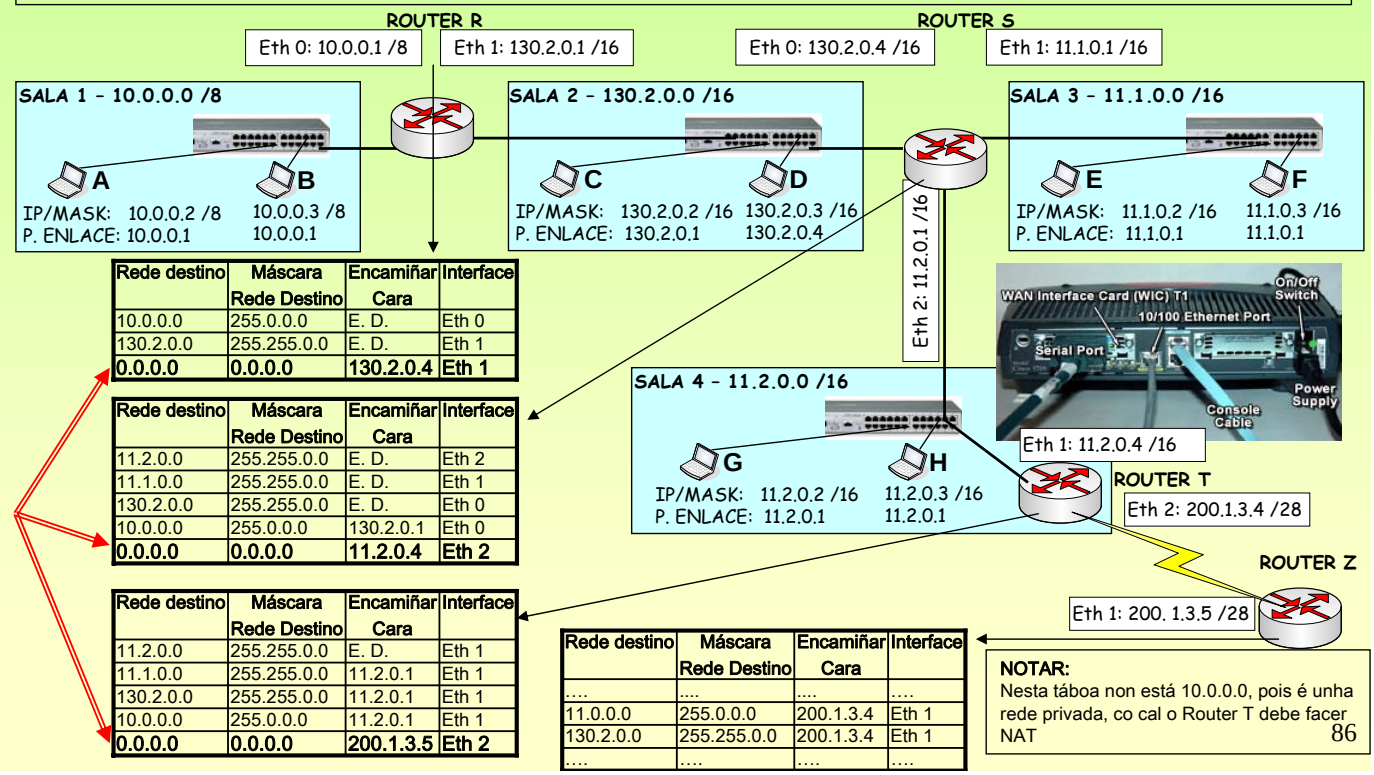
Se a rede 11.0.0.0 é toda da empresa. E se esta é a configuración final da rede, obsérvese como se podería modificar a táboa de encamiñamento do ROUTER R.

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



Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
10.0.0.0	255.0.0.0	E. D.	Eth 0
130.2.0.0	255.255.0.0	E. D.	Eth 1
0.0.0.0	**0.0.0.0**	**130.2.0.4**	**Eth 1**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 2
11.1.0.0	255.255.0.0	E. D.	Eth 1
130.2.0.0	255.255.0.0	E. D.	Eth 0
10.0.0.0	255.0.0.0	130.2.0.1	Eth 0
0.0.0.0	**0.0.0.0**	**11.2.0.4**	**Eth 2**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 1
11.1.0.0	255.255.0.0	11.2.0.1	Eth 1
130.2.0.0	255.255.0.0	11.2.0.1	Eth 1
10.0.0.0	255.0.0.0	11.2.0.1	Eth 1
0.0.0.0	**0.0.0.0**	**200.1.3.5**	**Eth 2**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
....	....	....	....
11.0.0.0	255.0.0.0	200.1.3.4	Eth 1
130.2.0.0	255.255.0.0	200.1.3.4	Eth 1
....	....	....	....

NOTAR:
Nesta táboa non está 10.0.0.0, pois é unha rede privada, co cal o Router T debe facer NAT

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 Provedor 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.
Dinse 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

Redes Área Local - OSI – TCP/IP

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 adáptanse 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 envíalla. 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, desfaise del tan pronto como poida e por calquera liña.

DISTRIBUÍDOS:

Equivale a ter Gardas nas rotondas pero cada un comunícase 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 print
===========================================================================
ILista de interfaces
0x1 ........................... MS TCP Loopback interface
0x4 ...00 0b 6a 2a 74 9a ...... VIA VT6102 Rhine II Fast Ethernet Adapter - Mini
puerto del administrador de paquetes
===========================================================================
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de acceso   Interfaz  Métrica
          0.0.0.0          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

L:\>
```

```
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
                    de puerta de enlace,
                    comandos, se borrarán las tablas antes de ejecutarse el
                    comando.
  -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.
```


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>]          List kernel routing tables
       route [-v] [-FC] {add|del|flush} ...  Modify routing table for AF.

       route {-h|--help} [<AF>]              Detailed usage syntax for specified AF

       route {-V|--version}                  Display version/author and exit.

        -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) ax25 (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)

☞ MÁIS 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)

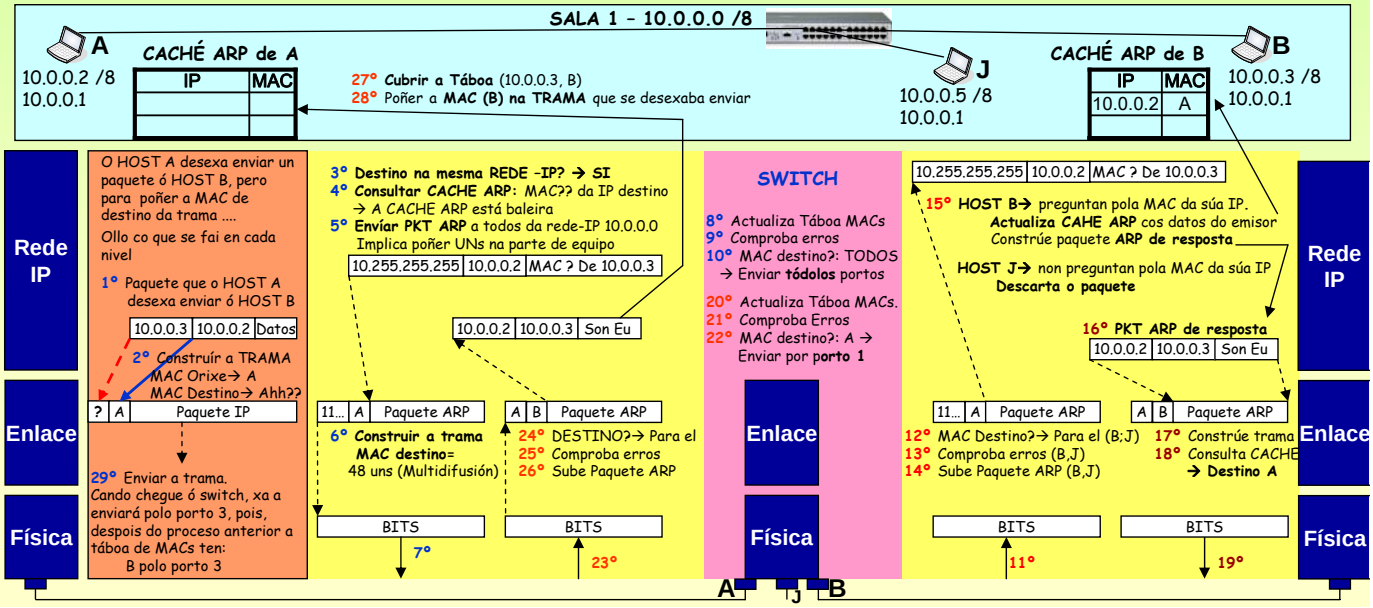
NIVEL IP: constrúe o datagrama cos **enderezos** orixe (10.0.0.2) e destino (10.0.0.3) e o campo de **datos.** Comproba se o destino está na mesma rede IP

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)

☞ MÁIS 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.

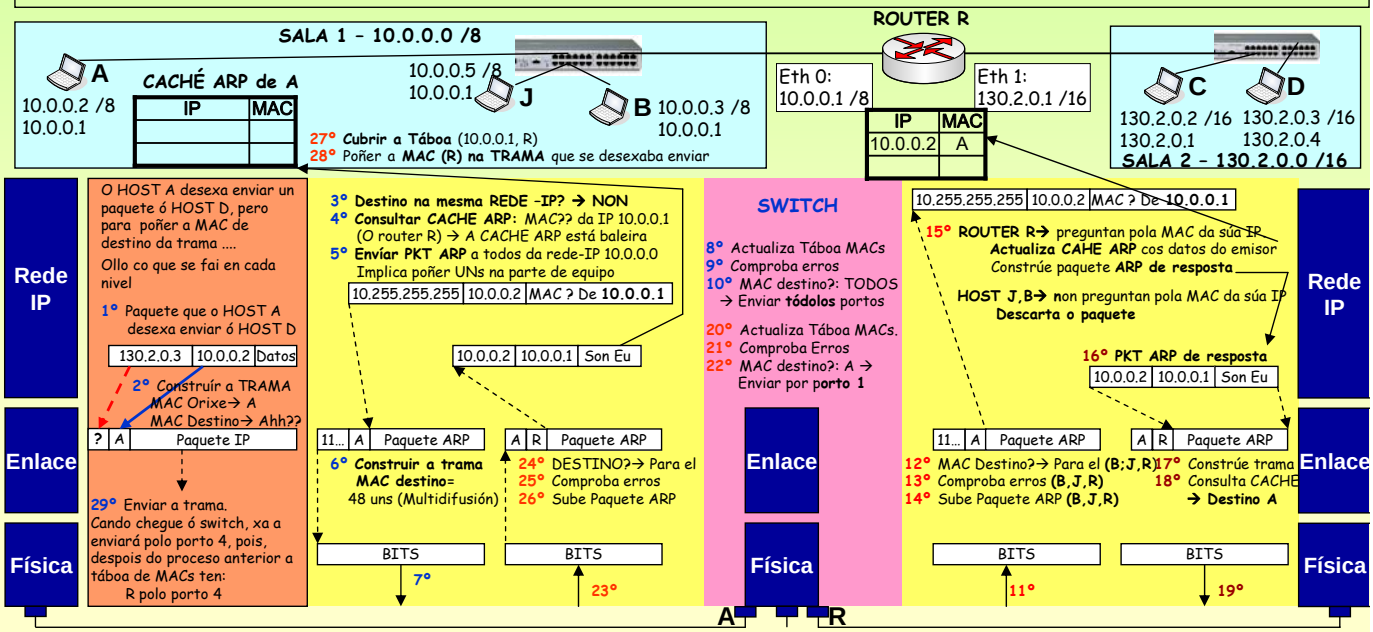
NIVEL IP: constrúe o datagrama cos **enderezos** orixe (10.0.0.2) e destino (130.2.0.3) e o campo de **datos.** Comproba se o destino está na mesma rede IP **É AQUÍ,** onde radica a diferencia co caso anterior. O **host A** tenlle que enviar o paquete ó Router para que el o encamiñe, co cal no nivel 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.

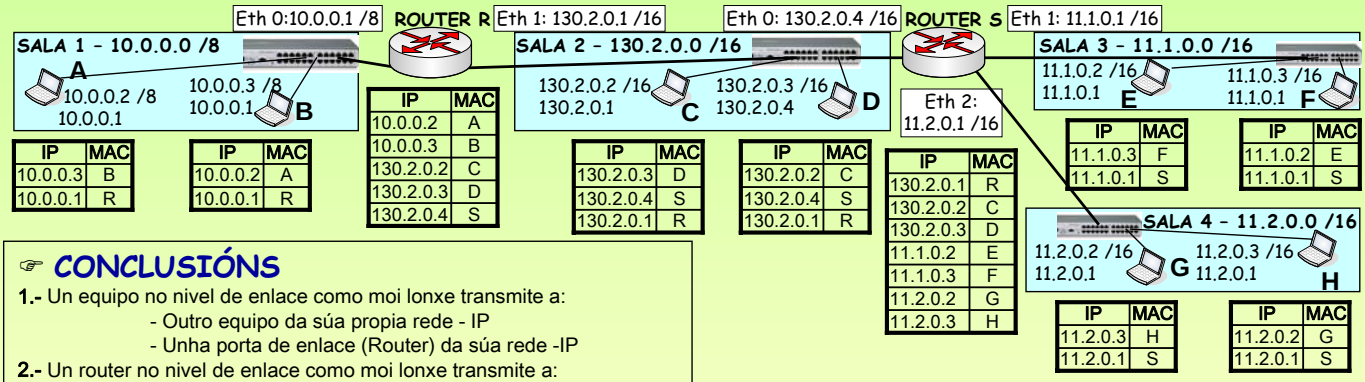
Unha vez que o HOST A averigue a MAC do router R enviaralle a trama a este. Logo, o router terá que facer todo o proceso pero cara á SALA 2.



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:



IP	MAC
10.0.0.3	B
10.0.0.1	R

IP	MAC
10.0.0.2	A
10.0.0.1	R

IP	MAC
10.0.0.2	A
10.0.0.3	B
130.2.0.2	C
130.2.0.3	D
130.2.0.4	S

IP	MAC
130.2.0.3	D
130.2.0.4	S
130.2.0.1	R

IP	MAC
130.2.0.2	C
130.2.0.4	S
130.2.0.1	R

IP	MAC
130.2.0.1	R
130.2.0.2	C
130.2.0.3	D
11.1.0.2	E
11.1.0.3	F
11.2.0.2	G
11.2.0.3	H

IP	MAC
11.1.0.3	F
11.1.0.1	S

IP	MAC
11.1.0.2	E
11.1.0.1	S

IP	MAC
11.2.0.3	H
11.2.0.1	S

IP	MAC
11.2.0.2	G
11.2.0.1	S

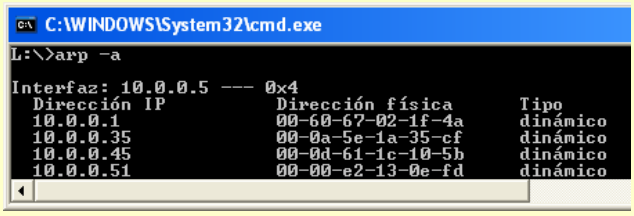
☞ CONCLUSIÓNS

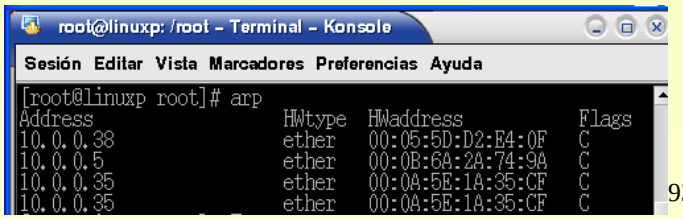
1.- Un equipo no nivel de enlace como moi lonxe transmite a:
- Outro equipo da súa propia rede - IP
- Unha porta de enlace (Router) da súa rede -IP

2.- 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





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

	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Encabezado	Versión	HLEN	Tipo de Servizo (ToS)	Lonxitude Total
	Identificación		Bandeiras	Desprazamento do fragmento
	Tempo de Vida (TTL)		Protocolo	Control de erros da cabeceira (Header CheckSum)
	ENDEREZO IP ORIXE			
	ENDEREZO IP DESTINO			
	OPCIÓNS IP (Se hai algunha)			
	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). Esto é 5x4= 20 bytes.
LONXITUDE 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 elimínano.
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)

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 coñecese 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.

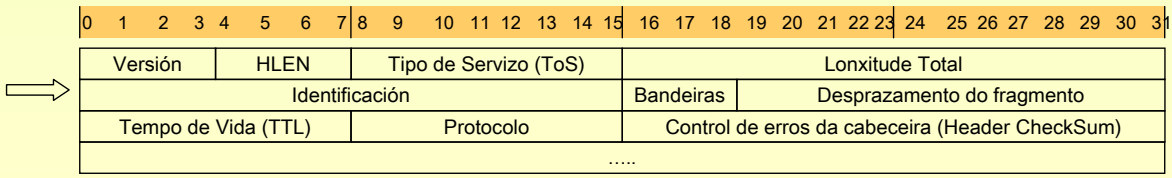
IDENTIFICACIÓN: identifica o número de paquete, se este se fragmenta, cada fragmento levará a mesma IDENTIFICACIÓN. Así o receptor saberá que fragmentos se corresponden a cada paquete orixinal.

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 fragamento).

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.



Redes Área Local - OSI – TCP/IP

8.4.- Datagrama IP

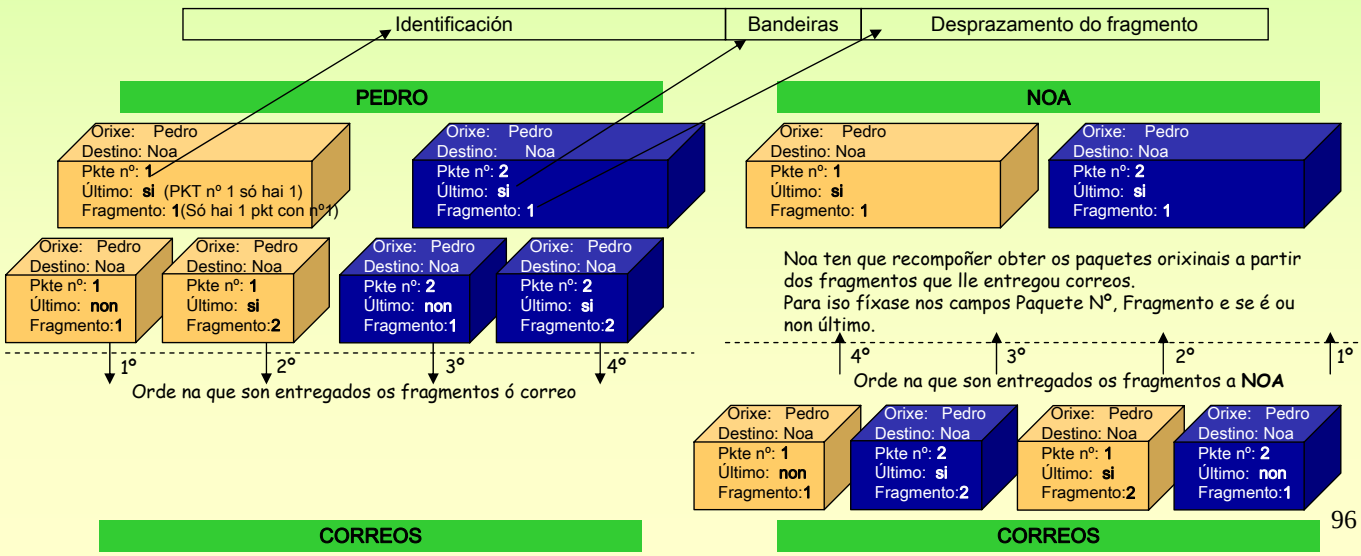
☞ IP (Internet Protocol) – A fragmentación: Exemplo de correos (II)

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 obrígao 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.

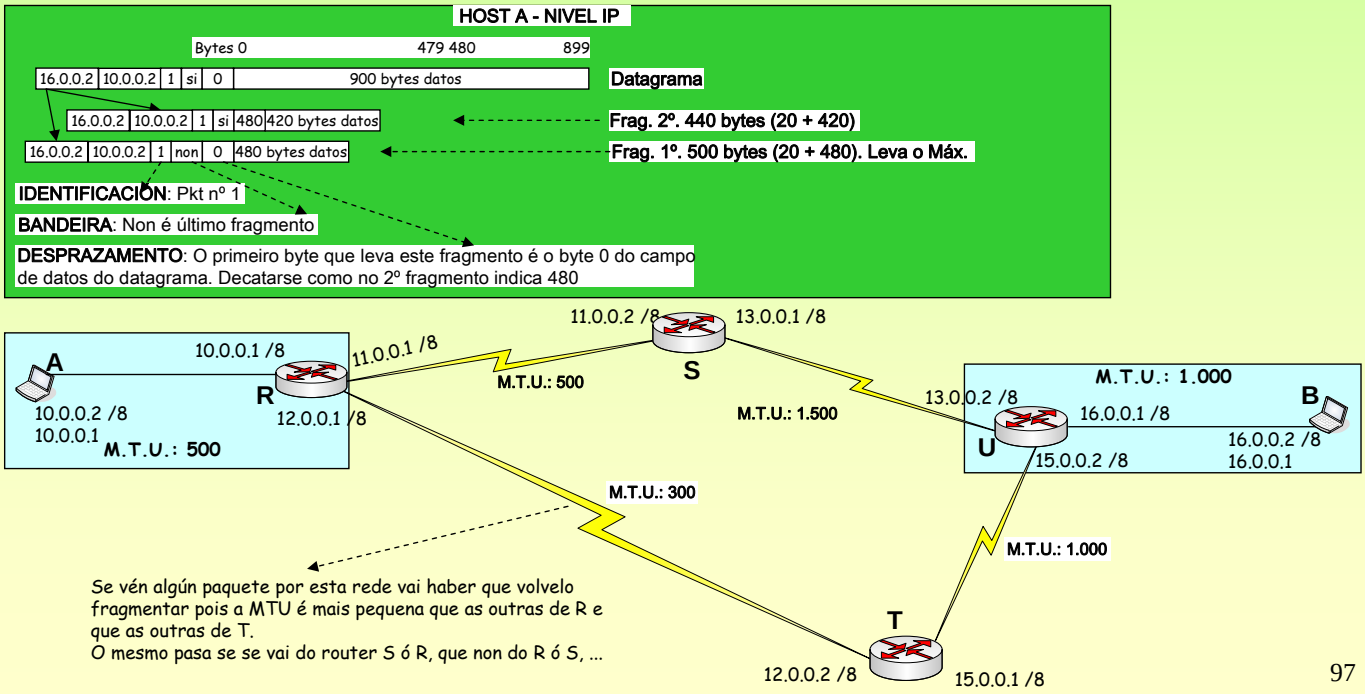
Obsérvese que Pedro envía os fragmentos nunha orde e que correos llos entrega a Noa noutra orde distinta. É Noa quen, coa infomación que ven en cada fragmento ten que recompoñer os paquetes orixinais.



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.

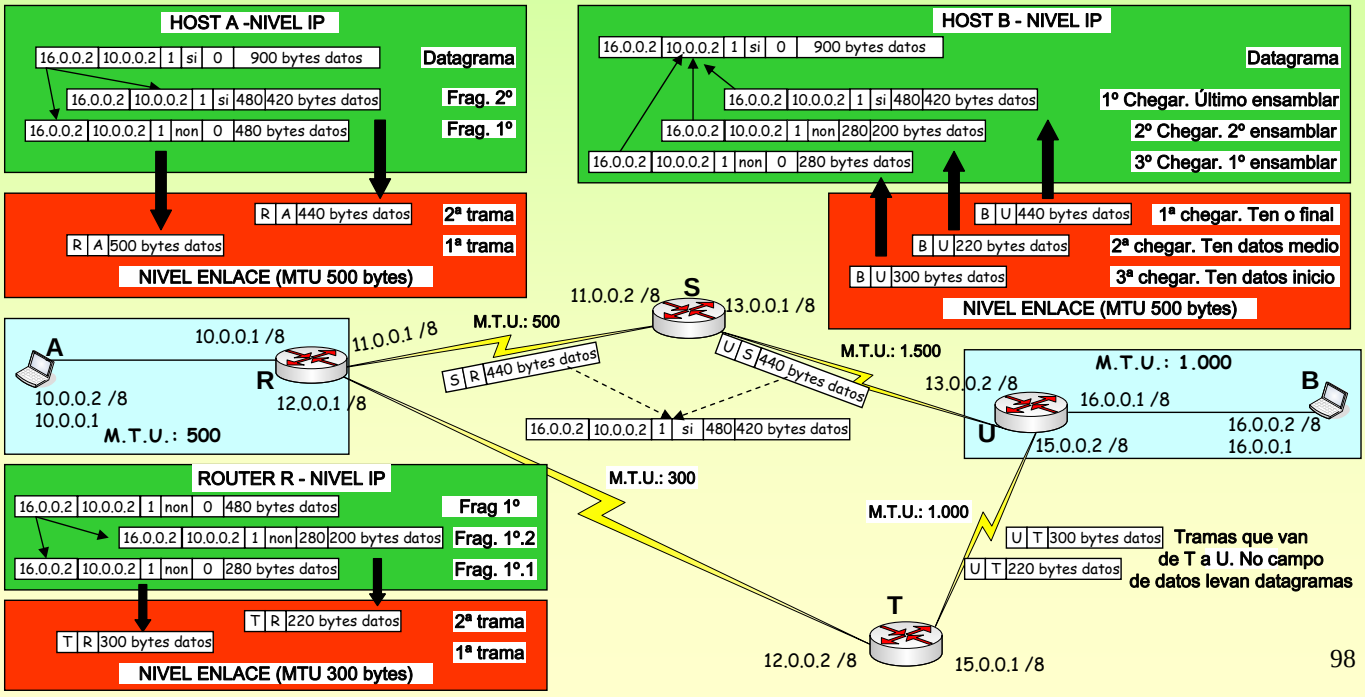


Redes Área Local - OSI – TCP/IP

8.4.- Datagrama IP

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

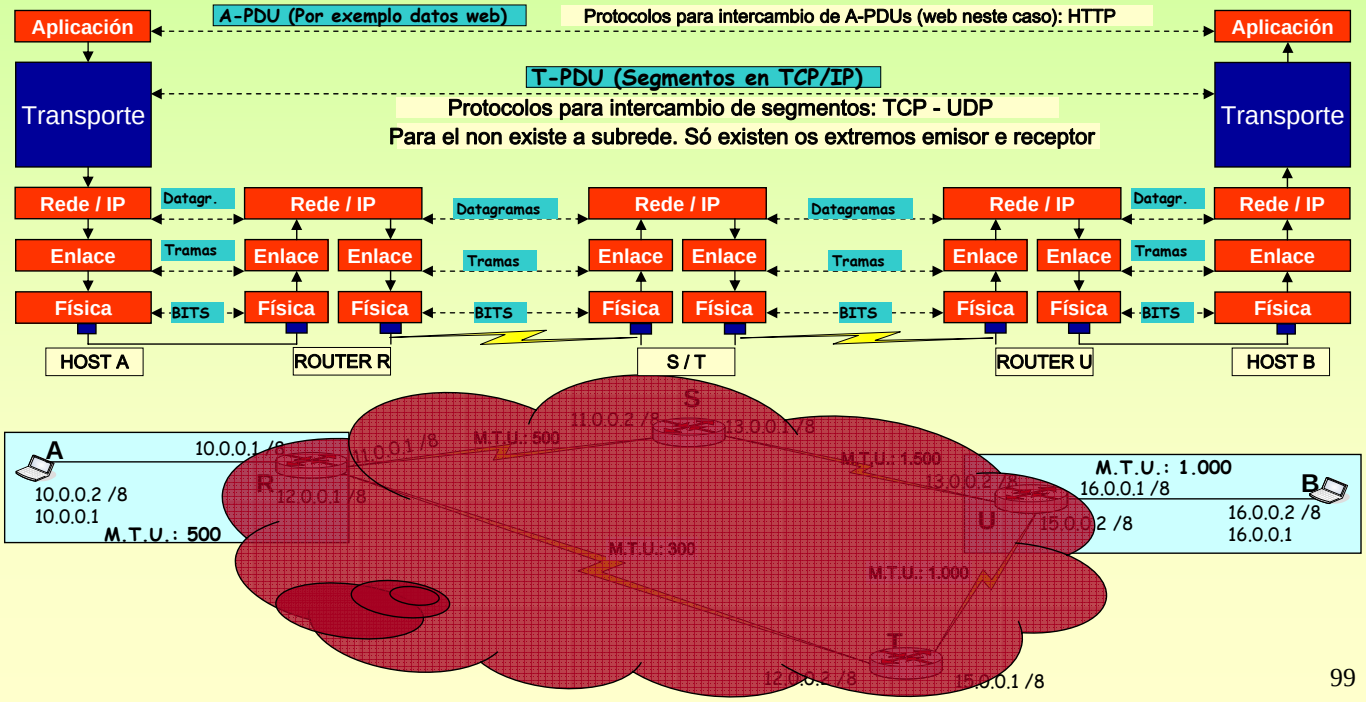
O router R envía o fragmento 2º pola liña superior e o outro pola inferior, que ten MTU=300, co cal ten que volver a fragmentar o fragmento 1º.
No HOST B recíbense os 3 fragmentos desordenados, é responsabilidade do NIVEL IP ordenalos e ensamblalos na orde correcta.
Se non chegou un fragmento, ou a cabeceira 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.



8.5.- TCP (Transport 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, físico).
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...

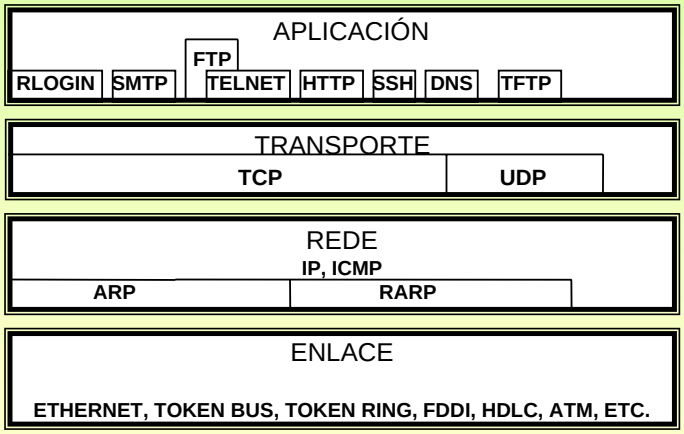


8.5.- TCP (Transport Control Protocol)

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



8.5.- TCP (Transport Control Protocol)

☞ TCP (Transmisión 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 asínalle un porto dos que teña libres. (Exemplo: navegador web, cliente ftp, etc)

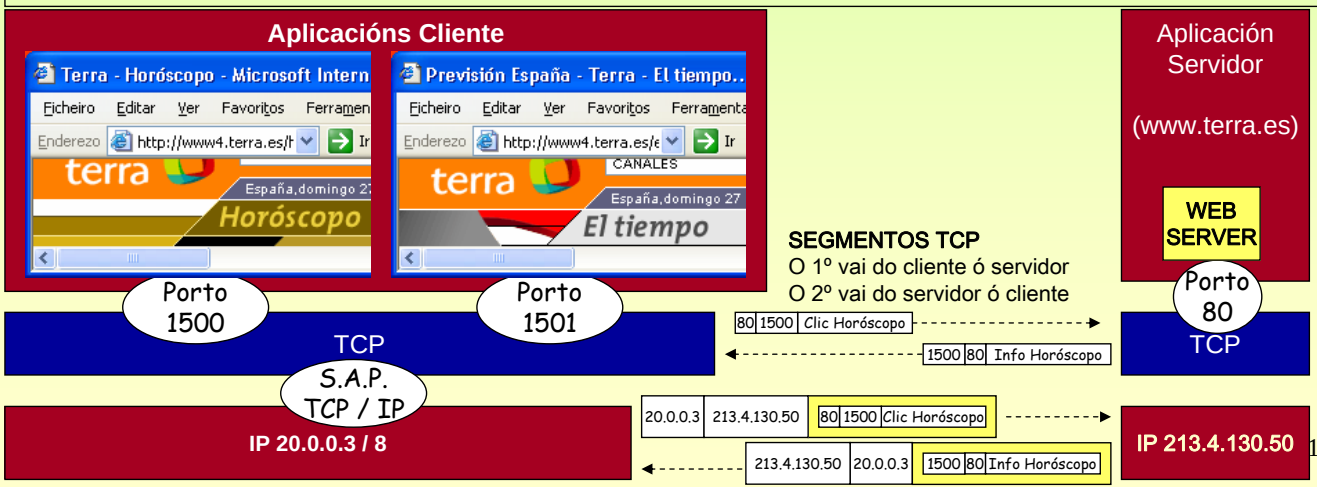
APLICACIÓN SERVIDOR: As aplicacións servidor están sempre escoitando nun porto chamado **BEN COÑECIDO.** Este porto é configurado manualmente. Exemplos **PORTOS BEN COÑECIDOS:**

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) asínalle 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: circuíto 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)



Redes Área Local - OSI – TCP/IP

8.5.- TCP (Transport Control Protocol)

☞ TCP (Transmisión 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.

ASENTIMENTO: **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: Permítelle ós 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 negóciase 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.

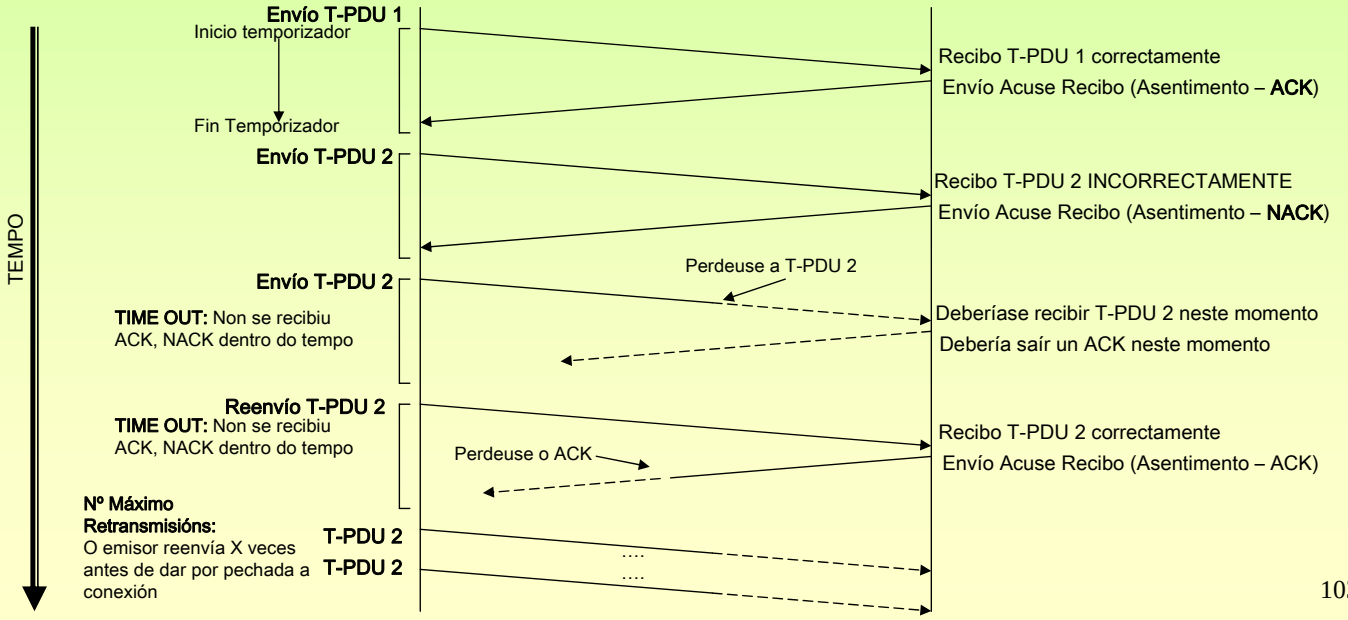
8.6.- TCP – Control de fluxo

☞ 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.
TIME OUT: indica que expirou o temporizador. Cando se trata de conectar a unha páxina e pasado un tempo dá erro.
Nº MAX. RETRANSMIS.: o emisor envía un mesmo bloque de información nun número máximo de X veces. Se se acada péchase a conexión



Redes Área Local - OSI – TCP/IP

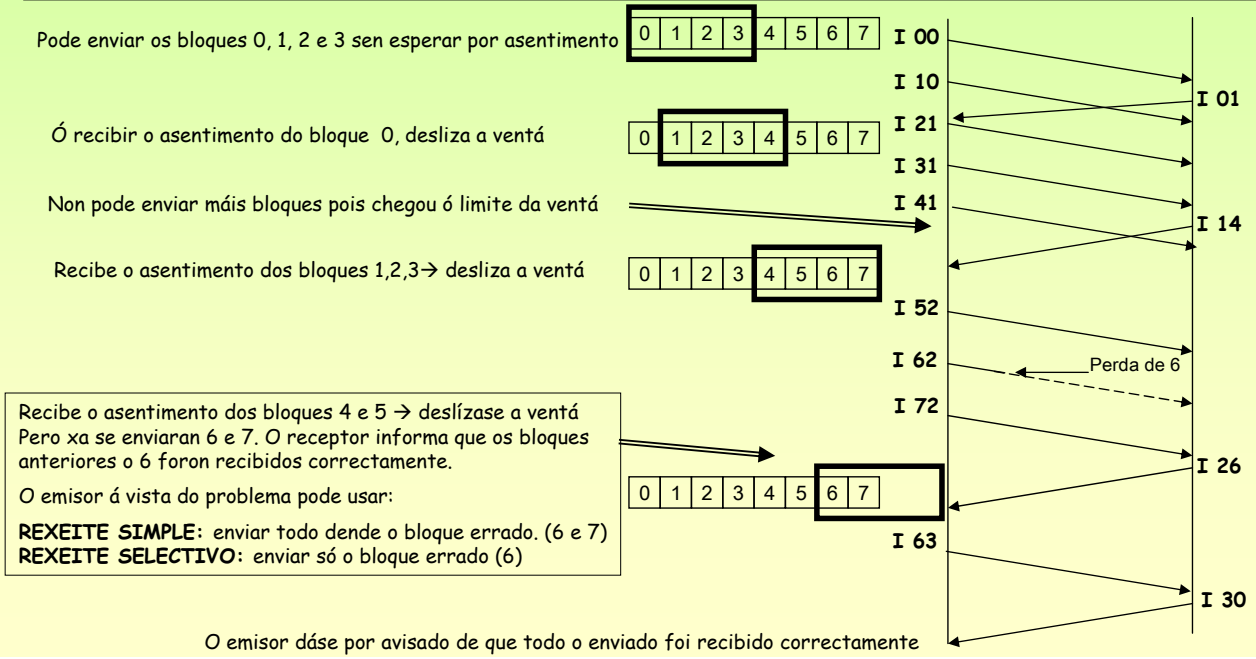
8.6.- TCP – Control de fluxo

☞ 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:** Nº 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.



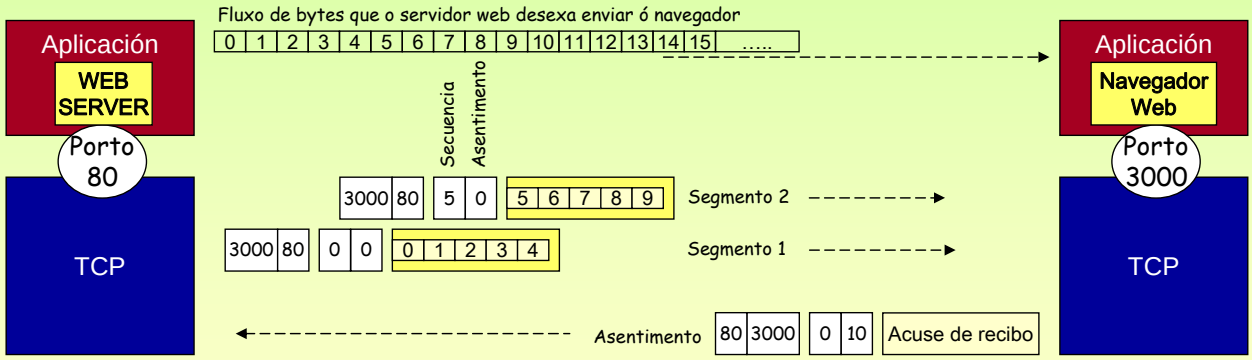
8.6.- TCP – Control de fluxo

☞ 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: Dados: 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.

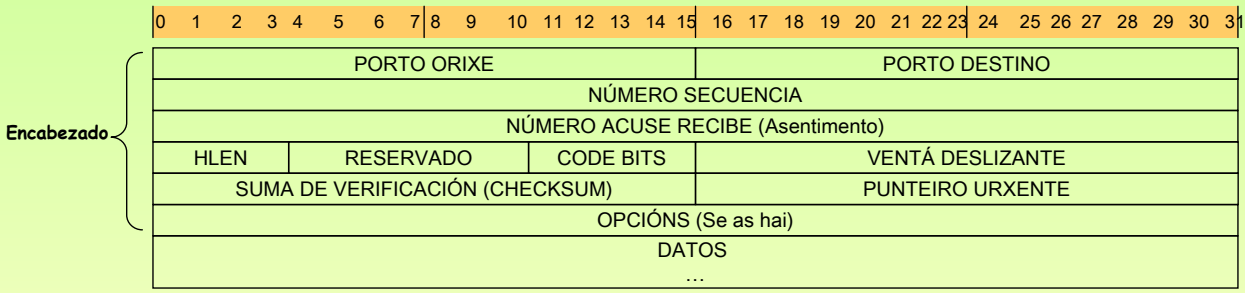
Deste xeito o nivel TCP é independente do IP, pois se este perde fragmentos, datagramas enteiros ou estes chegan con erros, ó non subir nada ó nivel TCP, este vaise decatar de que algo anormal está a pasar.

105

8.6.- TCP – Segmento

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

Os segmentos intercámbianse para establecer conexións, transferir datos, enviar acuses de recibo (asentimentos), indicar o tamaño da ventá deslizante 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: Conteñen 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 ultimo 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 *fóra 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.

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

106

8.6.- TCP – Segmento

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

Os segmentos intercámbianse para establecer conexións, transferir datos, enviar acuses de recibo (asentimentos), indicar o tamaño da ventá deslizante e pechar as conexións:
Un acuse de recibo que vaia do HOST A ó B, pode levar datos de A a B.

	0 1 2 3	4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Encabezado	PORTO ORIXE			PORTO DESTINO	
	NÚMERO SECUENCIA				
	NÚMERO ACUSE RECIBE (Asentimento)				
	HLEN	RESERVADO	CODE BITS	VENTÁ DESLIZANTE	
	SUMA DE VERIFICACIÓN (CHECKSUM)			PUNTEIRO URXENTE	
	OPCIÓNS (Se as hai)				
	DATOS …				

☞ 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, ainda 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.

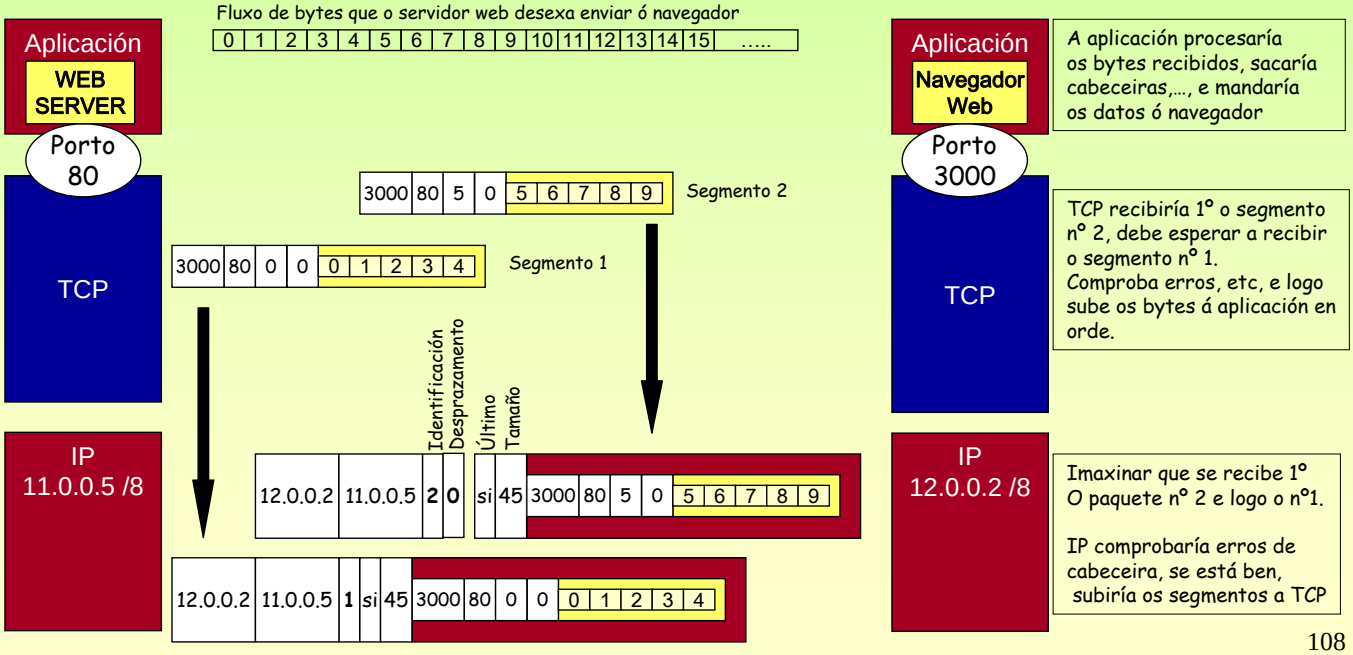
Nº ASENTIMENTO: O receptor informa ó emisor cal é o seguinte byte polo que está a esperar, confirmándolle así o emisor, que todo o enviado ata ese byte - 1 foi recibido correctamente.

8.7.- Relación entre TCP/IP

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

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

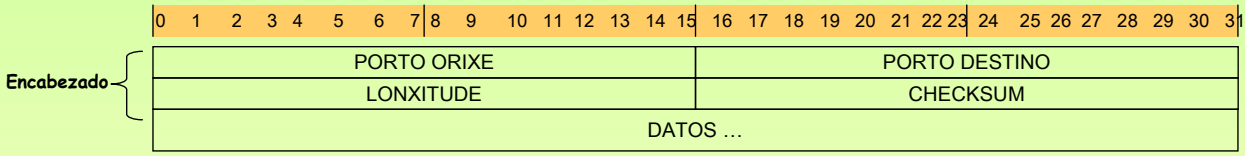
Construír os segmentos e datagramas necesarios ata o primeiro acuse de recibo. Fixarse no campo identificación do datagrama.
NOTA: Os enderezos están: 1º o destino e logo a orixe.



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 diferencia 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

☞ **COMANDOS**
Windows: netstat

C:\WINDOWS\System32\cmd.exe

```
L:\>netstat -?

Muestra estadísticas del protocolo y conexiones TCP/IP actuales.

NETSTAT [-a] [-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
                que puede ser TCP, UDP
                -s para mostrar estadí
                TCP, UDP, TCPv6 o UDPv
  -r            Muestra el contenido
  -s            Muestra estadísticas
```

C:\WINDOWS\System32\cmd.exe

```
L:\>netstat

Conexiones activas

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

8.9.- Comandos TCP

```
Sesión  Editar  Vista  Marcadores  Preferencias  Ayuda
[root@linuxp root]# netstat --help
usage: netstat [-veenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vnNcaeol] [<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.

Redes Área Local - OSI – TCP/IP

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           prsc12_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.txt) 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 estructura en forma de árbore de todos os dominios dende a raíz (" . ", punto) ata o nivel inferior da estructura. A estructura 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 sígueo sendo.
.EDU:	inicialmente era para universidades de EE.UU. e hoxe sígueo sendo.
.GOV:	é para organismos relacionados co goberno de EE.UU. e hoxe sígueo 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.

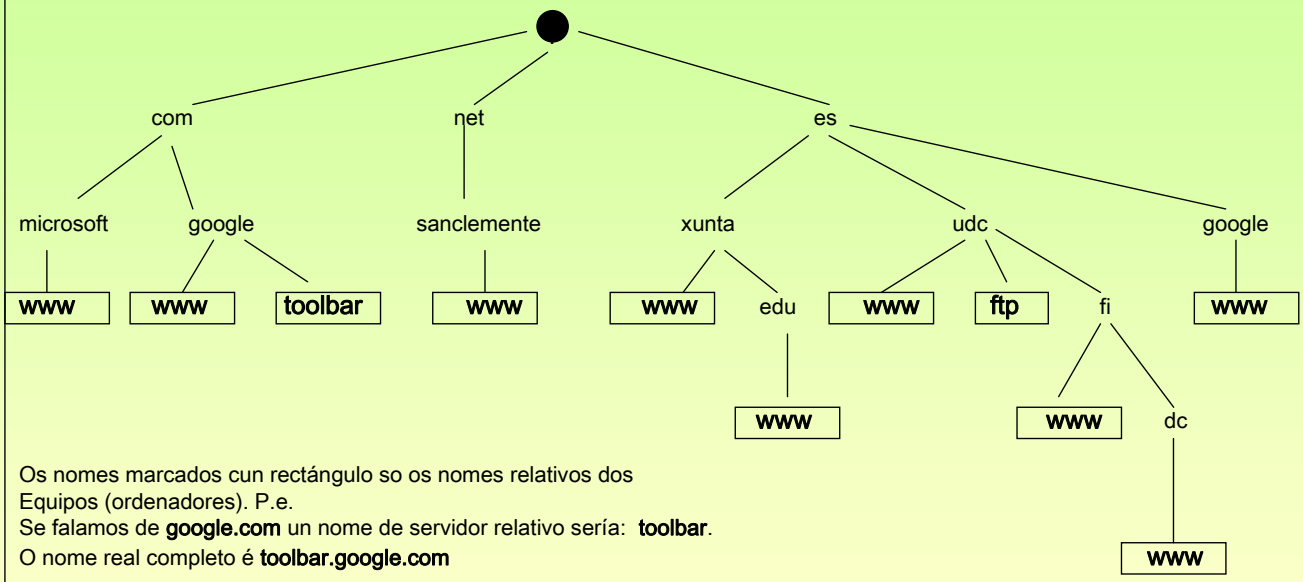
.ES	España. Non fixo control sobre os dominios secundarios.
.UK	Reino Unido. Fixo control sobre os dominios secundarios. P.e. co.uk, gov.uk, org.uk
.BR	Brasil. Fixo o mesmo que os inglese
.DE	Alemaña
.PT	Portugal

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

Redes Área Local - OSI – TCP/IP

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

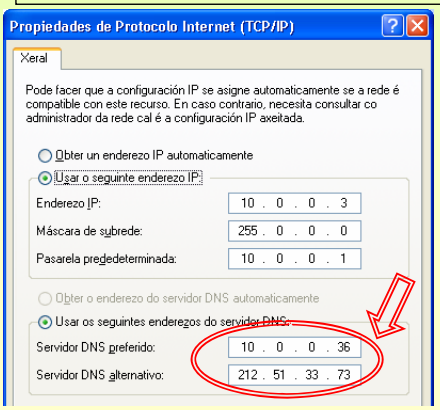
Analoxía con sistema telefónico: Unha persoa pode saber uns cantos números de teléfono, pero se descoñece algún pode chamar ó 11811 para preguntar polo número dun abonado, pero se este número non funciona ou está ocupado podes chamar a outro 11824.

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.

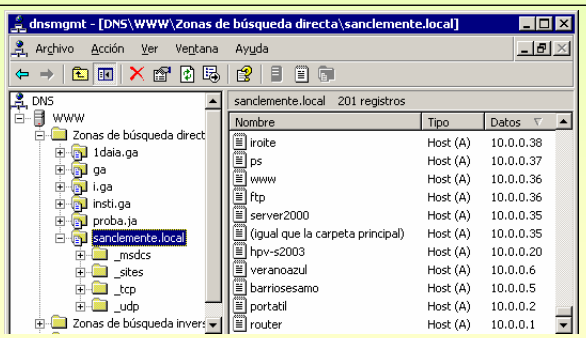
Os clientes configuraranse indicando a IP do servidor de DNS que pode resolver as súas consultas.

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.

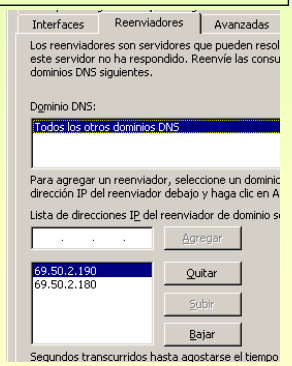
Os servidores DNS non saben tódalas IPs e nomes de dominio existentes. Estes organízanse en forma de árbore, de tal xeito que se un servidor de DNS non é capaz de resolver un nome de dominio este **REENVÍA** a pregunta a outro servidor de DNS ou usa **RECURSIVIDADE** ata atopar o nome de dominio ou obter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



Configuración cliente DNS



10.0.0.36. Configuración server DNS. Zonas e equipos

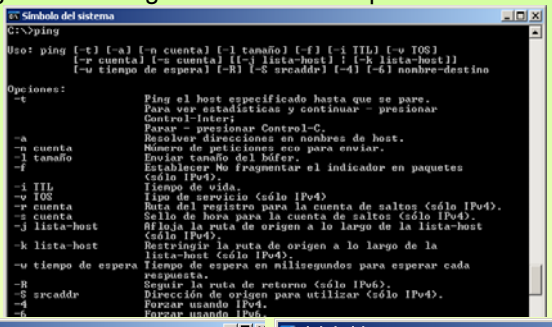


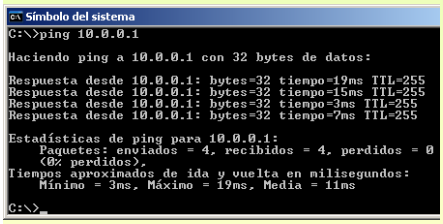
Configuración server DNS. Reenviador

9.- DNS (Domain Name Service)

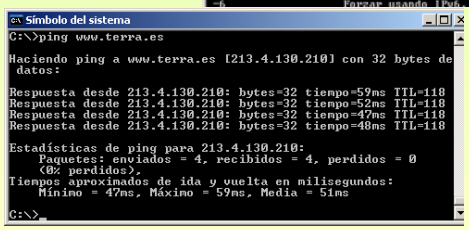
☞ PING (ICMP)

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.
Obsérvense os seguintes exemplos:

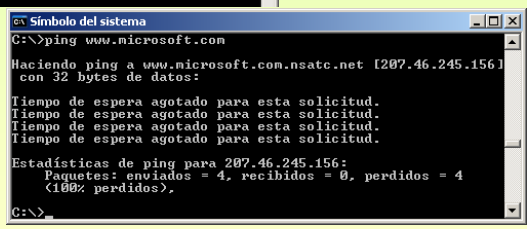




Ping a unha IP que coñecemos.
O respondernos indícanos canto tempo tarda en chegar un PKT. Deste xeito sabemos que 10.0.0.1 **is alive**



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.

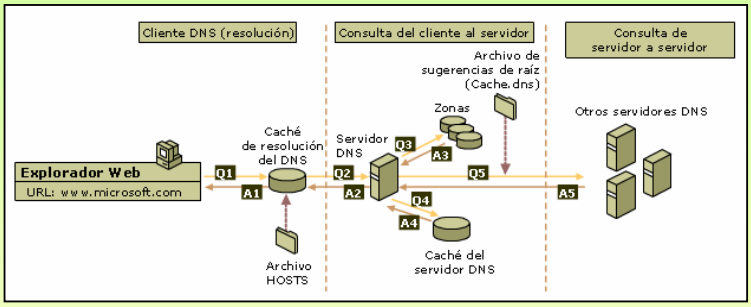


O programa averigua a IP e logo realiza o "ping". O host non responde:
A.- Pode ser que estea apagado, ou non que non se pode chegar a el.
B.- Pode estar acendido pero deshabiltada a resposta a pings.

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.



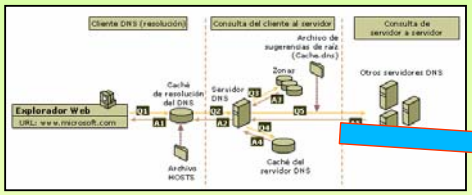
O cliente DNS dispón de:
Caché DNS: onde se almacena resultados de resolucións previas, incluso as de resultado negativo.
Arquivo HOSTS: está (...\system32\drives\etc\). Mantén asociacións estáticas de Nomes con IPs.

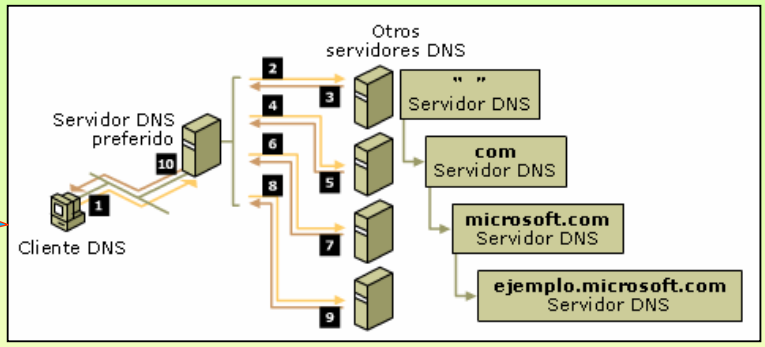
Q1: Cliente DNS consulta a súa cache DNS (xa inclúe os datos do arquivo HOSTS automaticamente) pregunta pola IP de www.microsoft.com.
A1: Se existe entrada devolve a IP senón sigue o proceso:
Q2: Pregunta ó servidor de DNS configurado como preferido:
Q3: O servidor de DNS consulta ás súas zonas (Os dominios 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.microsot.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 preguntarase 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.

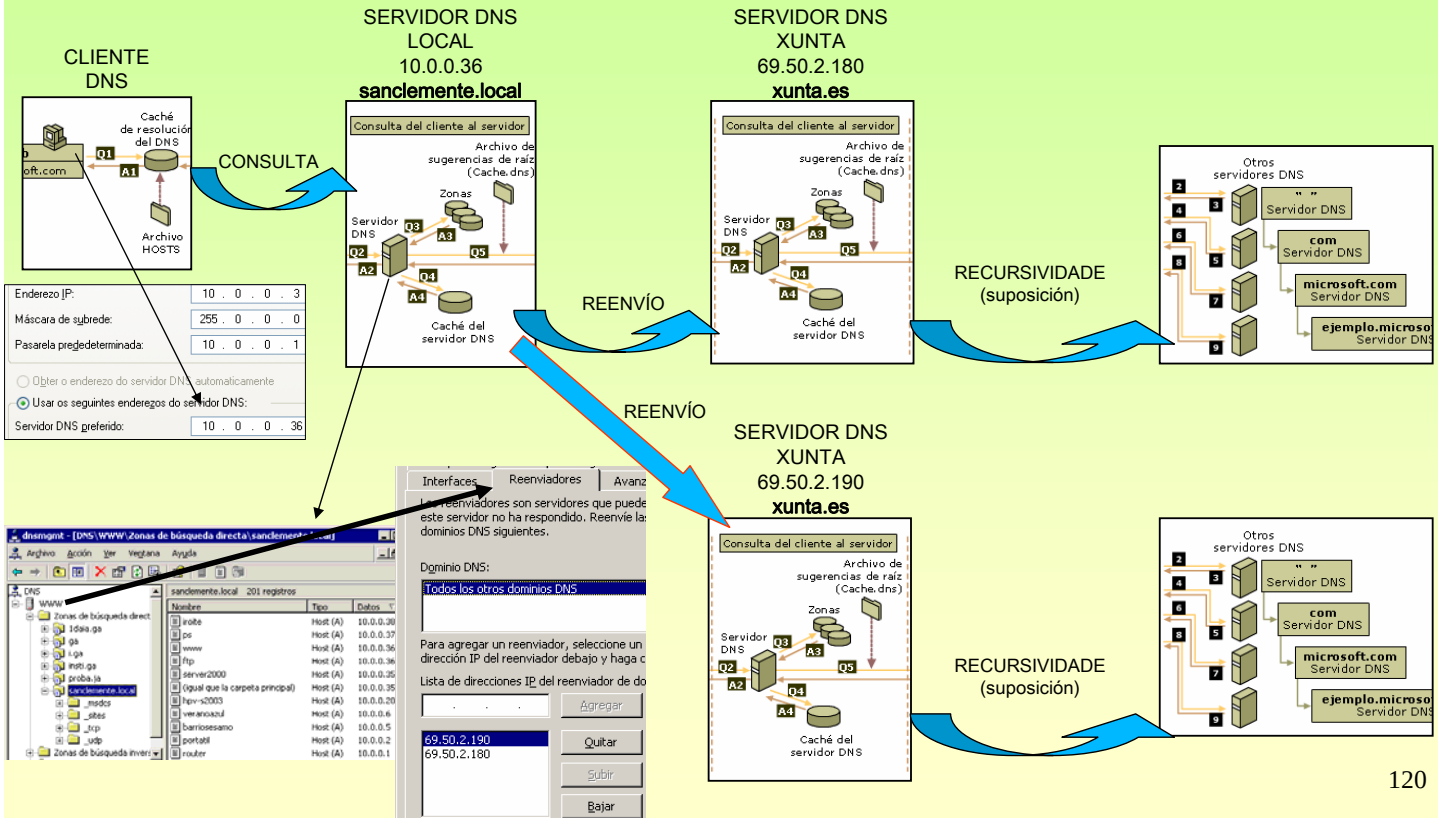
REENVÍO CONDICIONAL.

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

Redes Área Local - OSI – TCP/IP

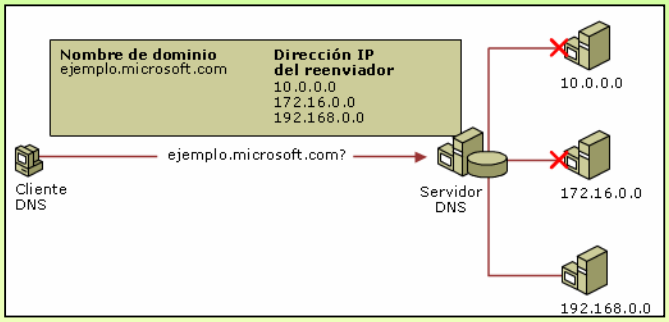
9.- DNS (Domain Name Service)

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

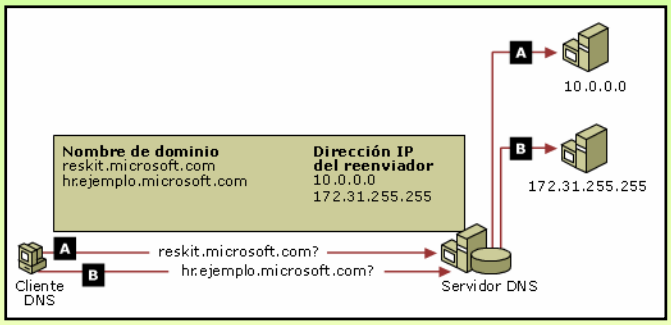


9.- DNS (Domain Name Service)

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



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



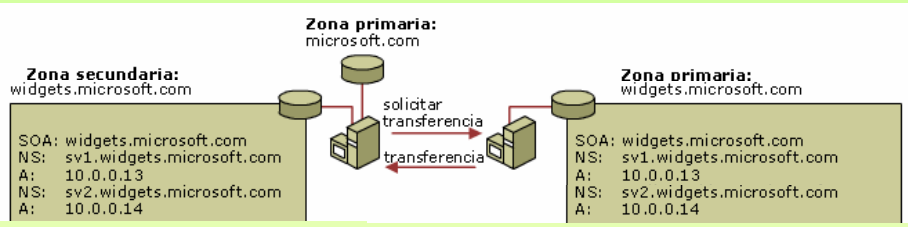
Servidor de reenvío condicional. Un dominio (A) é consultado a un reenviador e o outro dominio (B) a outro reeenviador.

Redes Área Local - OSI – TCP/IP

9.- DNS (Domain Name Service)

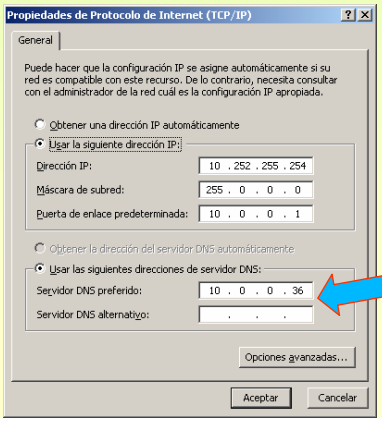
☞ ZONAS SECUNDARIAS

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 actualizarase, logo pídelle actualización completa (transferir todo de principal a secundario AXFR) ou incremental (IXFR).

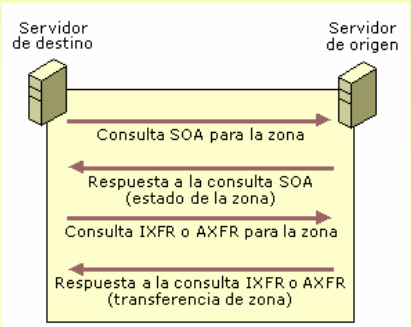


Configuración cliente DNS

Pódense especificar varios DNS ós que preguntar.

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

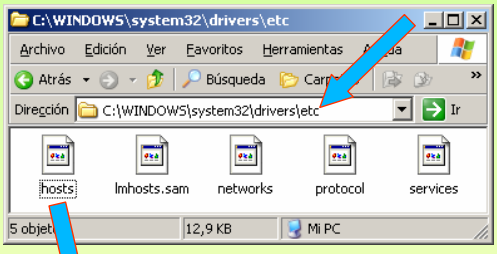
Ata que un deles dea unha resposta ben positiva ben negativa

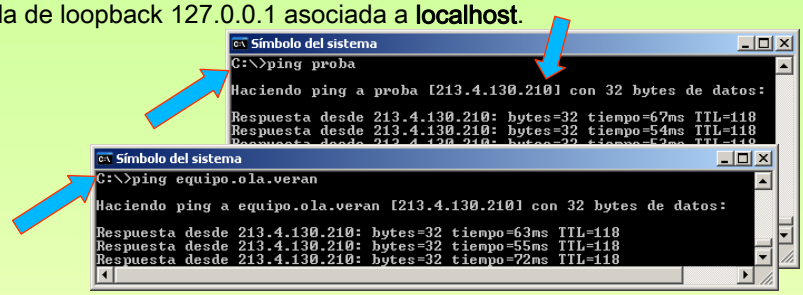


9.- DNS (Domain Name Service)

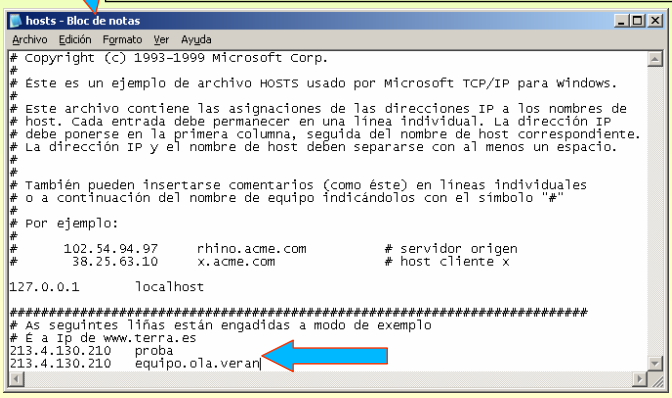
☞ ARQUIVO HOSTS

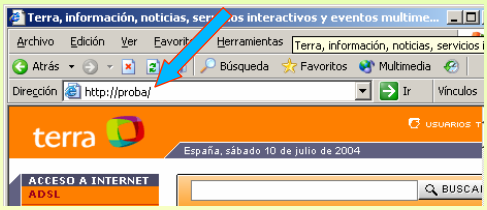
Todo cliente DNS ten un arquivo HOSTS, onde se almacena estaticamente asociacións de de nomes de equipos (con ou sen o dominio) e as súas IPs. Sempre ten a entrada de loopback 127.0.0.1 asociada a **localhost**.



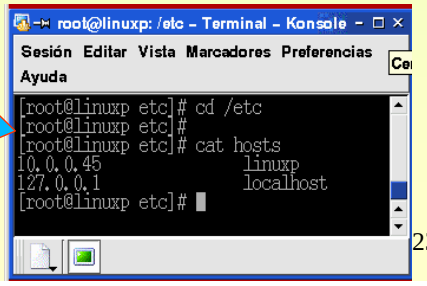


Engadíronselle dúas entradas o final a modo de exemplo. O resultado é o da dereita. Só modificable por administradores





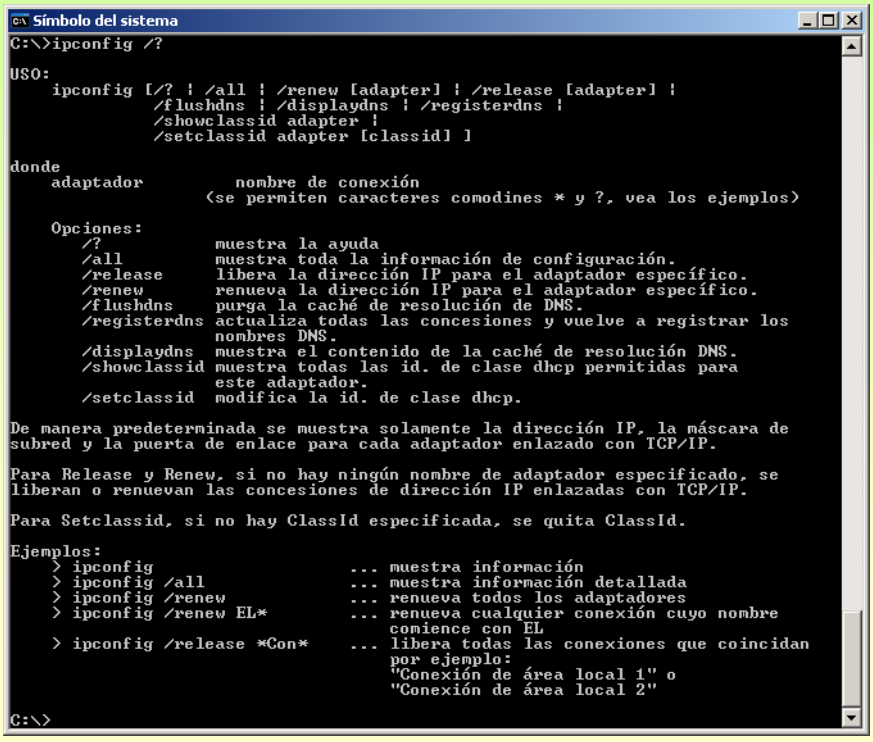
En Linux /etc/hosts



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.



9.- DNS (Domain Name Service)

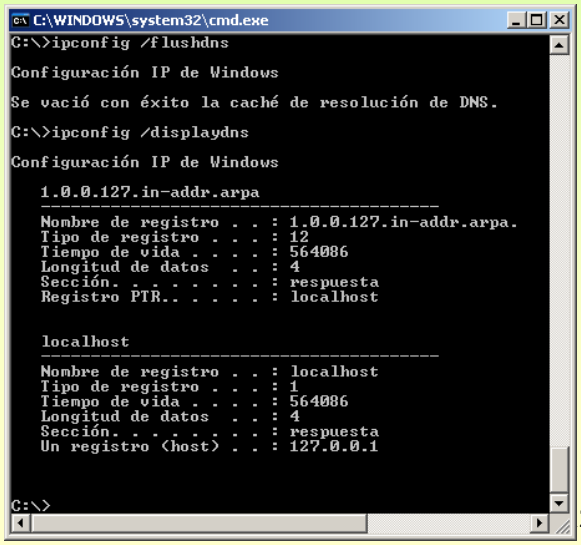
☞ COMANDOS: IPCONFIG (WINDOWS) (II) – BORRADO DA CACHÉ DNS DO CLIENTE

Mostra os valores da configuración TCP/IP. E actualiza a configuración de DHCP (Dyamic 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.

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.



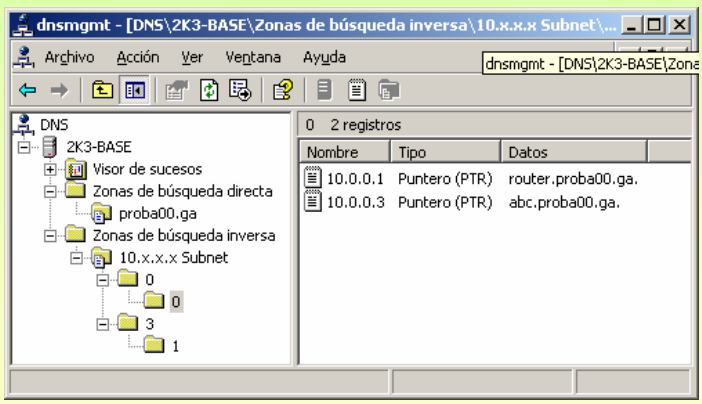
Redes Área Local - OSI – TCP/IP

9.- DNS (Domain Name Service)

☞ DNS (Domain Name System) – Zoas 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 conflicto 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 conflicto> 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 infraestructura dun servidor DNS

Iniciamos a aplicación
Nome e IP do servidor DNS que vai realizar as resolucións .

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

IP? do equipo **www.xunta.es**.

Observar o alias
Fixarse que servidor DNS e web están na mesma IP

IP? De que xestiona a zona **edu.xunta.es**

IP? Do equipo **www** dentro do dominio **edu.xunta.es**

IP? Do equipo **smtp** (Correo) dentro do dominio **edu.xunta.es**

Saímos

Redes Área Local - OSI – TCP/IP

9.- DNS (Domain Name Service)

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

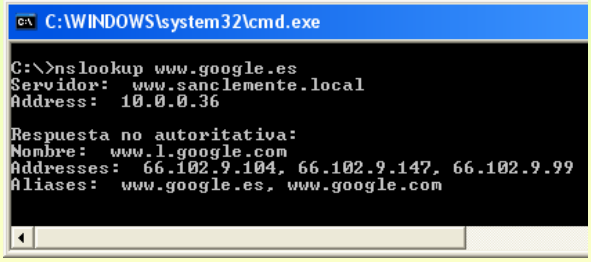
Imaxínese un servidor web (p.e. www.google.es) distribuído en 3 hosts distintos para balancear a carga. Ó mesmo tempo desexase que todos eles respondan ó mesmo nome de dominio (www.google.es).

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.

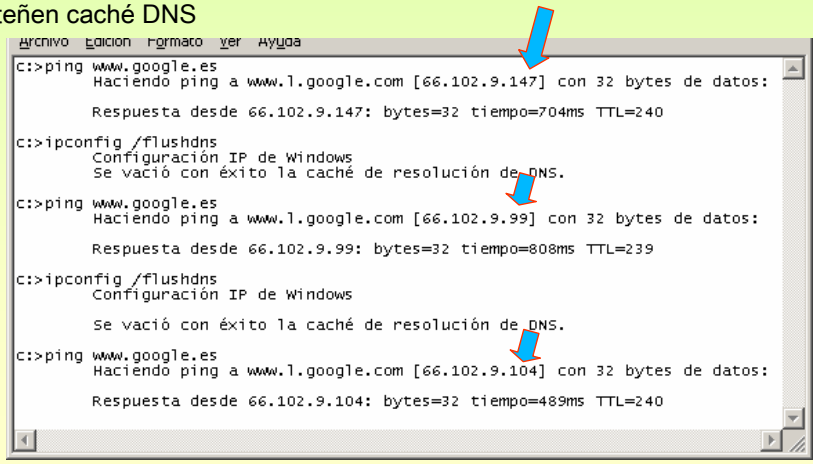
Deste xeito ó servidor DNS ó ser consultado dará unha IP distinta cada vez.

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



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



10.- DHCP (Dynamic Host Configuration Protocol)

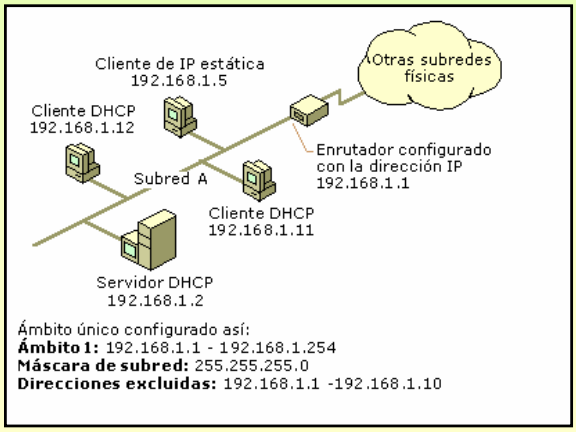
☞ DHCP (Dynamic Host Configuration Protocol).

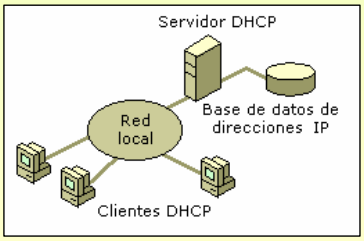
Hai veces nas que é interesante que os usuarios con ordenadores portátiles poidan chegar a un IES (p.e.), conectarse fisicamente á rede (por cable ou por wi-fi) e que o usuario nin o administrador teñan que estar a configurar as propiedades do protocolo de Internet.

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

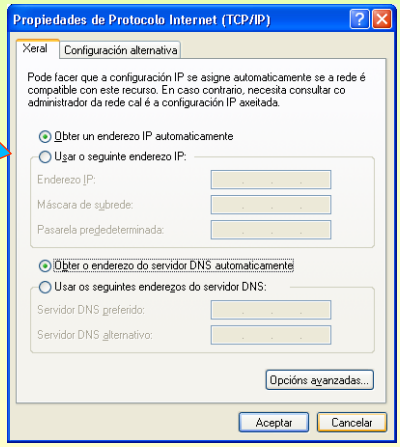
Ó acenderse un equipo que teña configurado **Obter automaticamente unha IP** este preguntará á toda a rede se hai alguén que lle poida dar unha IP, o servidor DCHP escoitará a petición e será el quen lla ofreza. O mesmo co DNS.

O servidor DHCP leva un control das IPs que leva asignadas





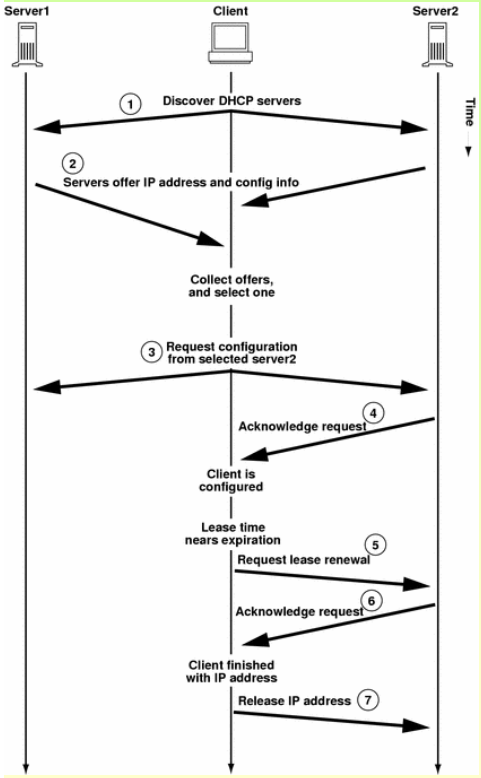
Configuración Cliente

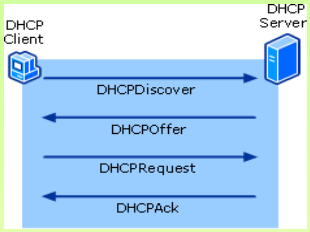


Redes Área Local - OSI – TCP/IP

10.- DHCP (Dynamic Host Configuration Protocol)

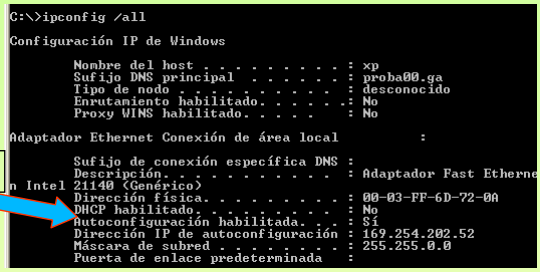
☞ FUNCIONAMENTO do DHCP (Dynamic Host Configuration Protocol).





APIPA

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

11.- PKI (Public Key Infraestructure)

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

A PKI encargase 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 esto 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

Redes Área Local - OSI – TCP/IP

11.- PKI (Public Key Infraestructure)

☞ 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: ainda que alguén intercepte unha mensaxe cifrado coa pública e teña a cha ve 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 resume 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 dicindolle a C que lle envía a chave pública B.

Verase máis adiante un estudio máis profundo dos certificados.

11.- PKI (Public Key Infraestructure)

☞ 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 publica 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 co privada do emisor: (rápido)
Non repudio: (Emisor non negue a paternalidade da mensaxe)	1.- Cifrar a mensaxe coa privada do emisor: (Lento). 2.- Realizar un resumo da mensaxe e cifralo co privada do emisor: (rápido) En calquera dos dous casos só o emisor ten a súa chave privada, co cal non pode negar a paternalidade da mensaxe

Redes Área Local - OSI – TCP/IP

11.- PKI (Public Key Infraestructure)

☞ 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 e 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 usario 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 recibeu 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 Infraestructure)

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

☞ Certificados: X.509 v3

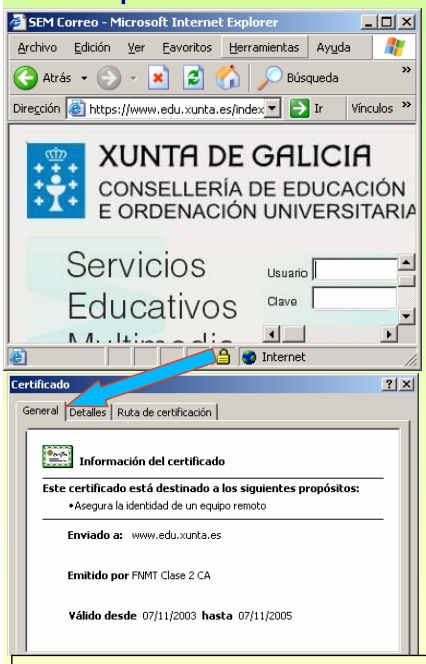
O estándar X.509 define o formato e contido dos campos dun certificado. Actualmente vai na versión 3, esta permite definir campos a parte dos xa establecidos.

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 incluir o usuario.
Firma	Resumo do resto dos campos obtido co algoritmo de firma e cifrado coa chave privada da CA

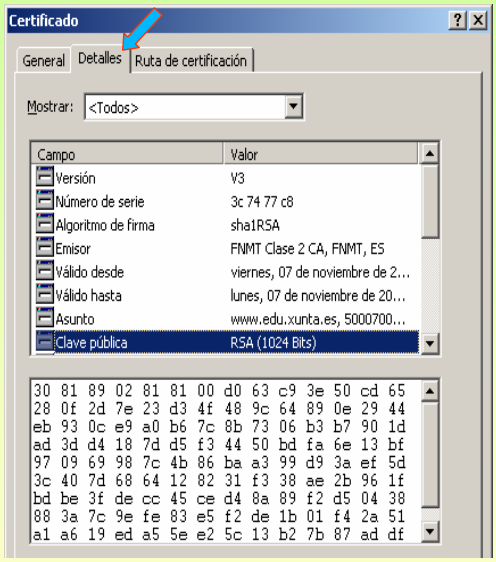
11.- PKI (Public Key Infraestructure)

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

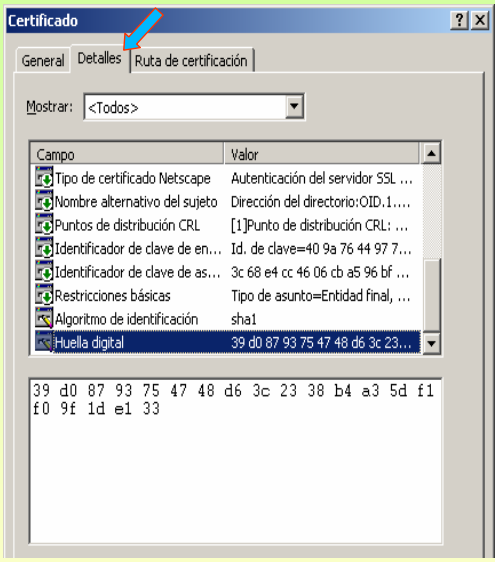
☞ Exemplo de certificado: correo web de www.edu.xunta.es



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



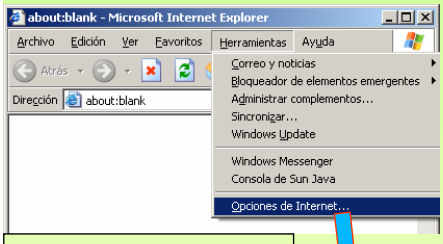
Obsérvese:
- Os campos antes indicados.
- Quen o emite.
- Para quen o emite, etc.
- A chave pública do dono do certificado



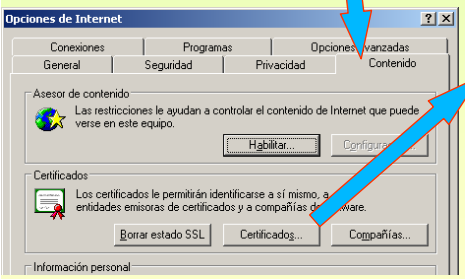
Obsérvese:
A firma dixital, obtida co algoritmo sha1RSA

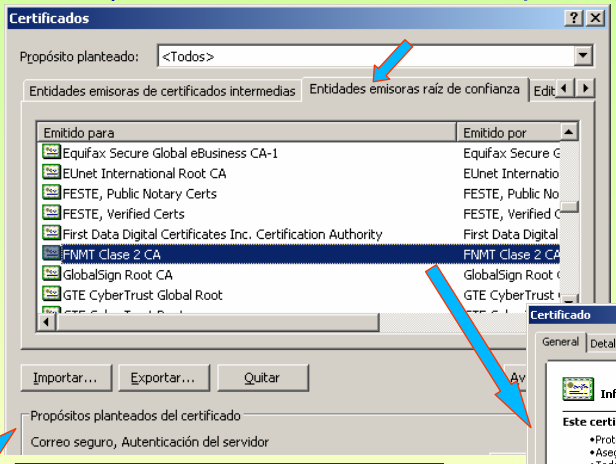
11.- PKI (Public Key Infraestructure)

- PKI (Public Key Infrastructure, Infraestructura de Chave Pública) (VII)
- Certificados raíz instalados nos clientes (certificados de emitidos da CA para a propia CA)



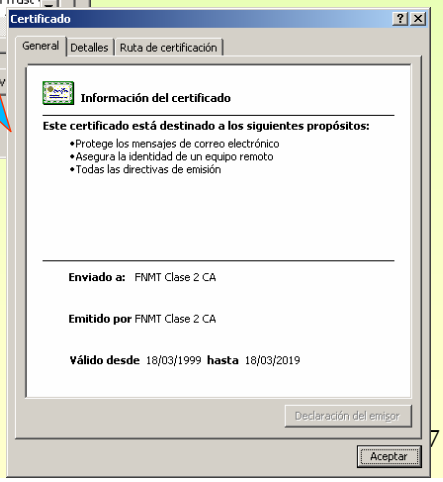
Neste caso trabalarase co Internet Explorer de MS





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

Obsérverse como o emite a FNMT para a FNMT



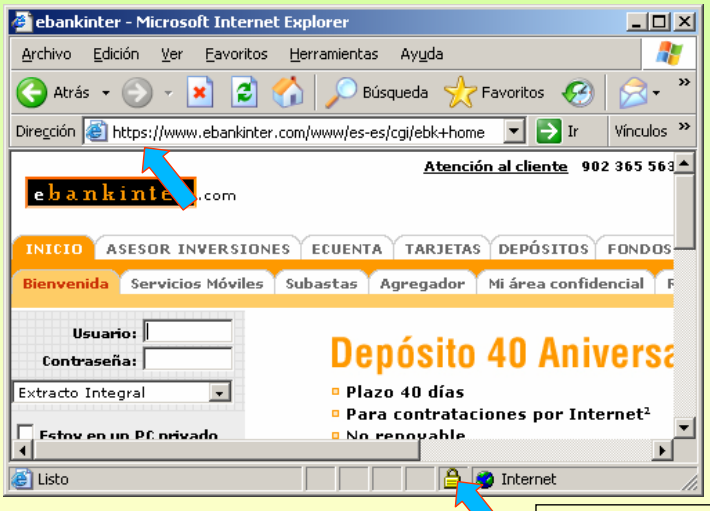
Redes Área Local - OSI – TCP/IP

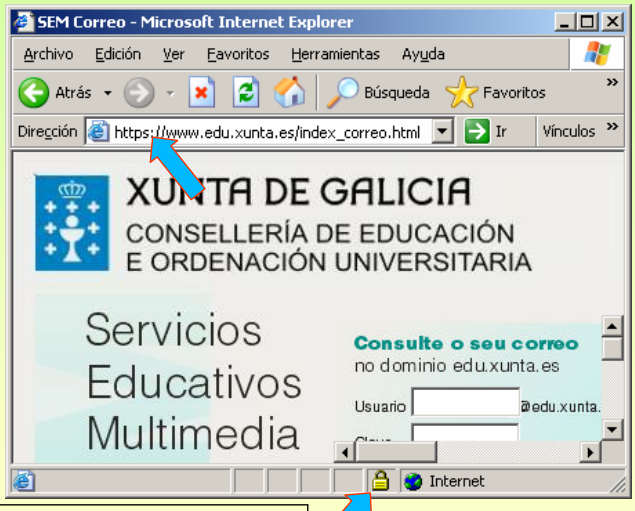
11.- PKI (Public Key Infraestructure)

- 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:





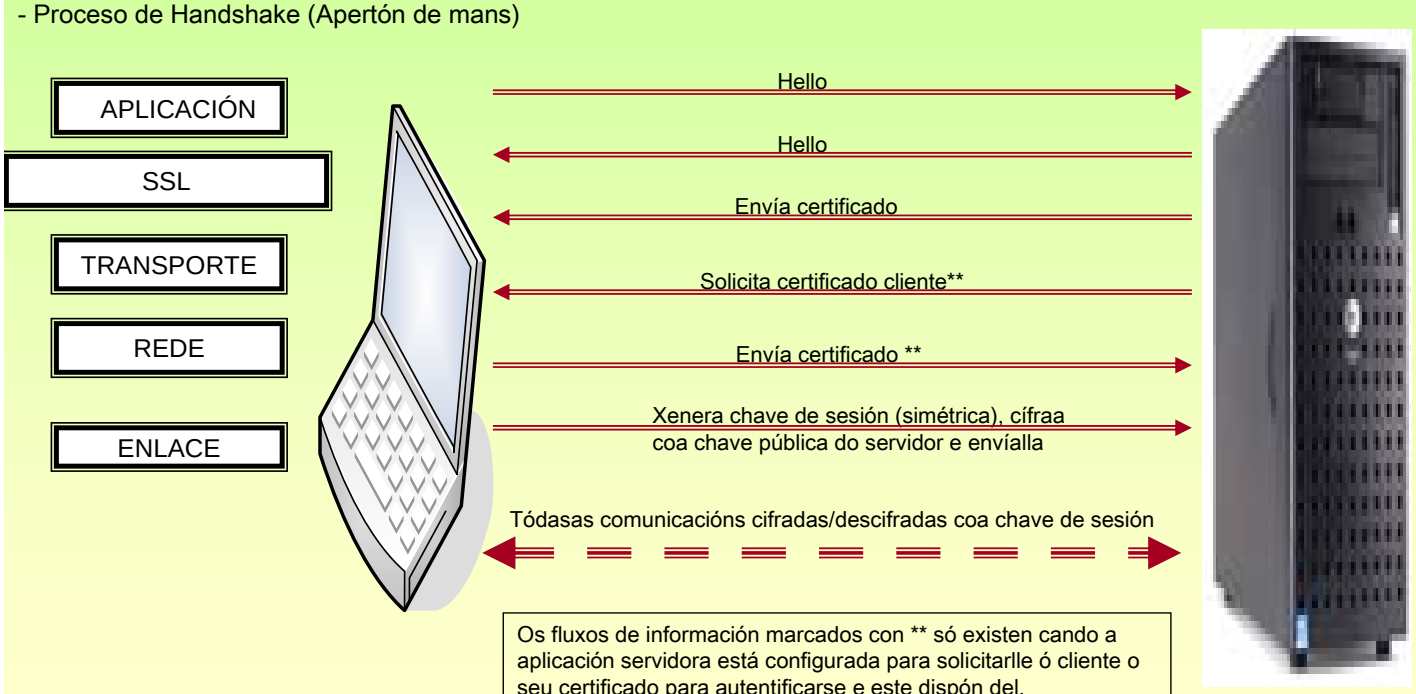
Conexións SSL.
Realizando dobre clic sobre o candado vense as propiedades do certificado.

11.- PKI (Public Key Infraestructure)

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

-Creado no 1944 por Netscape. Permite crear *túneles* seguros entre unha aplicación cliente e a aplicación servidor

- Proceso de Handshake (Apertón de mans)

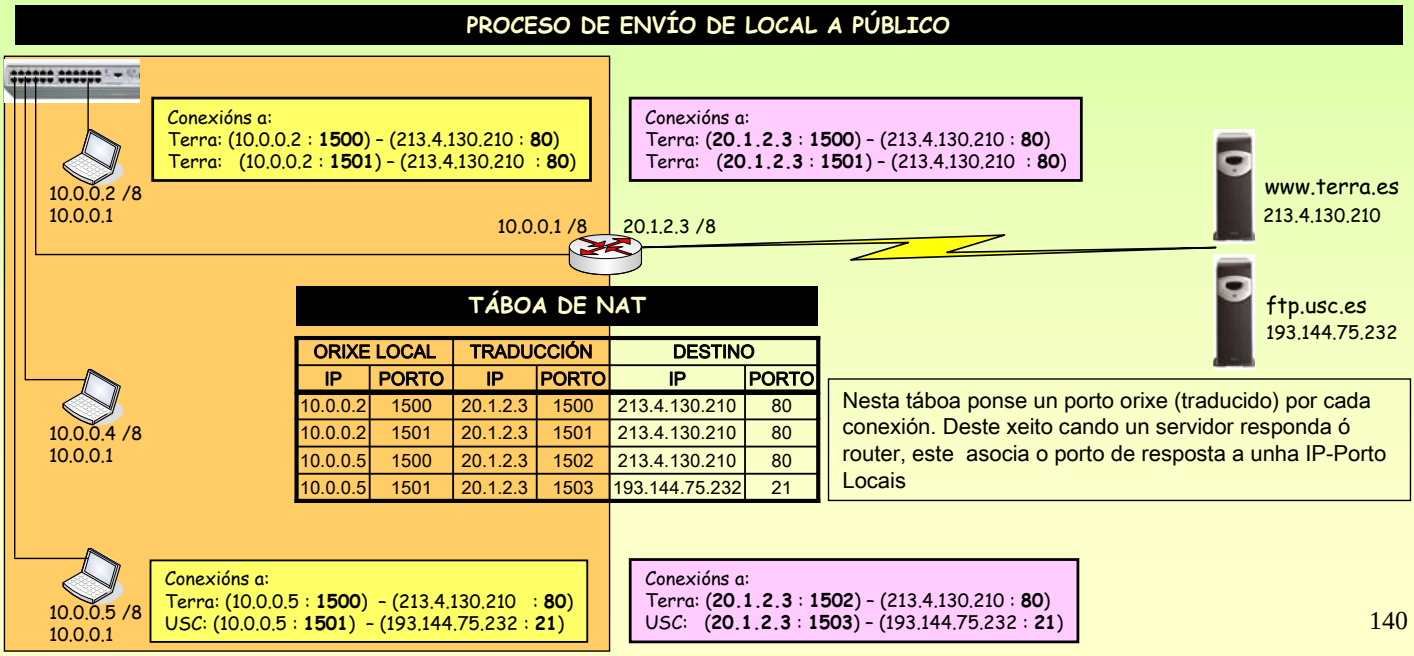


12.-NAT (Network Address Translation)

☞ NAT (Network Address Translation – Traducción de enderezos de rede) (I)

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. Esto é unha conexión ten que ser entre dúas **IPs PÚBLICAS.**

Solución: O router realiza NAT, esto 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.



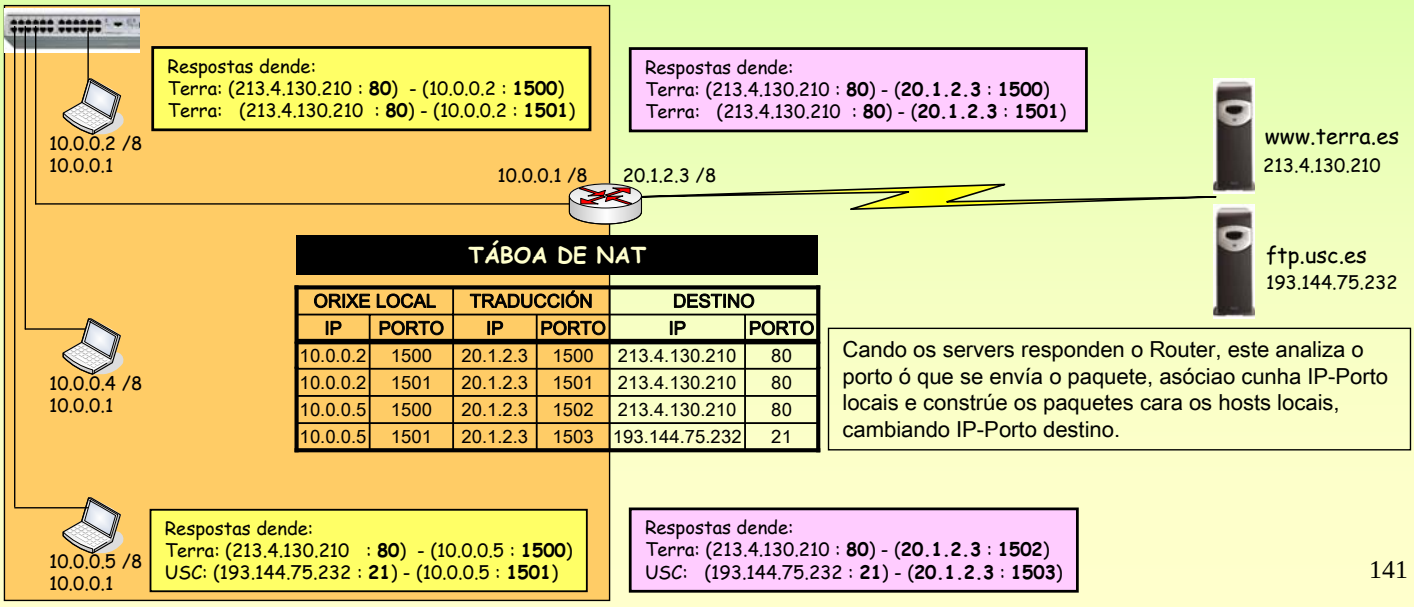
12.-NAT (Network Address Translation)

NAT (Network Address Translation – Traducción de enderezos de rede) (II)

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. Esto é unha conexión ten que ser entre dúas **IPs PÚBLICAS.**

Solución: O router realiza NAT, esto 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.

PROCESO DE RESPOSTA DE PÚBLICO A LOCAL



TÁBOA DE NAT

ORIXE LOCAL		TRADUCCIÓN		DESTINO	
IP	PORTO	IP	PORTO	IP	PORTO
10.0.0.2	1500	20.1.2.3	1500	213.4.130.210	80
10.0.0.2	1501	20.1.2.3	1501	213.4.130.210	80
10.0.0.5	1500	20.1.2.3	1502	213.4.130.210	80
10.0.0.5	1501	20.1.2.3	1503	193.144.75.232	21

Cando os servers responden o Router, este analiza o porto ó que se envía o paquete, asóciao cunha IP-Porto locais e constrúe os paquetes cara os hosts locais, cambiando IP-Porto destino.

141

Unidade de Traballo 3

Codificación da información e detección e corrección de erros

Comentario [CCA1]: García T. (135), Tanenbaum, (242), Equipos (Tema 3), Ciclo (47)

INDICE.

Unidade de Traballo 3

Codificación da información e detección e corrección de erros

Comentario [CCA2]: García T. (135), Tanenbaum, (242), Equipos (Tema 3), Ciclo (47)

4.1.- INTRODUCCIÓN.

- **Código:** Correspondencia entre un conxunto F, (alfabeto fonte) e S (Conxunto de símbolos).

  A cada elemento de F asígnaselle un grupo de símbolos **(Palabra)**.

  Para que o código sexa útil a correspondencia debe ser biunívoca, recíproca e inequívoca

- **Codificación:** proceso de conversión do conxunto F ó conxunto S

Palabra Fonte	**Palabra Código**.
A B	A B A+B
0 0	0 0 0
0 1	0 1 1
1 0	1 0 1
1 1	1 1 0
Función de codificación: f(A,B) = (A,B,A+B)	

- **Redundancia dun código**: diferencia entre a información máxima que podería proporcionar un código e a que realmente proporciona. Úsanse os díxitos que non transportan información como detectores e incluso correctores de erros.
- **Taxa de erros**: Relación entre os bit recibidos erróneos e os bits transmitidos, pois sempre existe a posibilidade de que se introduzan erros na información transmitida (*ruídos*).
- **Tipos de ruídos:**

  Ruído Impulsivo: Probabilidade de que un bit sexa erróneo. Por exemplo 10^{-3}.

  Ruído por Ráfagas: O erro comeza nun determinado bit e prodúcense erros aleatorios ó longo de toda a ráfaga. Erro por ráfaga de 100 bits.

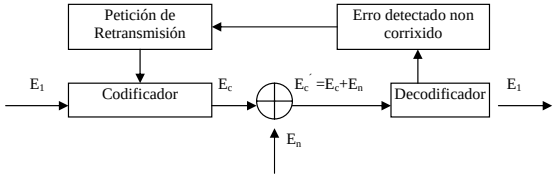
Exercicio:

1.- Deséxanse transmitir 100.000 bits. Estudia como afecta os distintos tipos de ruído a eses 100.000 bits, nos seguintes casos: Que se transmitan os 100.000 nun só bloque, que se transmitan en bloques de 1.000 bits ou que se transmitan en bloques de 100 bits.

- **Probabilidade de erro:** Depende das condicións dos elementos que interveñen na canle de transmisión, a saber

Canle	Probabilidade de erro/bit
Liñas telefónicas conmutadas	10^{-5}
Liñas telefónicas dedicadas a 1.200 bits/seg	10^{-6}
Liñas telefónicas dedicadas a 4.800 bits/seg	10^{-5}

- **Esquema básico dunha transmisión de información:**



E_1 é a mensaxe inicial e E_c, a mensaxe inicial codificada. A causa do ruído aditivo na liña aparece: $E´_c = E_c + E_n$.

O chegar $E´_c$ ó decodificador poden ocorrer dúas cousas:

Que $E´_c$ pertence ó conxunto de posibles palabras do código: A transmisión considerase boa e a decodificación da como resultado E_1.

Que $E´_c$ non sexa unha palabra do código: Detéctase ó erro, se este é corrixido pola lóxica do decodificador, extráese E_1 . Se só é detectado, pero non corrixido, pídese a repetición da mensaxe.

Segundo a potencia do código, os sistemas poden detectar erros, corrixilos ou ben ámbalas dúas cousas, corrixindo algúns tipos de erros e detectando outros.

Para que a detección e corrección de erros se leve a cabo é preciso unha serie de bits (r bits), *bits de redundancia*. Co cal a palabra código estará composta por n=m+r bits (m bits de información).

Comentario [CCA3]: Equipos (Tema 3), Alxebra (Tema Códigos Lineais)

3.2.- DISTANCIA HAMMING

A ***distancia Hamming*** entre dúas palabras dun código é o número de bits en que difiren ambas: por exemplo d(010010110, 110110111)=3

010010110 110110111	Estas dúas palabras difiren en 3 bits. H=3 (Distancia Hamming = 3 bits)
100100001	1 indica onde son distintos os bits

Defínese ***peso (w)*** dunha palabra X como d(X,0), noutras palabras é o número de 1s da palabra.

Dúas palabras serán máis fáciles de distinguir canto maior sexa a súa distancia Hamming, debido a que si a distancia é d, fan falla d bits erróneos para transformar unha palabra noutra. Co cal a eficacia dun código depende da *distancia Hamming mínima* que poida encontrase entre dúas das súas palabras:

- Un código C detecta p ou menos erros si $d_{min} \geq p+1$
- Un código C corrixe p ou menos erros si $d_{min} \geq 2p+1$

Exemplos

Código 1:

Mensaxes	Palabras Código = x
AB	AB+
00	000
01	011
10	101
11	110
Función de codificación: f(A,B) = (A, B, A+B)	

As palabras código son : {000, 011, 101, 110}. Si se observa vese que a $d_{min}= 2$, co cal este código detecta erros simples (nun só bit), pero non capaz de corrixilos.

O transmisor desexa enviar 01 para iso ***codifica*** como 011 e transmítea. O receptor recibe 111. A palabra 111 non é unha palabra código, co cal non pode ***decodificala*** e así obter a mensaxe orixinal. Esta palabra 111 non puido ser transmitida, co cal produxeuse un erro nun bit pero o decodificador non pode determinar en cal. Non podemos recuperar a mensaxe orixinal, esto implica que temos que solicitar unha retransmisión.

Código 2:

Mensaxes	Palabras Código = x
AB	ABABAB
00	000000
01	010101
10	101010
11	111111
Función de codificación: f(A,B) = (A, B, A, B, A, B)	

A distancia mínima deste código 2 é $d_{min}= 3$, co cal o decodificador corrixe erros simples e detecta erros dobres e simpres.

Podemos supor que os erros ocorren aleatoriamente e independentemente, e que a probabilidade de erro é igual en calquera dos díxitos (si $q \leq 0.5$, é máis probable que se produza un erro que 2, 2 que 3, ...). Por iso úsase a **decodificación de máxima verosimilitude**: e dicir, para decodificar a palabra recibida buscarase aquela palabra código máis probablemente transmitida, ou sexa a que defira no menor número de díxitos da palabra recibida.

Por exemplo si o código e C={000000, 010101, 101010, 111111} e si y=010111 é a palabra recibida, calcúlase:

.d(000000, 010111)=4
.d(010101, 010111)=1
.d(101010, 010111)=5
.d(111111, 010111)=2

A menor distancia Hamming entre as palabras código é a palabra recibida prodúcese no 2º caso (*decodificación de máxima verosimilitude*). Co cal, a palabra código máis probablemente transmitida sexa: x=010101. Neste caso o decodificador detecta e corrixe o erro.

O erro é e=000010, w(e)=1, y= 010101 + 000010
x ∈ C + e

Código 3:

Mensaxes	Palabras Código = x
ABC 000 001 010 011 100 101 110 111	
Función de codificación: f(A,B,C) = (A, B, C, A+B, B+C, A+B+C)	

Comentario [CCA4]: A distancia mínima é 3, existe unha folla de calculo chamda distancia min, para o calculo

Exercicios:

2.- ¿Que fai o decodificador no código 2 si o receptor recibe 000011?

3.- Desexase enviar 01 e o receptor recibe 010000, ¿Que pasou e como actúa o decodificador?

4.- Calcula as palabras códigos do código 3.

5.- ¿Cantos bits erróneos pode detectar e corrixir o código 3?

6.- ¿Cal dos tres códigos é mais efectivo atendendo a relación bits de información bits de redundancia?

7.- Transmítese unha palabra código, no código 3, producese un erro, ¿Como actúa o decodificador?. Faino poñendo un exemplo.

8.- Temos m bits para as mensaxes e r para a redundancia. ¿Cantos mensaxes podemos ter, e cantas palabras código legais?.¿Úsanse tódalas combinacións posibles dos n bits, sendo n=m+r?

Comentario [CCA5]: Existe na páxina 244 Tanenbaum un posible exercicio de exame

3.3.- CÓDIGOS DE CONTROL DE PARIDADE

3.3.1.- Paridade simple

O **bit de paridade** é aquel que se selecciona en función do número de 1s da palabra mensaxe. Así temos:

Tipo de paridade	Definición	Exemplo
Par	Número de 1s é par: engádese un 0	0011011 (0)
Impar	Número de 1s é impar: engádese un 0	0011011 (1)

O cálculo, realmente, faise coa función EXOR (OR-Exclusivo), definida como segue:

AB	$A \oplus B = \overline{A}.B + A.\overline{B}$
00	0
01	1
10	1
11	0

A partires de agora, salvo que se diga o contrario, cando se fale de paridade estarase falando de paridade par.

Este código ten unha distancia mínima de 2, co cal só detecta erros simples. Detecta tamén erros si o número de bits erróneos é impar, pois si fose para un erro compensaría có outro.

Exemplo:

Deséxase enviar a seguinte palabra 1001 o transmisor calcula o bit de paridade (0), deste xeito a palabra código que se envía é 10010. O receptor recibe 10011, este calcula de novo o bit de paridade e dálle (0) e el recibiu (1) co cal detecta o erro pero nono pode corrixir.

3.3.1.- Paridade de bloque

Trátase de organizar a información por bloques, compoñendo unha táboa de **k** x **m** bits (k palabras de m bits cada unha). Logo calcúlase os bits de paridade de cada unha das m filas (***paridade horizontal***) e k columnas (***paridade vertical***). Por último calculase o ***bit de paridade cruzada*** a partires da columna ou da fila de paridade calculada anteriormente.

Exemplo:

	Mensaxe	Paridade Horizontal
	101110	0
	011010	1
	111000	1
	101010	1
Paridade Vertical	100110	1 Bit de Paridade Cruzada

Neste caso o codificador fai bloques de 4 palabras de 6 bits cada unha, e calcula as distintas paridades, logo envía ó receptor, unha fila tras outra. Ter en conta que envía 5 palabras código de 7 bits cada unha.

O decodificador reconstrúe o bloque e volve a calcular os bits de paridade correspondentes e compáraos cos bits de paridade recibidos.

Este código ten unha distancia mínima de 4, co cal corrixe erros simples e detecta erros dobres, triples e cuádruples se estes non forman un rectángulo na matriz de díxitos.

Exercicios:

9.- Baseado no exemplo anterior. O emisor envía esas 4 palabras de 6 bits cada unha. Na canle producese ruído no 1º bit da 1ª palabra. ¿Qué pasos realiza o decodificador no caso de paridade simple e no caso de paridade de bloque?

10.- Igual que no exercicio anterior, pero esta vez tamén se produce un erro no 2ºbit da 2ª palabra. ¿Qué pasos realiza o decodificador no caso de paridade simple e no caso de paridade de bloque?

11.- ¿Cal é a efectividade deste código?

3.4.- CÓDIGOS HAMMING

Comentario [CCA6]: Alxebra (Tema Códigos Lineais), Tanenbaum (244), García Tomas (140)

Son un subconxunto dos códigos de control de paridade. Os díxitos de paridade dispóñense de maneira que localicen a presencia de erros dentro da palabra. Estes códigos teñen, xeralmente, distancia mínima 3.

Si temos palabras código de N bits. Para corrixir un erro ou detectar a ausencia de erros, precisamos, ó menos, R deses N bits como bits de control, de tal xeito que:

$N=2^R-1$

Desta fórmula dedúcese que o código máis pequeno terá 3 bits(2 de control e 1 de información).

Regras relativas o control de paridade nos códigos Hamming:

1.- Dous bits non poden controlar a paridade dun mesmo conxunto de bits da mensaxe.

2.- Non se debe incluír no conxunto de bits controlados por un bit de paridade a outros bits de paridade, pois el detecta o seu propio erro.

3.- Un erro nun bit de información debe afectar a un ou mais díxitos de paridade.

Exemplo:

Temos un código Hamming con 3 ($c_4\ c_2\ c_1$)bits de paridade. A lonxitude da palabra será 7 e haberá 4 bits de información ($b_7\ b_6\ b_5\ b_3$). Co cal a palabra código será da seguinte forma:

$b_7\ b_6\ b_5\ c_4\ b_3\ c_2\ c_1$

Haberá tantas ecuacións de paridade como díxitos de control. Para obter estas usase a seguinte táboa. Notar que cada bit de control ocupa unha posición potencia de 2, deste xeito el mesmo controla o seu propio erro.

Pos	c_4 c_2 c_1	ERRO	Ecuacións Codificador	Ecuacións Decodificador
0	0 0 0	NON ERRO	$c_1 = b_3 \oplus b_5 \oplus b_7$	$e_1 = b_3 \oplus b_5 \oplus b_7 \oplus c_1$
1	0 0 1	c_1 *Está na posición* 2^0	$c_2 = b_3 \oplus b_6 \oplus b_7$	$e_2 = b_3 \oplus b_6 \oplus b_7 \oplus c_2$
2	0 1 0	c_2 *Está na posición* 2^1	$c_4 = b_5 \oplus b_6 \oplus b_7$	$e_3 = b_5 \oplus b_6 \oplus b_7 \oplus c_4$
3	0 1 1	b_3		
4	1 0 0	c_4 *Está na posición* 2^2		
5	1 0 1	b_5		
6	1 1 0	b_6		
7	1 1 1	b_7		

Un emisor desexa enviar 0101, o codificador realiza o seguinte en base as ecuacións anteriores:

```
b7 b6 b5 c4 b3 c2 c1
0  1  0  1  1  0  1
```

Esta palabra transmítese pola canle e sufre un erro en b_2. O decodificador realizará a seguinte operación ó recibir a palabra código:

```
b7 b6 b5 c4 b3 c2 c1    e3 e2 e1
0  0  0  1  1  0  1     1  1  0  (=6 en decimal).
```

Como se pode observar o decodificador detectou en que posición se produxo o erro.

Exercicios:

12.- Baseado no exemplo anterior. O emisor envía 1011, pero pola canle o bit c_2 cambia. ¿Qué pasos realiza o decodificador?

13.- Igual que no exercicio anterior, pero esta vez tamén se produce un erro no bit b_7 ¿Qué pasos realiza o decodificador?

14.- ¿Cal é aCÓDIGOS efectividade deste código?

Comentario [ISC7]: Ciclo (48, 89), Tanenbaum(246-250)

3.5.- CODIGOS DE REDUNDANCIA CÍCLICA (CRC)

Baséanse no tratamento de series de bits como si foran representacións de polinomios, con coeficientes de valor 0 e 1, unicamente. Así 1011001 (son 7 bits) daría lugar a un polinomio de grado 6 (7-1):

$$1.x^6 + 0.x^5 + 1.x^4 + 1.x^3 + 0.x^2 + 0.x^1 + 1.x^0 = x^6 + x^4 + x^3 + 1$$

Emisor e receptor deben deben poñerse de acordo no polinomio divisor ou xerador. O emisor divide o polinomio-mensaxe entre o polinomio-xerador, obtendo un cociente que se ignora e un polinomio resto. Este polinomio é un secuencia de bits que se engaden o polinomio-mensaxe, este campo é chamado SVT (Servicio de Verificación de Tramas), constituíndo así a trama a enviar ó receptor.

Cando o receptor recibe a trama, volve a dividir a parte da trama que corresponde o polinomio-mensaxe entre o polinomio-xerador, obtendo un polinomio-resto. Este polinomio e comparado co SVT que recibiu na mesma trama. Si non coinciden interpretase que existiu un erro.

Estes algoritmos soen estar implementados en hardware, o que implica unha maior velocidade a hora de detectar un erro.

Os métodos CRC soen detectar os seguintes tipos de erros:

- Erros simples
- Erros de máis de 1 bit si o polinomio divisor é suficientemente grande.
- Un ráfaga de erros de lonxitude menor o SVT
- Outros moitos non descritos aquí.

Exemplo

O tamaño das mensaxes é de 6 bits e o polinomio xerador é x^2+1, co cal os seus coeficientes son 101. Desto dedúcese que o tamaño da trama (mensaxe+SVT) é de 8 bits (6+2 do grado do polinomio xerador).

O emisor desexa enviar 101111. O algoritmo para calcular a redundancia (SVT) é.

1º. Sexa r o grado do polinomio xerador, pois engadir r ceros no extremo inferior da trama: *no noso caso: 10111100*

2º. Facer a división binaria do polinomio resultante do paso anterior entre o xerador.

3º. Suma o resto resultante do paso anterior o polinomio do paso 1º.

```
10111100 | 101
---------|-----
101      | 100101
0001
 000
 0011
  000
```

```
 0111
  101
 0100
  000
 1000
  101
 0011
```

O resto desta división é 11, que será o SVT da trama a enviar, co cal esta queda da seguinte forma: 10111100.

Si pola canle de transmisión se produce un erro no 1º bit a esquerda do SVT, o receptor procedería da seguinte forma:

```
10111000 | 101
---------+------
101      | 100100
0001
 000
 0011
  000
  0110
   101
   0010
    000
    0100
     000
     0100
```

O resto desta división é 100 que comparado co SVT da trama recibida pódese comprobar que non coinciden co cal. Deste xeito o receptor detecta o erro producido.

Na maioría dos casos os códigos CRC só detectan os erros e non os corrixen. Nestes casos o receptor solicítalle o transmisor que lle retransmita a trama recibida erroneamente.

Existen tres polinomios xeradores que se converteron en normas internacionais:

CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$

CRC-16 = $x^{16} + x^{15} + x^2 + 1$

CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$

Os dous últimos capturan tódolos erros dos seguintes tipos:

- Erros simples
- Erros dobres
- Tódolos erros con un número impar de bits.
- Tódolos erros de ráfagas con CORRECCIÓNlonxitude de 16 bits ou menos.
- 99.997% dos erros de ráfagas de 17 bits.

3.6.- A CORRECIÓN DE ERROS

Unha vez que o receptor detectou unha situación de erro, esta situación debe ter unha solución. Neste senso existen dous métodos para corrixir unha situación de erro, a saber: Corrección de erros no destinatario e corrección de erros por retransmisión.

3.6.1.- Corrección de erros no destinatario

Neste caso cando o receptor detecte un erro intentará corrixilo coa información redundante que recibiu do emisor na propia trama. Son exemplos deste método:

- Os métodos de paridade de bloque.

- Os códigos Hamming.
- Códigos construídos tendo en conta as distancias Hamming.

Estes dous últimos códigos son moi seguros, pero precisan dun canal con maior capacidade (nº de bits pos segundo que pode transmitir o canal) para poder transmitir a mesma información que un canal con menor capacidade e que usa outro código con menor redundancia.

Por exemplo si temos un emisor que transmite palabras de 4 bits, teríamos os seguintes datos:

Exemplo 1º

	Paridade de bloque (bloques de 5 palabras)	**Códigos Hamming. (3 bits de redundancia)**
Nº Bits do bloque	6 filas x 5 columnas = 30 bits	5 palabras x 7 Bits=35 bits
Nº Bits de información	5 palabras x 4 bits = 20 bits	5 palabras x 4 bits = 20 bits
Nº Bits de redundancia	5 filas x 1 bit + 5bits hrzt =10	5 palabras x 3 bits = 15
Aproveito da canle **Fórmula xeral**	20/30 = 0,66 = 66% 4.palabras / 5.palabras + 5	20/35=0,57 = 57% 4 / 7
Capacidade da canle para poder transmitir a mesma info no mesmo tempo. C(bits/seg)	30 bits/seg. En 1 seg transmite 20 bits de información e 10 de control	35 bits/seg. En 1 seg transmite 20 bits de información e 15 de control

Exemplo 2º

	Paridade de bloque (bloques de 10 palabras)	**Códigos Hamming. (3 bits de redundancia)**
Nº Bits do bloque	11 filas x 5 columnas = 55 bits	10 palabras x 7 Bits=70 bits
Nº Bits de información	10 palabras x 4 bits = 40 bits	10 palabras x 4 bits = 40 bits
Nº Bits de redundancia	10 filas x 1 bit + 5bits hrzt =15	10 palabras x 3 bits = 30
Aproveito da canle	40/55 = 0,72 = 72% Pode chegar a aproveitar o 80%	40/70=0,57 = 57%
Capacidade da canle para poder transmitir a mesma info no mesmo tempo. C(bits/seg)	55 bits/seg. En 1 seg transmite 40 bits de información e 15 de control	70 bits/seg. En 1 seg transmite 40 bits de información e 30 de control
Outro exemplo de capacidade si temos unha velocidade 10 veces maior que a anterior		
Capacidade da canle para poder transmitir a mesma info no mesmo tempo. C(bits/seg)	1100 bits/seg. ≈ 1.1 Kbps En 1 seg transmite 800 bits de información e 300 de control	1400 bits/seg. ≈ 1.4 Kbps En 1 seg transmite 800 bits de información e 600 de control

3.6.2.- Corrección de erros por retransmisión

É moito máis sinxelo detectar o erro que corrixilo, pois a operación de corrección require calcular cales son as posicións dos bit erróneos. Na meirande parte das comunicacións actuais a corrección de erros faise por retransmisión das tramas, nas que se detectaron erros.

Obviamente este método require a comunicación bidireccional, semidúplex e preferiblemente full-duplex.

Dentro deste método existen 2 técnicas:

3.6.2.1.- Envío e espera

O transmisor envía a trama e non envía a seguinte ata que o receptor llo comunique. E dicir que o transmisor está as ordes do receptor. Pódese usar dúplex ou semidúplex. Poden acontecer dous casos:

- Se o receptor lle indica o transmisor que a trama anterior lle chegou incorrecta (NACK) o transmisor retransmite esa trama e espera ata nova orde.
- Se o receptor lle indica o transmisor que a trama anterior lle chegou correcta (ACK) o transmisor transmite a seguinte trama que corresponda e espera ata nova orde.

3.6.2.2.- Envío continuo

Esta técnica precisa comunicación dúplex, pois mentres o transmisor envía tramas o receptor vaille contestando cales recibiu correctas e cales incorrectas. Neste caso o transmisor vai enviando tramas sen parar e no caso de que reciba un NACK pode actuar de dúas formas.

Para elo imaxínese o seguinte que o transmisor ten que enviar 10 tramas (1-10), no momento en que xa ía enviando a trama 7 recibe un NACK2 (e dicir que o receptor comunicalle ó transmisor que a trama 2 estaba incorrecta), co cal o transmisor ten que retransmitir a trama 2, pois procede segundo da técnica que estea a usar:

- **Rexeite non selectivo:** retransmite todo dende a trama errónea. No caso do exemplo. Transmite 1, 2, 3, 4, 5, 6, 7 neste momento e cando recibe NACK2 e retransmite: 2, 3, 4, 5, 6, 7 e continúa con 8, 9, 10.
- **Rexeite selectivo:** Retransmítese só a trama errónea unha vez detectado polo transmisor o seu NACK. Neste caso o transmisor faría: 1, 2, 3, 4, 5, 6, 7, **2**, 8, 9, 10.

3.6.3.- Comparación dos códigos detectores o dos correctores de erros.

Sexa un sistema de transmisión coas seguintes características:

Pe_{bit} = 10^{-6} (e dicir, por cada 1.000.000 de bits un é erróneo)

Bloque = 1.000 bits

Bits a transmitir = 10^6 (e dicir, 1.000 bloques de 1.000 bits cada un, e ademais vai ocorrer un erro nun bit neste millón de bits)

	Código detector	**Código Corrector**
Nº Bits de redundancia	1 bit /bloque	10 bits / bloque
Nº total bits redundancia	1.000 bits	10.000 bits
Nº total de bits	Bits información 1.000.000 Bits redundancia 1.000 Bits retransmitidos 1.001 Total 1.002.001	Bits información 1.000.000 Bits redundancia 10.000 Total 1.010.000
Efectividade	99,8%	99 %

Conclusión: Si a probabilidade de erro é baixa e mellor usar códigos detectores que códigos correctores, xa que o tamaño da redundancia é menor.

Unidade de Traballo 4

Arquitecturas de Redes

INDICE.

FIGURAS / TÁBOAS

Unidade de Traballo 4

Arquitecturas de Redes

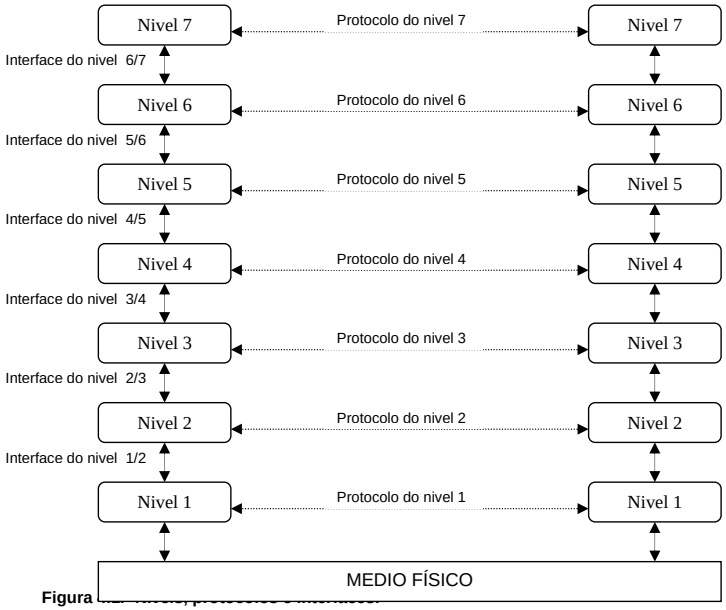
4.1.- INTRODUCCIÓN.

As redes organízanse en *capas* ou *niveis*, co obxecto de reducir a complexidade do seu deseño. Cada capa constrúese sobre a súa predecesora. O número de niveis, o nome, o contido e a función de cada un varía dunha rede a outra.

Sen embargo, en calquera rede, o propósito de cada nivel é ofrecer uns certos *servicios* ós niveis superiores, liberando a estes do coñecemento detallado sobre como se realizan ditos servicios.

Ó nivel *n* nunha máquina comunícase co nivel *n* de outra máquina. As *regras* e *convencións* usadas nesta comunicación coñécense como **protocolo de nivel n**, como se ilustra na figura 4.1.

Ás *entidades* que forman os niveis correspondentes en máquinas diferentes denomínaselles **procesos pares (igual a igual)**. E dicir, son os procesos pares os que se comunican mediante o uso dun protocolo.



Figura

Na realidade non existe unha transferencia directa de datos dende o nivel *n* dunha máquina ó nivel *n* de outra; senón que cada nivel pasa a información de *datos* e *control* ó nivel inmediatamente inferior e así sucesivamente ata acadar o nivel máis baixo da estructura. Debaixo do nivel 1 está o ***medio físico,*** a través do cal se realiza a comunicación real.

As liñas punteadas indican a comunicación virtual, en tanto que as liñas sólidas indican a traxectoria da comunicación física.

A **interface** entre dúas capas define os *servicios* e *operacións* (primitivas) que a capa inferior ofrece á capa superiores.

Ó conxunto de capas, protocolos denomínase **arquitectura de rede**.

4.2.- MODELO DE REFERENCIA OSI.

Na figura 4.2 mostrase un modelo, baseado nunha proposta desenvolvida pola ISO, como un primeiro paso hacia a normalización internacional de varios protocolos. Este modelo é coñecido como **Modelo de Referencia baseado OSI (Open System Interconection)**, porque precisamente se refire á conexión de sistemas heteroxéneos.

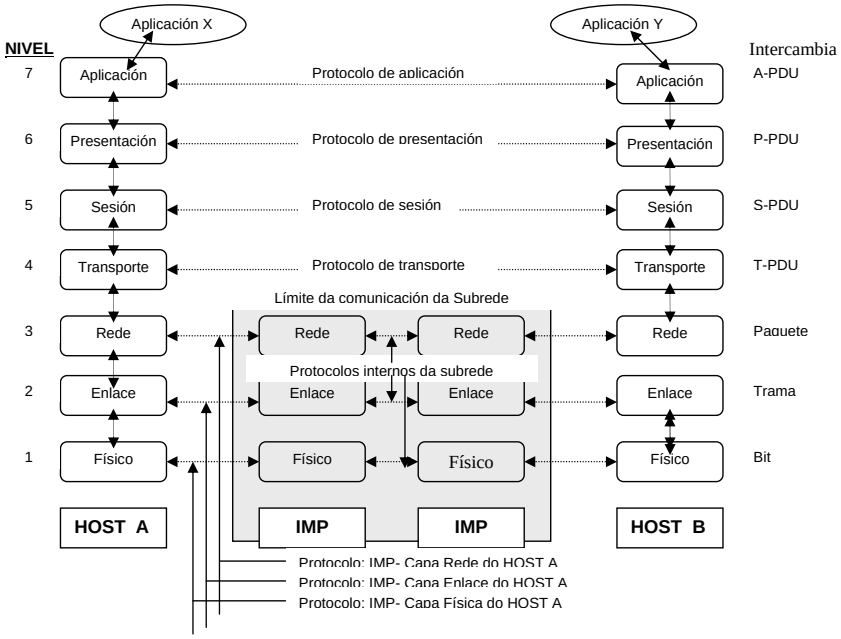


Figura 4.2.- Arquitectura de rede baseada no modelo OSI.

O modelo OSI ten sete niveis. Os principios para o establecemento dos sete niveis foron os seguintes:

1.- Un nivel crearase en situacións nas que se precise un grado diferente de abstracción.
2.- Cada nivel deberá efectuar unha función ben definida.
3.- A función que realizará cada nivel deberá seleccionarse coa intención de definir protocolos normalizados internacionalmente.
4.- Os límites dos niveis deberán seleccionarse tomando en conta a minimización de fluxo de información a través dos interfaces.
5.- O número de niveis deberá ser o suficientemente grande para que funcións diferentes non teñan que poñerse xuntas nun mesmo nivel e, por outra banda, tamén deberá ser o suficientemente pequeno para que a súa arquitectura non chegue a ser difícil de manexar.

4.2.1.- Nivel físico.

O nivel físico ocúpase da 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.

Encargase de transmitir en forma de voltaxe ou de modulación en función do medio que se estea usando.

A súa función e a de establecer a conexión entre os diferentes nodos que conforman a rede.

Este é o único nivel que ten conexión co medio físico, e este nivel está incluído dentro do dominio do Enxeñeiro Electrónico.

Preguntas comúns neste nivel son:

- Cantos voltios deberán usarse para representar un bit de valor 1 ou 0.
- Cantos microsegundos deberá durar un bit.
- Existe a posibilidade de realizar transmisións bidireccionais en forma simultánea.
- Como iniciar e terminar unha conexión.
- Cantos pins ten o conector de rede e cal é o uso de cada un delas, ...

Os problemas de deseño a considerar neste nivel son aspectos mecánicos, eléctricos e de procedemento de interface e o medio de transmisión física, que se encontra baixo a capa física.

4.2.2.- Nivel de Enlace.

A tarefa fundamental do nivel de enlace consiste en, a partir dun medio de transmisión común e corrente, transformalo nunha liña sen erros de transmisión para o nivel de rede. Esta tarefa realizase ó facer que o emisor trocee a entrada de datos en ***tramas de datos,*** as transmita en forma secuencial e procese as tramas de asentimento devoltas polo receptor.

O nivel físico acepta e transmite bits sen ter en conta a súa estructura ou significado, recae sobre o nivel de enlace a creación e o recoñecemento dos límites da trama.

Corresponde a este nivel resolver problemas causados por dano, pérdida ou duplicidade das tramas.

Outro dos problemas que aparecen neste nivel é referente a como evitar que un transmisor moi rápido sature con datos a un receptor moi lento. Para iso deben empregarse mecanismos de regulación de tráfico que lle permita ó transmisor coñecer o espacio de memoria libre que nese momento ten o receptor.

Outra dificultade reside en cando a liña ten a capacidade de utilizarse bidireccionalmente. O problema radica en que os *asentimentos* para o tráfico de *A* a *B* compiten polo uso da liña coas tramas de datos de tráfico que van de *B* a *A*. Para resolver este problema inclúense os asentimentos dentro dos mesmo datos (**piggy backing**).

4.2.3.- Nivel de rede.

O nivel de rede ocúpase do control do funcionamento da subrede:

- Determinar como *encamiñar* os ***paquetes*** de orixe ó destino.
- *Control da conxestión* no momento dado en que haxa demasiados paquetes na subrede, pois eles mesmos obstruiranse mutuamente e darán lugar a un cuello de botella.
- *Control das tarifas* en función dos paquetes, bits, caracteres, ... enviados.
- *Interconexión de redes (internetworking),* para resolver problemas de interconexión de redes heteroxéneas. (Protocolos distintos, paquetes de distintos tamaños, etc.). Nas LAN a penas existe o nivel de rede.

4.2.4.- Nivel de transporte.

É o primeiro nivel da arquitectura de tipo **extremo a extremo** (orixe da transmisión – destino da transmisión). Os protocolos dos niveis inferiores, son entre cada máquina e o seu veciño inmediato, e non entre as máquinas orixe e destino, as cales poderían estar separadas por moitos IMPs (Figura 4.2).

A función principal do nivel de trasporte consiste en aceptar os datos do nivel de sesión, dividilos, si é preciso, en unidades máis pequenas, pasarllos ó nivel de rede e asegurar que todos eles cheguen correctamente ó outro extremo.

Este traballo débese facer eficientemente, de tal xeito que aílle o nivel de sesión do hardware.

Baixo condicións normais, a capa de transporte crea unha conexión de rede distinta para cada conexión de trasporte solicitada pola capa de sesión. Pero esto non sempre ocorre, e así temos:

- **Segmentación e reensamblaxe**: se a conexión de trasporte precisase un gran caudal, esta podería crear múltiples conexións de rede, dividindo os datos entre as conexións do nivel de rede co obxecto de mellorar dito caudal (segmentar). No receptor reensamblaríanse os datos.
- **Bloqueo e desbloqueo**: noutros casos, a creación e mantemento dunha conexión de rede pode resultar custoso, neste caso o nivel de rede podería multiplexar varias conexións de trasporte sobre unha mesma conexión de rede (Bloqueo), e dicir, por unha mesma conexión de rede enviar varias T-PDUs distintas. No receptor separaríanse as T-PDUs para cada punto do nivel de trasporte.

Outras funcións que realiza o nivel de trasporte son:

- Control de fluxo entre host.
- Establecer e liberar as conexións a través da rede.

4.2.5.- Nivel de sesión.

Permite a usuarios de diferentes máquinas establecer **sesións** entre eles. A través dunha sesión pódese levar a cabo transporte de datos ordinario, tal e como o fai a capa de transporte, pero mellorando os servicios que esta proporciona. Podería permitir ó usuario acceder a un sistema en tempo compartido a distancia ou transferir un arquivo entre dúas máquinas.

En síntese é a verdadeira capa que establece sesións entre dous usuarios.

Servicios do nivel de sesión:

- **Xestión do diálogo entre dúas máquinas**, esto é, vaise permitir que o tráfico sexa full-dúplex, ou pola contra que só sexa semidúplex. Neste último caso, o nivel de sesión axudará no seguimento de quen ten o turno, (de forma análoga que un só sentido na vía do tren).
- **Administración do testemuña**: no caso de algúns protocolos resulta esencial que ambos lados non tenten realizar a mesma operación no mesmo instante. Para manexar estas actividades, o nivel de sesión proporciona testemuña que poden ser intercambiados. Soamente o extremo co testemuña pode realizar a operación crítica.
- **Sincronización**: Supoñer que se desexa enviar un ficheiro de dúas horas de duración entre dúas máquinas, nunha rede cun tempo medio de 30 min entre caídas. Despois de cada caída, teríase que iniciar a transferencia completa do arquivo, pois o emisor non sabe que parte do ficheiro xa recibiu o receptor. Para solucionar ese problema o nivel de sesión proporciona un mecanismo para inserir *puntos de verificación* no fluxo de datos, co obxecto de que despois de cada caída, só se repitan os datos que se atopan despois do último punto de verificación.

4.2.6.- Nivel de presentación.

As capas inferiores so están interesadas no movemento fiable de bits dun lugar a outro, pola contra a capa de presentación ocúpase dos seguintes aspectos:

- **Sintaxe** e **semántica** (traducción), da información que se transmite, pois o emisor pode traballar co formato EBCDIC e o receptor co formato ASCII, por exemplo, e debe haber unha traducción do contido da información dun formato a outro, para que ambos extremos entendan ese contido.
- **Compresión** dos datos, para deste xeito reducir o número de bits que se ten que transmitir.
- **Criptografía** dos datos, por razóns de seguridade, privacidade e autentificación.

4.2.7.- Nivel de aplicación.

Conten unha variedade de protocolos (aplicacións) que se precisan frecuentemente. Por exemplo, existen centos de terminais incompatibles no mundo. Problema que se aprecia cando se desexa traballar cun editor orientado a pantalla nunha rede con diferentes tipos de terminais, cada un con distintas formas de distribución de pantalla, de secuencias de escape para inserir e borrar texto, etc.

Este problema resolvese ó definir un **terminal virtual de rede abstrato**. Para iso é preciso ter un software que permita o manexo de cada tipo de terminal, e así "traduza" as operacións que se fan no terminal virtual ó terminal real. Este sw está na capa de aplicación.

Outra función é a transferencia de ficheiros, entre máquinas. Distintos sistemas de arquivos teñen diferentes normas para denominar un arquivo, así como para representar a súa información, almacenalo, etc. A transferencia destes arquivos entre dous sistemas diferentes require da resolución destas incompatibilidades.

Mais servicios son: o correo electrónico, entrada de traballo a distancia, o servicio de directorio, ...

4.2.8.- Transmisión de datos no modelo OSI.

Na figura 4.3 móstrase un exemplo de cómo poden transmitirse os datos mediante o emprego do modelo OSI. O proceso emisor ten uns datos que desexa enviar ó proceso receptor. Este entrega os datos a capa de aplicación, a cal engade entón unha cabeceira de aplicación **(AH = Aplication Head)** e a capa de aplicación entrega o elemento resultante a capa de presentación. E así sucesivamente.

É importante reseñar que a capa N-1 non ten que saber como é o protocolo da capa N. Considera os datos, a cabeceira e a cola, si esta existe, como un todo.

Este proceso séguese repetindo ata que os datos alcanzan a capa física, lugar onde efectivamente se transmiten os datos á máquina receptora.

Na outra máquina, vanse quitando unha a unha as cabeceiras e as colas, a medida que os datos se transmiten ás capas superiores, ata que finalmente cheguen ó proceso receptor.

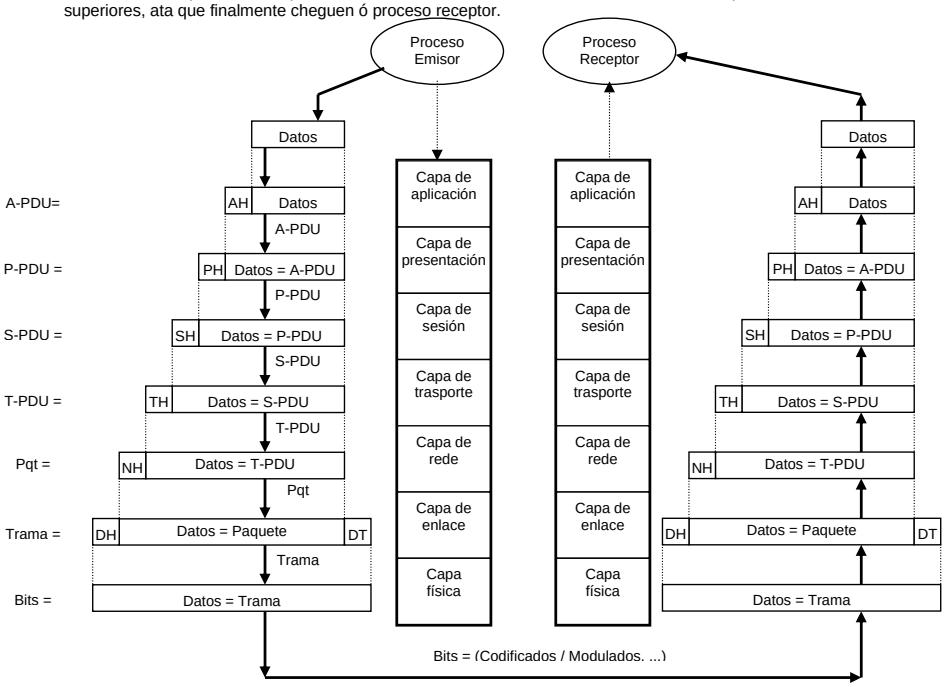


Figura 4.3.- Comunicacións entre niveis segundo o nivel OSI.

A idea fundamental é que si ben a transmisión efectiva de datos é vertical, cada unha das capas está programada como si realizara unha transmisión en horizontal.

Cando a capa de transporte, por exemplo, obtén unha mensaxe da capa de sesión, asígnalle unha cabeceira de trasporte e o envía a capa de trasporte receptora. Dende o punto de vista desta capa, o feito de que debe realmente entregar a mensaxe á capa de rede da súa propia máquina é un detalle sen importancia, xa que de forma virtual pareceralle que se está conectando co outro lado.

4.3.- SERVICIOS.

A verdadeira función de cada unha das capas OSI consiste en proporcionar servicios ás capas superiores.

4.3.1.- Terminoloxía OSI.

Entidades: son elementos activos que se atopan en cada unha das capas. As entidades poden ser software (un proceso), ou hardware (como un chip intelixente de E/S). As entidades da mesma capa, pero en diferentes máquinas, coñécense como **entidades pares ou iguales**.

As entidades da capa *N* desenvolven un servicio que usa a capa (*N+1*), neste caso á capa *N* denomínaselle **provedora de servicio** e á capa (*N+1*) **usuaria do servicio**. A capa *N* pode usar os servicios da capa (*N-1*) co obxecto de proporcionar o seu servicio. O servicio que pode prestar pode ser de varias clases, por exemplo, unha comunicación rápida e custosa, ou unha comunicación lenta e barata.

Os servicios atópanse dispoñibles no **SAP (punto de acceso ó servicio)**. Os SAP da capa *N* son os lugares onde a capa (*N+1*) pode acceder ós servicios que ofrecen as entidades da capa *N*.

Cada un dos SAP ten unha **dirección** que os identifica de forma particular. No sistema telefónico os enchufes sería os SAP e a dirección do SAP sería o número de teléfono correspondente a ese enchufe.

Para que se leve a cabo ó intercambio de información entre dúas capas, deberá existir un acordo sobre o conxunto de regras acerca da **interface**. Este proceso e os elementos relacionados móstrase na figura 4.4.

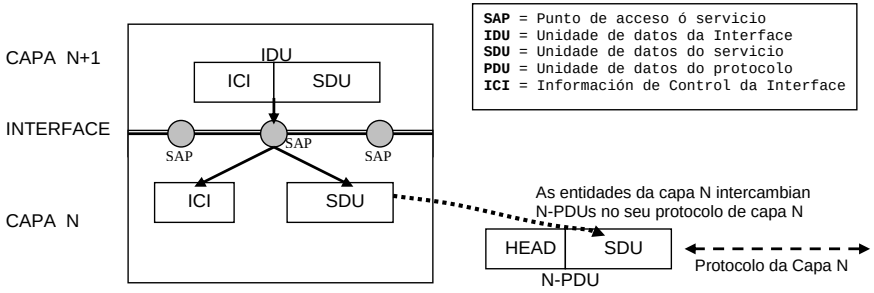


Figura 4.4.- Relación entre capas nunha interface.

SAP: Puntos nos que a capa (N+1) atopa os servicios ofrecidos polas entidades da capa N.
IDU (Unidade de datos do Interface): é o bloque de información que a *entidade* da capa (N+1) lle pasa a entidade correspondente da capa N, a través dun SAP. A IDU está dividida na información propiamente dita (SDU) e información de control (ICI).
SDU (Unidade de datos do servicio): É a información que pasa a través da rede, dunha entidade par orixe a outra entidade par destino da capa (N+1).
ICI (Información de control da interface): é a información na que a entidade da capa (N+1) lle indica a entidade correspondente da capa N como quere o servicio.
PDU (Unidade datos do protocolo): Para transmitir o SDU, pode ser preciso fraccionalo por parte da entidade da capa N en varias partes, de tal xeito que a cada unha delas se lle engada unha cabeceira e se envíe a entidade par correspondente da máquina destino como unha PDU. As entidades pares usan as cabeceiras da PDU para levar a cabo o seu protocolo de igual a igual.

Se á PDU do nivel N se lle engade un ICI indicándolle a entidade correspondente da capa (N-1) como desexa o servicio. Esa unión de ICI + PDU sería a nova IDU do nivel N que lla pasa ó nivel N-1.

4.3.2.- Servicios orientados a conexión e sen conexión.

As capas poden ofrecer dous tipos diferentes de servicios ás capas que se atopan sobre elas: un orientado a conexión e o outro sen conexión.

Servicio orientado a conexión: modelase baseándose no sistema telefónico. Para poder falar con alguén é preciso realizar 3 pasos:
establecer unha conexión (descolgar e marcar),
transmitir a información (falar),
e por último *liberar a conexión* (colgar) .
O aspecto fundamental da conexión é que actúa como un tubo, o emisor, introduce obxectos por un extremo, e o receptor os recolle, na mesma orden, polo outro.

Servicio sen conexión: modelase baseándose no sistema postal. Cada *mensaxe* (carta), leva consigo a dirección completa do destino e cada unha delas encamiñase de forma independente a través da rede. Con este tipo de servicio pode suceder que as mensaxes non cheguen na orde nas que foron enviadas.

O servicio orientado a conexión debería ser usado na transferencia de ficheiros, pois deste xeito chegaríannos os distintos mensaxes en que foi dividido o ficheiro na orde correcta. O servicio sen conexión poderíase usar no correo electrónico, pois non é preciso establecer e logo liberar unha conexión.

4.3.3.- Primitivas de servicio.

Un servicio está formalmente especificado por un conxunto de **primitivas** (operacións), a disposición de tódolos usuarios ou de outras entidades para acceder a ese servicio. Estas primitivas indícanlle ó servicio que debe efectuar unha acción ou notifican unha acción tomada por unha entidade par. Na táboa 4.1 mostra as catros clases de primitivas de servicio do modelo OSI.

PRIMITIVA	SIGNIFICADO
Solicitude, (request)	Unha entidade desexa que o servicio realice un traballo
Indicación, (indication)	Unha entidade é informada acerca dun evento
Resposta, (response)	Unha entidade desexa responder a un evento
Confirmación, (confirm)	Unha entidade é informada a cerca da súa solicitude

Táboa 4.1. Catro clases das primitivas de servicio.

A maioría das primitivas poden ter parámetros, por exemplo, os parámetros de *CONNECT.request*, poderían especificar, a máquina á que se vai conectar, o tipo de servicio que desexa, así como o tamaño máximo de mensaxe usado.

Na figura 4.5 móstrase un exemplo da idea de servicio orientado a conexión, con 8 primitivas de servicio. Na táboa 4.2 descríbense estas primitivas.

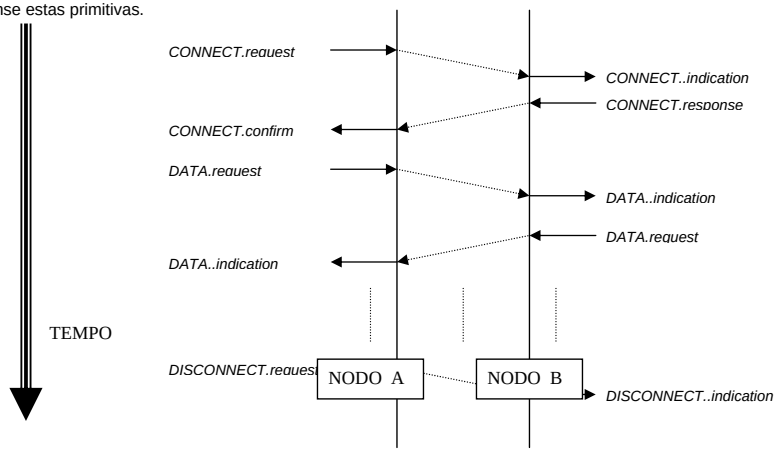


Figura 4.5.- Diagrama temporal dun servicio orientado a conexión.

Os servicios poden ser **confirmados** ou **non confirmados**. Nun servicio confirmado, hai petición, indicación, resposta e confirmación. Nun servicio sen confirmar, soamente hai petición e indicación.

	PRIMITIVA	SIGNIFICADO	CONFIRMADA
1	*CONNECT.request*	Solicitude para establecer unha conexión. (*Marcar nº de teléfono de Pepe*)	SI
2	*CONNECT.indication*	Aviso de chamada á entidade solicitada (*Soa o teléfono de Pepe*)	
3	*CONNECT.response*	A entidade corresponsal acepta/rexeita a chamada. (*Pepe descolga/non colle o teléfono*)	
4	*CONNECT.confirm*	Notifica ó que chama si a conexión é aceptada. (*Escoitamos que o telefono de Pepe deixou de soar*)	
5	*DATA.request*	Solicitude para enviar datos (*Falamos con Pepe*)	NON
6	*DATA.indication*	Aviso da chegada de datos (*Pepe escoita o que lle chega pola liña telefónica*)	
7	*DISCONNECT.request*	Solicitude para liberar a conexión (*Colgamos o teléfono*)	NON
8	*DISCONNECT.indication*	Aviso o receptor acerca da solicitude de desconexión. (*Pepe oe que se colgou o teléfono e ela colga tamén*)	

Táboa 4.2.- Descrición das primitivas orientadas a conexión.

4.3.4.- Relación entre servicios e protocolos.

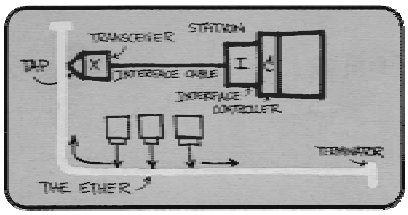
Os conceptos de servicio e protocolo teñen un significado diferente, a pesar de que con frecuencia se confunden.

Servicio: é un conxunto de primitivas (operacións), que unha capa proporciona á capa superior. O servicio define as operacións que a capa efectuarán en beneficio dos seus usuarios (capa superior), pero non di nada de cómo se realizarán esas operacións. Un servicio refírese a un interface entre dúas capas, sendo a capa inferior a que provee o servicio e a capa superior a que usa ese servicio.

Protocolo: é un conxunto de regras que gobernan o formato e o significado das tramas, paquetes ou mensaxes que son intercambiados entre entidades pares dunha capa. As entidades usan os protocolos para realizar as súas definicións de servicio, tendo a liberdade para cambiar ó protocolo, pero asegurándose de non modificar o servicio visible ó usuario. Os protocolos non son visibles para o usuario.

Redes de Area Local

Tema 6. Redes basadas en Paso de Testigo

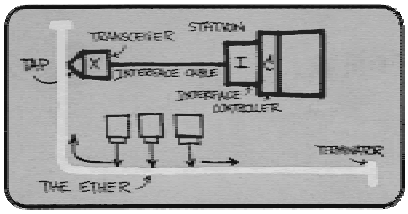


Facultad de Informática
Prof. Juan Carlos Cano

http://www.disca.upv.es/jucano
jucano@disca.upv.es

Redes de Area Local

Breves apuntes sobre Token Bus (IEEE 802.4)

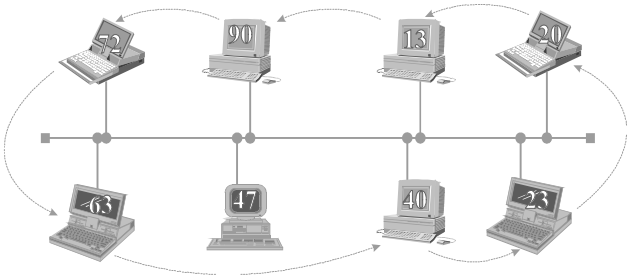


Facultad de Informática
Prof. Juan Carlos Cano

http://www.disca.upv.es/jucano
jucano@disca.upv.es

Introducción

- IEEE 802.4 (Token Bus), Anillo lógico
  - Simplicidad redes en bus
  - Garantía tiempo máximo de retardo



  - Usuarios, adaptados a los protocolos MAP
    - Manufacturing Automation Protocol

3

Método de acceso por testigo

- Un testigo, controla el acceso ordenado al medio físico
- El testigo circula por todas las estaciones que forman el anillo lógico
- el mantenimiento del anillo, se asegura por funciones realizadas por las propias estaciones de forma distribuida.
  - Iniciación del anillo
  - Recuperación del testigo
  - Adición de nuevas estaciones
  - eliminación de estaciones del anillo lógico
- El método alterna fases de transmisión de datos y transferencia del testigo.
- La estación poseedora del testigo puede transmitir datos durante un tiempo determinado a cualquier estación del Bus.

4

Formato de Trama

- Codificación Manchester

≥1	1	1	2 ó 6	2 ó 6	≥0	4	1
Preámbulo	SD	FC	Dir. Destino	Dir. Fuente	Datos LLC	CRC	ED

- FC: Trama de Control
  - Datos: 01MMMPPP
    MMM:Solicitud con o sin confirmación, o confirmación
    PPP: Prioridad
  - Control: 00CCCCCC
    000000 CLAIM_TOKEN
    000001 SOLICIT_SUCCESSOR_1
    000010 SOLICIT_SUCCESSOR_2
    000011 WHO_FOLLOWS
    000100 RESOLVE_CONTENTION
    001000 TOKEN
    001100 SET_SUCCESSOR

5

Gestión del anillo

- Tareas de mantenimiento y funcionamiento del anillo
  - Inclusión de nuevas estaciones
  - Exclusión de estaciones
  - Inicialización del Anillo
  - Manejo de fallos

6

Inclusión de nuevas estaciones
(estación intermedia)

- Periódicamente, cada estación poseedora del testigo, antes de pasarlo a su sucesora, emite una trama SOLICIT_SUCCESSOR_1, para permitir el acceso al anillo a nuevas estaciones.

Preámbulo	SD	00000001	Sucesora	Dir. Fuente	Datos LLC	CRC	ED

- Ventana de respuesta: 2 x retardo de propagación extremo a extremo
- Si alguna estación cuya dirección se encuentra entre la Dir. Fuente y la de su sucesora desea incluirse en el anillo emitirá una trama de SET_SUCCESSOR en la ventana de respuesta.

Preámbulo	SD	00001100	Dir. Destino	Dir. Fuente	Datos FTE	CRC	ED

7

Inclusión de nuevas estaciones
(estación intermedia)

- Al terminar la ventana de respuesta pueden encontrarse tres casos.
  - Ninguna estación contestó: Se pasa el testigo a la sucesora original
  - Solamente contestó una estación: Se le da de alta como sucesora y se le pasa el testigo (reconociendo la trama de SET_SUCCESSOR)
  - Contestó más de una estación (se produjo una colisión): hay que averiguar cual de ellas tiene la dirección más alta emitiendo una trama de RESOLVE_CONTENTION, y esperando 4 ventanas de respuesta
    - En la primera ventana contestan las que su dirección comienza por 11, en la segunda por 10, en la tercera por 01 y en la cuarta por 00. Si una estación detecta algo en una ventana anterior, no emitirá en la suya.
    - Si hay colisión en una ventana se emite otra trama de RESOLVE_CONTENTION y se accede a las ventanas con los siguientes dos dígitos de la dirección.

Preámbulo	SD	000001000	Sucesora	Dir. Fuente	Datos LLC	CRC	ED				

8

Inclusión de nuevas estaciones

(Última estación del anillo)

- La última estación del anillo, antes de pasarlo a su sucesora, emite una trama SOLICIT_SUCCESSOR_2.

Preámbulo	SD	00000010	Sucesora	Dir. Fuente	Datos LLC	CRC	ED

- La estación espera durante dos ventanas de respuesta
- Las estaciones con dirección inferior a la emisora responden con una trama SET_SUCCESSOR durante la primera ventana
- Si en la primera ventana no ha habido respuesta, las posibles estaciones con dirección superior contestarán en la segunda ventana con una trama de SET_SUCCESSOR
- El resto del proceso es equivalente al caso anterior de estación intermedia

9

Exclusión de Estaciones

- Para darse de baja las estaciones deben estar en posesión del testigo. Antes de cederlo deben emitir una trama de SET_SUCCESSOR a su predecesora poniendo en el campo de datos a su sucesora.
- Posteriormente cederá el testigo a su antigua sucesora.

Preámbulo	SD	00001100	Predecesora	Dir. Fuente	Datos Suces	CRC	ED

10

Inicialización del Anillo

- Cuando una estación entra en funcionamiento escucha durante un tiempo si hay actividad en el anillo (esperando un SOLICIT_SUCCESSOR_1). Si el anillo está inactivo reclama el testigo mediante un CLAIM_TOKEN.

Preámbulo	SD	00000000	Dir. Destino	Dir. Fuente	Datos (*)	CRC	ED

- Si no tiene competidores se pone ella como predecesora y sucesora de sí misma.
- Si hay competidores se sigue un algoritmo idéntico al de dar de alta nuevas estaciones, pero con tramas de CLAIM_TOKEN.
- Cuando en el anillo solo existe una estación, esta invita a las demás mediante tramas de SOLICIT_SUCCESSOR_2

Preámbulo	SD	00000010	Dir. Destino	Dir. Fuente	Datos LLC	CRC	ED

11

Manejo de Fallos

- Falla una estación mientras estaba dentro del anillo
  - Es detectado por su predecesora cuando intenta pasarle el testigo (TOKEN)

Preámbulo	SD	00001000	Dir. Destino	Dir. Fuente	Datos	CRC	ED

  - Después de pasar el testigo la estación escucha si su sucesora hace uso de él. Si no es así vuelve a pasarle el testigo una segunda vez. Si la segunda vez tampoco lo utiliza la da de baja como sucesora e intenta averiguar quién la seguía mediante WHO_FOLLOWS. La sucesora de la que ha fallado contestará mediante SET_SUCCESSOR.
  - Si nadie contesta se supone que la que seguía también ha fallado, y la poseedora del testigo reinicializará el anillo mediante una trama de SOLICIT_SUCCESSOR_2 y queda a la escucha

Preámbulo	SD	00000011	Dir. Destino	Dir. Fuente	Datos(falla)	CRC	ED

12

Manejo de Fallos (II)

- Falla la estación que poseía el testigo
  - Para manejar este fallo cada estación posee un reloj que se pone a cero cada vez que aparece una trama válida en la red. Si este reloj sobrepasa un determinado valor la estación genera una trama de CLAIM_TOKEN que produce la reinicialización del anillo.
- Multiplicidad de testigos
  - Si una estación que posee el testigo escucha la transmisión de otra estación, supone que otra estación esta en posesión de otro testigo, con lo que descarta su testigo, y se queda a la escucha hasta que le llegue de nuevo un testigo.

13

Gestión de prioridades

- Se definen 4 tipos de prioridades (tipo 6, 4, 2 y 0) siendo las de mayor prioridad las de tipo 6.
- Para gestionarlas se definen cuatro colas FIFO. El servicio de las colas se realiza atendiendo a la existencia de cuatro estaciones VIRTUALES en cada estación física que se pasan el testigo desde la de mayor prioridad a la de menor.
- El tiempo de servicio de cada cola se fija mediante un conjunto de temporizadores y variables que controlan el tiempo de rotación del testigo.
  - Hi Priority Token Holding Time (HPTHT): *"Máximo"* tiempo que puede utilizar una estación para transmitir clase i=6.
  - Token Rotation Timer, Clase 4,2,0 (TRT4,2,0):Tiempo máximo de rotación del testigo, para la clase 4,2,0, por debajo del cual se permiten transmisiones de datos de la clase 4,2,0

14

Algoritmo de transmisión

- Cuando una estación recibe el testigo, puede transmitir datos según las siguientes reglas
  - Puede transmitir datos de clase 6, mientras el tiempo transcurrido desde que comenzó a transmitir sea menor que el HPTHT
  - Tras transmitir datos de clase 6, puede transmitir datos de clase 4, mientras que el tiempo de rotación del testigo sea menor que el TRT4. Para las clases 2 y 0 el manejo es el mismo.
  - El tiempo de rotación incluye el tiempo de transferencia del Token

15

Medios alternativos del nivel físico (802.4)

Parámetro	Banda Portadora	Banda Portadora Fase Coherente	Banda Ancha			Fibra Optica
Velocidad de Transmisión	1 Mbps.	5 Mbps.	10 Mbps.	1 Mbps.	5 Mbps.	5, 10 ó 20 Mbps.
Ancho de Banda	-	-	-	1,5 MHz.	6 MHz.	270 nm.
Frecuencia Central	5 MHz.	7,5 MHz.	15 MHz.	-	-	800 - 910 nm.
Modulación	Manchester / Fase Continua FSK	Fase Coherente FSK	AM Multinivel duobinaria / PSK			On-Off
Topología	Bus Bidireccional	Bus Bidireccional	Bus Unidireccional			Estrella
Medio de Transmisión	Cable Coaxial (75 Ω)	Cable Coaxial (75 Ω)	Cable Coaxial (75 Ω)			Fibra Optica

16

CSMA/CD vs Token Bus

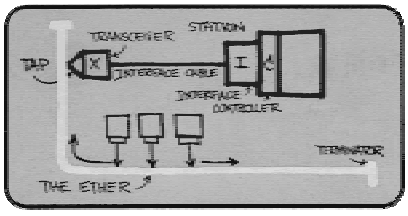
- Ventajas e Inconvenientes de CSMA/CD vs Token Bus

	Ventajas	Inconvenientes
CSMA/CD	Algoritmo sencillo	Requiere detección de colisiones
	Muy utilizado y probado	Problemas en diagnosticar fallos
	Acceso imparcial	Paquete de tamaño mínimo
	Buen rendimiento para carga media	Bajo rendimiento conforme aumenta la carga
Token Bus	Acceso regulado	Algoritmo complejo
	Red determinista	Tecnologia poco probada
	Tolera cambios dinámicos	

17

Redes de Area Local

IEEE 802.5 Token Ring



Facultad de Informática
Prof. Juan Carlos Cano

http://www.disca.upv.es/jucano
jucano@disca.upv.es

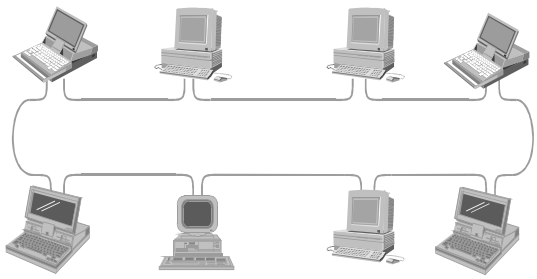
Indice

- IEEE 802.5 Token Ring
  - Introducción.
  - Control de acceso al medio.
  - Formato de trama.
  - Mantenimiento del anillo
  - Gestión de prioridades.
  - Medio físico.

19

Introducción

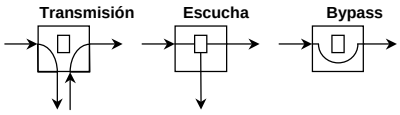
- IEEE 802.5 Token Ring
  - Topología en anillo físico.
  - Garantía de un tiempo máximo de retardo.
  - MAC: acceso por testigo.

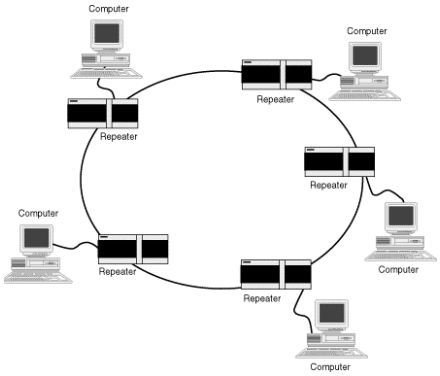


20

Topología

- IEEE 802.5 Token Ring
  - Estados del repetidor:





21

Control de acceso al medio

- Modo de Operación.
  - Por la red circula un testigo con una cierta prioridad.
  - Si una estación quiere transmitir una trama de igual o mayor prioridad que el testigo
    - cambia el bit T del campo de control de acceso del testigo, convirtiendo el testigo en una trama de datos e inserta su trama.
    - transmite las tramas.
    - cuando la trama última trama de datos vuelve al emisor éste regenera el testigo, cambiando otra vez el bit T del campo de control.

  Cuando una estación está transmitiendo no hay testigos circulando por la red, y por lo tanto, el resto de estaciones deben esperar.

22

MAC (I I)

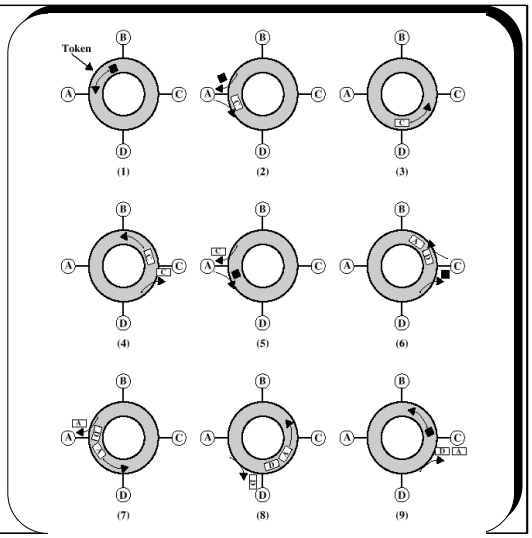
- Una vez se reinserta el testigo en la red la siguiente estación del anillo con tramas pendientes de transmisión podrá capturar el testigo y transmitir.

- Características
  - Control de acceso flexible, equitativo y eficiente para carga elevada.
  - Permite prioridades y anchos de banda garantizados.
- Mantenimiento del anillo.
  - A diferencia de la norma IEEE 802.4 aquí el mantenimiento del anillo (asegurar un único testigo en el anillo), es realizado por una sola estación en modo MONITOR.

23

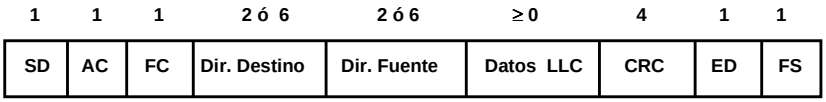
Funcionamiento

- Ejemplo
  - Testigo circulando.
  - A envía a C.
    - envía la trama
    - C la copia
    - A la reabsorbe
    - Inserta un testigo
  - C envía a A y D



24

Formato de trama



- Codificación: Manchester diferencial
- SD. Delimitador inicio JK0JK000 -> JK patrones de bits de No_Dato
- AC. Control de Acceso. PPPTMRRR
  - PPP=Bits Prioridad
  - T=Bit de testigo
  - M=Bit de monitor
  - RRR=bits de Reserva
- FC. Control de Trama. FFZZZZZZ
  - FF=Tipo de trama, Control (00), Datos (01)
  - ZZZZZZ= Tipo de trama de control

25

Formato de trama (II)

- Dir destino, Dir fuente y CRC = 802.3
- Datos LLC (No tienen definido tamaño máximo)
- ED: Delimitador Fin JK1JK1LE
  - L. Bit de trama intermedia
  - E. Bit de error detectado por estación intermedia
- FS: Estado de trama. ACrrACrr
  - A=Reconocimiento de dirección (receptor activo)
  - C=Reconocimiento de trama (CRC correcto)
  - rr=reservados
    - A=0 y C=0. Estación destino no existente o no activa
    - A=1 y C=0. Estación destino existe pero la trama no se copio
    - A=1 y C=1. Trama recibida en destino
- Un testigo sólo tiene los campos SD, AC y ED.

26

Mantenimiento del Anillo

- Pérdida del testigo
  - Debida a la desconexión de la estación que lo poseía o a un fallo de transmisión en el mismo.
  - La estación monitora tiene un reloj que arranca cada vez que una trama válida pasa a través de ella.
  - Si transcurrido un tiempo no escucha una trama válida, regenera un testigo con prioridad 0.

27

Mantenimiento del Anillo

- Circulación indefinida de Trama de Datos.
  - Debida a la desconexión de una estación antes de que retirase la trama de datos.
  - La estación monitora controla el bit M del AC de forma que la primera vez que una trama pasa por ella lo pone a 1. Si le llega una trama con este bit a 1 la retira de la red y regenera el testigo.
- Control de retardos
  - La estación monitora se encarga de introducir los retardos necesarios para que el testigo quepa en la red en toda su totalidad. (mínimo de 24 bits).

28

Mantenimiento del Anillo

- Fallo de transmisión de una estación
  - Cuando una estación detecta un fallo de transmisión (coloca a 1 el último bit del delimitador de fin) y sabe que es su predecesora la que lo ha producido.
  - Es necesario que cada estación conozca a su predecesora.
  - Cuando una estación detecta fallos repetidos de su predecesora la desconecta mediante una trama de BEACON.

29

Mantenimiento del anillo

- Esquema de notificación del vecino:
  - La estación monitora emite una trama de ACTIVE_MONITOR_PRESENT con los bits A y C a 0.
  - La estación sucesora detecta estos bits a 0, localiza a su predecesora y pone a 1 estos bits para que el resto no los capture. Cuando captura el testigo emite una trama de STANDBY_MONITOR_PRESENT con los bits A y C a 0.
  - Ahora será su sucesora la que detecta estos bits a 0 , localiza a su predecesora y pone a 1 estos bits para que el resto no los capture.
  - El esquema se repite hasta que la estación monitora detecta una trama de STANDBY_MONITOR_PRESENT con los bits A y C a 0. Lo que indica que todas las estaciones conocen a sus predecesoras.

30

Mantenimiento del Anillo

- Fallo de estación monitora.
  - Cada estación controla el tiempo transcurrido desde la última trama de ACTIVE_MONITOR_PRESENT, y el tiempo desde que recibió el testigo.
  - Si vence alguno de estos dos temporizadores, emite CLAIM_TOKEN solicitando el testigo.
  - Si la monitora no contesta se pone ella como monitora.
  - Ante varias estaciones solicitando el testigo, la resolución se basa en direcciones crecientes de las estaciones del anillo.

31

Mantenimiento del Anillo

- Múltiples estaciones monitoras
  - Cuando una estación monitora detecta ACTIVE_MONITOR_PRESENT de otra estación se pone como una estación normal o emite PURGE para reinicializar el anillo.

32

Gestión de Prioridades

- **Se contemplan 8 niveles de prioridad gestionados por 3 bits de prioridad y 3 bits de reserva de prioridad en cada trama de datos y testigo.**
- Sean:
  - Pf = prioridad de la trama a transmitir
  - Ps = prioridad de servicio (prioridad del testigo actual)
  - Pr = valor Ps contenido en el último testigo recibido por la estación
  - Rs = valor de reserva del testigo actual
  - Rr = mayor valor de reserva observado en las tramas en la última rotación del testigo

33

Gestión de Prioridades

- El esquema funciona como sigue:
  - Una estación que desee transmitir debe esperar un testigo con Ps <= Pf
  - Mientras espera puede reservar un testigo futuro con prioridad Pf (Rs := Pf) si:
    - Detecta una trama de datos con Rs < Pf
    - Detecta un testigo con Rs < Pf < Ps
  - Cuando una estación caza un testigo cambia el bit T a 1, pone el campo de reserva a prioridad 0 y no altera el campo de prioridad.

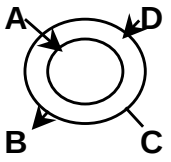
34

Gestión de Prioridades

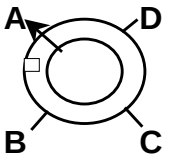
- Emisión del testigo
  - Una estación con tráfico de alta prioridad reserva en las tramas que pasan el siguiente testigo con su prioridad.
  - Cuando el siguiente testigo se emita, lo hará con la mayor prioridad reservada.
  - Las estaciones con menor prioridad no pueden capturarlo.
  - Sólo las estaciones con una prioridad igual o mayor pueden capturarlo.
  - Las estaciones que suben la prioridad del testigo son las responsables de bajar la prioridad a su antiguo valor, cuando lo vuelvan a ver con su prioridad.

35

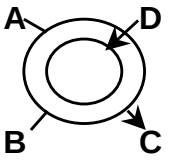
Gestión de Prioridades



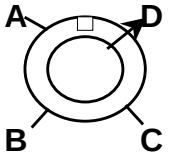
A transmite hacia B con P=0; D hace una reserva de P=3



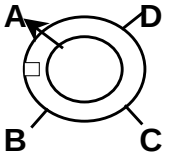
A genera un testigo con P=3 y almacena la prioridad inferior



D toma el testigo de P=3 y transmite datos hacia C , puesto que ni B ni C tienen datos con P>=3



D genera un nuevo testigo con P=3



A detecta un testigo con prioridad igual a la que utilizo en el último testigo P=3 y genera un testigo con prioridad inferior P=0

36

Gestión de Prioridades

- Resumen
  - Sx: Pila para los nuevos valores de prioridad.
  - Sr: Pila para los valores de prioridad antiguos.

Condiciones	Acciones
Trama disponible y Ps <= Pf	Transm trama
Trama no disponible y Pr >= MAX[Rr, Pf]	Transm testigo con Ps = Pf y Rs = MAX [Rr, Pf]
Trama no disponible y Sx < Pr < MAX[Rr, Pf]	Transm testigo con Ps = MAX [Rr, Pf] y Rs = 0 Push Sr = Pr Push Sx = Ps
Trama no disponible y Sx = Pr < MAX[Rr, Pf]	Transm testigo con Ps = MAX [Rr, Pf] y Rs = 0 Pop Sx Push Sx = Ps
(Trama no disponible o (Trama disponible y Ps > Pf)) y Ps = Sx y Rr > Sr	Transm testigo con Ps = Rr y Rs = 0 Pop Sx Push Sx = Ps
(Trama no disponible o (Trama disponible y Ps > Pf)) y Ps = Sx y Rr <= Sr	Transm testigo con Ps = Rr y Rs = 0 Pop Sx Pop Sr

37

Liberación rápida de testigo

- La liberación de un nuevo testigo viene determinada por la long. de la red y de la trama:
  - Si la longitud en bits del anillo es menor que la de la trama
    - La cabeza de la trama retorna antes de finalizar la txón.
    - El nuevo testigo se emitirá cuando se termine la txón.
  - Si la trama es más corta que la longitud en bits del anillo
    - La estación debe esperar hasta que retorne la cabeza de la trama antes de emitir el testigo
      - No se usa parte de la capacidad teórica del anillo

38

Liberación rápida de testigo

- Se ha incluido en 802.5 una opción de liberación rápida de testigo (ETR)
  - Permite a una estación emitir el nuevo testigo en cuanto termine la txón. de la trama
    - Independientemente de si la trama ha vuelto o no
    - Utilización más eficiente del anillo
  - La estación asignará al nuevo testigo la prioridad de la última trama recibida
  - ¿¿¿Problemas???
  - Las estaciones que incorporan ETR son compatibles y pueden interconectarse con aquellas que no disponen de él.

39

Medios de Transmisión

- Especificación del medio físico
  - Codificación Manchester Diferencial

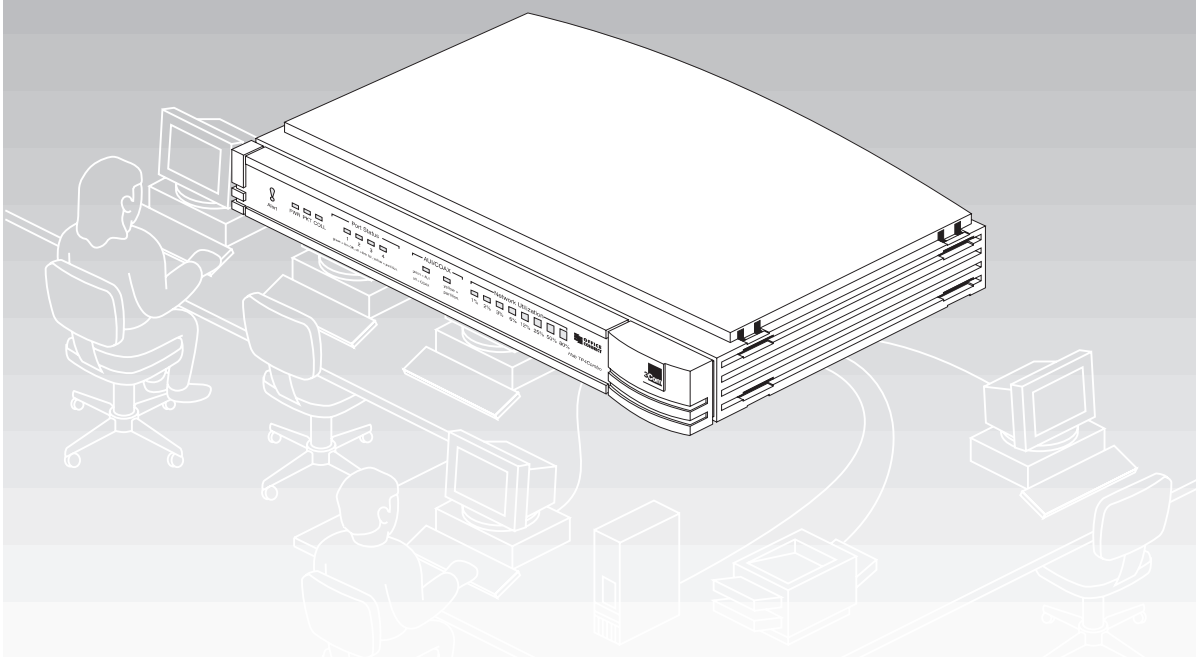
	Par trenzado apantallado	**Par trenzado sin apantallar**
Velocidad de transmisión (Mbps)	4 o 16	4
Número máximo de repetidores	250	72
Longitud máxima entre repetidor	No especificada	No especificada

40

OFFICECONNECT™ HUB

GUÍA DEL USUARIO

TP4, TP4COMBO, 8/TPO, 8/TPC, TP16C



Nº de pieza:
DUF1670-0AAA03

Publicado en
junio de 1998

Contenido

Introducción

Bienvenido al mundo de la trabajo en red con 3Com®. En el moderno mundo empresarial, comunicar y compartir información es crucial. Las redes de ordenadores han demostrado ser una de las formas más rápidas de comunicación, pero hasta ahora sólo las grandes empresas podían permitirse el lujo de disfrutar de las ventajas de la operación en red. La gama de productos OfficeConnect™ de 3Com ha cambiado esta situación, pues ha puesto las redes al alcance de la pequeña oficina.

Los hubs OfficeConnect Hub TP4, OfficeConnect Hub TP4Combo, OfficeConnect Hub 8/TPO, OfficeConnect Hub 8/TPC y OfficeConnect Hub TPIC6C son ideales para crear pequeñas redes. Su diseño compacto y atractivo es idóneo para el uso en sobremesa. Estos cinco productos forman parte de la gama OfficeConnect, que pueden apilarse cómodamente en un módulo funcional. Otras unidades de la gama ofrecen un gran número de recursos, por ejemplo, conmutación, acceso al Internet y otro acceso remoto. Si desea más información sobre estos productos, consulte la hoja informativa sobre la familia de productos de OfficeConnect que acompaña a este producto.

En esta guía del usuario se describe cómo utilizar los hubs OfficeConnect. Estos concentradores tienen características similares, por lo que esta guía contiene información general e información específica de cada uno. Para hacer referencia a todos los productos, se utiliza el término 'hub OfficeConnect'.

Un solo hub OfficeConnect permite crear una red de tamaño pequeño con un máximo de cuatro, ocho o dieciséis estaciones de trabajo, tal como se muestra en la Figura 1. Si necesita conectar más estaciones de trabajo, basta con conectar otro hub OfficeConnect y colocarlo sobre el resto mediante una sujeción para formar una pila (cada hub es un repetidor).

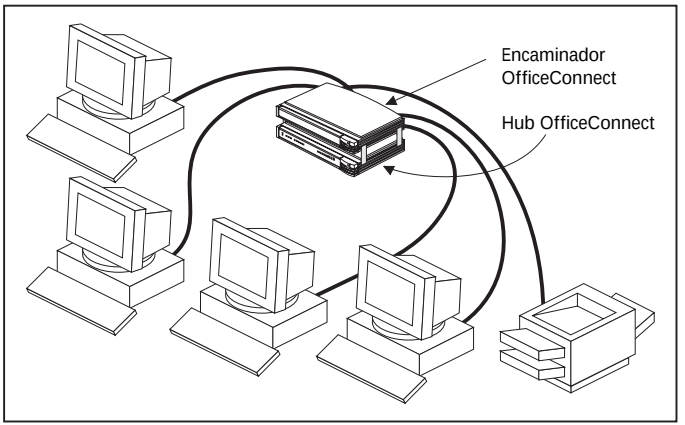


Figura 1 Red pequeña con un hub OfficeConnect y encaminador opcional

Los hubs OfficeConnect disponen de los siguientes puertos:

- El TP4 tiene cuatro puertos 10BASE-T.
- El TP4Combo tiene cuatro puertos 10BASE-T, un puerto 10BASE-2 y un puerto AUI.
- El 8/TPO tiene ocho puertos 10BASE-T.
- El 8/TPC tiene ocho puertos 10BASE-T y un noveno puerto 10BASE-2.
- El TPI6C tiene dieciséis puertos 10BASE-T y un séptimo puerto 10BASE-2.

Terminología de redes

Una **red** es un conjunto de estaciones de trabajo (por ejemplo, PC compatibles con IBM) y otros equipos (por ejemplo, impresoras), conectados entre sí con la finalidad de intercambiar información. Las redes pueden tener diferentes tamaños; algunas caben en una sala, mientras que otras se extienden por más de un continente.

Una **red de área local (LAN)** es una red, por lo general instalada en una oficina, que no suele ocupar más de un local.

Ethernet es un tipo de LAN; el nombre hace referencia a la tecnología que se utiliza para transmitir información a través de la red.

10BASE-T es la denominación del protocolo Ethernet, que funciona mediante un cable de **par trenzado (TP)**. El hub OfficeConnect utiliza conectores de tipo **RJ45** para conectar la red TP.

10BASE-2 es la denominación del protocolo Ethernet, que funciona mediante un cable **coaxial** de 50 ohmios.

Un **bucle de red** se produce cuando dos componentes del equipo de la red están conectados por más de una vía. El hub detecta esta situación y **particiona** (aísla) uno de sus puertos para interrumpir el bucle.

Un **segmento** es la extensión de cable Ethernet conectado a un puerto, ya sea el cable de tipo 10BASE-T, 10BASE-2 o de otro tipo. Cuando se conectan equipos mediante cable 10BASE-2, **todo** el cable forma un único segmento.

Los **paquetes** son las unidades de información que las estaciones de trabajo y otros equipos se envían a través de la red.

Las **colisiones** forman parte del funcionamiento normal de Ethernet, y se producen cuando dos o más dispositivos (componentes de equipo de la red) intentan transmitir al mismo tiempo. Un repentino aumento sostenido en el número de colisiones puede indicar un problema en un dispositivo, especialmente si no va acompañado de un incremento general del tráfico de la red. En los segmentos coaxiales, un aumento de las colisiones también puede indicar defectos de cableado.

Un puerto **AUI (interfaz de unidad de conexión)** es un tipo estándar de puerto que se utiliza para conectar transceptores Ethernet 10Mbps al equipo de red.

Otros componentes

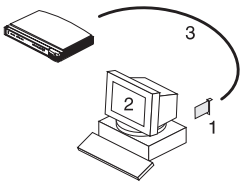
El hub OfficeConnect se entrega con:

- Un adaptador de corriente para utilizarlo con el hub OfficeConnect
- Una tarjeta de registro de garantía que debe cumplimentarse y remitirse
- Cuatro pies de caucho
- Cuatro sujeciones para apilar las unidades
- La hoja informativa sobre la familia de productos OfficeConnect

Para conectar estaciones de trabajo y hubs OfficeConnect adicionales al hub de que dispone, necesitará ocho componentes, que se indican en el resto de esta sección. Dichos componentes **no** se suministran con el hub.

Conexiones de estaciones de trabajo

Para conectar estaciones de trabajo y otros equipos al hub, necesita:



1. Conexiones 10BASE-T para todos los equipos. 3Com dispone de una gama de tarjetas adaptadoras fáciles de instalar, que proporcionan conexiones 10BASE-T a las estaciones de trabajo.
2. Un sistema operativo (por ejemplo, Novell o Windows 95) donde se haya configurado el soporte de red y que se ejecute en las estaciones de trabajo.
3. Un cable TP 'con empalme' para cada estación de trabajo, como se muestra en la Figura 3.

En conformidad con el estándar 10BASE-T, los puertos designados para conexiones de estaciones de trabajo se han marcado con el símbolo gráfico 'x', que indica un cruce en el cableado interno del puerto (por ejemplo 1x, 2x, 3x...).

Conexiones de transceptores

Si desea conectar un transceptor al hub (sólo TP4Combo), necesita:

- Un cable AUI. La extensión máxima permitida es 50 m.
- Un transceptor Ethernet 10Mbps para el tipo de soporte elegido. 3Com dispone de una gama de transceptores fáciles de utilizar.

Conexiones de hubs

Dependiendo de los puertos que tenga el hub, puede utilizar 10BASE-T o 10BASE-2 para conectar hubs entre sí:

- Con 10BASE-2 puede conectar hasta 30 hubs en un solo segmento, dejando todos los puertos 10BASE-T libres.
- Con 10BASE-T puede conectar hasta cuatro hubs en serie.

10BASE-2 Para conectar hubs adicionales utilizando 10BASE-2 (sólo TP4Combo, 8/TPC y TPI6C), necesita (como se muestra en la Figura 2):

- Un cable 10BASE-2 de 50 ohmios para cada hub adicional. La extensión mínima de cable que puede utilizar es 0,5 m. La extensión máxima que puede tener un segmento es 185 m.
- Una pieza 'Y' 10BASE-2 para cada hub. Puede utilizar piezas 'T', pero las piezas 'Y' proporcionan más espacio para acceder a los otros puertos.
- Dos terminadores (piezas de terminación) 10BASE-2 de 50 ohmios.

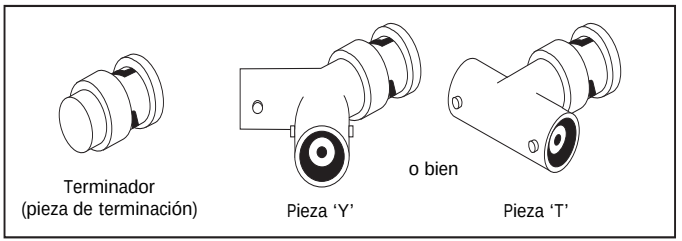


Figura 2 Parte del equipo 10BASE-2 que puede necesitar

10BASE-T Si desea conectar más hubs mediante 10BASE-T, necesita:

- Un cable TP 'con empalme' para cada hub adicional.

Cables de par trenzado (TP)

Para conectar estaciones de trabajo y hubs, debe utilizar cables TP 'con empalme' con conectores RJ45. Los cables pueden estar blindados (apantallados) o no, pero se recomiendan los primeros. La extensión máxima permitida es 100 m. En los cables 'con empalme' las patillas de un conector se conectan a las mismas patillas del otro conector. En casos especiales, es posible que tenga que utilizar cable cruzado en lugar de cable 'con empalme' (su proveedor le aconsejará sobre cuándo debe utilizar este tipo de cable). La Figura 3 muestra la conexión de las patillas en los diferentes cables TP.

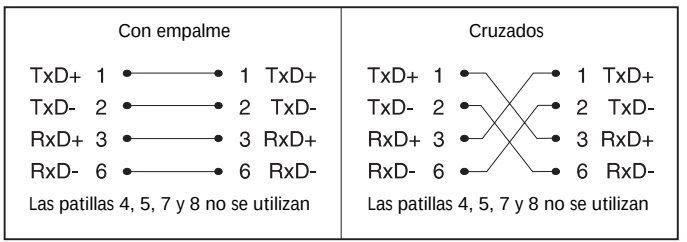


Figura 3 Cable con empalme y cable cruzado

Uso de los pies de caucho y las sujeciones de apilado

Los cuatro pies de caucho autoadherentes impiden que el hub se deslice sobre el escritorio. Adhiera los pies en las áreas marcadas en cada ángulo de la base del hub.

Las cuatro sujeciones de apilado permiten colocar las unidades OfficeConnect unas sobre otras de forma cómoda y segura.

PRECAUCIÓN: *Puede apilar un máximo de cuatro unidades. Las unidades pequeñas deben colocarse encima de las grandes.*

Para apilar las unidades, fije las sujeciones en un lateral y luego en el otro.

Para fijar las sujeciones de un lateral, siga este procedimiento, que se muestra en la Figura 4:

1 Coloque la unidad nueva sobre una superficie plana. Las sujeciones se fijan en estas posiciones del lateral de la unidad, como se muestra en el diagrama.

2 Coloque una sujeción sobre uno de los orificios y empújela hasta que encaje en su lugar. Repita la operación con la otra sujeción del mismo lateral.

3 Mantenga la parte frontal de las unidades alineada y apoye la parte inferior de la unidad nueva sobre los extremos de las sujeciones. Presione firmemente las sujeciones en la unidad existente hasta que encajen en su lugar.

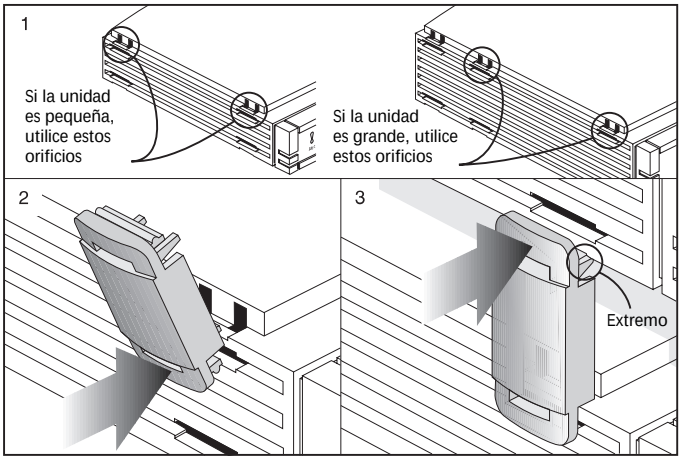


Figura 4 Unión de las unidades mediante sujeciones

Repita este procedimiento para sujetar el otro lateral.

Para extraer una sujeción, sostenga firmemente las unidades con una mano y pase el dedo índice de la otra por la parte posterior de la sujeción. Tire de ella con una fuerza razonable para extraerla.

Colocación del hub

Al instalar el hub OfficeConnect, asegúrese de que se cumplen las condiciones siguientes:

- No queda expuesto a la luz solar directa y queda apartado de fuentes de calor.
- El cableado está alejado de las líneas de alimentación, lámparas fluorescentes y fuentes de interferencias eléctricas como aparatos de radio, transmisores y amplificadores de banda ancha.
- No puede entrar agua o humedad en el bastidor de la unidad.
- El aire circula libremente alrededor de la unidad y a través de los orificios de ventilación del lateral del bastidor. Se recomienda dejar un espacio mínimo de 25,4 mm de separación.

Instalación mural del hub

Las dos ranuras de la base del hub OfficeConnect se utilizan para instalarlo en la pared. El hub puede montarse con los indicadores LED hacia arriba o hacia abajo, según convenga.

Cuando monte el hub en la pared, asegúrese de que no quede demasiado alejado de una toma de corriente.

Se necesitan dos tornillos adecuados. Asegúrese de que la pared en la que va a instalar el hub es lisa, plana y resistente, y está seca. Taladre dos agujeros con una separación de 150 mm. Utilice la plantilla que aparece en la última página de esta guía para marcar la posición de los agujeros. Fije los tornillos en la pared; deje que la cabeza de los tornillos sobresalga 3 mm de la superficie de la pared.

Desenchufe todas las conexiones del hub y colóquelo sobre las cabezas de los tornillos. Cuando esté alineado, presione el hub suavemente contra la pared y desplácelo hacia abajo para fijarlo. Cuando realice las conexiones, procure no presionar el hub hacia arriba de forma que pueda soltarse.

PRECAUCIÓN: *En la pared sólo pueden instalarse hubs individuales. No monte nunca hubs apilados.*

Utilización del hub

Ahora ya está preparado para crear una red mediante el hub OfficeConnect.

Lea las páginas 8–13 si tiene un:

- OfficeConnect Hub TP4
- OfficeConnect Hub TP4Combo

Lea las páginas 14–19 si tiene un:

- OfficeConnect Hub 8/TPO
- OfficeConnect Hub 8/TPC
- OfficeConnect Hub TPI6C

Cuando haya conectado su equipo, estará preparado para utilizar la red. Si sospecha de la existencia de algún problema, consulte (dependiendo del hub):

- "Resolución de problemas para TP4 y TP4Combo" en la página 13 (TP4 y TP4Combo)
- "Resolución de problemas para 8/TPO, 8/TPC y TPI6C" en la página 19 (8/TPO, 8/TPC y TPI6C)

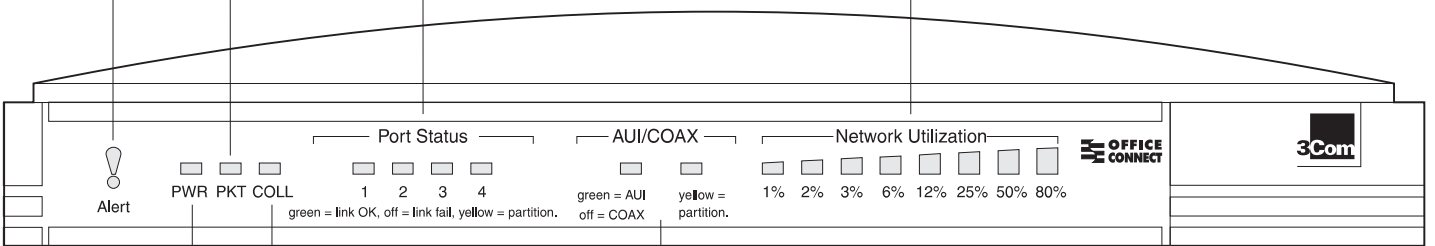
Utilización de TP4 y TP4Combo

Indicador LED de alerta
naranja
Alerta de un uso excesivo de la red o de un puerto 10BASE-T aislado (estropeado).

Indicador LED de recepción de paquetes (sólo TP4)
amarillo
Parpadea cada vez que se recibe un paquete en un puerto.

Indicadores LED de estado del puerto 10BASE-T
verde/amarillo
Indica el estado de cada puerto 10BASE-T.
verde - El enlace entre el puerto y el siguiente componente de equipo de la red es correcto.
amarillo - El puerto se ha particionado debido a una anomalía en ese segmento.
apagado - No hay nada conectado al puerto o se ha producido un error de enlace.

Indicadores LED de uso de la red (sólo TP4Combo)
verde/amarillo/naranja
Indica el porcentaje de red que se está utilizando.



Indicador LED de encendido
verde
Indica que el hub está encendido.

Indicador LED de colisión
amarillo
Parpadea cada vez que se detecta una colisión en la red. Las colisiones forman parte del funcionamiento normal de la red.

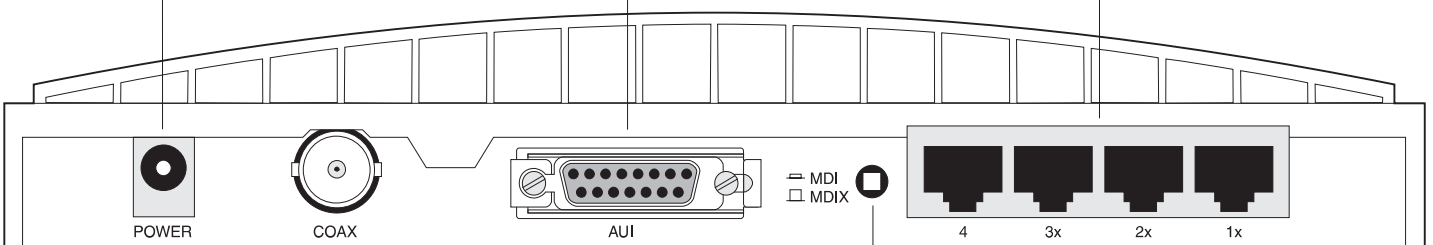
Indicadores LED de estado AUI/COAX (sólo TP4Combo)
verde/apagado=soporte, amarillo=partición
Indica el estado del puerto AUI o 10BASE-2, dependiendo de cuál se utilice.
verde/apagado - El indicador LED de estado situado a la izquierda es verde cuando se utiliza el puerto AUI, y está apagado cuando se utiliza el puerto 10BASE-2 o cuando no hay nada conectado al puerto.
amarillo - Si el indicador LED de estado situado a la derecha es amarillo, significa que el puerto que se utiliza se ha particionado.

Figura 5 Los indicadores LED y su significado

Toma de adaptador de corriente
Utilice únicamente el adaptador de corriente suministrado con el hub OfficeConnect. No utilice ningún otro adaptador.

Puerto AUI (sólo TP4Combo)
Permite a los transceptores de 10Mbps de diferentes tipos de soporte la conexión al hub. Al conectar un transceptor, el puerto 10BASE-2 se inhabilita automáticamente.

Cuatro puertos RJ45 10BASE-T
Utilice el cable 10BASE-T con conectores RJ45. Puede conectar el hub OfficeConnect a cualquier estación de trabajo o componente de equipo que tenga un puerto 10BASE-T. Consulte "Conexión de hubs con 10BASE-T", en la página 12.



Puerto 10BASE-2 (sólo TP4Combo)
Se puede utilizar para conectar el hub a otros hubs y equipo OfficeConnect con cableado 10BASE-2.
Si se utiliza, constituye un quinto puerto. Consulte "Conexión de hubs con 10BASE-2", en la página 11.

Conmutador MDI/MDIX
Afecta al funcionamiento del puerto 4. Para utilizarlo correctamente, consulte "Conexión de hubs con 10BASE-T", en la página 12.

Figura 6 Los puertos y cómo utilizarlos

Conexión de estaciones de trabajo y otros equipos al hub

ADVERTENCIA: *Asegúrese de haber leído con detenimiento la sección Información importante sobre seguridad antes de empezar.*

PRECAUCIÓN: *No apague y encienda el hub rápidamente. Espere cinco segundos entre una operación y otra.*

Conecte las estaciones de trabajo y otros equipos a cualquiera de los puertos 10BASE-T RJ45 del hub mediante cables 10BASE-T.

Para conectar un cable 10BASE-T, basta con enchufar el conector en el puerto RJ45 que corresponda. Cuando el conector está totalmente acoplado, queda bloqueado en su posición. Para desconectar el cable, presione el bloqueo del conector y quite el cable.

Si utiliza el puerto 4 para conectarse a una estación de trabajo mediante un cable TP con empalme asegúrese de que el conmutador MDI/MDIX está en la posición MDIX (no pulsado).

El hub detecta todas las conexiones de puertos, de forma que puede empezar a utilizar la red de inmediato. Cuando necesite más puertos, sólo tiene que añadir más hubs OfficeConnect.

Conexión de transceptores al puerto AUI

Puede conectar un transceptor Ethernet 10Mbps al hub (sólo TP4Combo) mediante un cable AUI estándar. Conecte un extremo del cable al transceptor y el otro extremo al puerto AUI que se encuentra en el panel posterior del hub. Esto inhabilita automáticamente el puerto 10BASE-2, y activa el LED AUI/COAX para indicar que se está utilizando el transceptor externo. Acople los bloqueos de deslizamiento a ambos extremos del cable AUI.

Conexión de hubs OfficeConnect entre sí

Para aumentar el número de estaciones de trabajo que pueden conectarse a la red, sólo es preciso añadir más hubs OfficeConnect. Para ello, puede utilizarse 10BASE-T o 10BASE-2 (sólo TP4Combo).

No conecte dos hubs iguales entre sí con un cable 10BASE-T y 10BASE-2, ya que se produciría un bucle de red.

Si no utiliza el puerto 10BASE-2, no necesita conectar un terminador (pieza de terminación) al mismo. Si no se utiliza el puerto AUI y no se conecta un terminador al puerto 10BASE-2, el puerto se particiona y el indicador LED de estado del puerto coaxial se enciende en color amarillo. Esto es indicativo de que el funcionamiento es correcto.

Conexión de hubs con 10BASE-2

Conecte una pieza 'Y' 10BASE-2 a cada uno de los hubs (sólo TP4Combo). Conecte cada pieza 'Y' mediante un cable 10BASE-2 para formar un único segmento, tal como se muestra en la Figura 7. Recuerde que debe colocar terminadores (piezas de terminación) en los dos extremos libres del segmento.

Para desconectar un cable 10BASE-2, gire cada conector en el sentido contrario a las agujas del reloj para desconectarlo y, a continuación, extráigalo.

Si ha conectado un transceptor Ethernet 10Mbps al puerto AUI, el puerto 10BASE-2 se inhabilitará. Puede utilizar este transceptor para conectar los hubs, pero se recomienda conectar los hubs mediante un cable 10BASE-T (consulte la sección siguiente).

Cuando utilice un cable 10BASE-2, es importante que en ambos extremos del segmento se coloquen terminadores (piezas de terminación) de 50 ohmios.

Sólo debe utilizar cables 10BASE-2 de 50 ohmios y una pieza 'Y' para cada hub. Puede utilizar piezas 'T', pero las piezas 'Y' dejan más espacio para acceder a otros puertos.

Comprobación de las conexiones

Cuando haya conectado los hubs, enciéndalos. Los indicadores LED de estado del puerto correspondientes a los puertos 10BASE-2 que ha utilizado deberían estar apagados. Si no lo están, compruebe las conexiones.

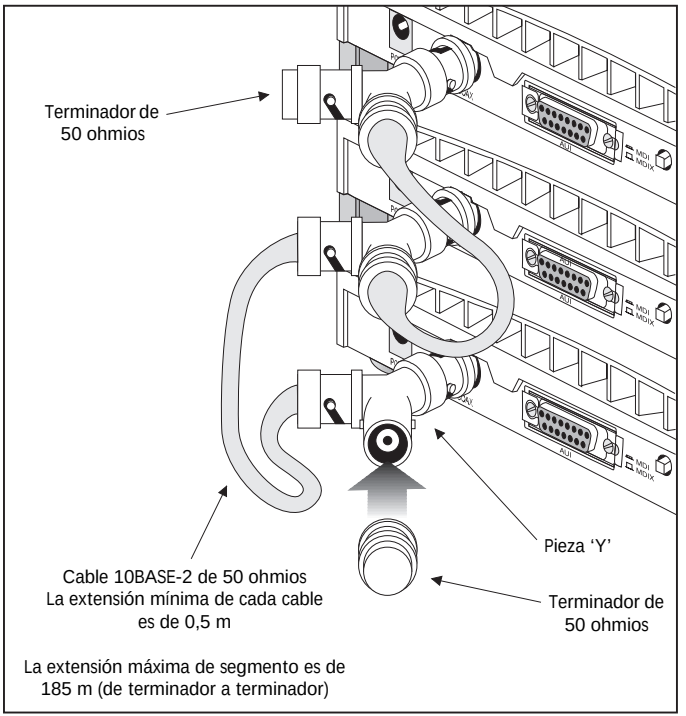


Figura 7 Conexiones correctas de los hubs mediante 10BASE-2

Conexión de hubs con 10BASE-T

Son varias las formas en que pueden conectarse hubs entre sí con 10BASE-T, pero para mayor simplicidad se recomienda el procedimiento siguiente, tal como se muestra en la Figura 8:

1. Empiece por la parte inferior y conecte el puerto 4 del hub inferior con el puerto 3 del hub inmediatamente superior. Repita este procedimiento para cada hub.
2. Coloque todos los conmutadores MDI/MDIX en la posición MDI (pulsado) excepto el hub superior (el que no tiene el puerto 4 conectado a ningún otro hub). Ese puerto no utilizado puede conectarse a una estación de trabajo siempre que el conmutador MDI/MDIX se encuentre en la posición MDIX (no pulsado).

Comprobación de las conexiones

Cuando haya conectado los hubs, enciéndalos. Los indicadores LED de estado del puerto correspondientes a los puertos 10BASE-T que ha utilizado deberían iluminarse en color verde. Si no lo están, compruebe las conexiones. Si el puerto 10BASE-2 no se utiliza y no tiene una pieza de terminación y tampoco se utiliza el puerto AUI (si existe), el indicador LED deberá iluminarse en color amarillo para indicar que ha sido particionado. Esto es indicativo de que el funcionamiento es correcto.

Inspección visual

Realice con frecuencia una comprobación visual de estas situaciones:

- El indicador LED de alerta está apagado. Ésta es la mejor forma de descubrir si hay problemas en la red.
- Los orificios de ventilación del bastidor no están obstruidos.
- Los cables están bien sujetos sin estar tensados.

Si sospecha que hay algún problema, consulte "Resolución de problemas para TP4 y TP4Combo" en la página 13.

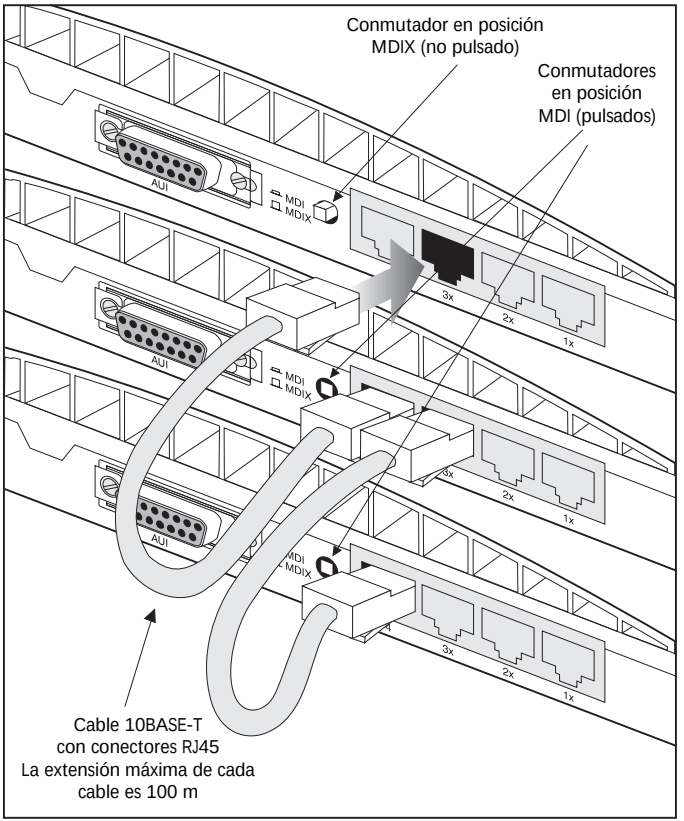


Figura 8 Conexiones correctas de los hubs mediante 10BASE-T

Resolución de problemas para TP4 y TP4Combo

El hub OfficeConnect se ha diseñado de forma que pueda prestar ayuda para detectar y solucionar posibles problemas en la red. Estos problemas raramente son graves; la causa suele ser un cable desconectado o deteriorado, o una configuración incorrecta. Si la información de esta sección no permite solucionar el problema, póngase en contacto con su proveedor para obtener información sobre los pasos que debe seguir.

Primero realice lo siguiente:

- Asegúrese de que todos los equipos están encendidos.
- Apague todos los hubs, espere unos 5 segundos y vuélvalos a encender.

Compruebe los siguientes síntomas y soluciones:

El indicador LED de encendido no se ilumina. Compruebe la conexión del adaptador de corriente. Si continúa sin encenderse, es posible que el adaptador de corriente sea defectuoso, por lo que deberá sustituirlo por otro adaptador de corriente OfficeConnect. **No utilice ningún otro adaptador de corriente en el hub.**

El indicador LED de alerta se queda encendido. Se hace un uso continuo y excesivo de la red (más del 80%) o, con mayor probabilidad, se ha particionado un puerto 10BASE-T debido a un bucle de la red (en cuyo caso, el indicador LED de estado del puerto correspondiente estará iluminado en amarillo). Examine las conexiones y elimine el bucle. Cada componente del equipo precisa únicamente una conexión al hub OfficeConnect.

El indicador LED de estado del puerto 10BASE-T está iluminado en amarillo. Es probable que exista un bucle en la red que haya causado la partición de este puerto. Examine las conexiones y elimine el bucle. Cada componente del equipo precisa únicamente una conexión al hub OfficeConnect. El indicador LED pasará de amarillo a verde cuando se reciba un paquete válido en el puerto.

El indicador LED de estado del puerto 10BASE-T que tiene una conexión no se enciende. Hay un problema en esta conexión. Compruebe que se utiliza un cable 10BASE-T con empalme bien conectado en ambos extremos y que no esté deteriorado. Si el cable está conectado al puerto 4, asegúrese de que el conmutador MDI/MDIX se encuentre en la posición MDIX (no pulsado). Asimismo, compruebe que el equipo conectado al hub está encendido y funciona correctamente.

El enlace entre dos hubs OfficeConnect no funciona. Compruebe las conexiones del hub; siga la información correspondiente a su hub. Con 10BASE-T, es probable que haya un conmutador MDI/MDIX en una posición incorrecta. Con 10BASE-2, probablemente un terminador (pieza de terminación) no está correctamente ajustado; esto haría que el indicador LED de estado del puerto coaxial estuviera iluminado en color amarillo (indicación de partición).

El indicador LED AUI/COAX de estado del puerto no se enciende cuando se utiliza el transceptor externo. Compruebe que el cable AUI está bien conectado al hub y al transceptor externo. Asegúrese de que los dos bloqueos de deslizamiento están acoplados.

El indicador LED AUI/COAX de estado del puerto se enciende en color amarillo cuando no se utiliza el puerto 10BASE-2. El puerto se ha particionado. Significa que el funcionamiento es correcto.

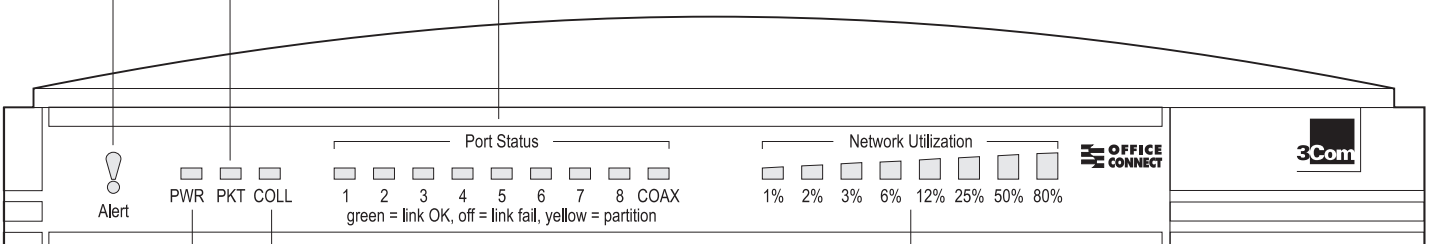
Utilización de 8/TPO, 8/TPC y TPI6C

Esta ilustración muestra el panel delantero del 8/TPC. El TPI6C es idéntico, excepto que tiene dieciséis LEDs que corresponden a su número de puertos.

Indicador LED de alerta
naranja
Alerta de un uso excesivo de la red o de un puerto 10BASE-T aislado (estropeado).

Indicador LED de recepción de paquetes (sólo 8/TPO)
amarillo
Parpadea cada vez que se recibe un paquete en un puerto.

Indicadores LED de estado del puerto
verde/amarillo
Indica el estado de cada puerto.
verde - El enlace entre el puerto y el siguiente componente de equipo de la red es correcto.
amarillo - El puerto se ha particionado debido a una anomalía en ese segmento.
apagado - No hay nada conectado al puerto o se ha producido un error de enlace.
El indicador LED de puerto 10BASE-2 (sólo 8/TPC y TPI6C) sólo puede estar iluminado en amarillo o apagado. Si está iluminado en amarillo significa que el puerto se ha estropeado.



Indicador LED de encendido
verde
Indica que el hub está encendido.

Indicador LED de colisión
amarillo
Parpadea cada vez que se detecta una colisión en la red. Las colisiones forman parte del funcionamiento normal de la red.

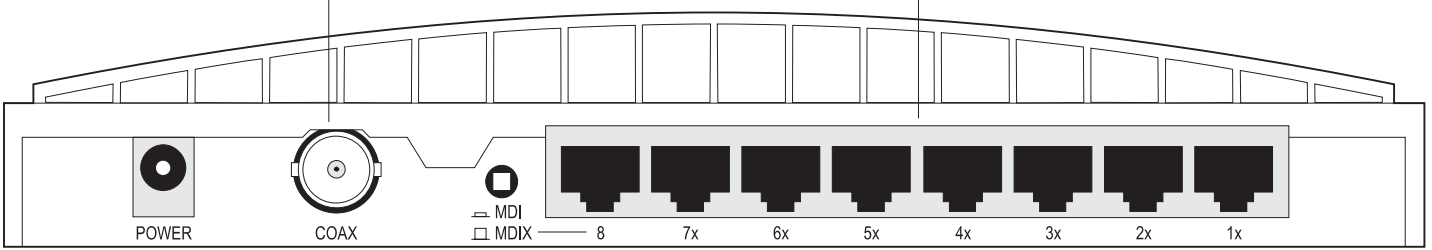
Indicadores LED de uso de la red (sólo 8/TPC y TPI6C)
verde/amarillo/naranja
Indica el porcentaje de red que se está utilizando.

Figura 9 Los indicadores LED y su significado

Esta ilustración muestra el panel trasero del 8/TPC. El TPI6C es idéntico, excepto que tiene dieciséis puertos 10 BASE-T RJ45.

Puerto 10BASE-2 (sólo 8/TPC y TPI6C)
Se puede utilizar para conectar el hub a otros hubs y equipo OfficeConnect con cableado 10BASE-2.
Si se utiliza, constituye un noveno puerto (puerto nº 17 para TPI6C). Consulte "Conexión de hubs con 10BASE-2", en la página 17.

Ocho puertos RJ45 10BASE-T
Utilice el cable 10BASE-T con conectores RJ45. Puede conectar el hub OfficeConnect a cualquier estación de trabajo o componente de equipo que tenga un puerto 10BASE-T. El puerto 8 (puerto 16 para TP16C) se puede utilizar para enlazar a otro hub OfficeConnect. Consulte "Conexión de hubs con 10BASE-T", en la página 18.



Toma de adaptador de corriente
Utilice únicamente el adaptador de corriente suministrado con el hub OfficeConnect. No utilice ningún otro adaptador.

Conmutador MDI/MDIX
Afecta al funcionamiento del puerto 8 (puerto 16 para TPI6C). Para utilizarlo correctamente, consulte "Conexión de hubs con 10BASE-T", en la página 18.

Figura 10 Los puertos y cómo utilizarlos

Conexión de estaciones de trabajo y otros equipos al hub

ADVERTENCIA: *Asegúrese de haber leído con detenimiento la sección Información importante de seguridad antes de empezar.*

PRECAUCIÓN: *No apague y encienda el hub rápidamente. Espere unos cinco segundos entre una acción y otra.*

Conecte las estaciones de trabajo y otros equipos a cualquiera de los puertos 10BASE-T RJ45 del hub mediante cables 10BASE-T.

Para conectar un cable 10BASE-T, basta con enchufar el conector en el puerto RJ45 que corresponda. Cuando el conector está totalmente acoplado, queda bloqueado en su posición. Para desconectar el cable, presione el bloqueo del conector y quite el cable.

Si utiliza el puerto 8 (puerto 16 para el TPI6C) para conectarse a una estación de trabajo mediante un cable TP con empalme, asegúrese de que el conmutador MDI/MDIX se encuentra en la posición MDIX (no pulsado).

El hub detecta todas las conexiones de puertos, de forma que puede empezar a utilizar la red de inmediato. Cuando necesite más puertos, sólo tiene que añadir más hubs OfficeConnect.

Conexión de hubs OfficeConnect entre sí

Para aumentar el número de estaciones de trabajo que pueden conectarse a la red, sólo es preciso añadir más hubs OfficeConnect. Para ello, puede utilizarse 10BASE-T o 10BASE-2 (sólo 8/TPC y TPI6C).

No conecte dos hubs iguales entre sí con un cable 10BASE-T y 10BASE-2, ya que se produciría un bucle de red.

Si no utiliza el puerto 10BASE-2, no necesita conectar un terminador (pieza de terminación) al mismo. Si no se utiliza un terminador, el puerto se particiona y el indicador LED 10BASE-2 de estado del puerto se enciende en color amarillo. Esta sería la operación correcta.

Conexión de hubs con 10BASE-2

Conecte una pieza 'Y' 10BASE-2 a cada uno de los hubs (sólo 8/TPC). Conecte cada pieza 'Y' con un cable 10BASE-2 para formar un único segmento, tal como se muestra en la Figura 11. Recuerde que debe colocar terminadores (piezas de terminación) en los dos extremos libres del segmento.

Para desconectar un cable 10BASE-2, gire cada conector en el sentido contrario a las agujas del reloj para desconectarlo y, a continuación, extráigalo.

Cuando se utiliza un cable 10BASE-2, es importante que ambos extremos del segmento acaben en terminadores (piezas de terminación) de 50 ohmios.

Utilice sólo cables 10BASE-2 de 50 ohmios y una pieza 'Y' para cada hub. Pueden emplearse piezas 'T', pero las piezas 'Y' proporcionan más espacio para acceder a los otros puertos.

Comprobación de las conexiones

Cuando haya conectado los hubs, enciéndalos. Los indicadores LED de estado del puerto correspondientes a los puertos 10BASE-2 que ha utilizado deben estar apagados. Si no lo están, compruebe las conexiones.

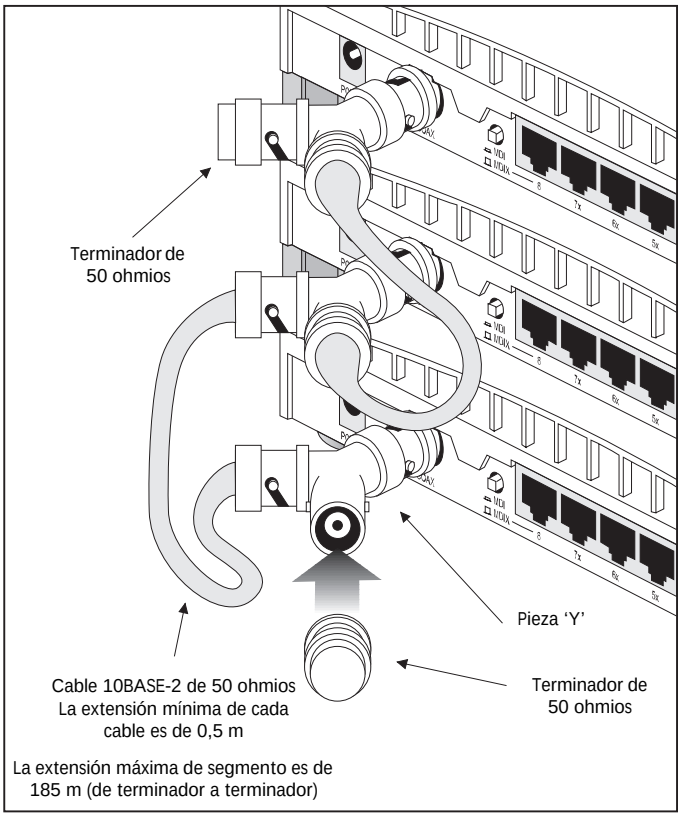


Figura 11 Conexiones correctas de hub con 10BASE-2

Conexión de hubs con 10BASE-T

Son varias las formas en que pueden conectarse hubs entre sí con 10BASE-T, pero para mayor simplicidad se recomienda el procedimiento siguiente, tal como se muestra en la Figura 12:

1. Empiece por la parte inferior y conecte el puerto 8 (puerto 16 para el TPI6C) del hub inferior al puerto 7 (puerto 15 para el TPI6C) del hub que es inmediatamente superior. Repita este procedimiento para cada hub.
2. Coloque todos los conmutadores MDI/MDIX en la posición MDI (pulsado) excepto el hub superior (el que no tiene el puerto 8 (puerto 16) conectado a ningún otro hub). Este puerto no utilizado puede conectarse a una estación de trabajo siempre que el conmutador MDI/MDIX se encuentre en la posición MDIX (no pulsado).

Comprobación de las conexiones

Cuando haya conectado los hubs, enciéndalos. Los indicadores LED de estado del puerto correspondientes a los puertos 10BASE-T que ha utilizado deben iluminarse en verde. Si no lo están, compruebe las conexiones. Si el puerto 10BASE-2 no se utiliza y no tiene una pieza de terminación y tampoco se utiliza el puerto AUI (si existe), el indicador LED debe estar en amarillo para indicar que ha sido particionado. Esto es indicativo de que el funcionamiento es correcto.

Inspección selectiva

Realice con frecuencia una comprobación visual de lo siguiente:

- El indicador LED de alerta está apagado. Ésta es la mejor forma de descubrir si hay problemas en la red.
- Los orificios de ventilación del bastidor no están obstruidos.
- Los cables están bien sujetos, sin estar tensados.

Si sospecha que hay algún problema, consulte la sección "Resolución de problemas para 8/TPO, 8/TPC y TPI6C", en la página 19.

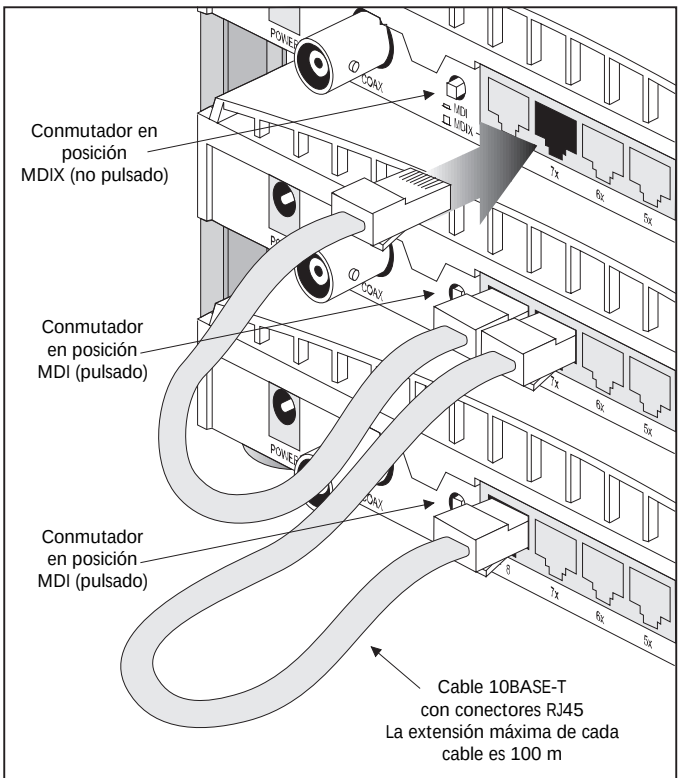


Figura 12 Conexiones correctas de los hub con 10BASE-T

Resolución de problemas para 8/TPO, 8/TPC y TPI6C

El hub OfficeConnect se ha diseñado de forma que pueda prestar ayuda para detectar y solucionar posibles problemas en la red. Estos problemas raramente son graves; la causa suele ser un cable desconectado o deteriorado, o una configuración incorrecta. Si la información de esta sección no permite solucionar el problema, póngase en contacto con su proveedor para obtener información sobre los pasos que debe seguir.

Primero realice lo siguiente:

- Asegúrese de que todos los equipos están encendidos.
- Apague todos los hubs, espere unos 5 segundos, y vuélvalos a encender.

Compruebe los siguientes síntomas y soluciones:

El indicador LED de encendido no se ilumina. Compruebe la conexión del adaptador de corriente. Si continúa sin encenderse, es posible que el adaptador de corriente sea defectuoso, por lo que deberá sustituirlo por otro adaptador de corriente OfficeConnect. **No utilice ningún otro adaptador de corriente en el hub.**

El indicador LED de alerta se queda encendido. Se hace un uso continuo y excesivo de la red (más del 80%) o, con mayor probabilidad, se ha particionado un puerto 10BASE-T debido a un bucle en la red (en cuyo caso, el indicador LED de estado del puerto correspondiente estará iluminado en amarillo). Examine las conexiones y elimine el bucle. Cada componente del equipo precisa únicamente una conexión al hub OfficeConnect.

El indicador LED de estado del puerto 10BASE-T l está iluminado en amarillo. Es probable que exista un bucle en la red que haya causado la partición de este puerto. Examine las conexiones y elimine el bucle. Cada componente del equipo precisa únicamente una conexión al hub OfficeConnect. El indicador LED pasará de amarillo a verde cuando se reciba un paquete válido en el puerto.

El indicador LED de estado del puerto 10BASE-T que tiene una conexión no se enciende. Hay un problema en esta conexión. Compruebe que se utiliza un cable 10BASE-T con empalme bien conectado en ambos extremos y que no esté deteriorado. Si el cable está conectado al puerto 8 (puerto 16 para el TPI6C), asegúrese de que el conmutador MDI/MDIX se encuentre en la posición MDIX (no pulsado). Asimismo, compruebe que el equipo conectado al hub está encendido, funciona correctamente y contiene el tipo de conexión correcto.

El indicador LED de estado del puerto se ilumina en amarillo en relación al puerto 10BASE-2 cuando dicho puerto no se utiliza. El puerto se ha particionado. Ésta es la operación correcta.

El enlace entre dos hubs OfficeConnect no funciona. Compruebe las conexiones del hub; siga la información correspondiente a su hub. Con 10BASE-T, es probable que haya un conmutador MDI/MDIX en una posición incorrecta. Con 10BASE-2, probablemente un terminador (pieza de terminación) no está correctamente ajustado; esto haría que el indicador LED 10BASE-2 de estado del puerto estuviera iluminado en color amarillo (indicación de partición).

Dimensiones y estándares

Dimensiones y condiciones de funcionamiento

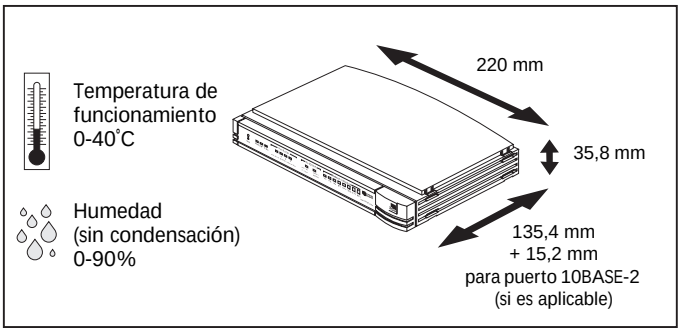


Figura 13 Dimensiones y condiciones de funcionamiento del hub

	Potencia	Peso
OfficeConnect Hub TP4	4 VA, 14 BThU/h	500 g
OfficeConnect Hub TP4Combo	12 VA, 40 BThU/h	550 g
OfficeConnect Hub 8/TPO	11 VA, 38 BThU/h	500 g
OfficeConnect Hub 8/TPC	12 VA, 40 BThU/h	550 g
OfficeConnect Hub TP16C	18 VA, 61 BThU/h	960 g

Estándares

Funcionamiento:	ISO 8802/3 IEEE 802.3
Seguridad:	UL 1950, EN 60950 CSA 22.2 nº950
EMC:	EN 55022 Clase B† EN 50082-1 FCC Parte 15 Clase B†* CSA C108.8 Clase B† VCCI Clase 2†
Entorno:	EN 60068 (IEC 68)

† Para garantizar el cumplimiento de los límites de la Clase B deben utilizarse cables apantallados de categoría 5. El uso de cables sin apantallar (categoría 3 o categoría 5) se ajusta a los límites de la Clase A.

*Consulte las condiciones de funcionamiento en la sección "Declaraciones EMC", en la página 21.

Información medioambiental

3Com sigue la política de favorecer la conservación del medio ambiente en todas sus operaciones. Este manual está impreso en papel procedente de bosques europeos cultivados para ese fin. El proceso de producción para formar la pulpa tiene un nivel reducido de AOX (halógeno orgánico absorbible), lo que produce un papel sin cloro elemental.

Este papel es totalmente biodegradable y reciclable.

Declaraciones EMC

DECLARACIÓN FCC: Este equipo se ha probado, y se ha verificado que se mantiene dentro de los l'mites correspondientes a un dispositivo digital de Clase B, tal como se define en la Parte 15 de las normas FCC. Estos l'mites se han definido con el fin de proporcionar una protección razonable contra interferencias perjudiciales en áreas residenciales. Este equipo genera, utiliza y puede emitir energ'a de radiofrecuencia y, si no se instala y utiliza de acuerdo con las instrucciones, puede ocasionar interferencias perjudiciales en las comunicaciones de radio. Si se instala correctamente, es probable que no interfiera con la radio o la televisión. No obstante, la ausencia de interferencias no puede garantizarse. Si el equipo llega a producir dichas interferencias (para determinarlo, debe encenderse y apagarse el equipo), el usuario debe intentar corregirlas con una o más de las siguientes medidas:

- Cambie la orientación o la posición de la antena receptora.
- Aumente la separación entre el equipo y el receptor.
- Conecte el equipo a una fase de corriente diferente de la toma a la que está conectado el receptor.
- Consulte a su distribuidor o a un técnico experto en radio y televisión.
- Para realizar la conexión de este equipo es preciso utilizar cables apantallados.

DECLARACIÓN CSA (CANADÁ): This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Este aparato digital de Clase B satisface todos los requisitos especificados en las regulaciones canadienses relativas a equipos causantes de interferencias.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

La siguiente publicación de la Comisión federal de comunicaciones (FCC) de Estados Unidos puede ser de utilidad:

'How to Identify and Resolve Radio-TV Interference Problems'

Puede solicitarla al servicio de publicaciones del Gobierno de Estados Unidos, Washington, DC 20402, Nº de artículo 004-000-00345-4.

Para cumplir los límites de emisiones de FCC, este equipo debe utilizarse sólo con cables que se ajusten a IEEE 802.3.

Información importante sobre seguridad

ADVERTENCIA: *Las advertencias contienen instrucciones que deben seguirse por razones de seguridad personal. Siga todas las instrucciones detenidamente.*
Lea atentamente la siguiente información antes de instalar el hub OfficeConnect:

- Al instalar o desmontar la unidad es preciso extremar las precauciones.
- Este hub OfficeConnect debe apilarse sólo con otras unidades OfficeConnect.
- Para garantizar el cumplimiento de las normas internacionales de seguridad, debe utilizarse exclusivamente el adaptador de corriente que se suministra con la unidad.
- Es esencial que la toma de corriente se encuentre cerca de la unidad y sea accesible. La única forma de cortar la alimentación al hub OfficeConnect consiste en desconectar el adaptador de corriente de la unidad o del enchufe.
- Esta unidad funciona bajo condiciones de voltaje de seguridad extra bajo (SELV) en conformidad con el estándar IEC 950; dichas condiciones sólo se mantienen si el equipo al que se conecta la unidad se ajusta también a las mismas.
- El hub no contiene fusibles que deba sustituir el usuario ni piezas que deba reparar. Si la unidad presenta algún problema físico que no pueda resolverse siguiendo las indicaciones de la resolución de problemas de esta guía, póngase en contacto con su proveedor.
- Antes de trasladar la unidad, desconecte el adaptador de corriente.

ADVERTENCIA: Puertos RJ45 de par trenzado. *Son tomas de datos RJ45. No pueden utilizarse como tomas de teléfono. Conecte sólo conectores de datos RJ45 en este tipo de tomas.*

3Com Corporation, 5400 Bayfront Plaza, Santa Clara, California, 95052-8145

DECLARACIONES APLICABLES AL GOBIERNO DE ESTADOS UNIDOS: Para las agencias gubernamentales estadounidenses, esta documentación y el software descrito en ella se proporcionan con sujeción a los siguientes derechos restringidos:

Para negociados del Ministerio de Defensa : *Declaración de derechos restringidos:* El uso, la duplicación o la divulgación por parte del Estado están sujetos a restricciones tal como se establece en el subpárrafo (c) (1) (ii) de la cláusula de derechos restringidos sobre documentación técnica y software de ordenadores en 48 C.F.R. 52.227-7013. 3Com Ireland, c/o 3Com Centre, Boundary Way, Hemel Hempstead, Herts, HP2 7YU, Reino Unido.

Para organismos civiles: *Declaración de derechos restringidos:* El uso, la reproducción o la divulgación están sujetos a restricciones tal como se establece en los subpárrafos (a) a (d) de la cláusula de derechos restringidos sobre software comercial de ordenadores en 48 C.F.R. 52.227-19 y a las limitaciones establecidas en el contrato comercial estándar de 3Com Corporation para el software. Derechos no publicados reservados bajo las leyes de copyright de Estados Unidos.

Si en esta documentación se ofrece una descripción de software en soporte extraíble, éste se proporciona bajo un contrato de licencia que se incluye con el producto como documento separado, en la documentación impresa o en el soporte extraíble en un archivo denominado LICENSE.TXT. Si no puede encontrarlo, póngase en contacto con 3Com para que se lo remitan.

A menos que se indique lo contrario, las marcas registradas de 3Com están registradas en Estados Unidos, y pueden estarlo o no en otros países.

3Com es una marca comercial registrada de 3Com Corporation. OfficeConnect es una marca comercial de 3Com Corporation.

Otras marcas y nombres de productos pueden ser marcas comerciales registradas o marcas comerciales de sus compañías respectivas.

Garantía limitada indefinida

El período de validez de la garantía de los OfficeConnect Hub TP4 (3C16704), OfficeConnect Hub TP4Combo (3C16703), OfficeConnect Hub 8/TPO (3C16700) y OfficeConnect Hub 8/TPC (3C16701) es indefinido, e incluye el adaptador de corriente.

Durante el primer año, a partir de la fecha de compra, se dispone del servicio avanzado de sustitución de hardware según los términos y las condiciones estándar de 3Com para dicho servicio. Tras el primer año, la garantía revierte a la garantía limitada indefinida estándar de 3Com.

Para tener derecho a la garantía limitada indefinida y el servicio avanzado de sustitución de hardware, debe remitirse a 3Com la tarjeta de registro de garantía del producto pertinente; de lo contrario, este producto tendrá una garantía de un período de un (1) año sin servicio avanzado de sustitución de hardware.

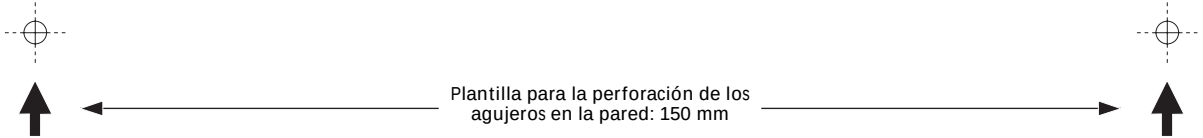
HARDWARE: 3Com garantiza que sus productos de hardware no presentarán defecto alguno de material ni fabricación, bajo condiciones normales de uso y servicio, durante los siguientes períodos a partir de la fecha de compra a 3Com o al concesionario autorizado:

Adaptadores de red	Indefinido
Otros productos de hardware	Un año (a menos que se especifique lo contrario)
Piezas y kits de recambio	90 días

En el supuesto de que un producto no funcionara tal como indica la garantía durante el período aplicable de la misma, 3Com efectuará la reparación del producto o componente defectuoso o bien entregará al cliente un producto o componente equivalente para sustituir el componente defectuoso, sin cargo alguno; o bien le reembolsará al cliente el precio que pagó por el producto defectuoso. Todos los productos que se sustituyan pasarán a ser propiedad de 3Com. Los productos de recambio podrán ser nuevos o productos reacondicionados. Cualquier producto o componente reparado o sustituido tiene noventa (90) días de garantía o bien el período restante de la garantía inicial (se considerará el período más largo).

3Com no se hará responsable del software, firmware, información o datos de la memoria que el cliente haya instalado, almacenado o integrado en cualquiera de los productos que entregue a 3Com para su reparación, ya estén o no en garantía.

SOFTWARE: 3Com garantiza que los programas de software para los que tiene licencia funcionarán de acuerdo con las especificaciones del programa durante un período de noventa (90) días a partir de la fecha de compra en 3Com o en un Proveedor autorizado. 3Com garantiza que los soportes magnéticos que contienen el software no presentarán errores mientras dure la garantía. No se proporcionarán actualizaciones. La única obligación de 3Com respecto a esta garantía expresa será (a discreción de 3Com)



el reembolso del precio pagado por el cliente por cualquiera de los productos de software defectuosos, o sustituir los soportes magnéticos defectuosos por un programa de software que cumpla substancialmente las especificaciones aplicables publicadas por 3Com. El cliente asume la responsabilidad de seleccionar las aplicaciones apropiadas y los materiales de referencia asociados. 3Com no garantiza que sus productos de software funcionen en combinación con otros componentes de hardware o aplicaciones de software de otros proveedores, que el funcionamiento de los productos de software no sufra interrupciones ni esté exento de errores, o que todos los defectos de los productos de software sean corregidos. En cuanto a los productos de otros proveedores que figuran en la documentación y las especificaciones de productos de software de 3Com que éste considera compatibles, 3Com realizará las tareas necesarias para que dicha compatibilidad se lleve a término, excepto cuando la falta de compatibilidad esté originada por un error o defecto en el producto del proveedor.

SERVICIO DE GARANTÍA ESTÁNDAR: Puede obtener el servicio estándar de garantía para los productos de hardware entregando el producto defectuoso, acompañado de una copia de la prueba de compra con la fecha especificada, al Centro de servicio técnico de 3Com o a un Centro de servicio técnico de 3Com autorizado, durante el período de validez de la garantía. El servicio de garantía estándar para los productos de software puede obtenerse telefoneando al Centro de servicio técnico de 3Com o a un Centro de servicio técnico 3Com autorizado, dentro del período de validez de la garantía. Los productos que se entreguen en el Servicio técnico de 3Com deben contar con una autorización previa de 3Com, con un número de Autorización de devolución de material (ADM) marcado en la parte exterior del paquete, y deberá enviarse a portes pagados, con seguro y debidamente embalado para garantizar la integridad del producto durante el envío. El producto reparado o sustituido se enviará al cliente con cargo a 3Com en el transcurso de treinta (30) días después de la recepción en 3Com del producto defectuoso.

CLÁUSULAS EXCLUSIVAS DE LA GARANTÍA: SI UN PRODUCTO 3COM NO FUNCIONA CONFORME A LA GARANTÍA ESPECIFICADA, EL ÚNICO RECURSO DEL CLIENTE FRENTE AL INCUMPLIMIENTO DE LA GARANTÍA SERÁ LA REPARACIÓN, SUSTITUCIÓN O REEMBOLSO DEL PRECIO DE COMPRA, A DISCRECIÓN DE 3COM HASTA EL MÁXIMO ESTABLECIDO POR LA LEY. LAS GARANTÍAS Y RECURSOS PRECEDENTES SON EXCLUSIVOS Y SUSTITUYEN CUALQUIER OTRA GARANTÍA, CLÁUSULA O CONDICIÓN, IMPLÍCITAS O EXPLÍCITAS, TANTO DE HECHO COMO POR CUMPLIMIENTO DE LA LEY, ESTATUTARIAS O DE OTRO TIPO, INCLUYENDO GARANTÍAS, CLÁUSULAS O CONDICIONES DE COMERCIALIZACIÓN, IDONEIDAD PARA UN PROPÓSITO DETERMINADO Y CALIDAD SATISFACTORIA. 3COM TAMPOCO ASUME NI AUTORIZA QUE NINGUNA OTRA PERSONA ASUMA EN SU NOMBRE OTRAS RESPONSABILIDADES EN RELACIÓN CON LA VENTA, INSTALACIÓN, MANTENIMIENTO O USO DE SUS PRODUCTOS.

3COM QUEDA EXONERADA DE CUALQUIER RESPONSABILIDAD, SEGÚN ESTA GARANTÍA, SI LA COMPROBACIÓN Y ANÁLISIS QUE SE EFECTÚEN REVELAN QUE EL DEFECTO ALEGADO DEL PRODUCTO NO EXISTE O FUE ORIGINADO POR USO INDEBIDO, NEGLIGENCIA, INSTALACIÓN O PRUEBA INCORRECTA, REPARACIONES O MODIFICACIONES NO AUTORIZADAS POR PARTE DEL USUARIO O DE TERCERAS PERSONAS, O POR CUALQUIER OTRA CAUSA QUE NO SEA EL PROPÓSITO A QUE ESTÁ DESTINADO, YA SEA POR ACCIDENTE, INCENDIO, TORMENTAS CON APARATO ELÉCTRICO U OTRAS CONDICIONES ADVERSAS.

DECLINACIÓN DE RESPONSABILIDADES: HASTA EL MÁXIMO ESTABLECIDO POR LA LEY, 3COM Y SUS PROVEEDORES QUEDAN EXONERADOS DE CUALQUIER RESPONSABILIDAD, YA SEA POR DAÑOS INDIRECTOS, ESPECIALES, DE CONTRATO, PUNITIVOS DE CUALQUIER TIPO, O POR LA PÉRDIDA DE BENEFICIOS, PÉRDIDA DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN O DATOS Y OTRAS PÉRDIDAS PECUNIARIAS QUE SE DERIVEN O ESTÉN RELACIONADAS CON LA COMPRA, INSTALACIÓN, MANTENIMIENTO, USO, FUNCIONAMIENTO O INTERRUPCIÓN DE SUS PRODUCTOS, INCLUSO AUNQUE 3COM O EL PROVEEDOR AUTORIZADO HAYA SIDO ADVERTIDO DE LA POSIBILIDAD DE QUE SE PRODUZCAN TALES DAÑOS, Y LIMITA SU RESPONSABILIDAD A LA REPARACIÓN, SUSTITUCIÓN O REEMBOLSO DEL PRECIO PAGADO, A DISCRECIÓN DE 3COM. ESTA DECLINACIÓN DE RESPONSABILIDADES POR DAÑOS NO SERÁ AFECTADA SI CUALQUIER REMEDIO PROVISTO EN EL PRESENTE NO CONSIGUE SU PROPÓSITO ESENCIA.L.

Algunos países, estados o provincias no contemplan la exclusión o limitación de las garantías implícitas o la limitación de daños accidentales o indirectos de determinados productos suministrados a clientes, o la limitación por daños personales, por lo que las limitaciones y exclusiones arriba mencionadas pueden estar restringidas en su localidad. Esta garantía le otorga derechos jurídicos específicos que pueden variar según la legislación vigente.

LEGISLACIÓN APLICABLE: Esta garantía limitada está regida por las leyes del estado de California.

3Com Corporation, 5400 Bayfront Plaza, Santa Clara, CA, 95052-8145, Estados Unidos.
Tel: (408) 764-5000
9/1/96

Servizos Internet en 2003 Server.

IES San Clemente
Ver. 3 (28-06-05)

Carlos Carrión Álvarez

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

Este documento irase completando con outros compoñentes.

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

0.- INDICE

Para instalar e configurar os distintos compoñentes debe estar claro todo o exposto nas transparencias:

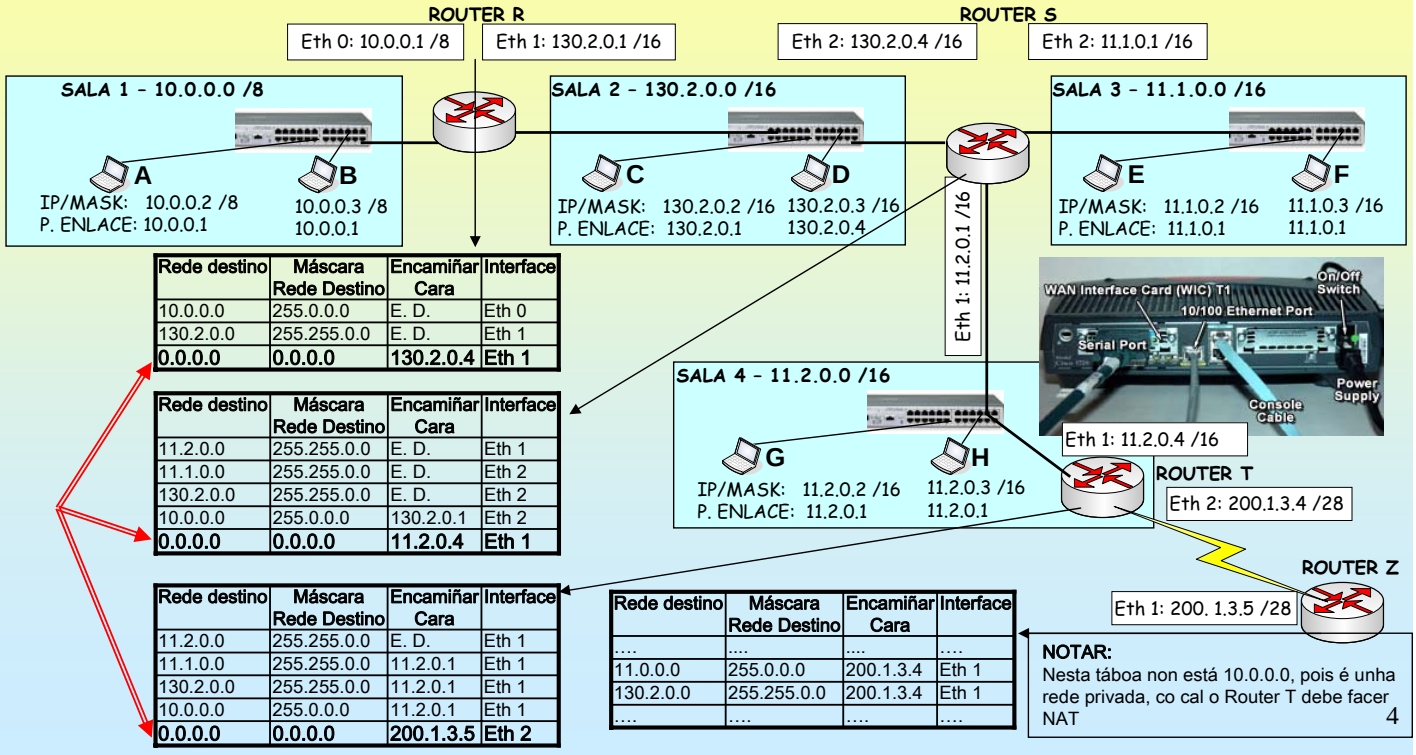
OSI – TCP/IP

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

1.- ENRUTAMENTO

☞ INTRODUCCIÓN

No seguinte debuxo o **router S** vai estar implantado nun **Windows 2003**.
Observar que une tres redes IP distintas.



Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
10.0.0.0	255.0.0.0	E. D.	Eth 0
130.2.0.0	255.255.0.0	E. D.	Eth 1
0.0.0.0	**0.0.0.0**	**130.2.0.4**	**Eth 1**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 1
11.1.0.0	255.255.0.0	E. D.	Eth 2
130.2.0.0	255.255.0.0	E. D.	Eth 2
10.0.0.0	255.0.0.0	130.2.0.1	Eth 2
0.0.0.0	**0.0.0.0**	**11.2.0.4**	**Eth 1**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 1
11.1.0.0	255.255.0.0	11.2.0.1	Eth 1
130.2.0.0	255.255.0.0	11.2.0.1	Eth 1
10.0.0.0	255.0.0.0	11.2.0.1	Eth 1
0.0.0.0	**0.0.0.0**	**200.1.3.5**	**Eth 2**

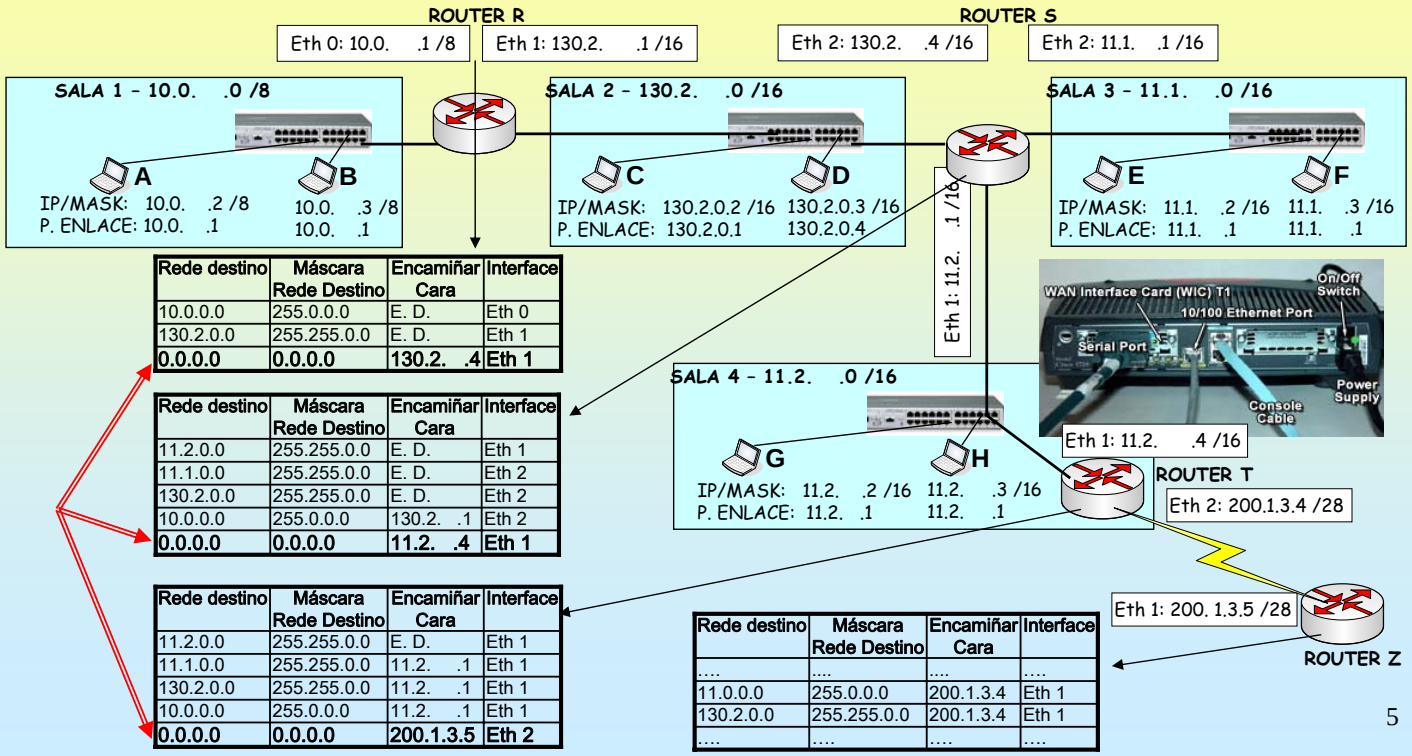
Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
....	....	....	....
11.0.0.0	255.0.0.0	200.1.3.4	Eth 1
130.2.0.0	255.255.0.0	200.1.3.4	Eth 1
....	....	....	....

NOTAR:
Nesta táboa non está 10.0.0.0, pois é unha rede privada, co cal o Router T debe facer NAT

1.- ENRUTAMENTO

☞ INTRODUCCIÓN

Exemplo para realiza en clase.



Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
10.0.0.0	255.0.0.0	E. D.	Eth 0
130.2.0.0	255.255.0.0	E. D.	Eth 1
0.0.0.0	**0.0.0.0**	**130.2. .4**	**Eth 1**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 1
11.1.0.0	255.255.0.0	E. D.	Eth 2
130.2.0.0	255.255.0.0	E. D.	Eth 2
10.0.0.0	255.0.0.0	130.2. .1	Eth 2
0.0.0.0	**0.0.0.0**	**11.2. .4**	**Eth 1**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 1
11.1.0.0	255.255.0.0	11.2. .1	Eth 1
130.2.0.0	255.255.0.0	11.2. .1	Eth 1
10.0.0.0	255.0.0.0	11.2. .1	Eth 1
0.0.0.0	**0.0.0.0**	**200.1.3.5**	**Eth 2**

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
....	....	....	....
11.0.0.0	255.0.0.0	200.1.3.4	Eth 1
130.2.0.0	255.255.0.0	200.1.3.4	Eth 1
....	....	....	....

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

1.- ENRUTAMENTO

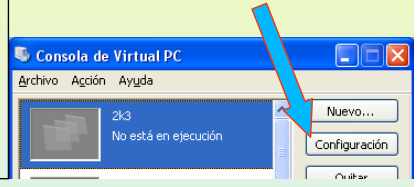
☞ PREPARATIVOS para VM-Ware ou Virtual PC

O 1º que hai que facer é configurar o interface de rede coas IPs do ROUTER S.
Notar que a un mesmo interface de rede pódenselle asinar as tres IPs do router S.

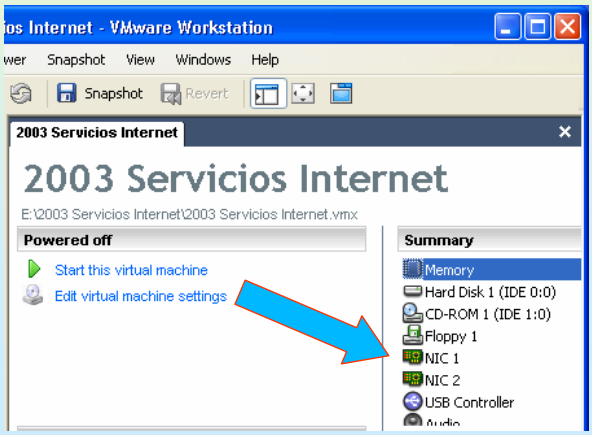
Neste exemplo terase un ordenador con dúas tarxetas de rede.
Unha tarxeta terá asignadas 2 IPs (eth2) e a outra 1 soa (eth1).

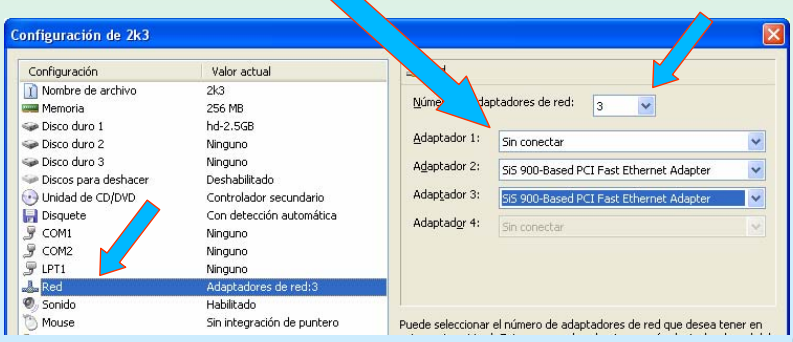
VirtualPC

OLLO:
Se se copia unha máquina instalada no Virtual PC que ten unha tarxeta de rede. E se se inician as dúas máquinas estas van ter a mesma MAC. Por iso, se desconecta a 1ª tarxeta.
Esto non pasa no VMware.



VmWare





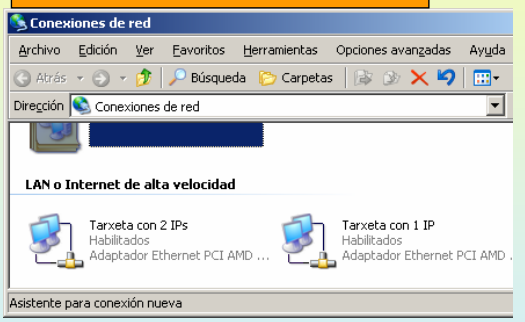
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

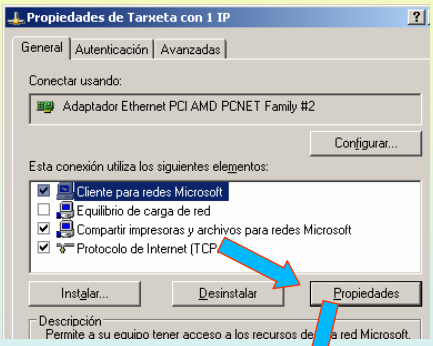
1.- ENRUTAMENTO

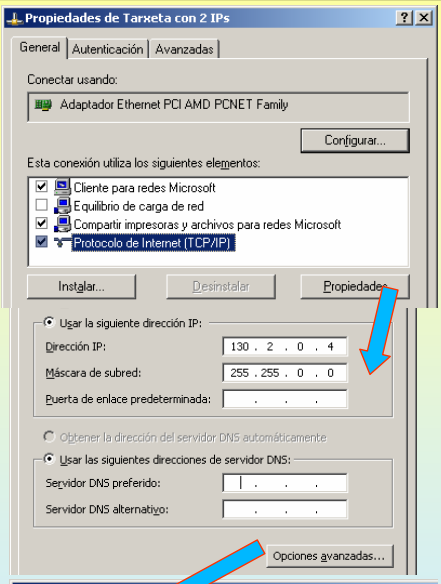
☞ Configurar IPs das tarxetas

Unha tarxeta terá asignadas 2 IPs (eth2) e a outra terá 1 soa IP (eth1).

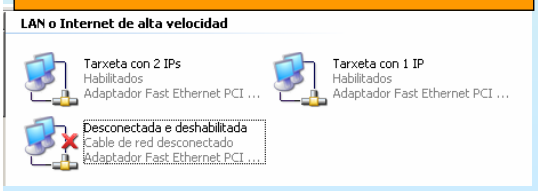
VmWare

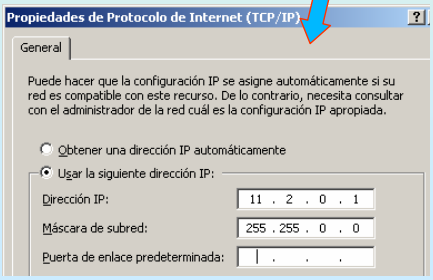


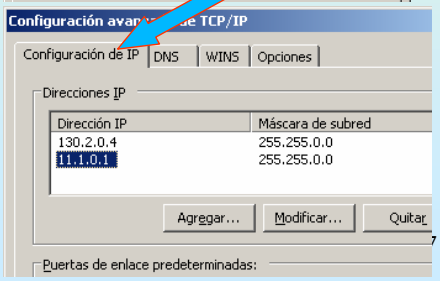




VirtualPC: Ollo que se deshabilitada a tarxeta que ten a mesma mac. Non debuxo non o está.





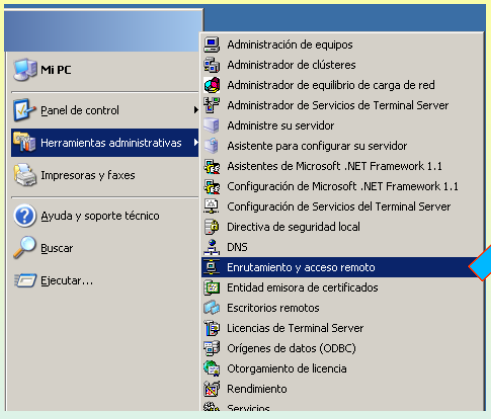


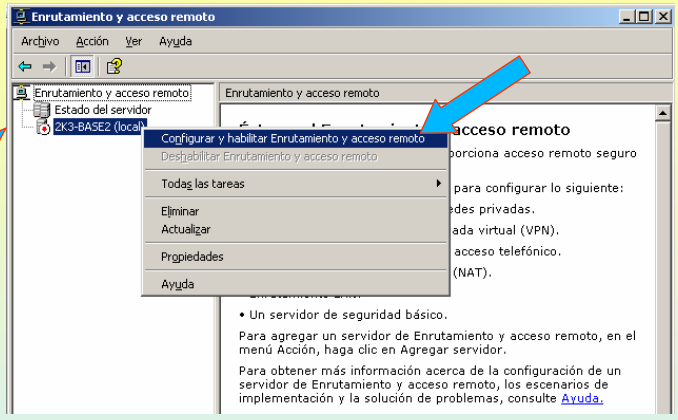
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

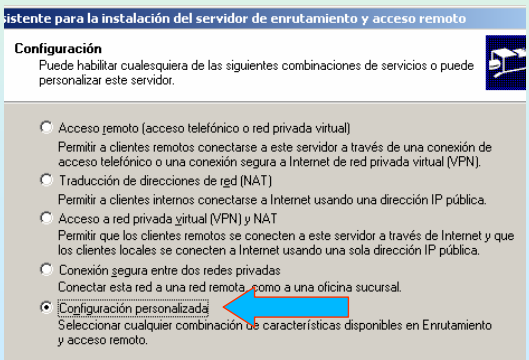
1.- ENRUTAMENTO

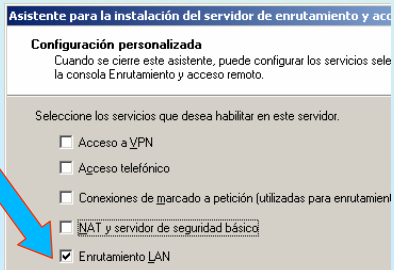
☞ CONFIGURAR ENRUTAMENTO E ACCESO REMOTO

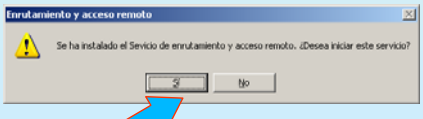
Windows 2003 instala por defecto esta ferramenta.







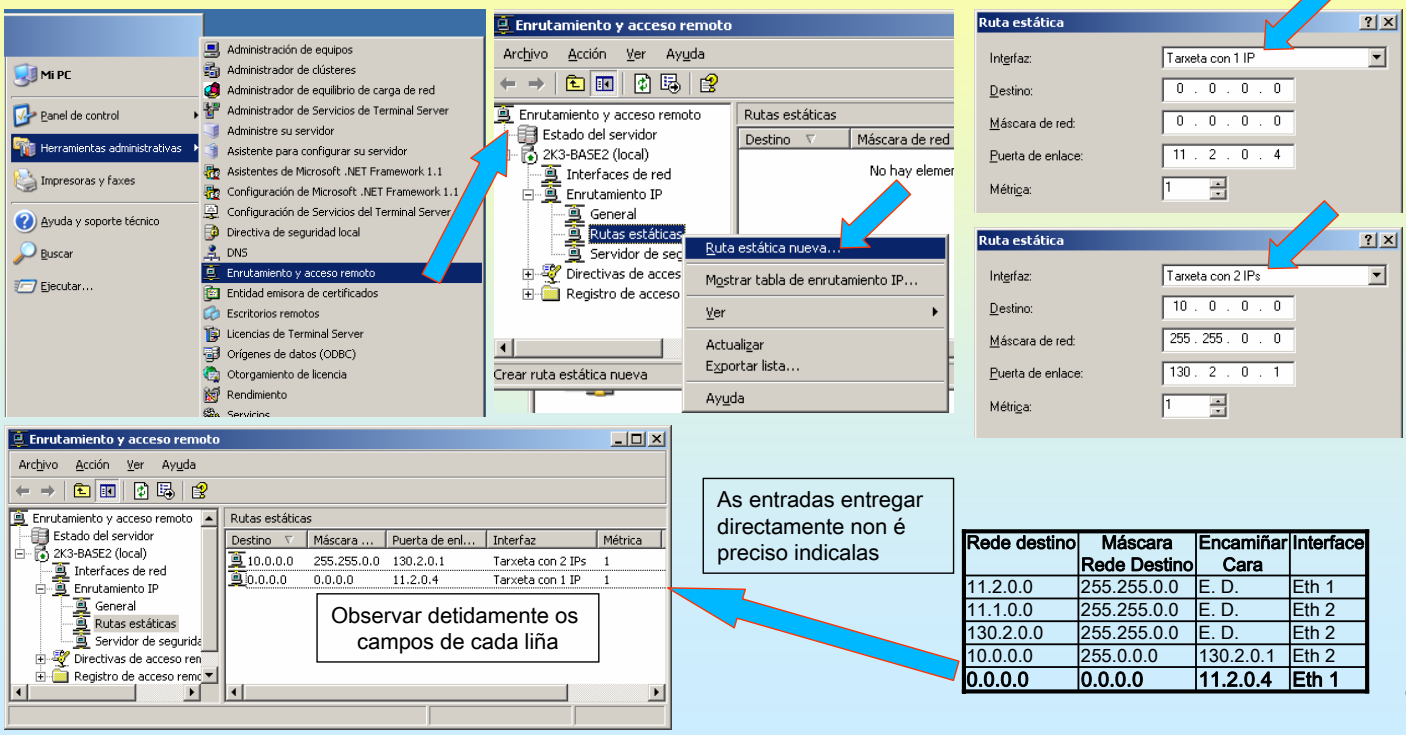




1.- ENRUTAMENTO

☞ ENGADIR A TÁBOA DE RUTEO

As entradas **ENTREGAR DIRECTAMENTE** da táboa de ruteo xa as introduce por defecto a ferramenta Enrutado e Acceso Remoto.



As entradas entregar directamente non é preciso indicalas

Rede destino	Máscara Rede Destino	Encamiñar Cara	Interface
11.2.0.0	255.255.0.0	E. D.	Eth 1
11.1.0.0	255.255.0.0	E. D.	Eth 2
130.2.0.0	255.255.0.0	E. D.	Eth 2
10.0.0.0	255.0.0.0	130.2.0.1	Eth 2
0.0.0.0	**0.0.0.0**	**11.2.0.4**	**Eth 1**

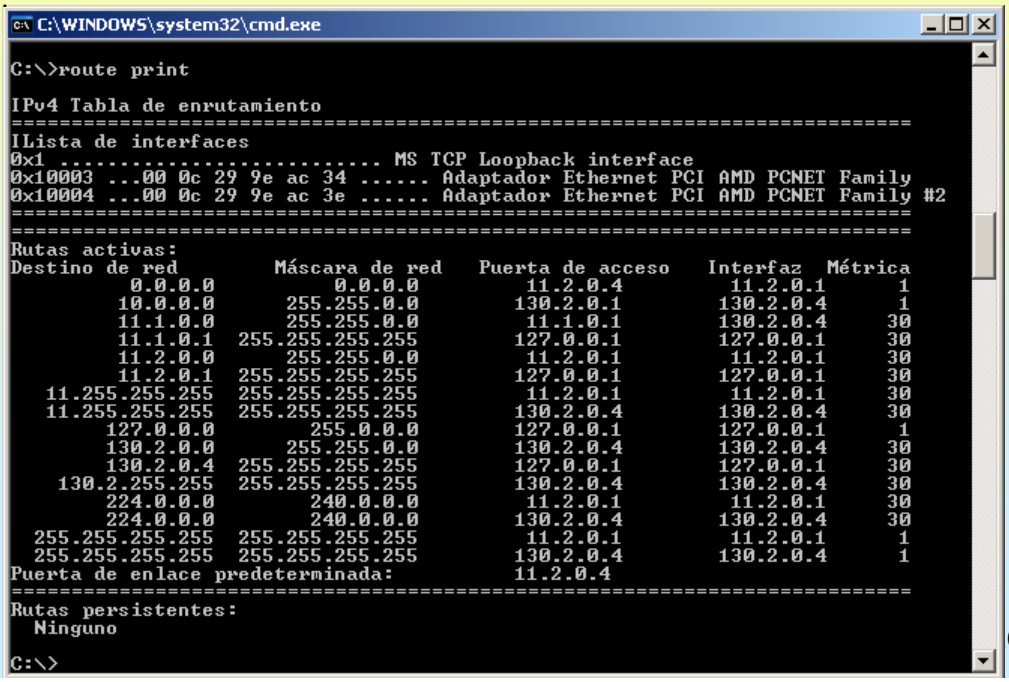
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

1.- ENRUTAMENTO

☞ TÁBOA DE ENCAMIÑAMENTO REAL

A táboa de encamiñamento real, sae de:

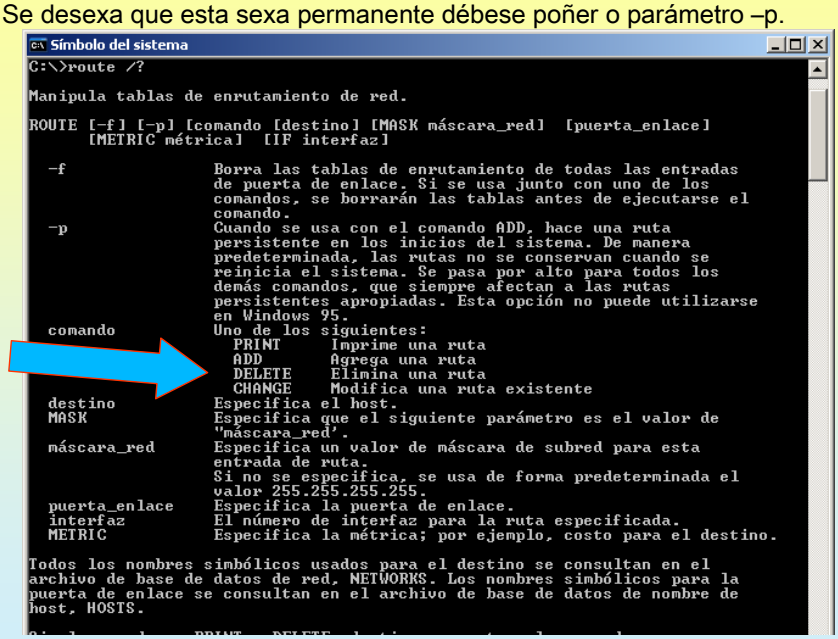
- IPS que ten cada tarxeta de rede,
- Rutas estáticas
- Multidifusión para cada rede IP
- Broadcast IPs tipo D.



1.- ENRUTAMENTO

☞ USAR O COMANDO ROUTE PARA ENGADIR/MODIFICAR/BORRAR UNHA RUTA

Se desexa que esta sexa permanente débese poñer o parámetro –p.



SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

1.- ENRUTAMENTO

☞ EXEMPLO DUN XP (I)

Nun SO cliente tipo xp, 2000 profesional tamén se pode manexar a táboa de ruteo.

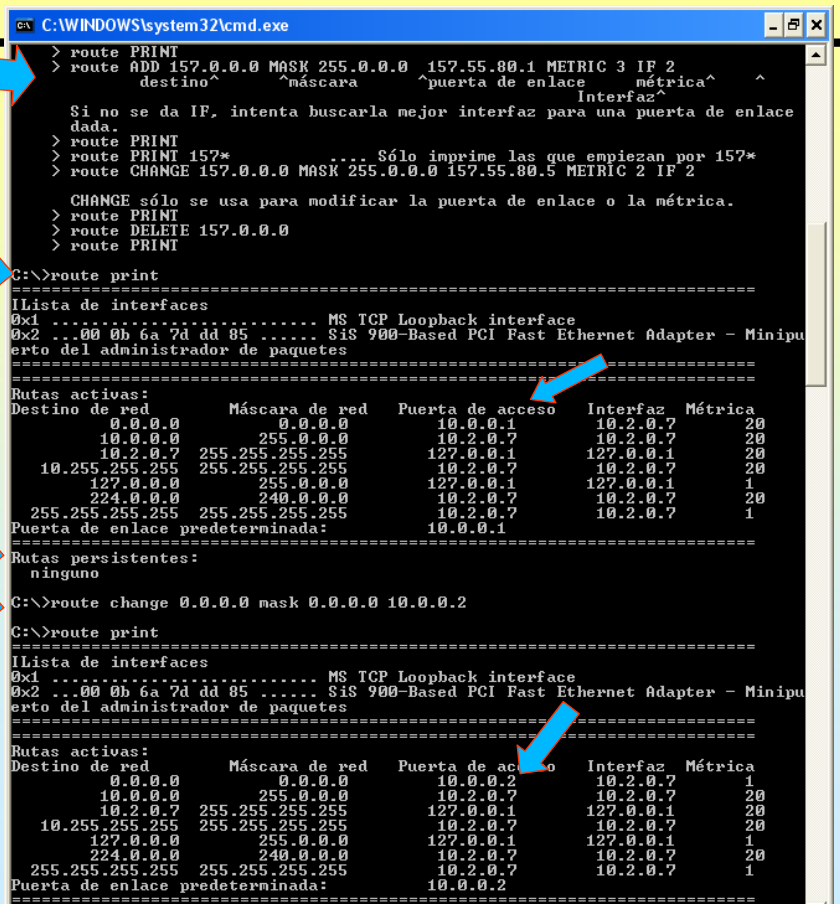
Todo equipo ten unha táboa de ruteo, no caso dos SO clientes a única forma de manexar esa táboa e co comando ROUTE

Exemplo:
A porta de enlace dun Equipo é 10.0.0.1. Interesa probar con outro router que está en probas. Este te por IP 10.0.0.2.

Entón imos cambiar a porta de enlace momentaneamente sen cambiar a configuración IP.

IMPORTANTE: se se desexa que ese cambio sexa permanente débese poñer o parámetro -p

Route –p change ....



1.- ENRUTAMENTO

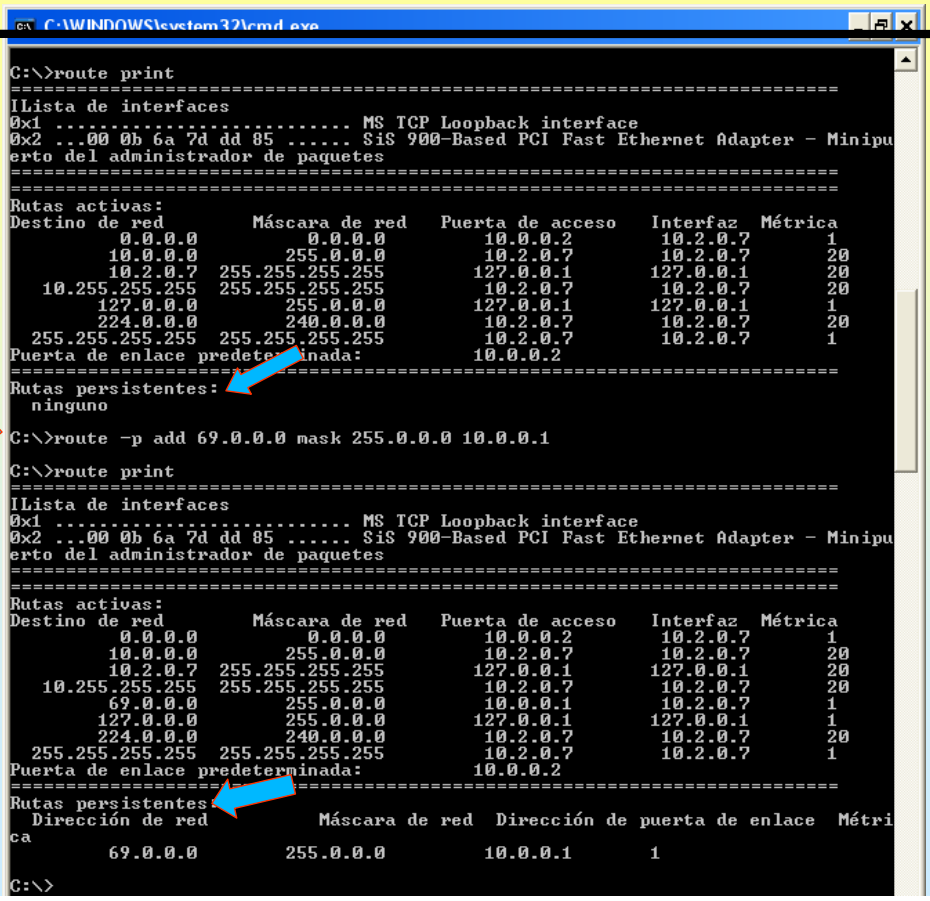
☞ EXEMPLO DUN XP (II)

Agora interesa que todo o tráfico que vaia para a rede 69.0.0.0 (da Xunta) siga saíndo polo router 10.0.0.1.

E que esta nova ruta sexa permanente.

As rutas permanentes introdúcense no rexistro de windows

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes



2.- DNS (Domain Name System)

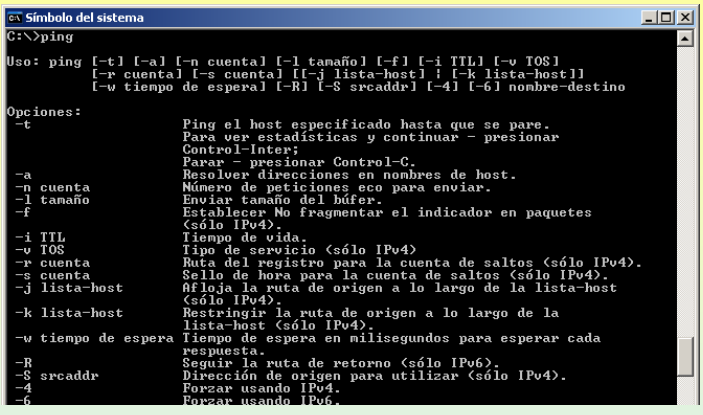
☞ PING

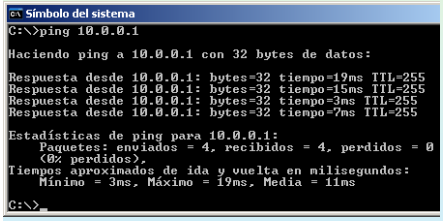
Antes de comezar co DNS imos estudiar o comando Ping.

Comando que axuda a comprobar a conectividade no nivel IP, esto é, comprobar que dous equipos se poidan conectar.

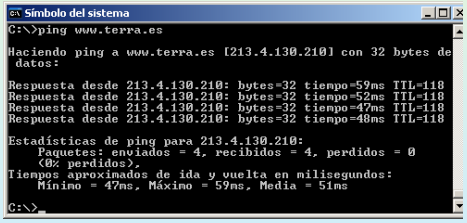
Para elo precisa coñecer a IP do destinatario.
Se se especifica un nome de dominio o ping encárgase de averiguar a IP usando o proceso de consultas DNS.

Obsérvense os seguintes exemplos:

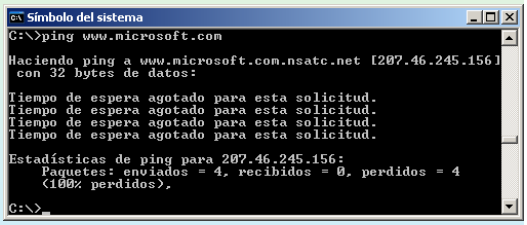




Ping a unha IP que coñecemos.
O respondernos indícanos canto tempo tarda en chegar un PKT. Deste xeito sabemos que 10.0.0.1 **is alive**



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.

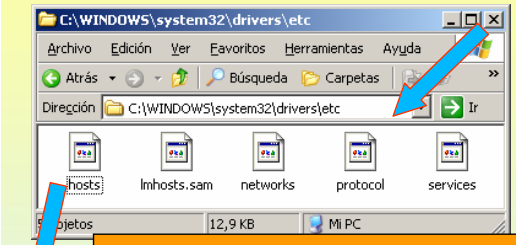


O programa averigua a IP e logo realiza o "ping". O host non responde:
A.- Pode ser que estea apagado, ou non que non se pode chegar a el.
B.- Pode estar acendido pero deshabiltada a resposta a pings.

2.- DNS (Domain Name System)

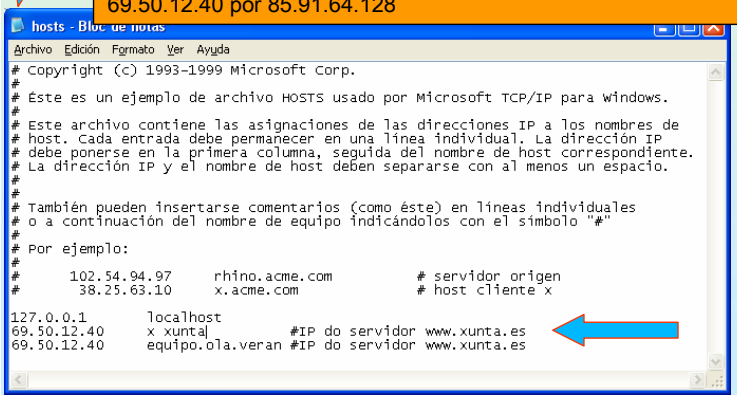
☞ ARQUIVO HOSTS

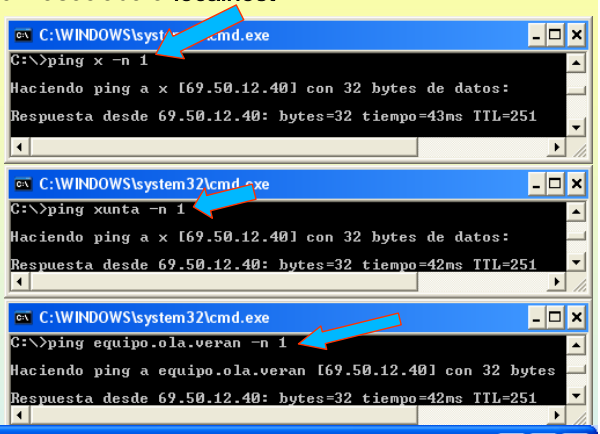
Todo cliente DNS ten un arquivo HOSTS, onde se almacena estaticamente asociacións de de nomes de equipos (con ou sen o dominio) e as súas IPs. Sempre ten a entrada de loopback 127.0.0.1 asociada a **localhost**.



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

IMPORTANTE: se se está fora da rede da Xunta substituír 69.50.12.40 por 85.91.64.128



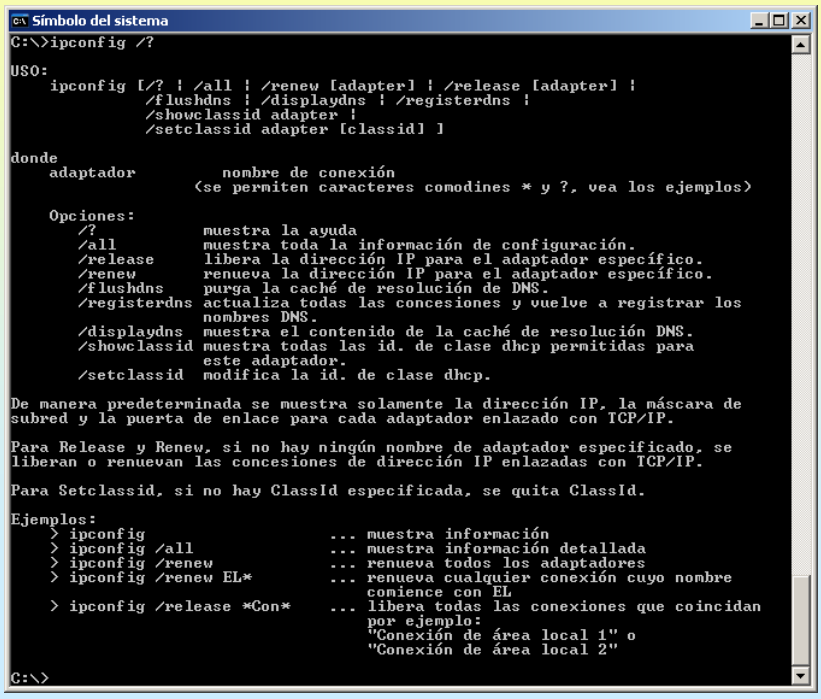


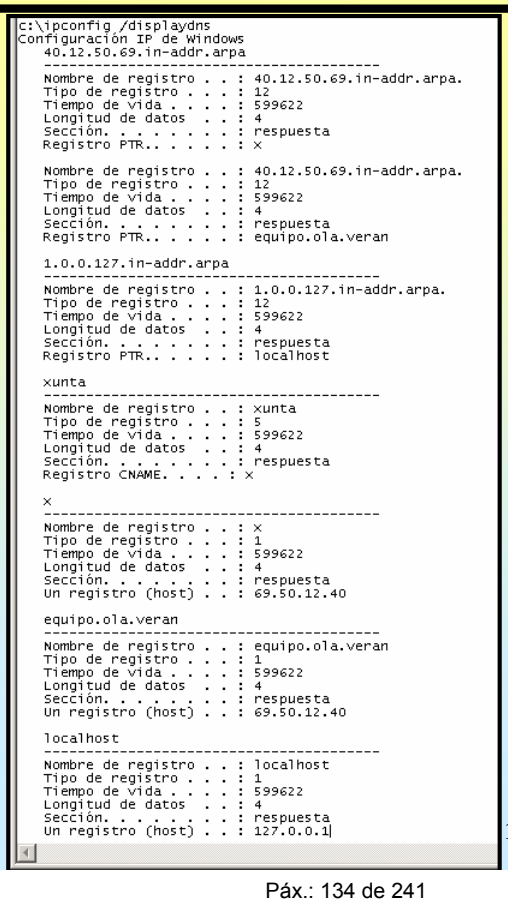
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

2.- DNS (Domain Name System)

☞ COMANDOS: IPCONFIG (WINDOWS) (I)

Mostra os valores da configuración TCP/IP e actualiza a configuración de DHCP (que se verá máis adiante) e a de DNS.
Neste caso mostra o contido do arquivo HOSTS



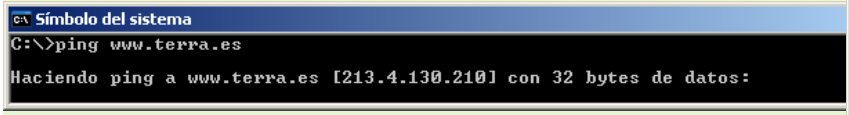


2.- DNS (Domain Name System)

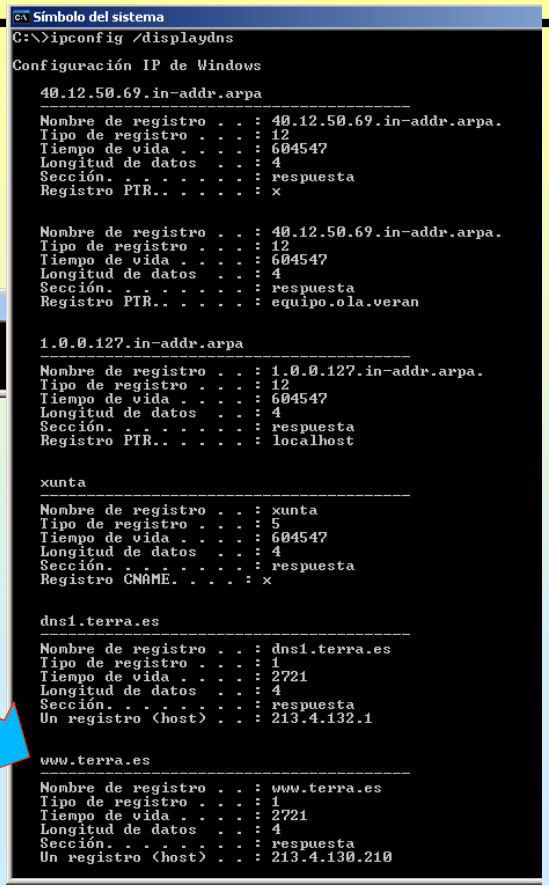
☞ COMANDOS: IPCONFIG (WINDOWS) (II)

O equipo o facer ping a **www.terra.es** por primeira vez realizase:

1º.- Consulta o caché DNS do equipo, como non atopa a entrada.
2º.- O equipo consulta ó servidor DNS que teña configurado.
3º.- Unha vez obtida a resposta do servidor DNS, esta almacénase na cache DNS, tal e como se mostra no exemplo da dereita.



Cada vez que o equipo desexe achar a IP de **www.terra.es** xa non precisa consultar ó servidor DNS, pois mentres non se baleire a caché DNS xa está aí a entrada.



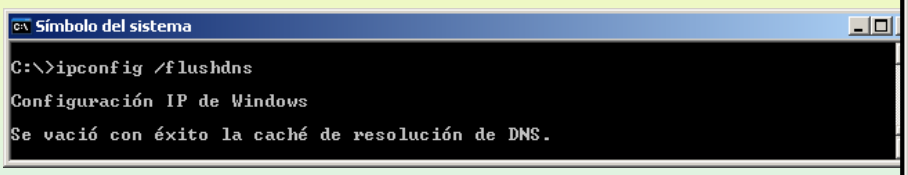
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

2.- DNS (Domain Name System)

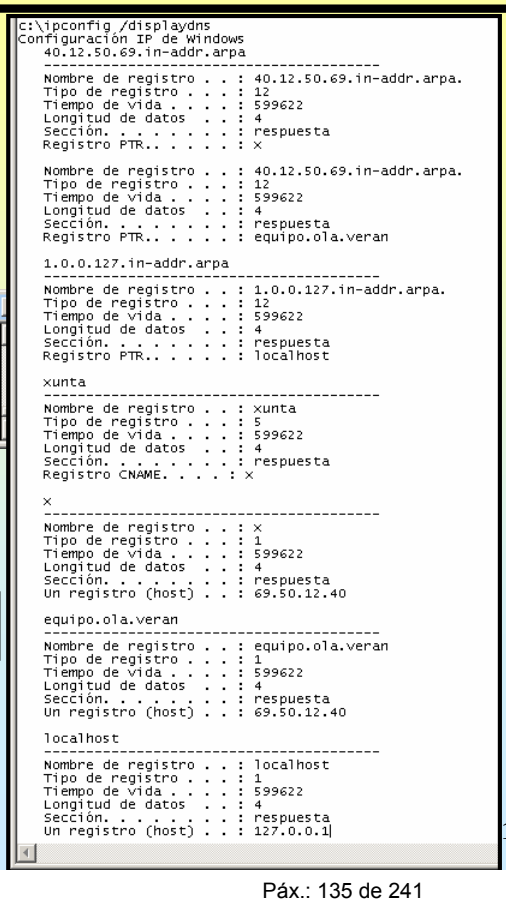
☞ COMANDOS: IPCONFIG (WINDOWS) (III)

O parámetro que permite baleirar a Caché DNS é **ipconfig /flushdns**.

Ollo non se eliminarán os datos procedentes do arquivo de HOSTS, só se eliminarán os procedentes de realizar consultas de DNS previas.



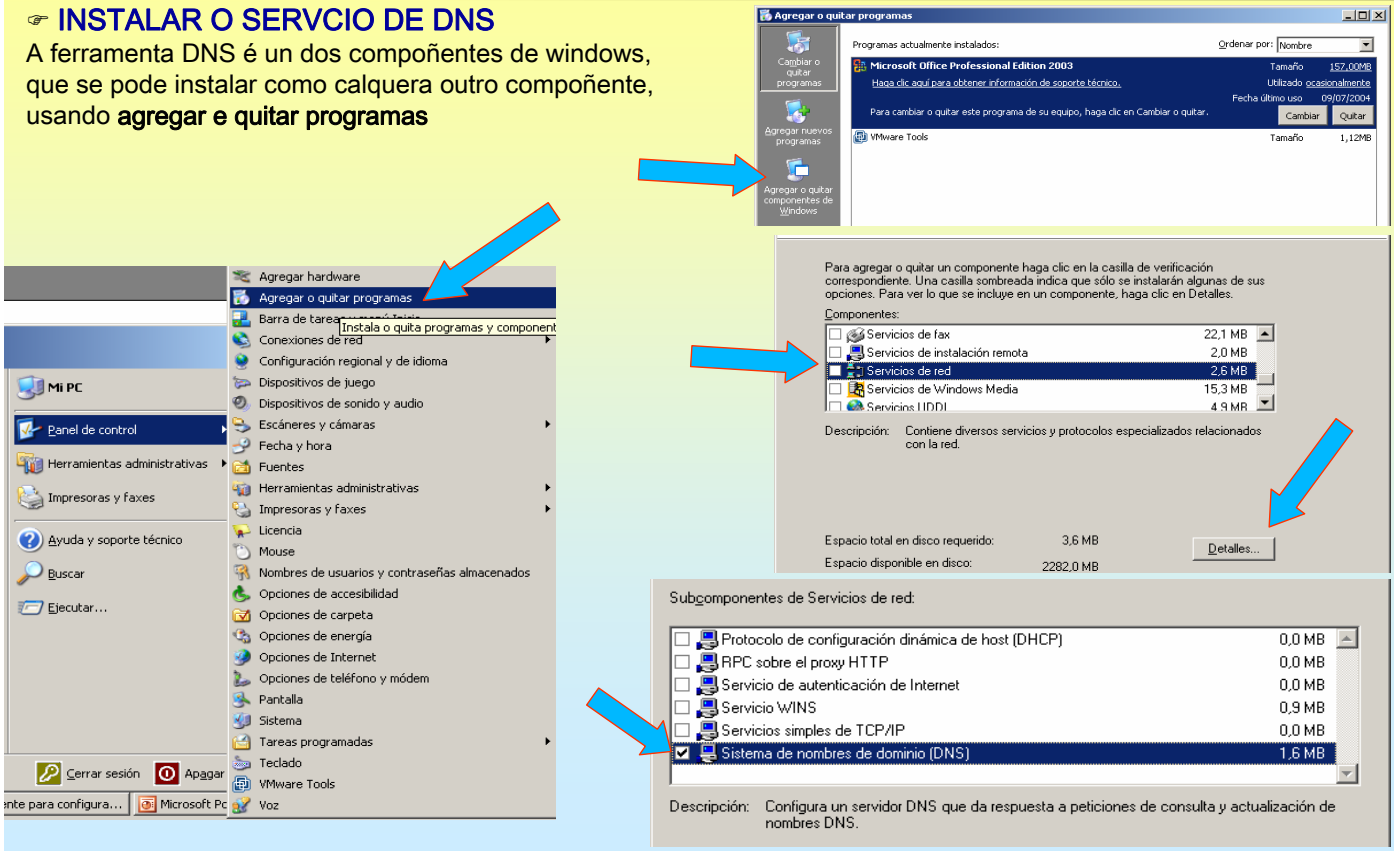
Agora a caché DNS só ten a información do arquivo de HOSTS



2.- DNS (Domain Name System)

☞ INSTALAR O SERVCIO DE DNS

A ferramenta DNS é un dos compoñentes de windows, que se pode instalar como calquera outro compoñente, usando **agregar e quitar programas**

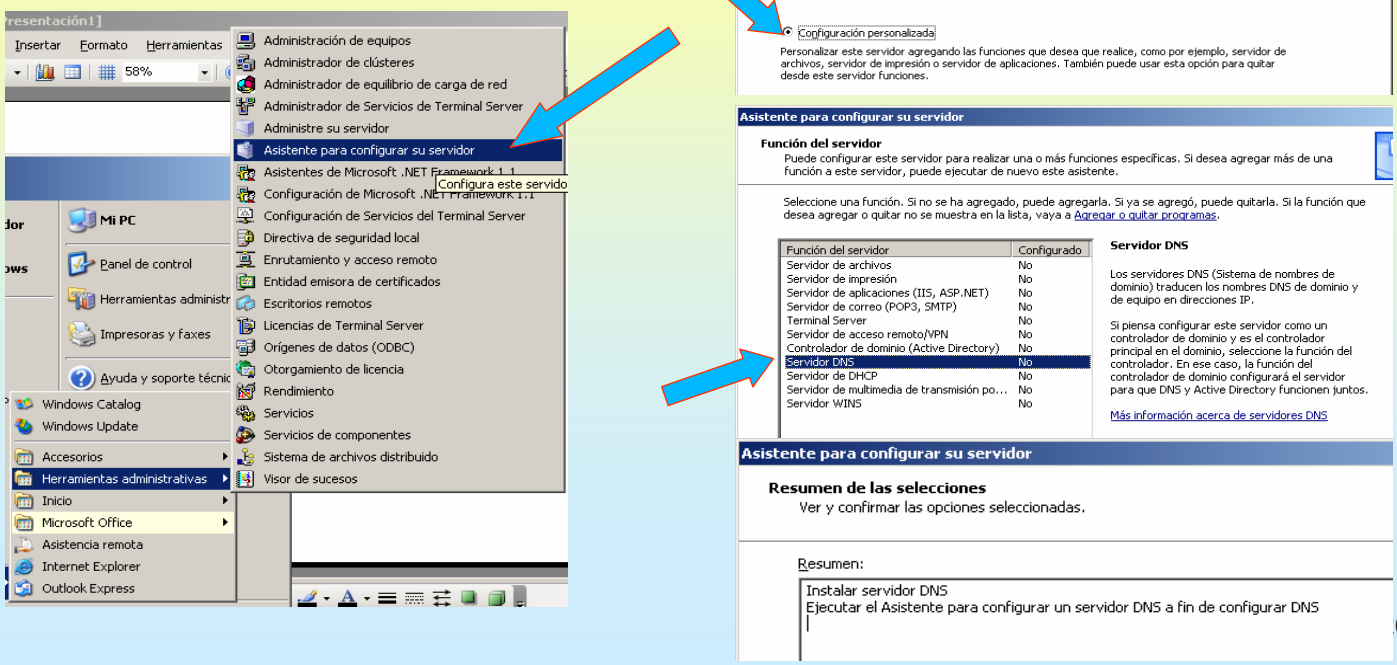


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

2.- DNS (Domain Name System)

☞ INSTALAR USANDO O ASISTENTE

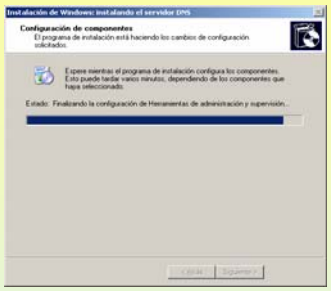
Neste caso usarase o asistente.

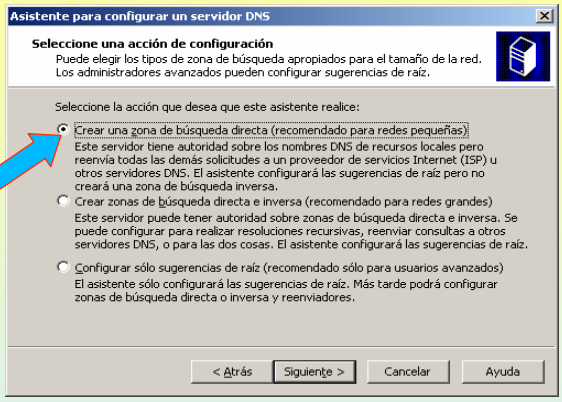


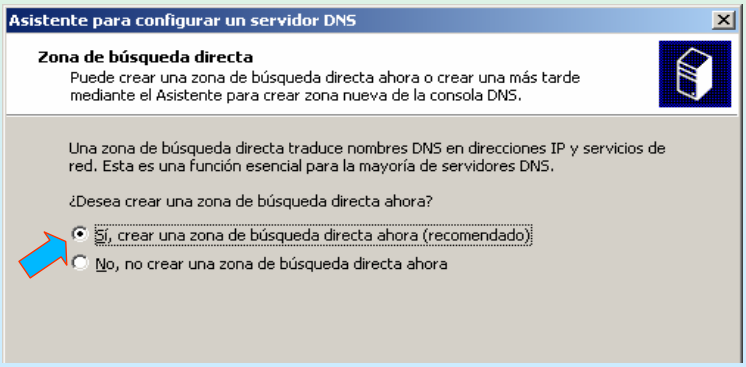
2.- DNS (Domain Name System)

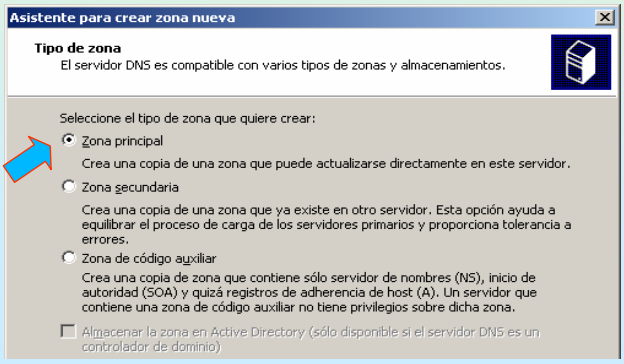
☞ CONFIGURAR USANDO O ASISTENTE

Crearanse a **Zoa de busca directa PRINCIPAL** (“onde se crearan as asociacións nome – ip”).







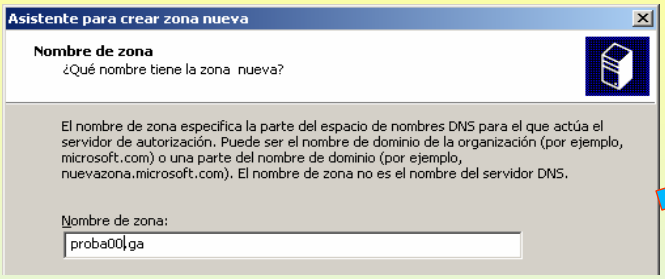


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

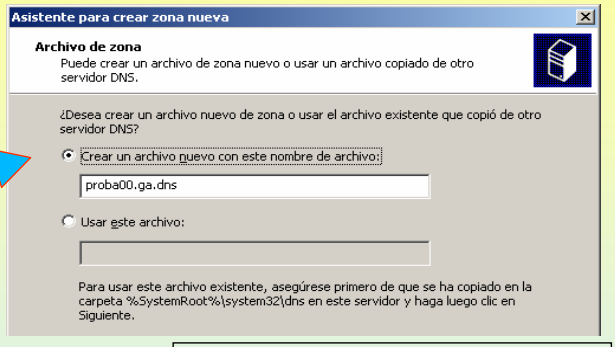
2.- DNS (Domain Name System)

☞ CONFIGURAR USANDO O ASISTENTE (II)

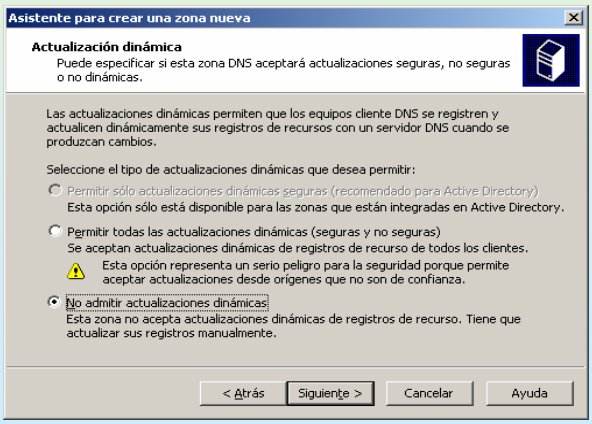
Crearanse a **Zoa de busca directa PRINCIPAL** (“onde se crearan as asociacións nome – ip”).



Indícase o nome da Zoa que vai xestionar



Indícase o nome do arquivo no que se van gardar tódolos datos da Zoa



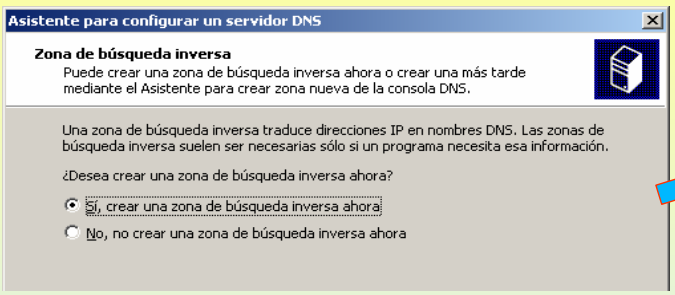
Actualizacións non dinámicas: as asociacións nome – ip débense introducir manualmente.

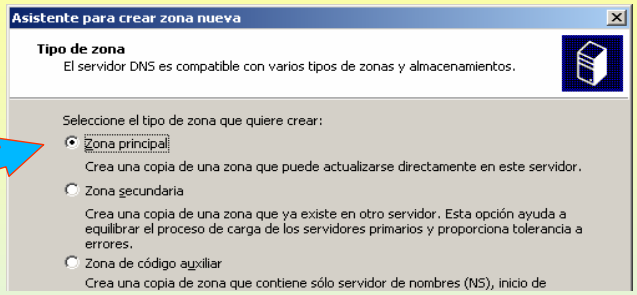
Actualizacións Dinámicas (DDNS): as asociacións nome – ip introdúceas automaticamente o ordenador cliente

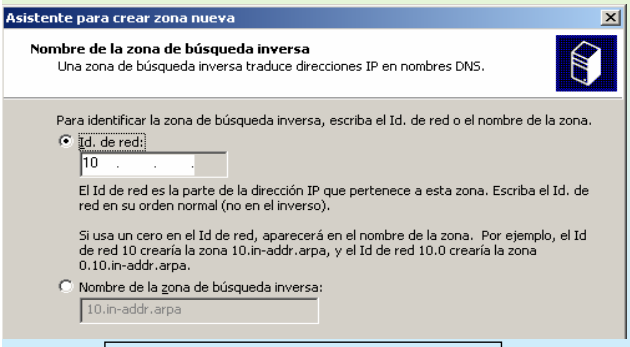
2.- DNS (Domain Name System)

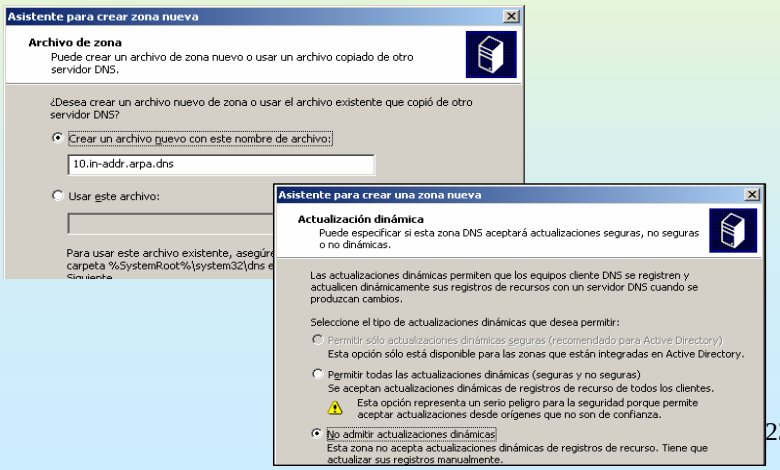
☞ CONFIGURAR USANDO O ASISTENTE (III)

Crearanse a **Zoa de busca INVERSA PRINCIPAL** ("onde se crearan as asociacións, **OLLO**, **IP – NOME**").









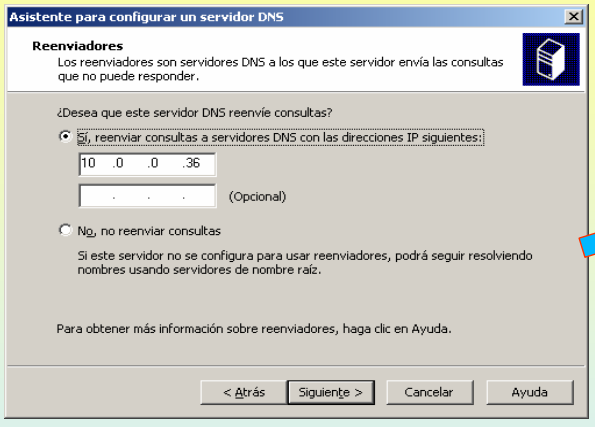
Débese introducir o **IDENTIFICADOR DE REDE** neste caso traballaráse cunha rede Tipo A (10.0.0.0)

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

2.- DNS (Domain Name System)

☞ CONFIGURAR USANDO O ASISTENTE (IV)

Configurar os **REEENVIADORES** e as **SUXERENCIAS RAÍZ.**



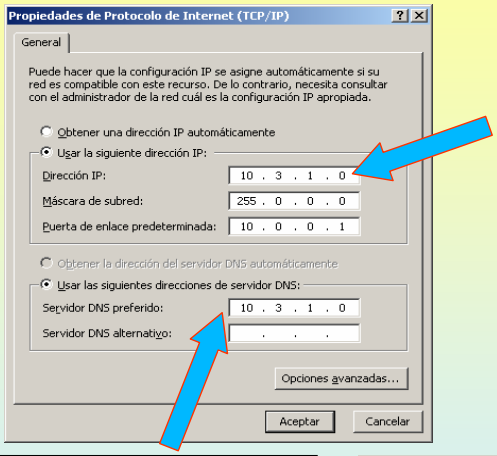
Débense especificar as IPs dos servidores DNS os que se preguntará no caso de non ter información sobre o nome-dominio preguntado a este servidor de DNS

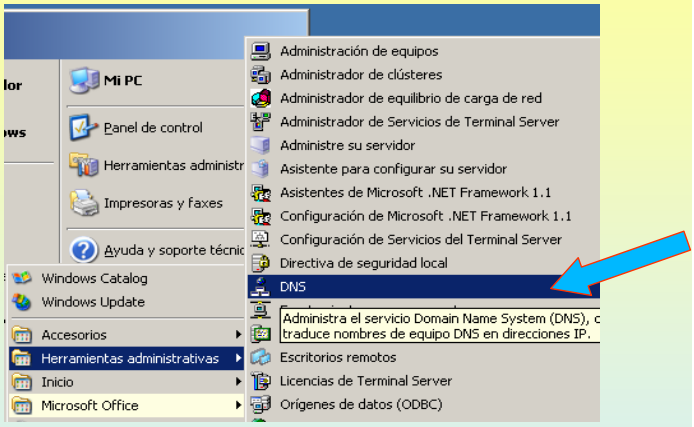
As **suxerencias raíz** configúranse automaticamente, se sae esta mensaxe é porque non hai conexión a Internet.

2.- DNS (Domain Name System)

☞ CONFIGURAR O CLIENTE DNS E O SERVIDOR DNS

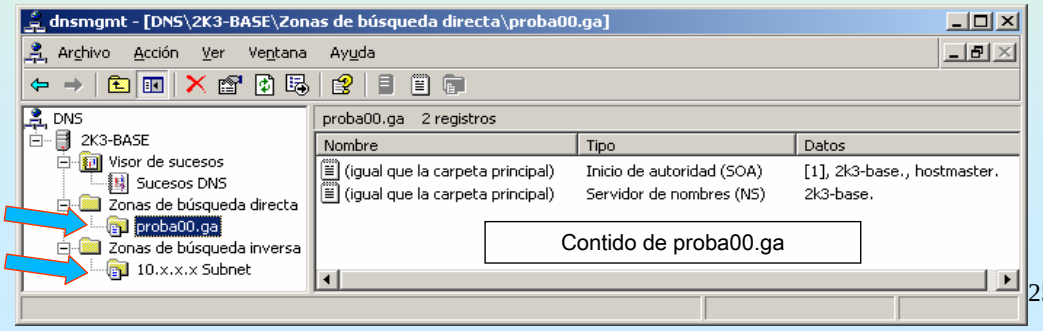
Ollo pois este servidor DNS segue sendo un cliente DNS que ten que preguntar a alguén para poder resolver.





Configuración CLIENTE.

Como cliente debe preguntar a algún servidor DNS.
Neste caso pregúntase a se mesmo, pois el é un servidor DNS

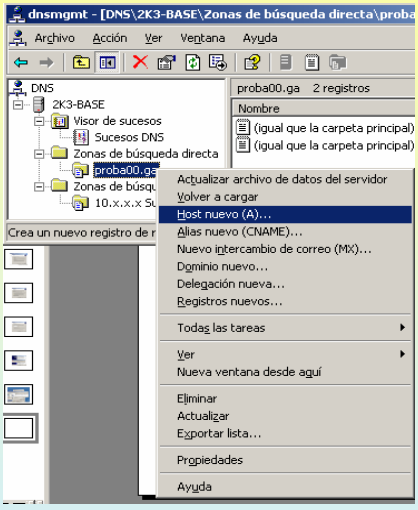


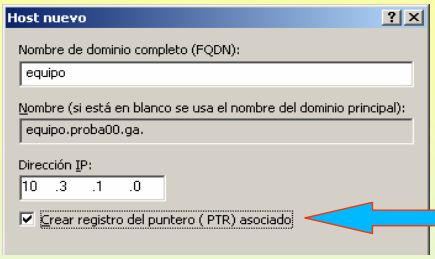
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

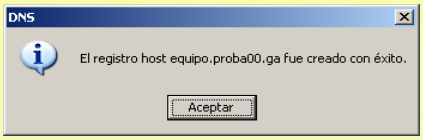
2.- DNS (Domain Name System)

☞ AGREGAR UNHA ENTRADA AS DÚAS ZOAS (DIRECTA E INVERSA)

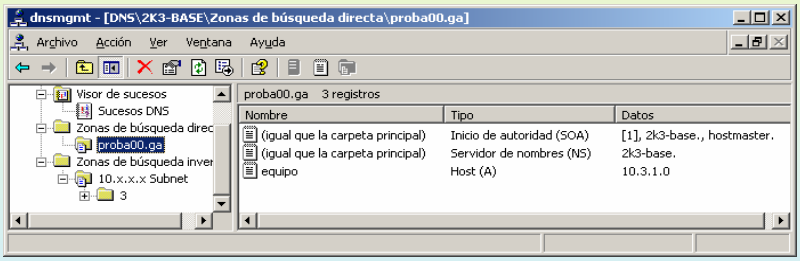
Especificar nome e IP do ordenador. Neste caso un nome distinto para a mesma IP do servidor

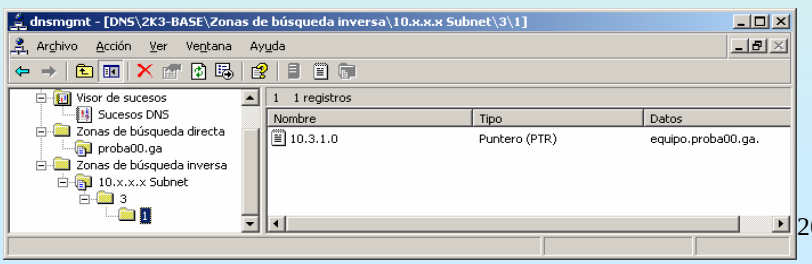






Agrega automaticamente na Zoa de Busca Inversa

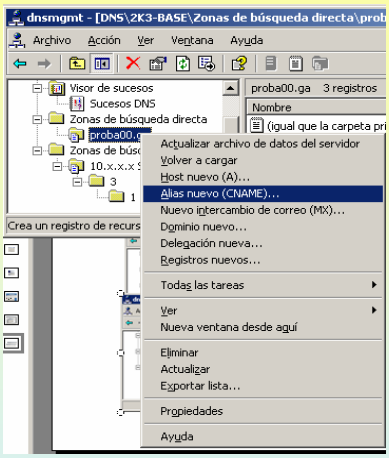


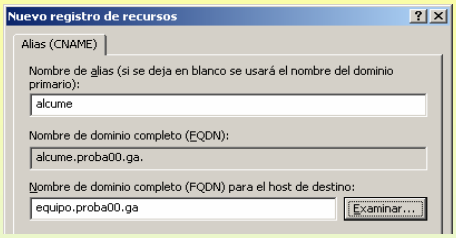


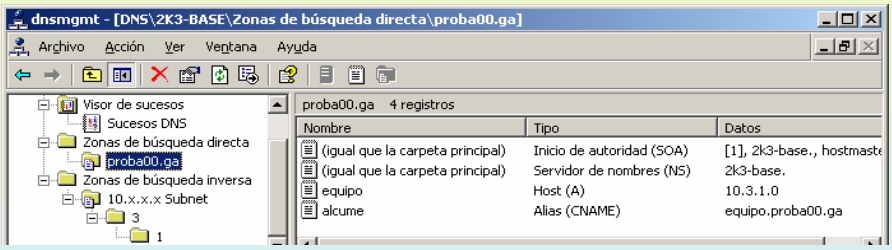
2.- DNS (Domain Name System)

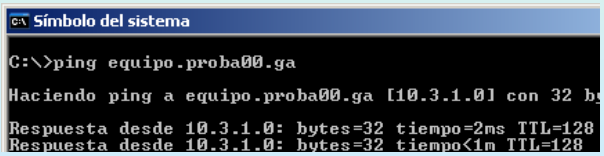
☞ **CREAR UN ALIAS. Comprobar que o servidor DNS resolve.**

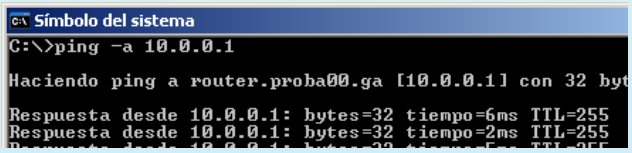
Vaise crear un alias par equipo.proba00.ga

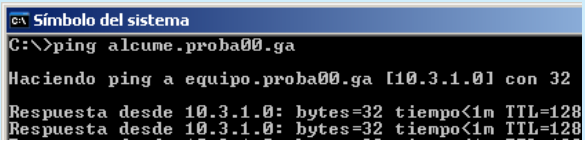










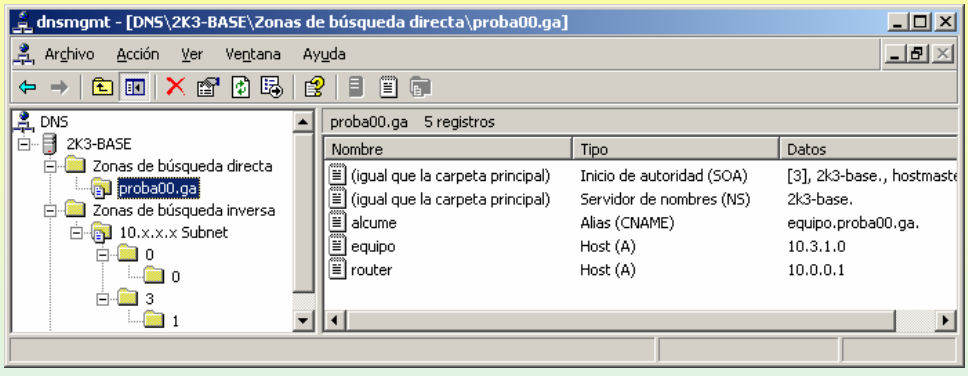


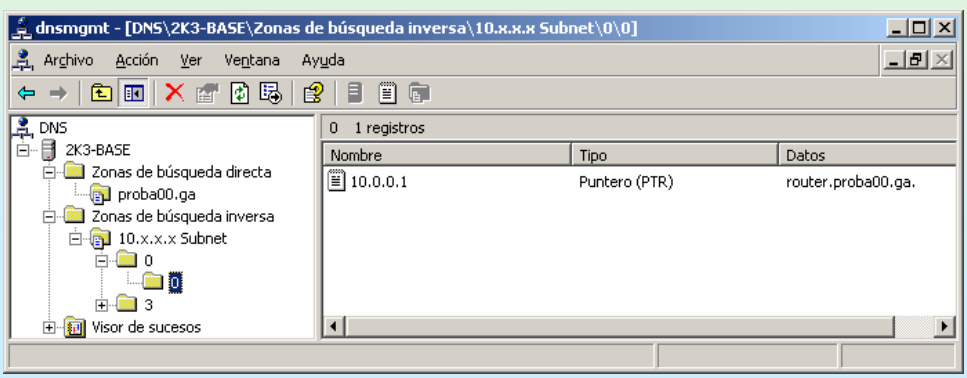
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

2.- DNS (Domain Name System)

☞ **CREAR OUTRA ENTRADA.**

Neste caso créase a IP do router do IES. Observar a zoa de busca inversa.

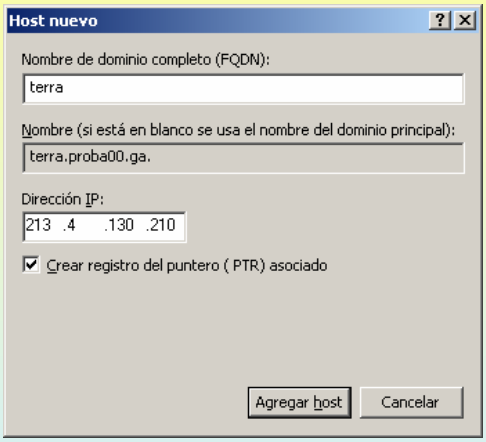


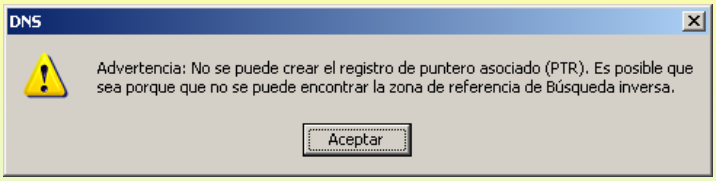


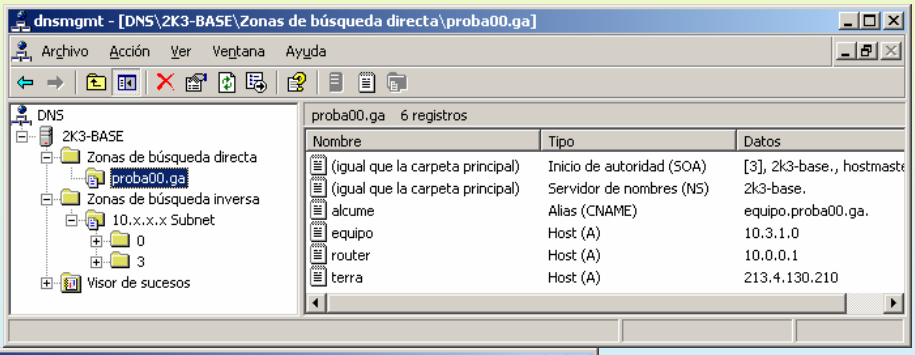
2.- DNS (Domain Name System)

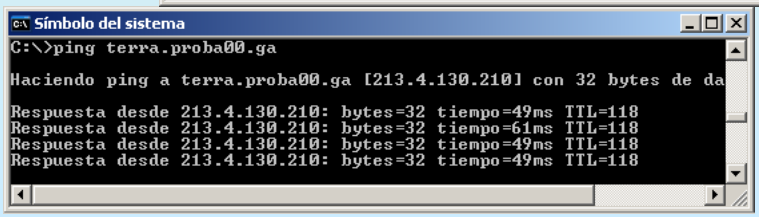
☞ CREAR OUTRA ENTRADA (II).

Neste caso á IP de **www.terra.es**. Observar como non pode crear a entrada na zoa de busca inversa. Pois non existe ningunha zoa na que poder introducir esa IP





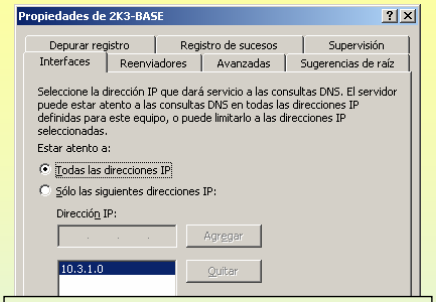




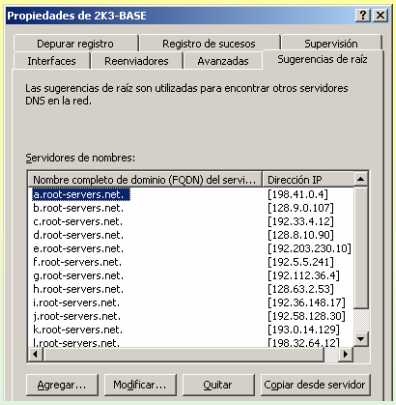
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

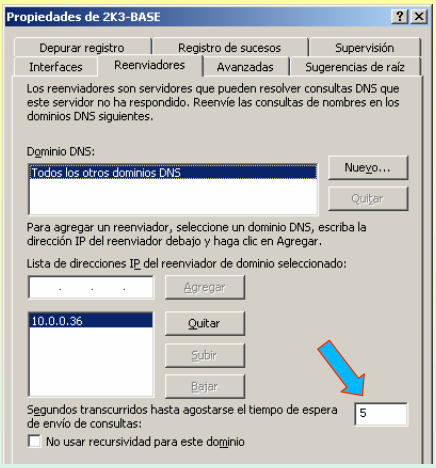
2.- DNS (Domain Name System)

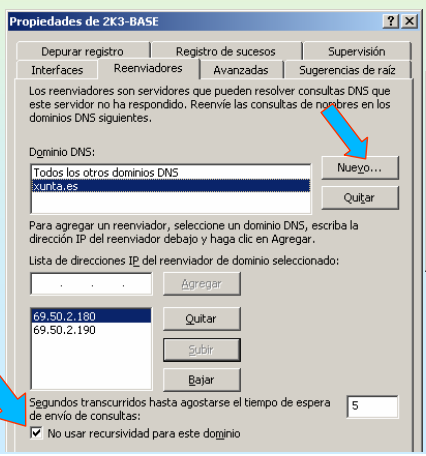
☞ PROPIEDADES DO SERVIDOR DNS.

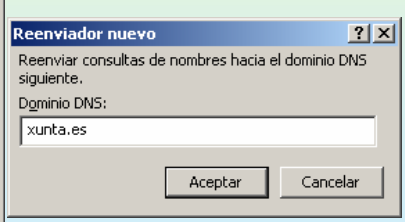


Se o servidor ten varias IPs, ¿por cal/cales delas vai atender as peticións?









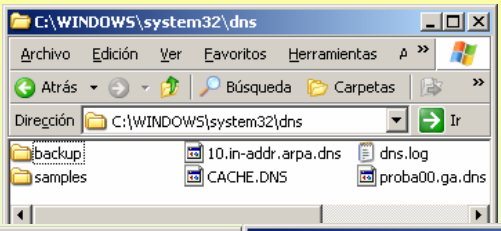
Reenviador:
Este é para todo dominio e dálle 5 segundos para que lle reposte.
No caso de non resposta no tempo establecido usará recursividade

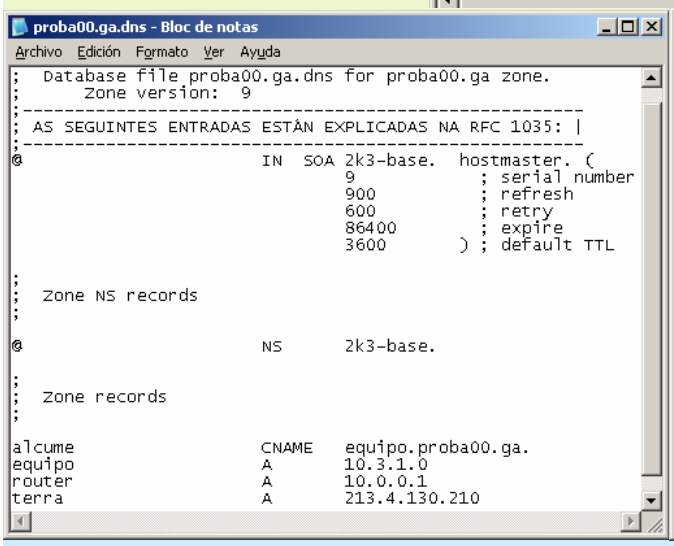
Reenviador condicional,
Neste caso para o dominio **xunta.es** pregúntaselle a outros servidores DNS es se estes fallan non se usará **recursividade**.

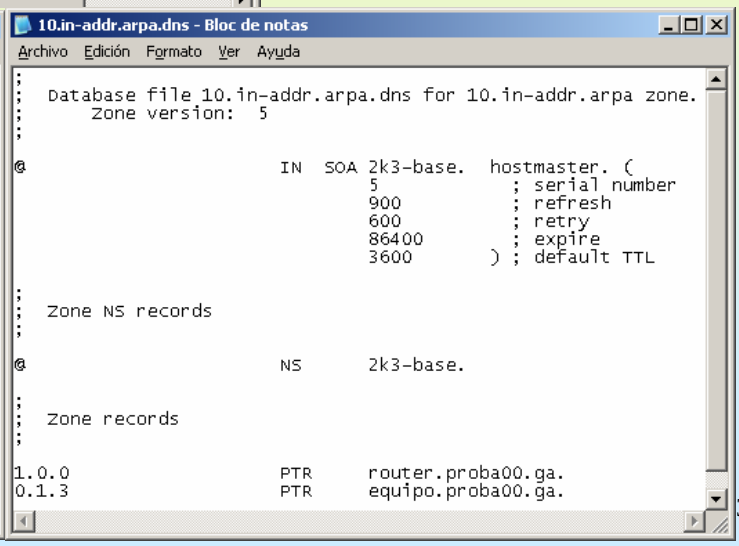
2.- DNS (Domain Name System)

☞ ARQUIVOS ONDE SE ALMACENA AS ZOAS

En ..\windows\system32\dns existe un arquivo por cada zoa creada. O significado das entradas e as especificación do formato destes están en RFC 1035.





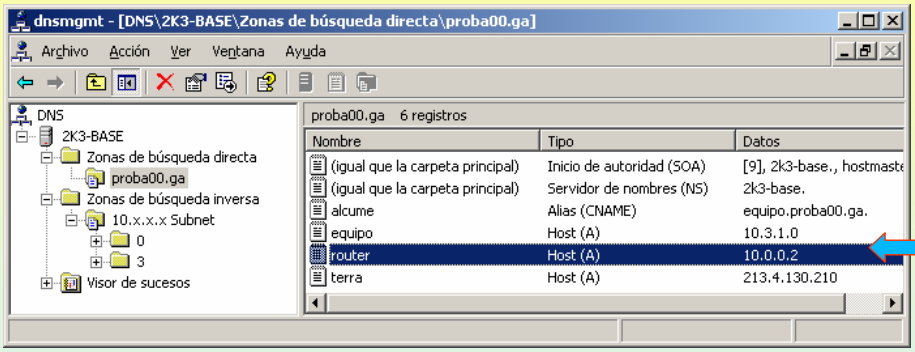


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

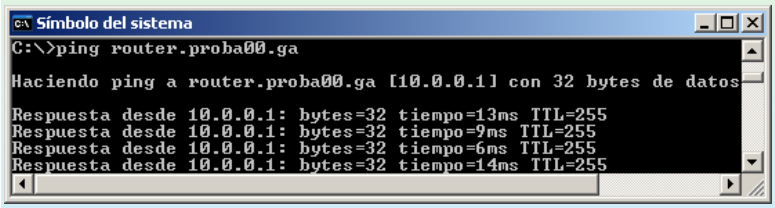
2.- DNS (Domain Name System)

☞ MODIFICAR A IP DUN ORDENADOR - BORRADO DA CAHÉ CLIENTE

Ó modificar a IP dun host débese borrar a caché DNS cliente pois se este fixo unha resolución de nome anterior ó cambio terá almacenada a Ip antiga.

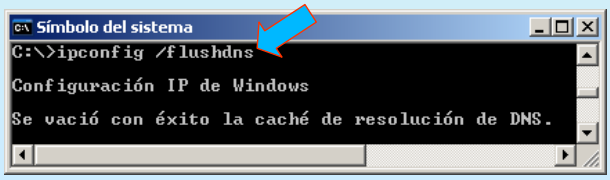


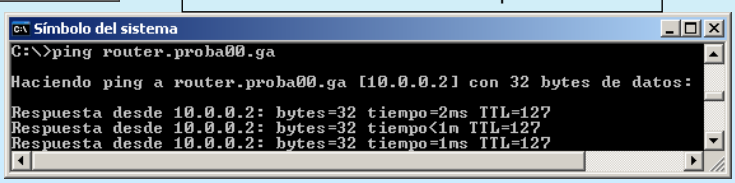
Cambiar a IP do host router a 10.0.0.2



O cliente ten almacenada na súa caché local a IP atiga dunha anterior resolucción.

Borrar caché cliente e volver a probar

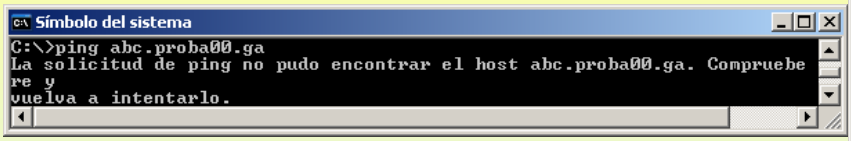




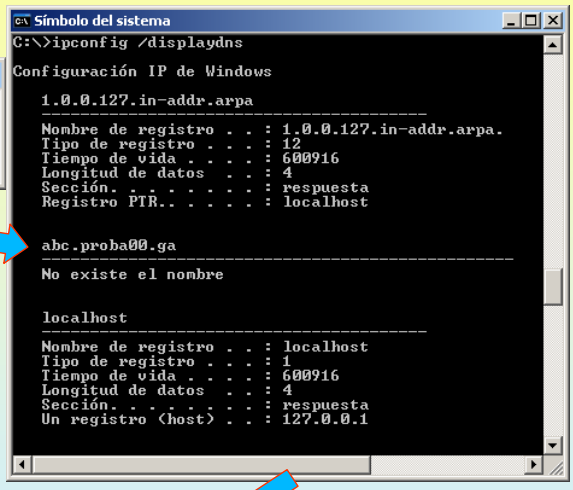
2.- DNS (Domain Name System)

☞ RESOLVER UN NOME QUE NON EXISTE E LOGO DALO DE ALTA NO DNS.

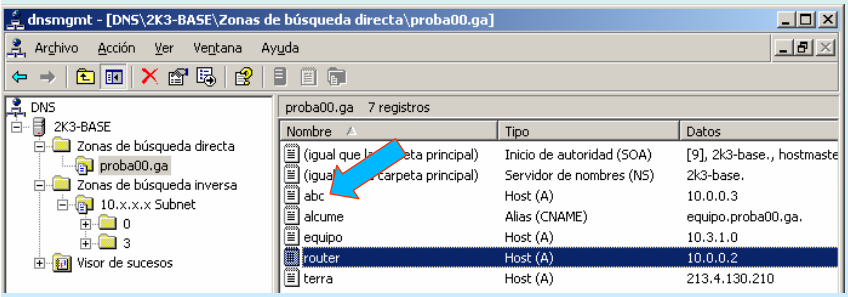
Parecido ó caso anterior, so que nesta ocasión o cliente DNS almacena na caché que o o host non existe. Se despois se da de alta hai que esperar a resetear a tarxeta, resetar o cliente o volver a baleirar a caché.

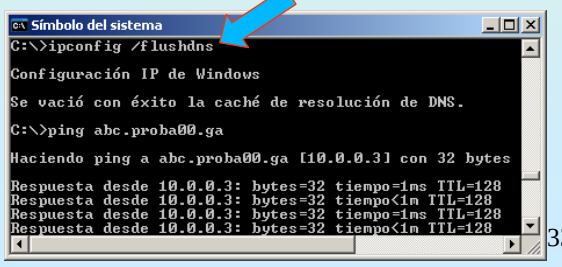


Realízase un ping a un nome que non existe. O cliente almacena esa resolución na caché.



Agora dáse de alta na Zoa correspondente. É preciso baleirar a caché do cliente.





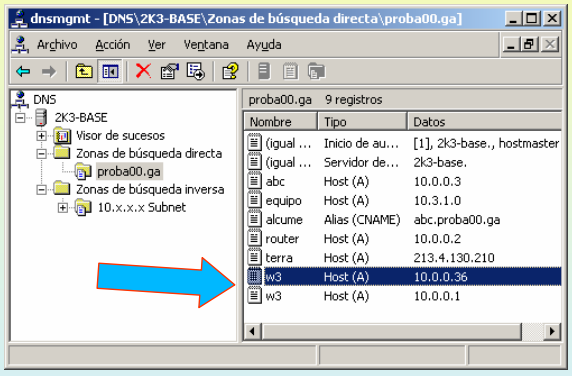
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

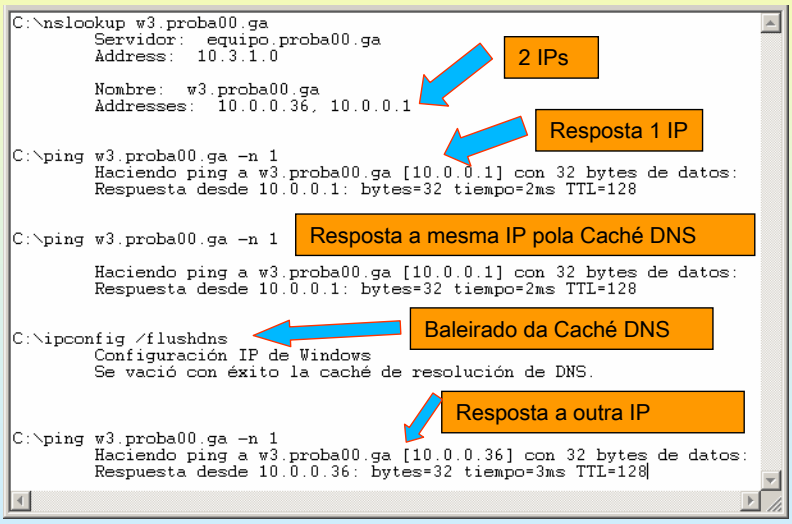
2.- DNS (Domain Name System)

☞ ASIGNAR VARIAS IPs A UN MESMO NOME DE DOMINIO.

Neste caso, supoñer que se desexa que dous ordenadores distintos (e con IPs distintas, obviamente) dean servizo da mesma aplicación servidor (web, ftp ou a que sexa). Interesa que o servidor DNS envíe as peticións dos clientes alternando entre un host e o outro.

O proceso consiste en dar de alta no servidor DNS 2 entradas co mesmo nome e coas IPs dos hosts servidores.

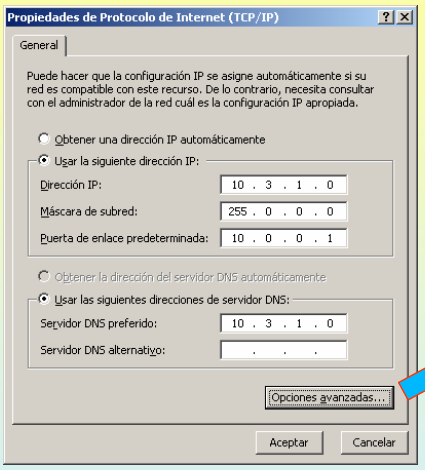




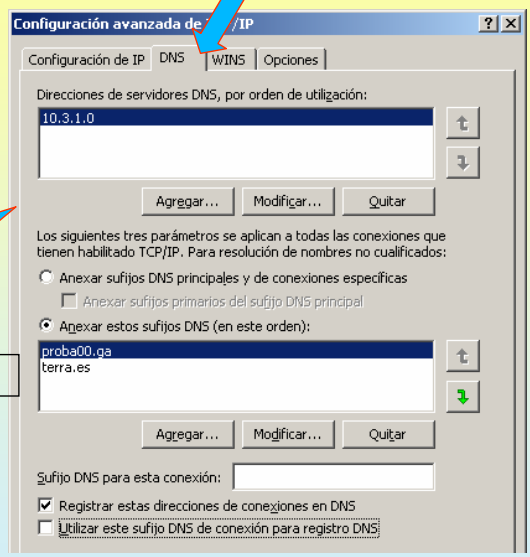
2.- DNS (Domain Name System)

☞ ANEXO DE SUFIXOS DNS

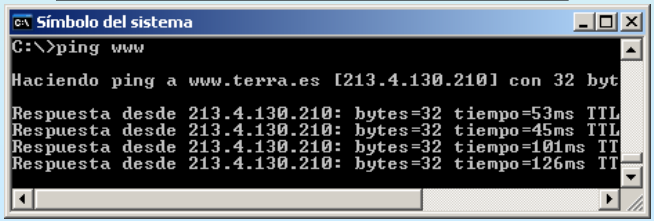
Os clientes DNS pódense configurar para que engadan un sufixo DNS automaticamente a un nome de equipo.

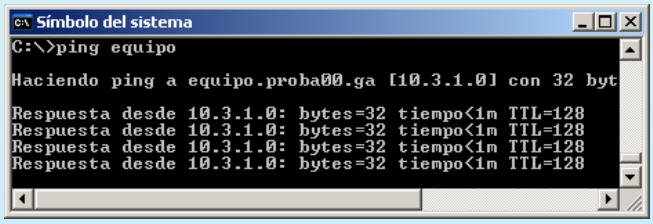


Engádense 2 sufixos



Trata de sesolver **www.proba00.ga**, se falla tratará de resolver **www.terra.es**, este é o caso.



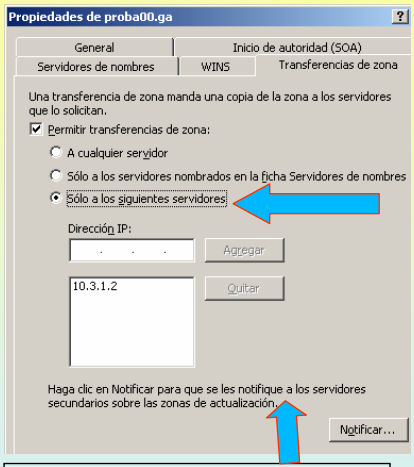


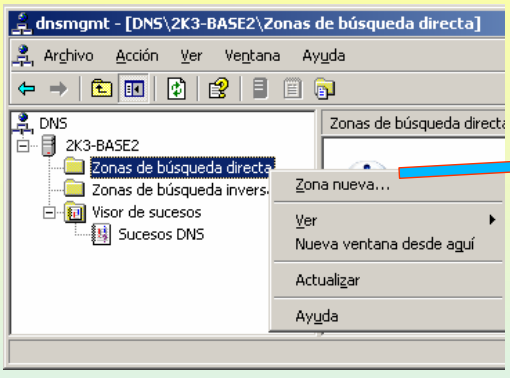
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

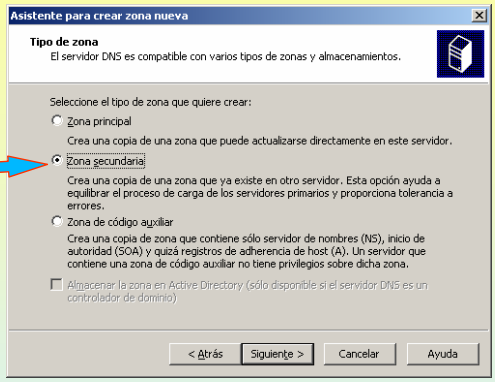
2.- DNS (Domain Name System)

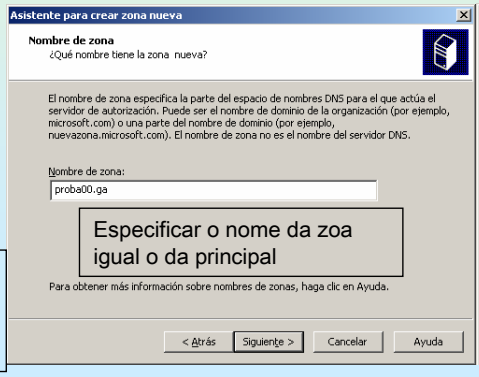
☞ CREAR ZOA SECUNDARIA

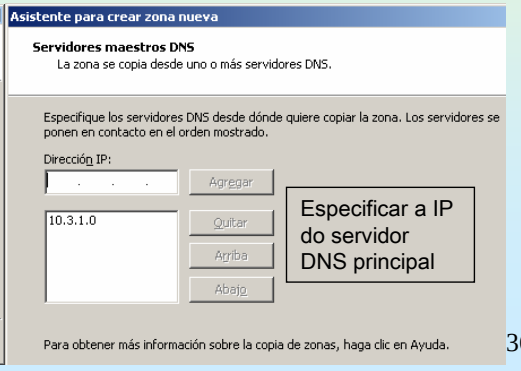
Vaise realizar un copia da zoa principal proba00.ga noutro ordenador (10.3.1.2).











Nas propiedades da zoa proba00.ga habilitase a IP do host que pode realizar unha **transferencia de zoa** para crear unha zoa secundaria

Especificar o nome da zoa igual o da principal

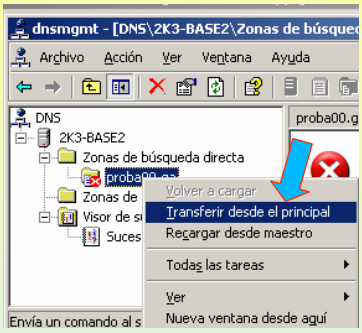
Especificar a IP do servidor DNS principal

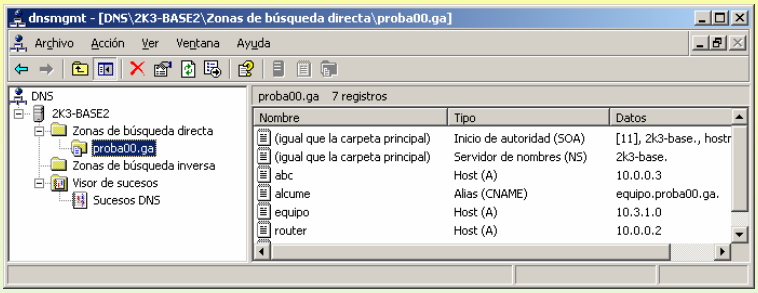
O resto das accións (imaxes) lévanse a cabo no host 10.3.1.2, onde se vai crear a zoa secundariaecundaria

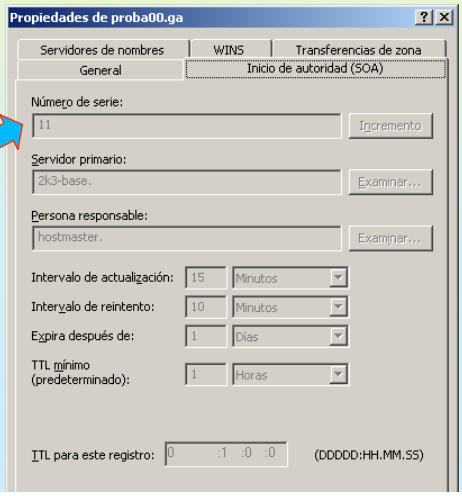
2.- DNS (Domain Name System)

☞ CREAR ZOA SECUNDARIA – TRANSFERIR DENDE PRINCIPAL

Cada zoa (principal e secundaria) mantén un número de serie. Este serve para saber cando hai que transferir dende pral.

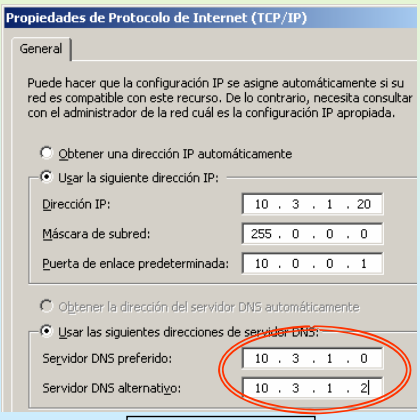






Número de serie da secundaria.
Se é inferior o número de serie da principal realiza unha transferencia de zoa.

Nunha zoa secundaria non se poden dar nada de alta.



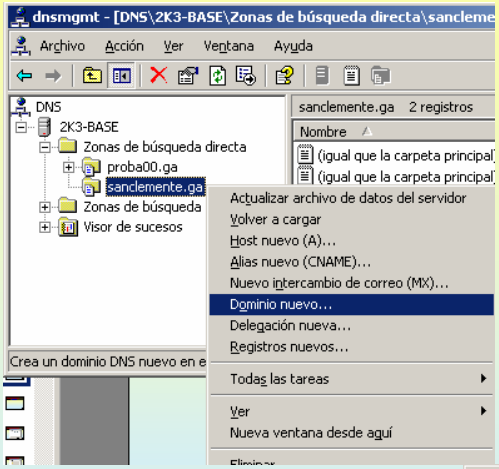
Configuración dun cliente DNS

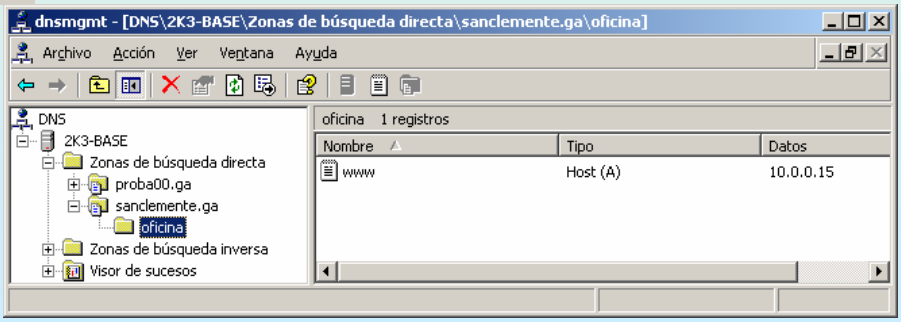
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

2.- DNS (Domain Name System)

☞ CREAR UN SUBDOMINIO

Crear un subdominio e logo engadirlle un host é semellante ós pasos vistos anteriormente



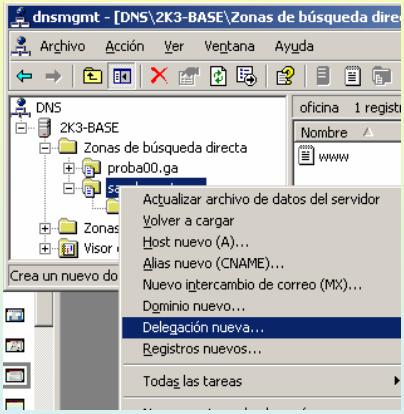


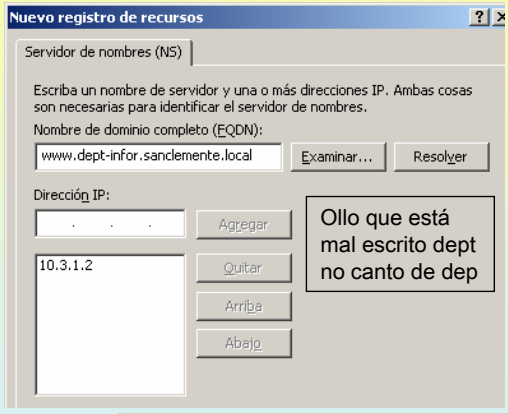
2.- DNS (Domain Name System)

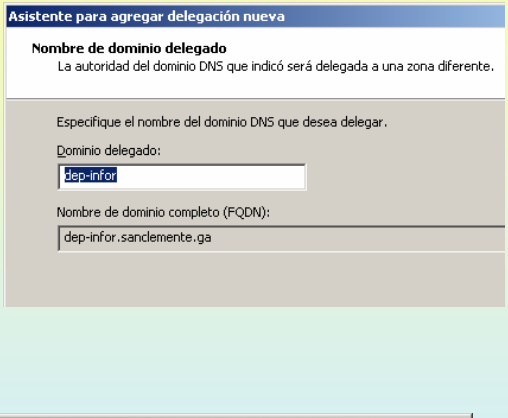
☞ CREAR UNHA DELEGACIÓN DE ZOA

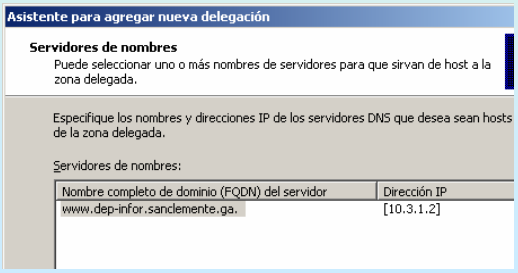
É semellante a creación dun subdominio, so que a xestion dese subdominio delégase a outro server.É en este onde se deben dar de alta as entradas.Crearáse no host 10.3.1.0 unha zoa delegada dep-infor.sanclemente.local no host 10.3.1.2

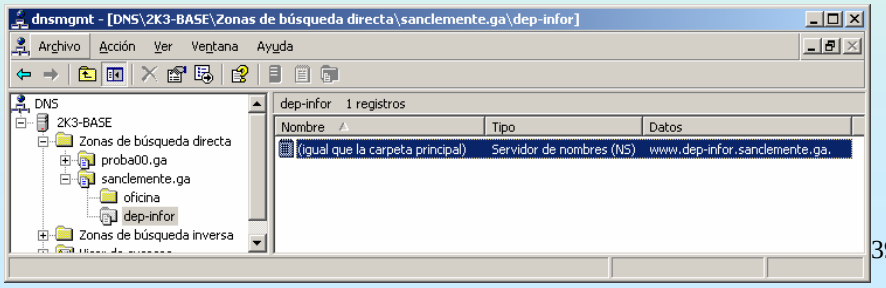
Actividades a realizar no host "**delegador"**







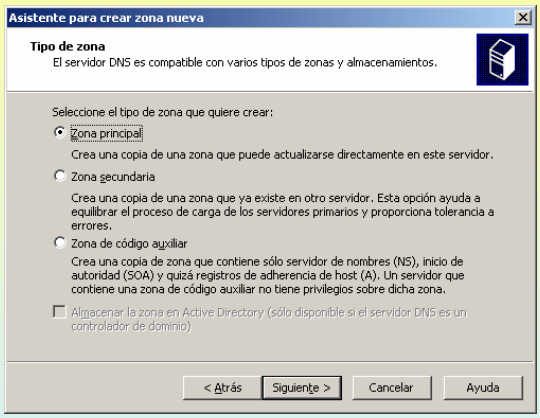


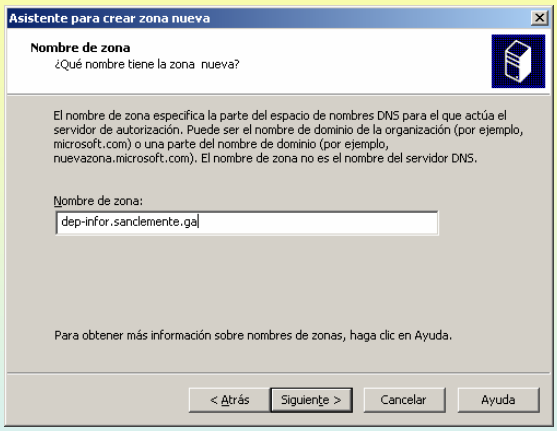


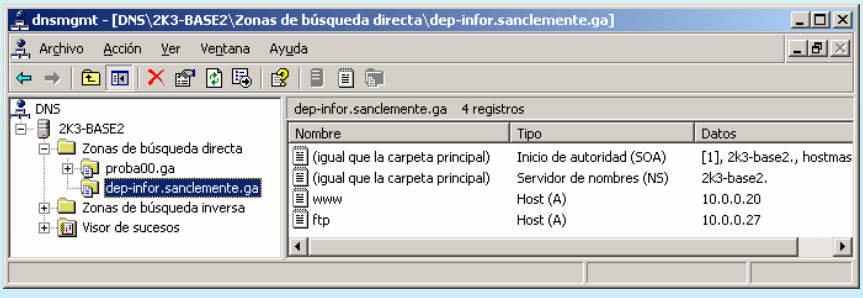
2.- DNS (Domain Name System)

☞ CREAR UNHA DELEGACIÓN DE ZOA

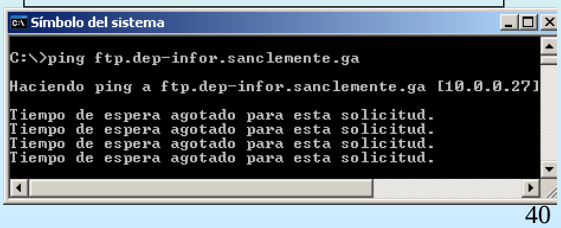
Actividades a realizar no host no que se delega a xestión dunha zoa.
Crear unha zoa como sempre e logo dar de alta un par de hosts (www, ftp)







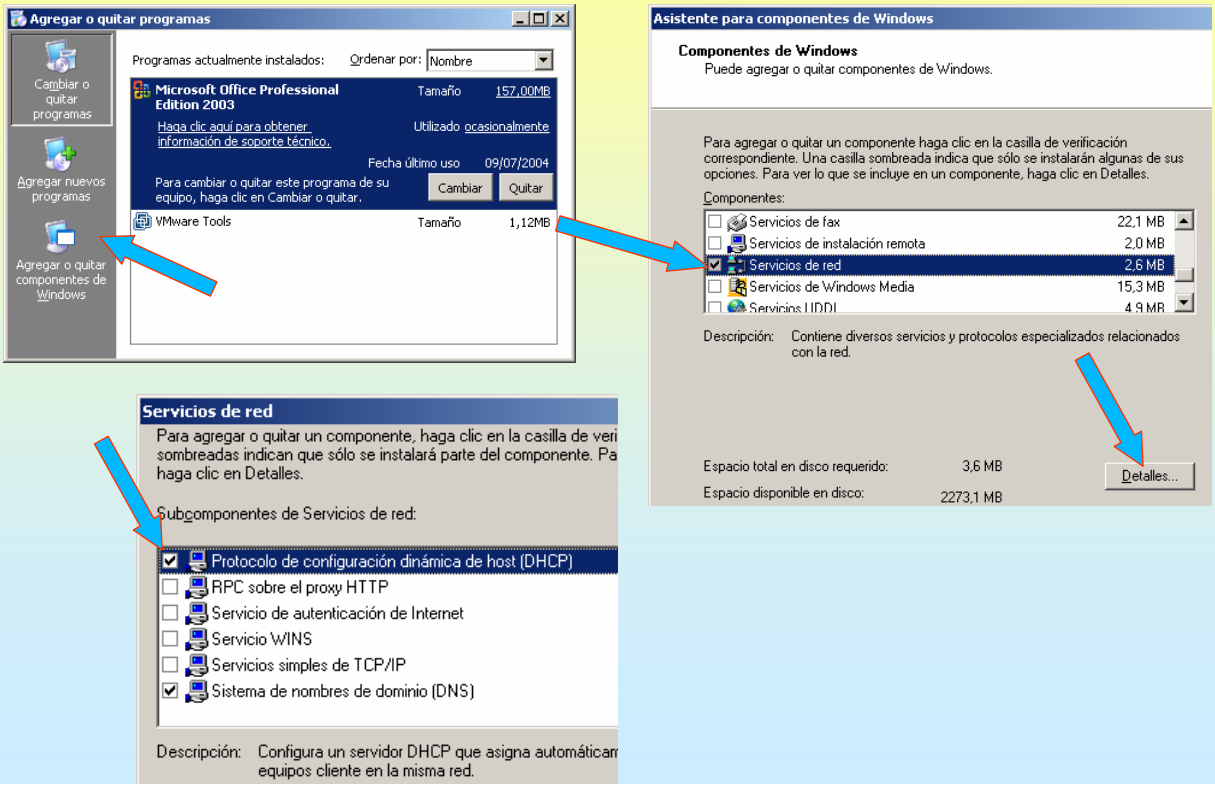
O ping resolve, logo, o equipo non resposta



3.- DHCP(Domain Host Configuration Protocol)

☞ INSTALACIÓN DA FERRAMENTA

Como sempre, instálase como un compoñente máis.

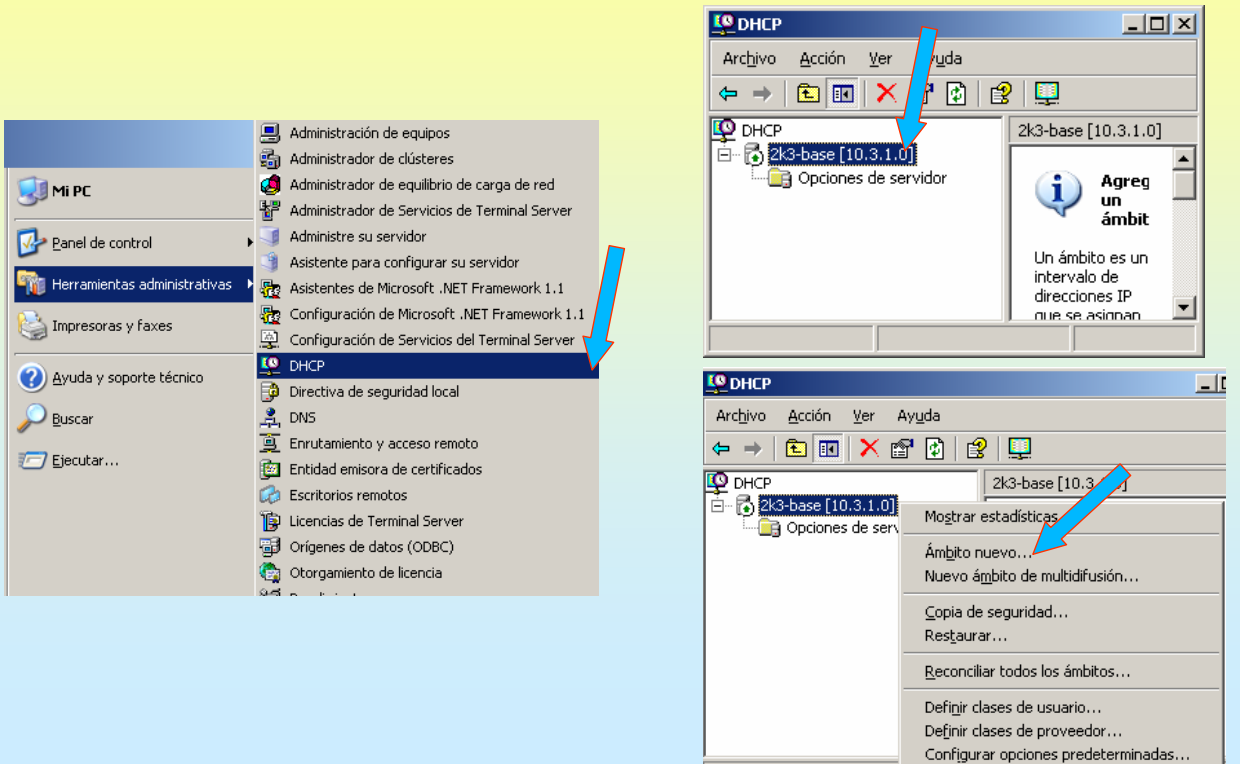


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

3.- DHCP(Domain Host Configuration Protocol)

☞ CREAR UN ÁMBITO

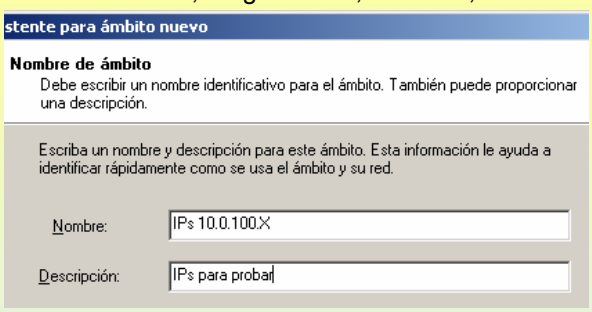
Nun ámbito é onde se especifica o rango de IPs que oferta o Servidor DHCP, a porta de enlace, o DNS, etc,

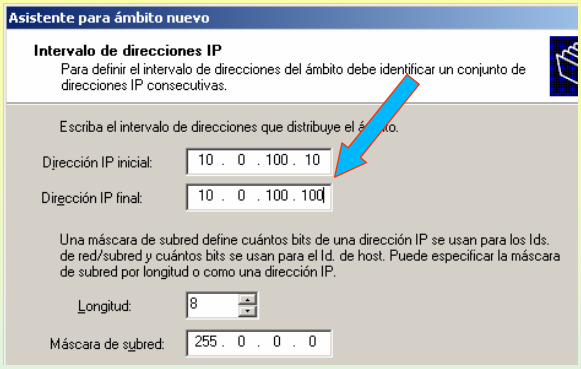


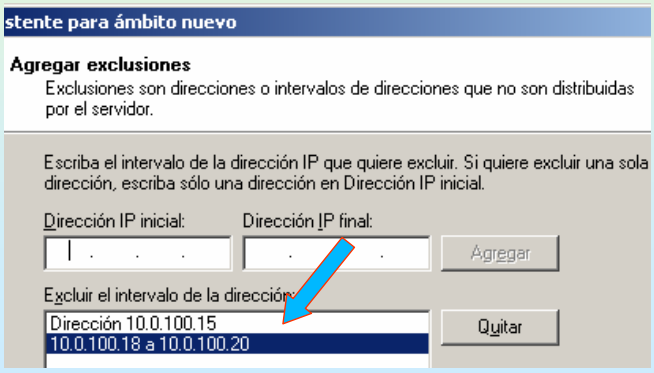
3.- DHCP(Domain Host Configuration Protocol)

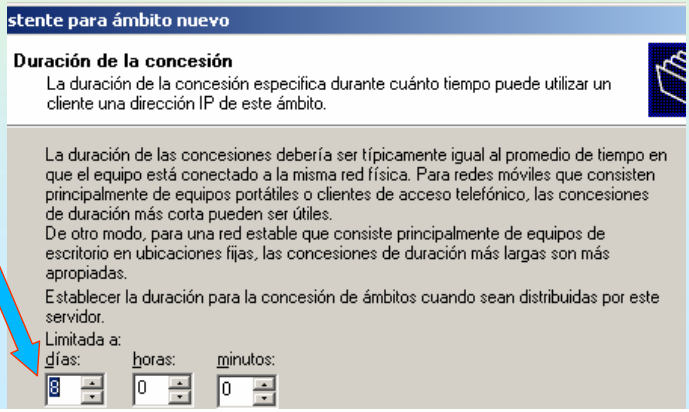
☞ CONFIGURAR O ÁMBITO

Darlle un nome, rango de IPS, máscara, exclusións, duración da concesión







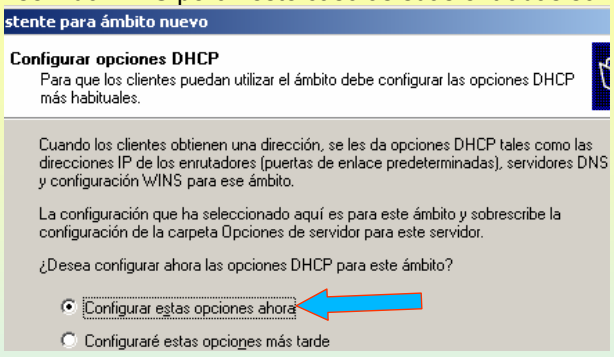


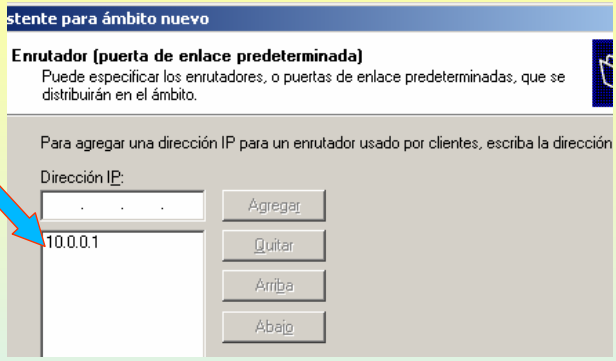
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

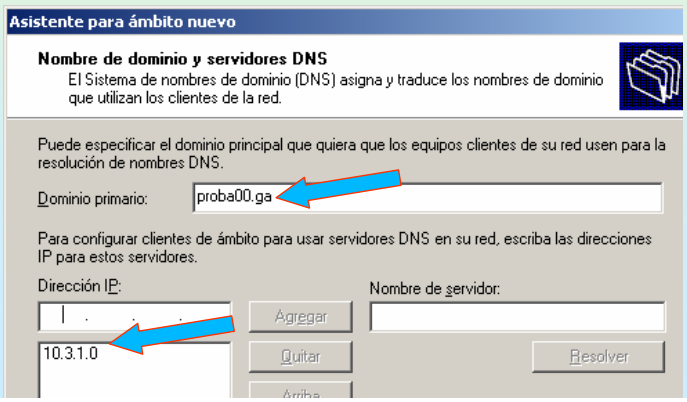
3.- DHCP(Domain Host Configuration Protocol)

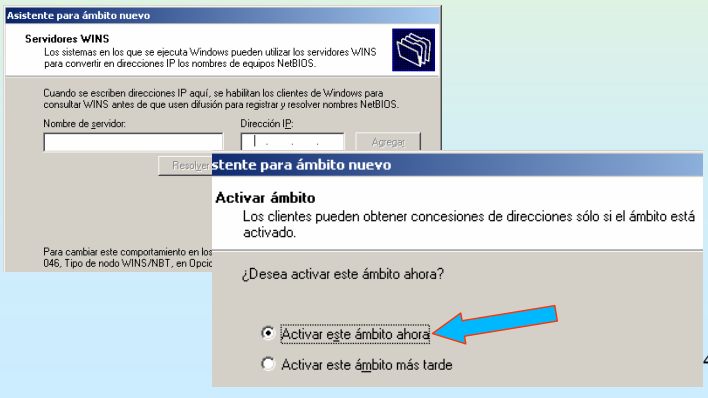
☞ CONFIGURAR ÁMBITO

Falta por indicar o router de saída, o DNS e finalmente activar o ámbito. O servidor WINS realiza algo semellante o servidor DNS pero neste caso as súas entradas son asociacións nome_netbio – IP. Neste caso non hai server WINS



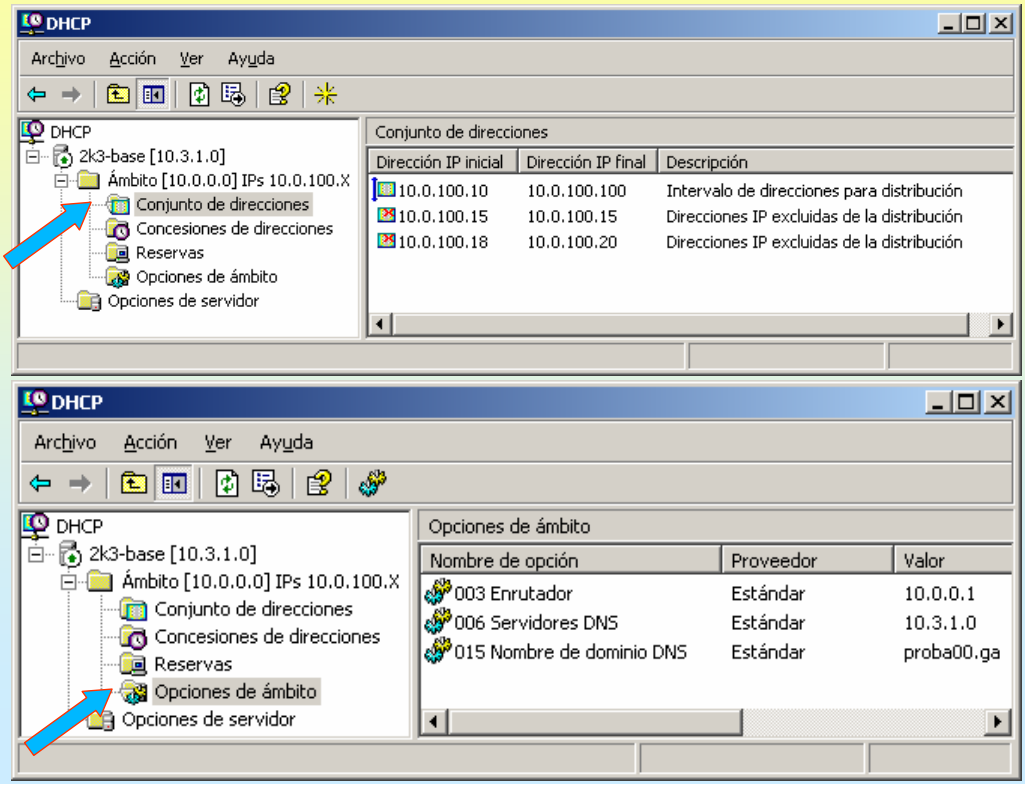






3.- DHCP(Domain Host Configuration Protocol)

☞ MOSTRAR INFORMACIÓN DO ÁMBITO

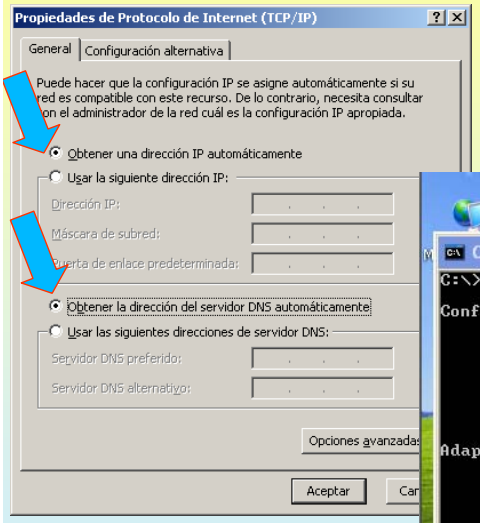


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

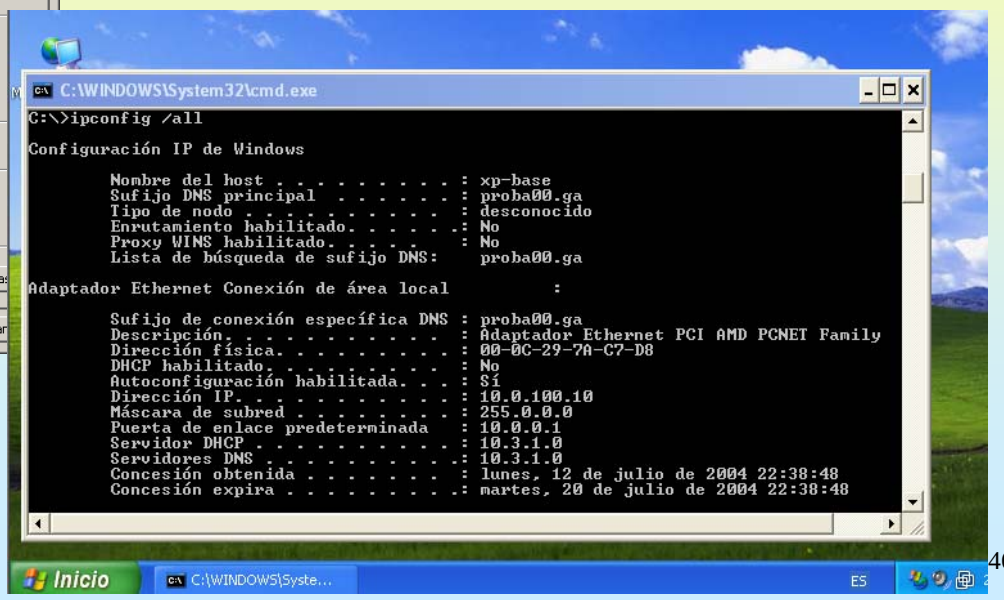
3.- DHCP(Domain Host Configuration Protocol)

☞ CONFIGURAR UN CLIENTE DHCP

Neste caso configurase un XP.



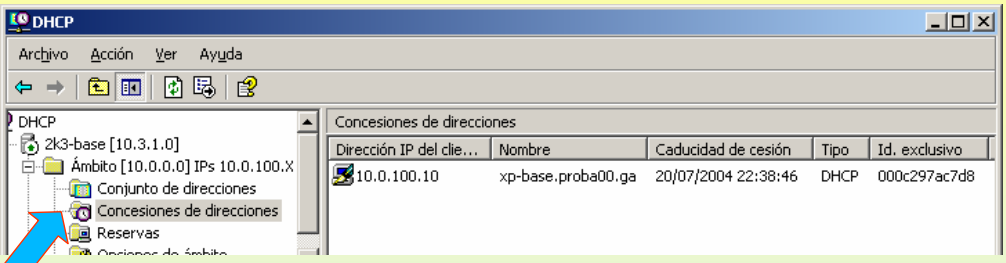
Tras indicarlle que se obteña automaticamente a configuración IP, o cliente busca un servidor DHCP que lle poida dar como mínimo unha IP e unha máscara

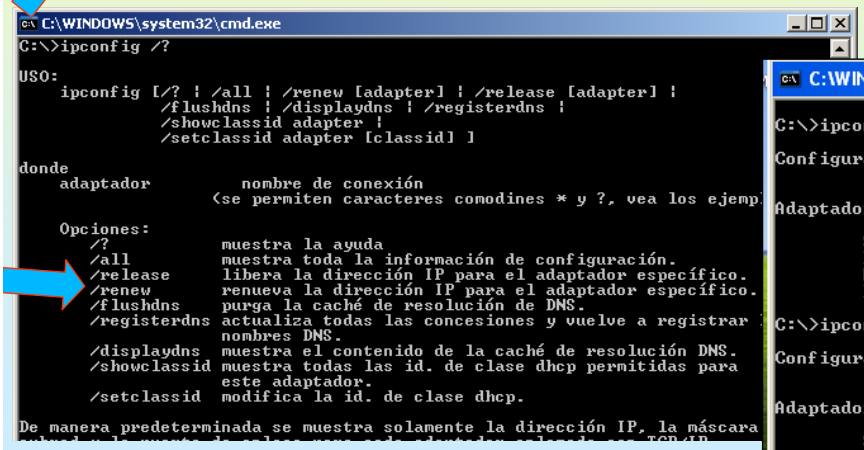


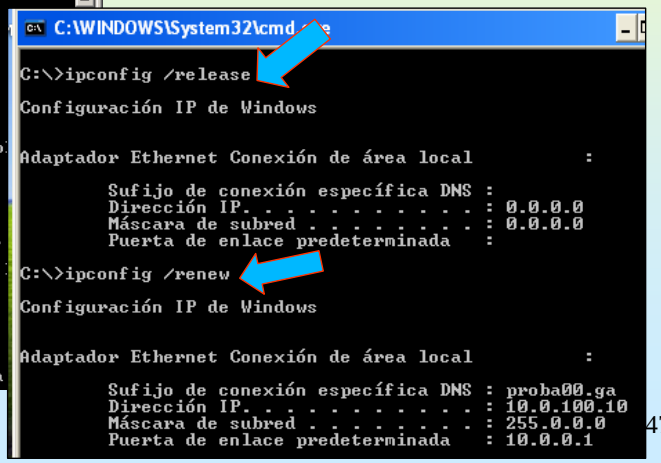
3.- DHCP(Domain Host Configuration Protocol)

☞ COMPROBAR AS CONCESIÓNS – UTILIDADE IPCONFIG

No servidor pódese levar conta das IPs asignadas e a quen se lle ofertaron.







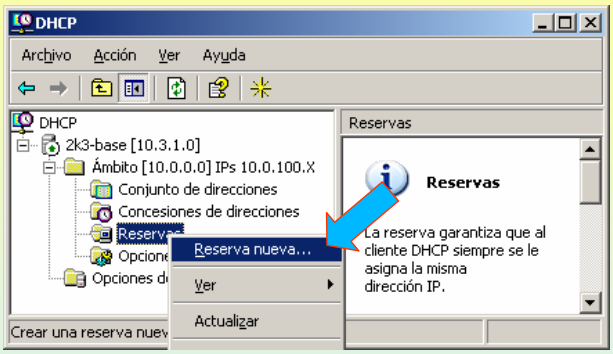
Dende o cliente pódese liberar a concesión ou renovala

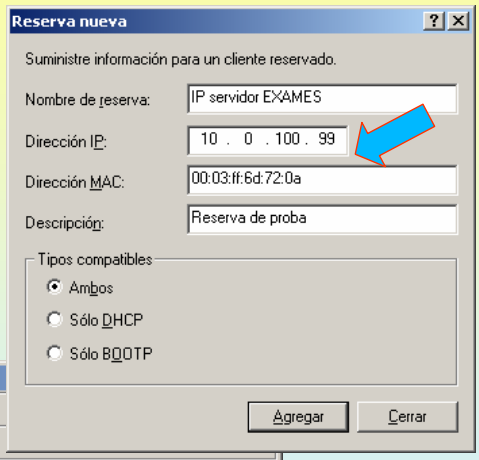
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

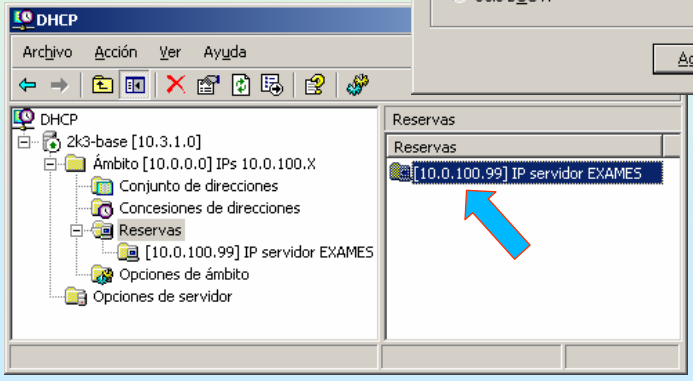
3.- DHCP(Domain Host Configuration Protocol)

☞ RESERVAR DE IPs

Consiste en asignar a sempre a mesma IP a un host determinado, para iso é preciso realizar unha reserva no servidor DHCP. Precísase indicar a MAC do equipo ó que se lle desexa asignar sempre a mesma IP.



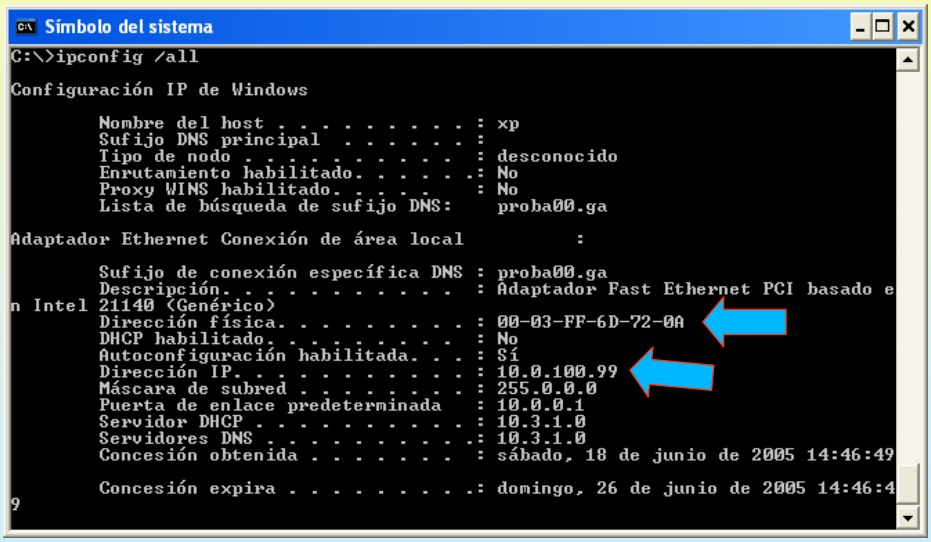




3.- DHCP(Domain Host Configuration Protocol)

☞ RESERVAR DE IPs (II)

IP asignada o cliente DHCP para o que se reservou a IP.



4.- FTP(File Transfer Protocol)

☞ COMANDOS CLIENTE FTP

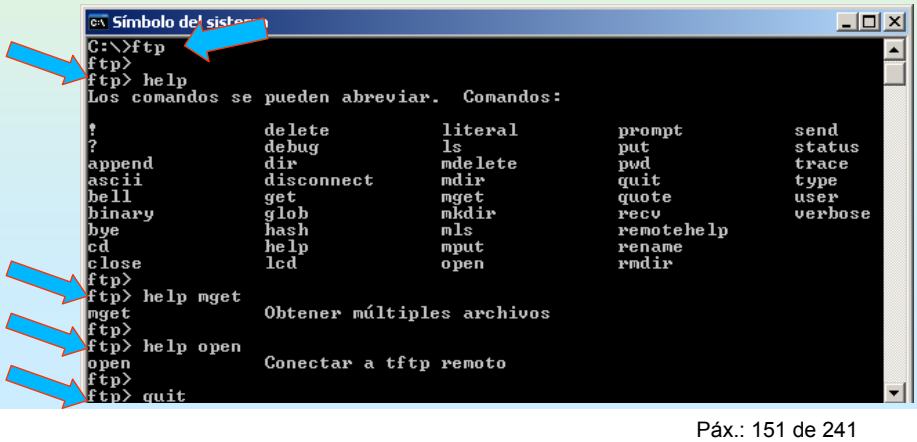
FTP é unha aplicación cliente servidor que basicamente serve para a Transferencia de arquivos entre cliente e o Server. Dende un cliente hai que conectarse a un servidor FTP. As accións básicas que se poden realizar son:

OPEN: Abre unha conexión contra un servidor FTP
CLOSE: Pecha unha conexión previa.

BAIXAR (DOWNLOAD): Transferir do servidor o cliente.
GET <arquivo>: baixa un arquivo. MGET : baixa un conxunto de arquivos

SUBIR (UPLOAD): Transferir dende o cliente ó servidor. Para poder realizalo débense ter permisos.
PUT <arquivo>: sobe un arquivo. MPUT : sobe un conxunto de arquivos.

QUIT: Sair do cliente e liberar a conexión existente.



4.- FTP(File Transfer Protocol)

☞ COMANDOS CLIENTE FTP

Establecer unha conexión co servidor FTP da Universidade de Santiago de Compostela: **ftp.usc.es**

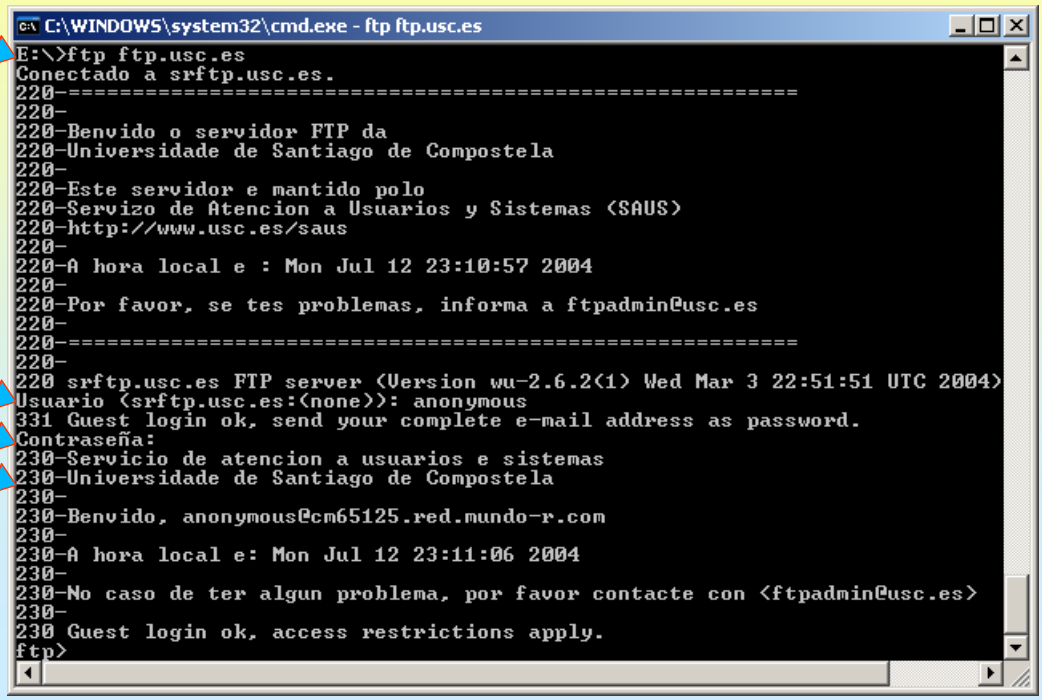
Abrir o cliente indicando xa o server.
Ó conectarse o server dános unha mensaxe de benvida

Tan pronto se abre a aplicación o SO asígnalle un porto dos que teña libres

Entrar como usuario anonimo

Un correo electrónico

Mensaxe de benvida unha vez validado o usuario

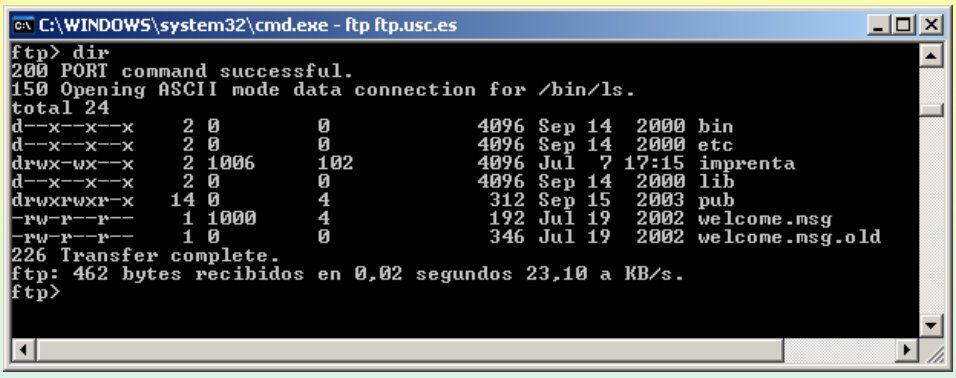


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

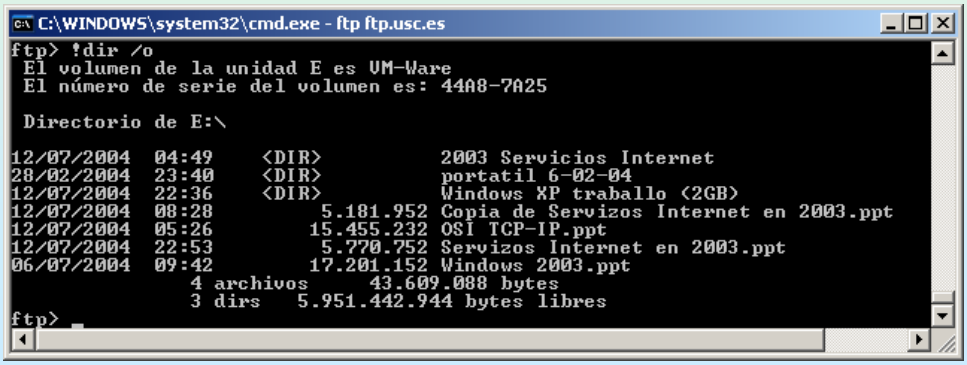
☞ DIR / LS

Para mostrar o que hai no servidor. Cando se desexe executar un comando no cliente débese poñer un signo de admiración diante do comando (!dir)



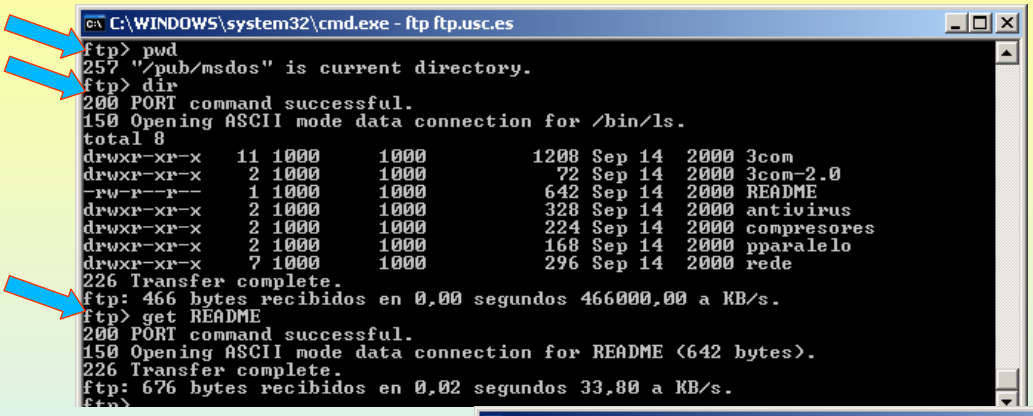
Dir remoto

Dir local

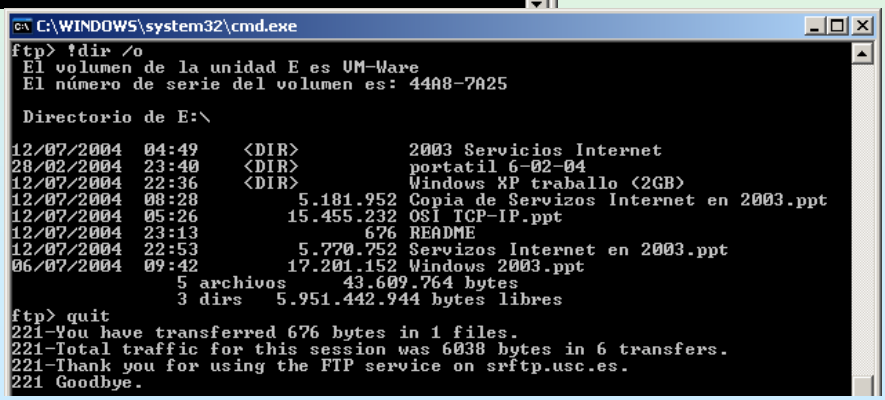


4.- FTP(File Transfer Protocol)

☞ BAIXAR UN ARQUIVO



Con **cd** moverse ata /pub/msdos



Observar en local como se transferiu o arquivo README.

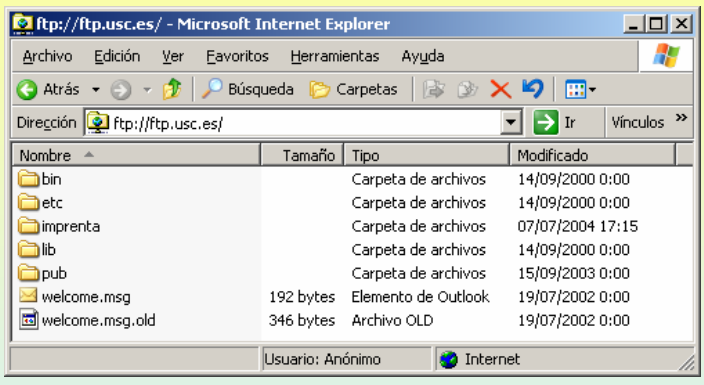
Ó saír tamén emite unha mensaxe de despedida

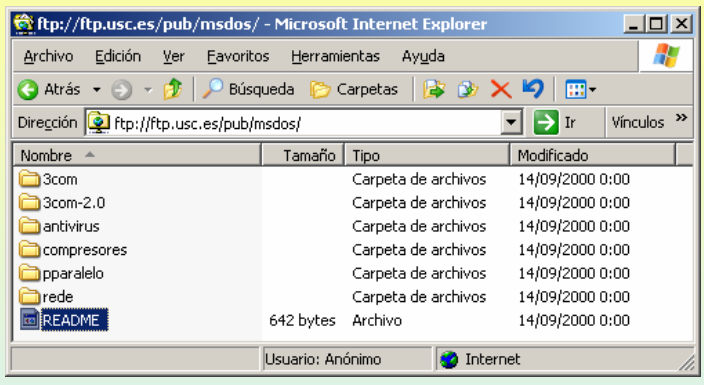
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

☞ CLIENTE GRÁFICO / WEB FTP

Todo o que se fixo anteriormente pódese realizar dende un explorador web.



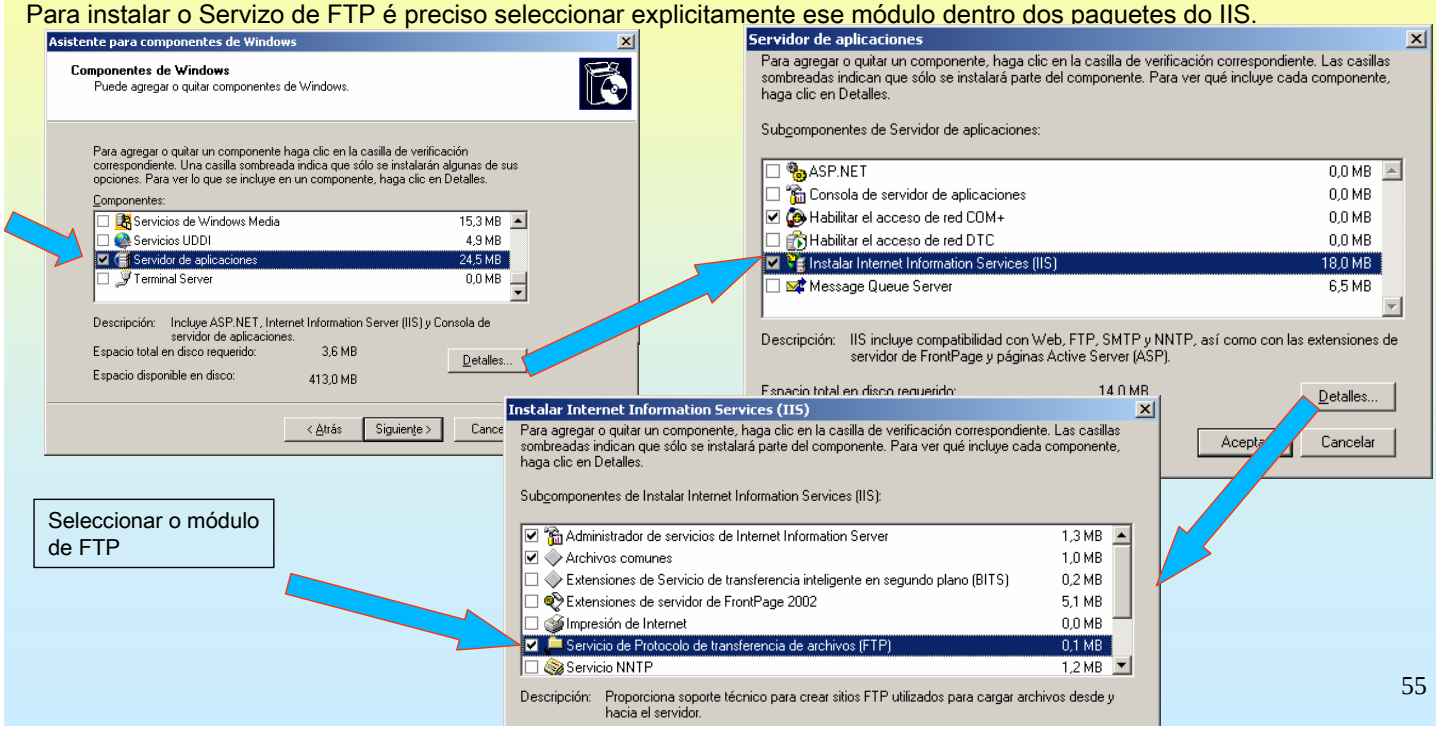


4.- FTP(File Transfer Protocol)

☞ INSTALACIÓN DO IIS (Internet Information Services) (SERVIDOR FTP E SERVIDOR WEB)

Instálase como calquera outro compoñente de windows. (Panel de control → agregar e quitar programas→ agregar ou quitar compoñentes de windows)

Ó instalar o IIS coas opcións que veñen por defecto só instala o servidor WEB, creando un sitio web predeterminado. Para instalar o Servizo de FTP é preciso seleccionar explicitamente ese módulo dentro dos paquetes do IIS.



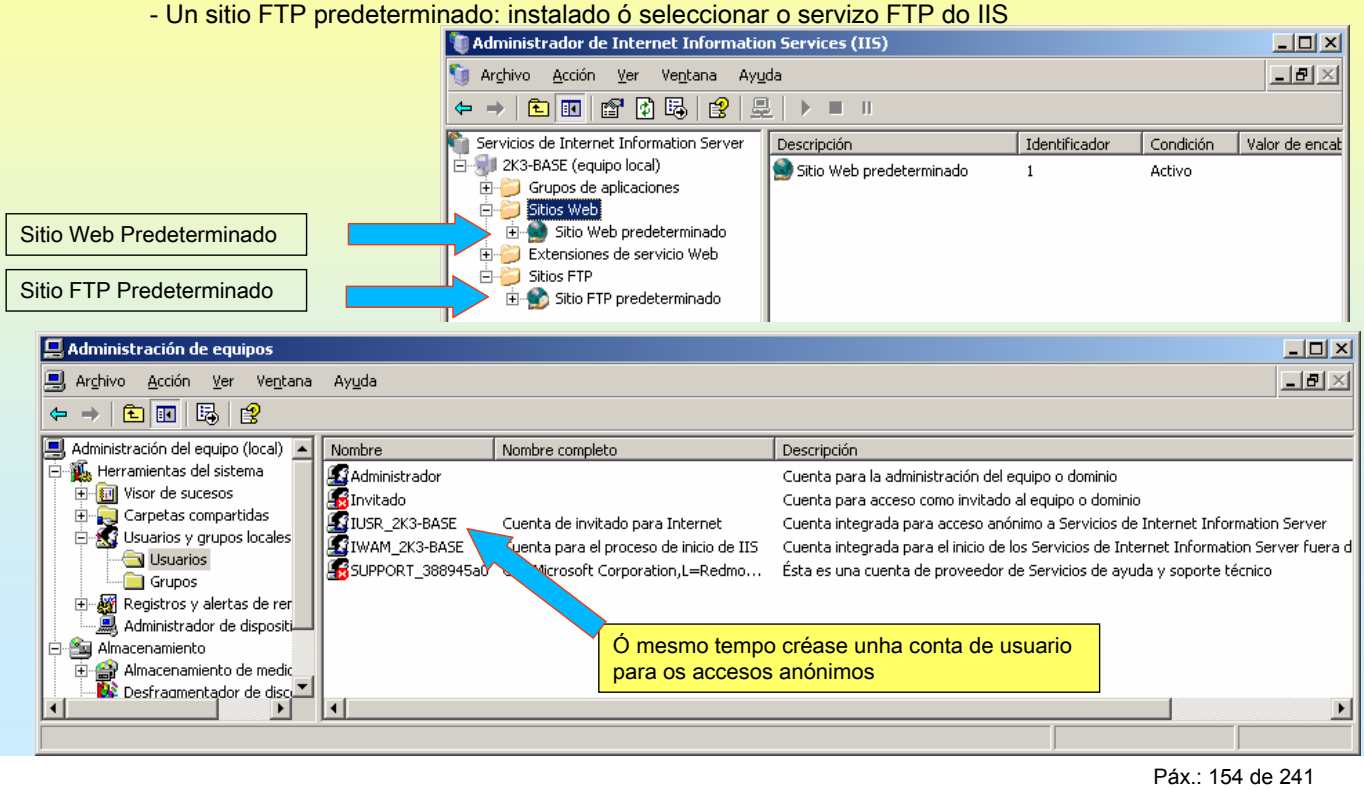
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

☞ INSTALACIÓN DO IIS (Internet Information Services) (SERVIDOR FTP E SERVIDOR WEB)

Unha vez instalado o IIS o que se ten son:

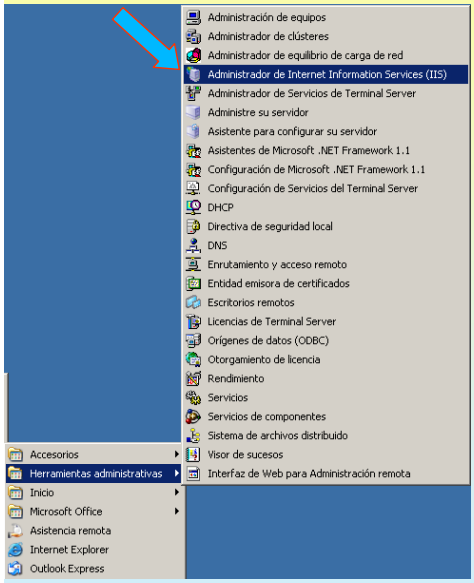
- Un **sitio web predeterminado**: instalado por defecto co IIS
- Un sitio FTP predeterminado: instalado ó seleccionar o servizo FTP do IIS

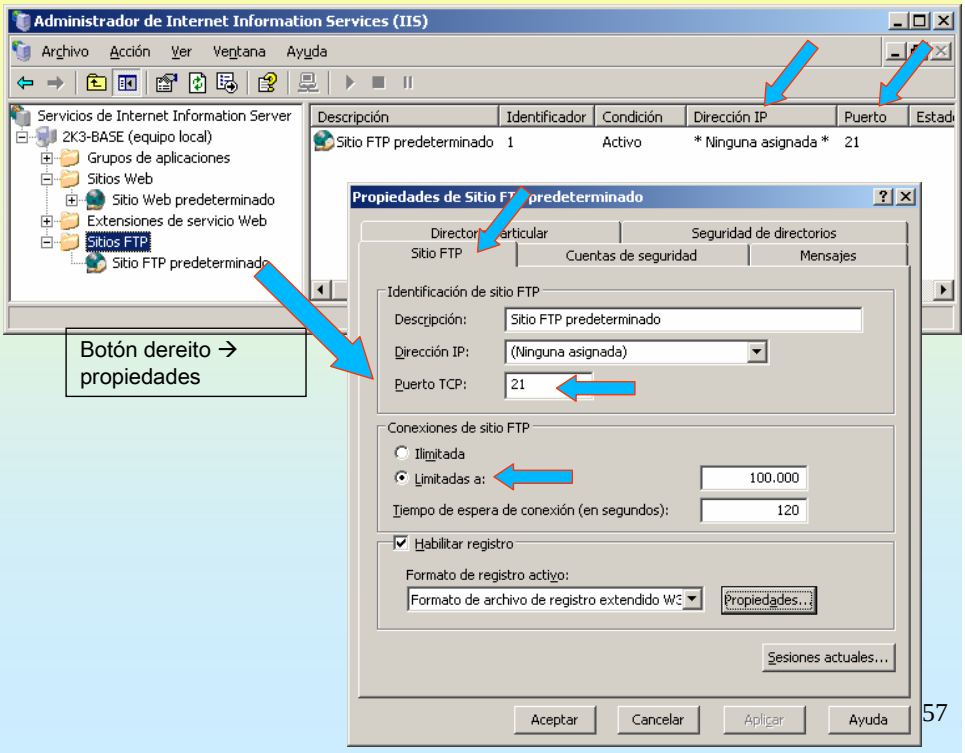


4.- FTP(File Transfer Protocol)

☞ CONFIGURACIÓN DO SERVIDOR FTP PREDETERMINADO

O servizoFTP ven cun sitio FTP xa configurado por defecto. Examinemos as súas propiedades



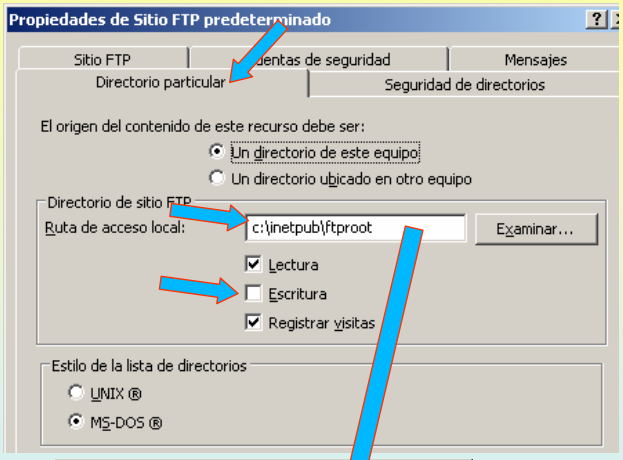


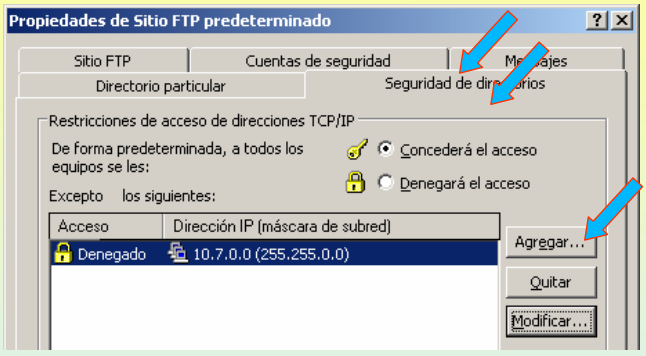
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

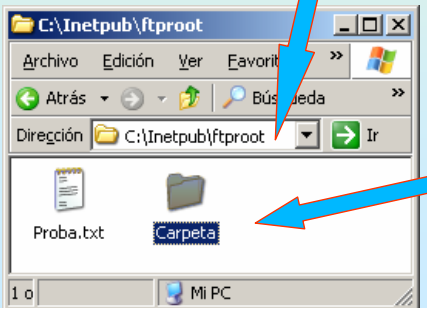
4.- FTP(File Transfer Protocol)

☞ CONFIGURACIÓN DO SITIO PREDETERMINADO

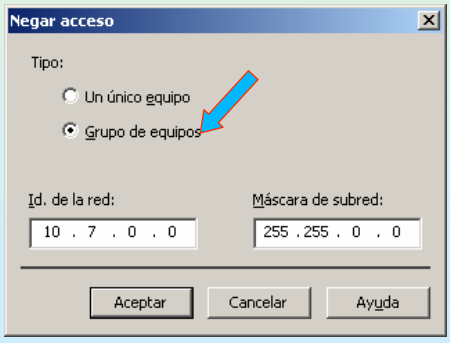
Carpeta de ubicación, permisos e dende que IPs se poden acceder.







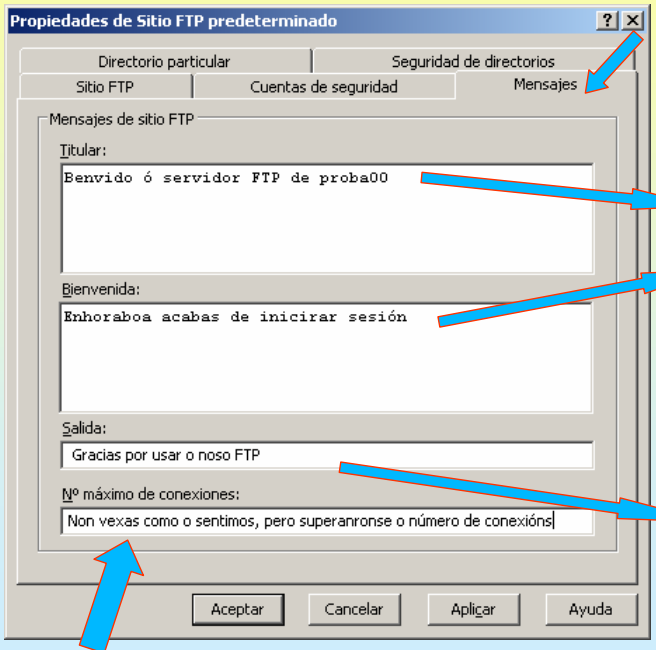
Introdúcese o seguinte contido na carpeta do Servidor FTP para probas futuras

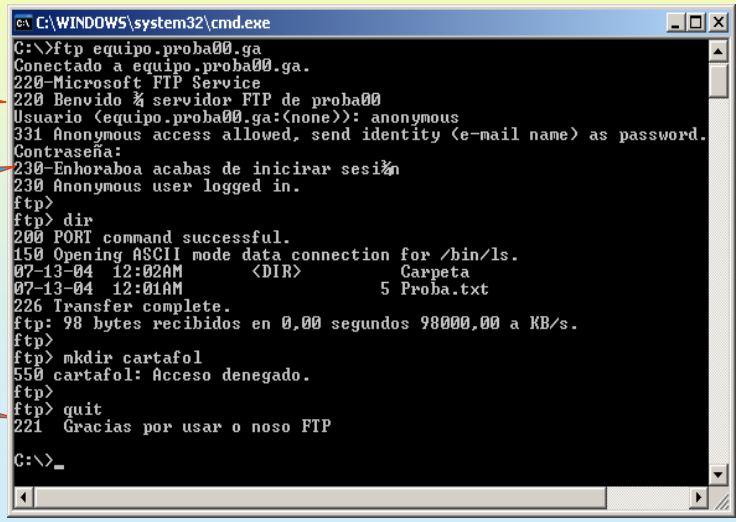


4.- FTP(File Transfer Protocol)

☞ CONFIGURACIÓN DO SITIO PREDETERMINADO

Mensaxes de benvida, despedida e número máximo de conexión.





Cando se superen ó número de conexións permitido aparecerá esta mensaxe

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

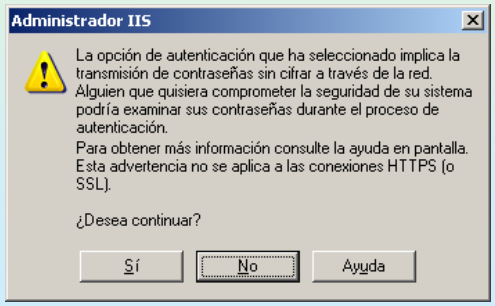
☞ CONFIGURACIÓN DO SITIO PREDETERMINADO

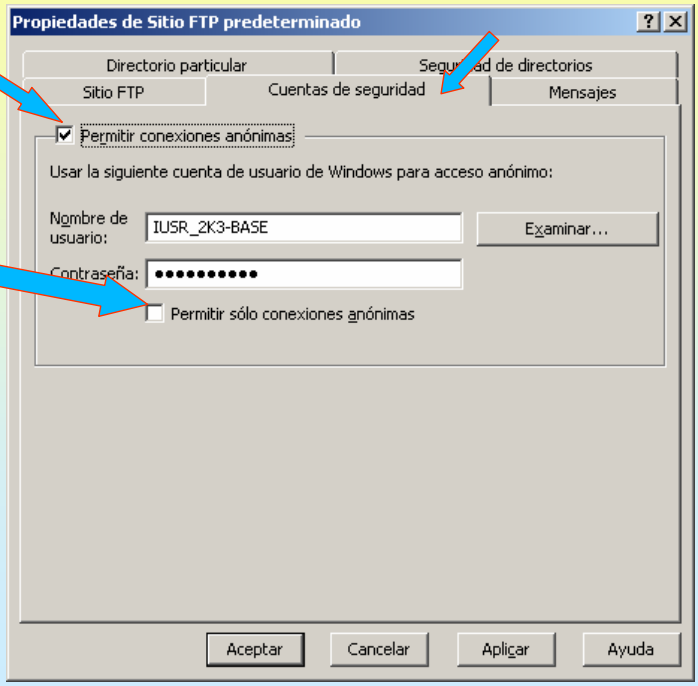
Configuración de contas, se se permite ou non conexións anónimas.

Se non se permiten conexión anónimas débese deseleccionar esta opción, pero

OLLO, pois a trasmisión das contrasinais dos usuarios iría sen cifrar, tal e como indica a Advertencia.

Se se selecciona, só se permitiría a conexión do usuario anónimo

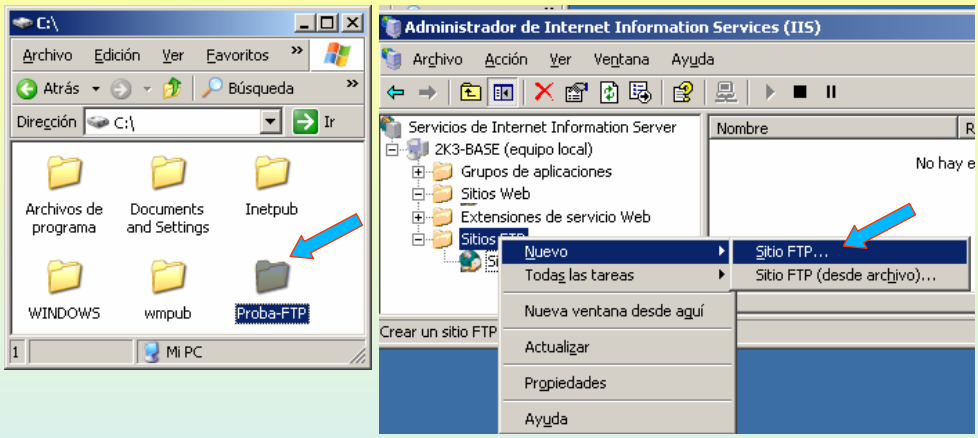


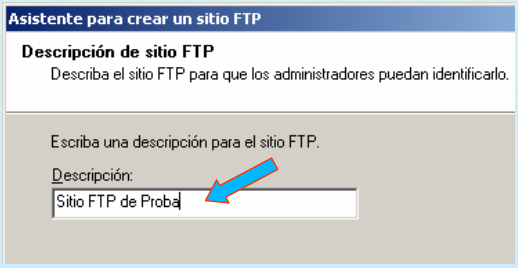


4.- FTP(File Transfer Protocol)

☞ CREAR UN NOVO SITIO FTP

Primeiro crease a carpeta onde van residir os arquivos e carpetas do sitio FTP



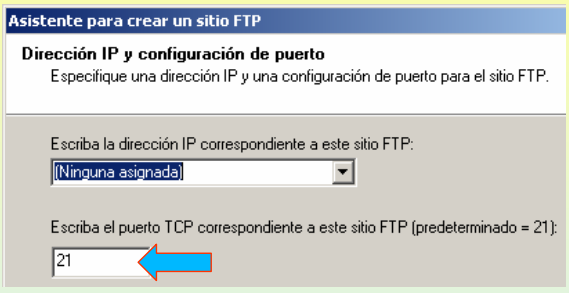


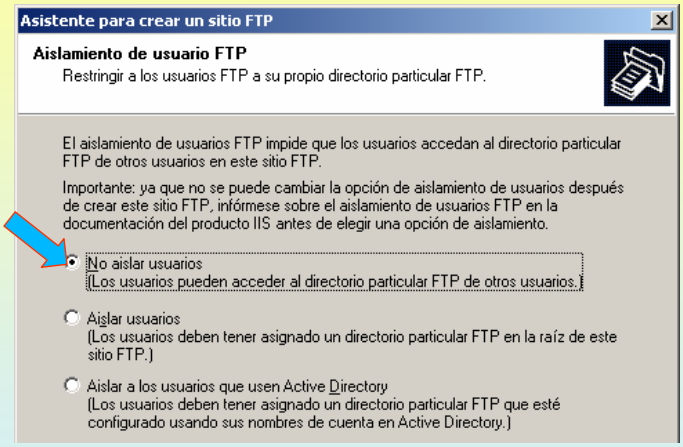
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

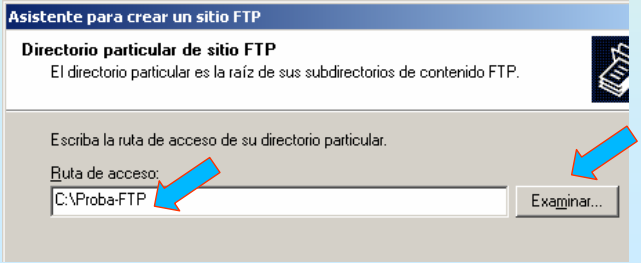
4.- FTP(File Transfer Protocol)

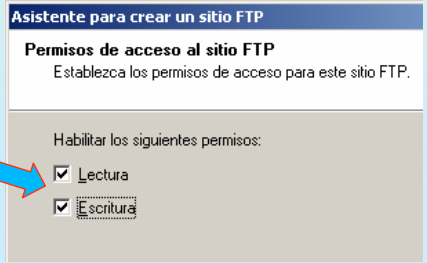
☞ CREAR UN NOVO SITIO FTP

Especificar porto (21 – vai fallar pois non pode haber dous servidores escoitando no mesmo porto)
Especificar rota e os permisos, neste caso dáselle permiso de escritura





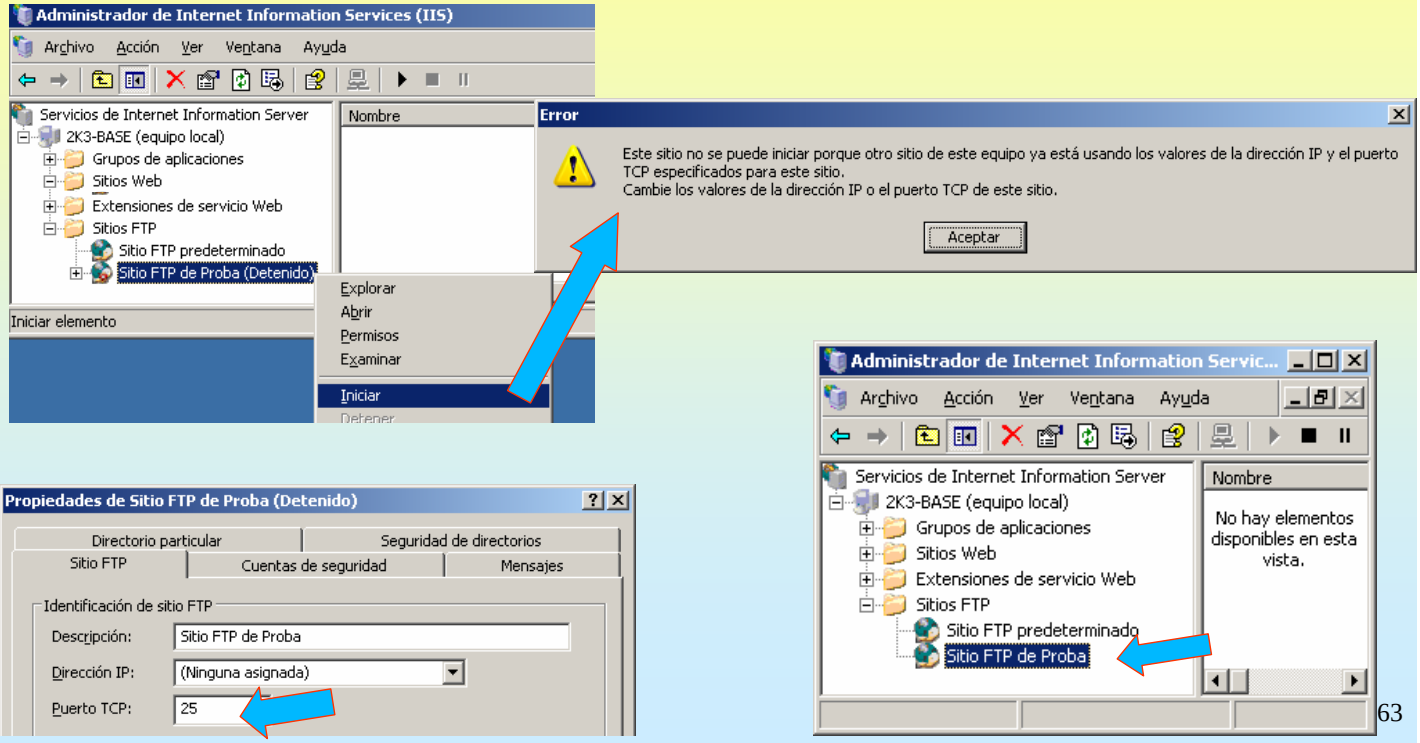




4.- FTP(File Transfer Protocol)

☞ INICIAR O NOVO SITIO FTP.

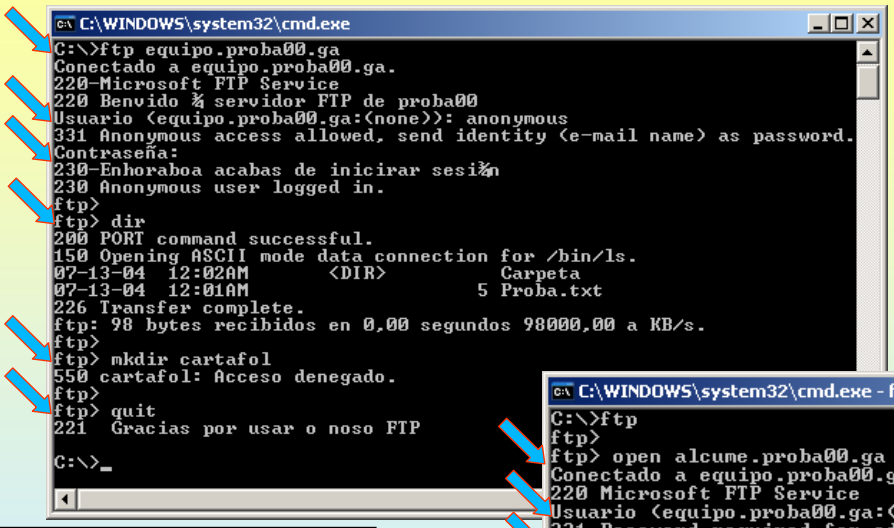
O novo sitio FTP está detido, porque quere traballar no mesmo porto que o outro sitio.
Se se inicia da erro. Para solucionalo cámbiaselle o porto de traballo e vólvese a iniciar



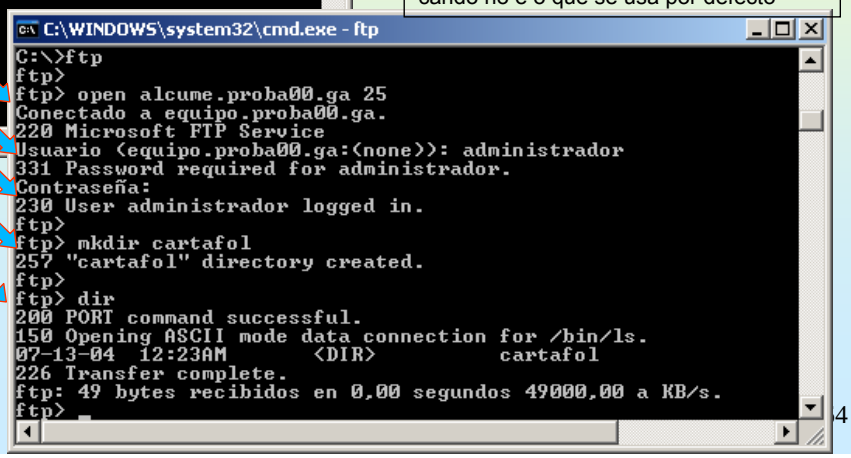
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

☞ CONEXIÓNS OS SITIOS FTP ANTERIORES DENDE UN CLIENTE



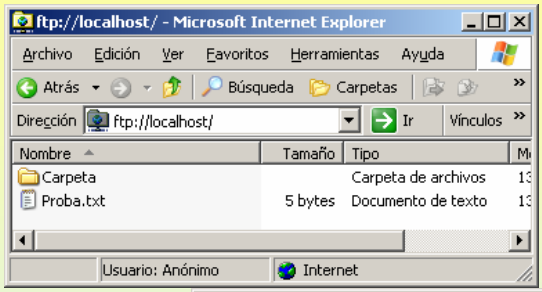
Neste caso entrouse como administrador (hai que poñer o seu contrasinal) e si que hao permisos de escritura, pois creouse un directorio.
Observar como se especifica o porto cando no é o que se usa por defecto

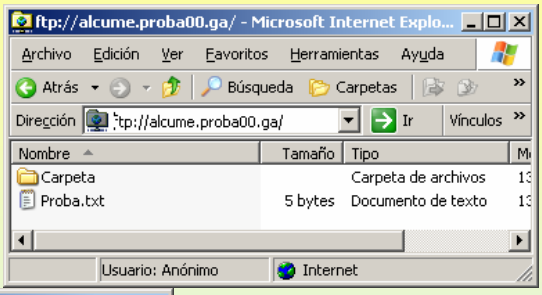


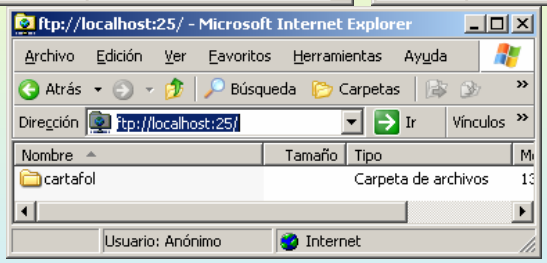
Observar as accións realizadas nas frechas, as mensaxes de benvida e como non deixa crear un directorio

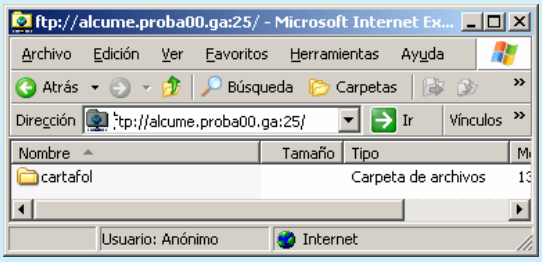
4.- FTP(File Transfer Protocol)

☞ CONEXIÓNS OS SITIOS FTP ANTERIORES DENDE UN CLIENTE GRÁFICO

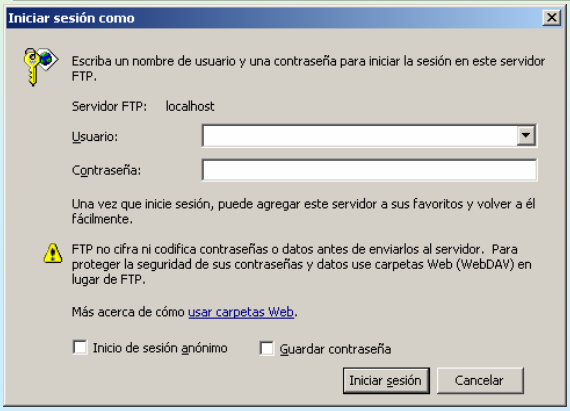








Se se desexa entrar cun usuario non anónimo especifícase en:
Archivo → Iniciar sesión como



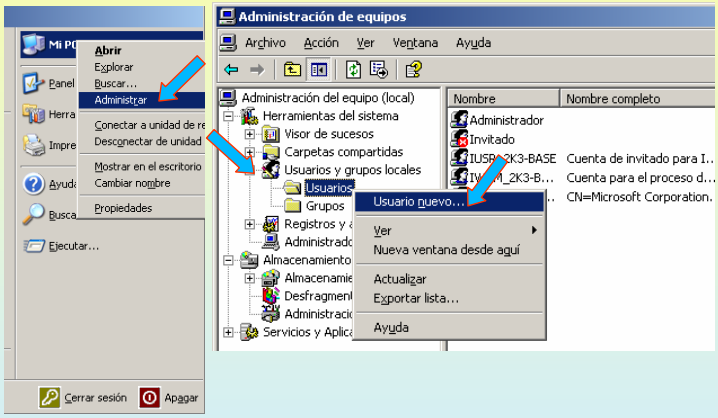
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

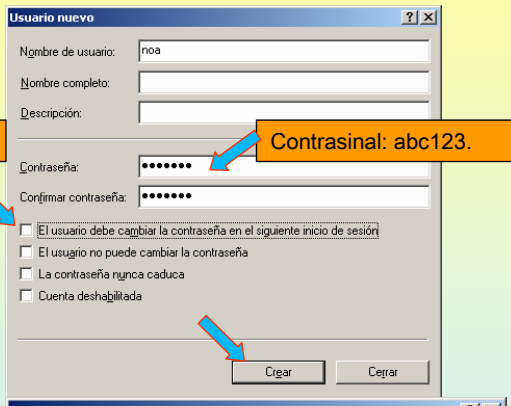
4.- FTP(File Transfer Protocol)

☞ ILLAMENTO DE USUARIOS FTP.

Esta opción permite crear sitios FTP nos que cada usuario (local ou de Active Directory) ten unha carpeta persoal. Cada usuario conéctase ó mesmo sitio FTP, pero só pode acceder á súa carpeta de FTP e non verá a dos demais.

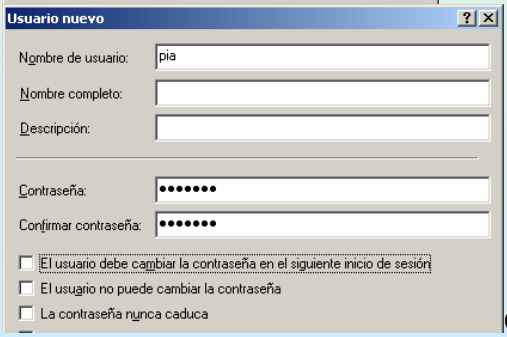
Neste exemplo crearanse dúas usuarios locais: Noa e Pia





Deshabilitar

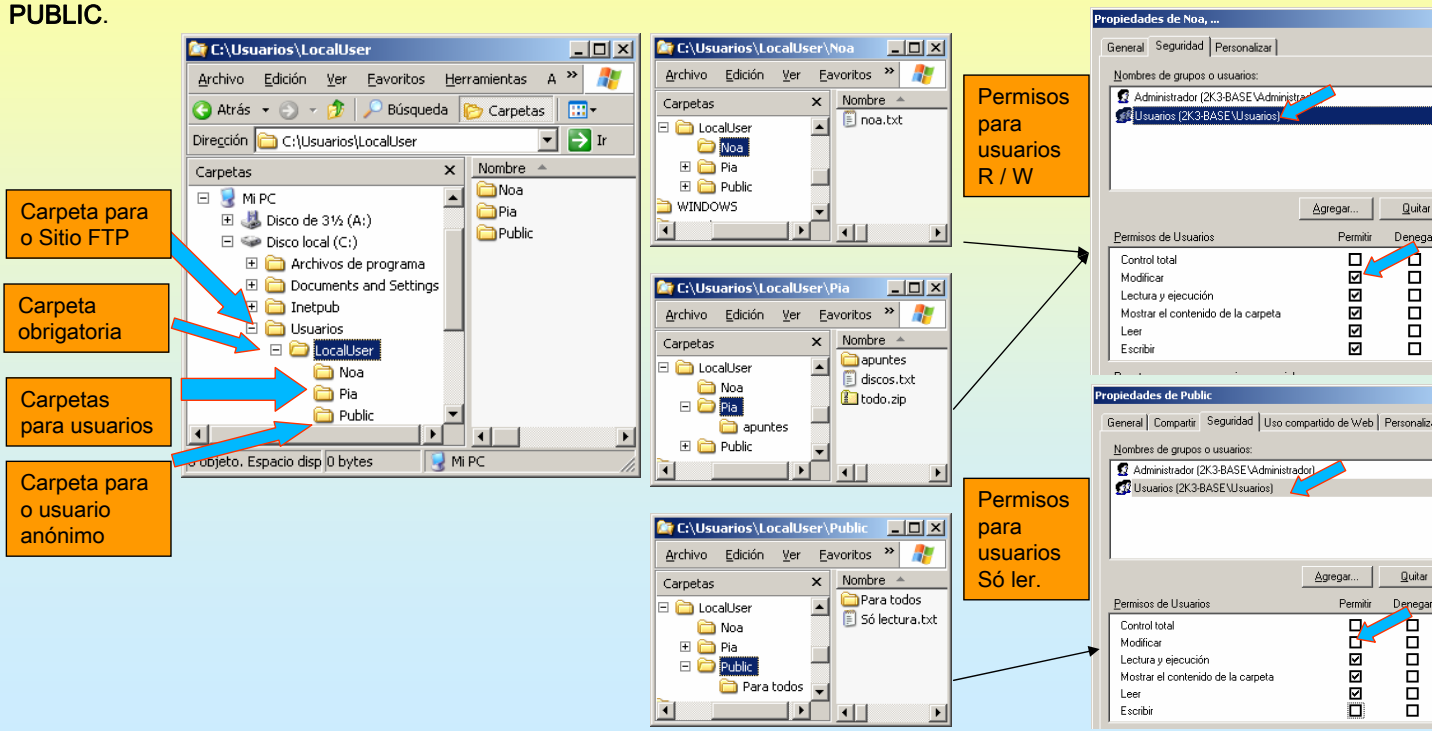
Contrasinal: abc123.



4.- FTP(File Transfer Protocol)

☞ ILLAMENTO DE USUARIOS FTP.

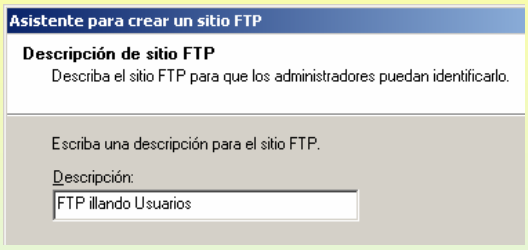
Débese crear unha carpeta para o sitio FTP, e **DENTRO DESTA,** unha carpeta que se chame **USERLOCAL**. Esta carpeta terá unha carpeta por cada usuario. Se se permite acceso anónimo tamén se debe crear unha que se chame **PUBLIC**.

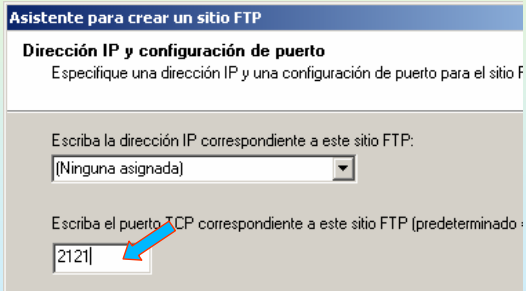


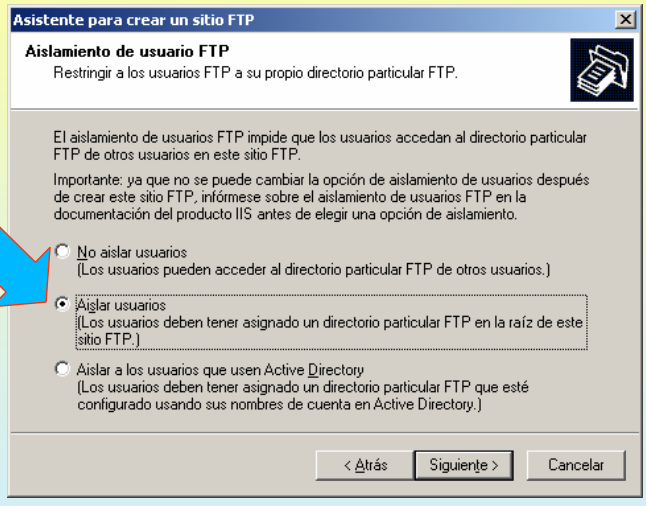
4.- FTP(File Transfer Protocol)

☞ ILLAMENTO DE USUARIOS FTP.

Agora crear un novo sitio FTP, coa opción de illar usuarios. OLLO co porto, non pode ser ningún dos xa usados.







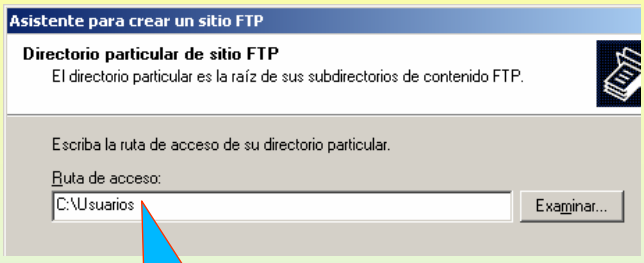
Para máis información sobre illamento de usuarios en FTP (sobre todo para a 3ª opción) recoméndase copiar o seguinte enlace navegador web nun windows 2003

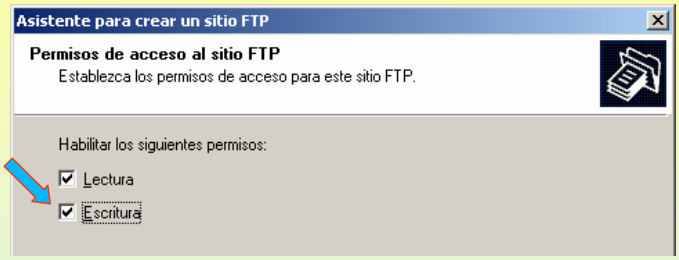
its:C:\WINDOWS\help\iismmc.chm::/htm/wsa_ftp_isolate.htm#

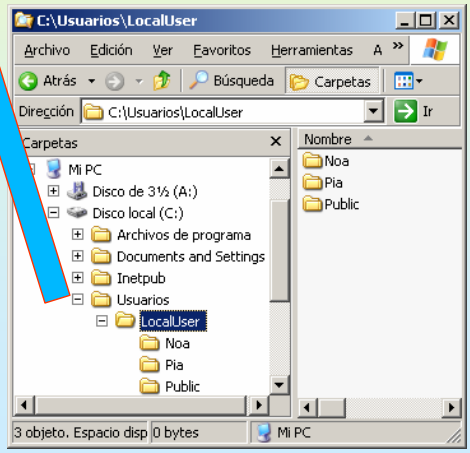
4.- FTP(File Transfer Protocol)

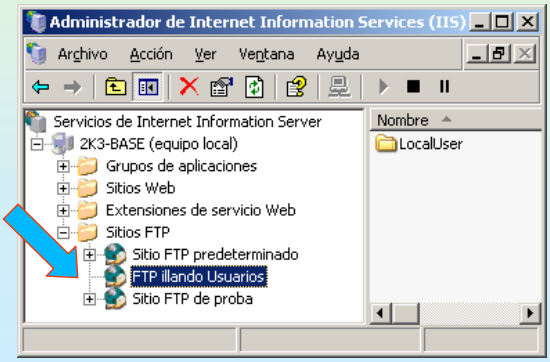
☞ ILLAMENTO DE USUARIOS FTP.

Escoller a carpeta anterior e dar permiso de Escritura, para que os usuarios poida ter ese permisos naquelas carpetas que tamén o teñen.







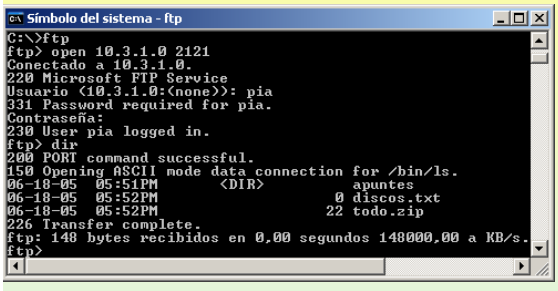


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

☞ ILLAMENTO DE USUARIOS FTP.

Validarse como PIA e crear unha carpeta

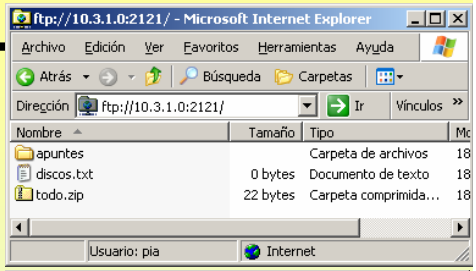


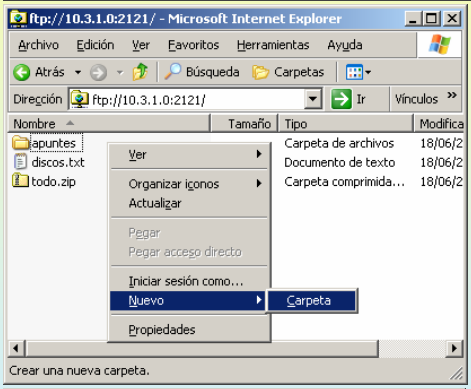
IMPORTANTE

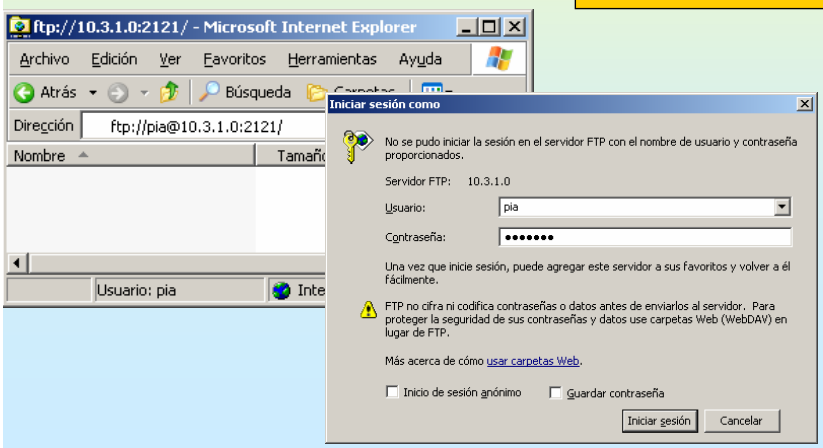
Todo o que se envía a través de FTP (información, contrasinais, etc)

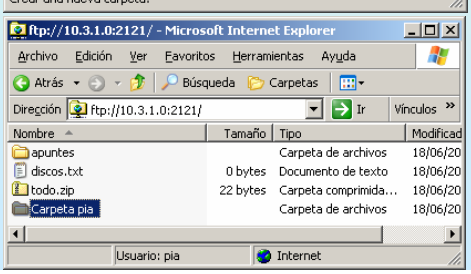
NON VAI CIFRADO

Se se desexa que os contrasinais vaian cifrados usar WebDav





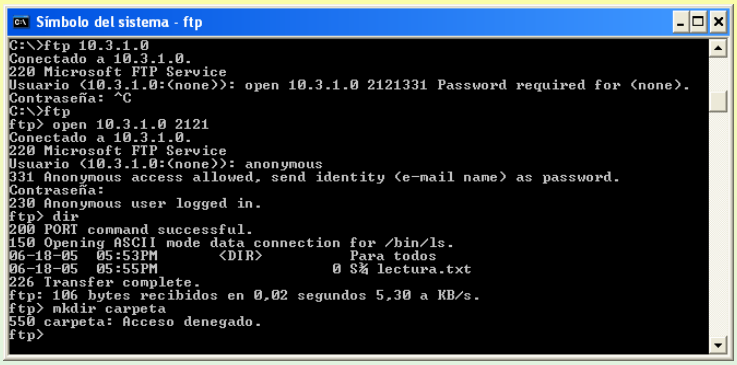


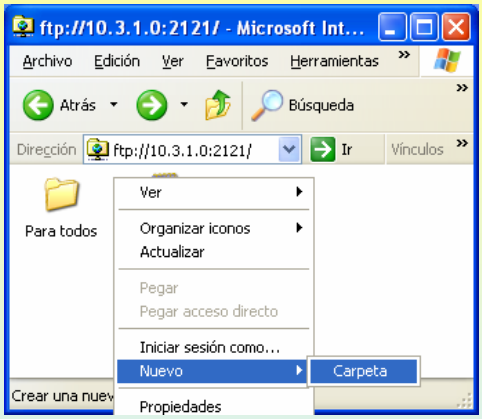


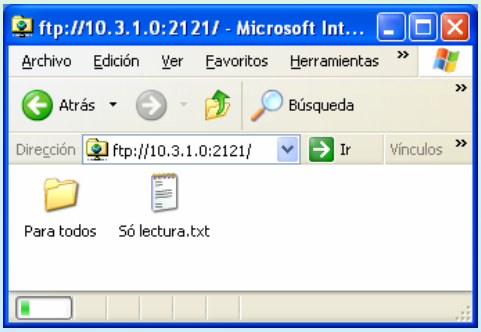
4.- FTP(File Transfer Protocol)

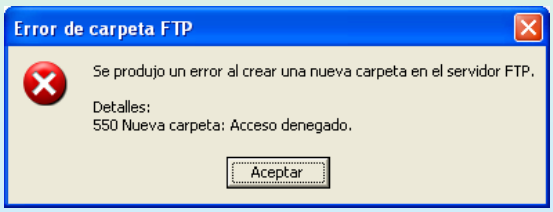
☞ ILLAMENTO DE USUARIOS FTP.

Validarse como **anonymous** e crear unha carpeta









Exercicio

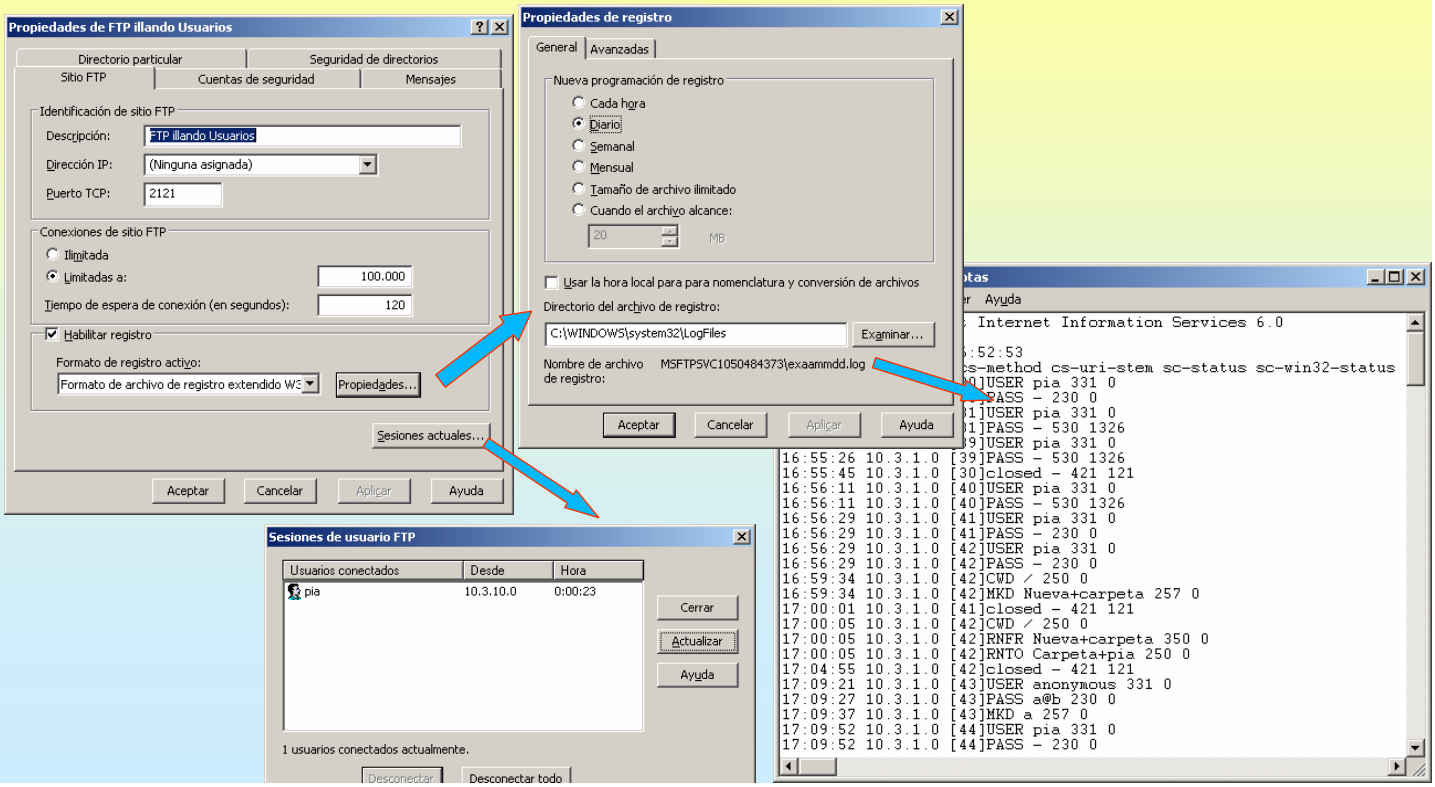
Crear un sitio FTP, no que Pia poida subir e baixar, mentres que noa só pode baixar o que pia subiu ou creou.

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

4.- FTP(File Transfer Protocol)

☞ REXISTRO DE ACCESOS E SESIÓNS ACTUAIS

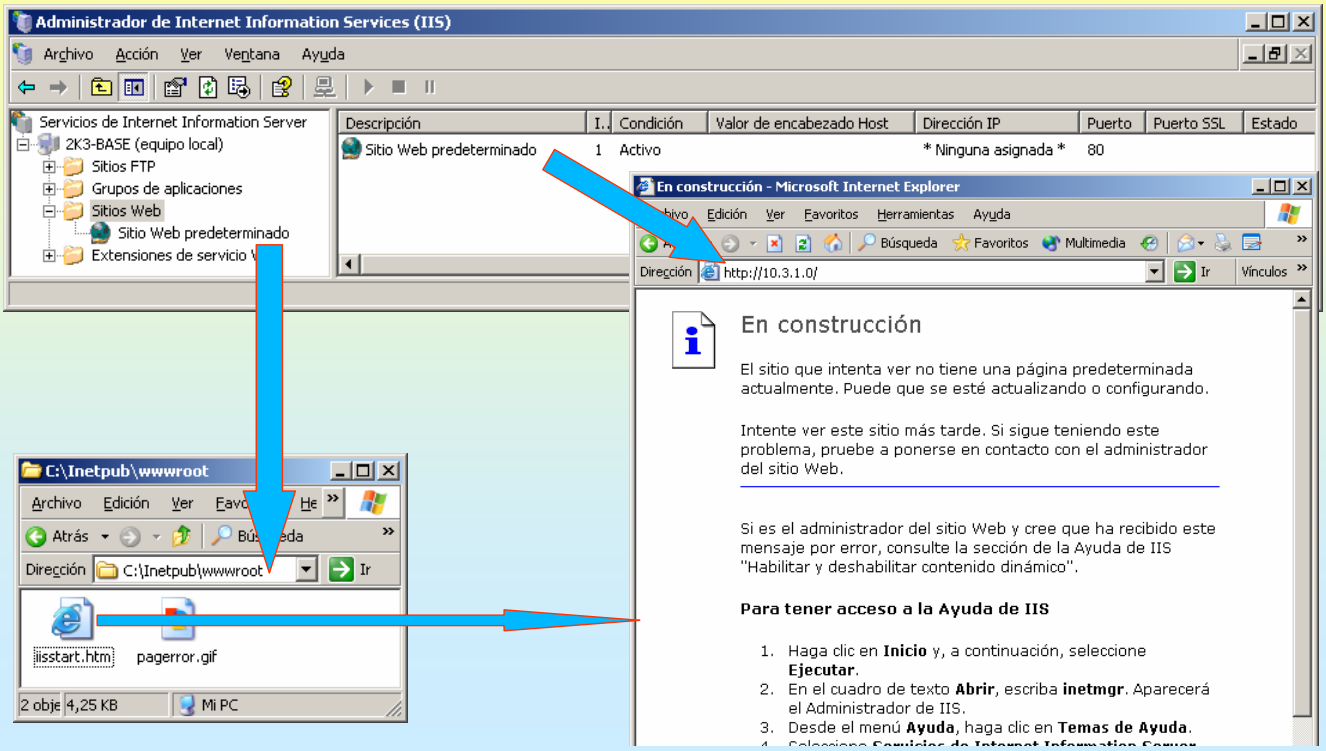
Por defecto na carpeta **c:\windows\system32\LogFiles** almacénase o rexistro das sesións que realizan os usuarios.



5.- Servidor WEB

☞ SERVIZO WEB

Cando se instalou o servizo FTP dentro do IIS tamén se instalou por defecto o servizo WEB.
Nese intre creouse o **Sitio WEB predeterminado.** Este sitio traballa no porto 80. E por agora di que está en construcción.

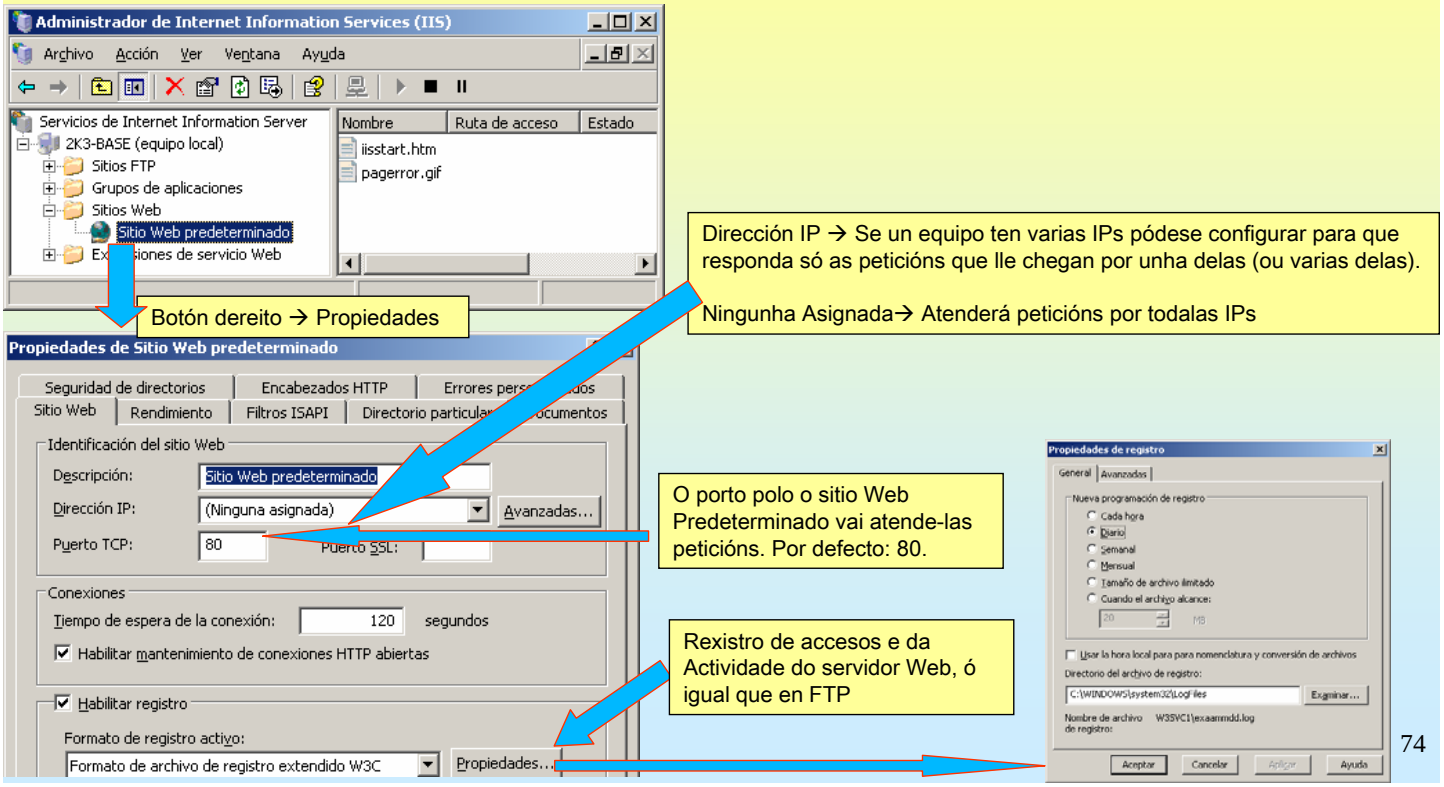


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ O SITIO WEB PREDETERMINADO

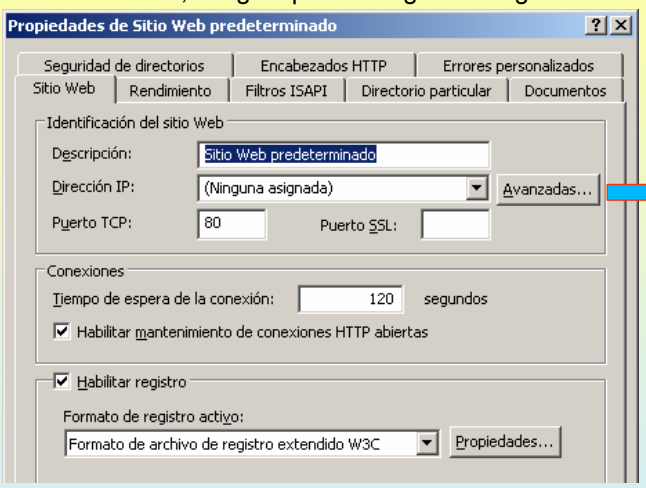
Escoita por defecto no porto 80 e non precisa encabezado (verase máis adiante)

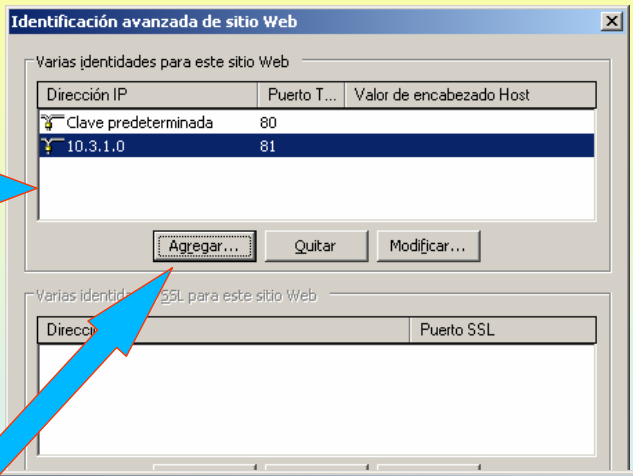


5.- Servidor WEB

☞ O SITIO WEB PREDETERMINADO

Configurar o sitio WEB predeterminado para que escoite nunha IP determinada e no porto 80. Neste caso como o hosgt só ten unha IP, dá igual poñer Ningunha asignada como a IP concreta.





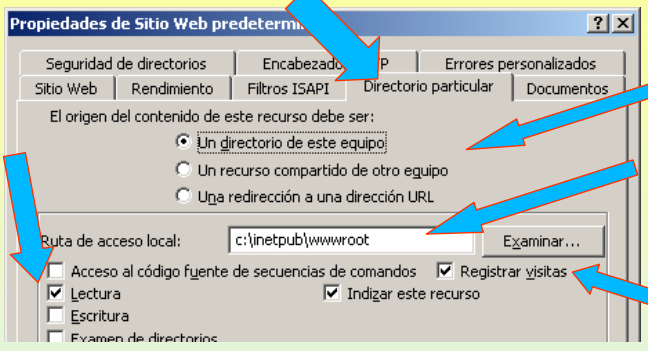
En avanzadas podemos configurar o Sitio para que responda a: varias IPs distintas, portos TCP distintos e encabezados distintos (esto último verase máis adiante)

Fixarse como agora o sitio web predeterminado tamén responde a url:
http://10.3.1.0:81 (Fixarse no porto, 81)

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

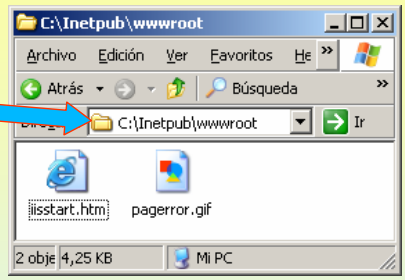
☞ Directorio do sitio web, rendemento.

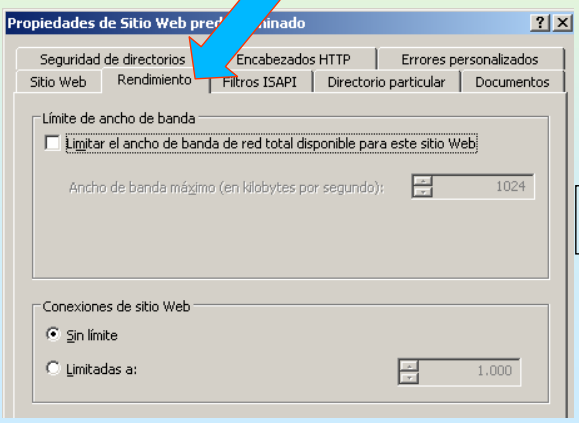


Observar onde podería estar almacenado o sitio WEB

Lugar onde están ubicadas ás páxinas e só se permite a lectura

As visitas van ser rexistradas no arquivo de log da diapositiva 74

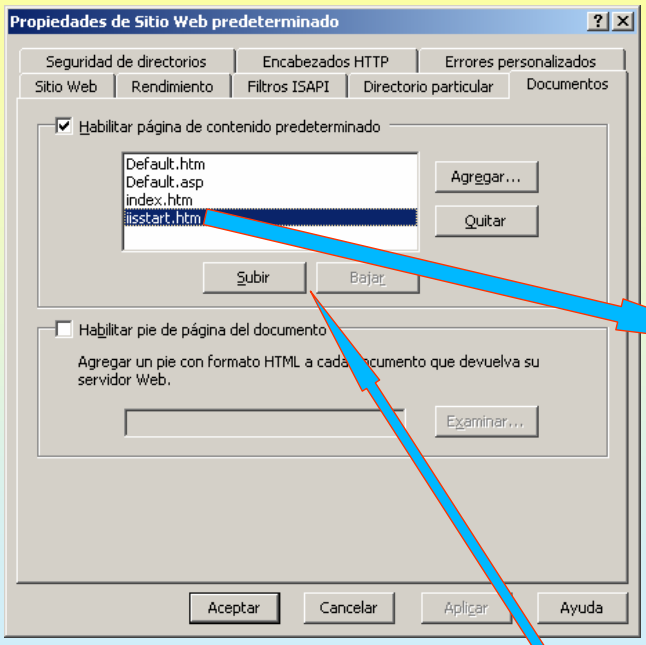


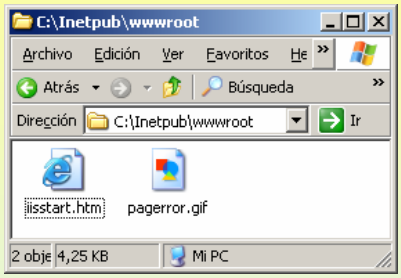


O sitio pódese limitar tanto en KB/seg ou en número de conexións simultáneas

5.- Servidor WEB

☞ Páxina predeterminada do stitio web





De tódalas páxinas que hai na carpeta do sitio Web indica cal é a que se debe cargar por defecto cando alguén se queira conectar ó sitio.

Se existise unha páxina chamada **Default.htm**, esta cargaríase antes que ningunha outra, e así sucesivamente.

Neste caso cando un navegador web se conecta a este sitio, este proporcionaralle a páxina **iistart.htm**, pois de tódalas posibles que podería enviar só existe na carpeta esa páxina.

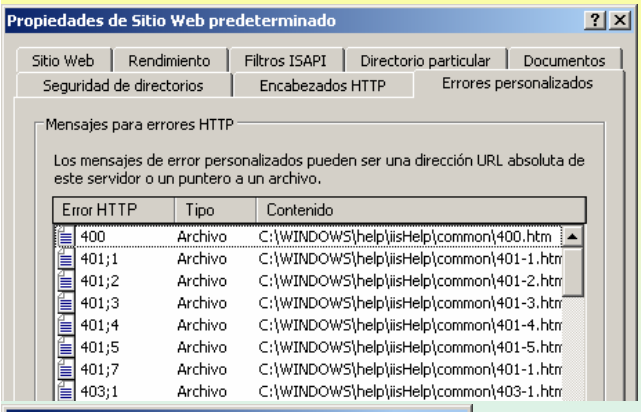
Tamén se pode alterar a orde coa que se van proporcionar as páxinas de inicio.

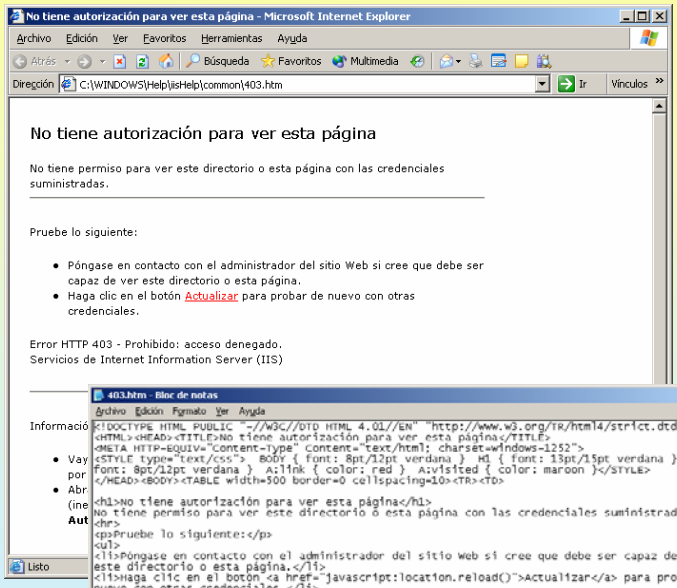
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

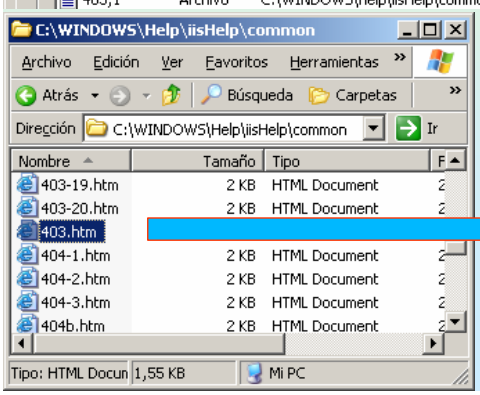
5.- Servidor WEB

☞ MENSAXES DE ERRO

As páxinas que informan de excepcións pódense configurar en **c:\windows\help\iishelp\common**





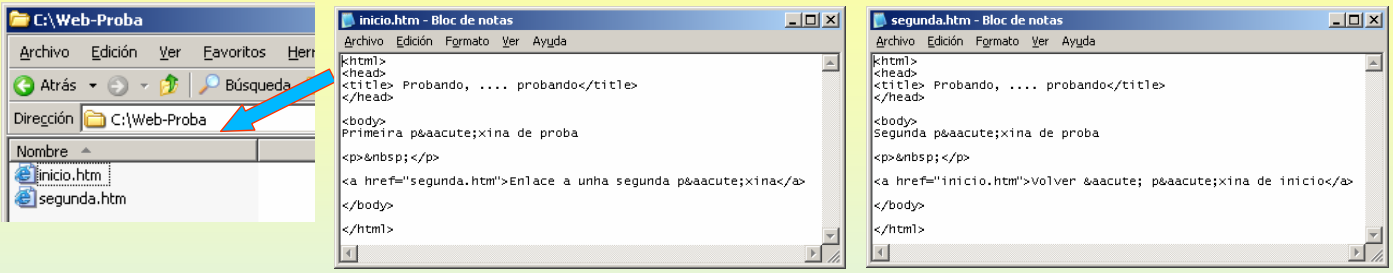


Arquivo aberto co bloc de notas no que se pode modificar a mensaxe de arriba

5.- Servidor WEB

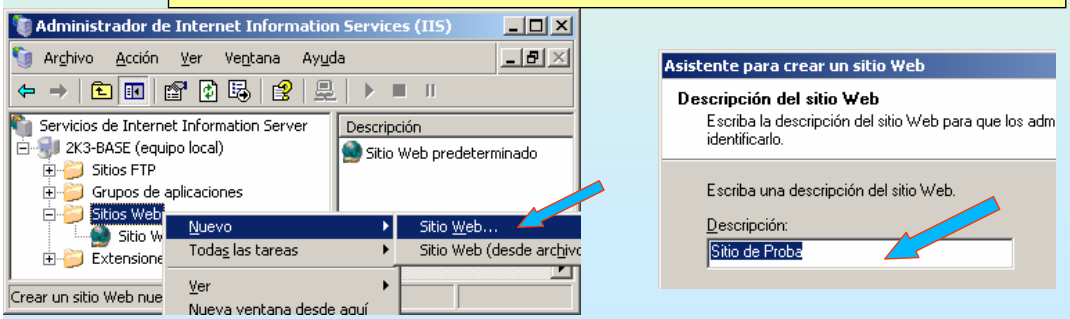
☞ CREAR UN SITIO WEB NOVO

Débese crear unha carpeta na que se albergarán os arquivos e logo crear un sitio novo indicando: ip, porto, encabezado, rota, ... Neste exemplo non se vai poñer encabezado, polo de agora.



Creamos unha carpeta e introducimos dous arquivos .htm

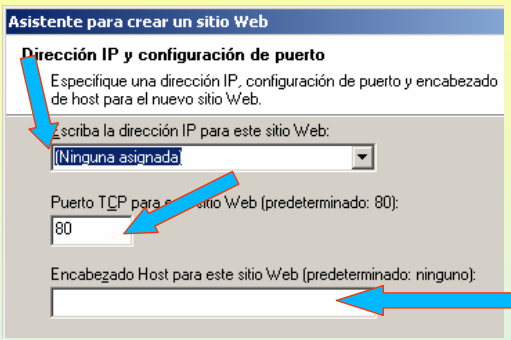
Crear un novo sitio web



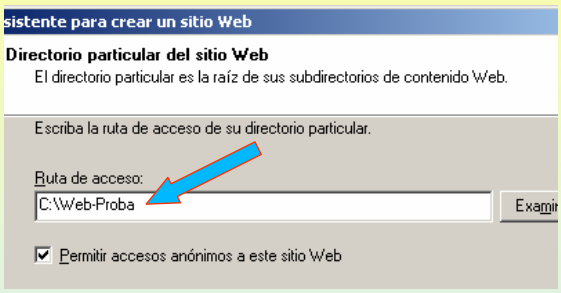
5.- Servidor WEB

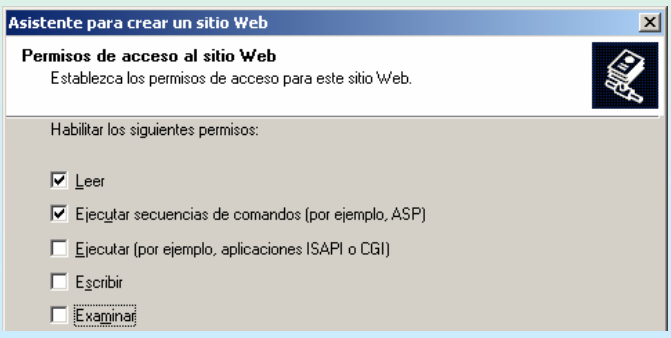
☞ CREAR UN SITIO WEB NOVO

O configurar IP e porto, neste exemplo, vanse deixar como veñen por defecto para observar os problemas que causa.



Notar que non se puxo ningún encabezado. O lóxico sería poñer un que estea dado de alta nun DNS, p.e.: **alcume.proba00.ga**





Deixar os permisos de acceso como veñen por defecto, máis adiante modificaranse

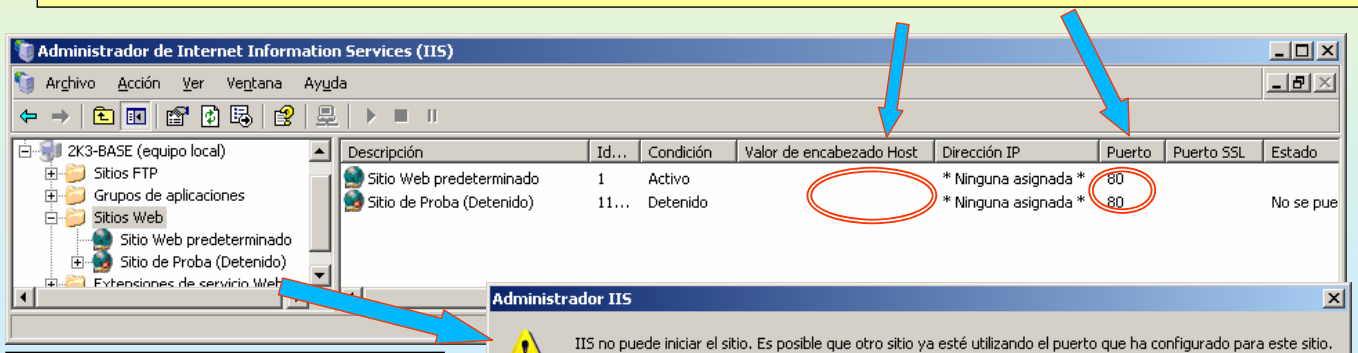
5.- Servidor WEB

☞ HABILITAR PERMISOS E FINALIZAR

Tras rematar o sitio esta detido, porque está traballando no mesmo porto que o sitio predeterminado. Neste caso non é preciso cambiar o novo sitio de porto. Logo se verá.

Un sitio web identifícase por:
IP.
Porto.
Encabezado (nome de dominio ou nome que se debe poñer logo no navegador)

Cando nun mesmo servidor residen varios sitios, que se desexan activos. Estes deben ter algún deses tres parámetros distintos. Neste caso coinciden os 3, IP, Porto e encabezado.



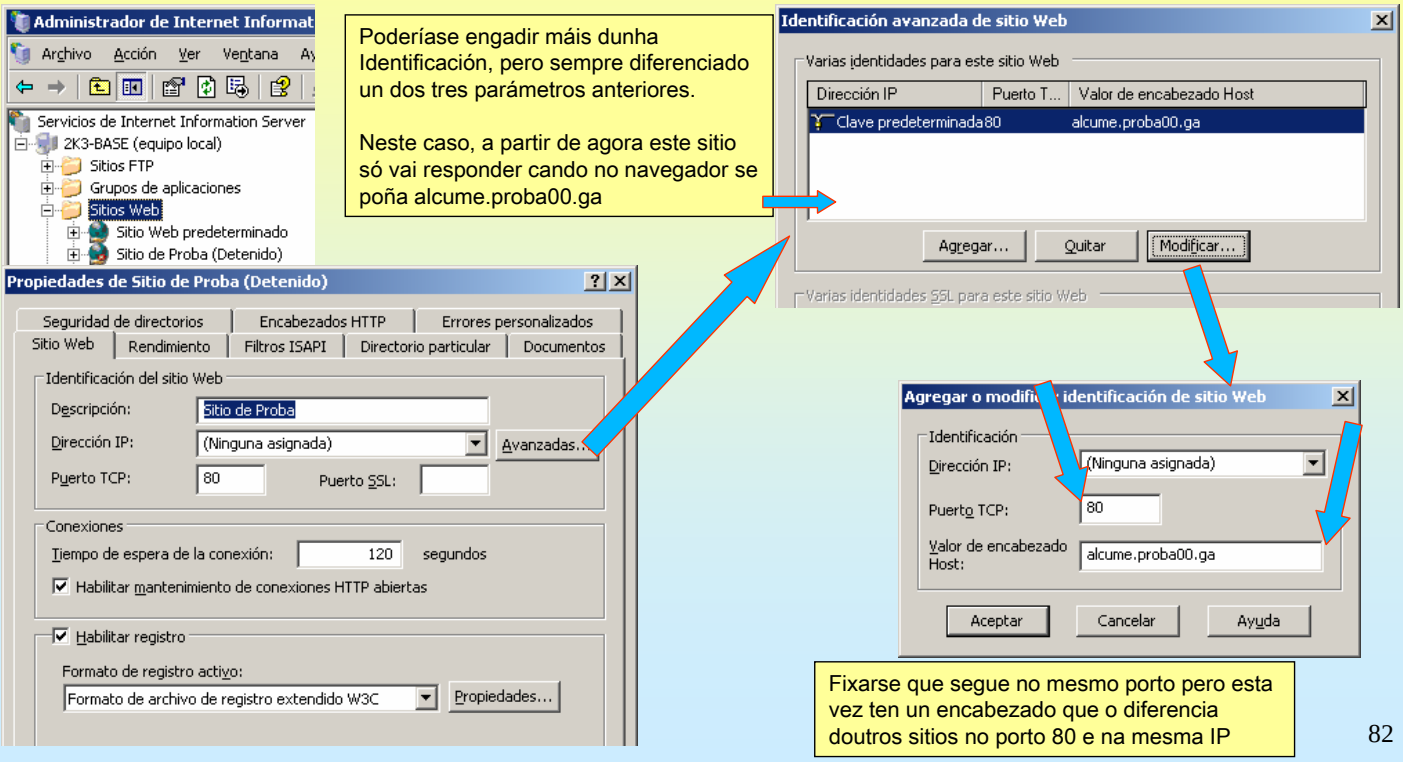
O sitio esta detido e o tratar de inicialo (botón dereito sobre el→ **iniciar**) advirte do que está a acontecer

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ CONFIGURAR O ENCABEZADO DUN SITIO WEB

Neste caso, ó novo sitio web váiselle poñer un escabezado que xa se debeu poñer cando se creou (transparencia 79)



Poderíase engadir máis dunha Identificación, pero sempre diferenciado un dos tres parámetros anteriores.

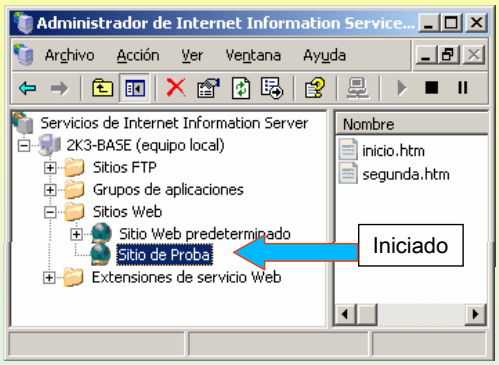
Neste caso, a partir de agora este sitio só vai responder cando no navegador se poña alcume.proba00.ga

Fixarse que segue no mesmo porto pero esta vez ten un encabezado que o diferencia doutros sitios no porto 80 e na mesma IP

5.- Servidor WEB

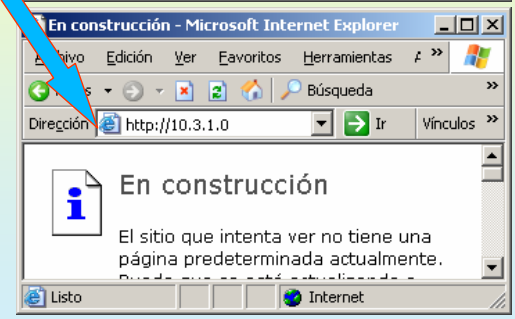
☞ DIFERENCIAS ENTRE USAR NA URL O ENCABEZADO DUN SITIO OU OUTRA COUSA

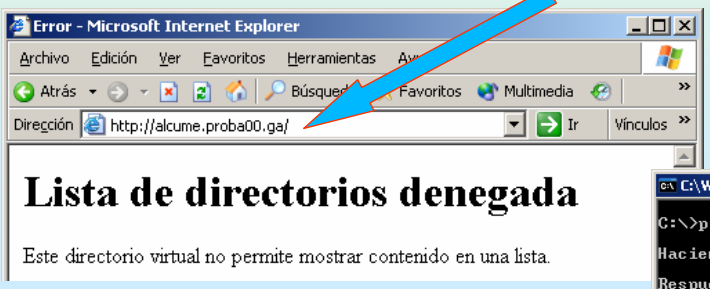
Observar as seguintes diferencias ó conectarse dende un cliente.

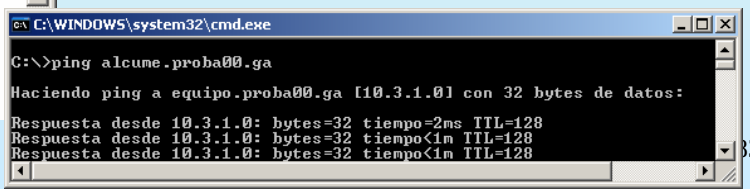


Nos dous casos se conecta ó sitio predeterminado, pois o que se envía na URL (Encabezado) non coincide co encabezado do Sitio de Proba

Ó conectarse a: **alcume.proba00.ga** responde o Sitio de Proba, pero aínda así non nos carga ningunha páxina





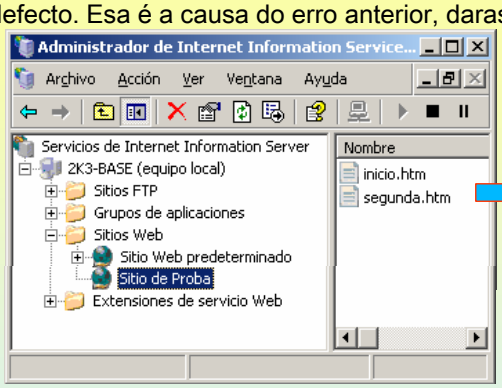


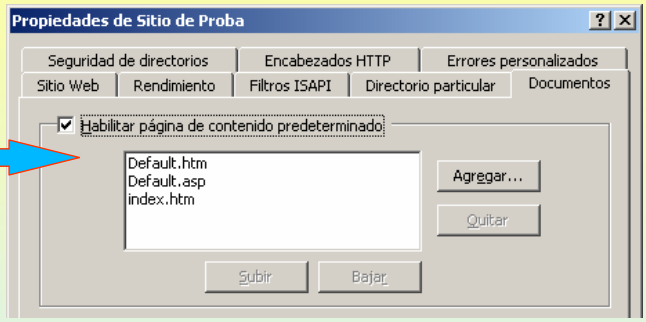
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

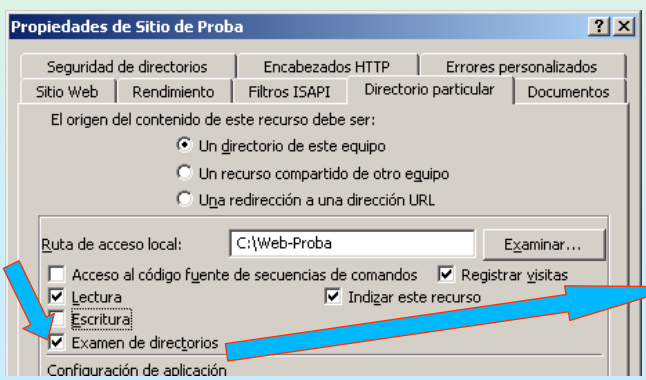
5.- Servidor WEB

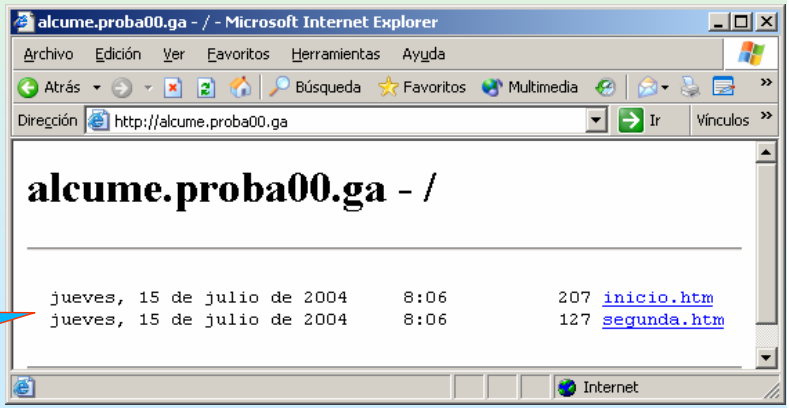
☞ SOLUCIONAR O PROBLEMA ANTERIOR

Como se pode observar ningunha das dúas páxinas do Sitio de Proba coincide coas páxinas que debe cargar o sitio por defecto. Esa é a causa do erro anterior, darase unha solución, que consiste en mostrar o contido do sitio (**examinar**)









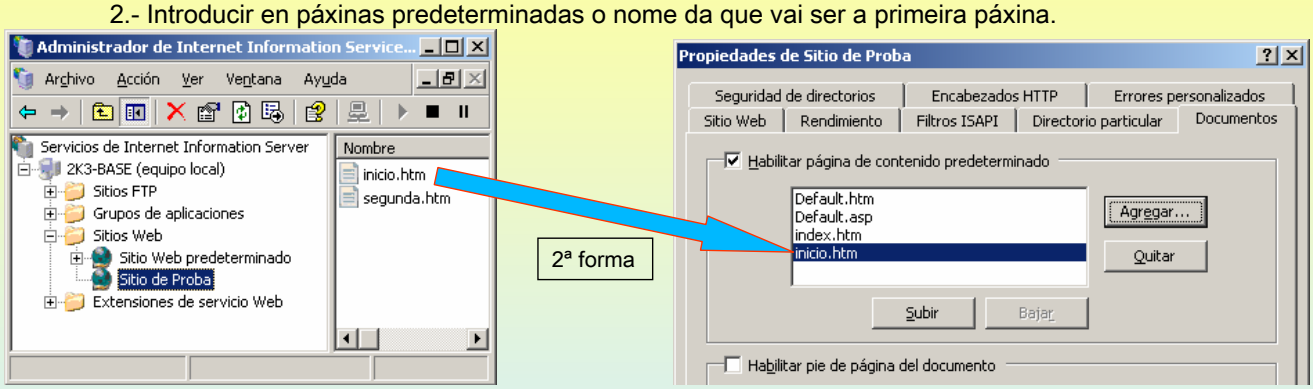
5.- Servidor WEB

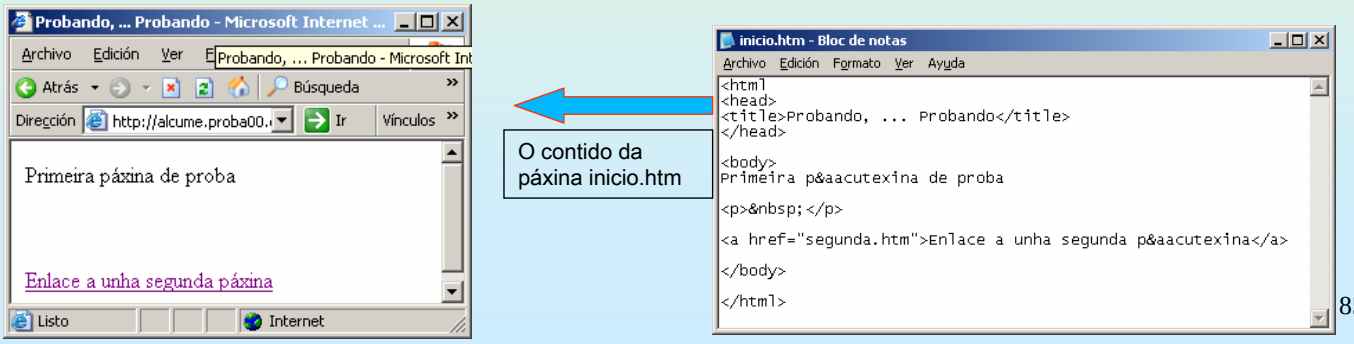
☞ CONFIGURAR PÁXINA DE INICIO POR DEFECTO

Pódese realizar de dúas formas:

1.- O nome da primeira páxina que sexa: **default.htm, default.asp ou index.htm**.

2.- Introducir en páxinas predeterminadas o nome da que vai ser a primeira páxina.





SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ DIRECTORIOS VIRTUAIS, ALIAS

Para publicar nun sitio web dende calquera directorio que non estea no directorio principal do sitio, débese crear un **directorio virtual**. Este é un directorio que non está contido no directorio particular, pero nos navegadores aparecerá como si o estivera.

Os directorios virtuais teñen alias, o nome que se usará nos exploradores para ter acceso a ese directorio.

Exemplos:
Crearemos varios directorios, uns virtuais e outros non, dentro do **Sitio web de Proba**

Directorio físico	Virtual	Tipo	Alias	URL
C:\web-proba	Non	Directorio do sitio	- - -	http://alcume.proba00.ga
C:\web-proba\dentro	Non	Directorio dentro do do sitio	- - -	http://alcume.proba00.ga/dentro
C:\paxinas	Si	Directorio fóra do do sitio	fora	http://alcume.proba00.ga/fora
\\ordenador\carpeta	Si	Directorio noutro ordenador	noutro	http://alcume.proba00.ga/noutro
http://www.google.es	Si	Apunta a outro sitio web	google	http://alcume.proba00.ga/google

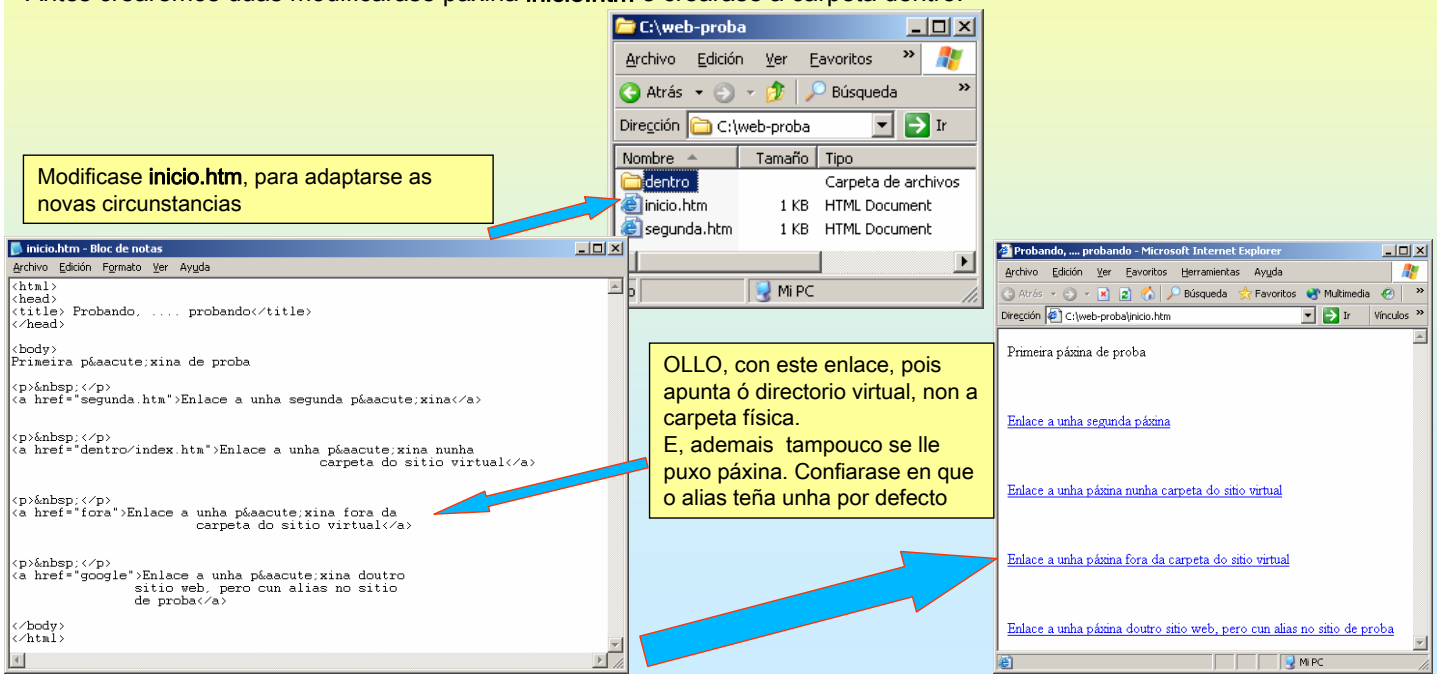
5.- Servidor WEB

☞ CREAR UN DIRECOTIO NON VIRTUAL

Comezarase creado o seguinte directorio anterior.

Directorio físico	Virtual	Tipo	Alias	URL
C:\web-proba\dentro	Non	Directorio dentro do do sitio	- - -	http://alcume.proba00.ga/dentro

Antes crearemos dúas modificarase páxina **inicio.htm** e crearase a carpeta dentro.



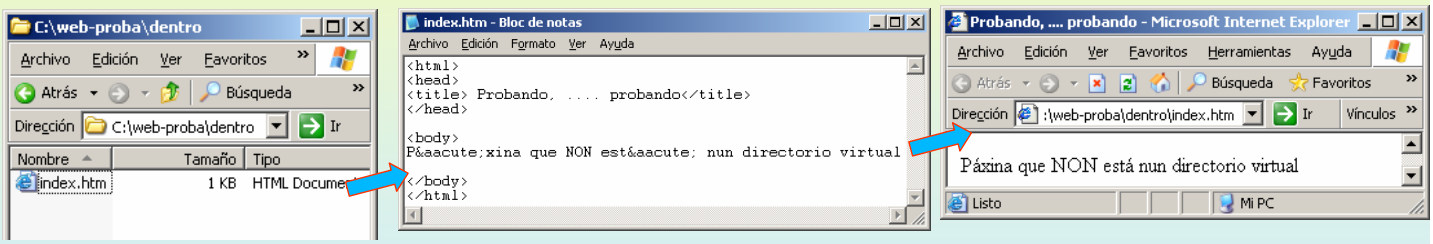
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ CREAR UN DIRECTORIO NON VIRTUAL

Directorio físico	Virtual	Tipo	Alias	URL
C:\web-proba\dentro	Non	Directorio dentro do do sitio	- - -	http://alcume.proba00.ga/dentro

Agora crearase a páxina **index.htm** dentro da carpeta c:\web-proba\dentro

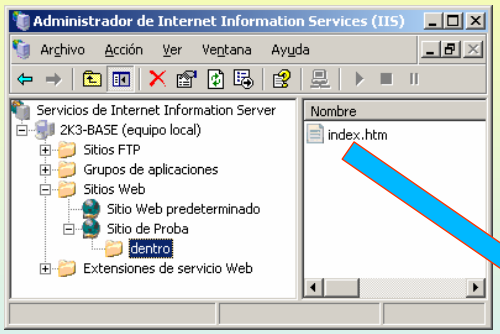


5.- Servidor WEB

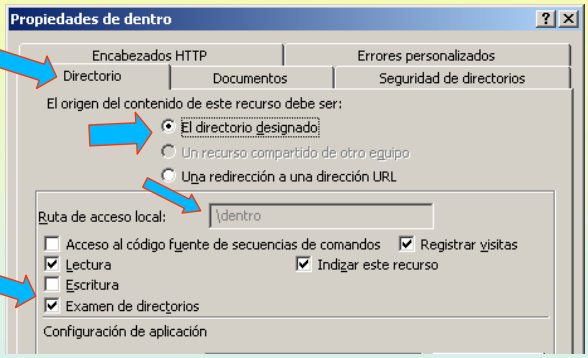
☞ CREAR UN DIRECTORIO NON VIRTUAL

Directorio físico	Virtual	Tipo	Alias	URL
C:\web-proba\dentro	Non	Directorio dentro do do sitio	- - -	http://alcume.proba00.ga/dentro

Sen facer nada en **Stio de Proba** xa aparece a carpeta cos seus documentos.Observar as propiedades desa carpeta.

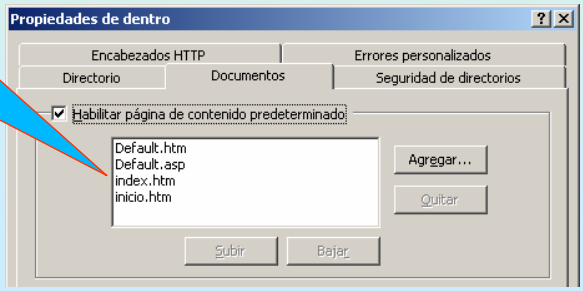


Herda as propiedades do sitio pai..
Fixarse no directorio e no exame de directorios.



A paxina que se creou púxoselle **index.htm**, porque unha das que por defecto está nos documentos de inicio.

Notar como tamén herdou **inicio.htm** do pai.



SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

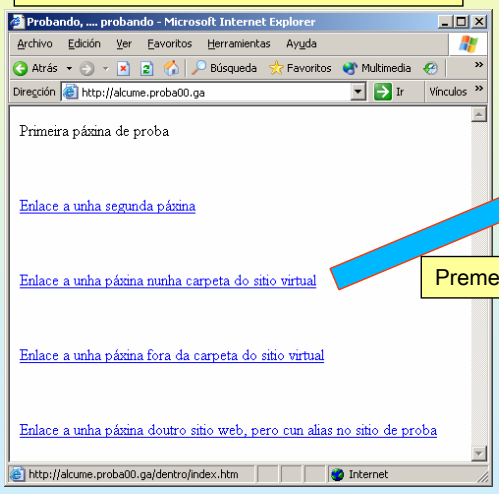
5.- Servidor WEB

☞ CREAR UN DIRECTORIO NON VIRTUAL

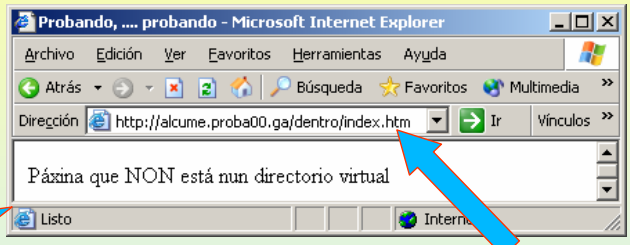
Directorio físico	Virtual	Tipo	Alias	URL
C:\web-proba\dentro	Non	Directorio dentro do do sitio	- - -	http://alcume.proba00.ga/dentro

Finalmente comprobar que funciona. Usaranse dous métodos.

PRIMEIRA FORMA
Conectarse ó servidor web e logo premer no enlace correspondente

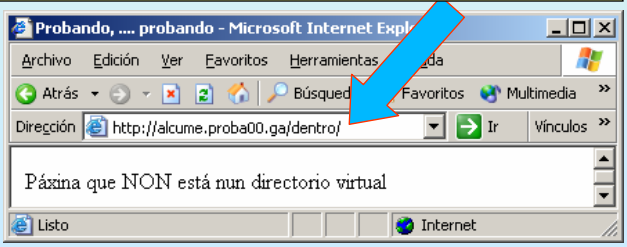


Premer



Notar como mostra o nome da páxina

OUTRA FORMA
Poñendo a ruta completa, sen ter que indicar a páxina, pois esta xa está nos documentos predeterminados de inicio



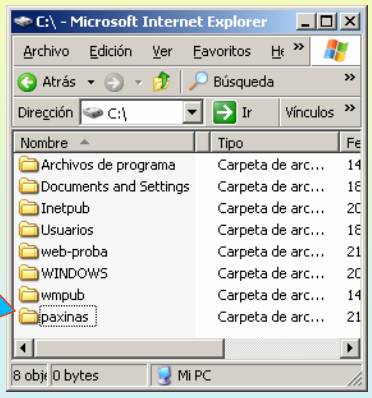
5.- Servidor WEB

☞ CREAR UN DIRECTORIO VIRTUAL

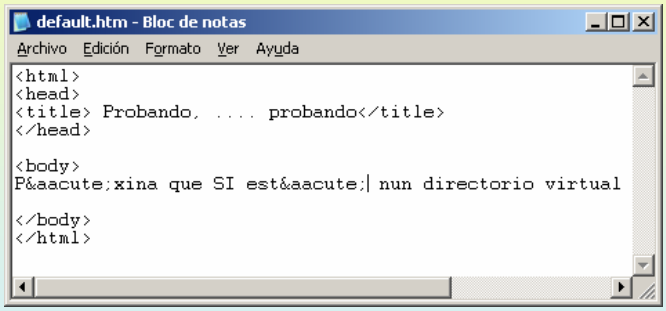
Directorio físico	Virtual	Tipo	Alias	URL
C:\paxinas	Si	Directorio fóra do do sitio	fora	http://alcume.proba00.ga/fora

Igual que no caso anterior comezarase creando a carpeta e a páxina, neste caso, **default.htm** (tamén se podería chamar index.htm, ou como se quixese)

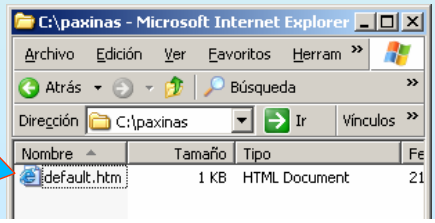
Crear a carpeta en c:\

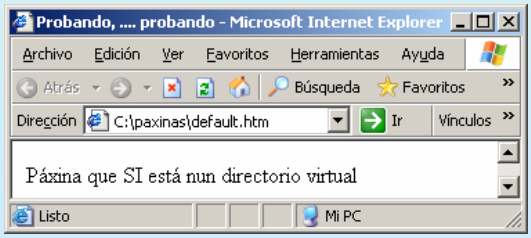


Créase a páxina **default.htm** en c:\paxinas



Crear a páxina default.htm





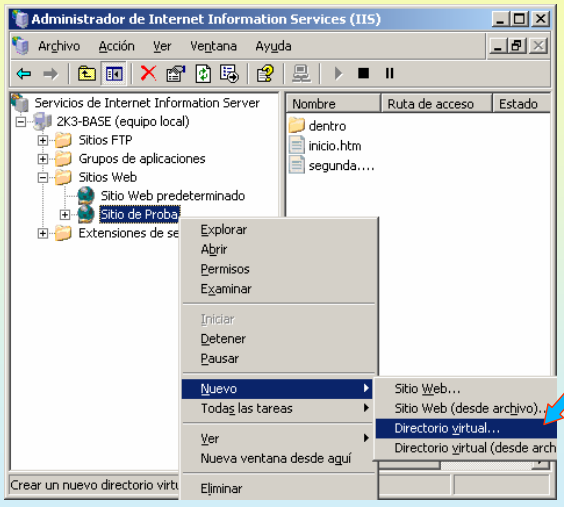
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

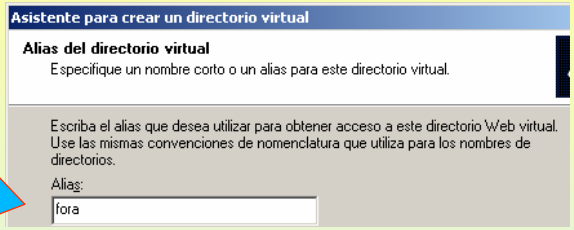
☞ CREAR UN DIRECTORIO VIRTUAL

Directorio físico	Virtual	Tipo	Alias	URL
C:\paxinas	Si	Directorio fóra do do sitio	fora	http://alcume.proba00.ga/fora

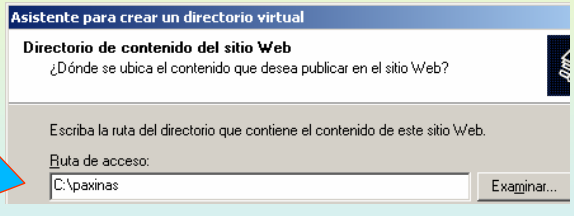
Crear o directorio virtual / alias no **Sitio web de proba**



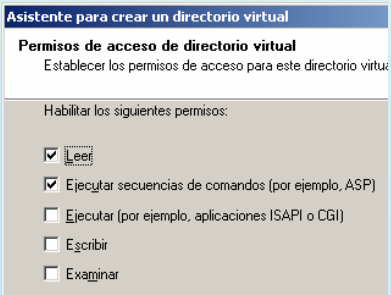
Nome do alias



Directorio físico



Permisos por defecto

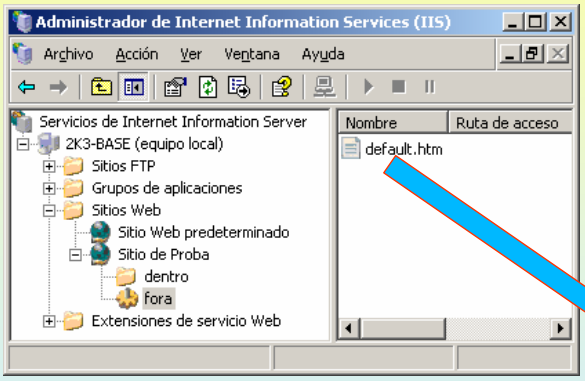


5.- Servidor WEB

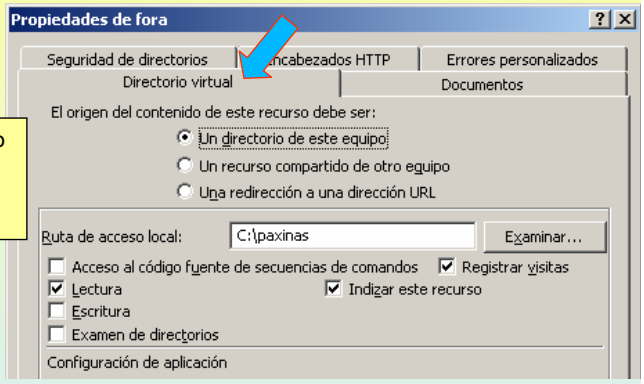
☞ CREAR UN DIRECTORIO VIRTUAL

Directorio físico	Virtual	Tipo	Alias	URL
C:\paxinas	Si	Directorio fóra do do sitio	fora	http://alcume.proba00.ga/fora

Examinar as propiedades do novo directorio virtual

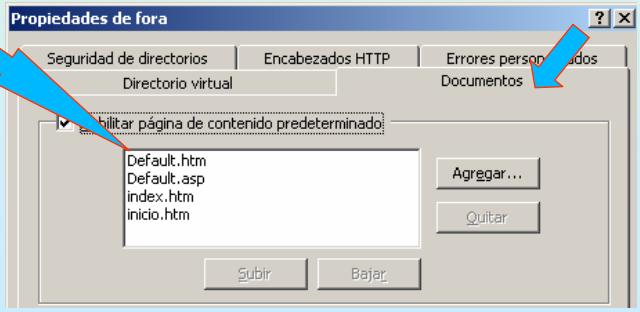


Observar o orixe do contido, rota de acceso e os permisos



A paxina que se creou púxoselle **default.htm**, porque unha das que por defecto está nos documentos de inicio.

Notar como tamén herdou **inicio.htm** do pai.



SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

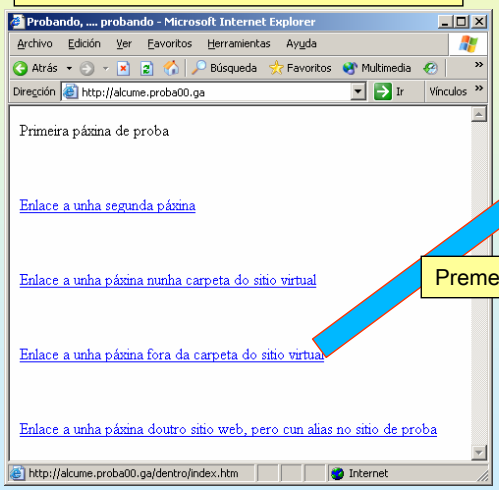
5.- Servidor WEB

☞ CREAR UN DIRECTORIO VIRTUAL

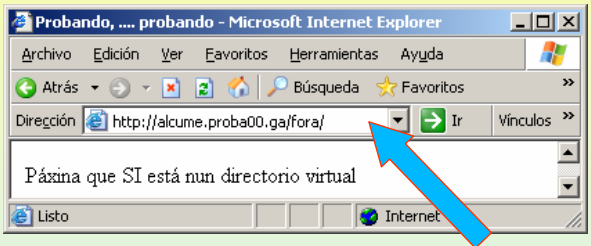
Directorio físico	Virtual	Tipo	Alias	URL
C:\paxinas	Si	Directorio fóra do do sitio	fora	http://alcume.proba00.ga/fora

Finalmente, comprobar que tamén funciona. Igual que no caso anterior, farase de dúas formas.

PRIMEIRA FORMA
Conectarse ó servidor web e logo premer no enlace correspondente



Premer



Notar como NON mostra o nome da páxina, consulta o código html da páxina inicio.htm

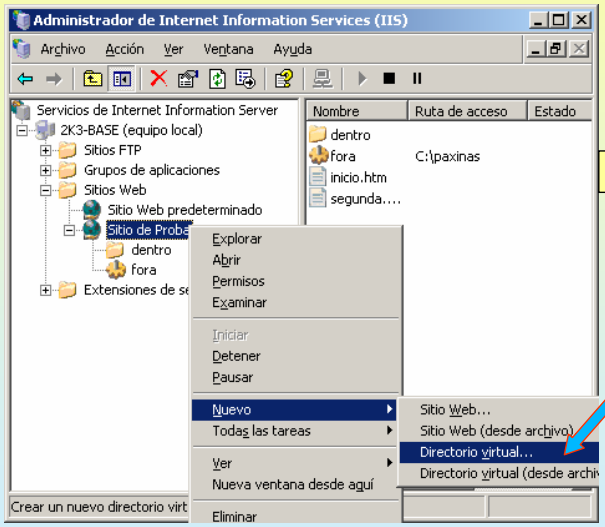
OUTRA FORMA
Poñendo a ruta completa, sen ter que indicar a páxina, pois esta xa está nos documentos predeterminados de inicio

5.- Servidor WEB

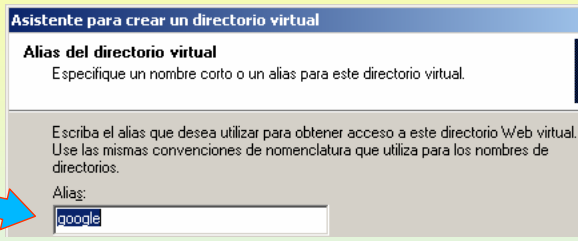
☞ CREAR UN DIRECTORIO VIRTUAL QUE APUNTE A OUTRO SITIO WEB. Redireccionar

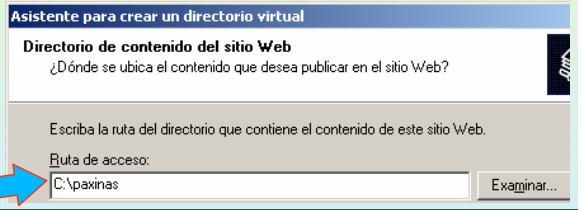
Directorio físico	Virtual	Tipo	Alias	URL
http://www.google.es	Si	Apunta a outro sitio web	google	http://alcume.proba00.ga/google

Neste caso comezamos creando o directorio virtual /alias dentro do **Sitio web de proba**

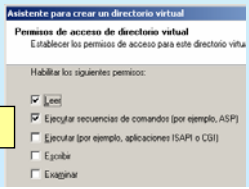


Nome do alias





Directorio físico, provisional, pois non deixa introducir http://www.google.es



Permisos por defecto

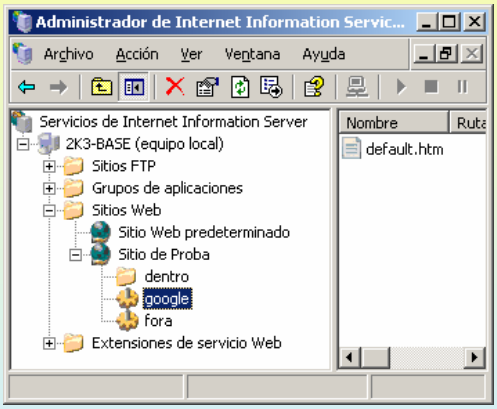
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

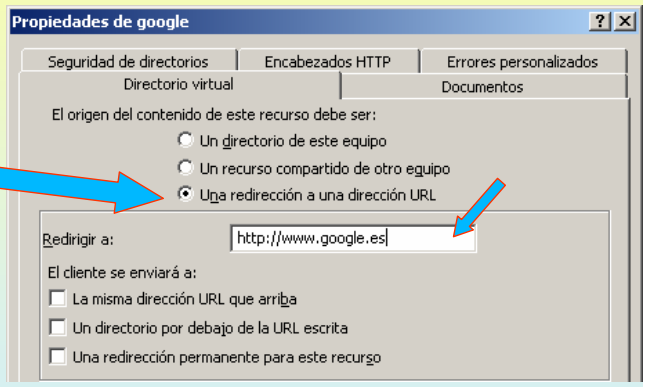
☞ CREAR UN DIRECTORIO VIRTUAL QUE APUNTE A OUTRO SITIO WEB. Redireccionar

Directorio físico	Virtual	Tipo	Alias	URL
http://www.google.es	Si	Apunta a outro sitio web	google	http://alcume.proba00.ga/google

Agora toca cambiar o directorio o que apunta o alias **google**.En propiedades do directorio virtual



Modificar a orixe do contido do directorio virtual



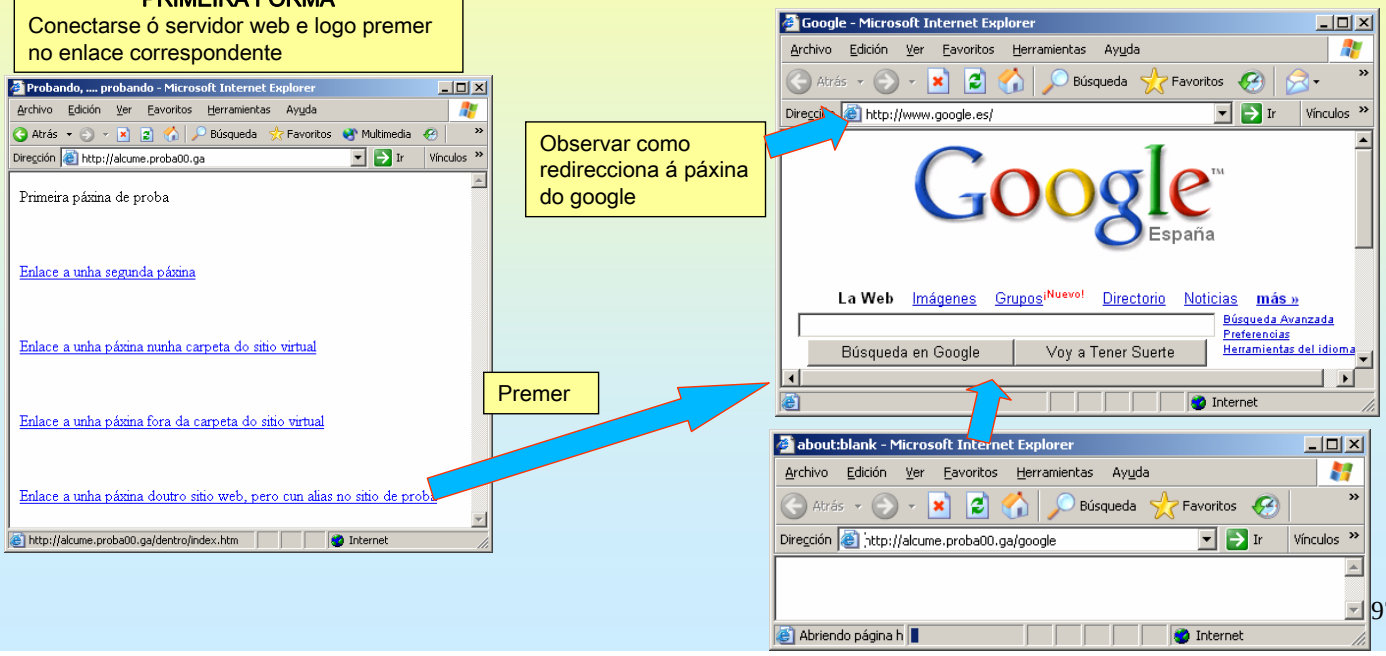
5.- Servidor WEB

☞ CREAR UN DIRECTORIO VIRTUAL QUE APUNTE A OUTRO SITIO WEB. Redireccionar

Directorio físico	Virtual	Tipo	Alias	URL
http://www.google.es	Si	Apunta a outro sitio web	google	http://alcume.proba00.ga/google

Probaremos, finalmente, neste caso redireccionarase ó web de google.

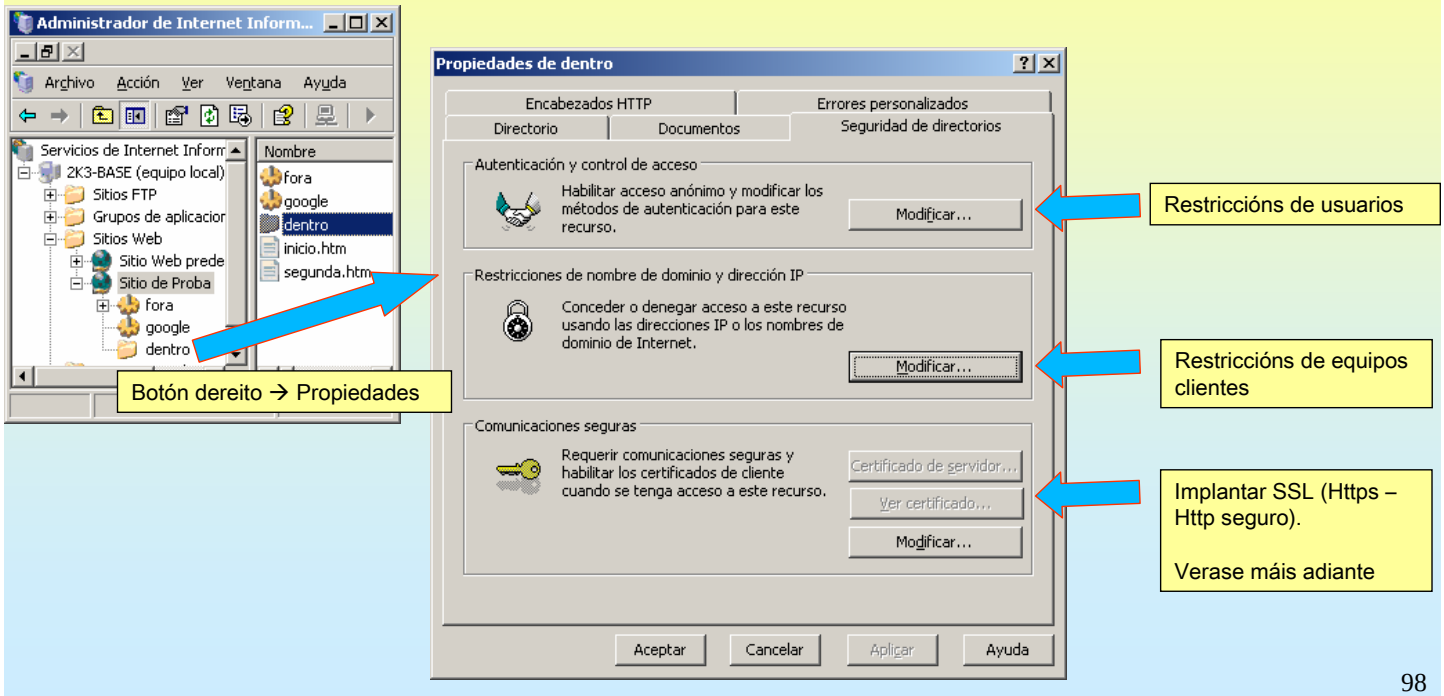
PRIMEIRA FORMA
Conectarse ó servidor web e logo premer no enlace correspondente



5.- Servidor WEB

☞ RESTRICCIÓNS E PERMISOS

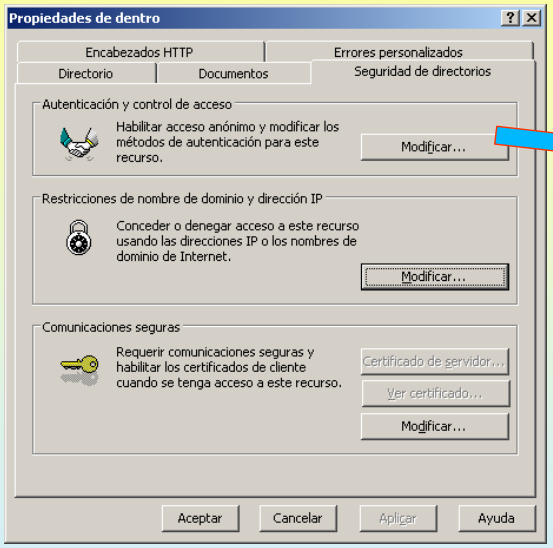
Tanto a un sitio web, coma a unha carpeta ou a un directorio se lle poden configurar opcións de seguridade.
Neste exemplo usarase a carpeta dentro para realizar as prácticas.



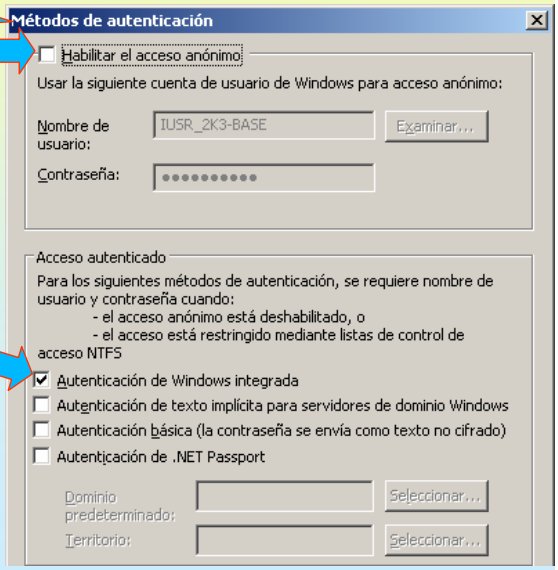
5.- Servidor WEB

☞ RESTRICCIÓNS E PERMISOS: Usuarios

Neste exemplo só se vai permitir a usuarios dos sistema e non a a usuarios anónimos



Por defecto está activada esta opción. Por eso non pide nome de usuario ó tratar de entrar.



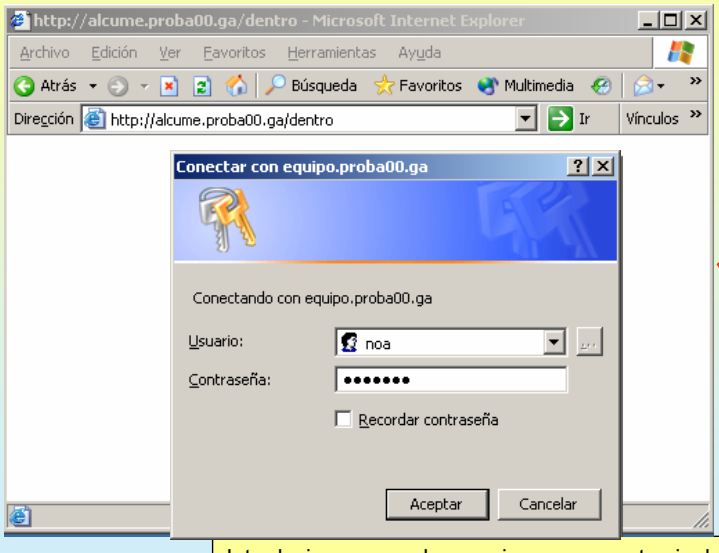
Dende agora só se permitiran os usuarios dados de alta no sistema.

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

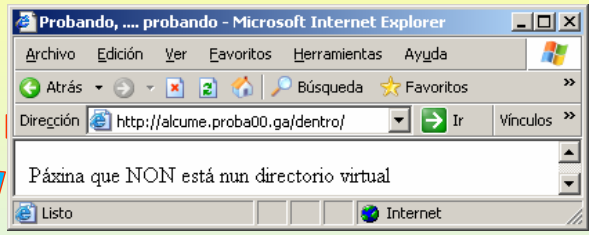
5.- Servidor WEB

☞ RESTRICCIÓNS E PERMISOS: Usuarios

Agora para entrar pide o nome dun usuario do sistema



Introducir un nome do usuario e o seu contrasinal

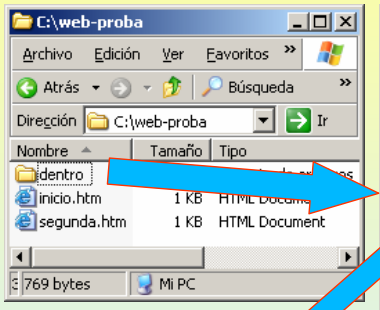


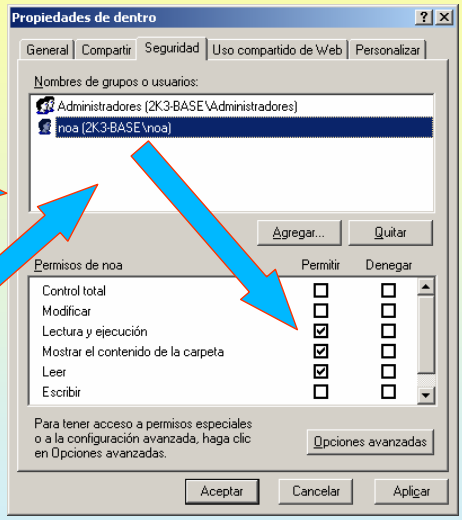
Dende agora só se permitiran os usuarios dados de alta no sistema.

5.- Servidor WEB

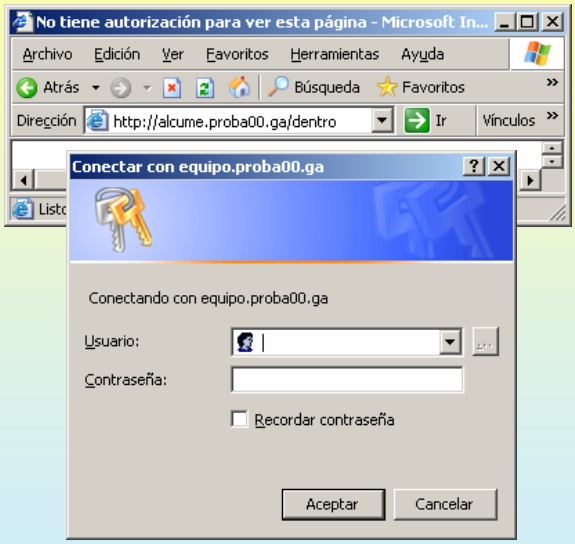
☞ RESTRICCIÓNS E PERMISOS: Usuarios

Agora para só se vai deixar entrar a NOA na carpeta de dentro.
Para elo usaremos a configuración da diapositiva 99, e ademais afinaranse os permisos na propia carpeta física.





Nesta ACL de seguridade deixanse só os usuarios/grupos ós que se lles concede acceso



So poden validarse NOA e usuarios que pertenzan o grupo Administradores.

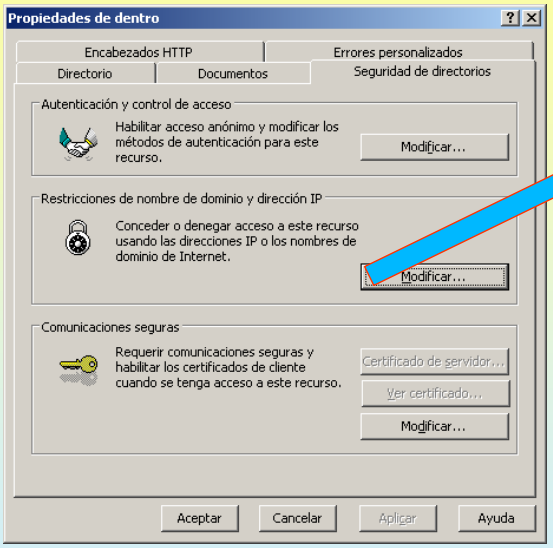
Probar con Pia

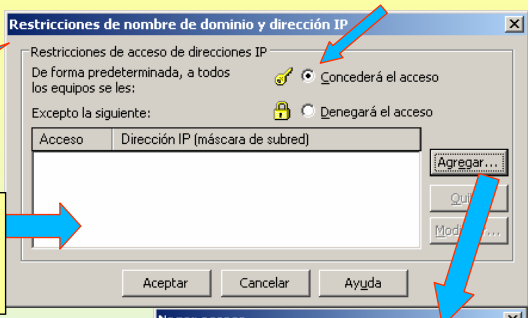
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

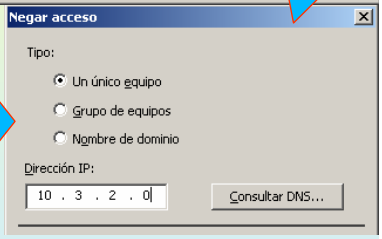
☞ RESTRICCIÓNS E PERMISOS: Equipos (nomes dominio / IPs)

Prohibirase a conexión a alcume.proba00.ga/dentro dende a IP 10.3.2.0

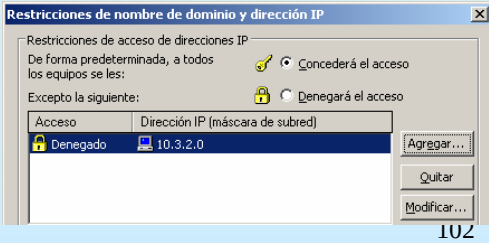




De forma predetermina concedese o acceso excepto a: (quen estea neste cadro branco)



Observar que tipos de negación de acceso se poden realizar

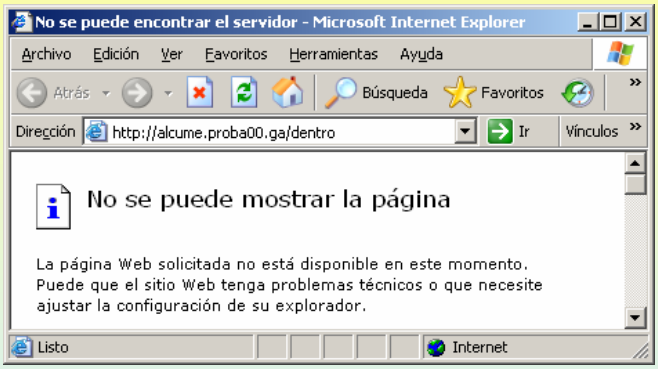


De forma predetermina concedese o acceso excepto á IP 10.3.2.0

5.- Servidor WEB

☞ **RESTRICCIÓNS E PERMISOS: Equipos (nomes dominio / IPs)**

Probase dende 10.3.2.0 e comprobase que denega o acceso.



5.- Servidor WEB

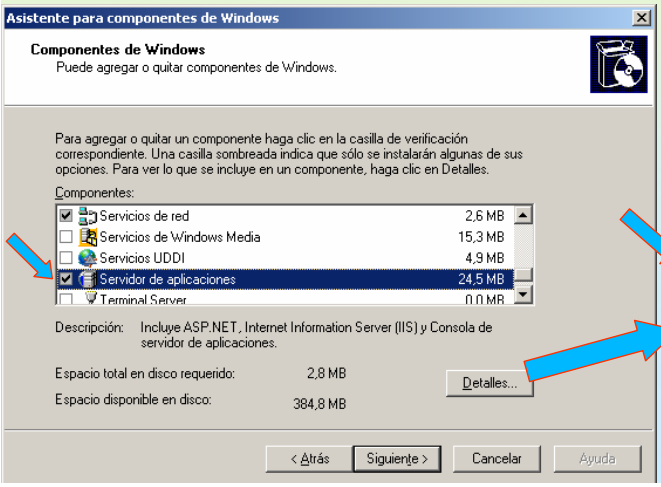
☞ **IMPRESIÓN DE INTERNET, ADMINISTRACIÓN REMOTA e CONEXIÓN WEB A ESCRITORIO REMOTO**

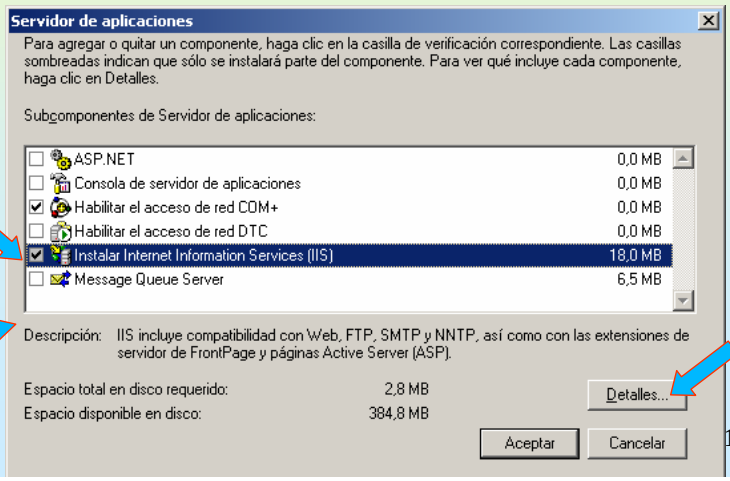
☞Nas seguintes diapositivas vanse instalar algunhas utilidades WEB que veñen co IIS, a saber:

Impresión de Internet: Permítelle a un equipo, que comparta impresoras, publicalas a través do web

Administración remota: esta utilidade permite xestionar vía web un equipo. Este debe ter instalada esta utilidade.

Conexión web a escritorio remoto: Aquel equipo que permita conexións a escritorio remoto (terminal server) (véxase os apuntes sobre Terminal Server en Windows 2003) e teña esta utilidade instalada, permitirá conexións de escritorio remoto vía web.

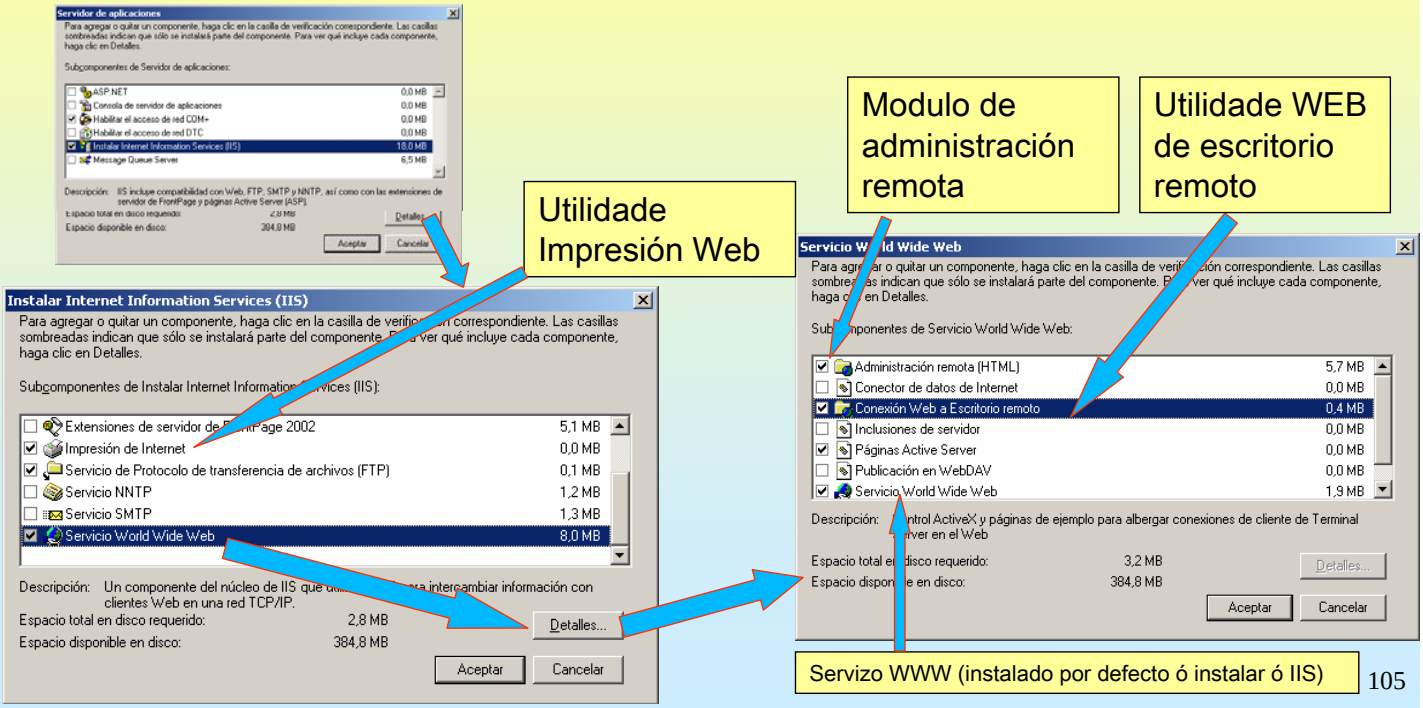




5.- Servidor WEB

☞ IMPRESIÓN DE INTERNET, ADMINISTRACIÓN REMOTA e CONEXIÓN WEB A ESCRITORIO REMOTO

Cada un deles poderíase instalar por separado, pero neste caso vanse instalar os tres módulos á vez.



SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ CONFIGURACIÓN DO IIS TRAS A INSTALACIÓN DAS TRES UTILIDADES ANTERIORES

O IIS conta con dous Sitios Web instalador por el.

- **PREDETERMINADO**: Está escoitando no porto 80

  Aparte de ser o sitio web predeterminado, dispón de dous directorio Virtuais:

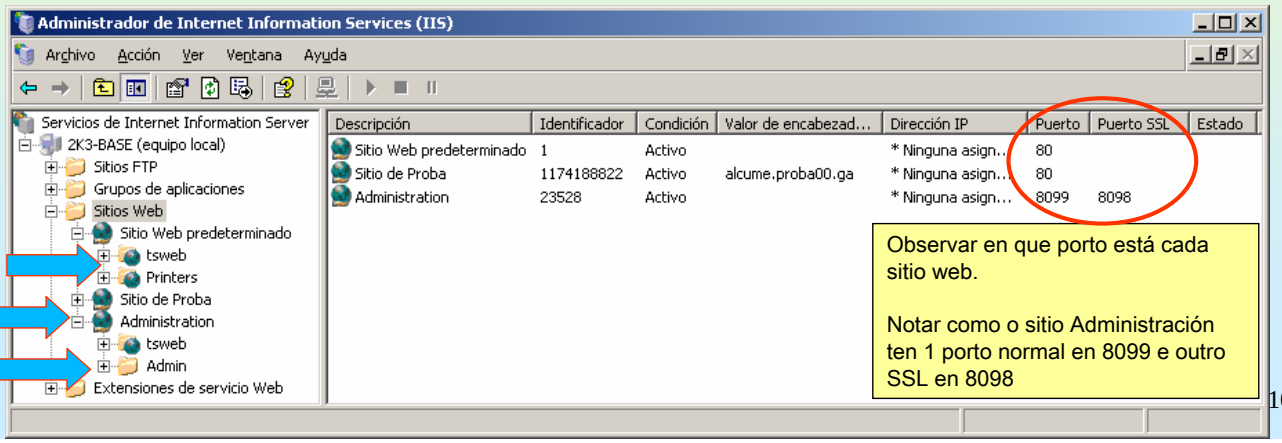
  tsweb: servidor de TS (Escritorio remoto) pero a través do web

  Printers: mostra as impresoras compartidas das que dispón o equipo, para poder instalalas nun cliente a través do web.

- **ADMINISTRACIÓN**: Escoita no porto 8098

  Usa Security Socket Layer (**SSL**) (https) para que o intercambio de información entre o navegador do cliente e o servidor vaia cifrada, deste xeito obtense un intercambio seguro.

  Serve para administrar o equipo dende un navegador web.



5.- Servidor WEB

☞ ADMINISTRACIÓN REMOTA DO SERVIDOR

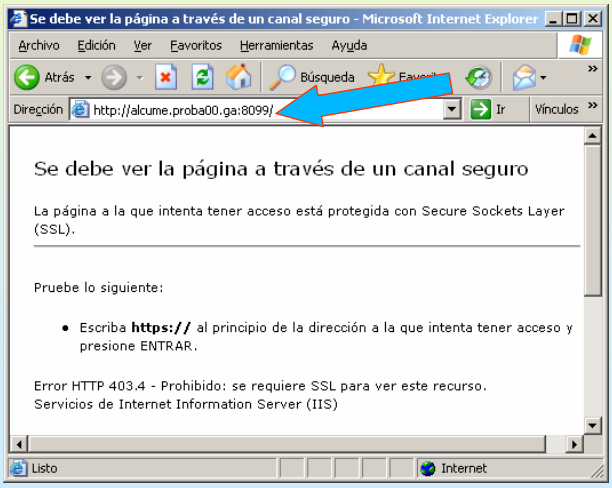
Pódense administrar: Usuarios, Sitios Web, etc ... OLLO CO PROTOCOLO DE CONEXIÓN: **HTTPS**

Observar que o sitio de administración atende en 2 portos

8099 → sen seguridade → http

8098 → con seguridade SSL → https

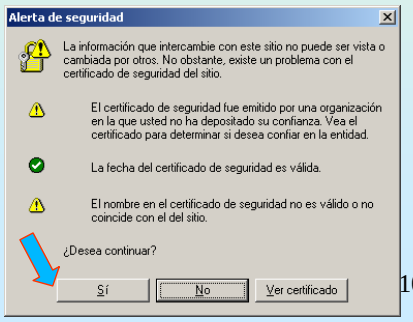
Neste caso o cliente esta conectado ó porto 8099 e a paxina advirte de que hai que usar un cal seguro (cifrado) SSL



Neste caso a conexión é usando https (SSL)e o porto 8098

As conexións SSL precisan dun certificado, que se estudiarán no próximo tema.

Premer en SI

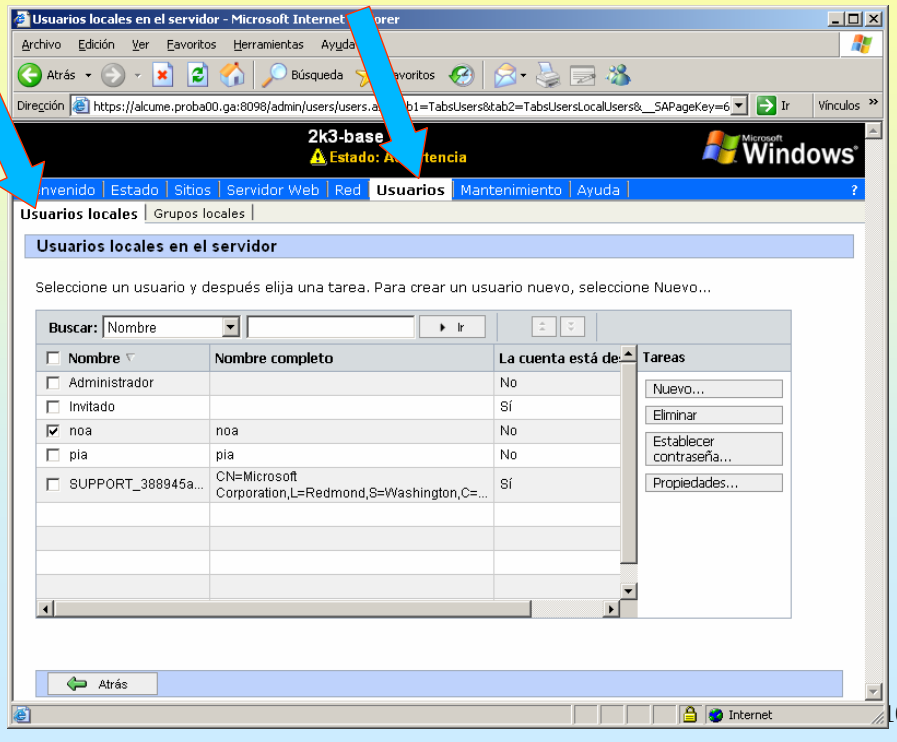


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ ADMINISTRACIÓN REMOTA DO SERVIDOR

Para conectarse pide un nome de usuario e contrasinal, este debe pertencer ó grupo de administradores.



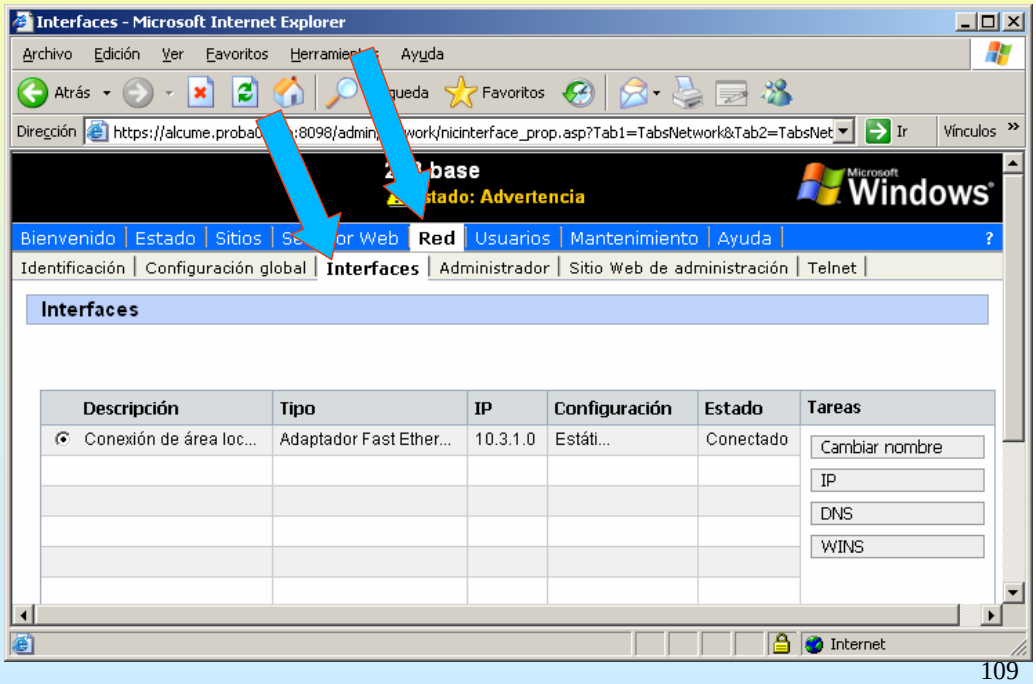
Nesta imaxe móstrase como se poden xestionar os usuarios a través do web.

5.- Servidor WEB

☞ ADMINISTRACIÓN REMOTA DO SERVIDOR

Máis exemplos. Xestión de interfaces de rede

Nesta imaxe móstrase como se poden xestionar os interfaces de rede (As tarxetas), IPs, DNS, etc.



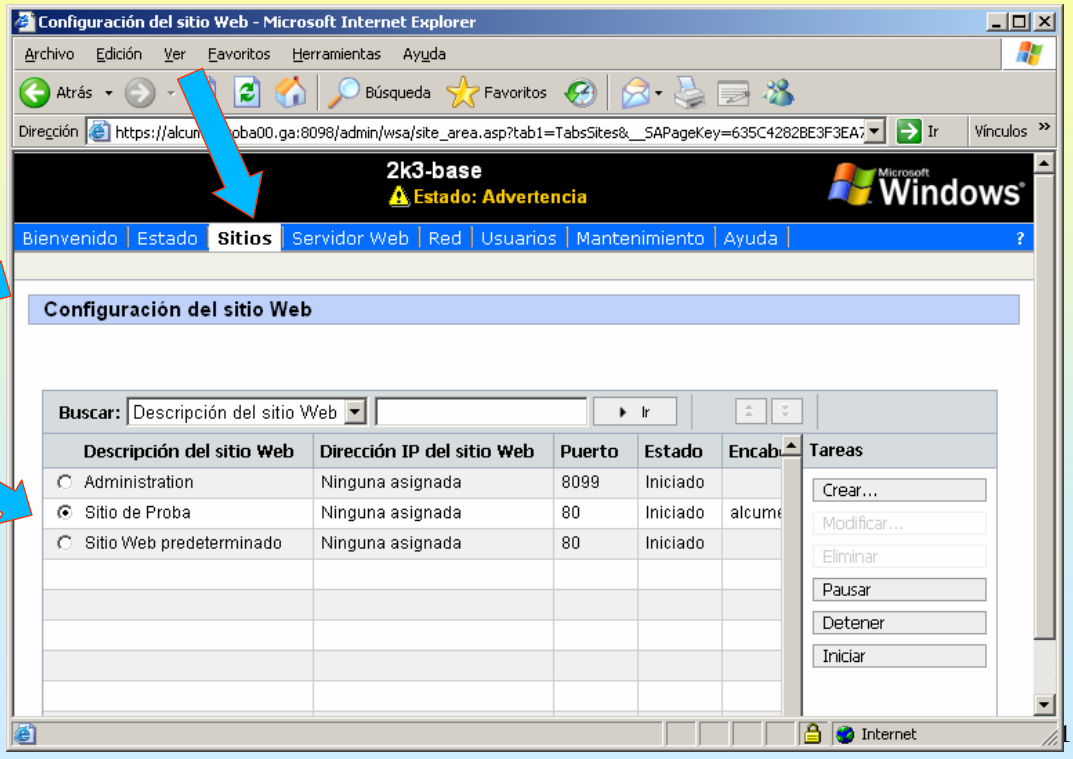
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ ADMINISTRACIÓN REMOTA DO SERVIDOR

Máis exemplos. Xestión dos sitios web creados previamente.

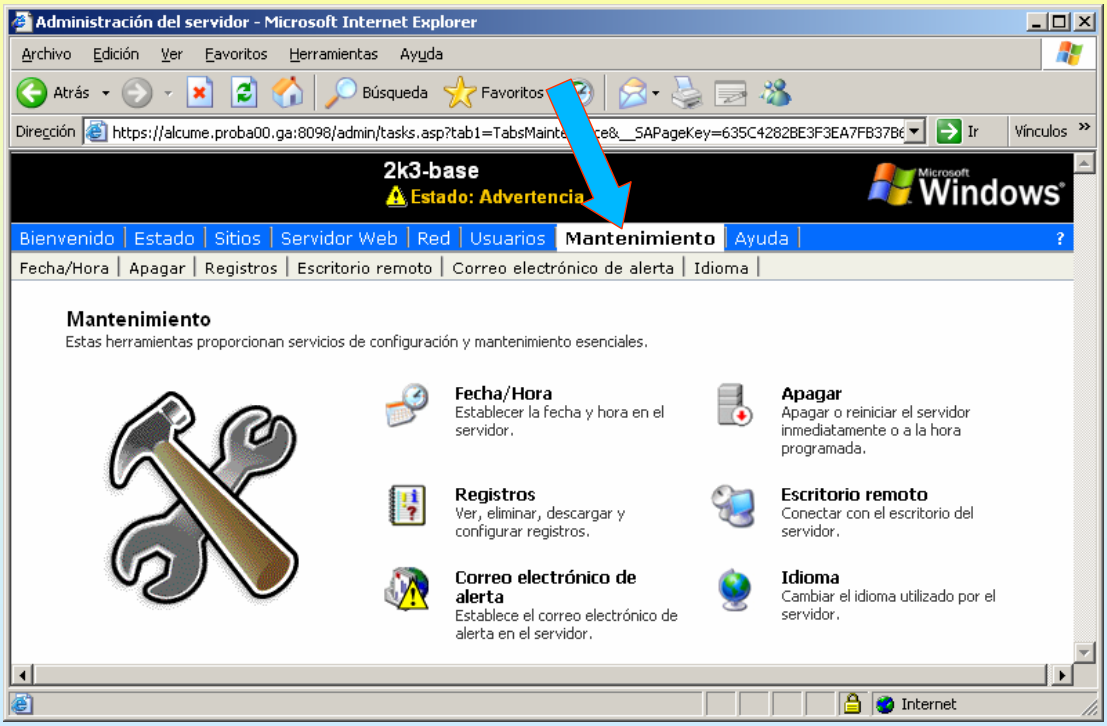
Nesta imaxe móstrase como se poden xestionar os sitios web.



5.- Servidor WEB

☞ ADMINISTRACIÓN REMOTA DO SERVIDOR

Máis exemplos. Finalmente, operacións de mantemento que se poden realizar



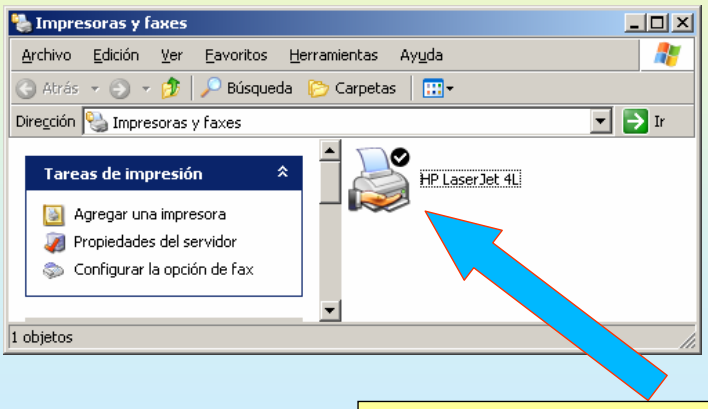
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ INSTALAR UNHA IMPRESORA A TRAVÉS DO WEB

Só é preciso ter un servidor de impresoras (estas deben estar compartidas) e conectarse ó web do servidor.
O servidor pode ser 2003 ou XP. Hai que ter o IIS instalado có módulo de Impresión Internet e compartir 1 impresora como mínimo.

Neste caso vaise instalar unha impresora e compartila. Logo tratarase de conectar ó cliente a través do web

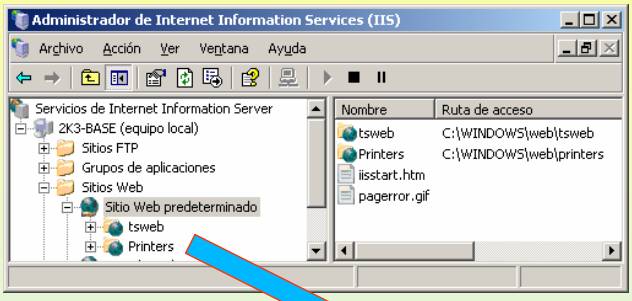


Impresora instalada localmente e compartida

5.- Servidor WEB

☞ INSTALAR UNHA IMPRESORA A TRAVÉS DO WEB

Só é preciso ter un servidor de impresoras (estas deben estar compartidas) e conectarse ó web do servidor.



Acceder vía web á impresora. Notar que se accede pola IP, pero poderíase acceder, polos nomes de dominio, nome de equipo, etc, con tal de que resolvan na IP dese equipo

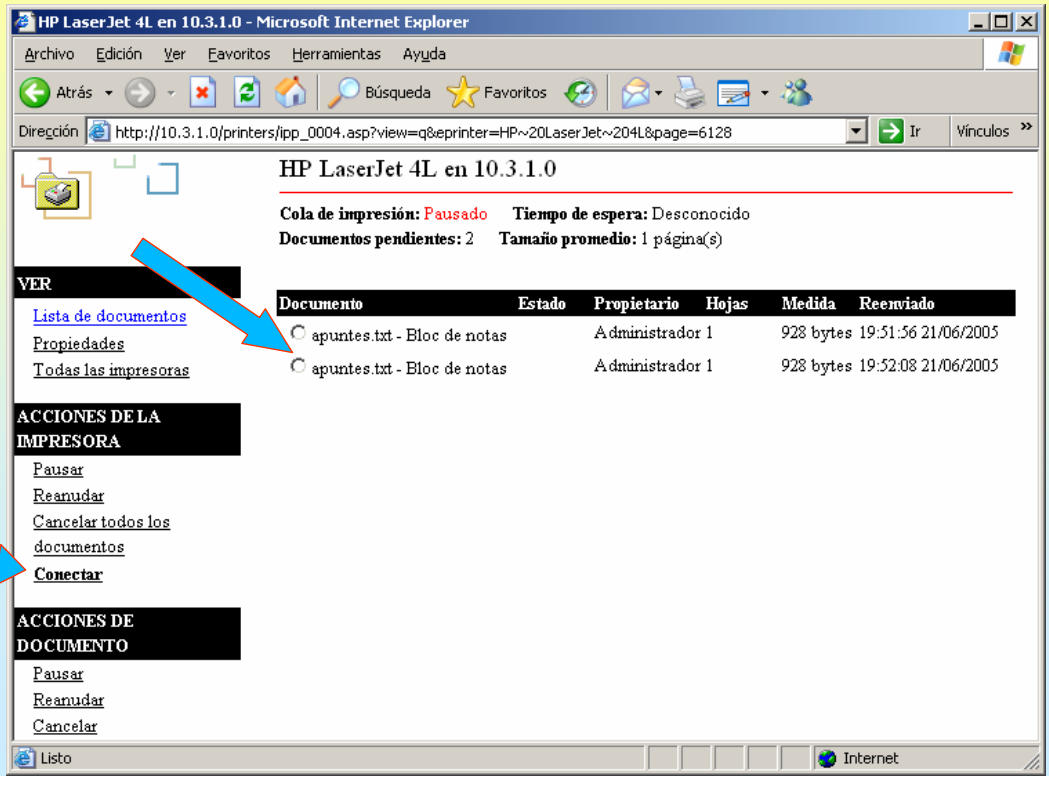
Sé o usuario co que se está no cliente non está na base de datos do equipo destino ou do dominio, o sitio pide un nome de usuario que exista no equipo/dominio que comparte a improsora.

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ INSTALAR UNHA IMPRESORA A TRAVÉS DO WEB

Para este exemplo pausouse a impresora e enviáronse dous documentos de texto.

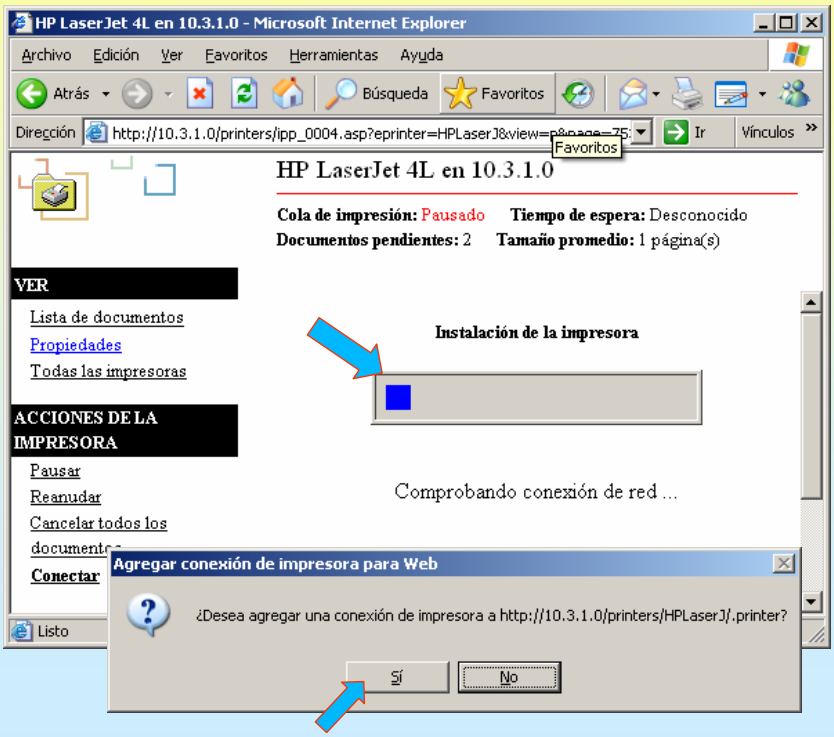


Premer aquí para instalar a impresora de rede no cliente.

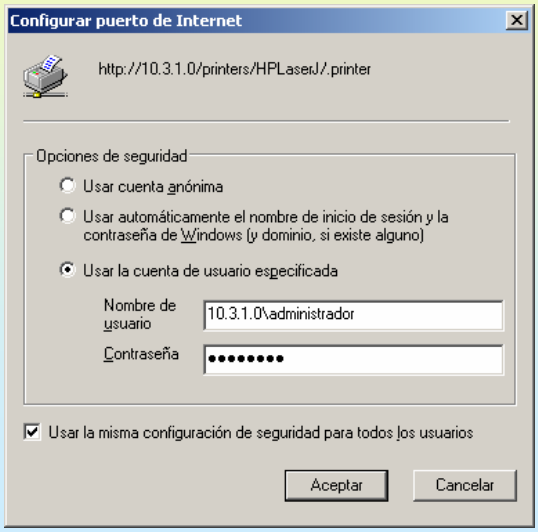
5.- Servidor WEB

☞ INSTALAR UNHA IMPRESORA A TRAVÉS DO WEB

Instalar a impresora de rede.



Polas mesmas razóns de antes volve a pedir un nome de usuario do equipo que posúe a impresora



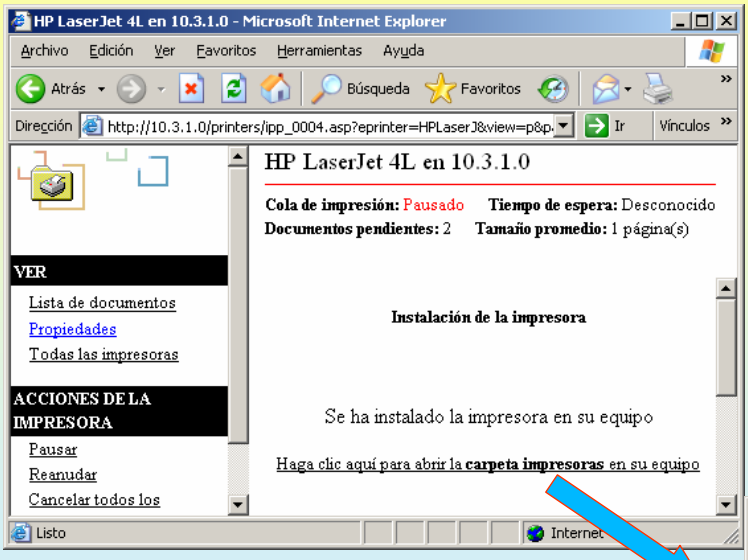
115

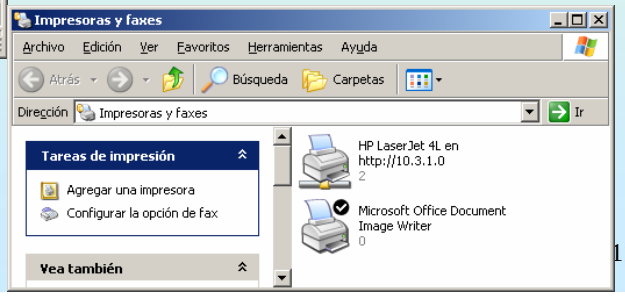
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

5.- Servidor WEB

☞ INSTALAR UNHA IMPRESORA A TRAVÉS DO WEB

Impresora xa instalada.





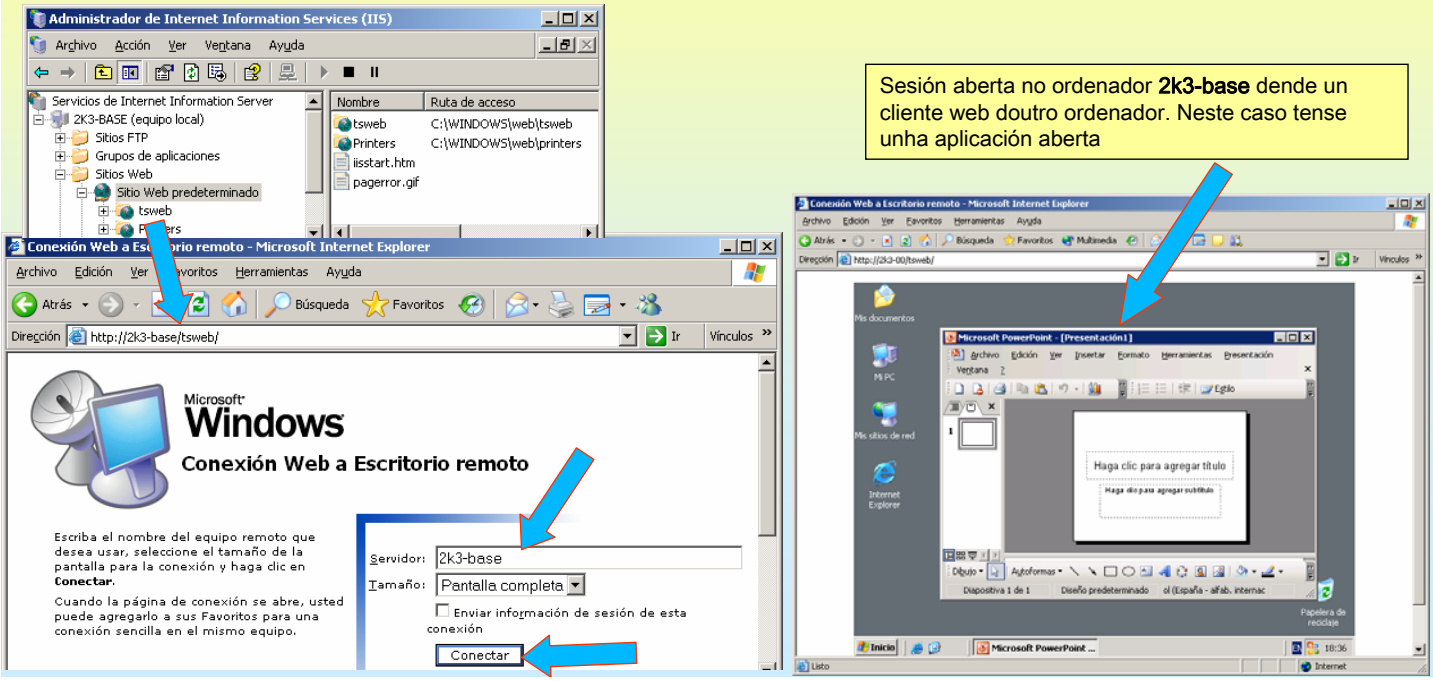
116

5.- Servidor WEB

☞ TERMINAL SERVER WEB – ESCRITORIO REMOTO A TRAVÉS DO WEB

Mais adiante vaise explicar o concepto de terminal server e escritorio remoto, será entón cando se faga referencia a **escritorio remoto a través do web**.

En esencia consiste en abrir unha sesión nun equipo, que ofreza esa posibilidade, tal e como se se estivera fisicamente sentado diante del, pero neste caso estaríase noutro ordenador.

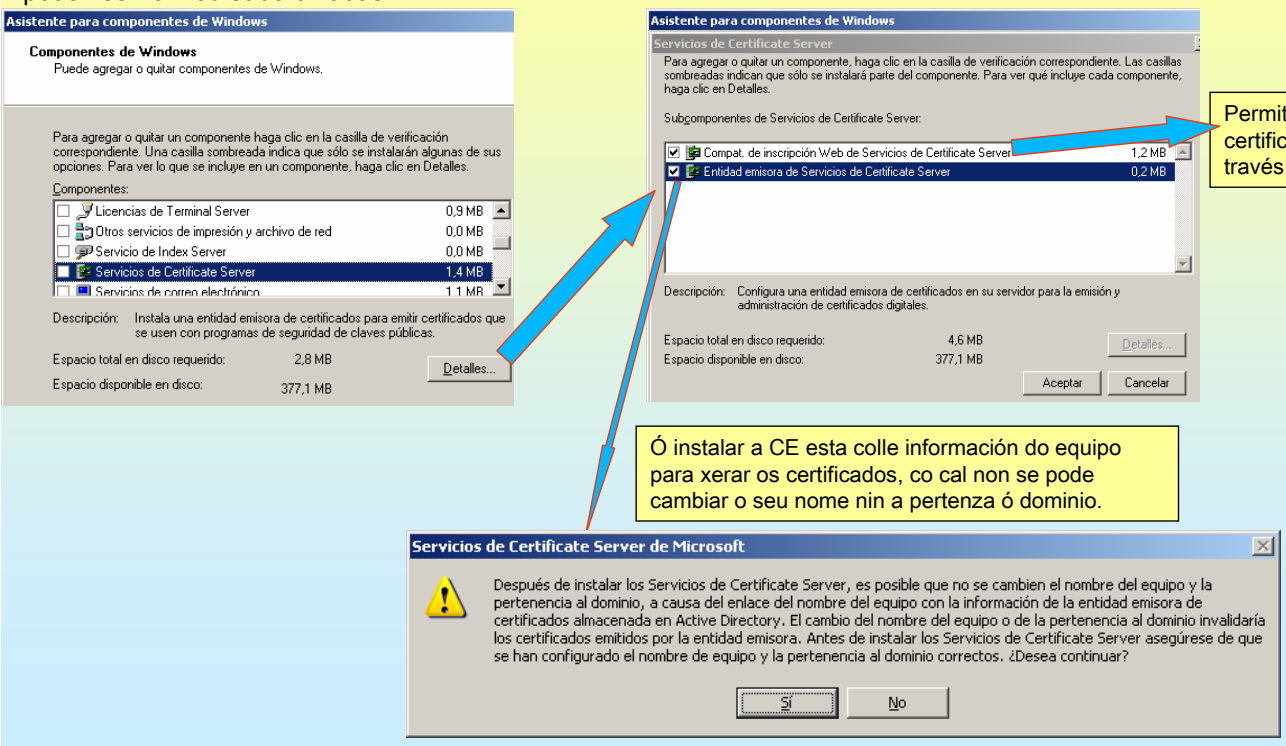


Sesión aberta no ordenador **2k3-base** dende un cliente web doutro ordenador. Neste caso tense unha aplicación aberta

6.- Servizos de Certificate Server

☞ Instalación dunha Entidade Certificadora Independente

En windows 2003 as CE poden estar integradas con Active Directory ou ser independentes. Ó mesmo tempo estas poden ser raíz ou subordinadas.



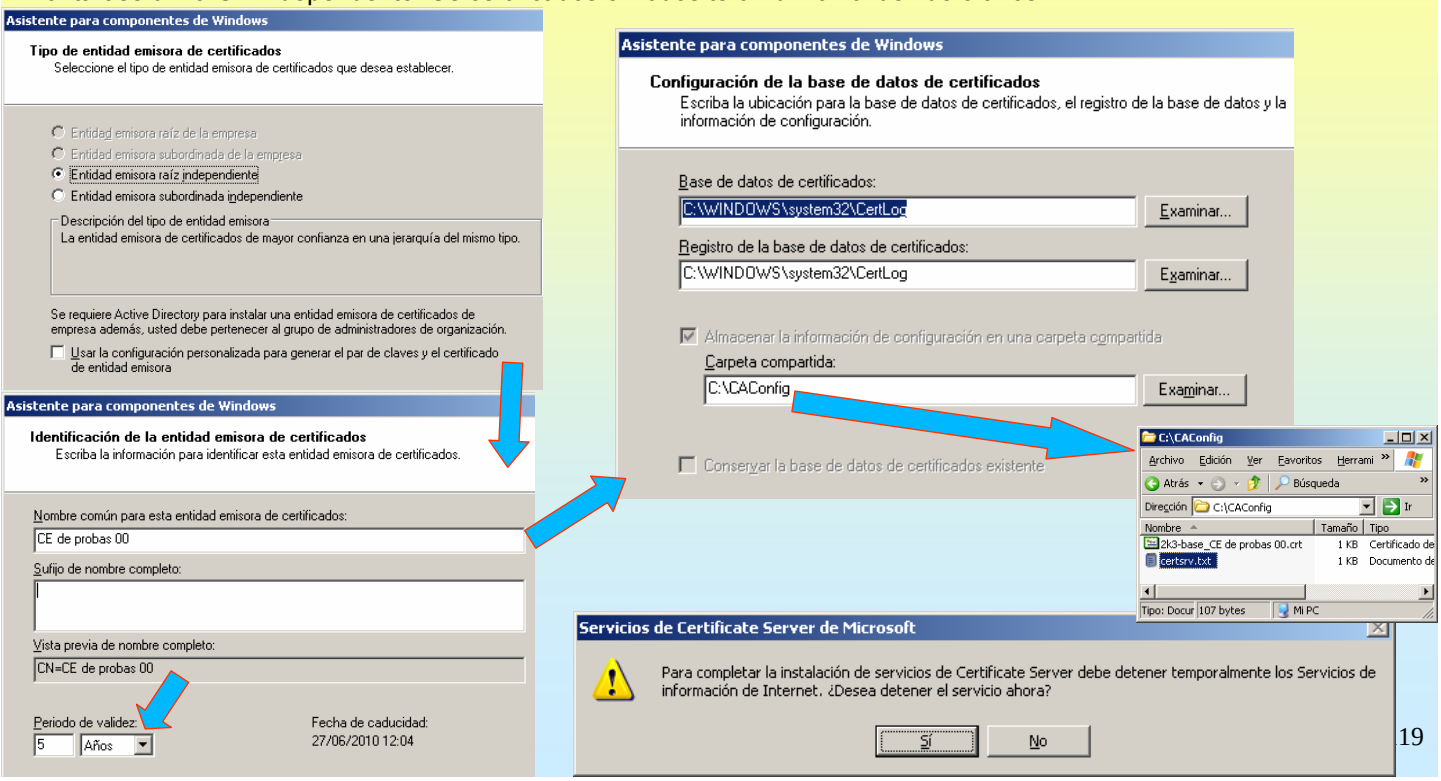
Permite solicitar certificados a través do web

Ó instalar a CE esta colle información do equipo para xerar os certificados, co cal non se pode cambiar o seu nome nin a pertenza ó dominio.

6.- Servizos de Certificate Server

☞ Instalación dunha Entidade Certificadora Independente

Montarase unha CE independente. Os certificados emitidos terán unha validez de 5 anos..

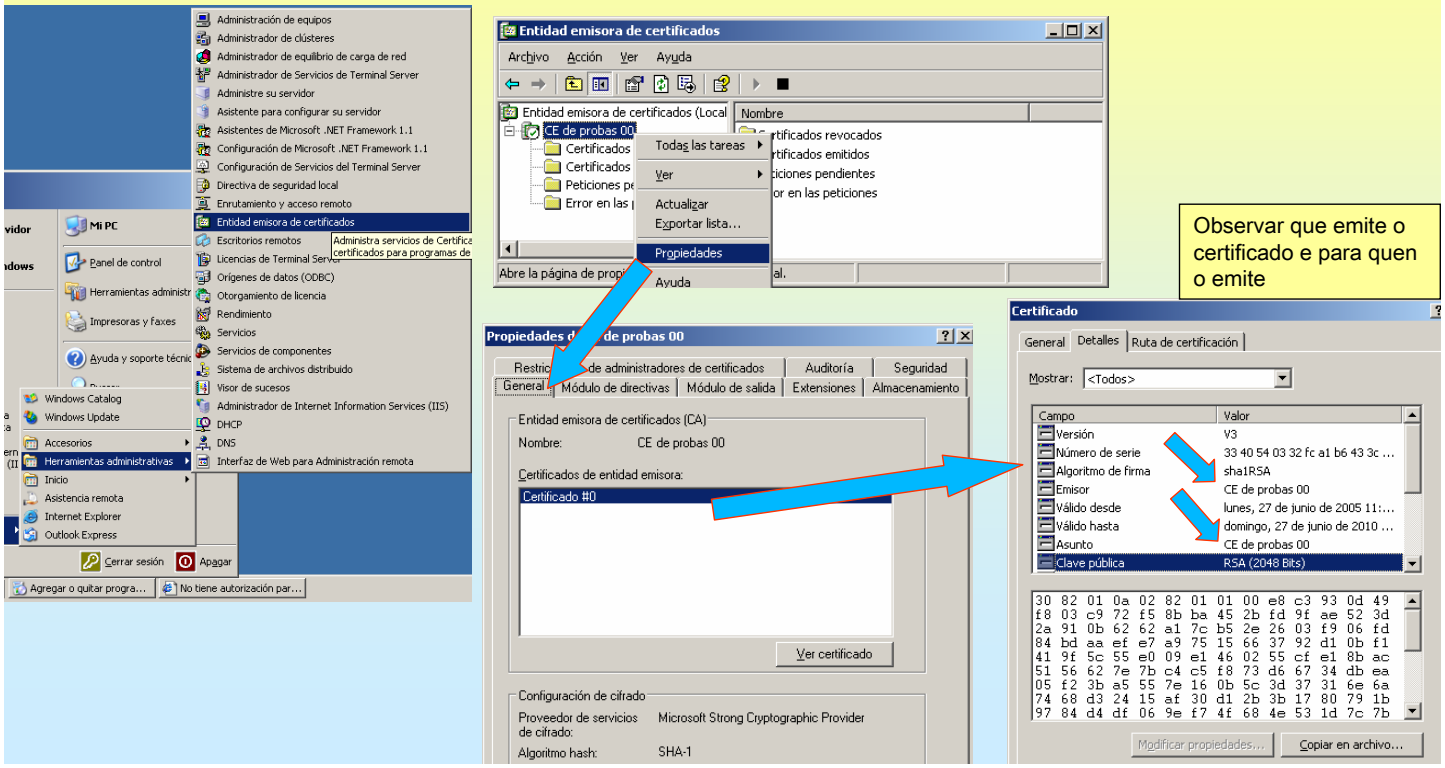


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

6.- Servizos de Certificate Server

☞ Propiedades da CE de probas

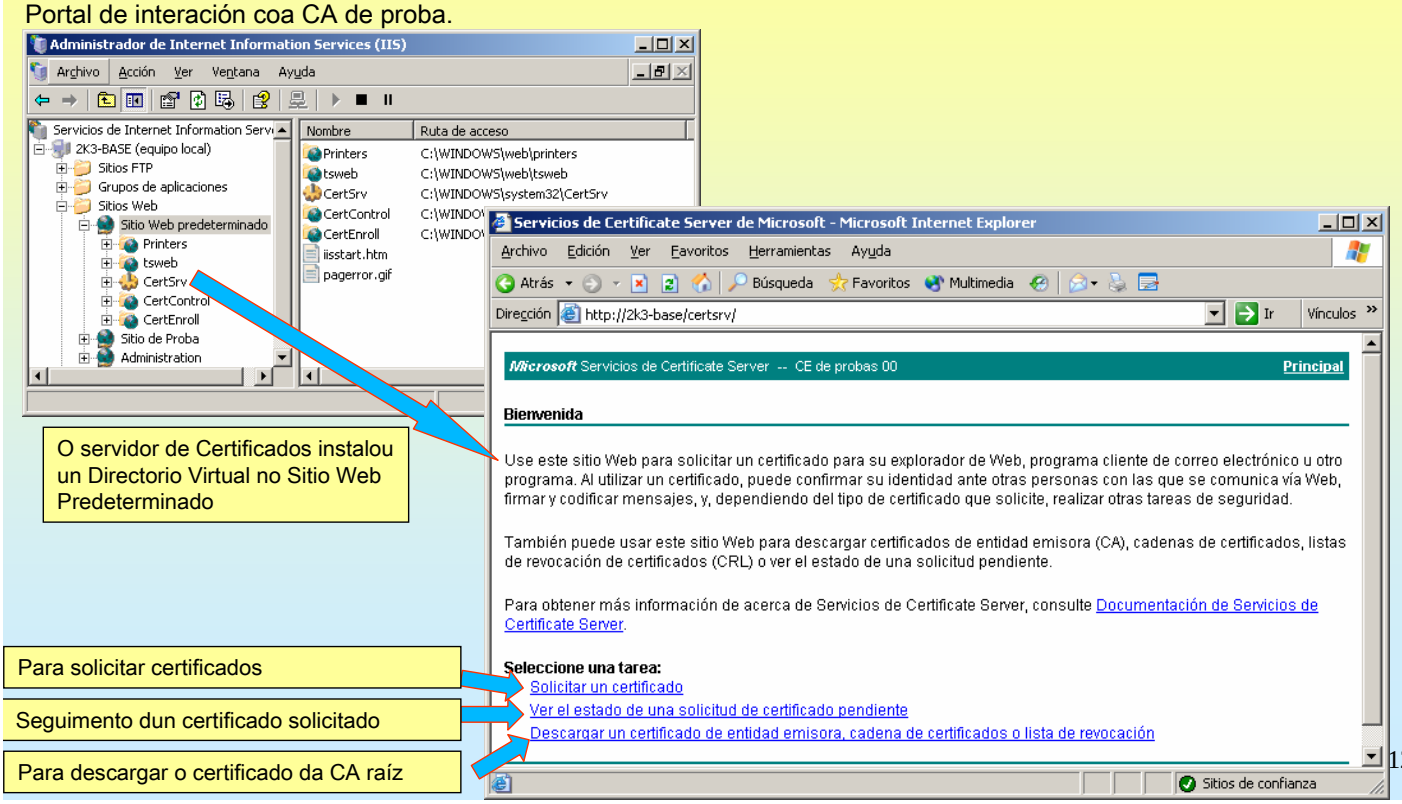
Observar o certificado da CA raíz de probas



6.- Servizos de Certificate Server

☞ Xestión da CA a través do web

Portal de interación coa CA de proba.



O servidor de Certificados instalou un Directorio Virtual no Sitio Web Predeterminado

Para solicitar certificados

Seguimento dun certificado solicitado

Para descargar o certificado da CA raíz

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

A construcción dun sitio seguro (SSL) implica o uso de certificados. O proceso desenvólvese en 3 pasos:

1º.- No sitio web desexado configúranse os datos que se precisen (identificación do usuario/sitio e chave pública do sitio)

2º.- Solicitar o certificado web a unha CA pasándolle a información anterior para que a firme a CA.

2.1.- A CA debe comprobar a identidade do usuario para posteriormente firmar o certificado.

3º.- Descargar o certificado que emitiu a CA

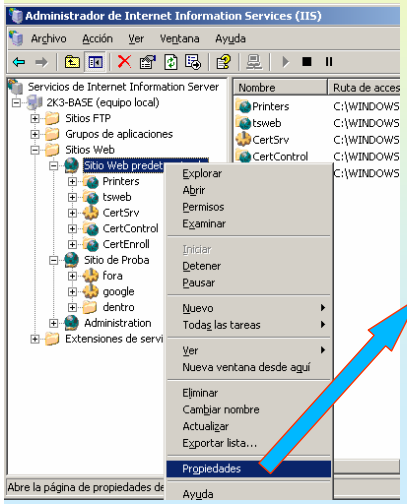
4º.- Instalar o certificado no sitio web que o solicitou anteriormente

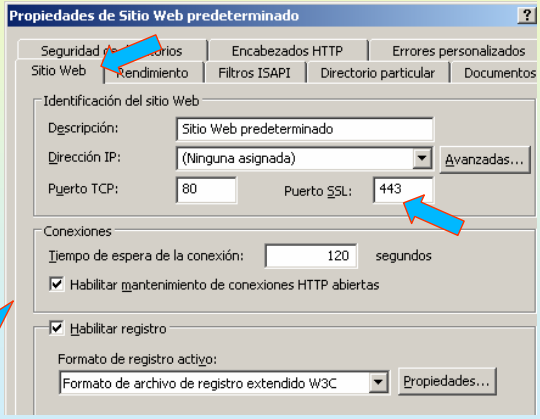
6.- Servizos de Certificate Server

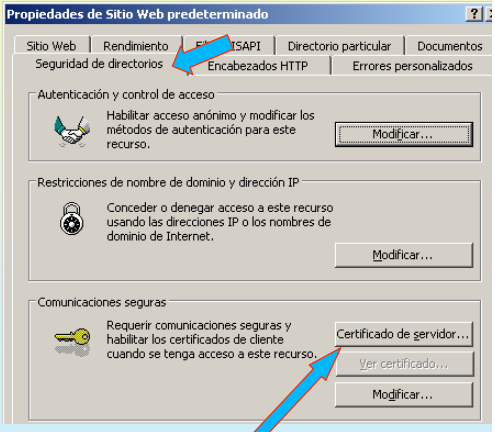
☞ Solicitude de certificado web para un sitio seguro (SSL)

Neste exemplo, crearase un sitio seguro para o **Sitio Web Predeterminado** con nome de dominio **equipo.proba00.ga** (Lembrar que a nivel DNS o nome de dominio é para resolver logo nunha IP)

1º.- Identificar ó sitio e crear a chave pública no IIS para o sitio desexado







O porto ben coñecido para Https (SSL) é o 443

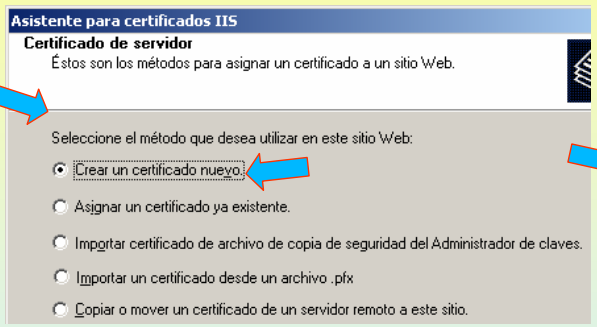
Para crear o certificado de servidor

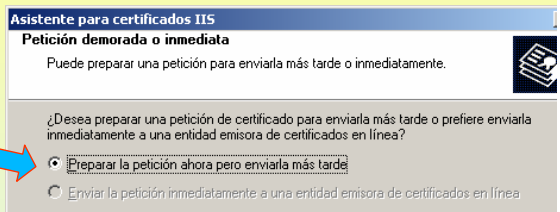
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

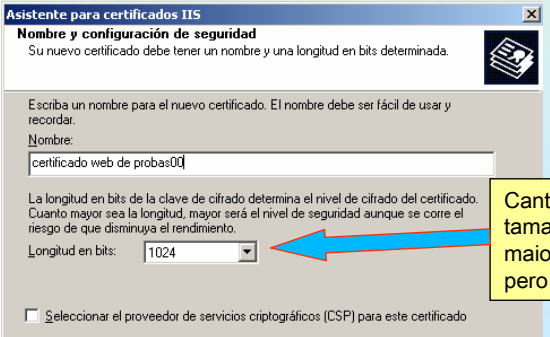
6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

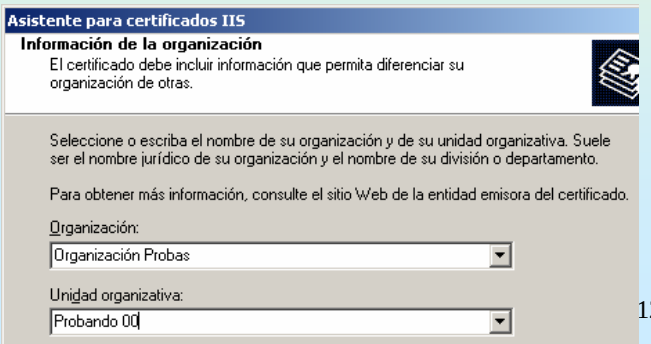
Introducir a información solicitada (I).







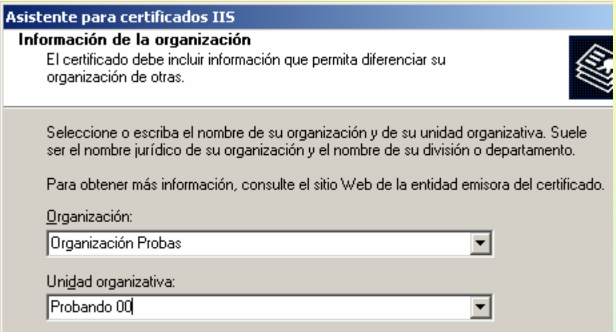
Canto maior sexa o tamaño da chave maior seguridade pero máis lentitude

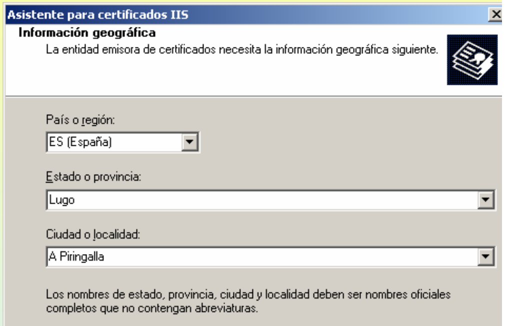


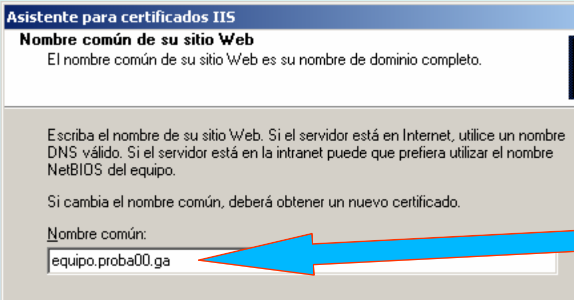
6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

Introducir a información solicitada (II)







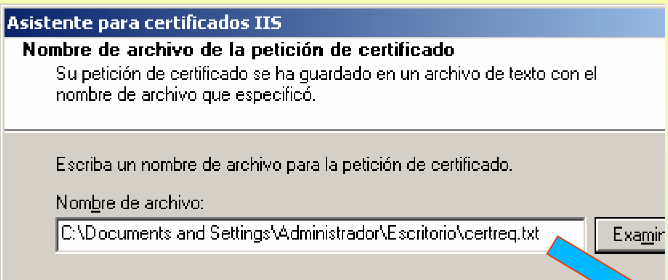
Este dato é un dos que vai comprobar a conexión SSL entre o cliente e o servidor.

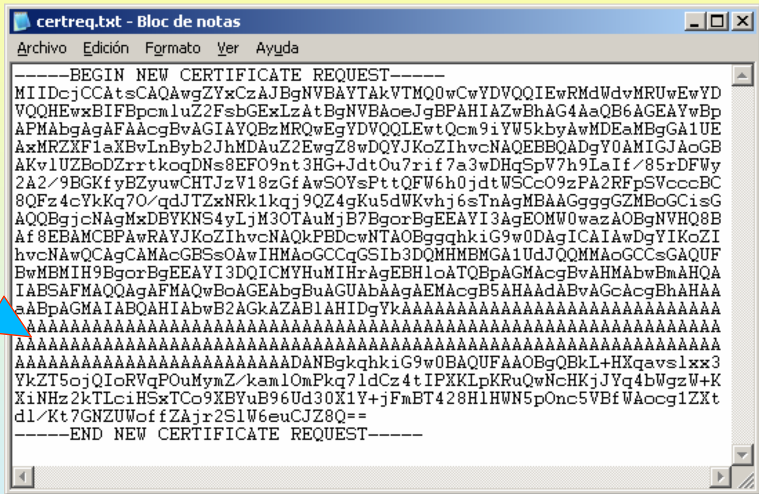
Polo tanto debe ser o correcto.

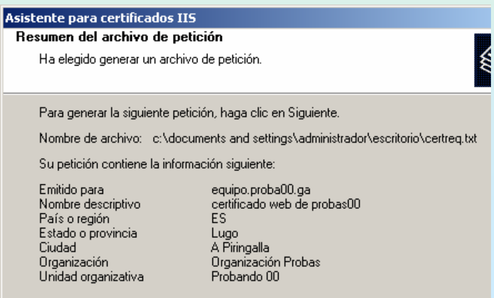
6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

Almacenar a información introducida e a chave pública xerada polo servidor IIS do **Sitio Web Predeterminado**







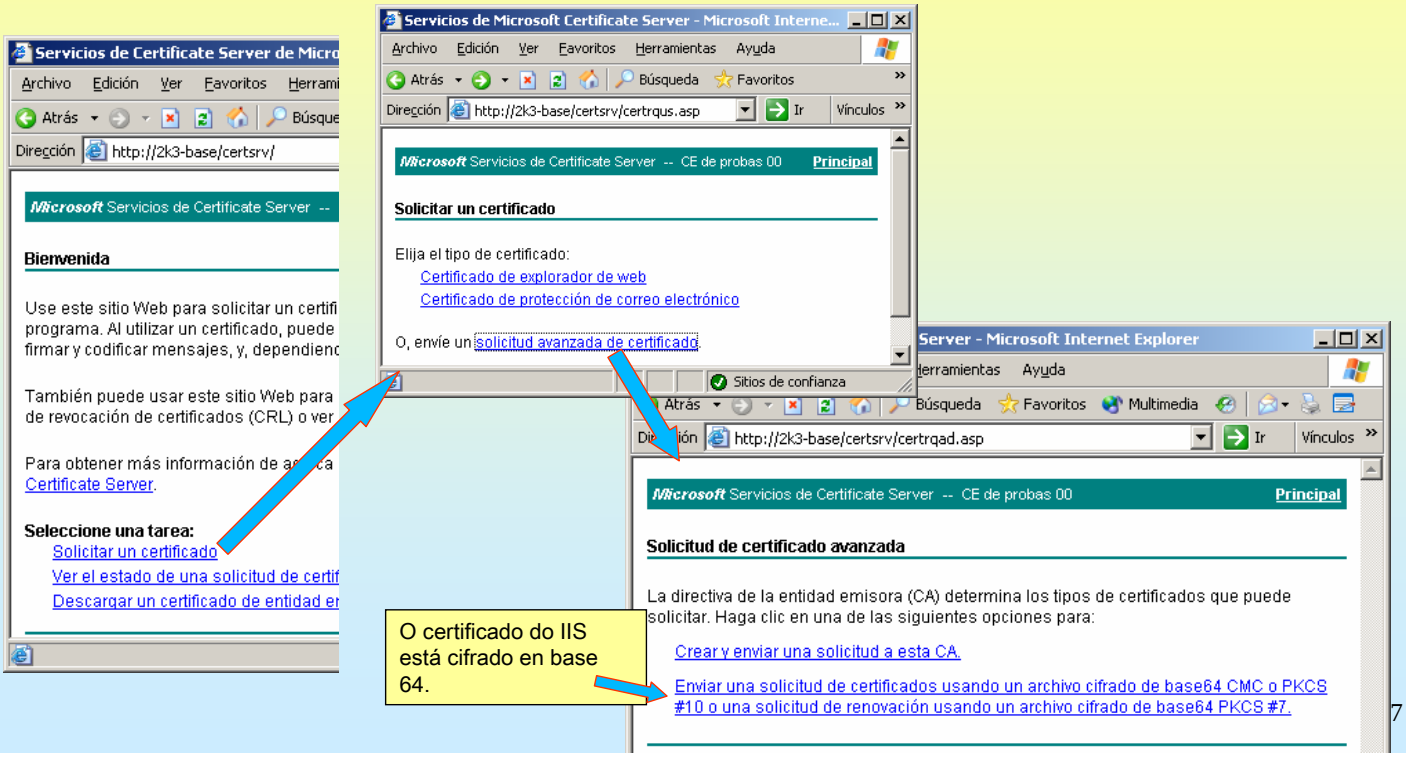
Solicitude de Certificado, inclúe os datos do sitio e a chave pública.

Este arquivo será o que se lle pase á CA para que o firme.

6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

2º.- Solicitar o certificado á CA. Para iso farase uso do portal web que facilita o Servidor de Certificados.



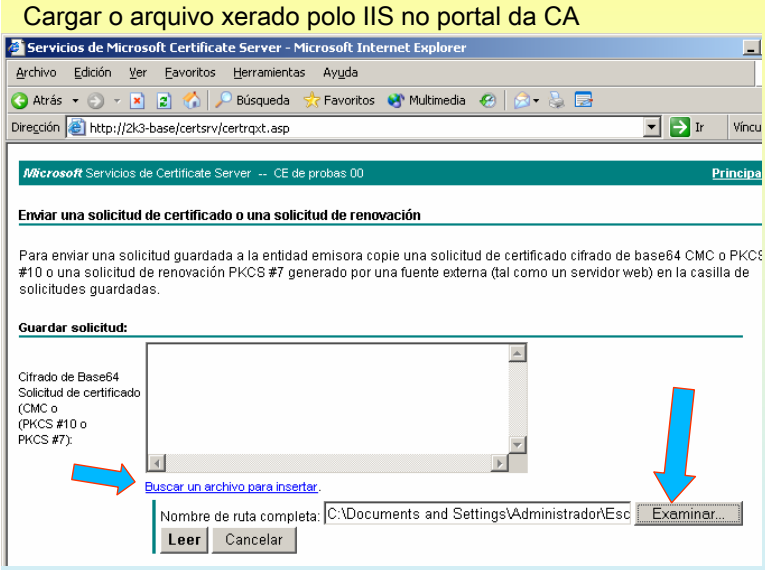
O certificado do IIS está cifrado en base 64.

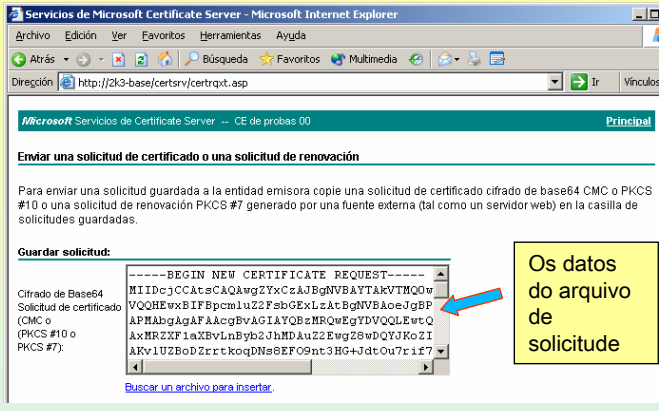
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

6.- Servizos de Certificate Server

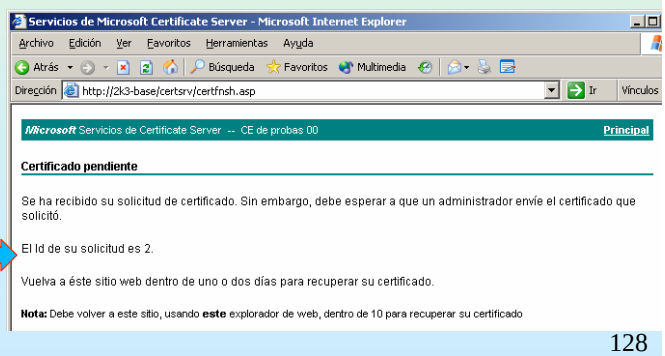
☞ Solicitude de certificado web para un sitio seguro (SSL)

Cargar o arquivo xerado polo IIS no portal da CA





Os datos do arquivo de solicitude

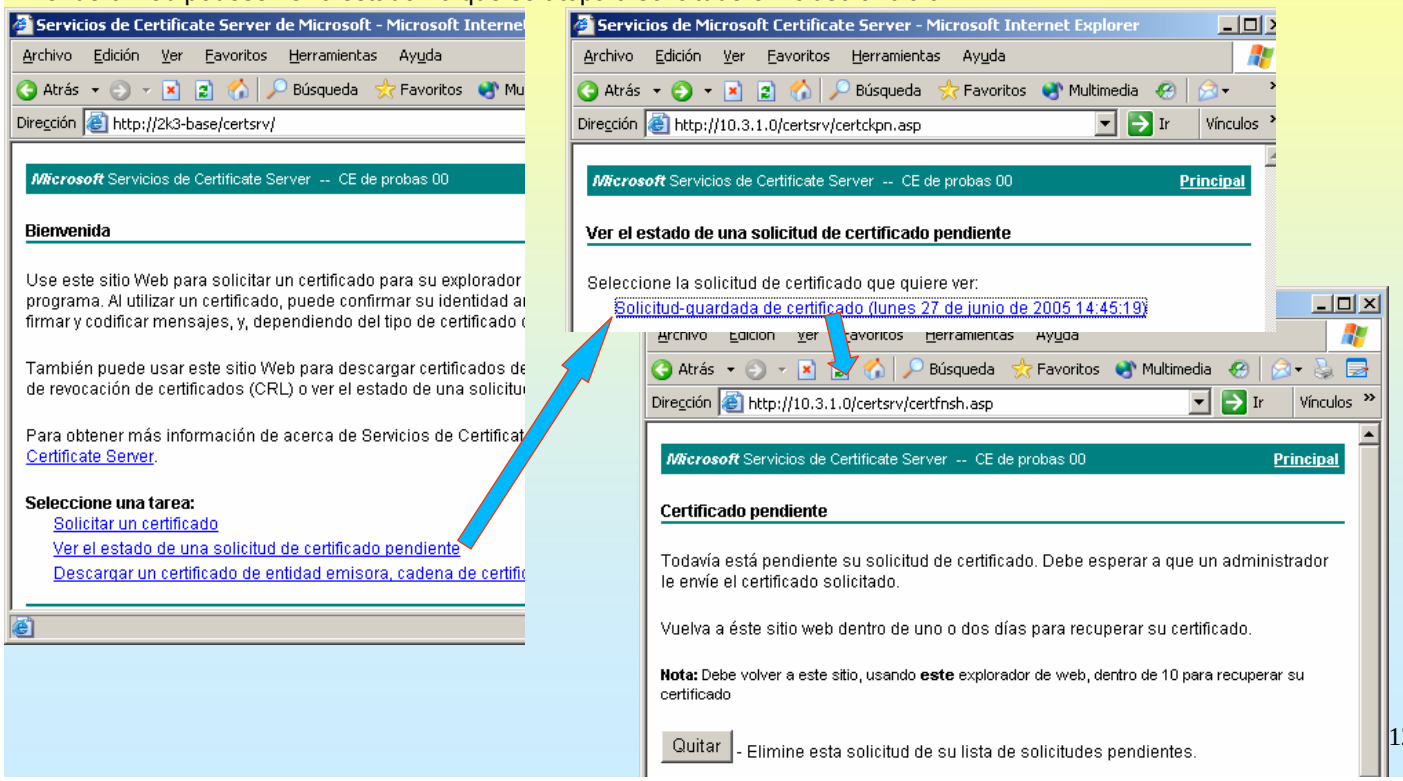


Nº de solicitude dentro da CA

6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

Dende o web pódese ver o estado no que se atopa a solicitude e incluso anulala

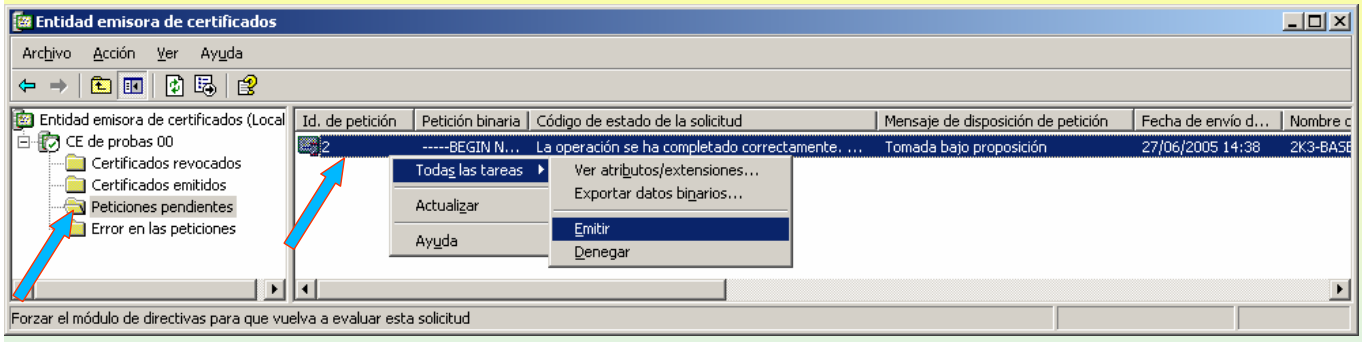


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

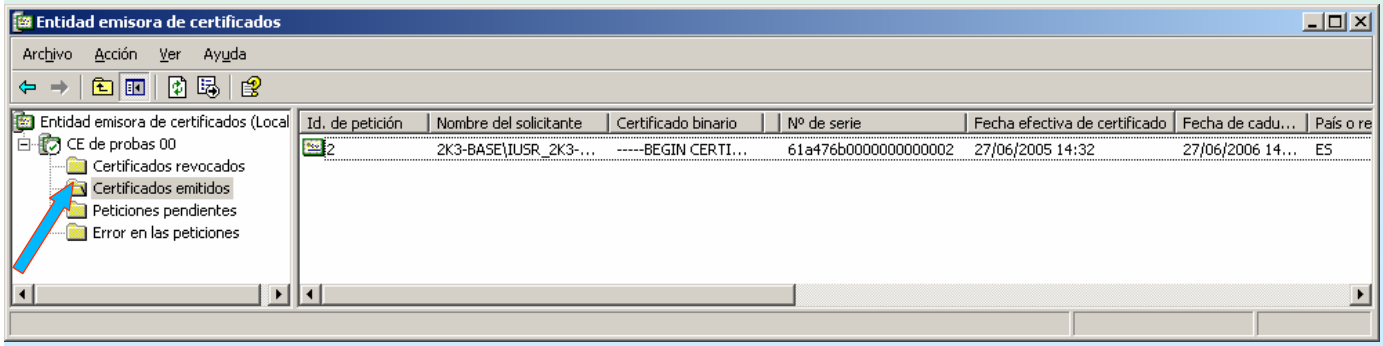
6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

2.1.- A CA debe emitir o certificado ou denegalo. Este estará na CA en Certificados pendentes.



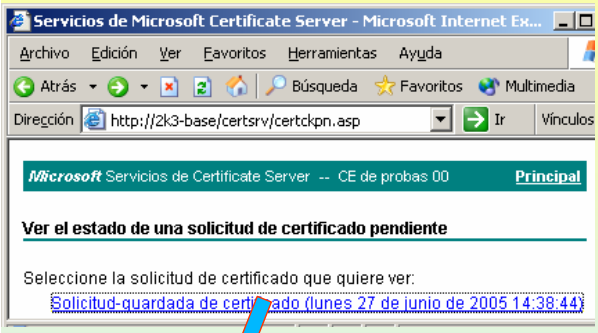
Emítese o certificado e este pasa de certificados pendentes a certificados emitidos. Antes de emitilo poderíase solicitar información ó dono de sitio (DNI, rexistro, etc) para asegurarse de que el é o dono do sitio



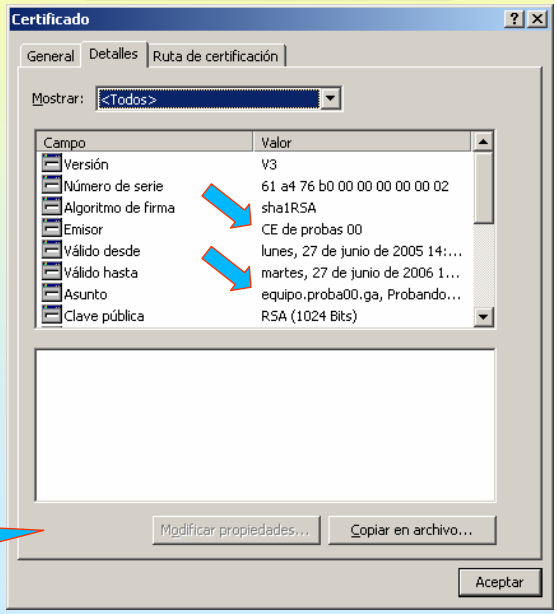
6.- Servizos de Certificate Server

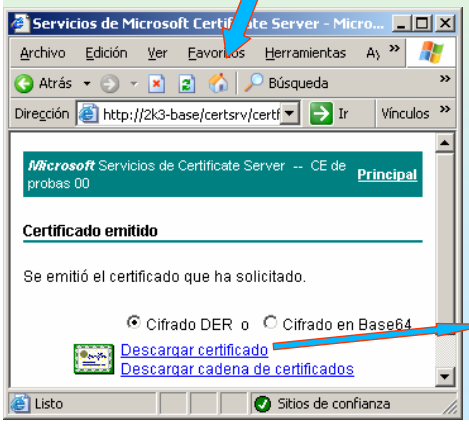
☞ Solicitude de certificado web para un sitio seguro (SSL)

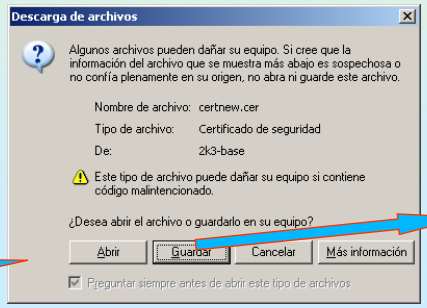
3.- Descargar o certificado do servidor IIS xa asinado e emitido pola CA. Usarase o portal WEB da CA



Observar quen o emite e para quen o emite





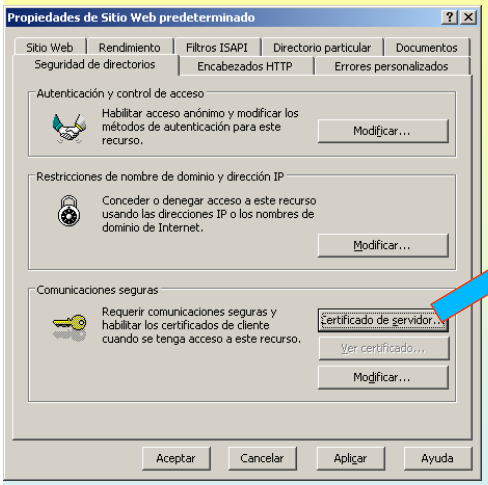


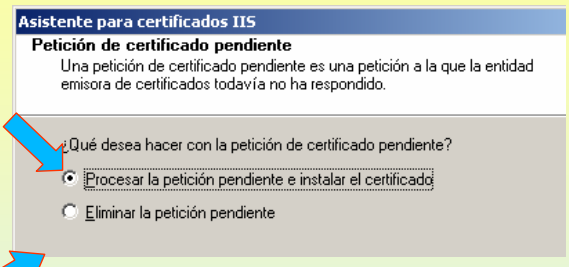
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

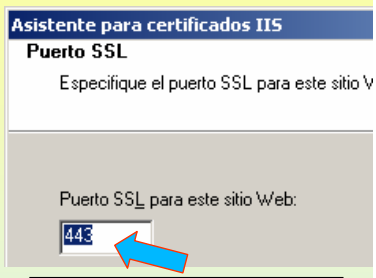
6.- Servizos de Certificate Server

☞ Solicitude de certificado web para un sitio seguro (SSL)

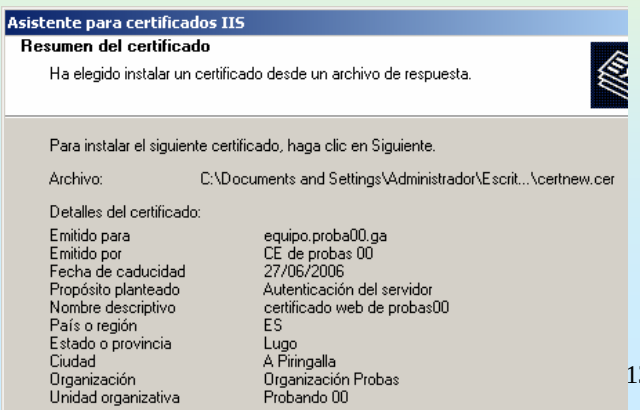
4º.- Instalar o Certificado, baixado anteriormente da CA,no IIS para o **Sitio Web Predeterminado.**

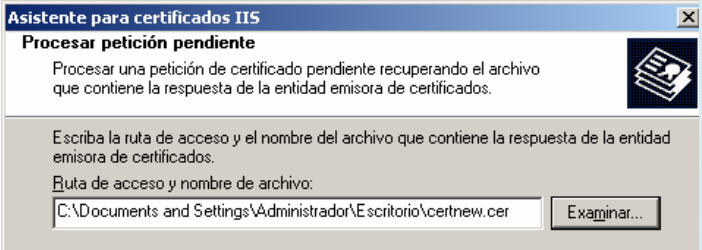






Configurar o porto para SSL

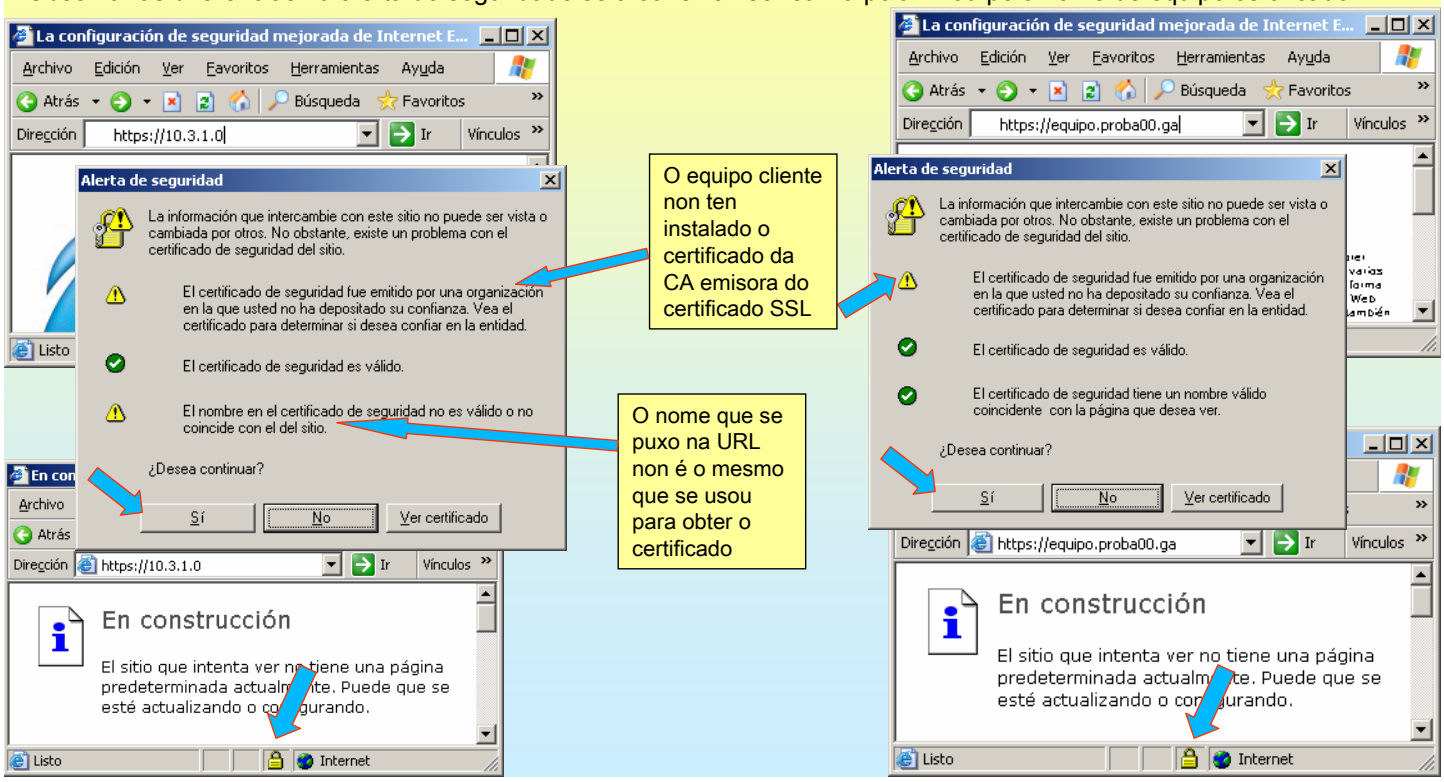




6.- Servizos de Certificate Server

☞ Realizar unha conexión web segura (https, ssl)

Observar as diferencias na alerta de seguridade se a conexión se realiza pola IP ou polo nome de equipo certificado.

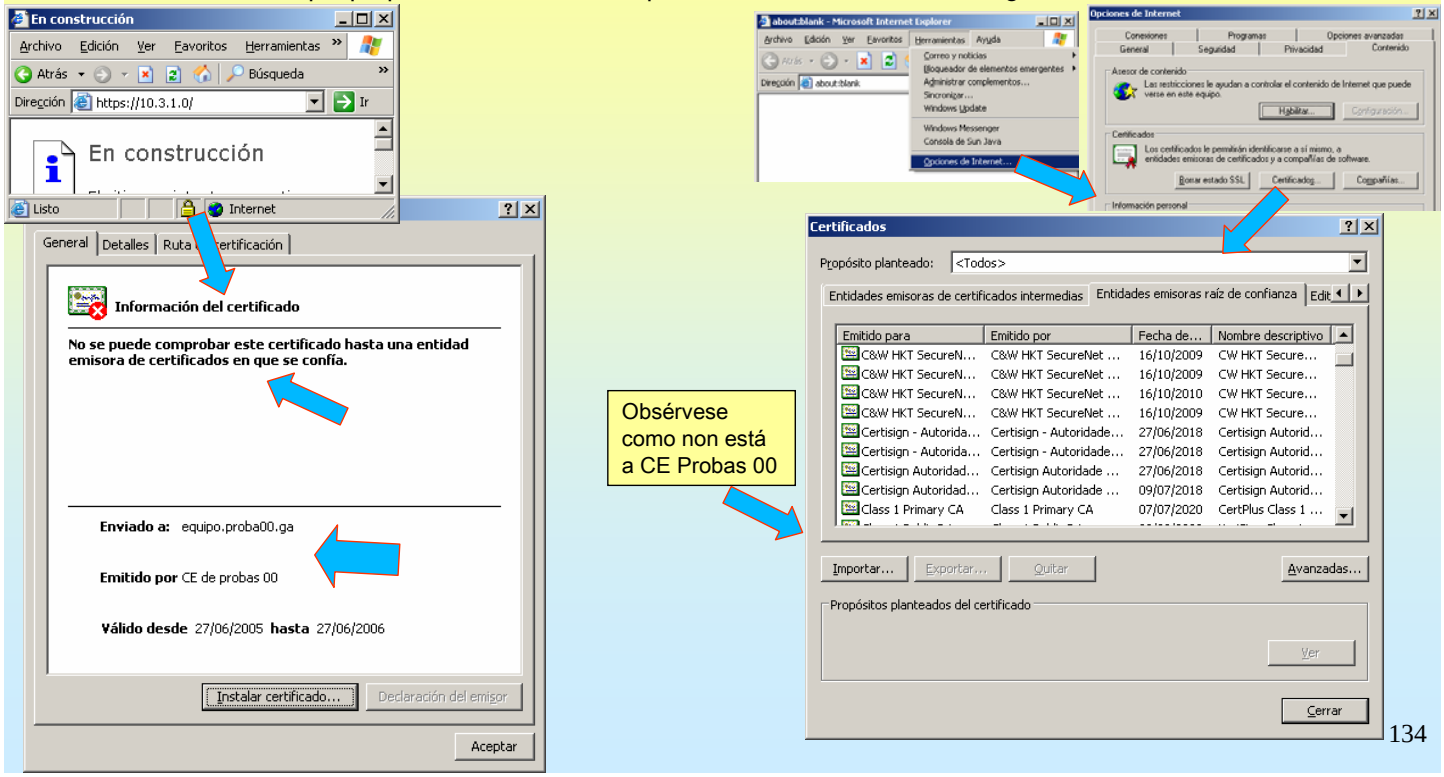


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

6.- Servizos de Certificate Server

☞ Realizar unha conexión web segura

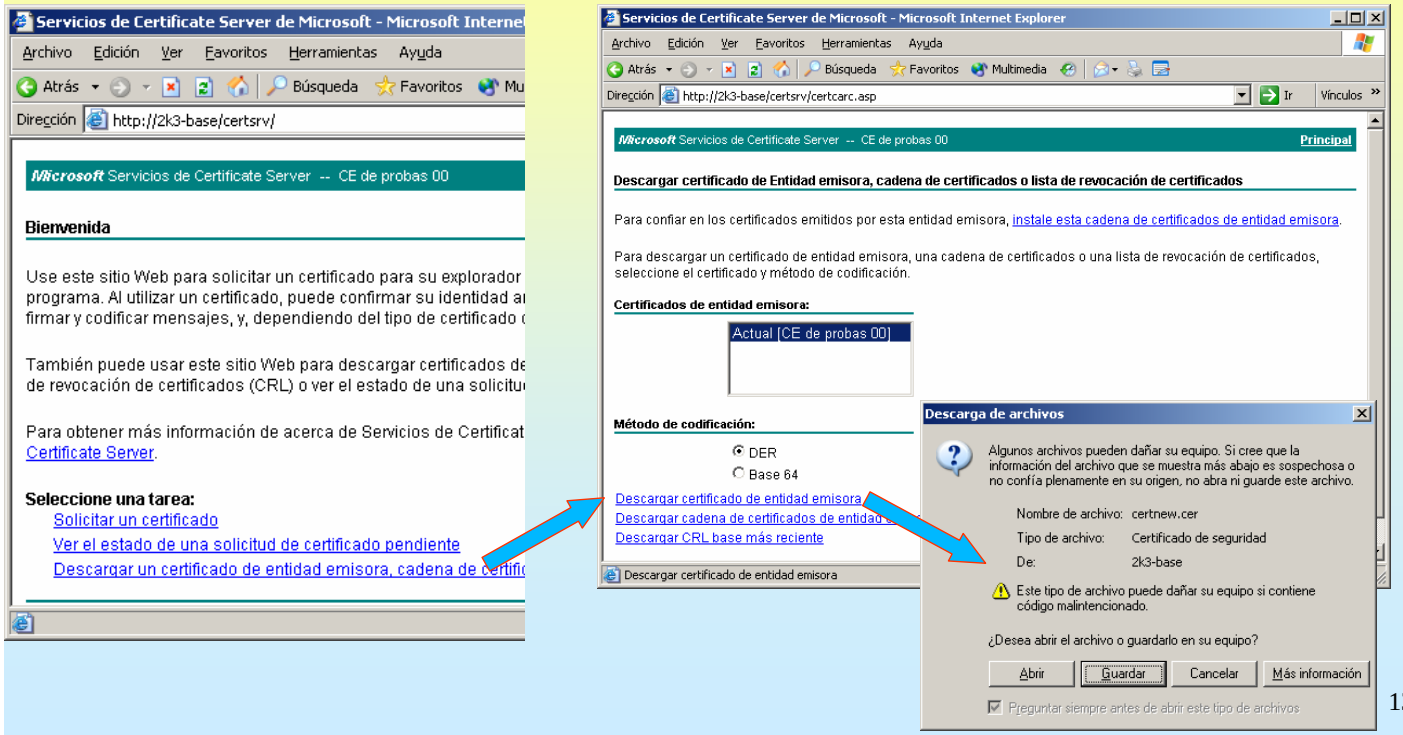
Observar a información que proporciona o certificado que lle enviou o Servidor ó navegador.



6.- Servizos de Certificate Server

☞ Instalar o certificado da CA emisora (raíz)

Primeiro debe descargarse o certificado raíz da CA para elo usarase o portal web da CA.

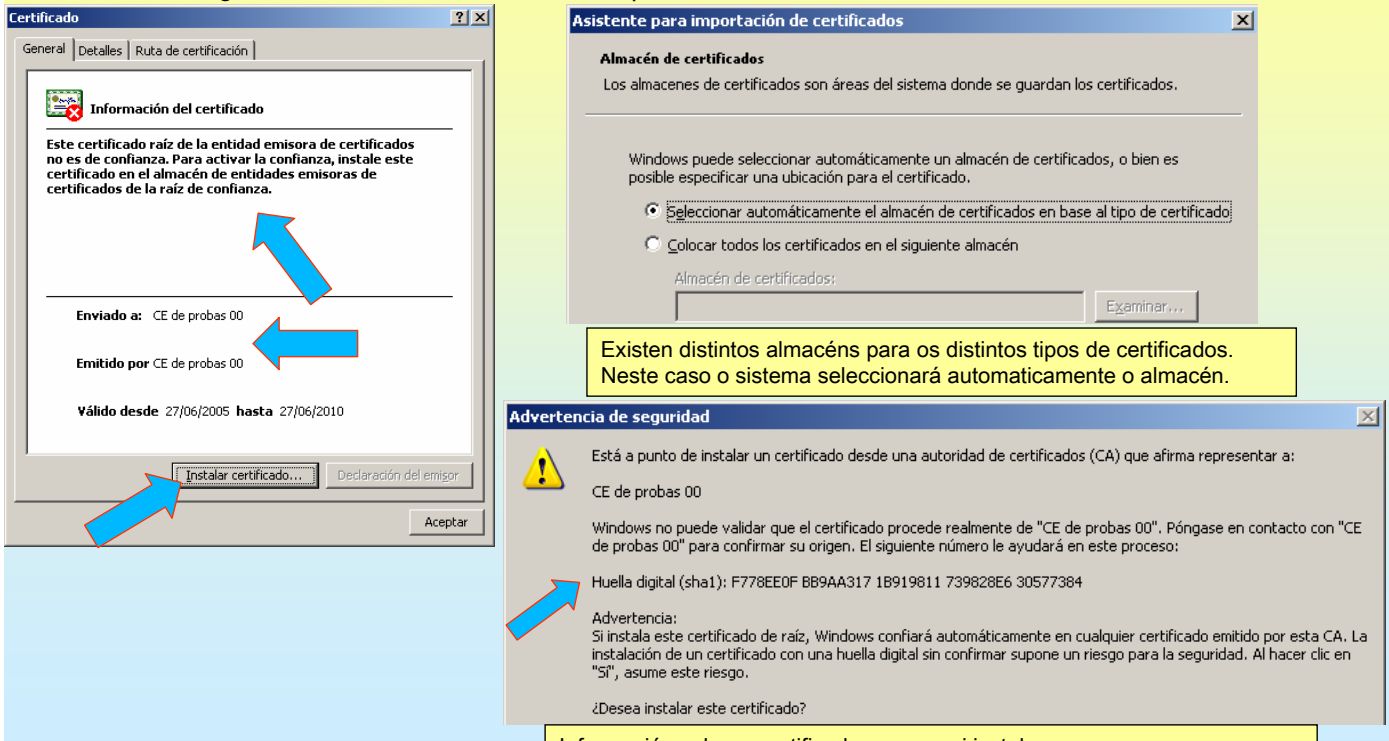


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

6.- Servizos de Certificate Server

☞ Instalar o certificado da CA emisora (raíz)

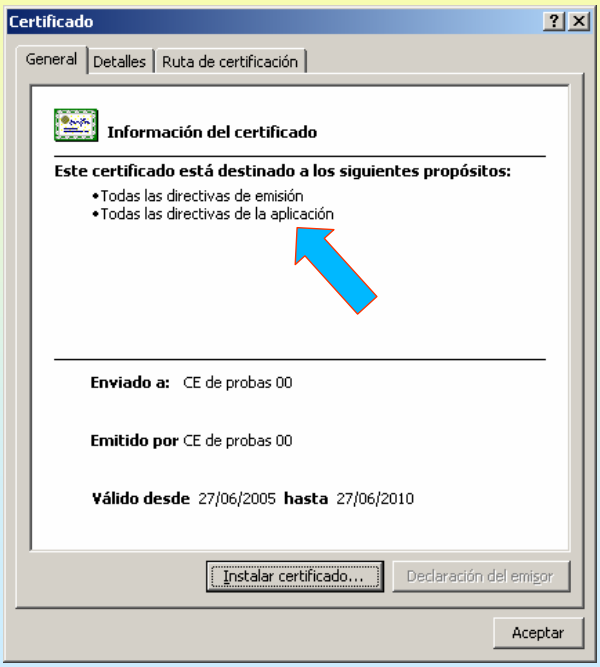
Unha vez descargado realizase doble clic sobre o arquivo do certificado.

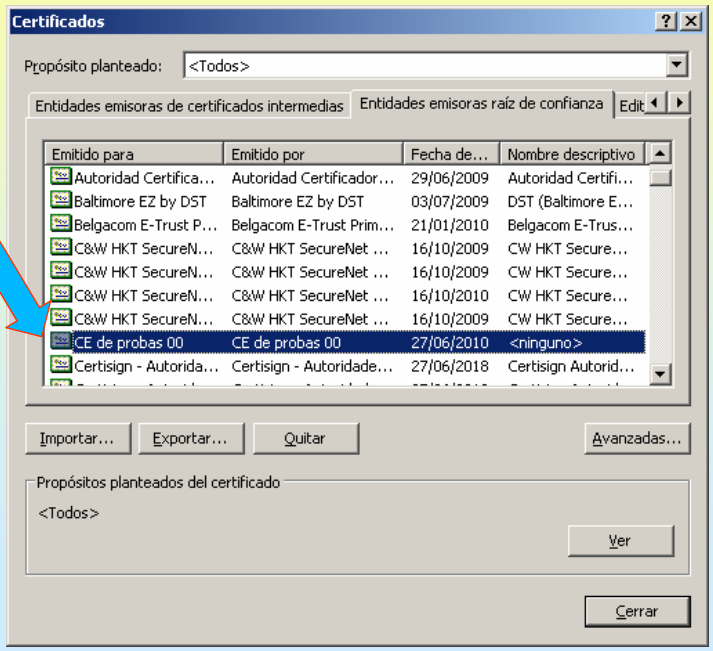


6.- Servizos de Certificate Server

☞ Instalar o certificado da CA emisora (raíz)

Agora pódese observar como o certificado no da advertencias e como está instalado no almacén de Entidades emisoras raíz de confianza

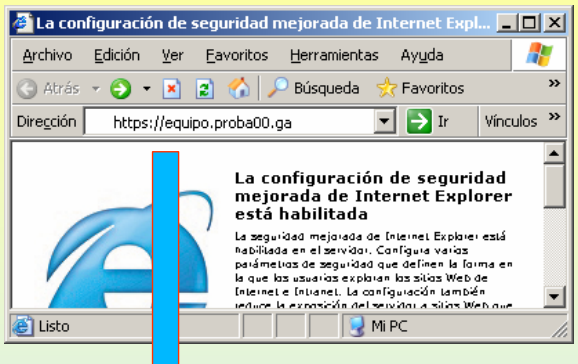


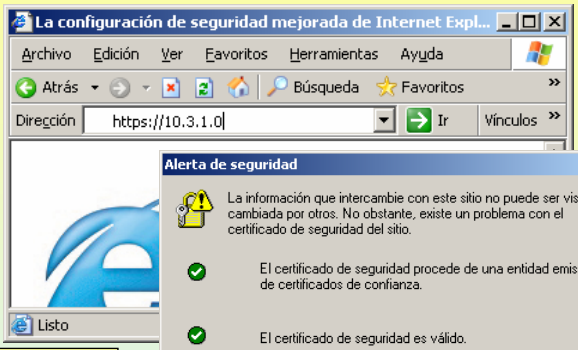


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

6.- Servizos de Certificate Server

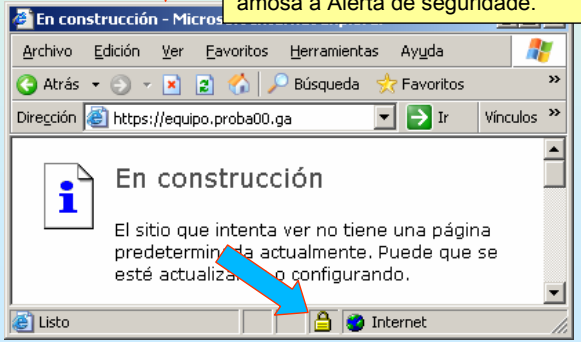
☞ Derradeira conexión dun cliente web usando https ó sitio web predeterminado

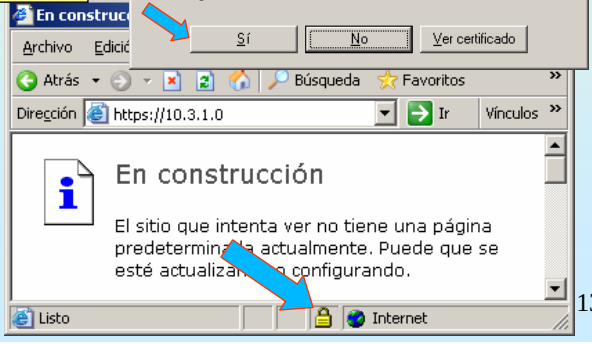




Tódolos aspectos de seguridade do certificado son correctos, por iso non amosa a Alerta de seguridade.

Problema co nome do sitio posto na URL





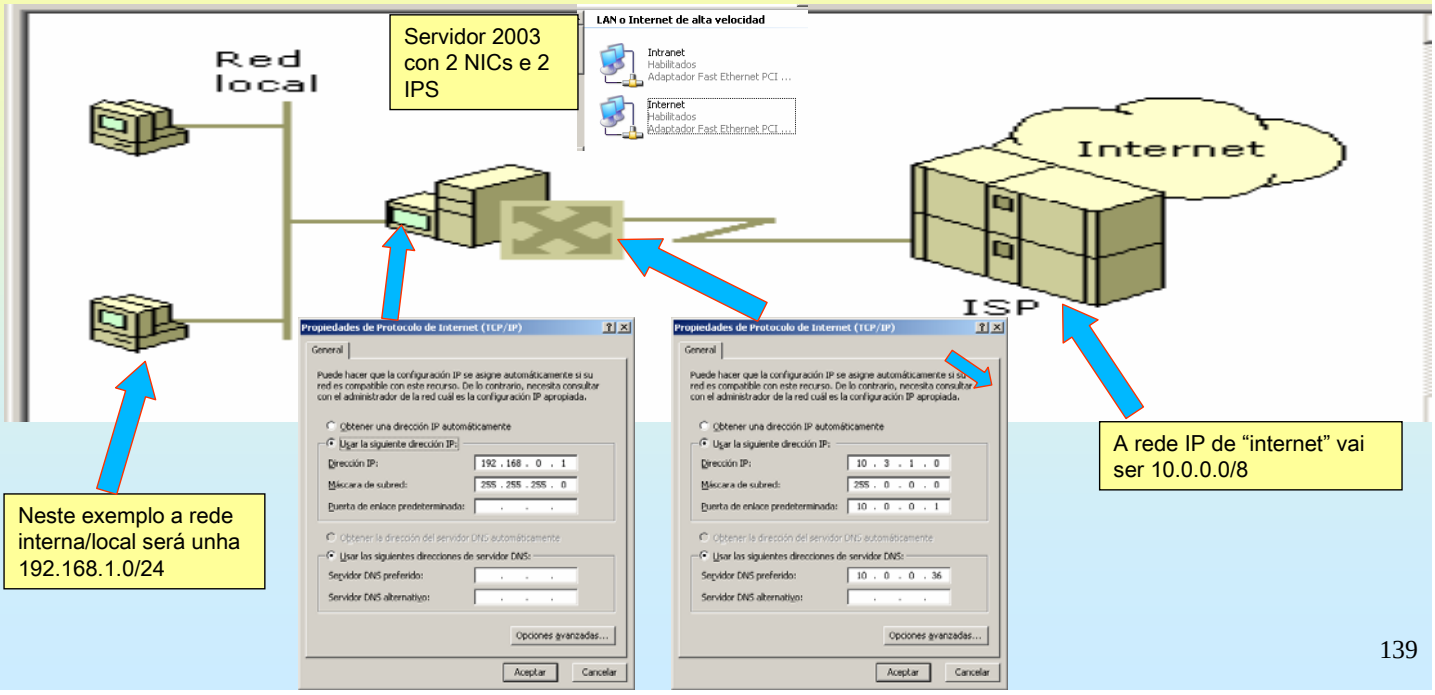
7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Configuración previa das tarxetas de rede

A seguinte imaxe mostra a esencia de NAT.

Para configurar NAT nun servidor windows 2003 é preciso dispor ó menos de 2 tarxetas de rede

- 1 para unir o servidor coa rede interna/local (**intranet, 192.168.0.1 / 24**)
- 2 para unir o servidor coa rede exterior (**internet, 10.3.1.0 / 8**)



Neste exemplo a rede interna/local será unha 192.168.1.0/24

A rede IP de "internet" vai ser 10.0.0.0/8

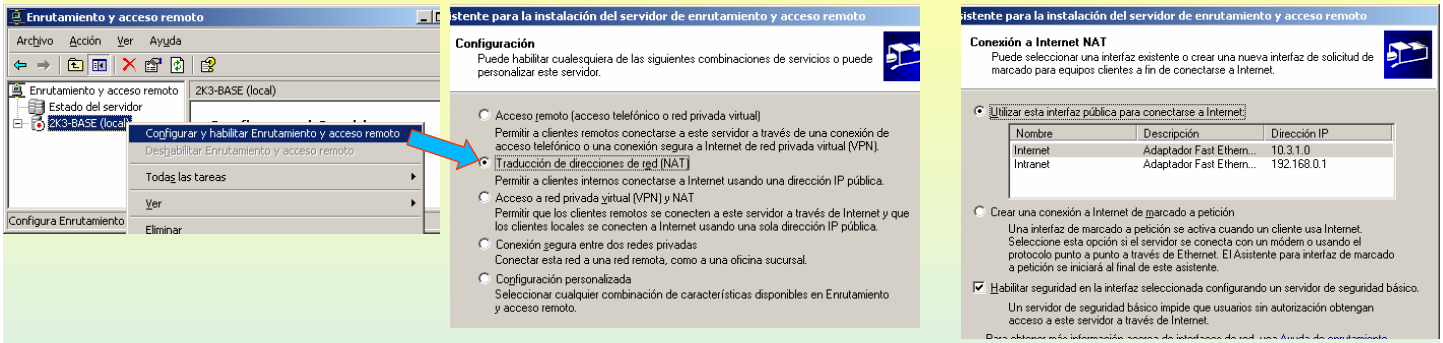
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

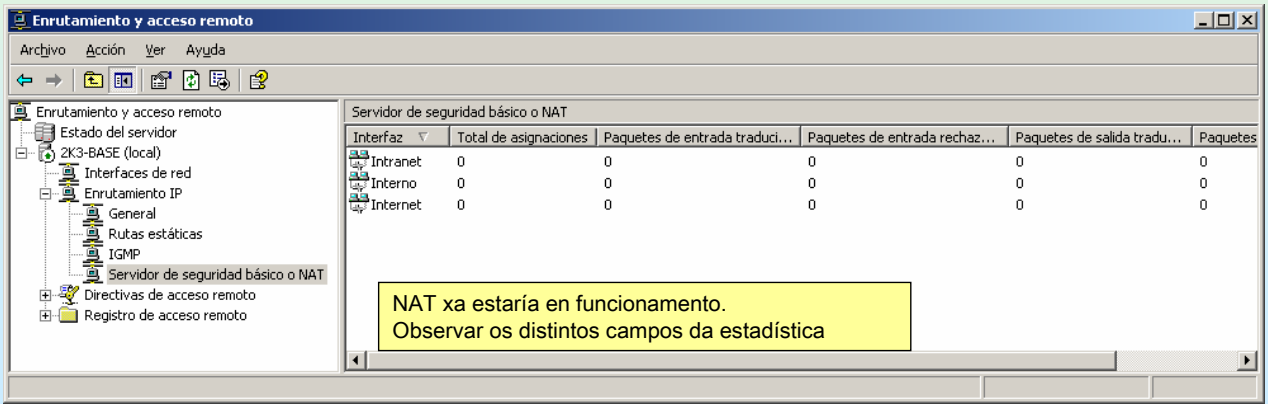
7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Habilitar o Servizo de enrutamento e acceso remoto (I)

Ó comezo destes apuntes (en enrutamento) explicouse como se habilitaba este servizo.

Usaremos na seguinte diapositiva o servizo xa instalado, nesta vaise mostrar como se habilitaría NAT partindo de cero.





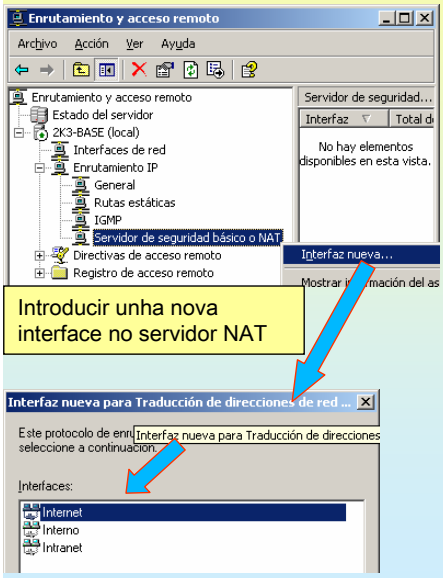
NAT xa estaría en funcionamento.
Observar os distintos campos da estadística

7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Habilitar o Servizo de enrutamento e acceso remoto (II)

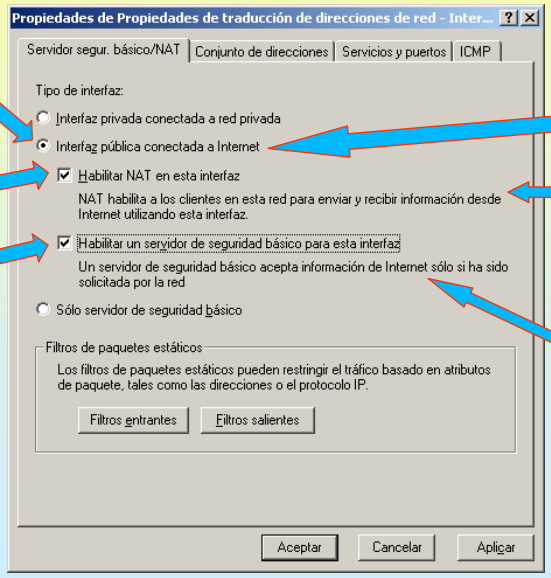
Aproveitando que se tiña o servizo habilitado de prácticas de enrutamento vaise proceder a configurar NAT sen o asistente.

1º.- Configurar a parte conectada a Internet. Hai que seleccionar a tarxeta e logo configurala como NIC Pública..



Introducir unha nova interface no servidor NAT

Seleccionar o NIC desexado, neste caso o que previamente se nomeou con Internet



Indicar que este NIC e o que ten conexión con internet

Habilitar NAT, para que realice a traducción de IPs

Non permitir entrar tráfico de internet á rede local, salvo no caso de que este fose solicitado dende a rede local.

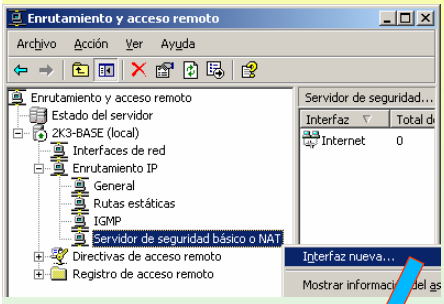
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

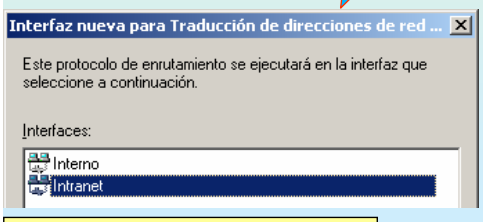
7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Habilitar o Servizo de enrutamento e acceso remoto (II)

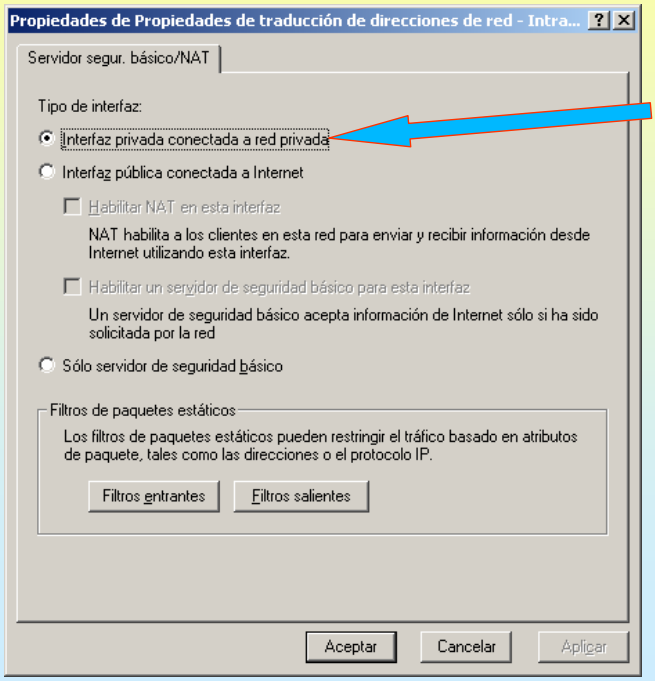
2º.- Configurar a parte conectada á Intranet / rede local.

Igual que no caso anterior instálase unha interfaz nova e configúrase como NIC privada





Seleccionar o NIC desexado, neste caso o que previamente se nomeou con Intranet



Indicar que este NIC e o que ten conexión coa Intranet

7.- NAT (Network Address Translation, Tradución de direccións de rede)

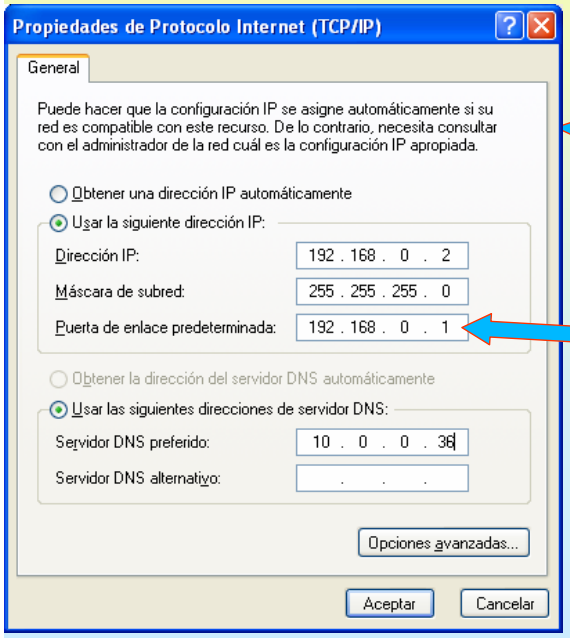
☞ Configurar un equipo da rede local

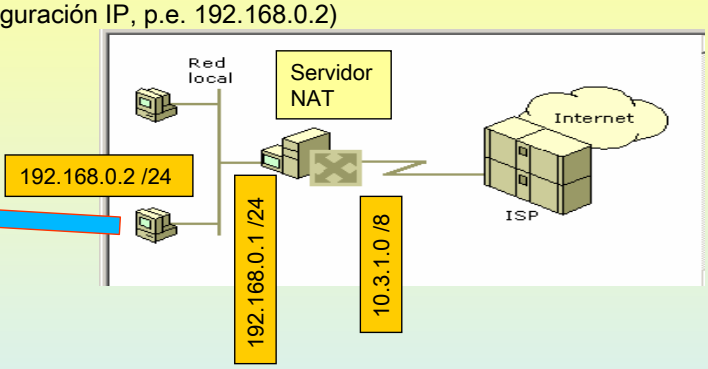
Xa está configurado o servidor NAT, este ten 2 IPs:

1.- 10.3.0.1/8 no NIC que está conectado á rede pública (internet)

2.- 192.168.0.1/24 no NIC que está conectado á rede privada (intranet)

Agora toca configurar un cliente da rede local (configuración IP, p.e. 192.168.0.2)





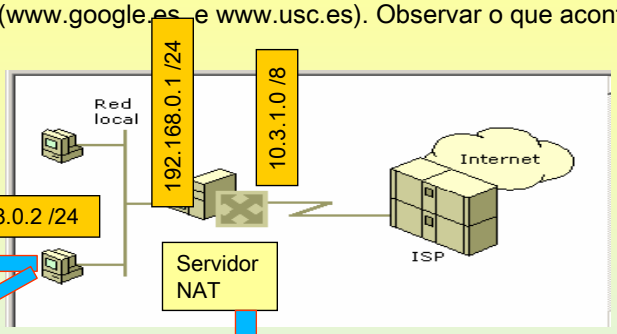
A porta de enlace é o NIC privado do servidor NAT, posto que este servidor será que acepte as peticións dos clientes privados e traduza as súas direccións a 10.3.1.0, así como os portos correspondentes.

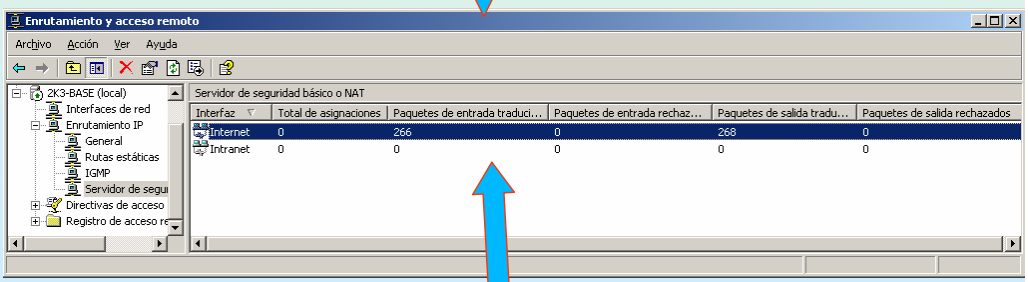
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Realizar unha conexión dende o cliente

Neste caso abrirase dous navegadores web no cliente (www.google.es e www.usc.es). Observar o que acontece no servidor NAT



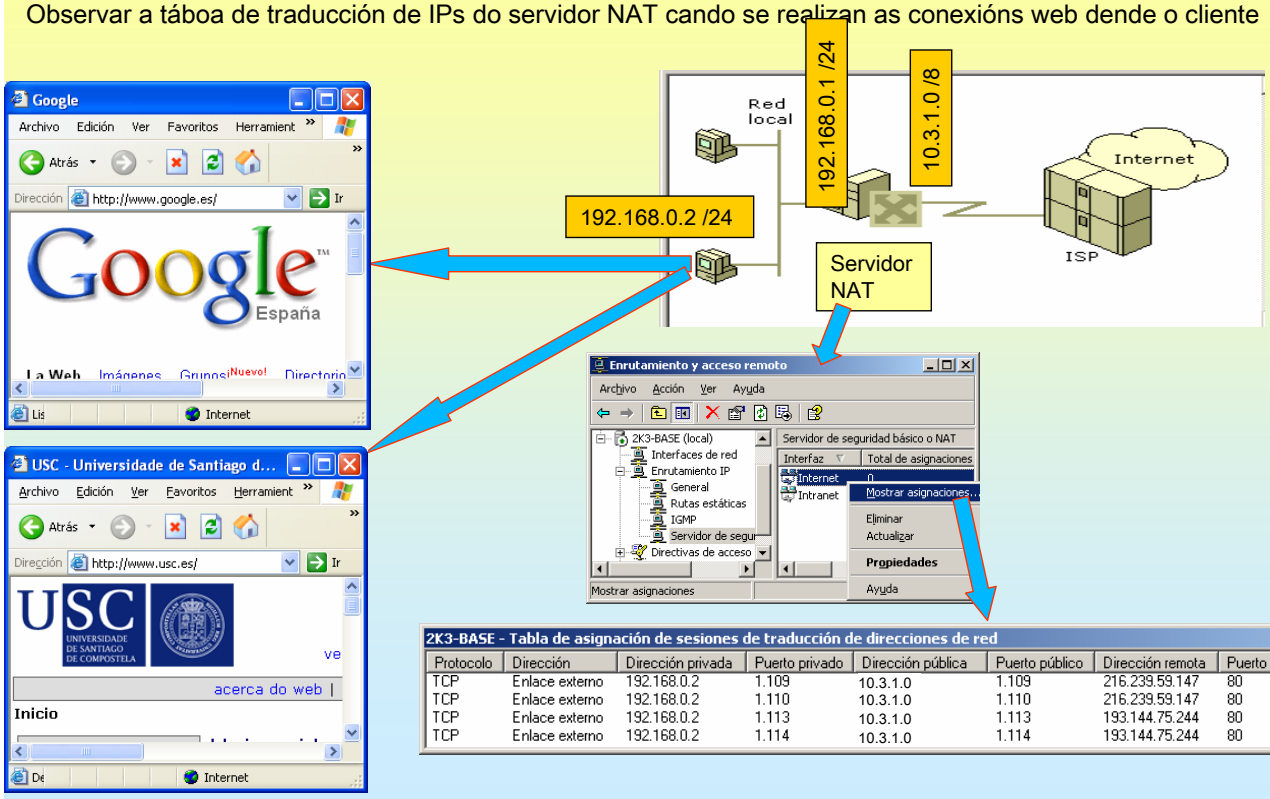


Observar as estadísticas

7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Táboa NAT

Observar a táboa de traducción de IPs do servidor NAT cando se realizan as conexións web dende o cliente



2K3-BASE - Tabla de asignación de sesiones de traducción de direcciones de red

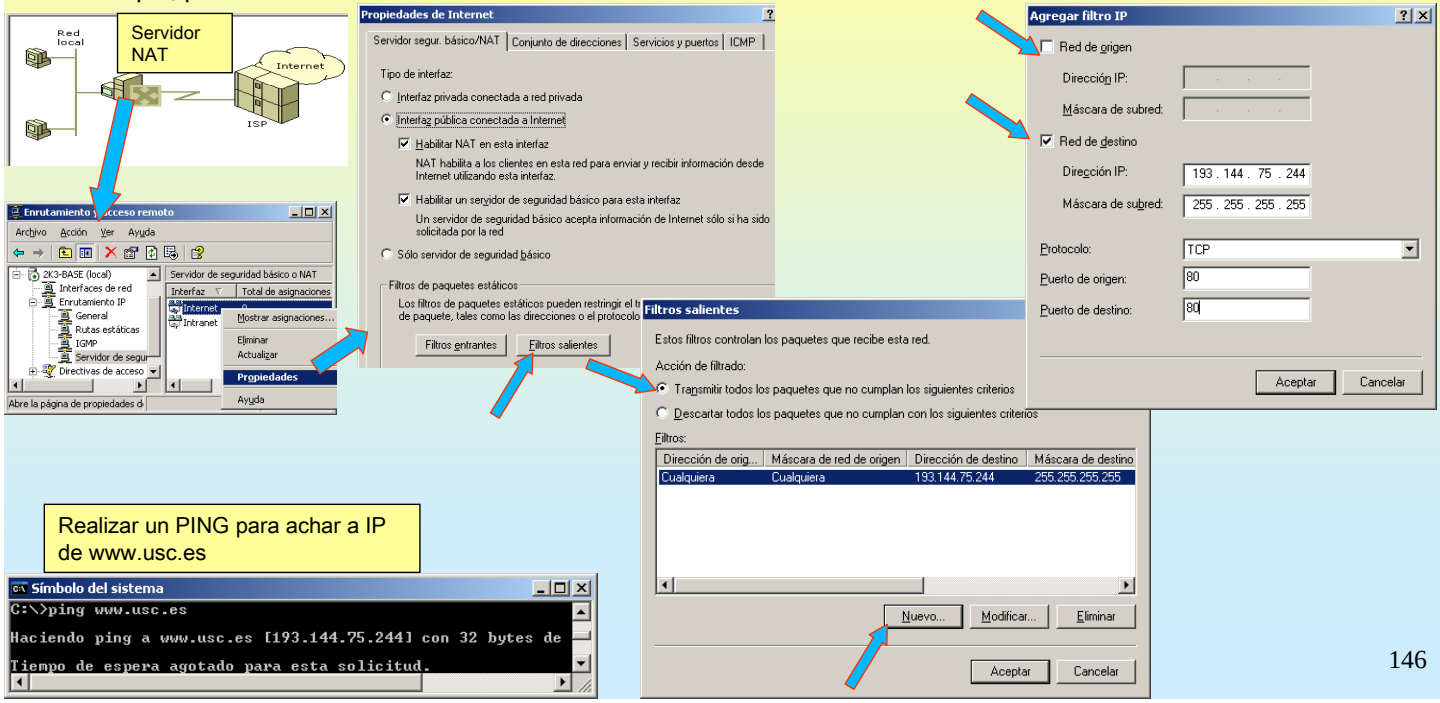
Protocolo	Dirección	Dirección privada	Puerto privado	Dirección pública	Puerto público	Dirección remota	Puerto remoto	Inactivo
TCP	Enlace externo	192.168.0.2	1.109	10.3.1.0	1.109	216.239.59.147	80	3
TCP	Enlace externo	192.168.0.2	1.110	10.3.1.0	1.110	216.239.59.147	80	3
TCP	Enlace externo	192.168.0.2	1.113	10.3.1.0	1.113	193.144.75.244	80	4
TCP	Enlace externo	192.168.0.2	1.114	10.3.1.0	1.114	193.144.75.244	80	4

7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ Filtros

No servidor NAT pódense configurar que IPs internas poden ou non poden saír a internet.
Tamén se pode configurar a que IPs se poden ou non se poden conectar os equipos locais.

Por exemplo, prohibir os clientes web internos conectarse ó servidor web da USC



Realizar un PING para achar a IP de www.usc.es

7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ NAT inverso

NAT proporciona ós equipos dunha LAN a posibilidade de conectarse a internet.
Pero, ¿que sucedede que si desde internet se desexa conectarse á LAN?, pois que nunca se vai poder chegara ningún equipo da LAN:

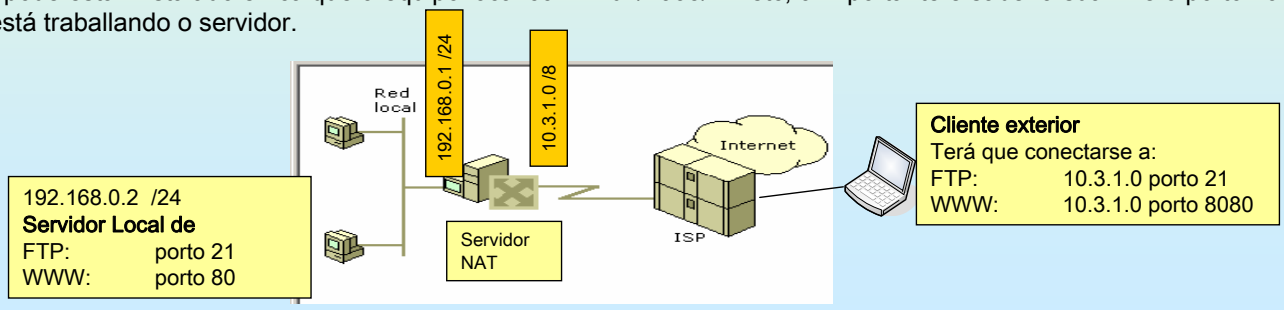
1º.- Porque non se saben as súas IPs.
2º.- Ó ser IPs privadas ningún router público ten entradas para encamiñar cara esas IPs.

Pois aínda así deséxase configurar un servidor web/FTP local ó cal se poida acceder dende o exterior. Para iso débese facer NAT inverso:

Os clientes de internet deben conectarse:
- á IP pública do servidor NAT (neste exemplo 10.3.1.0)
- un porto, con ese porto o Servidor NAT manda a petición a un equipo interno da LAN.

Neste exemplo vaise instalar IIS (con servicio FTP) nun XP cliente da rede local. A instalación do IIS é semellante a estudiada nos casos anteriores para windows 2003.

O IIS pode estar instalado en calquera equipo local con Linux/2003/XP etc, o importante e saber a súa IP e o porto no que está traballando o servidor.



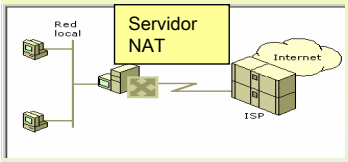
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

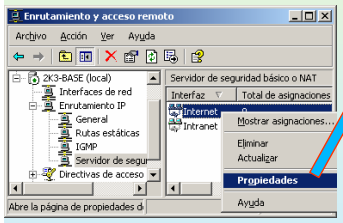
7.- NAT (Network Address Translation, Tradución de direccións de rede)

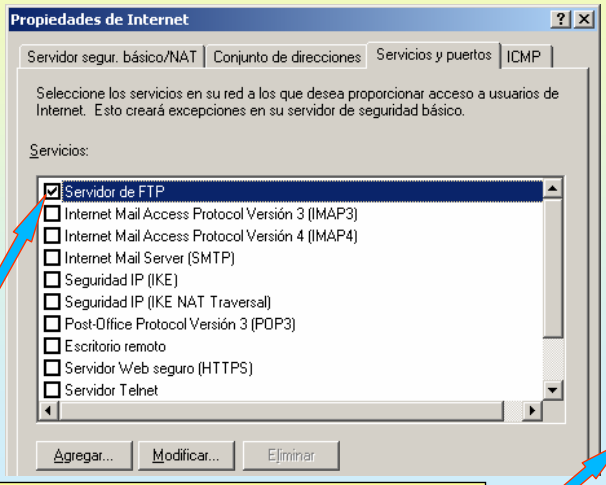
☞ NAT inverso: Dar paso ó servidor FTP local

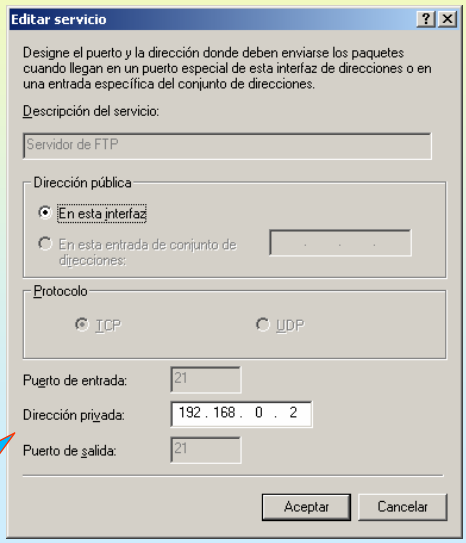
1º A vista da imaxe anterior desexase que cando un cliente de internet se conecte a 10.3.1.0:21 esto se traduza en 192.168.0.2:21. Pero hai un problema que é que este servidor de NAT tamén ten un sitio FTP (sitio FTP predeterminado) traballando nese porto, para solucionar o problema pódese facer:

1º.- Que o servidor NAT poña esa conexión o servidor FTP local noutro porto.
2º.- Cambiar o porto no que atende o Sitio Web Predeterminado do servidor 10.3.1.0
3º.- Deter o Sitio Web predeterminado. Esta é a que se vai seguir.









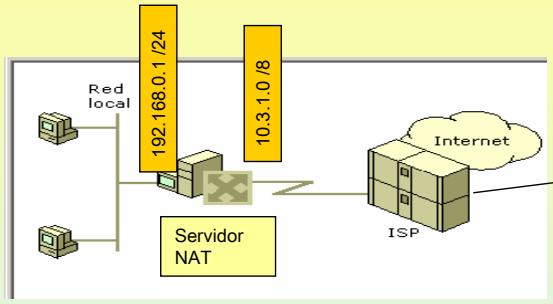
Configurar a IP local a cal se redirecionen as peticións FTP que reciba o servidor NAT.

Observar que os portos xa está por defecto tanto o de entrada como o público

7.- NAT (Network Address Translation, Tradución de direccións de rede)

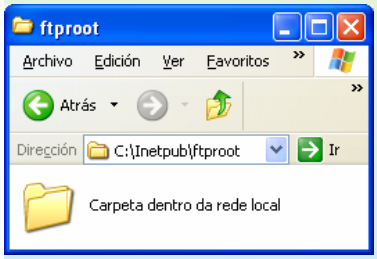
☞ NAT inverso: Dar paso ó servidor FTP local

Probar que dende un equipo exterior á rede local se poida acceder ó servidor FTP Local



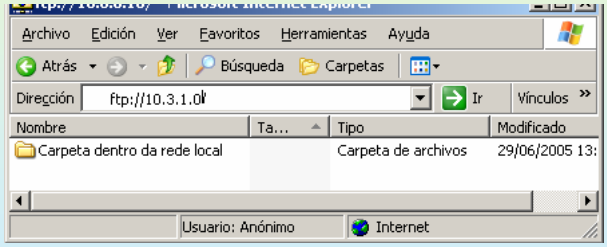
192.168.0.2 /24
Servidor Local de
FTP: porto 21

Cliente exterior
Terá que conectarse a:
FTP: 10.3.1.0 porto 21



Carpeta do sitio FTP local

Realiza a tradución de
10.3.1.0:21 a
192.168.0.2:21



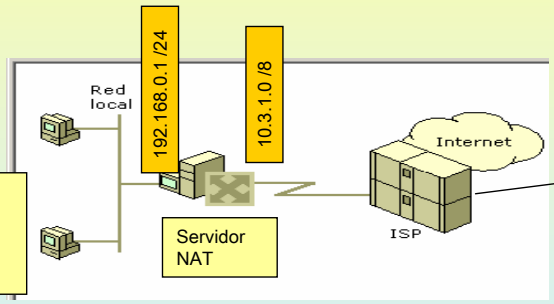
Acceso ó sitio FTP Local

7.- NAT (Network Address Translation, Tradución de direccións de rede)

☞ NAT inverso: Dar paso ó servidor WEB local

Neste caso para conectarse dende o exterior precisase configurar no servidor NAT que cando reciba unha petición dende internet a 10.3.1.0:8080 esta a envío o equipo local 192.168.0.2:80.

Neste caso, ó esixir ó cliente, que se ten que conectar ó porto 8080 non hai nada que facer servidor 10.3.1.0 pois non usa este porto.



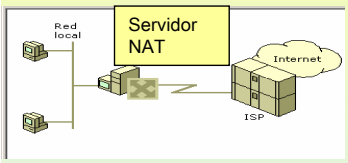
192.168.0.2 /24
Servidor Local de
FTP: porto 21
WWW: porto 80

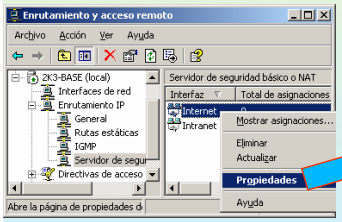
Cliente exterior
Terá que conectarse a:
FTP: 10.3.1.0 porto 21
WWW: 10.3.1.0 porto 8080

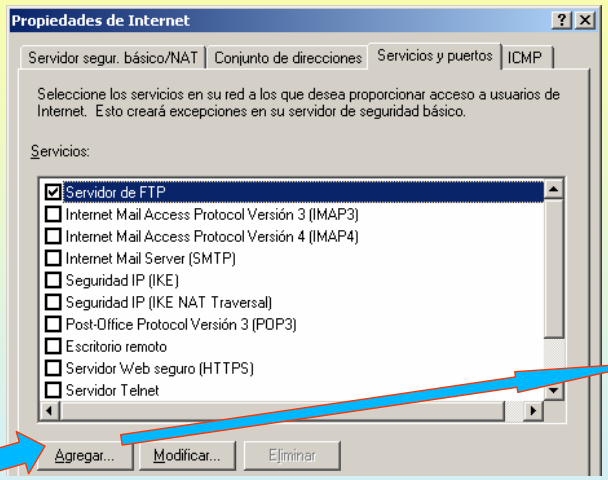
7.- NAT (Network Address Translation, Tradución de direccións de rede)

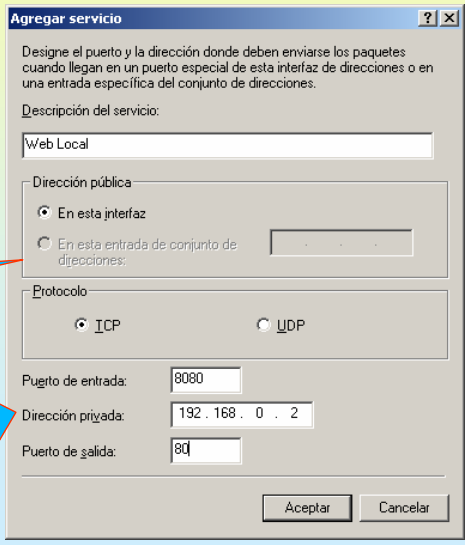
☞ NAT inverso: Dar paso ó servidor WEB local

Neste exemplo ó porto ó que se vai configurar para redirecionar 8080 non é un dos ben coñecidos co cal hai no servidor NAT todo para que se redirecione correctamente









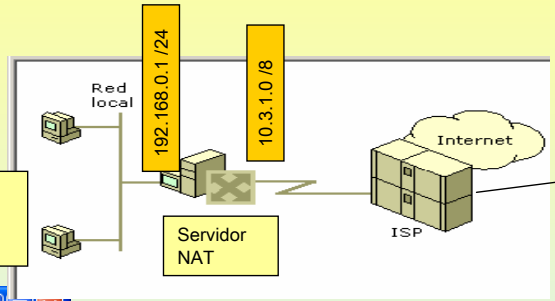
Configurar:
O porto polo que se van recibir as peticións na ip 10.3.1.0
A IP local a onde se mandarán as peticións
O porto onde estará escoitando o servidor local

SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

7.- NAT (Network Address Translation, Tradución de direccións de rede)

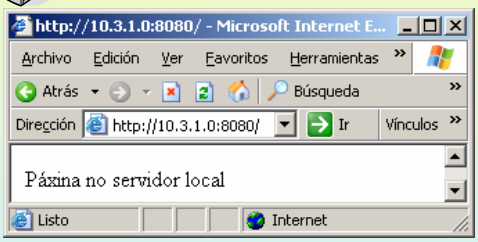
☞ NAT inverso: Dar paso ó servidor WEB local

Probar dende o exterior a conexión ó web local



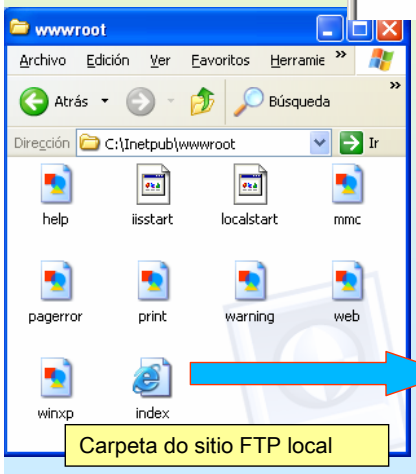
192.168.0.2 /24
Servidor Local de
WWW: porto 80

Cliente exterior
Terá que conectarse a:
WWW: 10.3.1.0 porto 8080

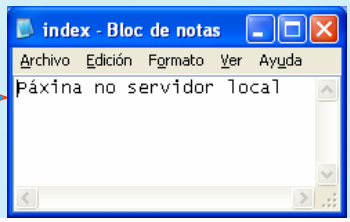


Realiza a tradución de
10.3.1.0:8080 a
192.168.0.2:80

Acceso ó sitio Web Local



Carpeta do sitio FTP local



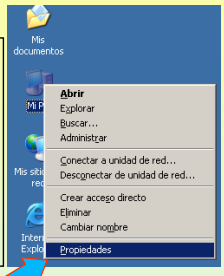
8.- ESCRITORIO REMOTO – TERMINAL SERVER

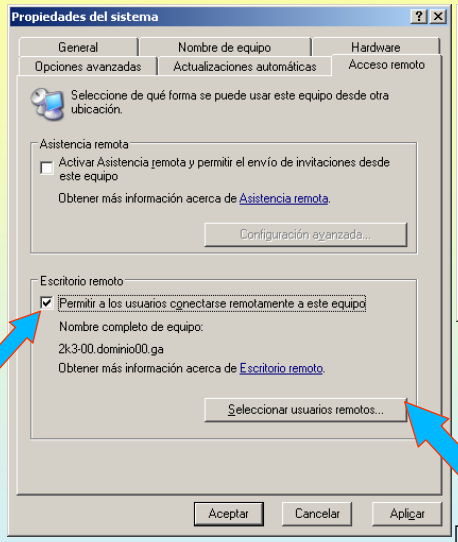
☞ ESCRITORIO REMOTO (MINI-TERMINAL SERVER)

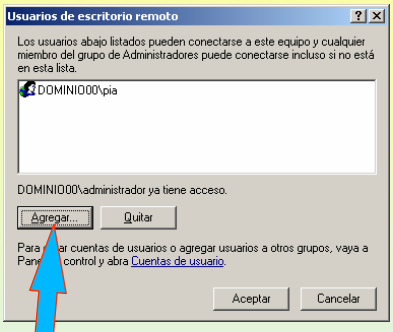
Permítelle ós usuarios conectarse a un servidor remotamente dende un cliente. O server fará o traballo e non o cliente que só recibirá pantallas do servidor.

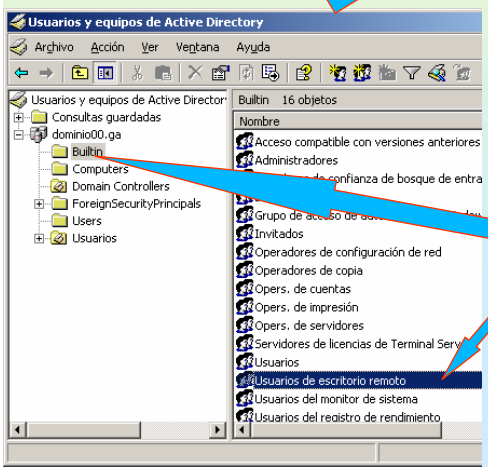
Activando o escritorio remoto de 2003 pódense ter 3 sesións no mesmo servidor (2 remotas e 1 directa), ...

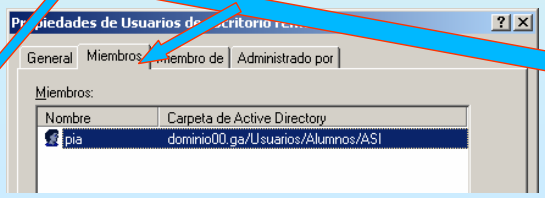
No caso do XP, só se pode ter un usuario, ben directo ou ben remoto.











Para que un usurario, non administrador, poida conectarse remotamente, debe pertencer ó grupo de Usuarios de Escritorio Remoto. Existen dúas formas de facelo.

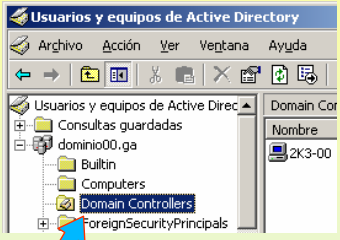
Para activar o escritorio remoto non é preciso o Active Directory.

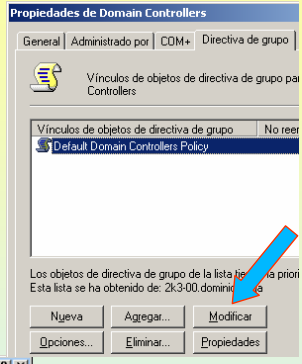
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

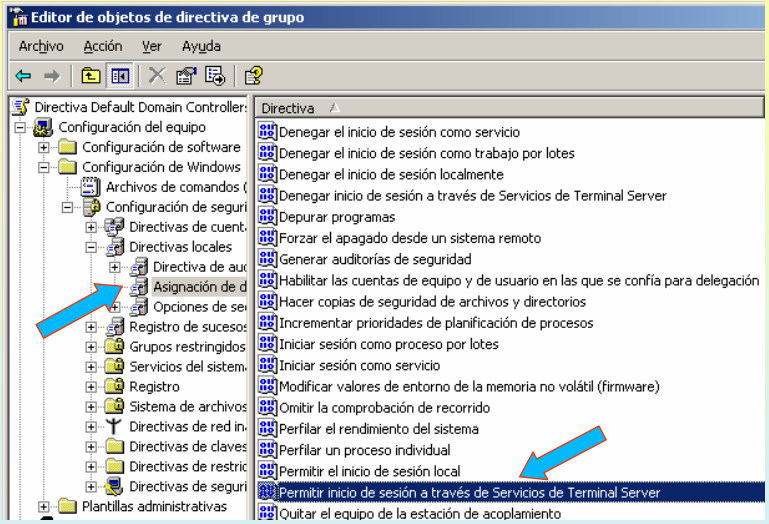
8.- ESCRITORIO REMOTO – TERMINAL SERVER

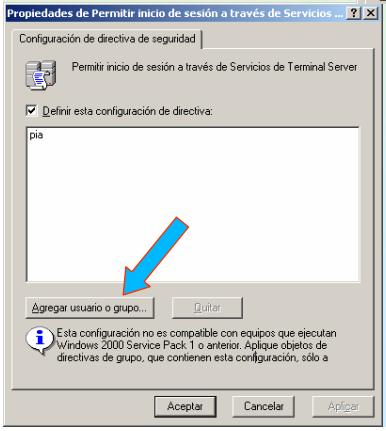
☞ ESCRITORIO REMOTO (MINI-TERMINAL SERVER)

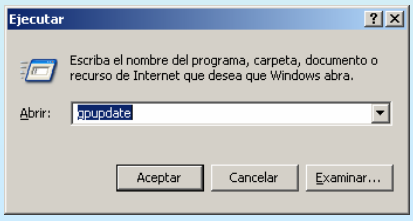
Ademais é preciso configurar a directiva de **Inicio de Sesión por Terminal Server** para usuarios non administradores.







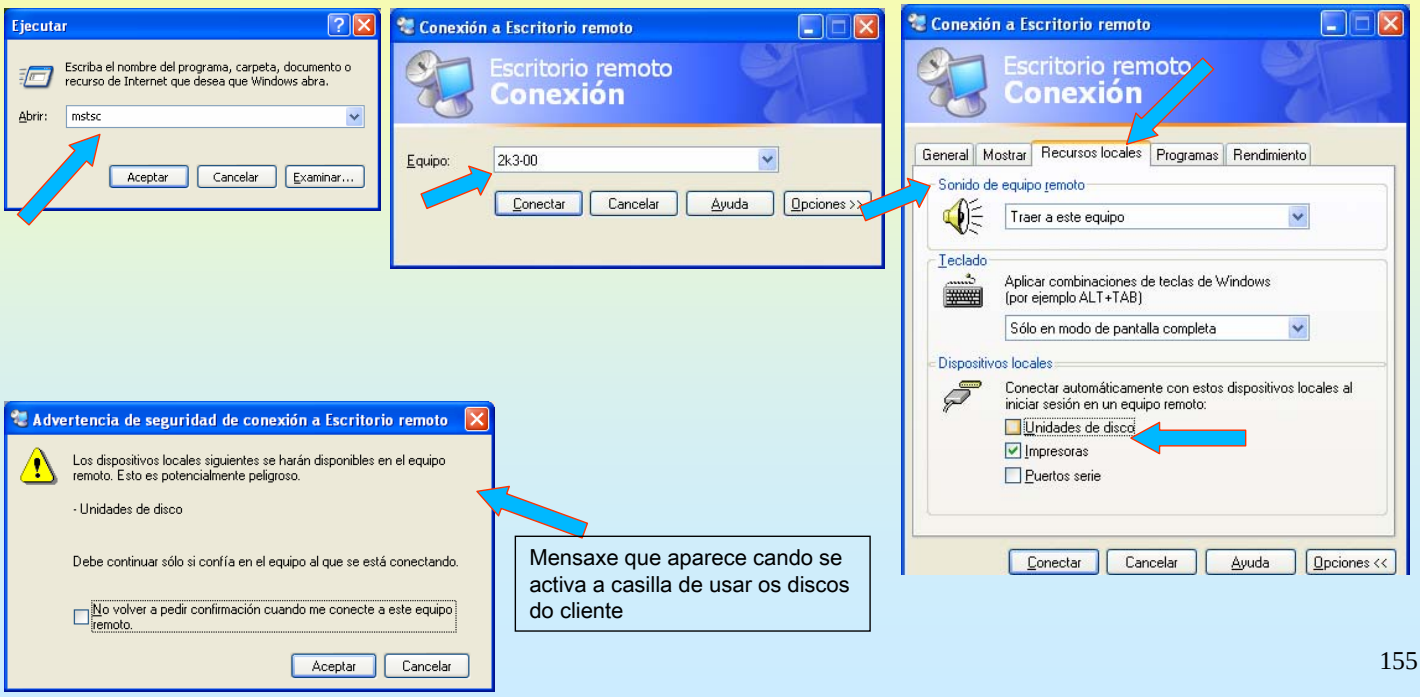




8.- ESCRITORIO REMOTO – TERMINAL SERVER

☞ CONEXIÓN A ESCRITORIO REMOTO

Dende outro equipo iniciar o **Microsoft Terminal Server Cliente (mstsc)**. Se se desexa pódese configurar para que conecte no server as impresoras e os discos locais. Deste xeito pódense copiar datos do servidor ós discos do cliente ou imprimir dende unha aplicación do servidor na impresora do cliente.



Mensaxe que aparece cando se activa a casilla de usar os discos do cliente

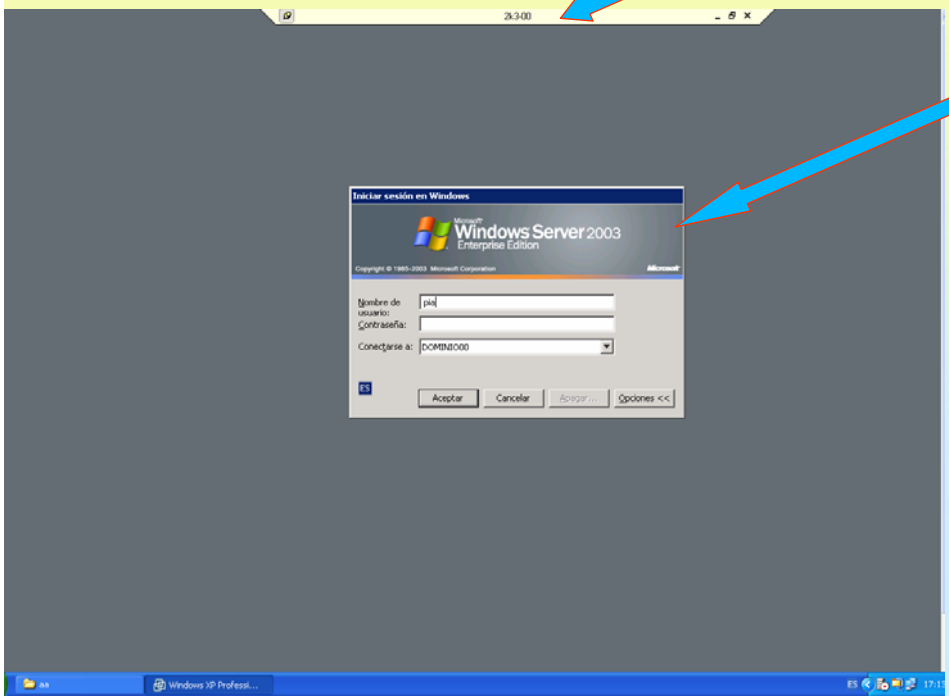
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

8.- ESCRITORIO REMOTO – TERMINAL SERVER

☞ PANTALLA DE CONEXIÓN Ó ESCRITORIO REMOTO

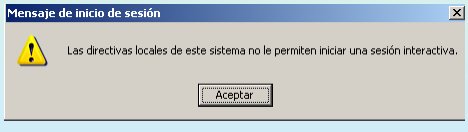
Contrasinal, permisos, ...

Solapa indicando o nome do servidor de Terminal Server (Escritorio Remoto)



Cadro de diálogo para validación do usuario no servidor de terminais.

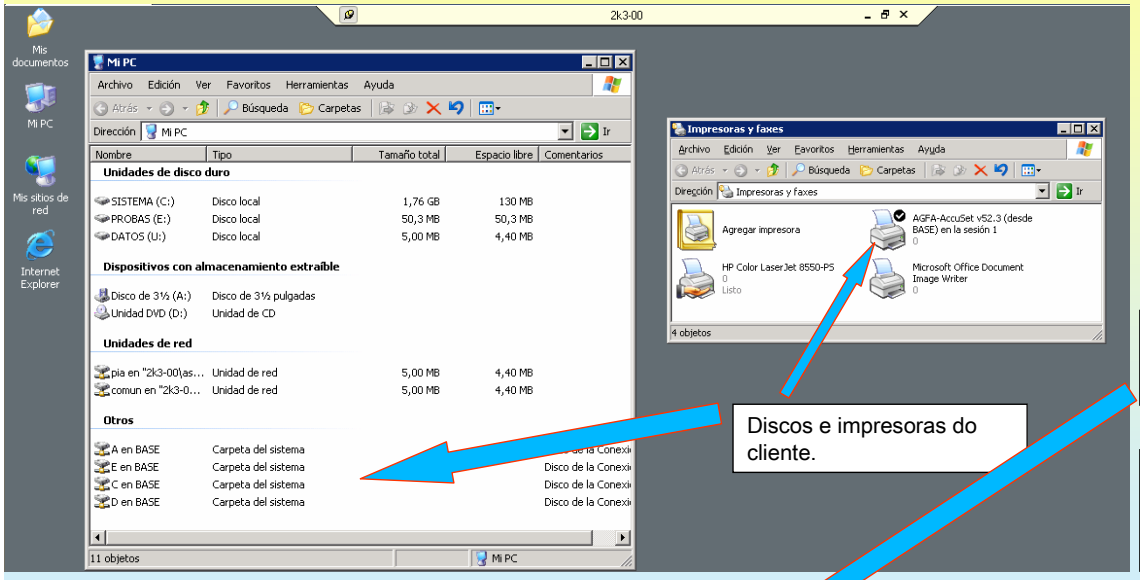
Mensaxe que aparece cando non se configura a directiva anterior (Transparencia 93)



8.- ESCRITORIO REMOTO – TERMINAL SERVER

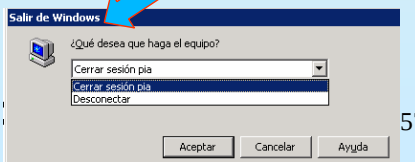
☞ O ESCRITORIO REMOTO

Unha vez dentro do escritorio remoto pódense executar as aplicacións do server tal e como se se estivera sentado fisicamente diante do server. O server só envía mapas de bits ó cliente o procesamento faino o servidor.



O cliente de TS minimizado na estación de traballo

Ó saír non existe a opción de apagar para os usuarios normais, pois apagaríase o servidor



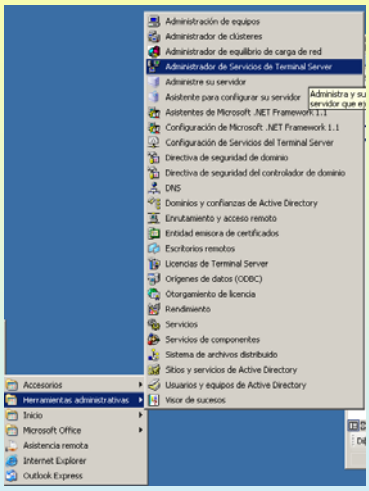
57

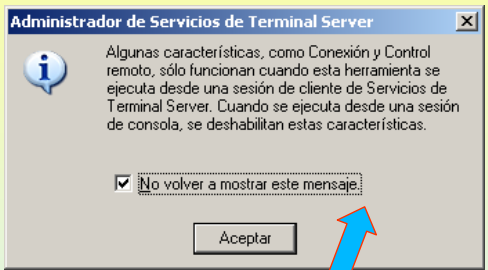
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

8.- ESCRITORIO REMOTO – TERMINAL SERVER

☞ ADMINISTRAR OS SERVICIOS DE TERMINAL SERVER

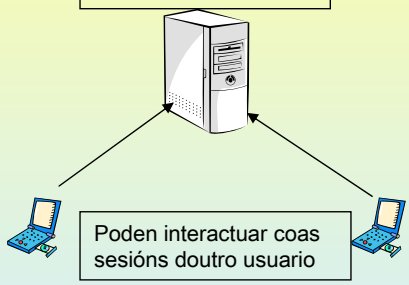
Dende o server pódense ver os usuarios conectados, as súas sesións e os procesos que se están executando, ...
Pero non se pode interactuar coas sesión dos usuarios. Función débese realizar dende outro cliente, esteo é para ver o escritorio dun usuario é preciso conectarse ó TS dende outro cliente.





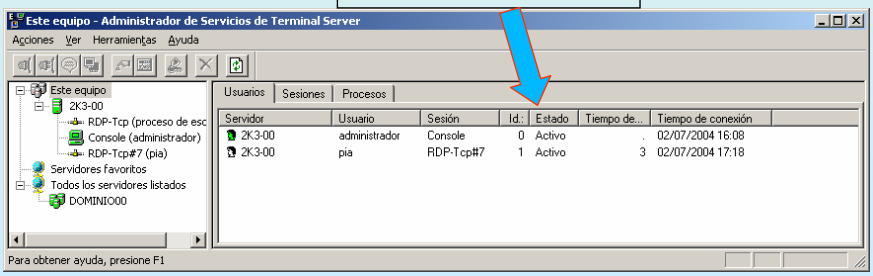
Aviso que indica que dende o servidor non están dispoñibles algunhas funcións

Non pode interactuar coas sesións abertas



Poden interactuar coas sesións doutro usuario

Estado actual das sesións



158

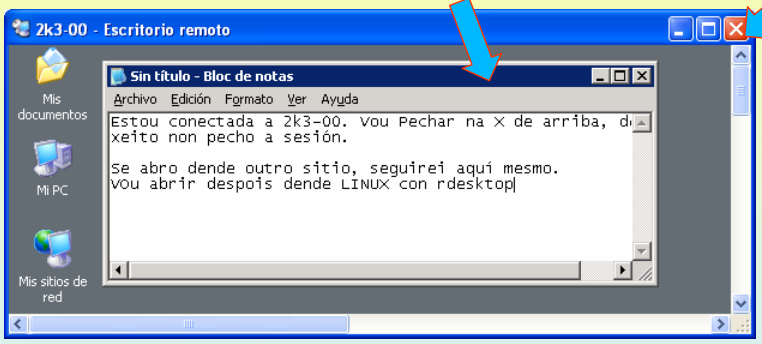
8.- ESCRITORIO REMOTO – TERMINAL SERVER

☞ PECHAR O ESCRITORIO REMOTO NO CANTO DE SAÍR

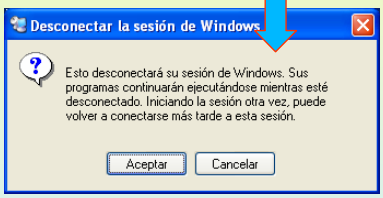
Se pecha o Escritorio Remoto, a sesión no servidor segue activada e cando PIA, neste caso, se volva a conectar seguira na sesión no mesmo sitio onde a deixou. Esto é util para poder cambiarse de ordenador cliente sen pechar ningún programa da sesión.

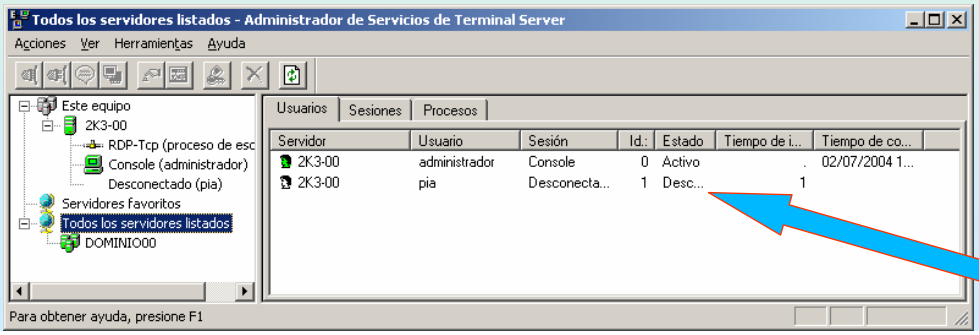
Documento de traballo de Pia

Peche da sesión sen saír



Aviso que di que os programas seguen executándose





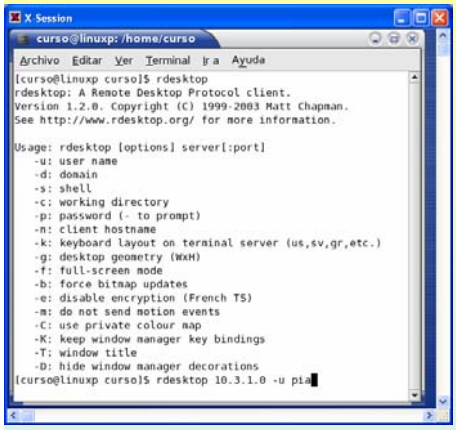
Esta opción débese usar con moito tento, pois se se pechan deste xeito 2 sesións, xa non se poderá conectar un novo usuario, pois as dúas sesións dispoñibles estarían ocupadas.

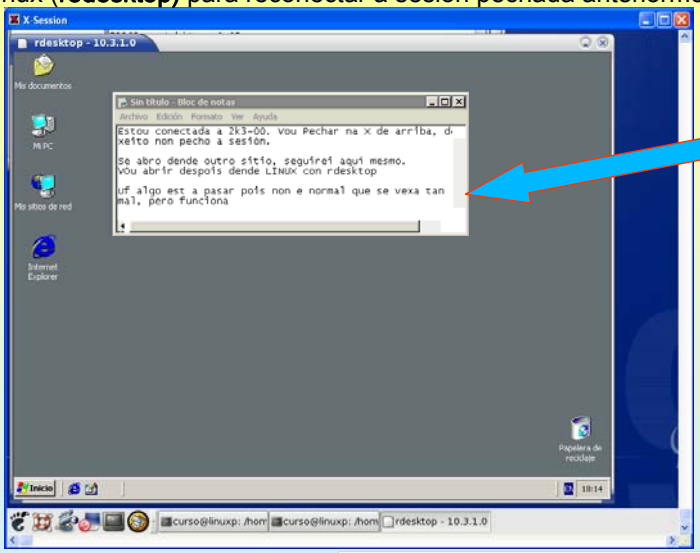
SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

8.- ESCRITORIO REMOTO – TERMINAL SERVER

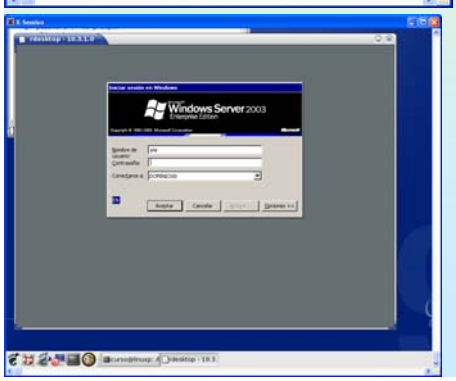
☞ RDESKTOP: CLIENTE DE TERMINAL SERVER DE LINUX

Nesta ocasión úsase un cliente de Linux (**redesktop**) para reconectar a sesión pechada anteriormente.

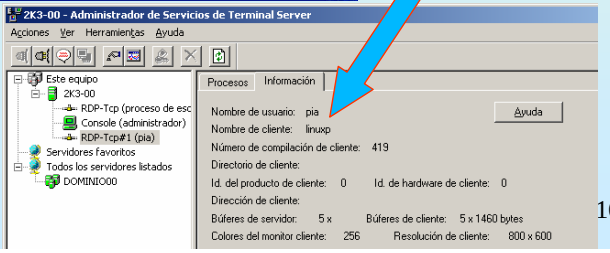




Pia continúa traballando no lugar no que deixou anteriormente o cliente de TS



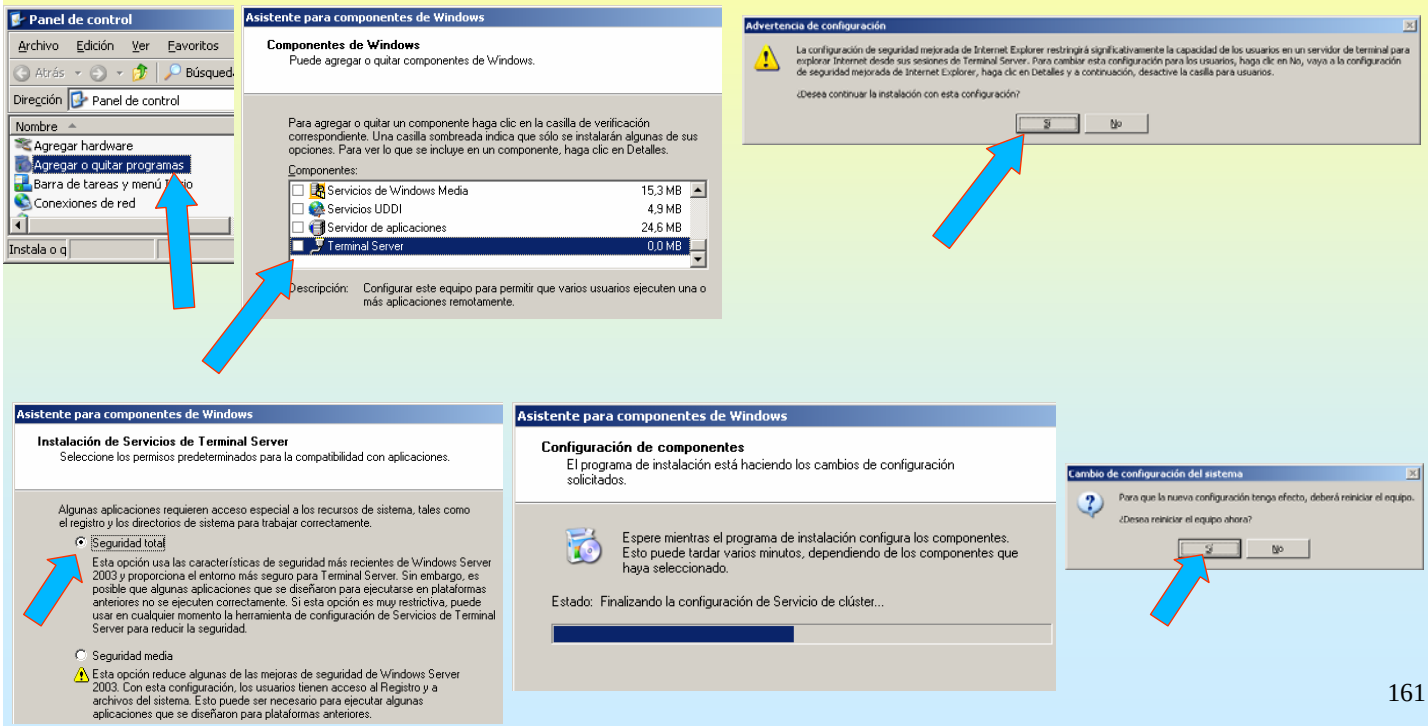
Información do Administrador de TS indicando p.e. Dende onde está Pia conectada



8.- ESCRITORIO REMOTO – TERMINAL SERVER

☞ INSTALAR TS COMPLETO

Para eliminar o límite de dúas sesións remotas débese instalar o TS. Se non se instala o servidor de licencias de TS este servidor caducará ós 120 días. A partir dese intre só poderán entrar os administradores

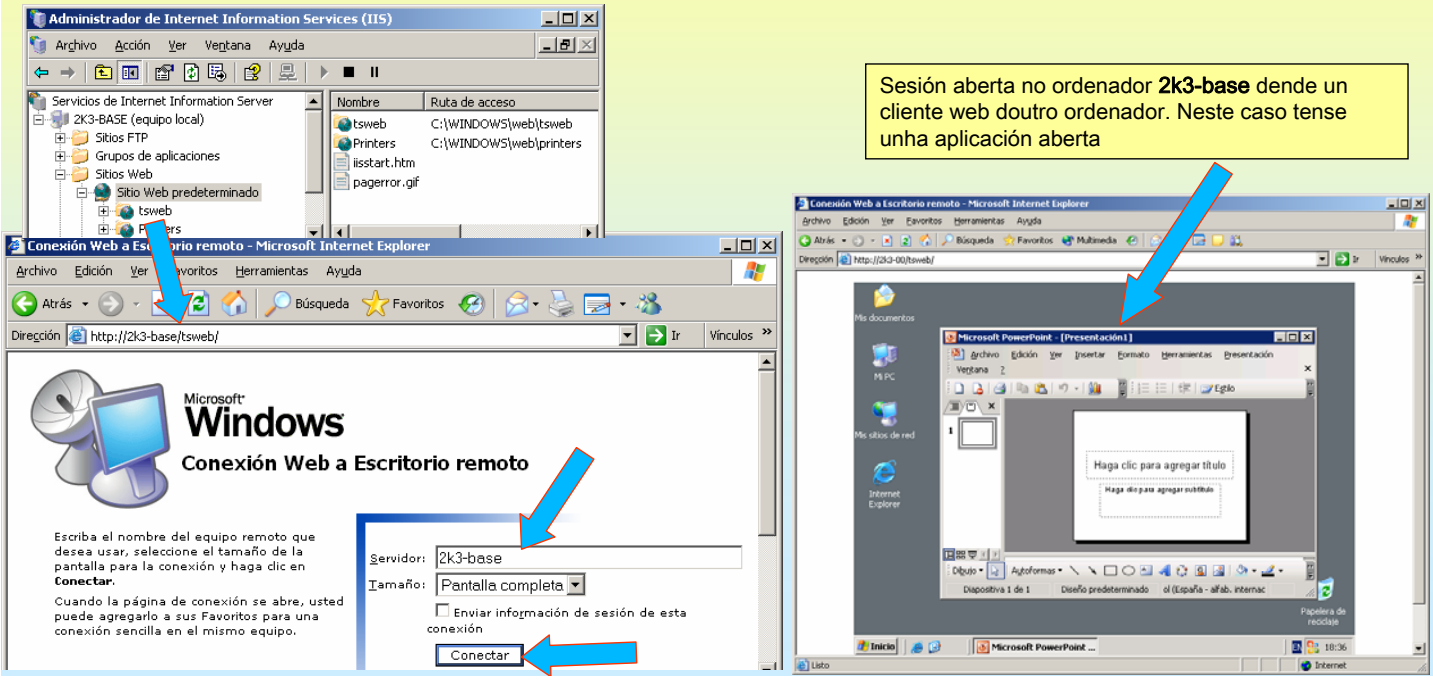


SERVIZOS INTERNET/INTRANET EN WINDOWS 2003

8.- ESCRITORIO REMOTO – TERMINAL SERVER

☞ TERMINAL SERVER WEB – ESCRITORIO REMOTO A TRAVÉS DO WEB

En esencia consiste en abrir unha sesión nun equipo, que ofreza esa posibilidade, tal e como se se estivera fisicamente sentado diante del, pero neste caso estaríase noutro ordenador.



Resolución dun exame prototipo de redes de 1º ASI e SIMR de 1º DAI

Ver. 3.0 Modificado 28-6-2004

Reseñas bibliográficas

Os libros que usamos para redes en 1º de ASI e en Proxecto Integrado de 2º ASI son:

Notar que en Proxecto Integrado cóllense 2 meses para rematar a formación teórica de redes, (sobre todo en redes de alta velocidade e WAN: RDSI, X.25, FRAME RELAY, GIGABIT ETHERNET e ATM, xerarquías dixitais plesiócronas e síncronas, etc.)

[STAL97] STALLINGS, WILLIAN. *Comunicaciones y redes de computadores, 5ª Edición.* PRETINCE HALL IBERIA, Madrid, 1997

[TANE97] TANENBAUM, ANDREW S. *Redes de computadores, 3ª Edición.* PRETINCE HALL HISPANOAMERICANA, México, 1997

[COME96] COMER , DOUGLAS E. *Redes globales de información con internet y TCP/IP. Principios básicos, protocolos y arquitectura, 3ª Edición.* PRETINCE HALL HISPANOAMERICANA, México, 1996

[KR-REDES] *Microsoft Windows NT SERVER, Kit de Recurso. Guía de redes* McGraw-Hill Interamericana de España. Madrid, 1997

[KR-INTERNET] *Microsoft Windows NT SERVER, Kit de Recurso. Guía de Internet* McGraw-Hill Interamericana de España. Madrid, 1997

[GARC90] GARCÍA TOMÁS, J. *Sistemas y redes Teleinformáticas, 1ª Edición.* RA-MA, Madrid, 1990

[GARC97] GARCÍA TOMÁS, J., FERRADO, G. S., VELTHUS, P. *Redes de alta velocidade, 1ª Edición.* RA-MA, Madrid, 1997

[ABAD97] ABAD, A., MADRID, .M. *Redes de área local, (*Libro do ciclo). McGraw-Hill Interamericana de España. Madrid, 1997

Notas a bibliografía

Os libros [STAL97] e [TANE97] son complementarios, moitas das cousas concernentes a redes LANs (IEEE 802.x) veñen nos dous, só que a min paréceme que están explicadas dunha forma máis clara e vistosa en [STAL97]

Con respecto a X.25, FR, ATM, RDSI, [GARC97] poderíase dicir qué unha copia de [STAL97], pero hai cousas que veñen mellor explicadas no primeiro.

Para entender as xerarquías é aconsellable botarlle un ollo ó apartado 2.4.4, a partir da páxina 121, de [TANE97]

Para TCP/IP, par min o mellor libro é [COME96], podendo complementar con [KR-REDES], [KR-INTERNET]

Con respecto ó libro de texto de redes [ABAD97], é moi simple, algunhas veces ata ó punto de que comete erros.

Grandes bloques de temas

Medios de Transmisión: [TANE97] Páx. 82-101
[STAL97], Capítulo 3

Nivel de control de enlace de datos: [ABAD97], Unidade 4, coidado que no HDLC ó final ten erros, Xa vos enviarei eu un ficheiro sobre HDLC
[STAL97], Capítulo 6

OSI a nivel xeral: Con mirarse a unidade de traballo 4 que vos envío, creo que xa chega.

IEEE 802.x: [TANE97] Tema 4, en particular a sección 4.3 e 4.5 (FDDI, inalámbricas)
[STAL97], Capítulos 12, 13 (a min gústame máis este, pero tamén hai que mirar o anterior)
[TANE97], Para pontes, sección 4.4
[STAL97], Para pontes,capitulo 14
Para ethernet podedes miar as transparencias que vos adxunto.

Grandes bloques de temas

Nivel de rede: [TANE97] Tema 5, pero é un auténtico rolo, existen explicacións mellores por aí
[STAL97], Capítulo 16, seccións 16.1-16.4: moito máis claro.
Routers: [STAL97], Capítulo 16
[TANE97] Sección 5.4
[COME96], as seccións 8.4 ata ó final

Conmutación xeral: [TANE97] Páx. 130-134
[GARC90], capítulo 12

Conmutación circuítos, RDSI-BE: [STAL97], Capítulo 8
[GARC97], capítulo 5

Conmutación paquetes, X.25: [STAL97], Capítulo 9
[GARC90], capítulo 14,15,16

Retransmisión de tramas, Frame Relay: [STAL97], Capítulo 10
[GARC97], capítulo 6

ATM, RDSI-BA: [STAL97], Capítulo 11
[GARC97], Temas 7, 8, 9

TCP / IP [COME96], Arquitectura : gráficos tema 11 e gráfico páx. 474.
[COME96], Direccións IP, sección 4.3, 4.5, 4.7.1, 4.9, 4.11, 4.13
[COME96], Máscaras, 10.8
[COME96], ARP, tema 5
[COME96], IP, tema 7
[COME96], Ruteo básico, tema 11. Ruteo real, Tema 10, en concreto algoritmo da sección10.12
[COME96], TCP/UDP, temas 12 e13

Exercicio

Unha empresa merca a INTERNIC as direccións **11.0.0.0 e 130.1.0.0.**

O dominio que xestiona denomínase **exame.es**

A rede TCP/IP está sobre 2 estándares distintos: **IEEE 802.3 e IEEE 802.5**

A topoloxía da rede está na seguinte figura.

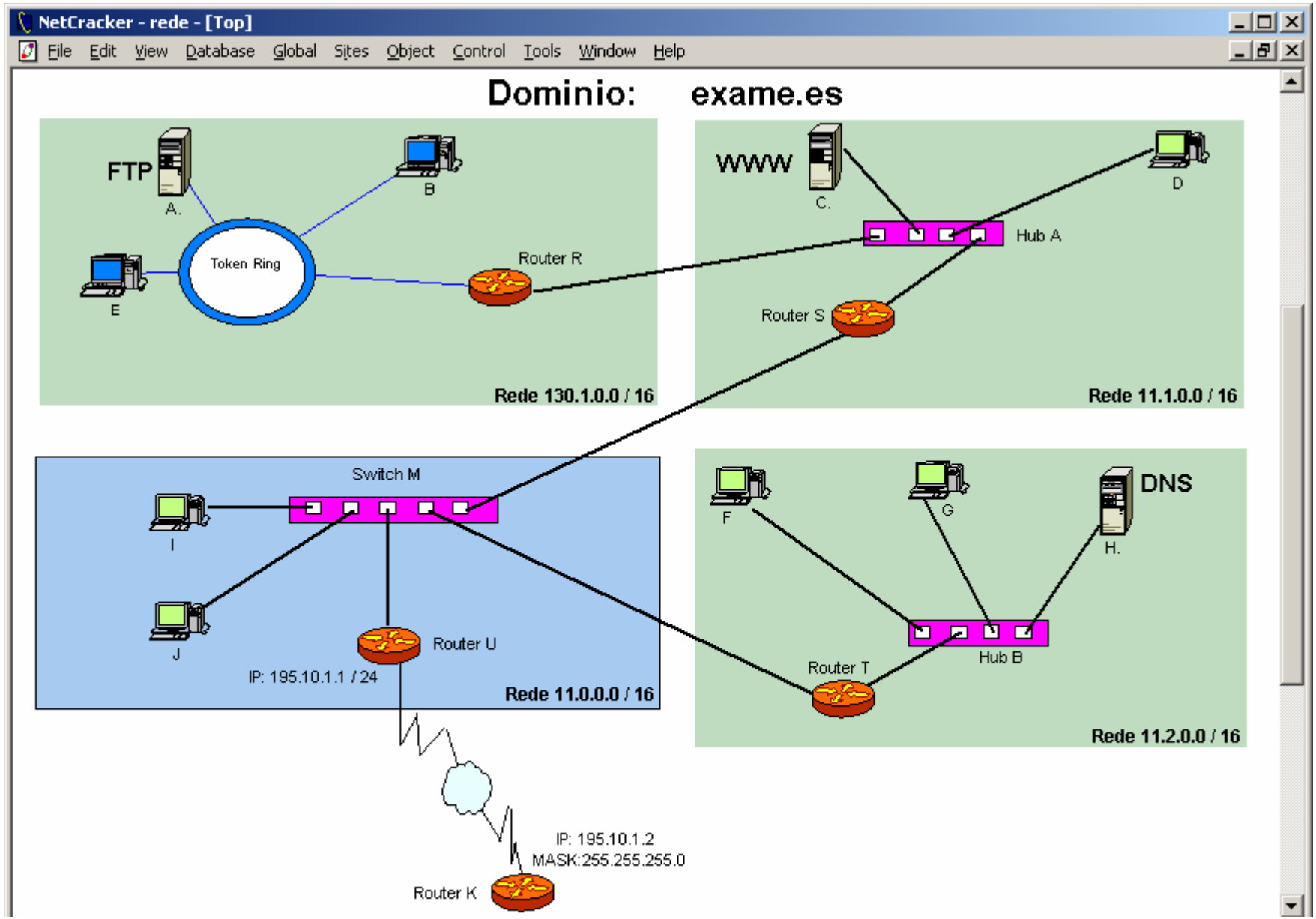
O router K pertence ó ISP (provedor de servicios de internet) (non o xestiona ó administrador da empresa). Só se usará nunha parte do exercicio, para indicar como sería parte da súa táboa de ruteo.

A rede está deseñada nun programa de Deseño e análise de redes: NetCracker Professional 3.2

Notar que a rede 11.0.0.0 está subnetada a unha rede de clase B, esto é máscara 255.255.0.0. **OLLO, unha das subredes é 11.0.0.0 /255.255.0.0, NON se soen facer subredes collendo a subrede 11.0.0.0 /255.255.0.0, en tal caso 11.1.0.0/255.255.0.0, etc.**

Nota: as letras, A, B, C, ... Supóñense que son as direccións MAC dos equipos.

Dada a seguinte rede, que usa a pila de protocolos TCP/IP sobre ETHERNET e TOKEN RING



Enunciado

1.a.- Configuración manual de tódolos equipos, para que todo ordenador poida ter acceso á intranet exame.es e a internet.

Ordenadores: Enderezo IP, máscara, porta de enlace e servidor de DNS (supoñer un só router de saída e un só servidor DNS)
Routers: Enderezo IP, máscara, táboa estática de encamiñamento. (non poñer porta de enlace dos routers). Incluído o router K.
Servidor DNS: Configurar o servidor de DNS, dun xeito xeral, para que todo equipo poida acceder www.exame.es e a ftp.exame.es
Só indicar como quedaría o ficheiro de configuración de DNS

1.b.- A rede leva unha hora funcionado e cada ordenador xa se conectou con tódolos restantes e ademais xa estiveron navegando por internet. Supoñendo que as entradas en cada táboa teñen unha duración ilimitada e as táboas un tamaño ilimitado, indica:

Táboas que se constrúen dun xeito dinámico
¿Como se construíron?
¿Cales son os seus valores actuais?
Nota*: Hai routers que teñen unha mac para cada interface, e outros unha soa mac para tódolos interfaces. Imos supoñer o último caso.*

1.c.- Indicar como se constrúen os campos Porto Destino e Porto Orixe do primeiro segmento TCP e os campos Dirección IP Orixe e Dirección IP Destino do primeiro datagrama IP, cando o ordenador con MAC J executa a seguinte sentencia:

```
>ftp ftp.exame.es
```

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

Esta pregunta é preferible dividila en dúas partes:

- Explicar como se constrúen os segmentos TCP, como se transmiten ó outro extremo e como funciona este protocolo, tendo en conta só as entidades pares de TCP.

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.

1.e.- Explica en que se diferenciaría o proceso anterior, se o que se fixese fose baixar o ficheiro proba2.txt de igual tamaño:

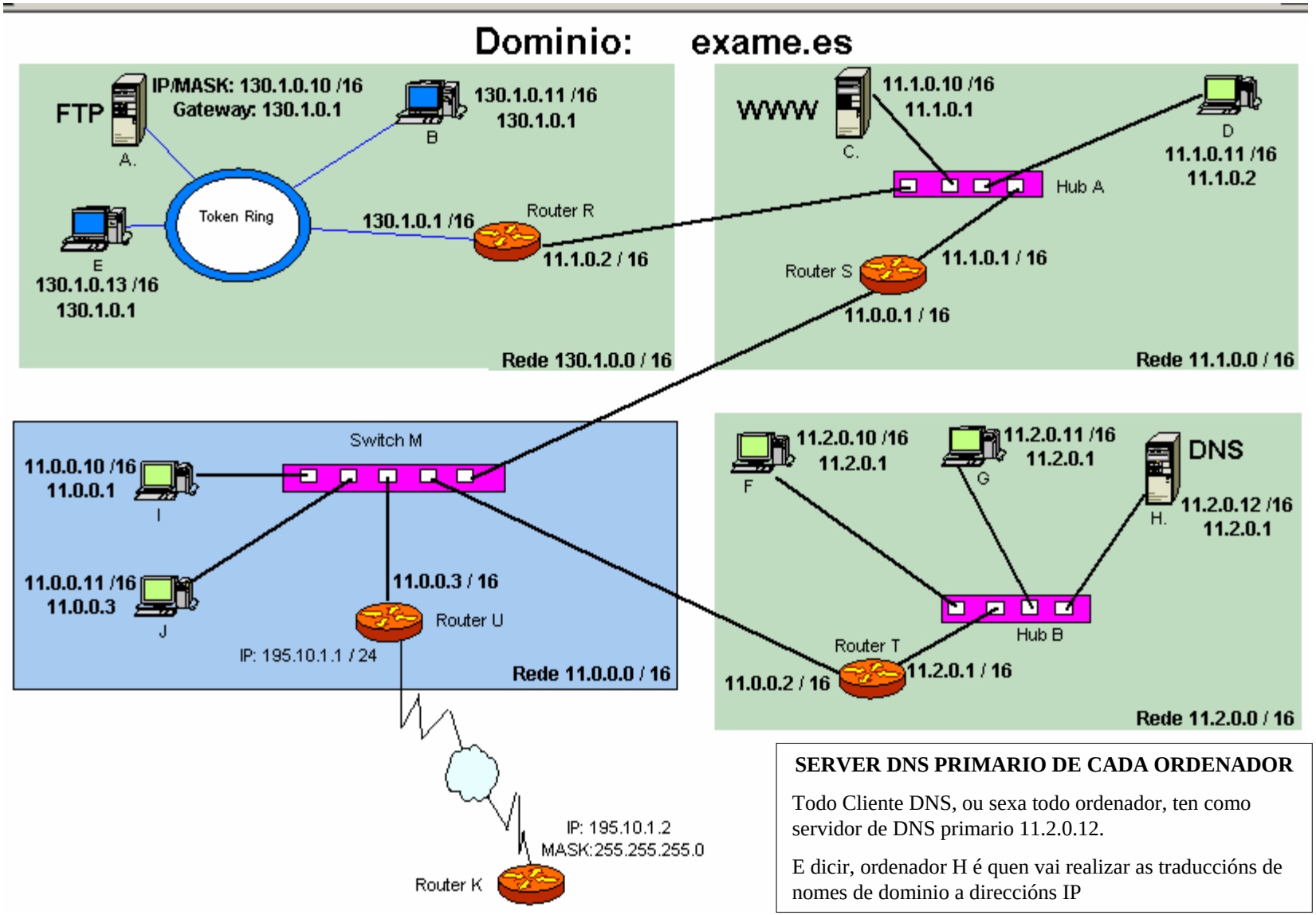
```
ftp> get proba2.txt
```

2.- Indica tódalas posibilidades de cableado, conectores e tarxetas de rede dos Host I e J en función dos distintos tipos de switch M que se poden instalar

1.a.- Configuración manual de tódolos equipos, para que todo ordenador poida ter acceso á intranet exame.es e a internet.

Ordenadores: Enderezo IP, máscara, porta de enlace e servidor de DNS (supoñer un só router de saída e un só servidor DNS)

Routers: Enderezo IP, máscara.



SERVER DNS PRIMARIO DE CADA ORDENADOR

Todo Cliente DNS, ou sexa todo ordenador, ten como servidor de DNS primario 11.2.0.12.

E dicir, ordenador H é quen vai realizar as traduccións de nomes de dominio a direccións IP

Aclaracións ó anterior

130.1.0.10 / 16 Significa
DIR IP: 130.1.0.10
Máscara Subrede: 255.255.0.0
Ou sexa, os 16 primeiros bits da máscara a 1 = 1111 1111 . 1111 1111 . 0000 0000. 0000 0000 = 255.255.0.0

Notar que a rede 11.0.0.0 está subnetada dentro da intranet, esto é, unha rede é de clase A, B, C en función da máscara, como neste caso as máscaras son /16 quere dicir que estaríamos falando de redes de clase B e non de clase A, como cabería supoñer a priori.
Co cal cóllense os 2 primeiros bytes da IP para identificar a rede. Deste xeito temos a Rede 11.1.0.0 (net id= 11.1) e distinta de 11.0.0.0 (net id = 11.0)

Todo Router ten unha dirección IP por cada rede IP á que está conectado. A IP de cada interface debe estar dentro da rede IP a que pertence a interface.

exame.es é unha intranet, que ten un router de saída cara internet (router U). O enderezo IP 195.10.1.1 de U vennos dada polo ISP (provedor de servicios de internet), aí non se podería facer nada.

O **Router K** non sería configurado polos administradores de **exame.es**, senón, polos administradores do ISP, aínda que no exercicio hai que configuralo para mirar como se tratan as redes subnetadas dende o exterior á intranet.

O **gateway, porta de enlace** ou **router** de cada equipo é o lugar por onde se vai saír da subrede cando a dirección IP de destino, non se atope na subrede. Hai equipos que están conectados a máis de un router (hosts C e D a Router S e Router R, hosts I e J a Router S, Router U e Router T).

Nos hosts pódense poñer varias portas de enlace, por orde de preferencia, pero pódese poñer unha soa. É o administrador quen debe elixir a orde de preferencia dos routers de saída ou que router seleccionar en caso de poñer un só.

Todo Router tamén leva unha dirección IP de porta de enlace á que enviar os paquetes cando non sabe como encamiñalos. Pero imos prescindir deso. Esto obriga a configurar os router ó 100%

1.a.- Configuración manual de tódolos equipos, para que todo ordenador poida ter acceso á intranet exame.es e a internet.

Routers: Táboa estática de encamiñamento. (non poñer porta de enlace dos routers). Incluído o router K

A táboa é estática porque a temos que meter á man e non varía en función da configuración da rede. Se cambiase a topoloxía da rede débense modificar as táboas de encamiñamento.

Router R		
Rede destino	**Máscara**	**Encamiñar cara**
130.1.0.0	255.255.0.0	Entregar Directamente
11.1.0.0	255.255.0.0	Entregar Directamente
0.0.0.0	0.0.0.0	11.1.0.1

Router S		
Rede Destino	**Máscara**	**Encamiñar cara**
130.1.0.0	255.255.0.0	11.1.0.2
11.1.0.0	255.255.0.0	Entregar Directamente
11.2.0.0	255.255.0.0	11.0.0.2
11.0.0.0	255.255.0.0	Entregar Directamente
0.0.0.0	0.0.0.0	11.0.0.3

FUNCIONAMENTO DUN ROUTER.
Cando lle chega un paquete colle a IP de destino do paquete e fai un AND coa máscara. O resultado compárao coa entrada correspondente en **REDE DESTINO**. Se coincide enruta para onde lle indique o campo **Encamiñar cara**.

EXEMPLO.
Chega un paquete a R con IP destino 11.1.0.1
11.1.0.1 AND 255.255.0.0 = 11.1.0.0 (lembrar operación en binario e comeza pola primeira entrada do router)
Comparar resultado con entrada correspondente: 130.1.0.0 ≠ 11.1.0.0 entón pasamos a seguinte entrada da táboa
11.1.0.1 AND 255.255.0.0 = 11.1.0.0. Comparar: 11.1.0.0 = 11.1.0.0 entón entregar directamente, esto é, ó ordenador destino está ó outro lado do router, non precisa pasar a información a outro router

0.0.0.0: significa que se chega un paquete a R, por exemplo, e non vai para ningunha das redes especificadas na táboa, pois que envíe ese paquete a outro router, neste caso a S. De feito si se segue o procedemento anterior, daría que 0.0.0.0 = 0.0.0.0. En cada router esta incidencia contémplase de distintas formas.

Notar que en R todo o que **non** vaia para 130.1.0.0 nin para 11.1.0.0 debémolo enviar a S independentemente de se vai para 11.2.0.0 ou se vai para internet, co cal non nos fai falla contemplar as redes 11.0.0.0 e 11.2.0.0 dun xeito explícito.

Por outra banda, no Router S a 3ª entrada do router (11.2.0.0) contemplámola se queremos enviar dun xeito máis rápido os paquetes que vaian para esas redes. Se non existise esa entrada na táboa sería contemplada como outro caso (0.0.0.0), co cal enviaríanse os paquetes ó Router U e este sería quen encamiñase os paquetes cara esa rede.

1.a.- Configuración manual de tódolos equipos, para que todo ordenador poida ter acceso á intranet exame.es e a internet.

Routers: Táboa estática de encamiñamento. (non poñer porta de enlace dos routers). Incluído o router K

Router U

Rede Destino	Máscara	Encamiñar cara
130.1.0.0	255.255.0.0	11.0.0.1
11.1.0.0	255.255.0.0	11.0.0.1
11.2.0.0	255.255.0.0	11.0.0.2
11.0.0.0	255.255.0.0	Entregar Directamente
195.10.1.0	255.255.255.0	Entregar Directamente
0.0.0.0	0.0.0.0	195.10.1.2

Router T

Rede Destino	Máscara	Encamiñar cara
130.1.0.0	255.255.0.0	11.0.0.1
11.1.0.0	255.255.0.0	11.0.0.1
11.2.0.0	255.255.0.0	Entregar Directamente
11.0.0.0	255.255.0.0	Entregar Directamente
0.0.0.0	0.0.0.0	11.0.0.3

ROUTER K

Rede Destino	Máscara	Encamiñar cara
130.1.0.0	255.255.0.0	195.10.1.1
11.0.0.0	255.0.0.0	195.10.1.1
.....	.	.....
.....	.	.....

Configurado polo administrador do ISP

NOTAS:

Router U: non faría falla contemplar a entrada 195.10.1.0, pois seguro que non imos ter ordenadores ó outro lado do router U, pero non pasa nada por poñelo.

ROUTER K.
Notar que o ISP non ten porque saber nada de como está rede 11.0.0.0 dentro da intranet, e dicir, non teñen porque saber si está ou non subnetada. Entón a táboa do router K debe contemplar só a rede xeral 11.0.0.0 e non cada caso particular. Ademais todas teñen en común o primeiro ítem da dirección IP: 11.x.x.x,

1.a.- Configuración manual de tódolos equipos, para que todo ordenador poida ter acceso á intranet exame.es e a internet.

Servidor DNS: Configurar o servidor de DNS, dun xeito xeral, para que todo equipo poida acceder **ftp.exame.es** e a **www.exame.es**

Só indicar como quedaría o ficheiro de configuración de DNS

Para configurar un servidor DNS, pódense usar diversas utilidades, pero o que pide o enunciado é o ficheiro resultado:

Ficheiro

```
ftp.exame.es        130.1.0.10
www.exame.es        11.1.0.10
```

Ó mesmo tempo, no servidor de DNS hai que configurar un servidor de reenvío, esto é, se o servidor de DNS local non é capaz de resolver, preguntará a outro servidor DNS, normalmente proporcionado polo ISP.

Por exemplo se F executa `ping www.iberia.com`. O ordenador F preguntaralle ó servidor de DNS local que resolva ese nome de dominio. O ficheiro de configuración do DNS local non ten esa entrada.

Entón será cando o servidor de DNS local pregunte ó servidor de DNS de reenvío. Se ese servidor non resolve, ese mesmo preguntaralle a outro servidor de DNS. Así ata resolver ou ata fallar, por non existir ese nome de dominio.

1.b.- A rede leva unha hora funcionado e cada ordenador xa se conectou con tódolos restantes e ademais xa estiveron navegando por internet. Supoñendo que as entradas en cada táboa teñen unha duración ilimitada e as táboas un tamaño ilimitado, indica:

Táboas que se constrúen dun xeito dinámico. ¿Como se construíron?. ¿Cales son os seus valores actuais?

Nota*: Hai routers que teñen unha mac para cada interface, e outros unha soa mac para tódolos interfaces. Imos supoñer o último caso.*

As táboas dinámicas son aquelas que varían no tempo, en función de parámetros como, que un ordenador estea apagado ou non, que leve un tempo sen transmitir ou que se cambie de lugar, etc.. etc..

Para construír as táboas dinámicas, primeiro hai que saber que elementos teñen táboas, de que tipo e que elementos non teñen táboas.

HUBS: traballan no nivel físico. Encárganse de mover bits e de nada máis. Non teñen capacidade para tomar decisións, pois non saben interpretar o que por el está pasando. Para nos é como se fora un "*cable*".
Ollo, hai hubs segmentables e máis tipos, que posúen intelixencia entre comiñas. Imos supoñer os hubs de toda a vida, os que son como cables. Esto é todo o que lle entra por un porto reexpídeo por tódolos portos excepto polo que entrou.

SWITCHS: é un caso particular de ponte ou bridge, só que se lle denomina así, ou conmutado, cando as redes que conecta son do mesmo tipo. Neste caso Ethernet (IEEE 802.3).

Imos supoñer, xa que o enunciado non di nada, que é unha **ponte transparente** ([TAN97], páx. 310). Esto é, ela mesma aprende a que portos están conectados os ordenadores, sen que ninguén lle especifique nada. Ou sexa, enchufar e listo. Para iso precisa dun algoritmo que vaia construíndo a táboa: **algoritmo de aprendizaxe cara atrás**

O switch entende as mensaxes do nivel 2, ou sexa, as *tramas* (Unidade de traballo 4 e transparencias Ethernet). Estas levan a dirección MAC orixe e MAC destino entre outras cousas. Esto é o que lle interesa o switch, as direccións MAC

NOTA: *As enderezos MAC de cada ordenador son os enderezos físicos da tarxeta de rede que veñen postas de fábrica e son inmodificables.*

Switch M	
Mac	**Porto**
I	1
J	2
U	3
S	5
T	4

O algoritmo funciona do seguinte xeito: (Para entendelo ben, débese coñecer o formato das tramas IEEE 802.x)

Cando I transmite unha trama a alguén, está trama levará a dirección MAC-I no campo MAC orixe da trama, entón cando a trama chegue ó switch, este analizará a dirección orixe da trama, e verá que MAC-I está alcanzable polo porto 1 do switch. O switch creará unha entrada na táboa de MACs indicando que ó ordenador con MAC I está alcanzable polo porto 1.

Mentres un ordenador non transmita, o switch non saberá por onde se alcanza ese ordenador.

Notar que ó lugar máis lonxe o que poden viaxar as tramas que saian de I será ó router S, e ó host J. No caso de ser o router U quen emita as tramas, os lugares ós que poden ir serían ós routers S, T e os hosts I, J.

Imaxinar que I desexa enviar información a D. Primeiro enviará unha trama ó router S, pasando previamente polo switch, coa súa dirección mac destino e a súa dirección mac orixe (S,I). O router S enviará unha **nova trama** a D, coa súa dirección MAC destino e a súa dirección mac orixe (D,S)

Para entender esto último debese ter claro como funciona o protocolo TCP/IP sobre IEEE 802.x (explícase pregunta 1.d.-)

OLLO, se ó porto 1, por exemplo, estivera conectado un hub, un switch, unha ponte (ou sexa algo de nivel 2 ou menos). Se ó elemento conectado ó porto 1 houbese HOSTS conectados. Na táboa do switch M habería unha entrada para cada HOST. Cada entrada indicaría que ese host alcánzase polo porto1.

1.b.- A rede leva unha hora funcionado e cada ordenador xa se conectou con tódolos restantes e ademais xa estiveron navegando por internet. Supoñendo que as entradas en cada táboa teñen unha duración ilimitada e as táboas un tamaño ilimitado, indica:

Táboas que se constrúen dun xeito dinámico. ¿Como se construíron?. ¿Cales son os seus valores actuais?

Nota*: Hai routers que teñen unha mac para cada interface, e outros unha soa mac para tódolos interfaces. Imos supoñer o último caso.*

ROUTERS: este elemento de interconexión traballa a nivel de rede co cal do que entende e de PAQUETES, e neste caso de datagramas IP, posto que estamos en TCP/IP. Unha táboa dinámica, ó marxe da estática, que teñen estes elementos chámase ***cache arp*** . Esta configúrase dinamicamente. Neste paso omitimos a táboa do router K, pois o que nos interesa é a intranet.

Router R			**Router S**			**Router T**			**Router U**	
IP	**MAC**		**IP**	**MAC**		**IP**	**MAC**		**IP**	**MAC**
130.1.0.10	MAC A		11.1.0.10	MAC C		11.0.0.1	MAC S		11.0.0.1	MAC S
130.1.0.11	MAC B		11.1.0.11	MAC D		11.2.0.10	MAC F		11.0.0.10	MAC I
130.1.0.13	MAC E		11.1.0.2	MAC R		11.2.0.11	MAC G		11.0.0.11	MAC J
11.1.0.10	MAC C		11.0.0.10	MAC I		11.2.0.12	MAC H		11.0.0.2	MAC T
11.1.0.11	MAC D		11.0.0.11	MAC J		11.0.0.10	MAC I		195.10.1.2	MAC K
11.1.0.1	MAC S		11.0.0.3	MAC U		11.0.0.11	MAC J			
			11.0.0.2	MAC T		11.0.0.3	MAC U			

Para ver como se constrúen esas táboas basearémonos no router R. (ARP [COME96] Tema 5)

U desexa enviar un datagrama IP a I. U debe construír a trama e logo enviala. Polo de agora, segundo o paquete que lle chegou, sabe que o destinatario ten a dirección IP 11.0.0.11, pero non sabe a súa MAC para poñela no campo de MAC-destino da trama que está construíndo. (lembrar paquetes no nivel 3-rede e tramas no nivel 2-enlace)

O problema soluciónase usando o protocolo ARP. Este serve para indagar que dirección MAC se corresponde cunha IP determinada. Neste caso U construirá unha trama de broadcast con MAC orixe a do Router. Esta trama será lida por tódolos elementos que están conectados ó switch. Esta trama pregunta cal e a dirección MAC do equipo que ten por enderezo-IP 11.0.0.11.

Cando I recibe esa trama ARP, ve que é el quen ten esa IP, co cal respóndelle ó Router U con outra trama: esta trama tería por direccións mac (destino, orixe) (U,I). U recibe a trama de I e analiza a dirección orixe desa trama. Deste xeito, U engade unha nova entrada a súa caché ARP, indicando IP coa súa MAC asociada.

Cando U teña que enviar algo a I antes de usar o protocolo ARP, consulta a táboa caché ARP, para ver si xa ten unha entrada para a IP de destino, si é así, xa colle a MAC asociada á IP de destino.

O comando **arp –a** mostra as entradas da cache arp de cada equipo. Outros comandos son **ipconfig /all** (configuración ip) e **tracert** (camiño que sigue un paquete)**.**

1.b.- A rede leva unha hora funcionado e cada ordenador xa se conectou con tódolos restantes e ademais xa estiveron navegando por internet. Supoñendo que as entradas en cada táboa teñen unha duración ilimitada e as táboas un tamaño ilimitado, indica:

Táboas que se constrúen dun xeito dinámico. ¿Como se construíron?. ¿Cales son os seus valores actuais?

Nota*: Hai routers que teñen unha mac para cada interface, e outros unha soa mac para tódolos interfaces. Imos supoñer o último caso.*

ORDENADORES: a única táboa dinámica que teñen e a de cahé arp, que se constrúe do mesmo xeito que no caso anterior.

HOST A	
IP	**MAC**
130.1.0.11	MAC B
130.1.0.13	MAC E
130.1.0.1	MAC R

HOST B	
IP	**MAC**
130.1.0.10	MAC A
130.1.0.13	MAC E
130.1.0.1	MAC R

HOST E	
IP	**MAC**
130.1.0.10	MAC A
130.1.0.11	MAC B
130.1.0.1	MAC R

HOST C	
IP	**MAC**
11.1.0.11	MAC D
11.1.0.2	MAC R
11.1.0.1	MAC S

HOST D	
IP	**MAC**
11.1.0.10	MAC C
11.1.0.2	MAC R
11.1.0.1	MAC S

HOST F	
IP	**MAC**
11.2.0.11	MAC G
11.2.0.12	MAC H
11.2.0.1	MAC T

HOST G	
IP	**MAC**
11.2.0.10	MAC F
11.2.0.12	MAC H
11.2.0.1	MAC T

HOST H	
IP	**MAC**
11.2.0.10	MAC F
11.2.0.11	MAC G
11.2.0.1	MAC T

HOST I	
IP	**MAC**
11.0.0.11	MAC J
11.0.0.1	MAC S
11.0.0.3	MAC U
11.0.0.2	MAC T

HOST J	
IP	**MAC**
11.0.0.10	MAC I
11.0.0.1	MAC S
11.0.0.3	MAC U
11.0.0.2	MAC T

NOTAR: que, por exemplo, o HOST A nunca enviará unha trama ó HOST C. Como moi lonxe enviará unha trama ó router R. O que si pode enviar a C é un paquete, pero ese paquete tense que meter no campo de datos da trama que A envía a R. R recibirá a trama, pasará o campo de datos da trama ó nivel IP. R consultará a táboa de ruteo, meterá o paquete nunha nova trama, que irá de R a C.

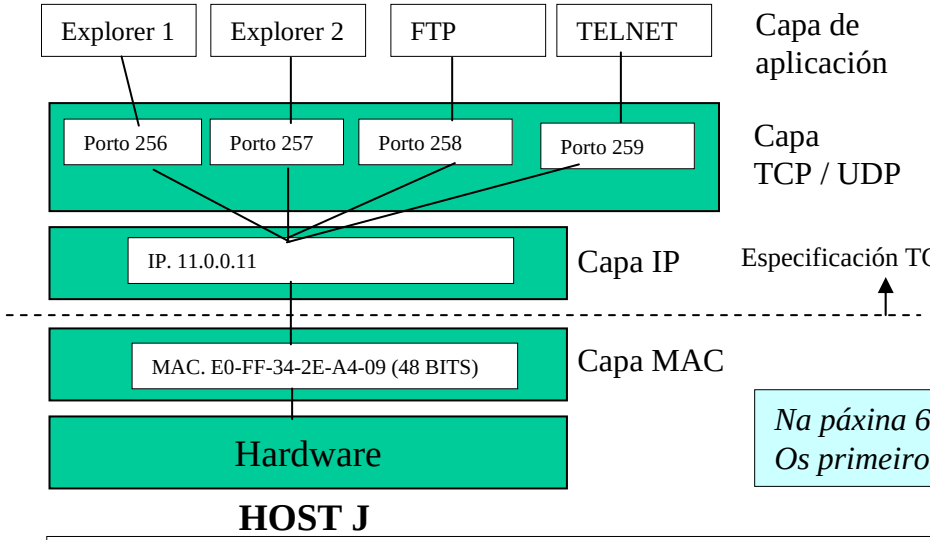
Este proceso verase con maior detalle na pregunta 1.d.

1.c.- Indicar como se constrúen os campos Porto Destino e Porto Orixe do primeiro segmento TCP e os campos Dirección IP Orixe e Dirección IP Destino do primeiro datagrama IP, cando o ordenador con MAC J executa a seguinte sentencia:

```
>ftp ftp.exame.es
```

PORTOS: son os puntos polos que se accede á capa de transporte da pila de protocolos TCP/IP. Os protocolos de transporte de TCP/IP son 2: TCP (orientado a conexión e fiable) e UDP (non orientado a conexión nin fiable)

As aplicacións que se executan na capa de aplicación, están conectadas a un porto na capa de transporte



Este gráfico simplifica a arquitectura de TCP/IP nun host.

Nun host podemos ter varias aplicacións executándose, imos supoñer clientes. Ese host ten unha soa dirección IP.

¿cómo poder enviar a información, que chega ó host J, á aplicación adecuada, se toda a información que chega leva a mesma dirección IP-Destino (11.0.0.11)?

Pois usando os portos. No nivel TCP (UDP) chegan segmentos indicando cal é porto de destino. E a ese porto estará conectada unha aplicación.

Na páxina 668 [KR REDES] está a descrición de tódolos portos
Os primeiros que aparecen libres son a partir do 256

Resolución da pregunta.

PORTOS:

Porto orixe: Cando se inicia a aplicación cliente ftp, o SO asínalle á aplicación un dos portos que teña libres nese momento, por exemplo o 258

Porto destino: Este porto é o porto no que vai estar o servidor de ftp escoitando peticións. Este porto pertence ós portos denominados **ben coñecidos**, polo cal todo servidor de ftp, estará escoitando no porto 21. (os datos recibiranse polo porto 20, pero para comprender o proceso imos usar só o porto 21) [COME96] 426-428

DIRECCIÓNS IP

IP orixe: a do propio HOST J : 11.0.0.11

IP destino: Se se houbera posto >ftp 130.1.0.10. Esta sería a dirección Ip de destino. Pero como se puxo un nome de dominio será preciso facer uso do Servidor de DNS para resolver a dirección. Ou sexa, que o host J preguntará ó ordenador con IP 11.2.0.12 (esta dirección foi introducida no cliente de DNS do ordenador J) se sabe cal é a dirección IP correspondente a ftp.exame.es. O servidor de DNS mirará o seu ficheiro de DNS e resolverá a dirección. Devólvelle a J a dirección IP que corresponde a ftp.exame.es.

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

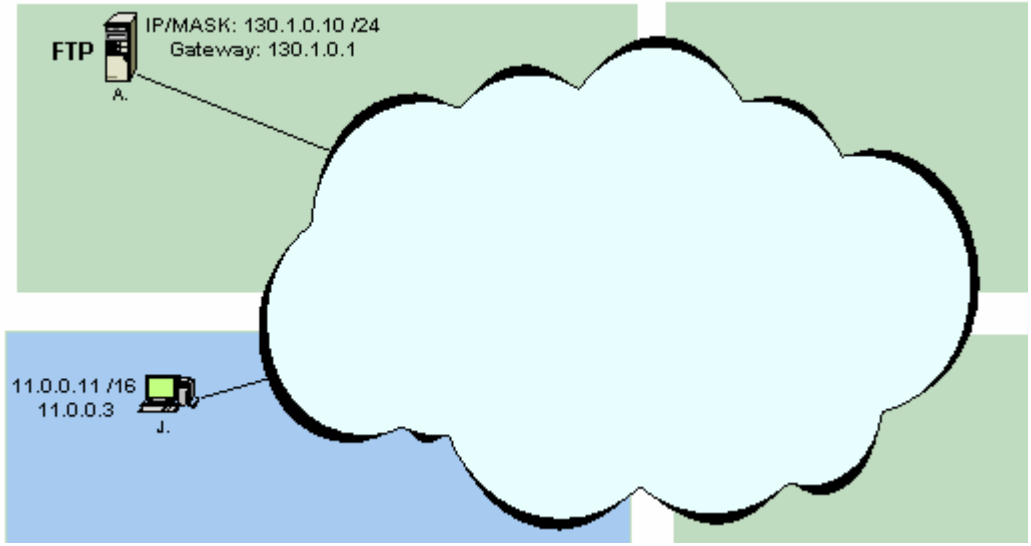
- Explicar como se constrúen os segmentos TCP, como se transmiten ó outro extremo e como funciona este protocolo, tendo en conta só as entidades pares de TCP.

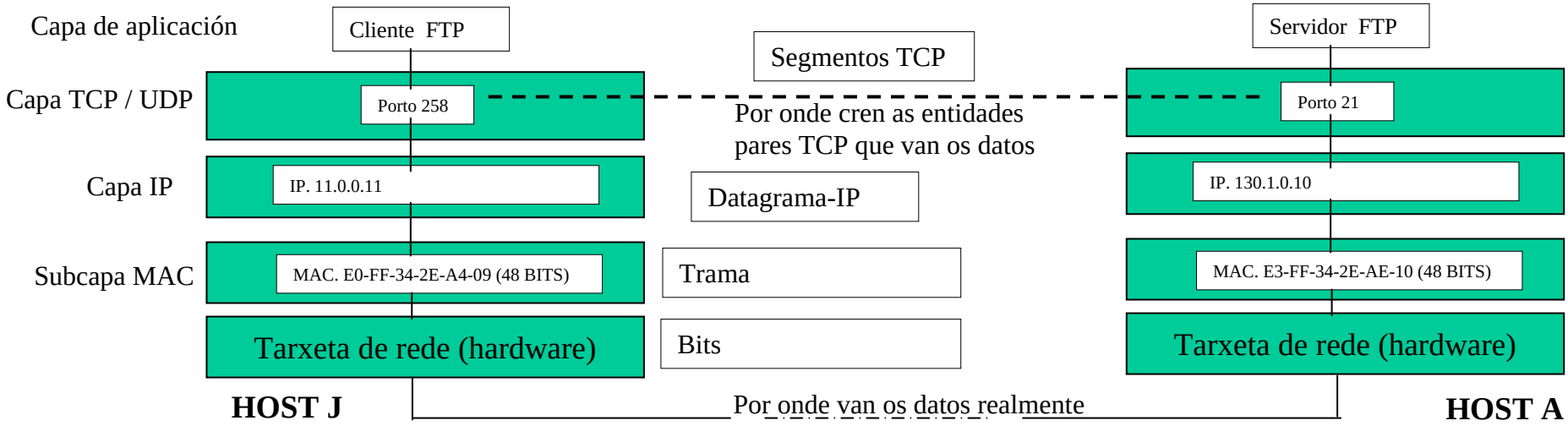
O primeiro que hai que ter claro cando se fala de TCP, é que se está na capa de transporte, onde a transmisión de información só ten senso extremo a extremo, e non equipo a equipo adxacente.

Enténdase por equipo: host, routers, switchs, etc.. Para TCP todo ese hardware é transparente, non sabe nin que existe. As seguintes figuras mostran o significado extremo a extremo.

Notar tamén, que entre entidades pares TCP intercámbianse **segmentos**. Eses segmentos serán os datos do **datagrama-IP**. Ese datagrama IP serán os datos da **trama**. E esa trama serán **bits**.

Ver Unidade de traballo 4





1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

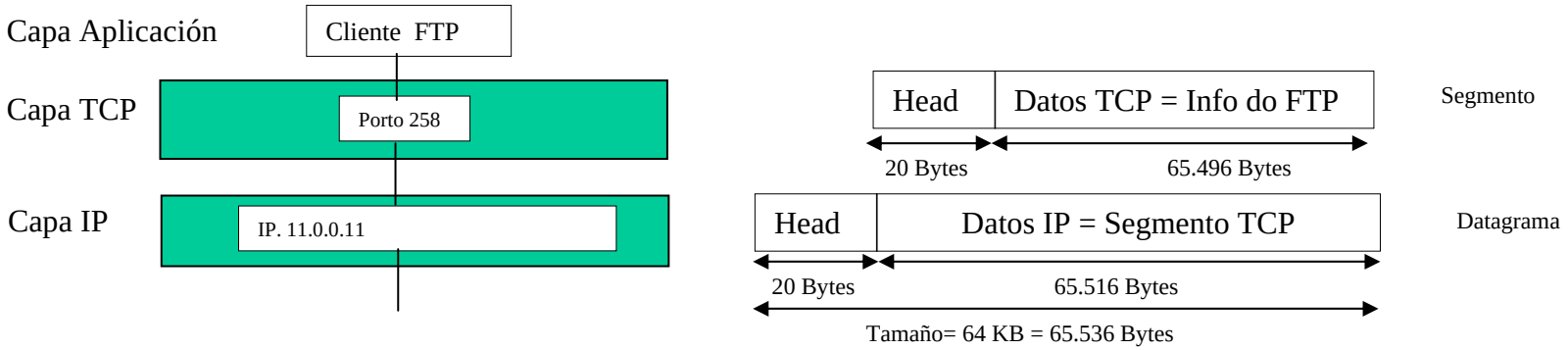
- Explicar como se constrúen os segmentos TCP, como se transmiten ó outro extremo e como funciona este protocolo, tendo en conta só as entidades pares de TCP.

Visto ó anterior esquema, pasamos a resolver o exercicio.

Para calcular o tamaño dos segmentos TCP imos supoñer un caso xeral, no que nos interesa que o segmento sexa o máis grande posible. Sobre o tamaño dos segmentos existe en [COME96], páx. 207, unha *agradable* discusión. Cada fabricante (Microsoft, Linux, Unix, …) implanta este protocolo de distintas formas. Por exemplo en Windows NT existe unha explicación sobre os tamaños dos segmentos en [KR-REDES] Páxs. 330-332.

Imos supoñer que o Host J non coñece a MTU da rede (MTU = maximum transfer unit, Esto é, o tamaño máximo que pode ter un datagrama-IP para atravesar una rede, está en función do tamaño das tramas, [COME96] páx. 97). Esto implica que o tamaño máximo do datagrama-IP vai ser de 64KB.
(Neste caso ó importante é ter os conceptos claros, e non si o tamaño e tal ou cal, prantexarase un suposto e resolverase a partires del).

Imos supoñer, tamén, que as cabeceiras dos segmentos (*[COME96], páx. 205*) e dos datagramas (*[COME96], páx. 95*) non teñen opcións, co cal cada cabeceira terá un tamaño de 20 bytes.



Baseándose no gráfico anterior vese que o campo de datos do datagrama-IP é de 65.516 Bytes (= 65.536 bytes de todo o datagrama - 20 da cabeceira sen opcións)

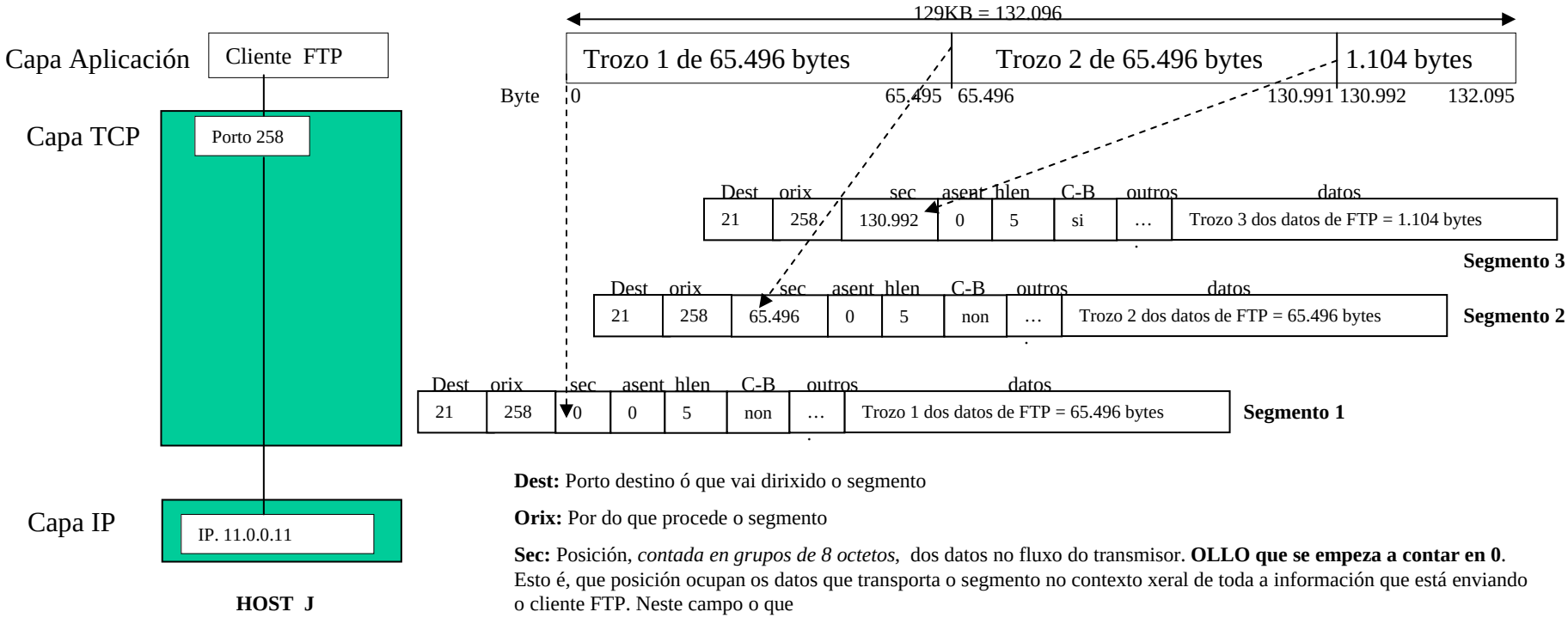
Deste xeito o segmento TCP pode ter un tamaño máximo de 65.516 bytes, pero tamén ten 20 bytes de cabeceira, co cal quedan 65.496 bytes para gardar os datos que nos envía o nivel FTP.

Se o nivel FTP envía a capa TCP 129 KB (132.096 bytes, entre información e datos de control) temos como resultado 3 segmentos TCP. Os dous primeiros teñen un campo de datos de tamaño de 65.496 bytes e o último ten un campo de datos de tamaño 1104 bytes. (65.496+65.496+1.104 = 132.096)

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar como se constrúen os segmentos TCP, como se transmiten ó outro extremo e como funciona este protocolo, tendo en conta só as entidades pares de TCP.



Dest: Porto destino ó que vai dirixido o segmento

Orix: Por do que procede o segmento

Sec: Posición, *contada en grupos de 8 octetos*, dos datos no fluxo do transmisor. **OLLO que se empeza a contar en 0**. Esto é, que posición ocupan os datos que transporta o segmento no contexto xeral de toda a información que está enviando o cliente FTP. Neste campo o que

Asent: Byte que esta esperando J recibir de A. Eso quere dicir que J lle asinte todo o enviado por A hasta ese byte (non incluído). Neste caso puxen 0, esto quere dicir que A aínda non lle enviou nada a J. Por eso J espera polo byte 0

Hlen: lonxitude da cabeceira, medida en palabras de 32 bits. Como neste caso non hai campo de opcións, HLEN =5

C-B:CODE-BITS Codificación do campo que indica si ese segmento é o último do fluxo de datos

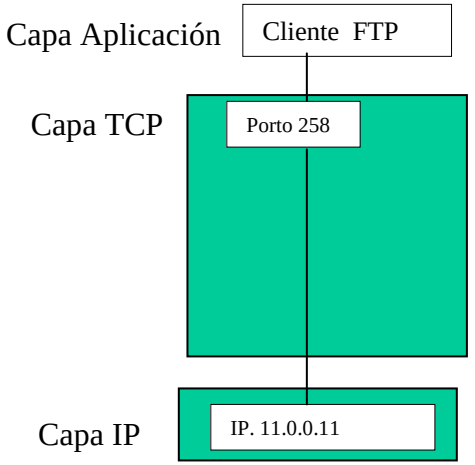
Outros: Os demais campos da cabeceira TCP (tamaño venta, Checksum, ….)

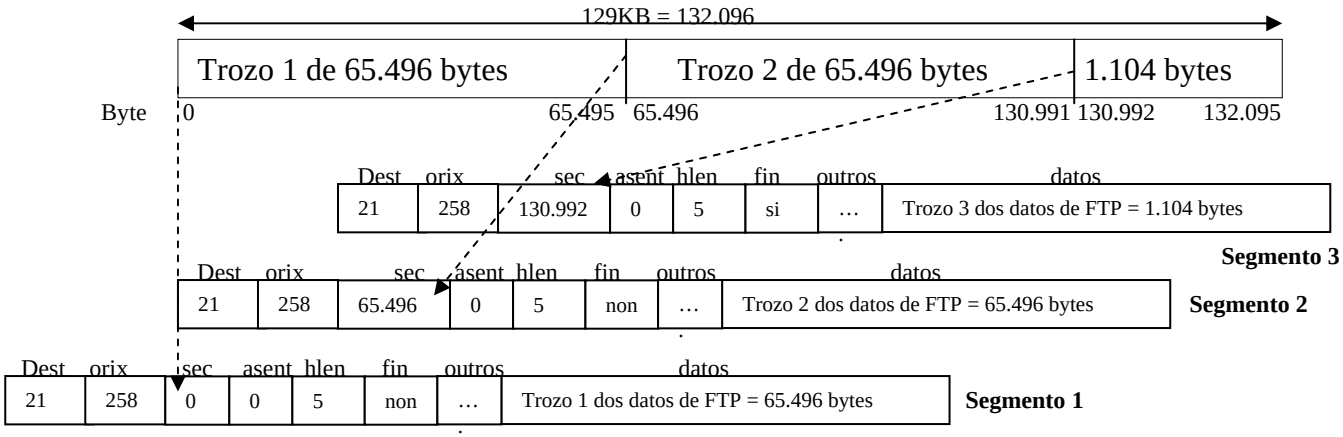
Datos: a información que está enviando o cliente FTP

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar como se constrúen os segmentos TCP, como se transmiten ó outro extremo e como funciona este protocolo, tendo en conta só as entidades pares de TCP.





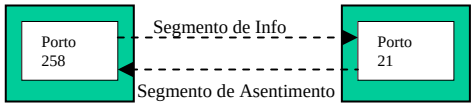
HOST J:

O anterior acontece no TCP do host J. Vanse creando os segmentos e vanse pasando ó nivel IP para ser transmitidos.

HOST A:

Cando á entidade par TCP do host A recibe o primeiro segmento fai control de erros do segmento. Se non hai erros pasa os datos á aplicación que está escoitando no porto 21(realmente sería ó porto 20, pero imos seguir co 21). Quen está escoitando nese porto é o servidor de FTP. El será quen reciba os datos.

ASENTIMENTOS:

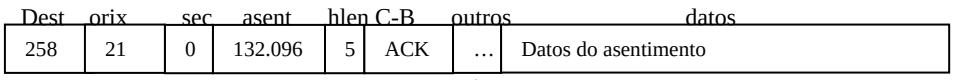


Como TCP é confiable proporciona control de erros é solución a estes mediante retransmisións. Deste xeito o receptor asíntelle a información recibida ó transmisor, ou pola contra dille que información está incorrecta.

Para realizar este proceso úsase o protocolo de ventá deslizante[COME96] páx197-199. (O funcionamento é similar o que se usa nas tramas HDLC).

O tamaño da ventá deslizante negóciase na fase de establecemento de conexión. Para simplificar imos supoñer un tamaño de ventá de 200 KB. Deste xeito A non emitira un segmento de asentimento cara J ata que reciba 200 KB de J, ou ben J finalice a súa transmisión.

Cando A reciba o terceiro segmento con CODE-BITS indicando fin de fluxo de información enviará un segmento de asentimento indicándolle a J que está esperando polo byte 132.096. Con esto A quere dicir " *J todo o que enviaches ata 132.095 está correctamente recibido*". O cliente FTP de J recibirá o asentimento, así darase conta de que todo se entregou correctamente. Como non ten nada máis que enviar, pois a outra cousa. NOTAR: O tamaño das ventás en WINDOWS NT é bastante máis pequeno.



Segmento Asentimento de A á J

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.

Antes de nada sería bo facer un esquema do camiño que vai percorrer a información dende o nivel IP de J ata o nivel IP de A´.

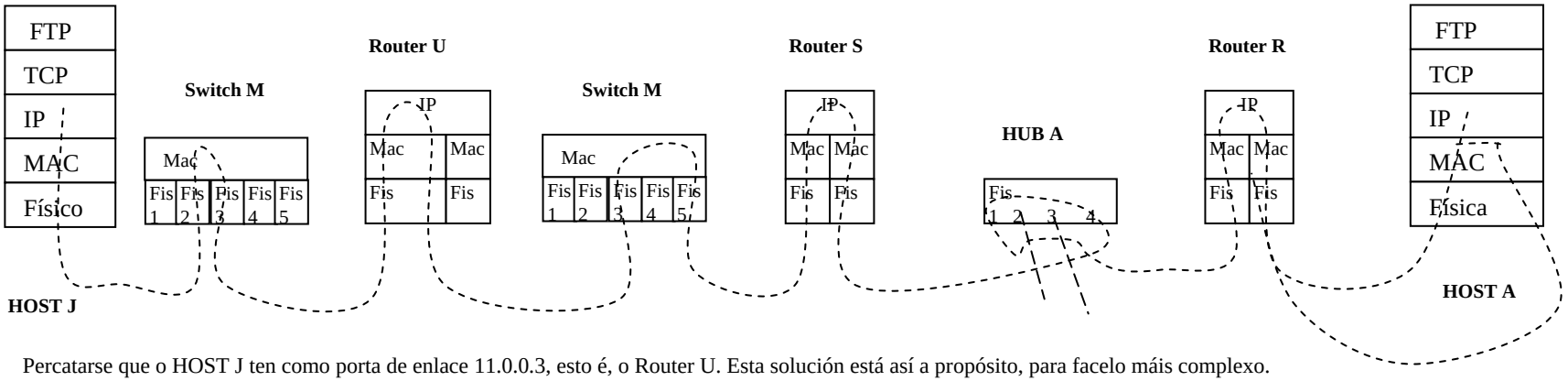
NOTA MOI IMPORTANTE

Nesta versión 2.3 da resolución do exame omitiuse o uso do protocolo ICMP (*[COME96], tema 9*). Omitiuse en concreto o uso de mensaxes **ICMP redirect**, (*[COME96], páx. 133*)

Estas mensaxes envíanas os Routers ós ordenadores para indicarlle unha ruta máis óptima pola que encamiñar que a que están usando ata o de agora.

Por exemplo, se o Host J está enviando paquetes ás redes 11.1.0.0 ou 130.1.0.0, este host enviaría os paquetes ó Router U, e este, ó Router S. Pero o Router S a parte de estudiar a dirección IP-Destino, tamén estudia a dirección IP-Orixe do paquete, 11.0.0.11. O Router S ve que o Host J está na mesma rede IP que el mesmo, polo de agora todo normal, PERO dáse conta de que eses paquetes non lle chegan directamente do Host J, senón que lle chegan a través do Router U, pois as tramas que conteñen ese paquete veñen coa MAC-orixe do Router U. Entón, o que fai o Router S é enviarlle unha mensaxe **ICMP redirect** ó Host J indicándolle que cambie a súa porta de enlace a 11.0.0.1, ou sexa o Router S.

O protocolo ICMP é unha parte obrigatoria do protocolo IP e está dentro da pila de protocolos TCP/IP dende o nacemento desta pila de protocolos



Percatarse que o HOST J ten como porta de enlace 11.0.0.3, esto é, o Router U. Esta solución está así a propósito, para facelo máis complexo.

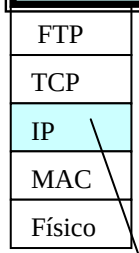
O switch M xa ten as táboas MAC configuradas do exercicio 1.b co cal xa sabe como encamiñar as tramas que lle chegan

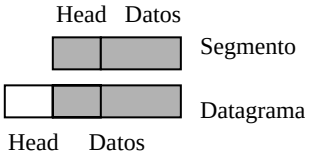
O hub A é como un cable, deste xeito todo o que lle entra polo porto 4 sae por tódolos demais.

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.





CONSTRUCCIÓN DO DATAGRAMA-IP

NOTA:

TCP: **segmentos**

IP: **datagramas** ou **paquetes**

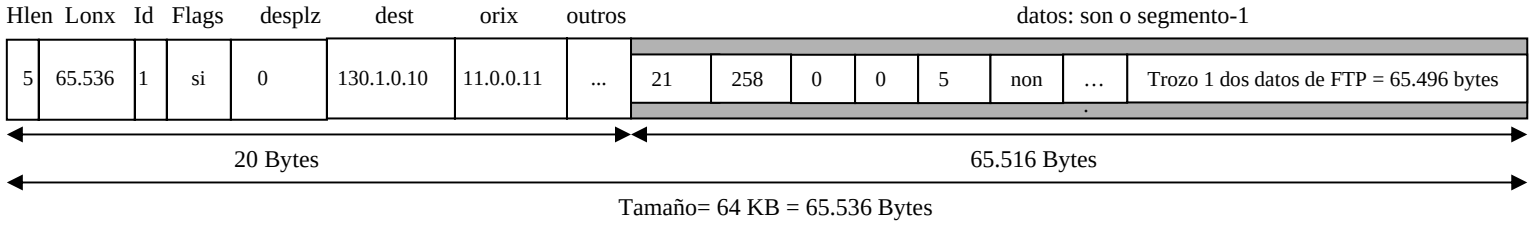
si se divide un datagrama: **fragmentos**

MAC: **tramas**

HOST J

Imos traballar só co 1º segmento TCP, cos outros faríase o mesmo.
Todo o segmento 1 serán os datos do 1º datagrama-IP. O segmento 2 serán os datos do datagrama 2 e o segmento 3 os datos do datagrama3. Revisade a páx. 18 anterior.

Datagrama IP con identificación 1. Contén os datos do segmento TCP-1



Hlen: Lonxitude da cabeceira do datagrama-IP. Ter en conta que non hai opcións, co cal a cabeceira van ser 5 palabras de 32 bits (20 bytes)

Lonx: Lonxitude total de todo o datagrama-IP

Id: Identificación do datagrama. O segmento-2 iría nun datagrama con identificación 2, … Este campo te mais senso cando se fragmenta o datagrama-IP

Flags: Entre outras cousas indica si é o ultimo datagrama con identificación 1. Neste caso é o primeiro, último e ademais único. Este campo ten máis senso nos fragmentos.

Desplz: Este campo ten senso cando se fragmenta o datagrama IP. Tódolos fragmentos excepto o último deben ter un múltiplo de 8 bytes salvo o último.

NOTA: para non liar o exercicio, no campo desplaz vou poñer nº de bytes totais e non cantos grupos de 8 bytes van no datagrama.

Dest: Dirección IP destino

Orix: Dirección IP orixe

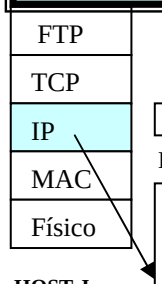
Outros: os demais campos da cabeceira

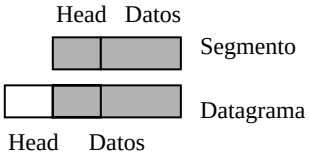
Datos: este campo contén os segmentos-TCP enteiros.

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

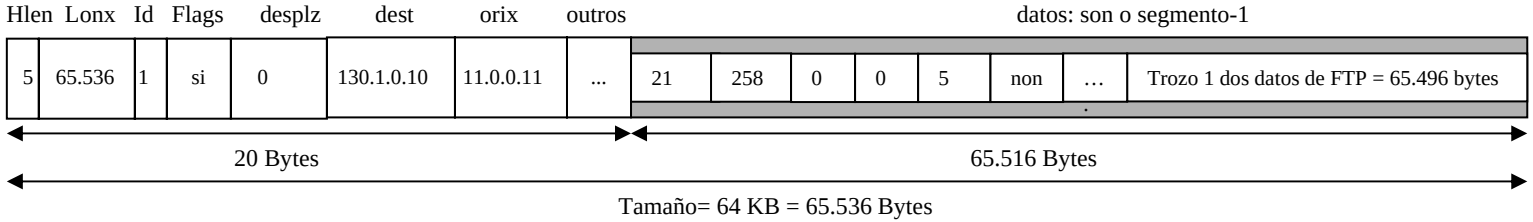
- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.





CONSTRUCCIÓN DOS FRAGMENTOS-IP

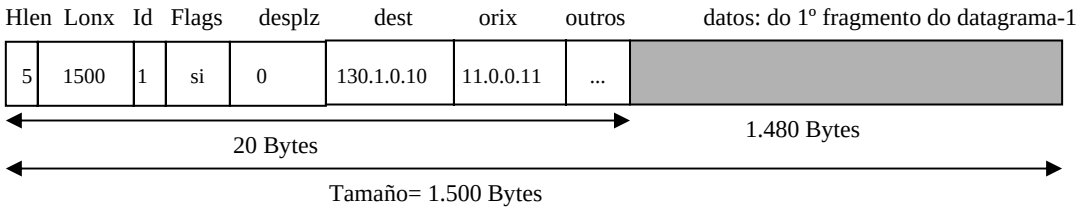
HOST J



O problema agora radica en que a MTU de ethernet é 1500 bytes, co cal, o tamaño de todo o datagrama IP debe ser de 1500 bytes. Esto é, as tramas ethernet teñen un campo de datos que so admite 1.500 bytes. Se se estivera usando token Ring non teríamos que fragmentar ese datagrama. Pero en ethernet hai que fragmentar ese datagrama en trozos de cómo máximo 1500 bytes.

Imos facer un inciso para mostrar dun xeito xeral o formato da trama ethernet

Visto ó anterior teremos que crear fragmentos-IP a partir do datagrama-IP anterior.
Cada fragmento-IP será como un novo datagrama-IP con 20 bytes de cabeceira e 1.480 bytes para datos. Sumados (20+1.480) dan os 1.500 bytes que acepta o campo de datos da trama ethernet.

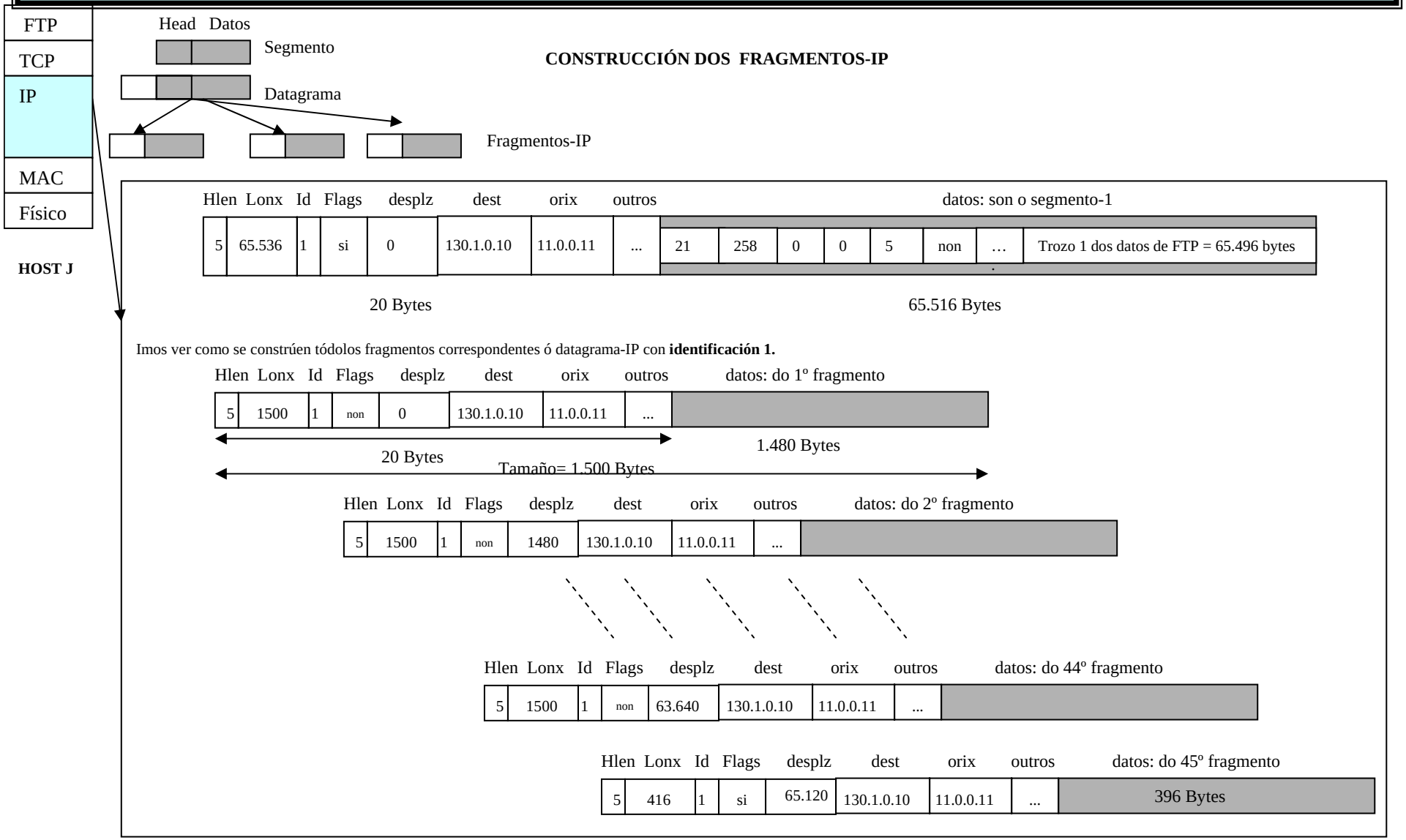


Na seguinte páxina explícanse os fragmentos

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

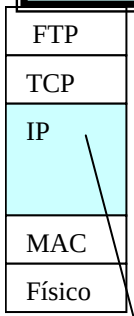
- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



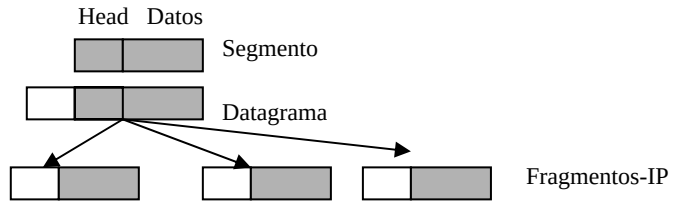
1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



HOST J



Hlen	Lonx	Id	Flags	desplz	dest	orix	outros	datos: son o segmento-1
5	65.536	1	si	0	130.1.0.10	11.0.0.11	...	21 258 0 0 5 non … Trozo 1 dos datos de FTP = 65.496 bytes

20 Bytes — 65.516 Bytes

Imos ver como se constrúen tódolos fragmentos correspondentes ó datagrama-IP con **identificación 1.**

Hlen	Lonx	Id	Flags	desplz	dest	orix	outros	datos: do 1º fragmento
5	1500	1	non	0	130.1.0.10	11.0.0.11	...	

20 Bytes — 1.480 Bytes

Tamaño= 1.500 Bytes

¿Número de fragmentos?

O datagrama-IP 1, ten 65.516 bytes de datos. Todos eles deben ser transmitidos en datagramas máis pequenos, con un campo de datos de tamaño 1480, bytes. Notar que son 1480 bytes porque o datagrama ten que ter como máximo 1.500, e hai que descontar os 20 da cabeceira.
65.516 bytes / 1480 = 44 fragmentos de 1.480 bytes (nestes 44 fragmentos van 44*1480= 65.120 bytes)
O fragmento 45 levará (65.516 -65.120)= 396 bytes no campo de datos. Co cal a lonxitude total do fragmento 45 será de (396 de datos + 20 de cabeceira)= 416 bytes

Explicación campos

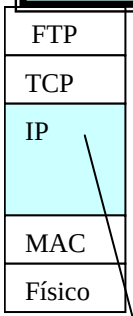
Ident: Agora si que ten senso este campo. O receptor A reensamblará nun so datagrama-IP todos aqueles fragmentos que cheguen con identificación 1.
Lonx: lonxitude total de todo o datagrama-IP (cabeceira + datos), non pode ser maior de 1.500
Desplz: Este campo indica que lugar, medido en bytes, ocupan os datos que leva o fragmento no contexto xeral de todo o datgrama-IP orixinal que se está a fragmentar.

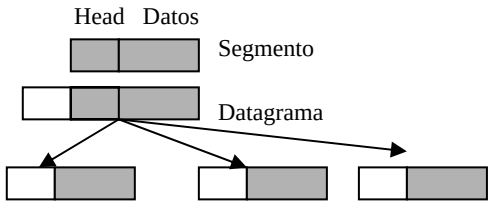
Fixarse nas diferencias entre o fragmento 1 e o 45
Sucedería algo semellante co datagramas-IP 2 (este datagrama levará o segmento-TCP 2)
O datagrama-IP 3, que levaría o segmento-TCP 3, non faría falla fragmentalo. Pois serían 1.144 bytes en total (40 de cabeceiras ip e TCP e 1104 de datos TCP)

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.





AVERIGUAR A DIRECCIÓN MAC DE DESTINO

HOST J

A partires de agora imos traballar co primeiro fragmento do primeiro datagrama-IP

Hlen	Lonx	Id	Flags	desplz	dest	orix	outros	datos: do 1º fragmento
5	1500	1	non	0	130.1.0.10	11.0.0.11	...	

Cando xa se ten o primeiro fragmento hai que envialo. Para iso precísase construír a trama ethernet. Pero para construír esa trama hai que averiguar a MAC de destino.

¿**Cálculo MAC destino?**

Primeiro temos que ver si destino e orixe están na mesma rede IP. Para iso collemos a MASK de J e facemos AND coas direccións IP. Deste xeito vemos si a parte de rede da dirección IP coincide.
130.1.0.1 * 255.255.0.0 = 130.1.0.0
11.0.0.11 * 255.255.0.0 = 11.0.0.0

Vemos que o destino está na rede 130.1.0.0 e a orixe na rede 11.0.0.0
J ten configurada unha porta de enlace á que enviar aqueles paquetes que non vaian dirixidos a súa rede. A porta é 11.0.0.3. Desta dirección IP é da que se ten que averiguar a MAC de destino.
OLLO que ninguén pense que a MAC de destino é a de A.

NOTAR:
Enderezos IP.: NON se modifican de orixe a destino, atravesen o que atravesen. (Existe un protocolo que se implanta nos Routers, NAT, que si pode cambialas)
Direccións MAC: van cambiado a medida que se pasa polo Routers.

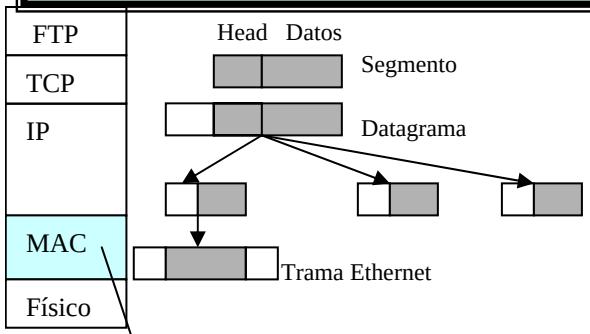
Para averiguar a MAC asociada a 11.0.0.3 mirase na caché ARP, se alí se atopa unha entrada para esa IP, pois xa se colle a MAC asociada, senón usaríase o protocolo ARP.
Partindo do exercicio 1.b esa entrada xa existe na táboa caché ARP.

A MAC de orixe, é a do propio Host J.

1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



CONSTRUCCIÓN TRAMA MAC ETHERNET

Fragmentos-IP

HOST J

A trama Ethernet sería como segue, faltan campos da cabeceira. Notar que este é o único nivel onde se lle engade unha cola, para control de erros, o CRC

Mac dest	Mac orix	Lonx	datos da trama = 1º fragmento-IP de tamaño 1.500 bytes								
Mac U	Mac J	1.500	5	1500	1	non	0	130.1.0.10	11.0.0.11	...	CRC

Trama Ethernet número 45º do primeiro datagrama-IP

Mac dest	Mac orix	Lonx	datos da trama = 45º fragmento-IP de tamaño 416 bytes								
Mac U	Mac J	416	5	416	1	si	65120	130.1.0.10	11.0.0.11	...	CRC

Faltarían as 45 tramas correspondentes ó segundo datagrama-IP
Faltaría a única trama correspondente ó terceiro datagrama-IP

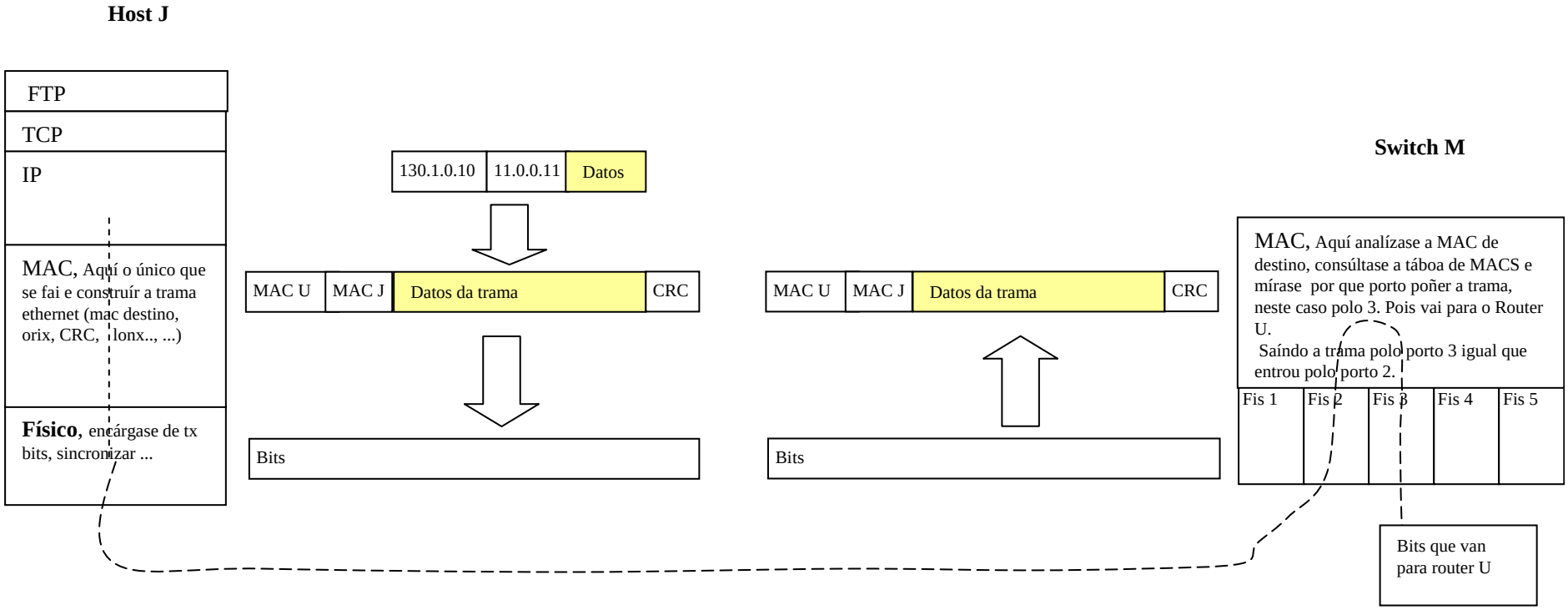
1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.

A PARTIR DE AGORA POÑERASE DUN XEITO RESUMIDO TODO O PROCESO

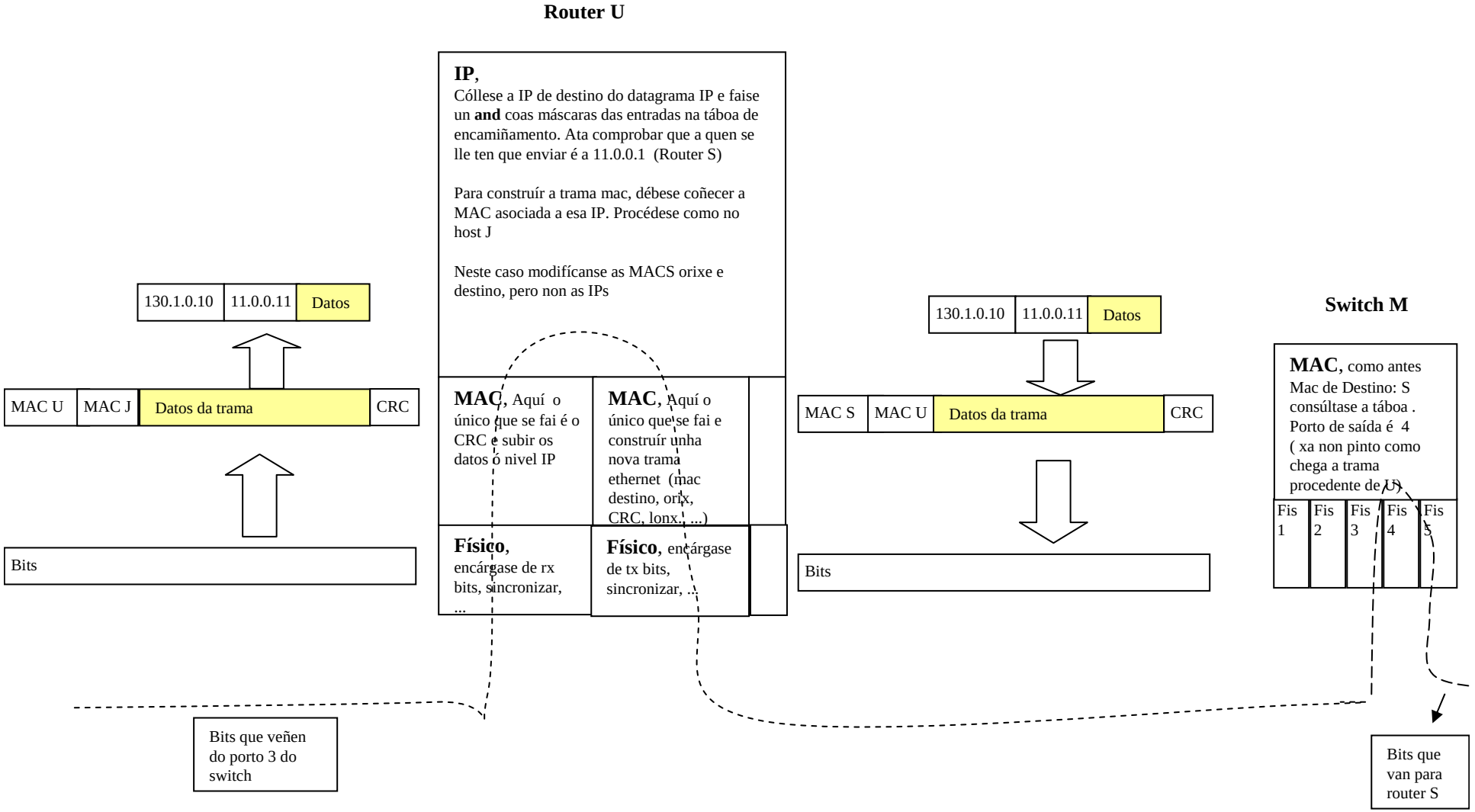
DENDE O HOST J ATA QUE CHEGA A INFORMACIÓN Ó HOST A



1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

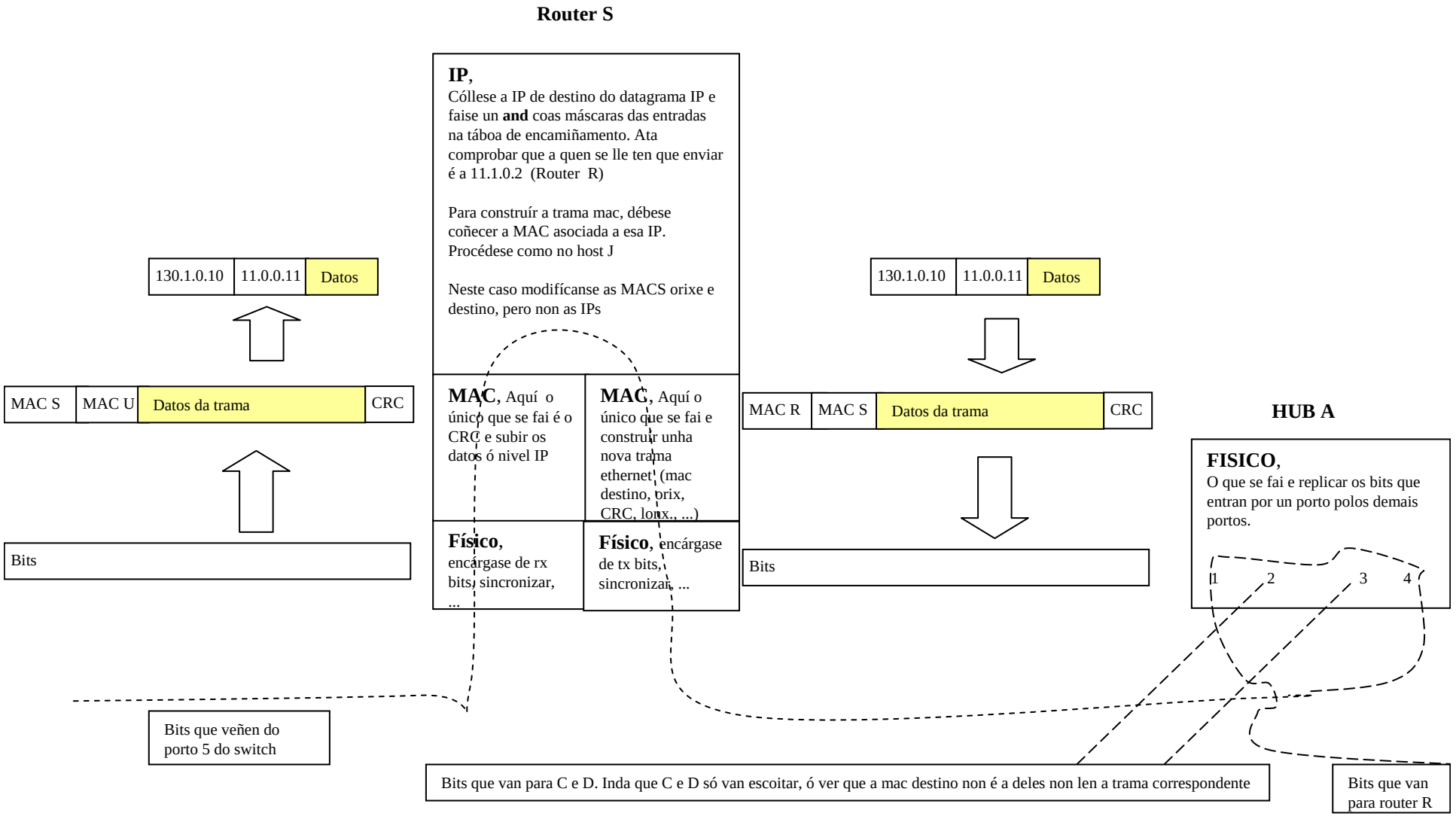
- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

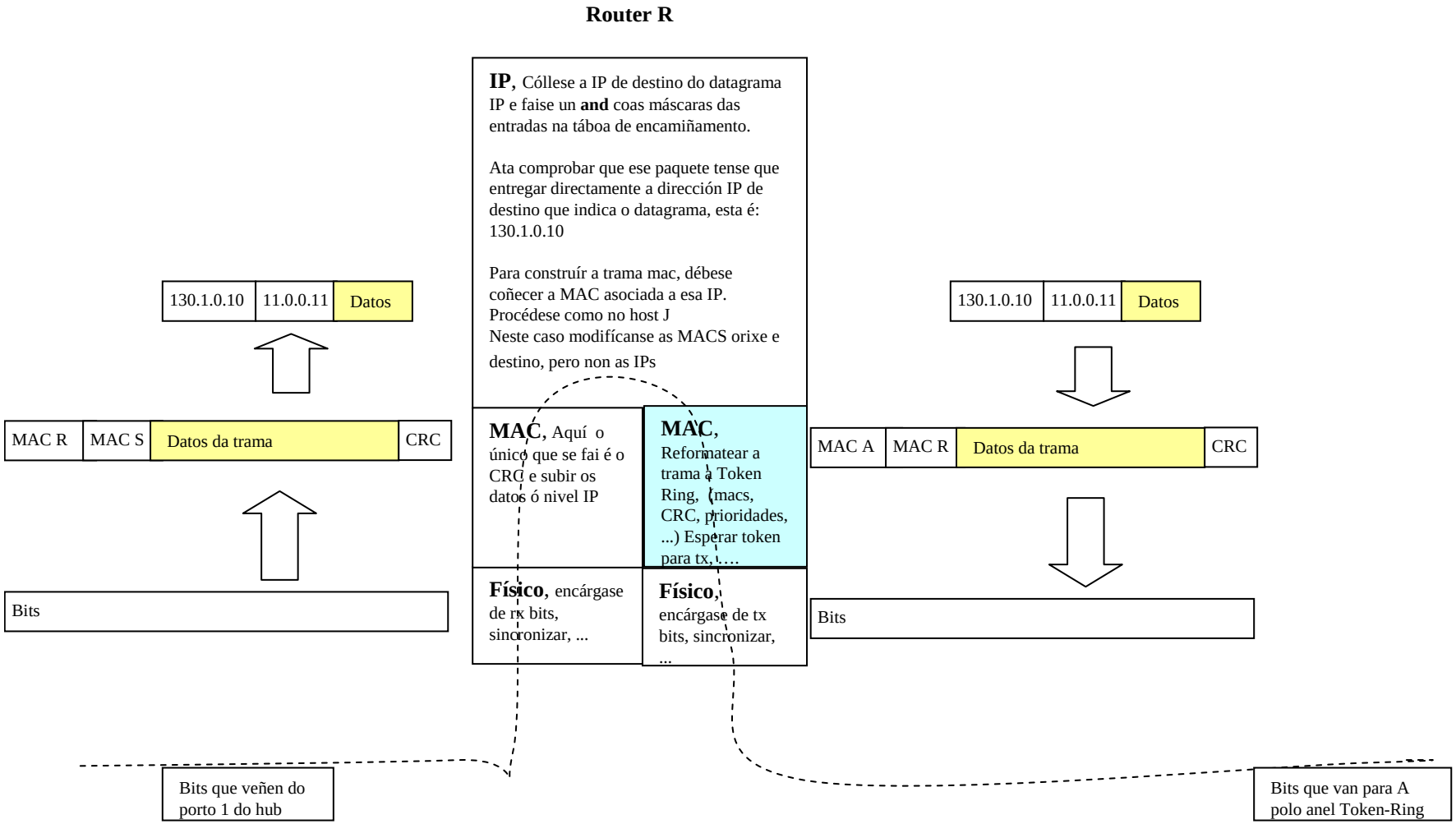
- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

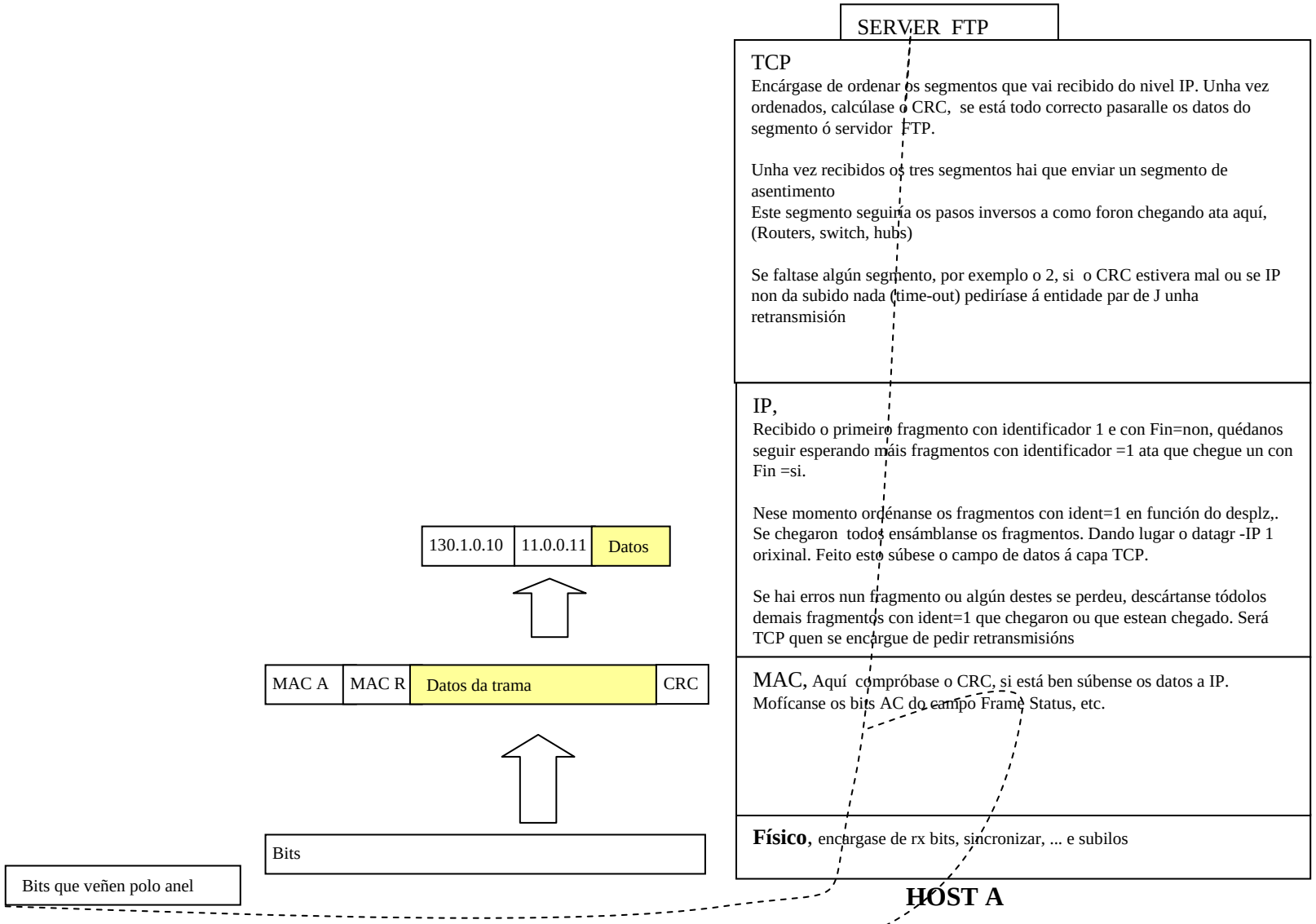
- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



1.d.- Baseándose no exercicio 1.b e 1.c explicar detalladamente, todo o proceso de transferencia do ficheiro proba.txt (tamaño 129 KB, incluídos datos de control e información propiamente dita), de J a A, cando J executa o seguinte comando ftp. Partir da capa TCP.

```
ftp> put proba.txt
```

- Explicar que elementos vai atravesar a información que vai de J a A e que decisións se toman neses elementos. Explicar, tamén, como se constrúen os datagramas IP e como chegan ata A, así como o funcionamento deste protocolo. Para finalizar indicar como se constrúen as tramas e como se van modificando ó longo do percorrido.



1.e.- Explica en que se diferenciaría o proceso anterior, se o que se fixese fose baixar o ficheiro proba2.txt de igual tamaño:

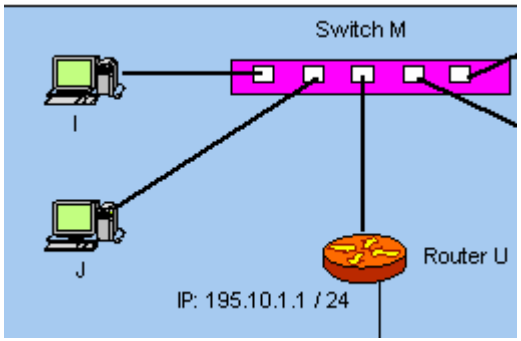
```
ftp>        get proba2.txt
```

HOST A está nunha token ring, neste caso as tramas teñen un campo de datos de tamaño ilimitado. Polo tanto no nivel IP non habería que facer fragmentación dos datagramas-IP.

Co cal de A sairían 3 tramas, cada unha contendo un datagrama-IP enteiro.

O problema está no Router R, por un lado está en token-ring, pero polo outro en ethernet, co cal sería o router que fragmentara eses datagramas-IP para adaptalos á MTU de ethernet

2.- Indica tódalas posibilidades de cableado, conectores e tarxetas de rede dos Host I e J en función dos distintos tipos de switch M que se poden instalar



Velocidades dos cables	
UTP categoría 3:	16 Mbps
UTP categoría 4:	20 Mbps
UTP categoría 5:	100 Mbps
UTP categoría 5e:	1.000 Mbps (Gigabit Ethernet)
FTP, STP:	100 Mbps

Antes de resolver o exercicio.

Se un extremo é 10 BASE T o outro pode ser 10 BASET ou 10/100 BASE T, deste xeito a conexión entre eles vai funcionar a 10 Mbps.

O extremo con 10/100 BASET detectará o estándar do outro extremo. Intentará negociar a máxima velocidade.

Se un extremo é 100 BASE T o outro pode ser 100 BASET ou 10/100 BASE T, deste xeito a conexión entre eles vai funcionar a 100 Mbps.

O extremo con 10/100 BASET detectará o estándar do outro extremo. Intentará negociar a máxima velocidade.

Se un extremo é 10/100 BASE T o outro pode ser 10BASET, 100 BASET ou 10/100 BASE T, deste xeito a conexión vai funcionar a 10/100.

O extremo con 10/100 BASET detectará o estándar do outro extremo. Intentará negociar a máxima velocidade.

O switch M, basicamente, podería ser dun dos 3 tipos seguintes:

10 BASET

2 tarxetas de rede: ben, 10 Base T ou ben 10/100 BaseT

2 cables de pares: ben UTP cat,3,4,5, ben FTP ou ben STP

100 BASET

2 tarxetas de rede: ben, 100 Base T ou ben 10/100 BaseT

2 cables de pares: ben UTP cat 5, ben FTP ou ben STP

Se os equipos teñen 100 BASET e se usa UTP cat 3,4 o sistema non funcionará. UTP cat 3, 4 non soportan os 100 Mbps

10/100 BASET

2 tarxetas de rede: ben 10 Base T, ben 100 BaseT ou ben 10/100 Base T

2 cables de pares: ben UTP cat 3, 4, 5, ben FTP ou ben STP

Se os equipos teñen 10/100 BASE T e se usa UTP cat 3,4 o sistema funcionará a 10 Mbps,

CONECTORES: 4 conectores RJ45: Apantallados (para STP, FTP) ou sen apantallar (para UTP)