



5 Conexión de sistemas en rede

Sumario

5 Conexión de sistemas en rede.....	1
5.1 Convencións empregadas.....	5
5.2 Introdución aos sistemas en rede. Direccionamento IP.....	6
5.2.1 Redes. Características e clasificación.....	6
5.2.1.1 Clasificación de Redes. Tipos de redes.....	6
5.3 Arquitectura da rede. Modelos OSI e TCP/IP.....	9
5.3.1 Protocolo de comunicación.....	9
5.3.2 Modelos por capas ou niveis.....	9
5.3.3 Modelo OSI.....	11
5.3.4 Modelo TCP/IP.....	12
5.3.4.1 Nivel 1. Nivel de ligazón ou acceso.....	14
5.3.4.2 Nivel 2. Nivel de rede.....	15
5.3.4.3 Nivel 3. Nivel de transporte.....	16
5.3.4.4 Nivel 4. Nivel de aplicación.....	17
5.3.5 Versións de Ethernet. Estándar IEEE 802.3.....	18
5.4 Topoloxías de rede.....	19
5.4.1 Topoloxía en bus.....	19
5.4.2 Topoloxía en anel.....	20
5.4.3 Topoloxía en estrela.....	21
5.4.4 Redes sen fíos. Modo de conexión: infraestrutura e ad-hoc.....	24
5.4.4.1 Modo infraestrutura.....	24
5.4.4.2 Modo ad-hoc.....	25
5.5 Compoñentes físicos das redes informáticas.....	26
5.5.1 Medios de transmisión.....	26
5.5.2 Clasificación dos medios de transmisión.....	27
5.5.2.1 Cable coaxial.....	27
5.5.2.2 Cable de par trenzado.....	28
5.5.2.3 Fibra óptica.....	30
5.5.2.4 Cableado estruturado.....	31
5.6 Elementos de interconexión.....	31
5.6.1 Tarxetas de rede e direccionamento MAC.....	32
5.6.2 Comutadores ou switches.....	33
5.6.3 Enrutadores ou routers.....	35
5.7 Redes sen fíos.....	37
5.7.1 Tipos de redes 802.11. Características.....	37
5.7.2 O SSID dunha rede 802.11.....	38
5.7.3 Seguridade en 802.11.....	39
5.7.3.1 Tipos de cifrado.....	39
5.7.3.2 Ocultar SSID.....	39
5.7.3.3 3.3. Deshabilitar WPS.....	39
5.7.3.4 Filtrado de direccións MAC.....	39
5.8 Sistema binario. Conversión decimal - binario.....	40
5.8.1 Sistema binario. O bit e o byte.....	40
5.8.1.1 Sistema binario.....	40
5.8.1.2 Bit e byte.....	40
5.8.1.3 Conversión decimal a binario.....	41
5.8.1.4 Conversión binario a decimal.....	41
5.8.1.5 Múltiplos do byte.....	42

5.8.2 Diferenza entre Kilobyte e Kibibyte.....	43
5.9 direcccionamento lóxico. Clases de redes e división en subredes.....	43
5.9.1 Direccións IP Versión 4. IPv4.....	43
5.9.2 Direccións específicas. Regras e convenios.....	44
5.9.3 Porta de ligazón.....	45
5.9.4 División de redes en clases.....	45
5.9.5 Clase A.....	46
5.9.6 Clase B.....	46
5.9.7 Clase C.....	47
5.9.8 Clases D e E.....	48
5.9.9 Redes privadas.....	48
5.9.10 División de redes en subredes.....	49
5.10 Configuración de routers.....	50
5.10.1 Táboas de encamiñamento.....	50
5.10.2 Formas de cubrir as táboas de encamiñamento.....	52
5.10.3 Como se aplican as táboas de encamiñamento.....	54
5.10.4 O encamiñamento nos hosts.....	56
5.11 Efecto das subredes nos routers externos.....	56
5.11.1 Esquema de exemplo sen subredes.....	56
5.11.2 Esquema de exemplo con subredes.....	57
5.11.3 Seguridade na arquitectura de rede.....	58
5.11.3.1 Esquema de rede básico.....	59
5.11.3.2 Esquema de rede cunha zona neutra.....	60
5.12 Administración de redes Windows.....	62
5.12.1 Configuración de rede en Microsoft Windows.....	62
5.12.2 Exercicio configuración Rede. Instalación de 2 máquinas Windows en Rede en grupo de traballo.....	62
5.12.3 Compartir recursos na Rede.....	68
5.12.3.1 Solapa Compartir.....	69
5.12.4 Servizos de redes.....	73
5.12.4.1 Arquitectura cliente-servidor.....	74
5.12.4.2 Servizos de infraestrutura de rede.....	76
5.12.4.3 Servizo FTP (File Transfer Protocol, Protocolos de transferencia de ficheiros.....	80
5.12.4.4 Servizo Web. Protocolo HTTP (Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto).....	81
5.12.4.5 Servizo de correo electrónico.....	82
5.12.4.6 Acceso remoto.....	84
5.12.5 Comandos de rede.....	92
5.12.5.1 Comandos TCP/IP en Windows.....	92
5.13 Administración de redes GNU-Linux.....	97
5.13.1 Configuración de rede e router en Linux.....	97
5.13.2 Encamiñamento en Linux.....	102
5.13.3 Servizos e comandos TCP/IP en GNU-Linux.....	105
5.13.4 Servizo SAMBA.....	106
5.13.5 Conexión desde máquinas cliente.....	109
5.13.6 Servizo NFS.....	111
5.13.7 Cliente NFS.....	112
5.13.8 Servizo ssh.....	114
5.13.9 Servizo Web: Apache.....	116

5.13.10 Apache con PHP.....	119
5.13.10.1 Servizo FTP: vsftpd.....	121
5.13.11 Configuración de parámetros de rede.....	123

Material docente elaborado a partir da base dos materiales formativos de FP En liña propiedade do Ministerio de Educación e Formación Profesional.

[Aviso Legal](#)

5.1 Convencións empregadas

	Esta icona fai referencia a notas de introdución
	Esta icona indica aclaración
	Esta icona fai referencia a arquivos de configuración, de rexistro...
	Esta icona indica casos de uso
	Esta icona fai referencia a avisos o advertencias
	Esta icona indica incidentes
	Esta icona fai referencia a sección que inclúen instrucións paso a paso
	Esta icona fai referencia a sección que inclúen capturas de pantalla
	Esta icona fai referencia a actividades
	Esta icona fai referencia a documento esencial (licenza: http://www.ohmyicons.com)
	Referencia a ligazón recomendada (licenza: http://iconleak.com)

5.2 Introdución aos sistemas en rede. Direccionamento IP

5.2.1 Redes. Características e clasificación

Nesta unidade van estudar os conceptos teóricos de redes coas súas direccións físicas (MAC) e direccións lóxicas (IP), elementos físicos de conexión e cálculos de direccións IP.

Definimos rede informática como dúas ou máis dispositivos conectados para compartir os compoñentes da súa rede, e a información que poida almacenarse en todos eles.

Unha definición más formal é a dada por Andrew S. Tanenbaum, **unha rede de computadoras**, tamén chamada rede de computadores ou **rede informática**, é un conxunto de equipos informáticos conectados entre si por medio de dispositivos físicos que envían e reciben impulsos eléctricos, ondas electromagnéticas ou calquera outro medio para o transporte de datos, coa finalidade de compartir información e recursos.

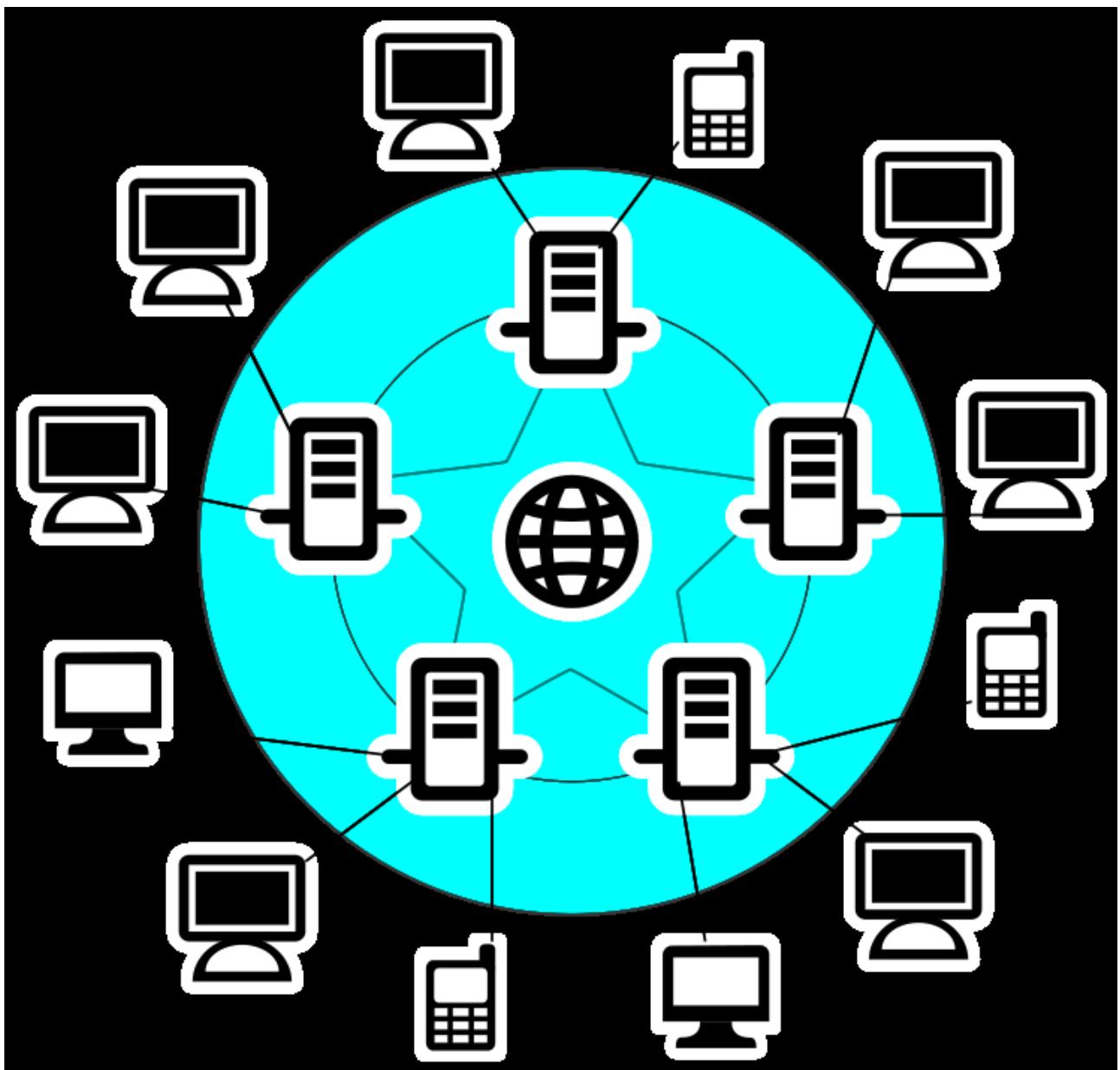
Redes de computadores. Vantaxes.

Se conectamos dous computadores entre si xa temos unha rede, se conectamos máis ordenadores, agregámoslle impresoras, e conectámonos a dispositivos que permitan saír a Internet, estamos a conseguir que a nosa rede sexa cada vez maior e poida dispoñer de maiores recursos, xa que os recursos individuais poden compartirse. Esta é a idea principal das redes, a medida que conectamos máis dispositivos e estes comparten os seus recursos, a rede será más potente.

- As principais vantaxes das redes de computadores serán:
- A posibilidade de compartir recursos.
- A posibilidade de compartir información.
- Aumentar as posibilidades de colaboración.
- Facilitar a xestión centralizada.
- Reducir custos.

5.2.1.1 Clasificación de Redes. Tipos de redes

Ilustración que mostra esquema simplificado da internet, onde se conectan diferentes tipos de computadores, sobre círculos concéntricos de cor azul clara, e que representa a conectividade que permite internet.



[Davide Capasso / daccap \(CC0\)](#)

As redes pódense clasificar segundo diferentes conceptos.

Por alcance ou extensión:

- **Rede de área local ou LAN (local area network)** é unha rede que se limita a unha área especial, relativamente pequena, tal como un cuarto, unha aula, un só edificio, unha nave, ou un avión. As redes de área local adoitan ter maiores velocidades e a unión delas crearán redes más grandes.
- **Rede de área metropolitana ou MAN (metropolitan area network)** é unha rede de alta velocidad (banda ancha) que dá cobertura nunha área xeográfica extensa.

Este concepto utilízase para definir redes que abordan extensións relativamente grandes, e que necesitan recursos adicionais aos que necesitaría unha rede local.

- **Rede de área ampla ou WAN (wide area network)** son redes informáticas que se estenden sobre unha área xeográfica extensa. Dentro desta clasificación podemos atopar as redes de telecomunicacións que permiten o uso da internet, e a propio Internet que pode considerarse como unha xigantesca rede WAN.

Segundo as funcións dos seus compoñentes:

- **Redes de igual a igual ou ente iguais**, tamén coñecidas como redes peer-to-peer, son redes onde ningún computador está a cargo do funcionamento da rede. Cada computador controla a súa propia información e pode funcionar como cliente ou servidor segundo necesíteo. Os sistemas operativos más utilizados inclúen a posibilidade de traballar desta maneira, e unha das súas características más destacadas é que cada usuario controla a súa propia seguridade.
- **Redes cliente-servidor**, baséanse na existencia dun ou varios servidores, que darán servizo ao resto de computadores que se consideran clientes. Este tipo de redes facilitan a xestión centralizada. Para crear redes deste tipo necesitamos sistemas operativos de tipo servidor, tales como Windows Server ou GNU-Linux.

Segundo o tipo de conexión:

- **Redes cableadas:** Neste tipo de redes utilízanse diferentes tipos de cables para conectar os computadores.
- **Redes sen fíos:** Son as redes que non necesitan cables para comunicarse, existen diferentes tecnoloxías inalámbricas que se estudan máis adiante.

Segundo o grao de difusión:

- **Internet** é un conxunto descentralizado de redes de comunicación interconectadas que utilizan a familia de protocolos TCP/IP, garantindo que as redes físicas heteroxéneas que a componen funcionen como unha rede lóxica única, de alcance mundial. Precisamente esta característica é a que fixo que o uso da internet xeneralícese e que todas as redes funcionen utilizando protocolos TCP/IP.
- **Intranet** é unha rede de computadoras que utiliza algunha tecnoloxía de rede para usos comerciais, educativos ou doutra índole de **forma privada**, isto é, que non comparte os seus recursos ou a súa información con outras redes. Aínda que a intranet non estea conectada a Internet, tamén adoitan utilizar os protocolos TCP/IP. Dito doutra forma, o funcionamento dunha intranet baséase nos mesmos principios que Internet, pero sen conexión a Internet.

5.3 Arquitectura da rede. Modelos OSI e TCP/IP

Cando se fala de arquitectura de rede refírese a como está construída a rede, co **hardware e software** utilizado.

En canto ao hardware, definiranse que **cables, equipos e conexións** utilizanse. Á parte de decidir que equipos se van a utilizar para a conexión, hai que **definir uns protocolos** na comunicación. Pero, que é un protocolo? Do mesmo xeito que a linguaaxe ten unhas normas e sintaxes para comunicarse dúas persoas, os **protocolos marcarán a forma de comunicarse dous dispositivos físicos**. Igual que hai distintas linguaxes, español, inglés, francés; tamén hai distintos protocolos.

A arquitectura de rede terá en conta **tres factores importantes**:

- **Topoloxía**: A forma de como se conectan os nodos (distintos equipos) dunha rede.
- **Método de acceso**: O medio utilizado para a transmisión dos datos: cable, aire.
- Os **protocolos** de comunicación.

5.3.1 Protocolo de comunicación

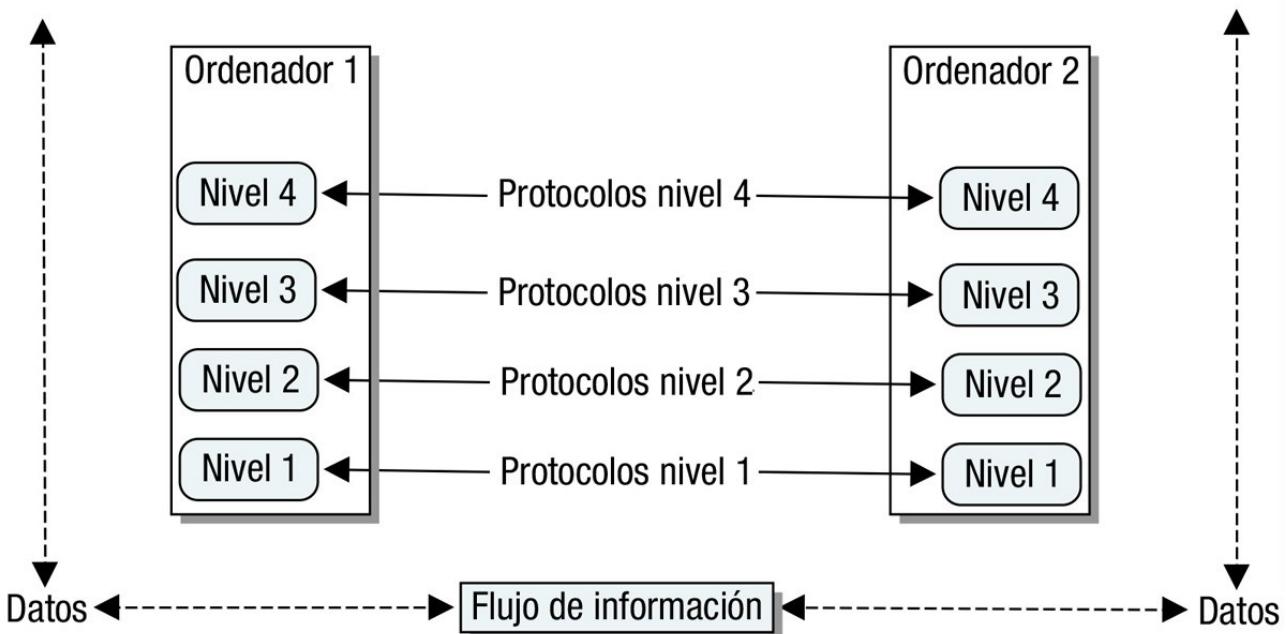
Como se dixo un protocolo de comunicacóns é un conxunto de regras normalizadas para a representación, sinalización, autenticación e detección de erros necesario para enviar información a través dunha canle de comunicación.

Necesítanse distintos protocolos para:

- Identificar o emisor e o receptor.
- Definir o medio ou canle que se pode utilizar na comunicación.
- Definir a linguaaxe común a utilizar.
- Definir a forma e estrutura das mensaxes.
- Establecer a velocidade e temporización das mensaxes.
- Definir a codificación e encapsulación da mensaxe.

5.3.2 Modelos por capas ou niveis

Ilustración que mostra dous rectángulos que representan dous computadores, e dentro deles ven catro rectángulos, cada un representando un nivel da arquitectura de rede. Entre cada nivel de cada computador debúxase unha frecha con dúas direccións que representan os protocolos entre niveis. Ademais debúxase o fluxo de información representado polo camiño que percorre os datos para chegar dun computador a outro, o cal empeza no nivel superior dun dos computadores e, pasando por todos os niveis inferiores, chega ao nivel superior do outro computador.



Imaxe obtida de materiais orixinais de FP a Distancia (Dominio público)

A arquitectura de rede divídese en niveis ou capas para reducir a complexidade do seu deseño. As capas están xerarquizadas, cada unha son os seus servizos e funcións asignadas, para o que utilizará os protocolos necesarios. Cada nivel só se comunica co nivel superior ou o inferior.

Entón, como funciona unha arquitectura baseada en niveis? Na figura anterior obsérvanse dous computadores conectados cunha arquitectura de catro niveles. Supoñamos que o computador primeiro quere realizar unha transferencia de datos ao computador segundo.

Na capa superior é onde se ordena realizar esa transferencia, pero a capa superior non se fixa nos detalles (como chegar ao segundo PC, a súa dirección, roteiro para chegar, medio de transmisión a utilizar...) Os detalles son as funcións das capas inferiores. De aí, que hai que pasar por todas as capas desde a cuarta capa superior á primeira capa inferior, onde cada capa realiza as súas funcións de buscar o mellor camiño para chegar ao destino. Desde a primeira capa, pásase a información ao computador de destino á súa primeira capa. Xa no computador de destino, séguese a secuencia contraria, vaise subindo de capa a capa, para que a capa superior só coñeza os datos recibidos, sen coñecer os detalles de como chegou esa información.

Unha boa analogía é mandar unha carta. Como clientes de Correos estaríase na capa superior, sen que importe ao remitente e ao destinatario como chega a carta. Eses detalles, escalas que realiza a carta, transporte utilizado (avión, tren ou furgón), carteiros utilizados son as funcións das capas inferiores. Ao destinatario só interésalle que chegue a carta e sen erros.

Neste tipo de arquitectura cada nivel xera o seu propio conxunto de datos, que se pasa cos datos orixinais á seguinte capa.

As arquitecturas de rede baseadas en capas facilitan as compatibilidades, tanto de software como de hardware, pois non é necesario cambiar todas as capas cando queremos mellorar o sistema. Bastaría modificar os protocolos afectados.

5.3.3 **Modelo OSI**

O **modelo OSI** que significa Open System Interconnection “Interconexión de sistemas abertos” é o modelo de rede creado pola Organización Internacional para a Normalización (ISO) no ano 1984. OSI agrupa os procesos de comunicación en sete capas que realizan tarefas diferentes. É conveniente ter en conta que o modelo OSI, non é unha arquitectura desenvolvida en ningún sistema, senón unha referencia para desenvolver arquitecturas de rede, de forma que os protocolos que se desenvolvan poidan ser coñecidos por todos.

Os niveis ou capas OSI son:

Capa 1, capa física. Encárgase das conexións físicas, incluíndo o cableado e os compoñentes necesarios para transmitir o sinal.

Capa 2, capa de enlace de datos. Empaquea os datos para transmitilos a través da capa física. Nesta capa defíñese o direccionamento físico utilizando as coñecidas direccións MAC. Ademais encárgase do acceso ao medio, o control de ligazón lóxica e da detección de erros de transmisión, entre outras cousas.

Capa 3, capa de rede. Separa os datos en paquetes, determina o roteiro que tomasen os datos e define o direccionamento.

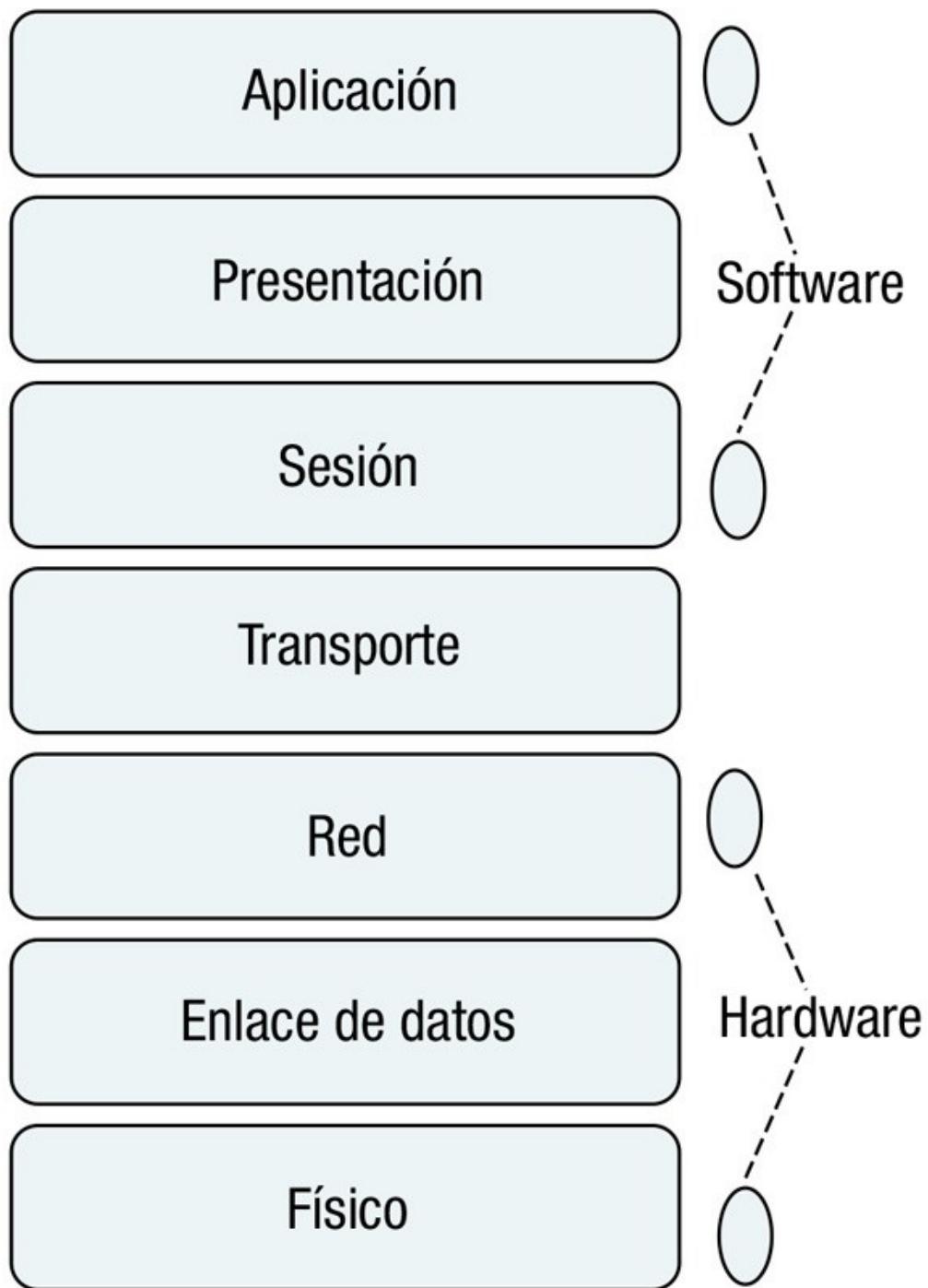
Capa 4, capa de transporte. Encárgase de que os paquetes de datos teñan unha secuencia adecuada e de controlar os erros.

Capa 5, capa de sesión. Mantén e controla a ligazón entre os dous extremos da comunicación.

Capa 6, capa de presentación. Determina o formato das comunicacións así como adaptar a información ao protocolo que se estea usando.

Capa 7, capa de aplicación. Define os protocolos que utilizan cada unha das aplicacións para poder ser utilizadas en rede.

Ilustración de sete rectángulos, un sobre outro, que representan os niveis do modelo OSI. Empezando por arriba temos as capas de: Aplicación, Presentación, Sesión, Transporte, Rede, Ligazón de datos e Física. Ademais móstrase como as tres capas inferiores estean relacionadas co hardware e as tres superiores co software, sendo a de transporte unha capa intermedia.



Imaxe obtida de materiais orixinais de FP a Distancia

Na imaxe represéntase os distintos niveis de OSI. **As capas 1, 2 e 3 do modelo están relacionadas co hardware e as capas 5, 6 e 7 están relacionadas co software, sendo a capa 4 unha capa intermedia entre hardware e software.** O cal quere dicir que os dispositivos e componentes de rede físicos, adoitan traballar nos niveis inferiores 1 a 3, sendo os programas os que traballan nos niveis superiores

5.3.4 **Modelo TCP/IP.**

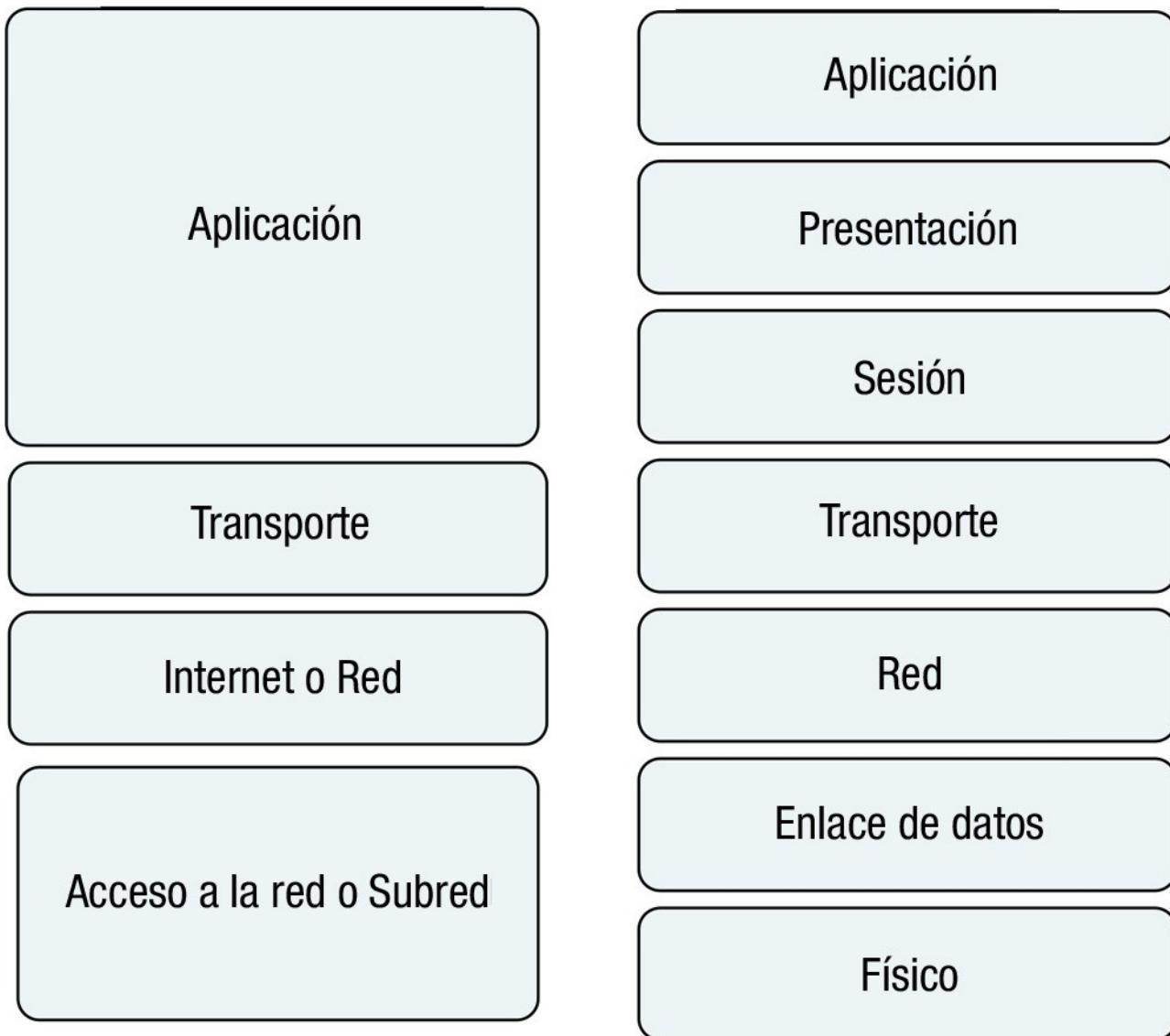
O modelo TCP/IP é a arquitectura de redes máis utilizada. É a base das comunicacóns da internet e dos sistemas operativos modernos.

Cando nos referimos á arquitectura TCP/IP ou modelo TCP/IP, estamos a referirnos a un conxunto de regras xerais de deseño e implementación de protocolos de rede, que permiten a comunicación dos computadores. O seu nome débese a que os dous protocolos más importantes que utiliza son o protocolo TCP (Protocolo de Control de Transmisión) e o protocolo IP (Protocolo da internet).

A arquitectura **TCP/IP está composta de catro capas ou niveis** que son:

- **Nivel de subred, nivel acceso á rede ou nivel de ligazón.** Encárgase do acceso ao medio de transmisión, é asimilable aos niveis 1 e 2 do modelo OSI. Permite e define o uso de direccións físicas utilizando as direccións MAC.
- **Nivel de rede ou nivel da internet.** Esta capa equivale á capa 3 do modelo OSI, co mesmo nome e encárgase de estruturar a información en paquetes e determinar o roteiro do PC orixe ao destino que tomarán os paquetes.
Os paquetes poden viaxar ata o destino de forma independente e desordenada. A ordenación e control de errores non será responsabilidade desta capa. O protocolo más significativo desta capa é o protocolo IP, e entre as súas funcións está a de dar unha dirección lóxica a todos os nodos da rede.
- **Nivel de transporte.** Esta capa equivale á capa 4 do modelo OSI. Encárgase de que os paquetes de datos teñan unha secuencia adecuada e de controlar os errores. Os protocolos más importantes desta capa son: TCP e UDP. O protocolo TCP é un protocolo orientado a conexión e fiable, e o protocolo UDP é un protocolo non orientado a conexión e non fiable.
- **Nivel de aplicación.** Esta capa engloba ás capas 5, 6 e 7 do modelo OSI. Inclúe todos os protocolos de alto nivel relacionados coas aplicacións que se utilizan na internet.

No gráfico seguinte vese a equivalencia dos modelos OSI e TCP/IP.



Imaxe obtida de materiais orixinais de FP a Distancia

Ilustración que mostra á esquerda da imaxe móstrase o esquema da arquitectura TCP/IP que consta de catro niveles, e á dereita os sete niveles do modelo OSI. Compárase, empezando por arriba, a capa de Aplicación TCP/IP coas capas de Aplicación, Presentación, Sesión. A capa de Transporte que coincide nos dous modelos. A de Rede que tamén coincide. Por último a capa de Acceso á rede que sería equivalente ás Ligazón de datos e Física do modelo OSI.

5.3.4.1 Nivel 1. Nivel de ligazón ou acceso

A principal función deste nivel é converter a información fornecida polo nível de rede, en sinais que poidan ser transmitidas polo medio físico ao nodo de destino. A función inversa é converter os sinais que chegan polo medio físico en paquetes de información manexables para o nível de rede.

Neste nivel débense ter en conta as cuestiós relacionadas coas conexións físicas, que nas redes locais veñen definidas polo estándar IEEE 802.3 que se estuda no seguinte libro.

Un aspecto moi importante deste nivel é o **direcciónamento físico**, coñecido como **control de acceso ao medio**, con siglas MAC. A dirección MAC é un identificador de 48 bits, que se representa con 12 díxitos hexadecimais, representado habitualmente no formato FF:FF:FF:FF:FF:FF

Ao dicir díxitos hexadecimais, faise referencia a que se utiliza o sistema de numeración basee 16, que significa que cada cifra pode tomar 16 valores distintos:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Desta forma, **todas as tarxetas de rede teñen unha dirección física ou dirección MAC única no mundo.**

Dos 12 díxitos hexadecimales, os 6 primeiros representan o fabricante da tarxeta de rede.

Neste nivel hai dous **protocolos** relacionados co direcciónamento físico: **ARP e RARP**.

ARP (Address Resolution Protocol, Protocolo de resolución de direccións) encárgase de relacionar a dirección física (dirección MAC) coa correspondente dirección lóxica (dirección IP). Mientras que a dirección física traballa no nivel de subred, a dirección lóxica traballa no nivel de rede. Pero necesítanse ambas as para enviar mensaxes dun computador a outro.

O protocolo **RARP** (Reverse ARP, Protocolo de resolución de nomes inverso) realiza a función contraria.

Estes dous protocolos tamén traballan no seguinte nivel, por ser o que traballa coas direccións IP.

Desta forma, a información para enviar ao computador de destino, será a recibida da capa superior (capa de rede), xunto coa dirección MAC do equipo orixe e a dirección MAC do equipo destino. A esta información chámase trama.

5.3.4.2 Nivel 2. Nivel de rede

O obxectivo principal do nivel de rede será encamiñar os paquetes desde o nodo orixe ata o nodo destino, aínda que estean en distinta rede. A información divídese en paquetes, que viajan de forma independente, atravesando distintas redes e sen orde. A capa de rede non se preocupa das tarefas de ordenación dos paquetes cando chegan ao seu destino. Isto é o que se coñece como servizo non orientado a conexión. Cada paquete recibe o nome de datagrama.

As funcións más importantes da **capa de rede** son:

- **O direcciónamento lóxico:** Permite identificar de forma única cada nodo dunha rede. As direccións lóxicas reciben o nome de IP. Neste nivel fálase de

direcciónamento lóxico, para distinguilo do direcciónamento físico visto no nivel de subred.

- **O encamiñamento:** Tamén chamado encamiñamento, os protocolos desta capa deben ser capaces de atopar o mellor camiño entre dous nodos.

Para realizar estas funcións o nivel de rede utiliza como protocolos más destacados deste nivel:

- **IP: Internet Protocol, ou Protocolo da internet** proporciona un encamiñamento de paquetes non orientado a conexión e é usado tanto pola orixe como polo destino para a comunicación de datos.

O protocolo IP, tamén proporciona as direccións IP. A dirección IP é a dirección lóxica que identifica dentro dunha rede a un nodo ou tarxeta de rede. Coexisten na actualidade dúas versións de IP, IPv4 (versión 4) e IPv6 (versión 6). Diferéncianse no número de bits que utiliza cada dirección, IPv4 utiliza direccións de 32 bits e IPv6 6 utiliza direccións de 128 bits.

Exemplos de direccións IP son:

IP versión 4: 192.168.1.11 (Utilizando valores en decimal).

IP versión 6: 2001:0DB8:0000:0000:0000:1428:57AB (Utilizando valores en hexadecimal e pode simplificarse como: 2001:0DB8::1428:57AB)

- **ARP e RARP:** Tamén se utilizan na capa de subred de datos e serven para relacionar direccións IP con direccións MAC e viceversa.
- **ICMP: Protocolo de mensaxes de control na internet**, fornece capacidades de control e envío de mensaxes. **Tamén se considera protocolo do nivel de transporte, e ferramentas tales como ping e tracert utilizano** para poder funcionar (estas ferramentas estudarémolas na unidade 9 e 10).

5.3.4.3 Nivel 3. Nivel de transporte.

Cumpe a función de establecer as regras necesarias para establecer unha conexión entre dous dispositivos remotos. Como a capa de rede na arquitectura TCP/IP non se preocupa da orde dos paquetes nin dos erros, é nesta capa onde se coidan estes detalles.

Este nivel é o encargado da transferencia libre de erros dos datos entre o emisor e o receptor, aínda que non estean conectados na mesma rede.

Do mesmo xeito que as capas anteriores, a información que manexa esta capa ten o seu propio nome e chámase segmento. Por tanto a capa de transporte débese de encargar de unir múltiples segmentos do mesmo fluxo de datos.

Os dous protocolos más importantes que traballan neste nivel son o TCP e o UDP.

TCP é un protocolo orientado a conexión e fiable, deseñouse especificamente para proporcionar un fluxo de bytes confiable de extremo a extremo a través de redes non fiables. Por iso é tan útil na internet, xa que as redes que configuran Internet poderían ter diferentes topoloxías, anchos de banda, retardos, tamaños de paquete, etc. Pero TCP ten un deseño que se adapta de maneira dinámica ás propiedades destas redes e permite a conexión en moitos tipos de situacóns.

UDP é un protocolo non orientado a conexión e non fiable, este protocolo proporciona todo o necesario para que as aplicacións envíen datagramas IP encapsulados sen ter unha conexión establecida. Un dos seus usos é na **transmisión de audio e vídeo en tempo real**, onde non é posible realizar retransmisións polos estritos requisitos de retardo que se ten nestes casos.

5.3.4.4 Nivel 4. Nivel de aplicación.

O **nivel aplicación** contén os **programas de usuario (aplicacións)** que fai que o noso computador poida crear textos, chatear, ler correo, visitar páxinas web, etc. Neste nivel inclúense todos os protocolos de alto nivel que utilizan os programas ou servizos para comunicarse.

Algúns dos protocolos da capa de aplicación son:

- **HTTP:** Protocolo de transferencia de hipertexto, é o protocolo utilizado nas páxinas web. Por iso é polo que unha páxina web, sempre se pon previamente http:// que significa que se está utilizando o protocolo http. É un protocolo orientado a transaccións e segue o esquema petición-resposta entre un cliente e un servidor. Ten unha versión segura que é o **HTTPS**
- **FTP:** Protocolo utilizado na transferencia de ficheiros entre un computador e outro.
- **DNS:** Servizo de nomes de dominio, é o sistema utilizado na internet para converter os nomes dos nodos de rede en direccións de rede. Grazas a este servizo, ao navegar por páxinas web utilízanse nomes do dominio (exemplo, www.mipagina.es) no canto de direccións IP, más difíciles de memorizar.
- **SMTP e POP:** Protocolos para o correo electrónico. SMTP é o protocolo simple de trasferencia de correo, baseado en texto e utilizado para o envío de mensaxes de correo. POP é o protocolo de oficina de correo, e utilízase nos clientes de correo para obter as mensaxes de correo almacenados nun servidor.
- **SNMP:** Protocolo de administración de redes, permite monitorar e controlar os dispositivos de rede e de administrar configuracións e seguridade.

Porto e socket

A cada aplicación asígnaselle unha dirección de transporte, chamado porto.

Por exemplo a aplicación ou protocolo HTTP utiliza o porto 80. Desa forma, nun servidor de páxinas web, sempre está aberto ou escoitando o porto 80, que significa que está a

esperar peticións de páxinas web polo devandito porto desde calquera outro computador do mundo para atendela.

O concepto de porto é similar, a dicir que nunha casa existan varias portas (principal, xardín, lateral). Cada servizo utiliza distintos portos.

- HTTP utiliza o porto 80, mentres que HTTPS utiliza o porto 443.
- O servizo FTP utiliza os portos 20 e 21.
- O servizo DNS utiliza o porto 53.

Un socket é unha conexión única, que está formada pola unión da dirección IP máis o porto. Se nunha navegador web escribimos <http://www.empresas.es>, e supoñamos que o servidor web que atende <http://www.empresas.es> corresponde á dirección IP 192.168.1.11, é equivalente a escribir no navegador 192.168.1.11:80

5.3.5 Versións de Ethernet. Estándar IEEE 802.3

Nos seguintes apartados vai estudar como se conectan os computadores na rede (topoloxía de rede) e que dispositivos físicos utilizan para a súa conexión.

Antes diso, dedícase este apartado para o estándar IEEE 802.3 que regulas as redes cableadas, chamadas redes Ethernet.

Desde os anos 80, estandarizáronse moitas versións, para ver as distintas versións visitar https://es.wikipedia.org/wiki/IEEE_802.3

Aquí, simplemente vaise a apuntar as velocidades alcanzadas más importantes e os nomes denominados comercialmente.

- Ethernet: velocidad de 10 Megabit/seg
- Fast-Ethernet: velocidad de 100 Megabit/seg
- Gigabit-Ethernet: velocidad de 1 Gigabit/seg
- 10 Gigabit-Ethernet: velocidad de 10 Gigabit/seg

Nas redes locais, as velocidades más habituais na actualidade son Fast-Ethernet e Gigabit-Ethernet. As instalacións novas realizan con Gigabit. Cando incorporemos un computador á nosa rede, teremos que ter en conta que a tarxeta sexa compatible coa velocidad da nosa LAN. Igualmente hai cableado con distintas categorías, con velocidades máximas admitidas.

As distintas versións IEEE 802.3 especifican que compoñentes se deben utilizar para esa versión.

Topoloxías de rede e modos de conexión.

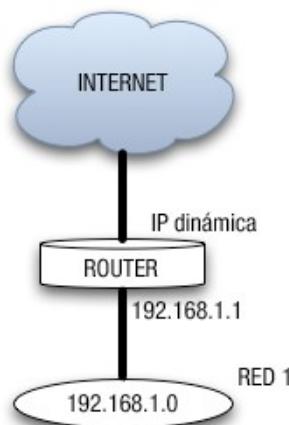
5.4 Topoloxías de rede

A **topoloxía de rede desde o punto de vista físico**, considérase a forma en que se conectan os computadores dunha rede. As topoloxías de conexión principais son **bus, anel e estrela**.

Cando se fai unha instalación de rede realiza un esquema de rede onde se mostre a localización de cada computador, cada equipo de interconexión e o cableado utilizado. Realízase utilizando os planos do edificio e é unha ferramenta útil á hora do mantemento e actualización.

A **topoloxía desde o punto de vista lóxico** ou esquema lóxico, móstranos o uso da rede, o nome dos computadores, as direccións, as aplicacións, etc.

Como exemplo na figura seguinte móstrase un esquema lóxico dunha rede de computadores que terá conexión a Internet grazas a un router. A rede represéntase cun óvalo onde dentro ten a dirección de rede e fóra o nome da rede.



Imaxe obtida de materiais orixinais de FP a Distancia

Illustración que mostra unha nube que representa Internet, que se conecta a un cilindro plano que representa un router. O router conecta cunha rede que se representa cun óvalo onde dentro ten a dirección de rede 192.168.108.0 e fóra o nome da rede, REDE 1.

Nas redes wifi ou inarámicas, fálase de modo **de conexión**. Defínense dous modos de conexión **inarámica**, que son **modo infraestrutura** (necesítase punto de acceso) e modo ad-hoc (non necesita punto de acceso)

Comézase o apartado coas topoloxías desde o punto de vista físico: bus, anel e estrela.

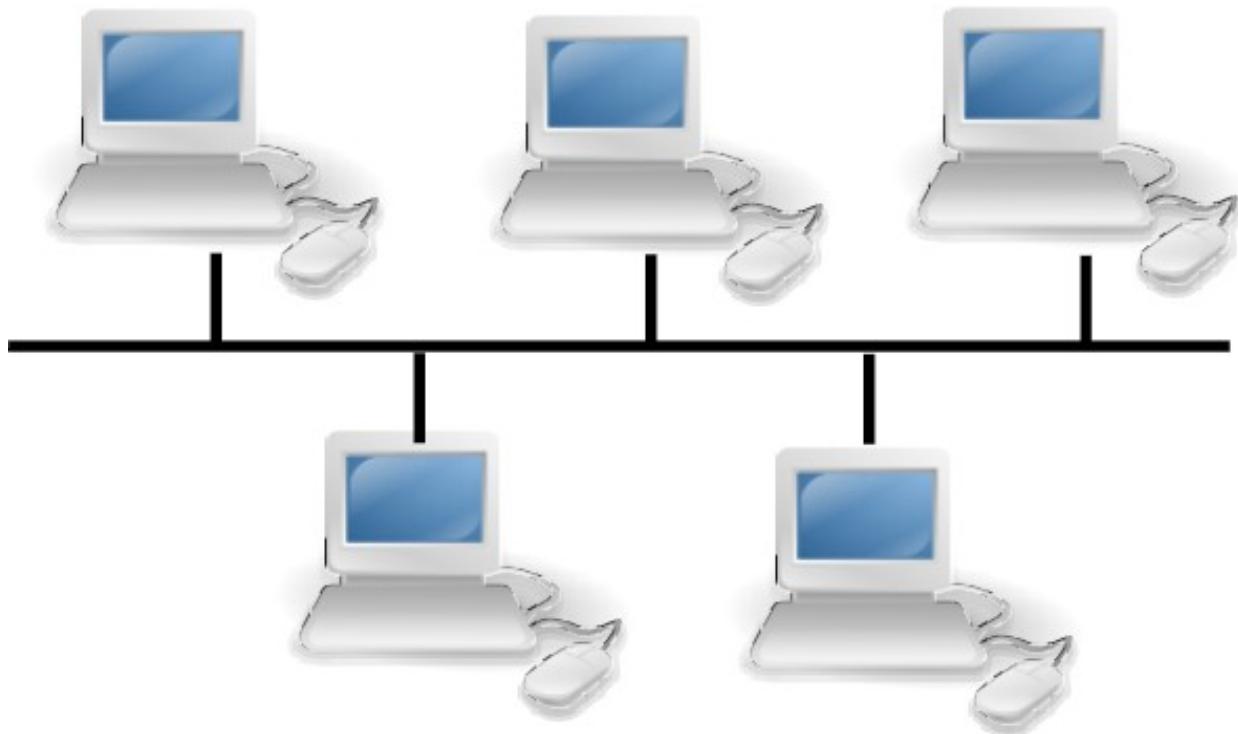
5.4.1 Topoloxía en bus

A topoloxía en bus utiliza **un único cable troncal con terminacións nos extremos**, de tal forma que os computadores da rede conéctanse directamente á rede troncal. As primeiras redes Ethernet utilizaban esta topoloxía usando cable coaxial (igual que o cable de televisión)

Actualmente empréganse variantes da topoloxía en bus nas redes de televisión por cable e en equipamentos industriais.

Deixouse de utilizar pola súa pouca flexibilidade ante fallos. Ao observar a figura é fácil darse conta de que a rotura dun punto da rede, deixa toda a rede inutilizable.

Ilustración que mostra esquema da topoloxía en bus:. Cinco ordenadores conectados a un bus central.



[Lmbuga](#) (Dominio público)

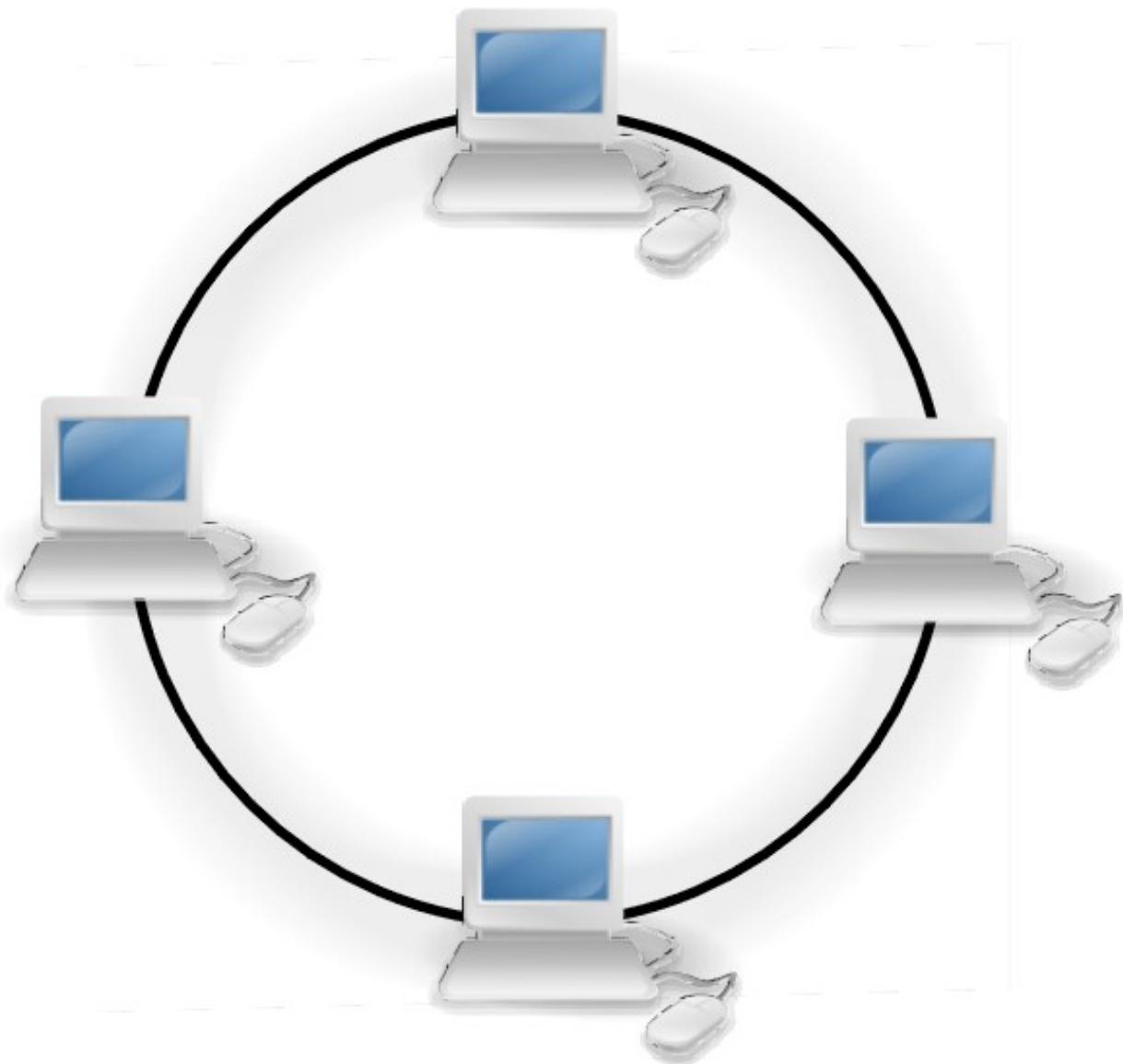
5.4.2 Topoloxía en anel

A topoloxía en anel conecta cada computador ou nodo co seguinte e o último co primeiro, creando un anel físico de conexión. Cada estación ten un receptor e un transmisor que fai a función de repetidor, pasando o sinal á seguinte estación. Neste tipo de rede a comunicación dáse polo paso dunha testemuña, desta maneira evítanse eventuais perdas de información debidas a colisións. As redes locais Token-ring empregan unha topoloxía en anel aínda que a conexión física sexa en estrela.

O habitual, é que os datos se envíen en ambas as direccións, creando redundancia e tolerancia a fallos (pois ao contrario que na topoloxía en bus, cun único punto de ruptura a rede segue operativa)

Esta topoloxía utilízase actualmente nas redes FDDI (Fiber Distributed Data Interface, Interface de datos distribuídos por fibra) como parte dunha rede troncal que distribúe datos por fibra óptica.

Ilustración que mostra esquema da topoloxía en anel. Catro ordenadores conectados entre si formando un anel.



[Lmbuga](#) (Dominio público)

5.4.3 Topoloxía en estrela

A topoloxía en estrela conecta **todos os computadores a un nodo central**, chamado **equipo de interconexión**, que pode ser: un router, un conmutador ou switch, ou, un

concentrador ou hub. As **redes de área local modernas** baseadas no estándar **IEEE 802.3** utilizan esta topoloxía.

O equipo de interconexión central canaliza toda a información e polo pasan todos os paquetes de usuarios, este nodo central realizará funcións de distribución, conmutación e control. Este equipo debe estar sempre activo, xa que se falla toda a rede queda sen servizo.

Entre as vantaxes de utilizar esta topoloxía temos que esta topoloxía é tolerante a fallos xa que a ruptura dun cable, só deixa inoperativo un nodo. Ademais facilita a incorporación de novos computadores á rede sempre que o nodo central teña conexións libres.

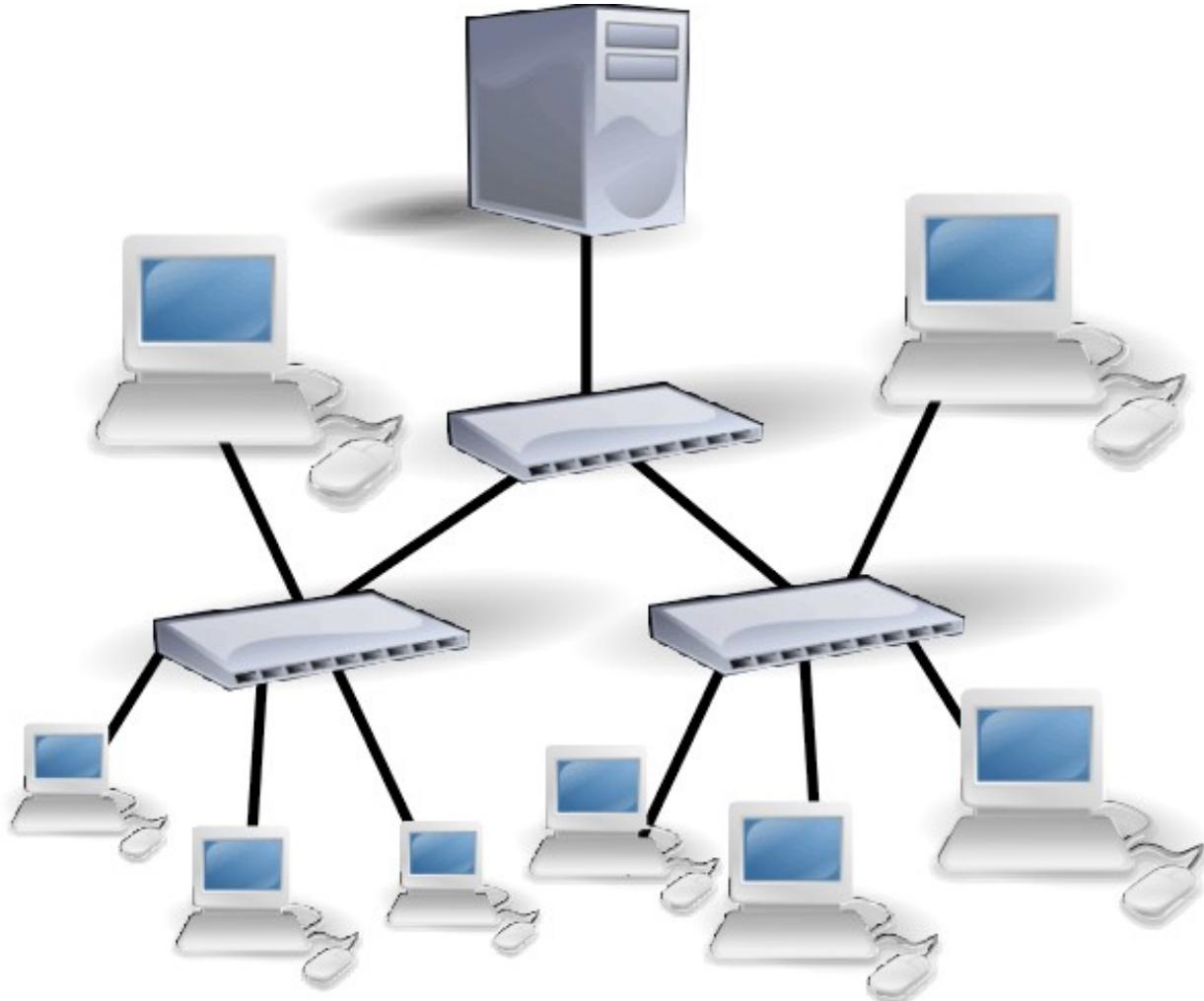
Ilustración que mostra a conexión de computadores en estrela



[Lmbuga](#) (Dominio público)

O habitual nun edificio é que se utilice unha **estrela estendida ou árbore**, onde as redes en estrela conéctanse entre si con switch (comutadores)

Ilustración que mostra varios conectados conectados en estrela a un switch, e estes switch conectados formando unha árbore de conexións.

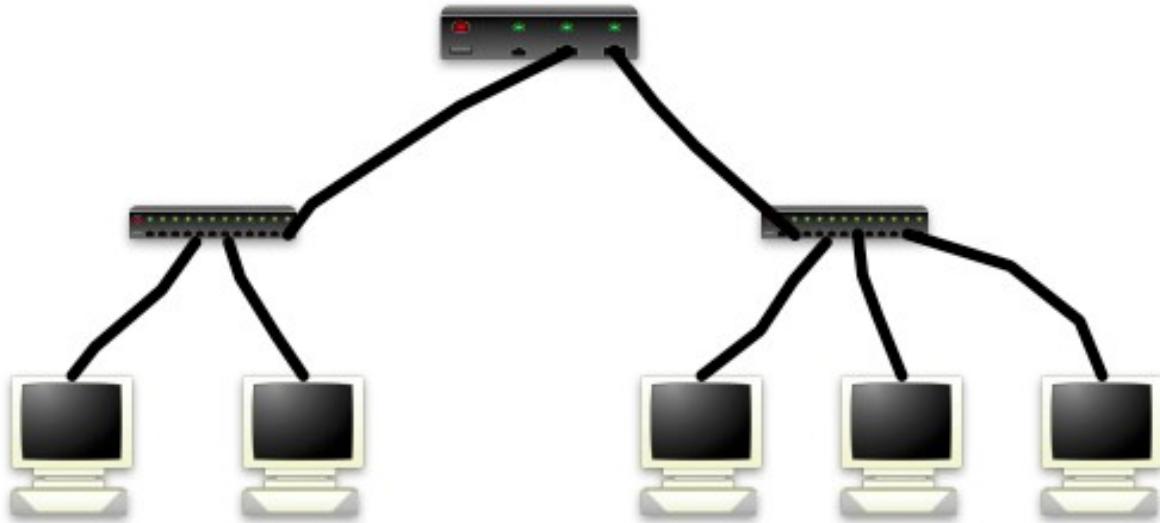


[Lmbuga](#) (Dominio público)

A estrela estendida habitualmente é unha **estrela xerárquica** onde un nodo marca o inicio da estrutura. É habitual que ese nodo inicial sexa un router que serve para a comunicación co exterior con internet, e a partir dese router créase unha rede de área local que permite dar servizos a redes de área locais más pequenas.

Na imaxe móstrase un router, ao que se conectan dous switch e 3 PC conectados a cada switch.

Ilustración que mostra dous computadores conectados a un switch, outros tres ordenadores conectados a outro switch, e os dous switch conectados a un router.



Imaxe obtida de materiais orixinais de FP a Distancia

Esta topoloxía ten a vantaxe que a partir dunha única conexión a Internet podemos dar servizo a varias redes ou subredes locais, co que se aforran custos.

Todos estes elementos entenderanse mellor no próximo libro donse estúdanse os elementos de interconexión.

5.4.4 Redes sen fíos. Modo de conexión: infraestrutura e ad-hoc.

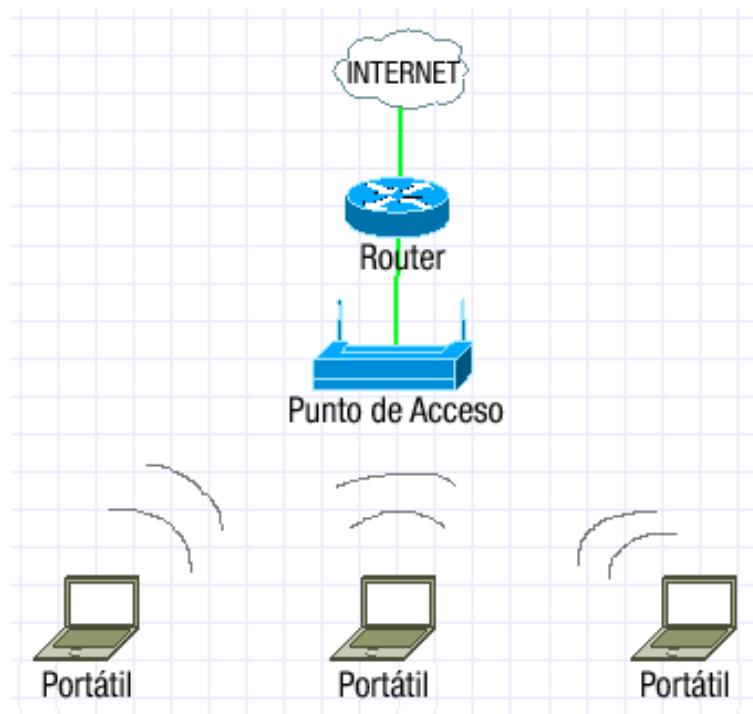
En redes sen fíos ou redes Wifi, que seguen o estándar IEEE 802.11, introdúcese un concepto diferente ao de topoloxía, que é o de modo de conexión. Especifícanse dous modos de conexión, que son o modo infraestrutura e o modo ad-hoc.

5.4.4.1 Modo infraestrutura

O **modo infraestrutura** adóitase utilizar para conectar equipos inalámbricos a unha rede cableada xa existente, **utilízase un equipo de interconexión como ponte entre a rede sen fíos e a cableada**. Este equipo denominase **Punto de Acceso** e pode ser un equipo especial que faga só esta función, ou o mesmo router (o que adoita instalar a compañía de telecomunicacións) que á súa vez faga de punto de acceso.

Na imaxe aparece un router, conectado ao momento de acceso, onde tres portátiles conéctanse á rede a través do punto de acceso.

Ilustración que mostra esquema de rede, onde se pode ver tres portátiles que de forma inalámbrica, teñen conexión cun punto de acceso. Este punto de acceso ten conexión a un router a través dun cable. O router permite conectarse a Internet.



Imaxe obtida de materiais orixinais de FP a Distancia

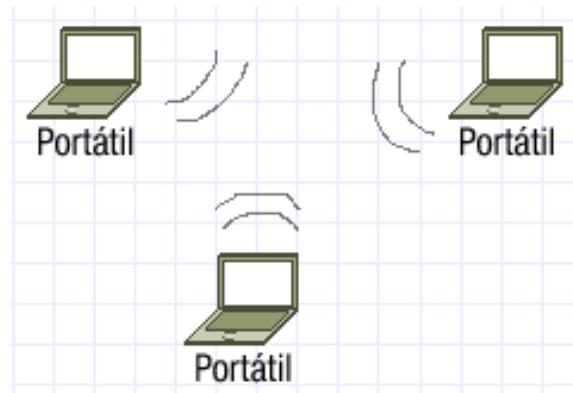
5.4.4.2 Modo ad-hoc

O modo ad-hoc permite conectar dispositivos inalámbricos entre si, **sen necesidade de utilizar ningún equipo como punto de acceso**. Desta forma cada dispositivo da rede forma parte dunha rede de igual a igual (Peer to Peer).

Este tipo de conexión permite compartir información entre equipos de forma puntual e a pouca velocidad, estando dirixidas para redes sen fíos persoais. Un exemplo de modo ad-hoc son as conexións a través de Bluetooth.

Na imaxe ven tres equipos portátiles conectados entre eles sen ningún elemento máis.

Ilustración que mostra tres portátiles que se conectan de forma inalámbrica entre eles.



Imaxe obtida de materiais orixinais de FP a Distancia

5.5 Compoñentes físicos das redes informáticas

5.5.1 Medios de transmisión

Pódese considerar compoñentes da rede aos propios computadores cos seus sistemas operativos e a todo o hardware e software que axuda a que a rede funcione. Este punto vai centrar nos compoñentes hardware.

Algúns destes compoñentes son:

- O **cableado de rede e as súas conectores**, que permite a transmisión do sinal.
- O **rack ou armario de conexións**, destinado a aloxar equipamento electrónico, informático e de comunicacóns.
- Os patch panel, **paneis de parcheo** que serven para organizar o cableado no rack.
- As **tarxetas de rede**, que permiten a conexión física do computador, ben por cable ou de forma inalámbrica.
- Os **conmutadores ou switches**, que **permiten a conexión** de diferentes computadores entre si e de segmentos da mesma rede entre si.
- Os **enrutadores ou routers**, tamén coñecidos como encaminadores, que **permiten conectar redes diferentes**, por exemplo unha rede de área local con Internet.
- Os **puntos de acceso**, que **permiten a interconexión de dispositivos inalámbrios** entre si, e/ou a conexión de dispositivos cableados cos inalámbrios.
- As devasas, que poden ser dispositivos hardware cun software específico para bloquear accesos non autorizados á rede, ou software específico que se instale nos servidores para evitar os accesos non autorizados.
- Os servidores, que non son máis que ordenadores pero con software de servidor.
- Os **nodos de rede**, onde se fai referencia ás estacións de traballo, que son os computadores que traballarán en rede, así como calquera periférico conectado a un equipo ou directamente á rede, por exemplo impresoras ou discos duros de rede.

Na imaxe pódese visualizar un armario de distribución onde se atopan varios switches, routers, con conexións de cables de par trenzado e paneis de parcheo.



Imaxe obtida de materiais orixinais de FP a Distancia

5.5.2 Clasificación dos medios de transmisión.

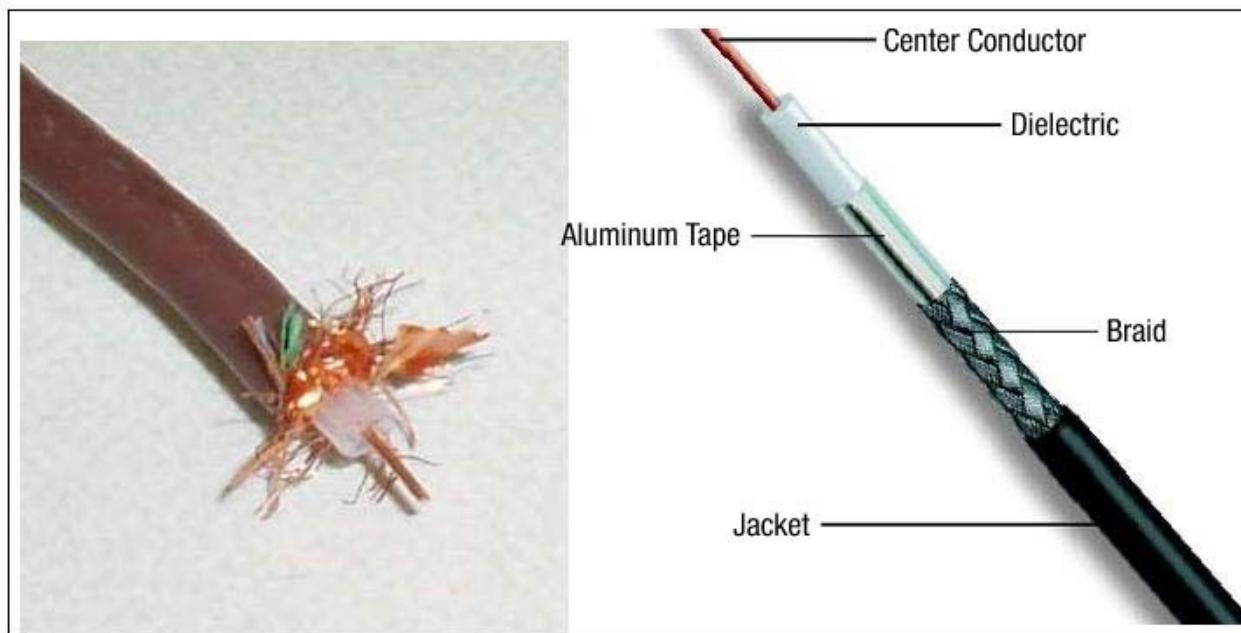
O medio de transmisión nas redes de computadores serán as canles que transmiten a información entre os nodos da rede, as transmisións realizanse habitualmente empregando ondas electromagnéticas. As ondas electromagnéticas son susceptibles de ser transmitidas polo baleiro. Por ese motivo podemos clasificar os medios de transmisión como:

- **Medios guiados:** conducen as ondas electromagnéticas a través dun camiño físico. Entre os tipos de cables más utilizados atopamos o par trenzado, o coaxial e a fibra óptica.
- **Medios non guiados:** proporcionan un soporte para que as ondas transmítanse, pero non as dirixen. As ondas transmítense **a través do aire ou do baleiro**.

ven a continuación os distintos tipos de cables utilizados.

5.5.2.1 Cable coaxial

Ilustración de dúas imaxes, á esquerda apréciase un cable coaxial e á dereita un esquema de como está formado, coas descripcións en inglés, e que podemos traducir como: (empezando en grao sumo externo) illante externo, malla, protector de aluminio, dieléctrico, condutor central.



[RONALD \(CC0\)](#)

O **cable coaxial**, está composto dun fío condutor chamado núcleo e dun mallazo externo separados por un dieléctrico ou illante.

Os conectores que se adoitan utilizar son o **BNC** e o **tipo N**.

Actualmente o cable coaxial non se utiliza para montar redes de computadores, se non para a distribución dos sinais de televisión, internet por cable, etc.

5.5.2.2 **Cable de par trenzado**

Ilustración de cable de par trenzado tipo FTP, onde se aprecian as distintas cores e os pares trenzados correspondentes, ademais do apantallamiento do cable.



Baran Ivo (Dominio público)

O cable máis utilizado en redes de área local, é o par trenzado de oito fíos. Consta de oito fíos con cores diferentes e utilízase en redes de computadores baixo o estándar IEEE 802.3 (Ethernet). Dise par trenzado, porque van de 2 en 2 fíos trenzados.

As cores son: branco-laranxa, laranxa, branco-verde, verde, branco-azul, azul, branco-marrón e marrón. Cando se fala de cor branca-laranxa está a falarse dun fío laranxa, cunha liña branca pintada, de forma que o par de fíos trenzado fórmano o laranxa co branco-laranxa.

A distribución destas cores cando se conectan no conector vén estandarizada, para que as conexións de rede sexan facilmente recoñecibles.

No mercado atópanse cables de par trenzado de distintas categorías. Para as redes actuais Ethernet utilízanse cables de categoría 5, 5e, 6, 7..

- Os de categoría 5 admiten só transferencias de 100 Megabit/seg. Válidos para redes Fast-Ethernet.
- Os de categoría 5e, 6 e 7 alcanzan os 1000 Megabit/seg = 1 Gigabit/seg. Obrigatorio para redes Gigabit-Ethernet

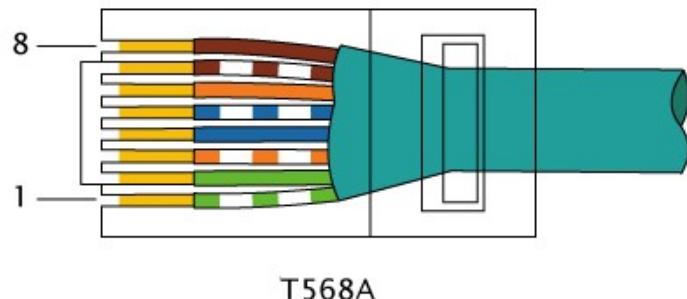
O conector que se utiliza con este cableado é o RJ-45. Para realizar o cable, conéctanse 2 conectores RJ-45 machos ás puntas do cable cunha ferramenta específica, chamada crimpadora. Este cable unha vez terminado, poderase conectar ás conexións femias habituais nas tarxetas de rede, router e switch.

Para a conexión dos 8 fíos ao conector RJ-45 realiza-se segundo os estándares ANSI/EIA/TIA 568 A e B.

Nas conexións de rede usaremos cables directos, que significa que os dous extremos utilizarán o mesmo estándar, recoméndase usar a 568B.

En caso de querer facer un cable cruzado, usarase a norma 568A en un extremo e a norma 568B no outro.

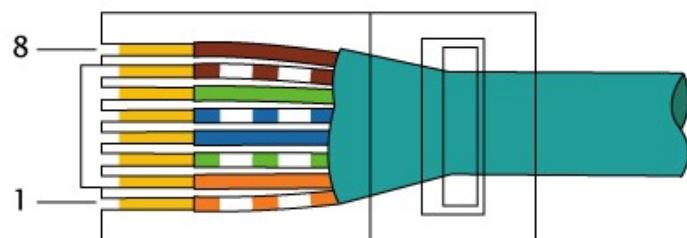
Ilustración de esquema da conexión 568A.



T568A

[Ip](#) (Dominio público)

Esquema da conexión 568B



T568B

[Ip](#) (Dominio público)

O habitual é utilizar cables directos. Os cables cruzados úsanse para conectar dous equipos do mesmo tipo (que non é o habitual), por exemplo, computador con computador, router con router. Ao final do libro, unha vez vistos os dispositivos de interconexión, aclárase cando se utilizan cables directos e cables cruzados.

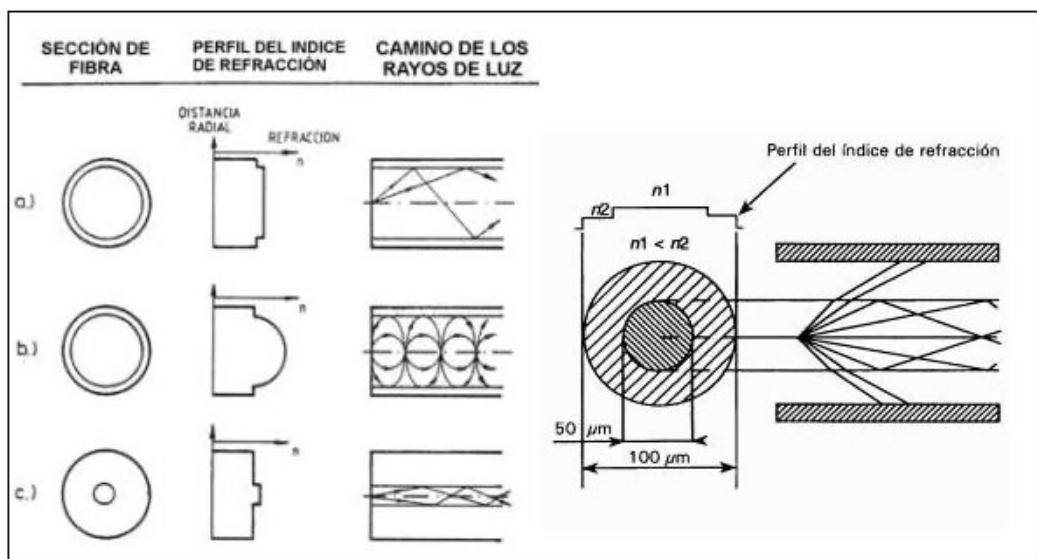
Táboa de estándar 568A e 568B:

Pin	568-A	568-B
1	Blanco-verde	Blanco-naranja
2	Verde	Naranja
3	Blanco-naranja	Blanco-verde
4	Azul	Azul
5	Blanco-azul	Blanco-azul
6	Naranja	Verde
7	Blanco-marrón	Blanco-marrón
8	Marrón	Marrón

5.5.2.3 Fibra óptica

A fibra óptica é un fío moi fino de material transparente, vidro ou materiais plásticos, polo que se envían pulsos de luz. A fonte de luz pode ser láser ou un led e é inmune ás interferencias electromagnéticas, polo que é moi fiable. Ademais permite transmitir gran cantidade de datos a unha gran distancia e a unha gran velocidade.

Ilustración que mostra esquema dos tipos de fibra óptica, onde se aprecia, de esquerda a dereita, a sección, o perfil de refracción, o camiño dos raios de luz, e un corte esquemático da fibra óptica.



Ronald (CC BY-SA)

Existen dous tipos de fibra óptica, a multimodo e a monomodo. Os conectores que se utilizan son FC e FDDI.

5.5.2.4 Cableado estruturado

Chámase cableado estruturado á infraestrutura de telecomunicacións necesaria para conectar un edificio ou un conxunto de edificios. Nesta infraestrutura inclúense cables, conducións, regletas, armarios, dispositivos, espazos específicos, etc.

Elementos incluídos no cableado estruturado son:

- Armarios de distribución, onde conflúen os cables e onde se montan os equipos de interconexión, utilizando rack e paneis de parcheo.
- Cableado horizontal, o cableado de planta.
- Cableado troncal ou vertical de distribución entre plantas.
- Sala de equipamento, sala onde se distribúen todas as conexións do edificio, para os distintos armarios de distribución.

- Entrada do edificio, por onde se conectan os cables exteriores cos interiores.
- Cableado de interconexión de edificios.

Os estándares de cableado estruturado especifican como organizar a instalación do cableado, tipo de cable, conectores, lonxitudes máximas dos tramos, etc. Por exemplo, no cableado horizontal recoméndase un máximo de 100 metros desde o armario de distribución ou rack ata a área de traballo.

5.6 Elementos de interconexión

Os elementos de interconexión refírense aos equipos que permiten conectar equipos nunha rede local ou rede extensa. Unha forma de clasificar aos equipos de interconexión é teniendo en cuenta o nivel no que traballan tomando como referencia o modelo OSI.

- No **nivel 1 ou nível físico** temos:

Tarxetas de rede: cableadas ou inarámicas. Permiten conectar os equipos á rede.

Concentradores ou hubs: Son un dispositivo que permiten conectar varios computadores, pero realiza de forma non intelixente, pois envía a información a todos os computadores, sen regular o tráfico. Como analogía, é coma se un carteiro non soubese localizar a un destinatario, e enviase unha copia da carta a todo o mundo, sendo labor do destinatario, ver se esa carta era para el ou non.

A maior eficiencia dos switches e o seu baixo custo, fixo desaparecer a venda de hubs.

Repetidores: poden ser locais ou remotos, e a súa función é repetir o sinal para rexenerala e/ou amplificarla.

- No **nivel 2 ou nível de ligazón de datos** temos:

• **Comutadores ou switches:** Son un dispositivo que permiten conectar varios computadores, pero de forma intelixente (ao contrario que un hub), xa que só se envía a información ao computador que a necesita. Desta forma o tráfico é moito máis rápido que cun hub. Tamén se di que conectan segmentos e computadores da mesma rede.

Pontes ou bridges: conectan subredes, transmitindo dunha a outra o tráfico xerado non local.

Puntos de acceso: encárganse de conectar elementos inalámbricos entre si, e de permitir o acceso de dispositivos inalámbricos a redes cableadas.

- No **nivel 3 ou nível de rede:**

Enrutadores ou routers: encárganse de conectar **redes diferentes**. O seu principal uso está na conexión a Internet, xa que permite que redes de área local poidan conectarse a Internet. Como une redes diferentes, necesita polo menos dúas direccións IP, unha para cada rede. Por exemplo, os router que nos ofrecen

as compañías telefónicas, traballan con dous IP, unha delas está na rede do operador telefónico, que chamamos nosa IP externa, porque é a dirección coa que nos ven desde fóra, e a outra está na rede interna nas nosas casas, chamada IP interna.

- **Nos niveis superiores:**

Pasarelas: adoita denominarse pasarelas aos **equipos de interconexión que traballan nos niveis superiores do modelo OSI**. Existen **diferentes tipos** de pasarelas, podemos ter as que se encargan de conectar redes con tecnoloxías diferentes, as que facilitan o control de acceso a unha rede, a que controlan o acceso non autorizados. Segundo a súa función poden tamén ser **servidores, devasas, etc.**

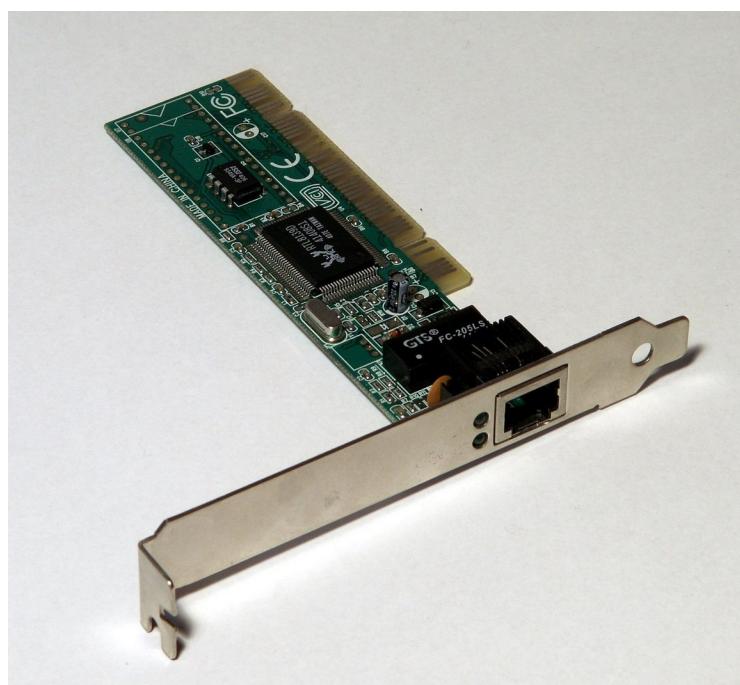
Vai profundar nos elementos más utilizados: tarxeta de rede, switch e router.

5.6.1 Tarxetas de rede e direccionamento MAC

Unha tarxeta de rede ou adaptador de rede **traballa en nivel 1 de OSI ou nivel físico**. Ás tarxetas de rede tamén se lles chama NIC (Network interface card, “Troxeta de interface de rede”)

A función principal dunha tarxeta de rede é a de permitir a conexión do computador á rede. Todas as tarxetas de rede teñen a **dirección MAC** composta de **48 bits ou 12 cifras hexadecimales** e coñéceselle como dirección física e é única no mundo.

Ilustración de tarxeta rede: Obsérvase unha tarxeta de rede, cos seus circuítos e o seu conector externo.



[Sub](#) (Dominio público)

As tarxetas de rede poden conectarse ao equipo utilizando algunha ranura de expansión como o PCI-Express, utilizando o USB ou estar integradas na placa basee.

As tarxetas de rede teñen unha velocidade de transferencia máxima, sendo as actuais de 1000 Megabit /seg = 1Gigabit /seg (Gigabit-Ethernet)

Estas velocidades coinciden coas velocidades dos cables de par trenzado de categoría 5e ou superior.

A instalación e configuración da tarxeta dependerá do sistema operativo, pero en xeral, necesitaremos que teña configurada unha dirección IP, unha máscara de rede e unha porta de ligazón. Estes conceptos estudaranse nos últimos apartados desta unidade.

5.6.2 Conmutadores ou switches

Ilustración switch: Un conmutador 3COM de 24 portos sobre unha mesa.



Phil Campbell (CC BY)

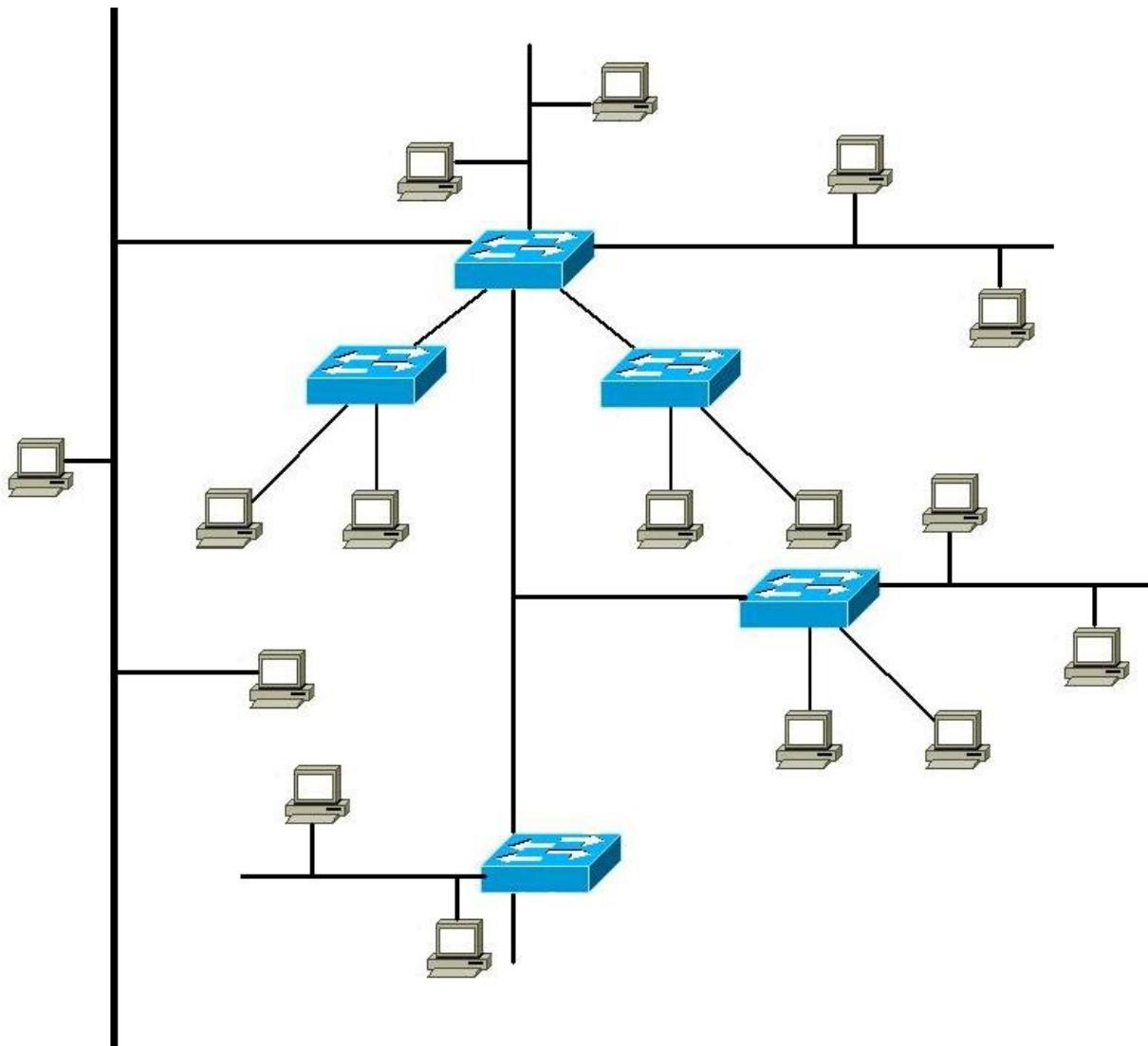
O conmutador ou switch é un elemento de interconexión que traballa en capa 2 ou nivel de ligazón de datos, permite conectar dous ou máis segmentos de rede. O conmutador permítenos conectar diferentes computadores para que poidan conectarse entre si, e que estes teñan acceso a outros segmentos de rede.

O conmutador funciona almacenando as direccións MAC dos computadores que están conectados a el e dos dispositivos que se atopan en cada segmento. Grazas a iso é capaz de conectar un computador con outro de forma eficiente, sen necesidade de enviar a información a toda a rede (ao contrario que o hub, xusto por iso o hub é de nivel 1, mentres que o switch é de nivel 2)

Esta característica é a que fai que o switch sexa o elemento principal de interconexión nas redes de área local con topoloxía en estrela.

Na imaxe, pódese ver un switch central, ao que se conectan outros 2 switch, e a cada un deles dous equipos.

Ilustración switch conectado a outros: Esquema de rede onde se aprecia un comutador que ten conectados outros dous comutadores. Desta forma visualízase a conexión de dous segmentos de rede.



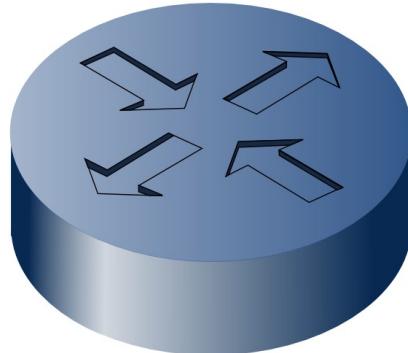
[wierzbadark](#) (Dominio público)

Existen algúns comutadores ou switch que permiten definir redes de área local virtuais ou VLAN. As VLAN son redes lóxicamente independentes dentro de una mesma rede física.

5.6.3 Enrutadores ou routers

O enrutador ou router traballa na capa 3, capa de rede do modelo OSI. É o equipo de interconexión que se encarga de conectar dúas ou máis redes diferentes. Na imaxe vese a icona co que se representa un router.

Ilustración dun router, que se debuxa como un cilindro de pouca altura con catro frechas distribuídas como unha cruz, onde dúas apuntan cara a dentro e dúas cara a fóra.



[Tosaka \(CC BY-SA\)](#)

Os routers dirixen o tráfico de rede, buscando o mellor camiño para chegar ao destino.

Cada interface do router conectarase a unha rede diferente. Necesitan unha **configuración inicial, para gardar a dirección IP de cada interface ou porto**, e a súa máscara de rede. Tamén se poden configurar servidores DNS e se se admiten direccións IP dinámicas (protocolo DHCP).

A maior parte das veces utilizaremos un router para conectarnos a Internet, xa sexa por ADSL ou por cable. Nos domicilios particulares os routers adoitan vir configurados polos provedores de servizos da internet.

Para realizar as súas funcións un router garda información das redes ás que pode acceder, isto faio a través da táboa de encamiñamento, que non é máis que unha táboa onde se garda como se chega dunha rede a outra e que servizos se permiten.

Ilustración dun router inalámbrico con dúas antenas



[OSA \(CC BY-SA\)](#)

Neste apartado é importante **diferenciar un router profesional**, por exemplo da marca Cisco, aos **router que facilitan os operadores telefónicos**.

Un router profesional, se ten 10 tomas RJ45 é para unir 10 redes diferentes.

Os routers que temos nas casas, facilitados polos operadores telefónicos só poden unir dúas redes: A rede externa, pola que estamos conectados a Internet (a toma de teléfono ou fibra óptica) e a rede interna. Para a rede interna, adoita ter conexión inalámbrica e varios portos RJ45; neste tipo de routers, estes portos RJ45 son un switch, pois todos os equipos que se conecten a eles, están na rede interna (unen nodos da mesma rede, pero non de redes distintas). Ademais, se o router é inalámbrico, tamén realiza a función de punto de acceso. Por tanto, estes routers son básicos, pero con todo é un dispositivo de varias capas OSI á vez: a 3 ou capa de rede (router), a 2 ou capa de ligazón (switch) e a 1 ou capa física (punto de acceso).

5.7 Redes sen fíos

As redes sen fíos WLAN (Wifi Lan) basean o seu funcionamento no estándar IEEE 802.11. O funcionamento dunha rede Wi-fi é similar ao funcionamento dunha rede de área local cableada, xa que o estándar define o formato de trama lixeiramente diferente ao das redes cableadas, uso da MAC, a forma de acceder ao medio, etc.

As redes ad-hoc permiten conectarse entre si, pero a velocidades baixas e cunha seguridade mínima. O modo **infraestrutura**, onde se utiliza un punto de acceso para que actúe como canalizador de todas as conexións mellora a velocidad e a seguridade.

É usual que o punto de acceso conéctese a unha rede de área local a través dun cable, coa idea de poder dar acceso a Internet. Ou que, tal como acábase de comentar en anterior apartado o router incorpore un punto de acceso Wifi.

Algunhas vantaxes das redes Wi-fi son:

- Movilidad: pódense conectar dispositivos estáticos e móbiles.
- Escalabilidade: fáciles de ampliar.
- Flexibilidade: pódese conseguir un alto grao de conectividade.
- Menor tempo de instalación: instalando un punto de acceso conséguese conectividade rápida.

As maiores desvantaxes son:

- A seguridade: é difícil conseguir un alto grao de seguridade.
- Interferencias: ao traballar en rangos de frecuencias compartidos por outros dispositivos pódense ter moitas interferencias.

5.7.1 Tipos de redes 802.11. Características

O **estándar IEEE 802.11** define diferentes **versións**:

- **IEEE 802.11a**: opera na banda de 5 Ghz cunha velocidade máxima de 54 Mbps.
- **IEEE 802.11b**: opera na banda de 2,4 Ghz cunha velocidade máxima de 11 Mbps. Non pode interoperar con equipos do estándar 802.11^a por operar noutra banda.
- **IEEE 802.11g**: opera na banda de 2,4 Ghz polo que é compatible coa versión b, pero ofrece as mesmas taxas de transferencia que a versión a, por tanto pode alcanzar unha velocidade máxima de 54 Mbps. Hai que resaltar que aínda que a versión b e a g son compatibles recoméndase usar versión g, xa que se unha dispositivo versión b conéctase a piques de acceso g, baixa a velocidade de toda a área de cobertura, prexudicando aos outros dispositivos.
- **IEEE 802.11n**: opera simultaneamente nas bandas de 5 Ghz e na de 2,4 Ghz, grazas a isto a versión n é compatible coas outras versións. Ademais é útil que traballe na banda de 5 Ghz xa que está menos conxestionada e sofre menos interferencias doutros dispositivos. Ten unha velocidade máxima de 600 Mbps. Do mesmo xeito que a versión g se os dispositivos que se conectan son de versións anteriores, as velocidades e coberturas baixan.
- **IEEE 802.11ac**: opera na banda de 5 Ghz cunha velocidade máxima de 1,3 Gbps, dobrando a velocidade do estándar IEEE 802.11n.

É importante apuntar que as velocidades aquí indicadas son máximas, pero as velocidades reais obtidas son bastante menores, polo que as versións más utilizadas na actualidade son as versións g, n e ac polas súas altas velocidades.

Así mesmo, indicar que a banda de 5Ghz incorpora maior calidade, pois ten menor ruído por non interferir con outras tecnoloxías. Pero ten menor alcance (un 10%) e é máis sensible aos muros dos edificios. Isto corrixiuse nos router ac inalámbricos que alcanzan maiores distancias.

5.7.2 O SSID dunha rede 802.11

O **SSID** (Identificador de conxunto de servizo) é **unha cadea alfanumérica de 32 caracteres de lonxitude, onde se distinguen as maiúsculas das minúsculas, e serve para identificar á rede**. Cando algúen se conecta cun móvil a unha rede Wifi, ten que seleccionar a que rede se conecta, os nomes que aparecen son os SSID das distintas redes WLAN.

É necesario que todos os dispositivos inalámbricos da mesma rede configúrense co mesmo SSID.

Nunha rede tipo infraestrutura o SSID configúrase no punto de acceso (no router se é inalámbrico). Se a rede é tipo ad-hoc o SSID configúrase en cada computador.

Cada punto de acceso que a súa área de cobertura se solape coa área dun punto de acceso próximo deberá utilizar canles diferentes, que no caso do estándar IEEE 802.11b/g, implica utilizar canles cunha diferenza de 5.

Se o punto de acceso non consegue a cobertura necesaria, pódense conectar varios puntos de acceso entre si, preferiblemente con cable. Cada punto de acceso utilizará unha canle diferente, pero o SSID será o mesmo.

5.7.3 Seguridade en 802.11

As redes Wifi son moi vulnerables á interceptación de paquetes e a usuarios non autorizados que aproveiten a conexión, por tanto é conveniente implementar medidas de seguridade que preveñan un uso indebido da rede.

5.7.3.1 Tipos de cifrado

As medidas habituais son encriptar ou codificar a información da rede. Para iso úsanse distintos tipos de cifrado:

- **WEP** (Privacidade equivalente a cableado): é un método débil pois é facilmente descifrable, polo que é recomendable utilizalo.
- **WPA** (Acceso Wi-fi protexido): considérase un método relativamente seguro polo seu cifrado.
- **WPA2**: versión WPA mellorada. Recoméndase utilizar WPA2 co algoritmo AES. Esta é a versión máis segura hoxe día.

5.7.3.2 Ocultar SSID

Unha medida que non proporciona ningún tipo de seguridade, pero dificulta aos clientes o conectarse, é ocultar o SSID. Desde os puntos de acceso difúndese o SSID, se esa función desactivase os computadores deben configurar manualmente o SSID. Isto é facilmente salvable xa que existen ferramentas que detectan o SSID oculto, pero é un primeiro paso.

5.7.3.3 3.3. Deshabilitar WPS

Para a seguridade inarámica, é importante falar de WPS (Wifi Protected Setup, Instalación a Wifi protexida) que trata da posibilidade de conectar dispositivos á rede sen fíos sen utilizar contrasinal. Esta utilidade incluída en moitos router inalámbricos, facilitan a conexión de distintos dispositivos, pero a cambio comprométese a seguridade da conexión, polo que se queremos ter unha rede segura é conveniente deshabilitar WPS no router inalámbrico ou punto de acceso.

5.7.3.4 Filtrado de direccións MAC

O filtrado de direccións MAC é unha boa medida de seguridade adicional e recoméndase utilizala como complemento dalgúns dos métodos de encriptación. Consiste en configurar o punto de acceso ou router de tal forma que teña unha listaxe de direccións MAC dos equipos autorizados a conectarse á rede sen fíos, para que aqueles equipos que non estean na lista non poidan conectarse.

No exemplo dunha casa, trataríase de pescudar as direccións MAC de todos os computadores, móbiles, impresora de rede, Smart-tv e configurar no router inalámbrico a lista de direccións MAC permitidas.

Filtrar por direccións MAC é unha boa medida de seguridade.

5.8 Sistema binario. Conversión decimal - binario.

5.8.1 Sistema binario. O bit e o byte

5.8.1.1 Sistema binario

No apartado seguinte van estudar as direccións lóxicas dunha rede, é dicir as direccións IP. Para entender os seus cálculos é necesario coñecer o binario. De aí, que este libro vai utilizar para aprender binario e a súa conversión de binario a decimal e viceversa.

Na nosa linguaxe utilizamos cifras e letras. Nos números utilizamos o sistema decimal, chamado así porque utiliza 10 cifras distintas: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

O sistema binario utiliza dúas cifras distintas: 0. 1. Un número binario pode ser 101110 pero non 101120 porque o díxito 2 non é admitido.

Os computadores só utilizan 0 e 1, polo que utilizan o sistema binario.

Notación: Como o número 101110 existe tanto en binario como en decimal, faise necesario cando estamos utilizando distintos sistemas utilizar unha notación, de forma que anotaremos cun subíndice o sistema que estamos a utilizar. Para binario utilizamos 101110_2 e se fose decimal 10111010

5.8.1.2 Bit e byte

O bit é un número binario cunha única cifra. De forma que cun bit só pódese escribir 0 ou 1 e anótase por b. Hai $2^1 = 2$ números distintos (do 0 ao 1)

O byte vai ser un conxunto de 8 bits. Para entender cantos números distintos pódense escribir con 1 byte, seguimos o seguinte razonamento:

- Con dous bit pódese escribir 00, 01, 10, 11. Hai $2^2 = 4$ números distintos (do 0 ao 3)
- Con tres bit pódense escribir 000, 001, 010, 011, 100, 101, 110, 111. Hai $2^3 = 8$ números distintos (do 0 ao 7)
- Por tanto, con cada bit dóbranse os números posibles a escribir. Desta forma estamos preparados para definir que é o byte.

O byte é un número binario de 8 cifras e anótase por B. Ao ser 8 cifras, pódense escribir $2^8 = 256$ números distintos (do 0 ao 255)

A importancia do byte débese a que cun byte, pódense representar 256 caracteres alfanuméricos distintos, que son necesarios para escribir calquera texto na nosa linguaxe. Se escribimos no bloc de notas a palabra ola e gardámolo como proba.txt e miramos a

continuación en propiedades canto ocupa o arquivo veremos que ocupa 4 bytes. Isto débese a que para cada letra utilizouse un byte (código ascii estendido).

Debido a esta equivalencia, moitas veces ao byte identifícaselle con carácter. De forma que se di que o arquivo proba.txt ocupa 4 bytes ou 4 caracteres.

Unha pregunta sería porque fan falta 1 byte para unha letra. Por que fan falta 8 bits que serven para representar 256 caracteres distintos para unha letra se só temos preto de 30 letras no abecedario? Hai que ter en conta que na nosa linguaxe utilizamos o abecedario, pero temos distintas representacións para as maiúsculas e as minúsculas, ademais temos vocais acentuadas e non acentuadas, tamén temos signos de puntuación e paréntese; e mesmo escribimos díxitos numéricos nos nosos textos e caracteres invisibles, chamados de control como o tabulador e intro.

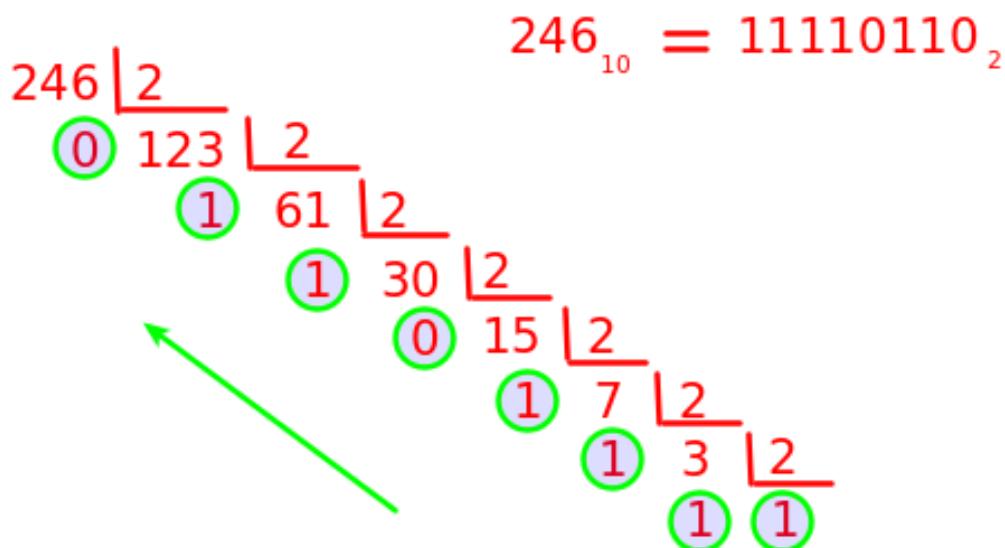
Con vistos ao cálculo de direccións IP nas redes que vemos é moi importante lembrar a idea de potencia vista aquí:

- Con 1 byte ou 8 bits, pódense representar $2^8=256$ números distintos, do 0 ao 255 (do 00000000 ao 11111111)
- Con 16 bits, pódense representar $2^{16}=65536$ números distintos, do 0 ao 65535 (do 0000000000000000 ao 1111111111111111)

5.8.1.3 Conversión decimal a binario

Para converter un número decimal a binario, realizanse divisións enteiras por 2, utilizando o cociente enteiro para dividir de novo por 2, ata que o cociente sexa 0 ou 1. Para obter o número binario, coler como cifra máis significativa o último cociente, e despois todos os restos, empezando desde os últimos.

Ilustración para pasar de decimal a binario



Miguel Ángel García Lara (CC BY-NC-SA)

5.8.1.4 Conversión binario a decimal

Cada bit multiplícase por unha potencia de 2, comezando desde o bit menos significativo (pola dereita)

Exemplo: Converter 11110110_2 a decimal

$$\begin{aligned}11110110 &= 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 = \\&= 0 \cdot 1 + 1 \cdot 2 + 1 \cdot 4 + 0 \cdot 8 + 1 \cdot 16 + 1 \cdot 32 + 1 \cdot 64 + 1 \cdot 128 = \\&= 2 + 4 + 16 + 32 + 64 + 128 = 246\end{aligned}$$

Obtense $11110110_2 = 246_{10}$

O anterior proceso, poderíase resumir en sumar a potencia de 2 correspondente cando o bit é 1, e non sumar nada cando o bit é 0.

Aquí reflíctese unha táboa con 4 exemplos de binario a decimal, utilizando este esquema.

Binario	$2^7 = 128$	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	Suma	Decimal
00000000	0	0	0	0	0	0	0	0	$0+0+0+0+0+0+0+0=0$	0
10101100	1	0	1	0	1	1	0	0	$128+32+8+4$	172
00111110	0	0	1	1	1	1	1	0	$32+16+8+4+2$	62
11111111	1	1	1	1	1	1	1	1	$128+64+32+16+8+4+2+1$	255

5.8.1.5 Múltiplos do byte

Normalmente cando se fala de que un arquivo ocupa 5 megas, esa información é incompleta, pois ocupará 5 megabytes ou 5 megabits. (Mega só significa un millón, 1.000.000). Os sistemas operativos danno a información dos arquivos en bytes, con todo noutros ámbitos a información adoita ser en bits.

Os operadores telefónicos ao contratar unha conexión a Internet, ofrécenos unha velocidade de 100 megas /seg, pero iso segue sendo incorrecto, e o que ofrecen realmente é 100 Megabits / seg (que é 8 veces inferior á velocidade de 100 Megabytes / seg). Todas as velocidades vistas nesta unidade de traballo 8, son en bi

Neste módulo seguiuse sempre o convenio de que cando se fala de bits anótase por b e cando se fala de bytes anótase por B.

Inclúese a táboa de múltiplos KB, MB, GB, TB

Nombre	Notación	Equivalencia
Bit	b	
Byte	B	8 b
Kilobyte	KB	$1000 \text{ B} = 10^3 \text{ B}$
Megabyte	MB	$1000 \text{ KB} = 10^3 \text{ KB} = 10^6 \text{ B}$
Gigabyte	GB	$1000 \text{ MB} = 10^3 \text{ MB} = 10^9 \text{ B}$
Terabyte	TB	$1000 \text{ GB} = 10^3 \text{ GB} = 10^{12} \text{ B}$
Petabyte	PB	$1000 \text{ TB} = 10^3 \text{ TB} = 10^{15} \text{ B}$
Exabyte	EB	$1000 \text{ PB} = 10^3 \text{ PB} = 10^{18} \text{ B}$

5.8.2 Diferenza entre Kilobyte e Kibibyte

Desde que comezou a informática considerouse 1 Kilobyte = 1024 bytes = 2^{10} B

Con todo, quilo significa 1000 e nunca debe ser 1024. Isto xerou que se normalizaron 2 notacións con nomes distintos (estándar IEC 80000-13 do ano 2008)

- Utilizando múltiplos de 1000, fálase de Kilobyte (KB), Megabyte (MB), Gigabyte (GB), Terabyte (TB).
- Utilizando múltiplos de 1024, fálase de Kibibyte (KiB), Mebibyte (MiB), Gibibyte (GiB), Tebibyte (TiB); onde Kibibyte é a contracción de Kilobyte binario.

Este tema xera moita controversia na informática, pois son más de 50 anos onde 1 KB = 1024 B.

Mesmo, Ubuntu e Windows utilizan distintas notacións.

Cando se instalou Windows e Linux en máquinas virtuais cun disco duro de 1 TB, ambos os sistemas operativos recoñecen discos de distintos tamaños. Ubuntu recoñece un disco duro de 1000 GB (utilizando múltiplos de 1000), mentres que Windows recoñece un disco duro de 939 GB (utilizando múltiplos de 1024).

5.9 direccionamento lóxico. Clases de redes e división en subredes

5.9.1 Direccións IP Versión 4. IPv4

En anteriores apartados estudouse o direccionamento físico coas direccións MAC. Neste libro vai estudar o direccionamento lóxico, ou o que é o mesmo as direccións IP das redes.

Todos os equipos que estean na mesma rede, teñen unha dirección IP única pero coa mesma dirección de rede.

O direccionamento IP é a parte encargada de asignar de forma correcta a cada equipo unha dirección IP, de forma que os equipos poidan comunicarse correctamente entre si.

O estudo vai concretar na versión IPv4.

Unha dirección IP ten 32 bits, como cada 8 bits forman 1 byte, unha dirección IP ten 4 bytes.

Como sería moi incómodo dar unha dirección IP cos seus 32 bits (32 cifras binarias) substitúese cada 8 bits polo seu valor decimal, separándose con puntos.

Exemplo

A dirección IP: 11010001 11011000 00110111 00000011 escríbese 209.216.55.3

Todos os equipos que están na mesma rede, teñen a mesma dirección de rede, chamado identificador de rede (netid). Despois cada equipo, ten un número que lle identifica de forma única dentro da rede, chamado identificador de equipo ou host (hostid).

A dirección IP dun equipo ten ambas as partes, por exemplo na IP anterior:

11010001 11011000 00110111 00000011

Netid - identificador rede

Hostid - identificador equipo (host)

Todos os equipos desta rede comezan por 209.216.55.X onde X vai de 0 a 255, aínda que non son válidos nin o 0 nin o 255 como imos ver agora mesmo.

Esta IP ao ser de clase C (entenderase por que en seguintes apartados) ten 24 bits para a dirección de rede e 8 bits para dirección de equipo; pero non é así sempre. Depende das clases de redes utilizanse más ou menos bits para a dirección de rede.

5.9.2 Direccións específicas. Regras e convenios

Existen unhas regras e convenios en canto a determinadas direccións IP que hai que coñecer:

- A dirección 0.0.0.0 identifica ao host actual, polo que non se pode utilizar para ningunha rede.
- A dirección co campo identificador de equipo todo a ceros utilízase para indicar a dirección de rede, e por tanto non se pode utilizar para ningún equipo.
- Coñécese por broadcast ou multidifusión ou multicast á posibilidade de enviar unha mensaxe a todos os equipos da mesma rede. Para este obxectivo resérvanse algunas direccións, de forma que ningún equipo pode ter esa rede.

- A dirección 255.255.255.255 é o broadcast de todas as redes, de forma que se se envía algo a esa dirección, envíase ese datagrama a todos os equipos da rede.
- A dirección co campo identificador de equipo todo a uns utilízase como a dirección broadcast da rede indicada, e por tanto non se pode utilizar para ningún equipo.
- Todas as redes teñen unha máscara de rede, para calcular a máscara pónense todos os bits da dirección de rede a 1, e todos os bits do host a 0. O obxectivo da máscara é marcar os límites da rede, de forma que todos os equipos da mesma rede teñen a mesma máscara.
- A dirección 127.0.0.1 utilízase para loopback. Cando se envía unha mensaxe a esta IP, devólvense á dirección de orixe todas as mensaxes sen tentar envialos a ningunha parte. Trátase de probar a conectividade local.

Como consecuencia das regras 2 e 3 sempre hai dúas direccións que non se poden asignar a ningún equipo, que son o primeiro (por ser a dirección de rede) e o último (por ser o broadcast da rede)

5.9.3 Porta de ligazón

Cando configuremos as IP nos computadores, haberá que configurar cal é a porta de ligazón. A porta de ligazón é unha IP da nosa rede, e é o equipo polo que saímos ao exterior (co que nos comunicamos con outras redes). Habitualmente é a dirección IP do router co que nos conectamos a Internet.

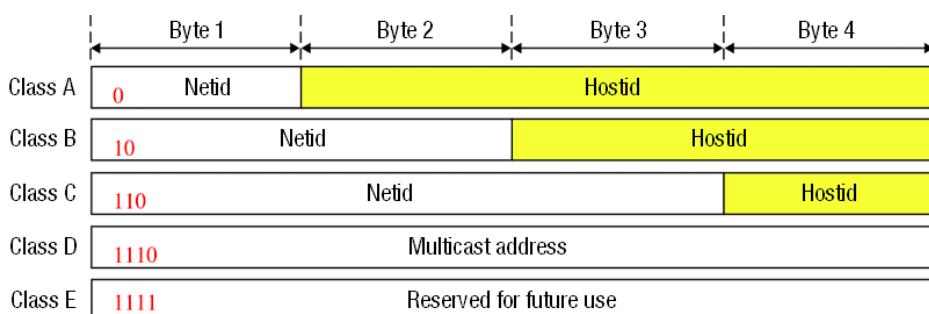
5.9.4 División de redes en clases

Hai 5 clases principais de redes: A, B, C, D, E:

- As clases normais son A, B, C.
- D son redes multicast (redes multidifusión)
- E son direccións reservadas

A distinción das clases vai vir dadas por cuntos bits utilízanse para o número de rede e os valores dos primeiros bits. Na seguinte imaxe móstrase esa información para cada clase.

Ilustración que mostra as clases de redes



Imaxe de materiais orixinais de FP a distancia

Fixarse na figura, que na clase A, utilizanse 8 bits (1 byte) para dirección de rede e 24 bits (3 bytes) para identificador de equipo.

En clase B, utilizanse 16 bits (2 bytes) para dirección de rede, e 16 bits (2 bytes) para dirección de host ou equipo.

En clase C, utilizarse 24 bits (3 bytes) para dirección de rede, e 8 bits (1 byte) para dirección de host ou equipo.

O obxectivo é poder ter redes máis grandes e redes máis pequenas, a máis bits para equipo, pódese ter unha rede máis grande.

5.9.5 Clase A

Dirección de rede

Utilízanse 8 bits de rede, co primeiro bit a 0.

Se nos fixamos no primeiro byte, leste pode ir de 00000000 a 01111111 que en decimal vai de 0 a 127. Pódese ver doutra forma, e dos 8 bits, o primeiro sempre é 0, polo que as posibles redes veñen dadas por 7 bits: $2^7 = 128$

Pero as redes 0 e 127 non se poden utilizar, pois a rede 0 representa a todas as redes, lembrar que o propio equipo recoñécese pola dirección 0. E a rede 127 representa o loopback.

Por tanto só hai **126 redes posibles de clase A ..**

Dirección de equipo ou host

A dirección de equipo fórmala 24 bits, 224 por tanto a rede pode ter aproximadamente 16 millóns de equipos.

Observación: Só hai 126 posibles redes de clase A, pero con moitísimos equipos.

Ejemplo de clase A	
Dirección de red	126.0.0.0
Primer equipo	126.0.0.1
Último equipo	126.255.255.254
Broadcast red	126.255.255.255
Máscara de red	255.0.0.0

5.9.6 Clase B

Dirección de rede

Utilízanse 16 bits de rede, cos 2 primeiros bit a 10.

Se nos fixamos só en primeiro byte, este pode ir desde 10000000 a 10111111 que en decimal vai de 128 a 191. Aquí hai que ter en conta, que estamos a falar só do primeiro byte. Pero que o segundo byte, tamén é dirección de rede.

Cantas redes pode haber? Das 16 cifras para a rede, as 2 primeiras son obligatorias (10), por tanto $2^{14}=16384$ redes

Dirección de equipo ou host

A dirección de equipo fórmala 16 bits, $2^{16} = 65536$, pero en toda rede, non se pode utilizar a primeira nin a última. A primeira, porque representa a dirección de rede, e a última porque é o broadcast da rede. De aí, que as redes de clase B poden ter 65534 equipos ou hosts.

Ejemplo de clase B	
Dirección de red	150.85.0.0
Primer equipo	150.85.0.1
Último equipo	150.85.255.254
Broadcast red	150.85.255.255
Máscara de red	255.255.0.0

5.9.7 Clase C

Dirección de rede

Utilízanse 24 bits de rede cos 3 primeiros bit a 110.

Se nos fixamos só en primeiro byte, este pode ir desde 11000000 a 11011111 que en decimal vai de 192 a 223. Pero a rede 192 está reservada para redes privadas.

Cantas redes pode haber? Das 24 cifras para a rede, as 3 primeiras son obligatorias (110), por tanto, 2^{21} , aproximadamente 2 millóns de redes.

Dirección de equipo ou host

A dirección de equipo fórmala 8 bits, $2^8 = 256$, por tanto a rede pode ter 256 equipos, pero como non se poden utilizar nin a primeira nin a última, as redes de clase C poden ter 254 hosts.

Ejemplo de clase C	
Dirección de red	196.220.53.0
Primer equipo	196.220.53.1
Último equipo	196.220.53.254
Broadcast red	196.220.53.255
Máscara de red	255.255.255.0

5.9.8 Clases D e E

Non se utilizan para a configuración xeral das redes

Clase D son as redes que comezan por 1110 polo que van desde a 224 a 239 e que se utilizan para multidifusión.

Clase E comezan por 1111 polo que van desde a 240 á 254 e que están reservadas para uso futuro (a 255 non se pode utilizar por ser o broadcast xeral de todas as redes)

5.9.9 Redes privadas

Algúns direccións IP resérvanse para redes privadas, o que significa que esas IP non se poden asignar a ningún computador na internet.

Táboa de direccións privadas

Clase	Rango	Número de redes
A	10.x.x.x	1
B	172.16.x.x a 172.31.x.x	16
C	De 192.168.x.x a 192.168.255.x	256

As redes privadas utilízanse para a intranet. Para entendelo, como mellor explícase é coa estrutura dos domicilios particulares. Neles, tense o router facilitado polo operador telefónico, ese router une 2 redes:

- A dirección IP pública ou externa, é a que está conectada a Internet, e é única na internet.
- A IP privada ou interna, é a que está na rede do domicilio, co resto de aparellos (móviles, computadores, impresora, Smart-tv), a IP de cada aparello é distinta. É esta IP privada, onde se utilizan estas redes privadas.

De feito, a privada de moitos routers, é a mesma (moi habitual a 192.168.0.1), iso non crea ningún problema, pois non están na mesma rede. Cada domicilio vese desde fóra co seu IP externo, que esas se son únicas na internet.

Para pescudar nosa IP pública ou externa do router, abrir na navegador web a dirección <http://cualesmiip.es/>

5.9.10 División de redes en subredes

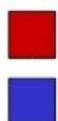
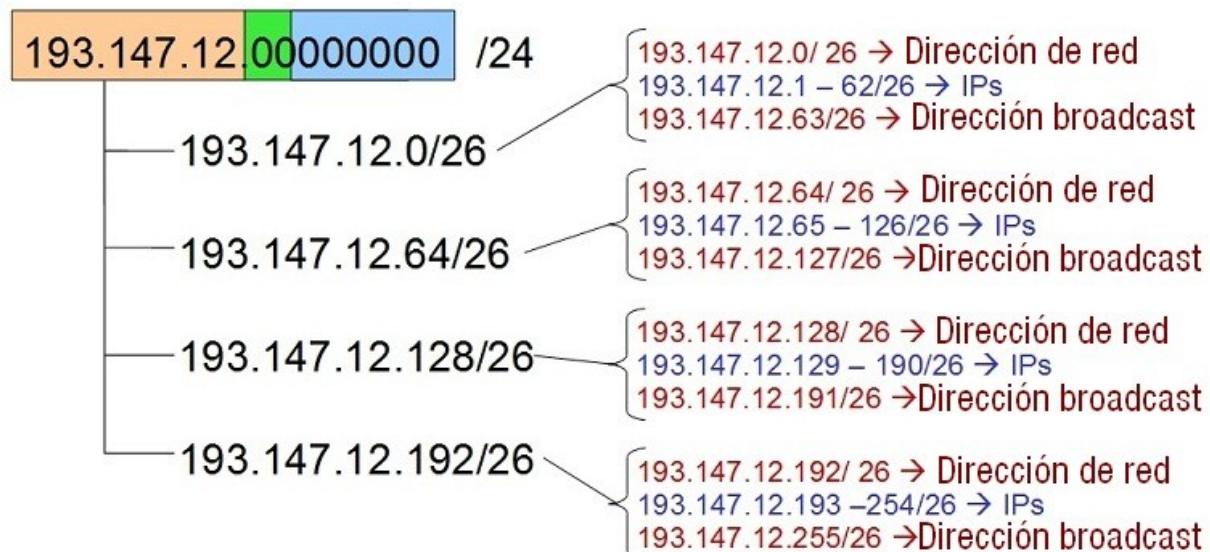
Á hora de deseñar a rede dunha empresa uno dos aspectos que hai que ter en conta é optimizar o uso das redes.

En principio se todos os equipos están na mesma rede, terán visibilidade entre eles. Se non queremos que teñan visibilidade as distintas aulas, necesitaremos que estean en subredes distintas.

O direccionamento IP dános a posibilidade de crear subredes, onde cada unha delas terá a súa dirección de subred, a súa broadcast de subred e un rango de IP permitidas.

Na seguinte imaxe móstrase unha rede de clase C, (por empezar por 193), onde se ha subdividido en 4 subredes. Como unha rede de clase C, ten 256 posibles equipos (realmente 254), ao dividila en 4 subredes, téñense 4 subredes de 64 equipos (realmente 62, ao non poder utilizar a dirección de subred e a dirección de broadcast).

Ilustración que mostra a división de redes en subredes



- Direcciones IP que NO se pueden asignar a equipos**
- Direcciones IP que se pueden asignar a equipos**

Imaxe obtida de materiais orixinais de FP a Distancia

No exemplo da figura, ao haber 4 subredes, 2 bits de identificador de equipo da clase C pasan a ser dirección de subred, de forma que o identificador de subred son 26 bits e o identificador de equipo son 6 bits.

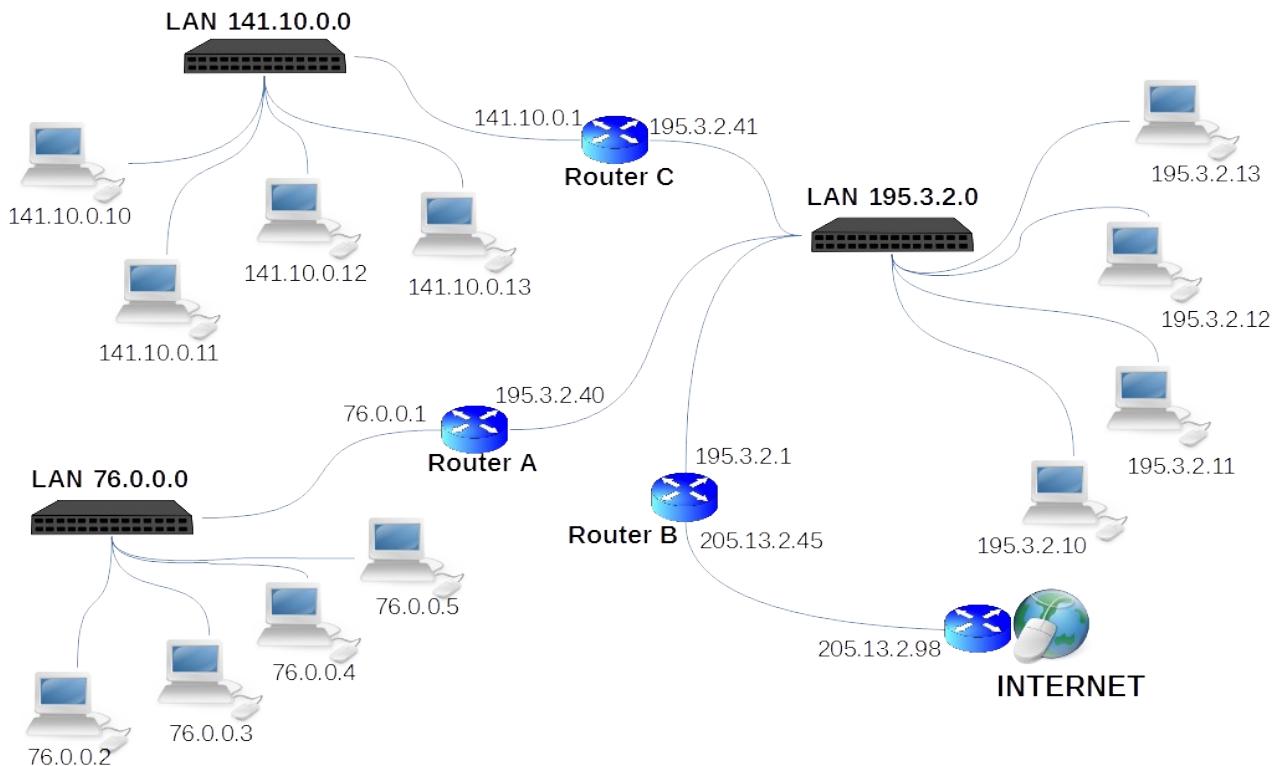
Ao dividir a rede en subredes, calcúlase a máscara, dirección de subred e broadcast da subred coas mesmas normas que nas redes.

Para aclarar todos estes termos, inclúese a continuación dous exercicios de división en subredes.

5.10 Configuración de routers

5.10.1 Táboas de encamiñamento

A mellor forma de comprender o contido das táboas de enrutamento é ver un exemplo concreto dunha serie de redes conectadas por routers e analizar cales serían as súas táboas de enrutamento. Se temos a rede da seguinte figura:



A táboa de enrutamento do router A sería:

Rede destino	Máscara	Seguinte	Métrica
76.0.0.0	255.0.0.0	76.0.0.1	0
195.3.2.0	255.255.255.0	195.3.2.40	0
141.10.0.0	255.255.0.0	195.3.2.41	1
<i>default</i>	*	195.3.2.1	*

Imos destacar os aspectos más salientables da información que atopamos nesta táboa:

- Na columna Rede destino sempre aparecerá a dirección IP dunha rede ou subrede, nunca a dirección IP dun equipo concreto. Hai que ter en conta que os routers encamiñan os paquete entre redes. Desta maneira se consegue que as táboas non crezan demasiado, tendo en conta que as máquinas dunha mesma rede están todas no mesmo punto no nivel de rede. Polo tanto, a misión dos routers é facer chegar o paquete á rede que lle corresponden pero non se preocupan de facer chegar o paquete ao equipo concreto da rede; diso encárganse os switchs.
- Na columna Máscara figurará a máscara da rede ou subrede de destino. Podemos ver na táboa do router A que na primeira fila aparece a máscara de clase A, xa que a rede de destino é de clase A. O mesmo pasa nas seguintes filas.
- A columna Seguinte indica a dirección IP do router ao que este router debe reenviar o paquete para que acabe chegando ao seu destino. Polo tanto, hai que ter en conta que:
 - Neste campo sempre aparecerá a dirección IP dun equipo, nunca a dunha rede.
 - O único que nos importa é cal é o seguinte router para que o paquete poida chegar correctamente ao seu destino, non a ruta completa ata ao final do camiño. Será responsabilidade dos seguintes routers que o paquete siga polo seu camiño correcto ata o destino.
- No caso de que a rede de destino do paquete sexa unha rede á que o router está conectado directamente (neste caso pasa cos destinos 76.0.0.0 e 195.3.2.0), non teremos que reenviar o paquete a outro router senón entregalo directamente á rede pola interface do router correspondente. Entón no campo “Seguinte” en lugar de poñer a dirección IP de outro router, poremos a dirección IP do propio router polo que habería que enviar o paquete para que chegue a esa rede. Isto é unha forma de expresalo a nivel conceptual, xa que en función do sistema operativo do router as interfaces de identifican de forma diferente.
- Por último, a columna de Métrica (que no caso dos routers Cisco se engade tamén a outro campo chamado "distancia administrativa") está indicando neste exemplo o número estimado de saltos (é dicir, número de routers que terá que atravesar) o paquete para chegar a destino se se envía por ese camiño. Este dato será útil canto haxa distintas rutas para poder chegar ao mesmo destino, xa que escolleremos sempre a ruta que presente un menor número de saltos. Na práctica, non se utiliza exactamente o número de saltos senón que a métrica é un valor que indica o peso ou custe que ten unha ruta. Habitualmente o equipo seleccionará, en caso de poder escoller entre varias rutas posibles, aquela que teña un menor valor nestes campos, que virán determinados polo número de saltos e outros factores como capacidade dos enlaces, saturación de tráfico na rede, etc.
- A última entrada da táboa, con destino default, indica o router ao que se enviarán os paquetes que teñan un destino que non pertenza a ningunha das redes de

destino que se indican nas filas anteriores da táboa. Este router é o que se denomina porta de enlace predeterminada, xa que é a saída predeterminada para os paquetes que cheguen a este router e non se teña unha saída especificada.

Unha vez entendido o significado dos distintos campos, podemos deducir como sería a táboa de enrutamento do router B:

Rede destino	Máscara	Seguinte	Métrica
195.3.2.0	255.255.255.0	195.3.2.1	0
205.13.2.0	255.255.255.0	205.13.2.45	0
141.10.0.0	255.255.0.0	195.3.2.41	1
76.0.0.0	255.0.0.0	195.3.2.40	1
<i>default</i>	*	205.13.2.98	*

Podemos destacar que o contido desta táboa non ten nada que ver coa do router A. Aínda que se trate das mesmas redes, a táboa de enrutamento de cada router representa a visión da rede dende a súa perspectiva, e non ten nada que ver coa visión dende a perspectiva de outro router.

Xa para rematar, podemos ver como quedaría a táboa do router C:

Rede destino	Máscara	Seguinte	Métrica
141.10.0.0	255.255.0.0	141.10.0.1	0
195.3.2.0	255.255.255.0	195.3.2.41	0
76.0.0.0	255.0.0.0	195.3.2.40	1
<i>default</i>	*	195.3.2.1	*

5.10.2 Formas de cubrir as táboas de encamiñamento

As filas da táboa de encamiñamento dun router poden ser cubertas de distintas formas.

- **De forma automática polo sistema operativo:**

- Isto é o que ocorre habitualmente con aquelas redes ás que o router está directamente conectado.
- Por exemplo, cando no exemplo do apartado anterior configuramos unha das interfaces do router C coa dirección IP 141.10.0.1 e a máscara 255.255.0.0, o sistema operativo dese router vai concluír que esa interface está conectada á rede 141.10.0.0 (simplemente facendo un AND da dirección IP coa máscara) e engadirá automaticamente na táboa de enrutamento a seguinte fila:

Rede de destino	Máscara	Seguinte	Métrica
141.10.0.0	255.255.0.0	141.10.0.1	0

- **De forma estática:**
 - Este método consiste en que se introduce manualmente a dirección IP do router ao que hai que reenviar os paquetes para un destino determinado.
 - Presenta o inconveniente de que a administración da táboa pode volverse moi laboriosa sobre todo cando o número de destinos posibles é grande, xa que ademais da configuración inicial do router hai que ter en conta que continuamente poden aparecer redes e desaparecer outras, ou cambiar de localización, o que obriga a modificar as táboas de enrutamento dos routers que tiñan información desas redes.
- **De forma dinámica:**
 - Para evitar o traballo que supón a configuración manual das rutas, os router poden utilizar un algoritmo de encamiñamento para descubrir de xeito automático as rutas polas que deben encamiñar os paquetes.
 - De forma moi básica, estes algoritmos se basean en que os routers se comuniquen entre eles información sobre as redes ás que están conectados, e logo ás que están conectados os seus routers veciños, e así sucesivamente.
 - Con esta información os routers construirán e actualizarán de forma automática as súas táboas de encamiñamento.
 - Este algoritmo de encamiñamento debe ser rápido e simple, xa que se non as comunicacíons se verán retardadas. É por iso que haberá que buscar unha solución de compromiso entre a busca da ruta ideal e a simplicidade do algoritmo de encamiñamento.
 - Os algoritmos de encamiñamento dinámicos poden clasificarse entre aqueles que encamiñan dentro dun mesmo Sistema Autónomo (AS) e os que camiñan entre distintos Sistemas Autónomos. Un AS é un conxunto de redes que comparten unha política de encamiñamento propia; habitualmente, todas as redes dun mesmo Provedor de Servizos de Internet (ISP). O primeiro tipo de algoritmos coñécense como IGP (Interior Gateway Protocols) e o segundo como EGP (Exterior Gateway Protocols).
 - Unha característica importante dun algoritmo de encamiñamento é a súa capacidade de que as táboas de encamiñamento dos router converxan para reflectir as rutas axeitadas segundo as redes existentes.
 - Dentro dos protocolos máis utilizados que implementan estes algoritmos, destacan:
 - Dentro dos IGP:
 - **RIP** (Routing Information Protocol - Protocolo de Información de Encamiñamento): Foi dos primeiros protocolos de enrutamento utilizados, aínda que presenta problemas cando a rede crece en tamaño.

Deste protocolo publicouse a versión 1 (que utiliza enrutamento con clase, sen usar máscaras de subrede), a versión 2 (que soporta subredes e mellora os mecanismos de autenticación) e RIPng para IPv6.

- **OSPF** (Open Shortest Path First - Primeiro o Camiño Aberto Máis Curto): Desenvolvido para satisfacer as necesidades de enrutamento dinámico en redes más grandes. A súa versión más recente é OSPFv3.
- **IGRP e EIGRP**: Protocolos de enrutamento interno propios de Cisco.
- **EIGRP** é a versión mellorada de IGRP.
- **IS-IS**: Protocolo de enrutamento deseñado conforme ao modelo OSI, pero menos usado que os anteriores.
- Dentro dos EGP:
 - **BGP** (Border Gateway Protocol): É o protocolo de gateway exterior más utilizado en Internet, que usa o router de fronteira dun Sistema Autónomo para comunicar todas as rutas das súas redes internas aos routers de fronteira dos outros Sistemas Autónomos. A súa versión actual é a 4.

5.10.3 Como se aplican as táboas de encamiñamento

Unha vez construída a táboa de encamiñamento, cando un encamiñador recibe un paquete aplicará o seguinte proceso con cada entrada da táboa de enrutamento comezando pola primeira delas.

Executa a operación AND da dirección IP de destino do paquete coa máscara de rede que figura na entrada da táboa, para poñer a cero todos os bits correspondentes co número de máquina e obter polo tanto a dirección de rede á que pertence ese destino supoñendo esa máscara.

Compara o resultado obtido co destino da entrada:

- Se coincide, entón iso quere dicir que o destino do paquete pertence á rede que se indica na entrada, e polo tanto se pode aplicar esa ruta. Poderá reenviar o paquete segundo o que se indique no campo “Seguinte”, salvo que haxa outra ruta coincidente que teña unha métrica menor.
- Se non coincide, iniciamos de novo o proceso coa seguinte fila.

Se o destino da ruta é “default”, entón aplicarase esta ruta sexa cal sexa o destino do paquete (En realidade esta fila ten como destino “0.0.0.0” con máscara “0.0.0.0” e por iso ao facer a operación AND de calquera IP con esa máscara, o resultado sempre será “0.0.0.0”). Polo tanto, é importante que esta entrada en caso de existir na táboa sexa a última, porque senón as filas que aparecesen despois dela nunca se executarían.

Se chegamos ao final da táboa e non se puido aplicar ningunha das entradas (hai que ter en conta que non sempre ten que haber unha entrada “default”), o router non poderá reenviar o paquete, xa que ese destino é inaccesible para el. Nese caso, aínda que haxa

conectividade física entre o router e a rede, diremos que non hai conectividade IP entre eles.

Vexamos un exemplo deste proceso sobre o router A do exemplo, que ten a seguinte táboa de encamiñamento:

Rede destino	Máscara	Seguinte	Métrica
76.0.0.0	255.0.0.0	76.0.0.1	0
195.3.2.0	255.255.255.0	195.3.2.40	0
141.10.0.0	255.255.0.0	195.3.2.41	1
<i>default</i>	*	195.3.2.1	*

Que pasará se este router recibe un paquete con IP de destino 195.3.2.12?

- O router fará o AND da IP de destino coa máscara da primeira fila (255.0.0.0), e obterá como resultado 195.0.0.0. Esa sería a rede de destino do paquete se a máscara fose a de clase A.
- Comparamos ese resultado co destino da fila (76.0.0.0) e vemos que non coincide, polo que seguimos coa seguinte fila.
- Facemos a operación AND da IP de destino coa máscara desa fila (255.255.255.0) e obtemos como resultado 195.3.2.0, que agora si que coincide co destino da entrada.
- Polo tanto, aplicamos esa ruta, que di que o paquete hai que entregalo directamente pola interface do router que ten a dirección IP 195.3.2.40.

Que pasará se este router recibe un paquete con IP de destino 141.10.0.13?

- Fará o AND da IP de destino coa máscara da primeira fila obtendo como resultado 141.0.0.0, que non coincide co destino da fila, polo que pasamos á seguinte fila.
- Agora o resultado do AND coa máscara será 141.10.0.0, que tampouco coincide co destino.
- Pasamos á terceira fila, na que o resultado do AND coa máscara será 141.10.0.0, que si coincide co destino. Polo tanto o router reenviará o paquete ao router coa dirección IP 195.3.2.41.

Por último, que pasará se este router recibe un paquete con IP de destino 167.98.12.1?

- Fará o AND da IP de destino coa máscara da primeira fila obtendo como resultado 167.0.0.0, que non coincide co destino da fila, polo que pasamos á seguinte fila.
- Agora o resultado do AND coa máscara será 167.98.12.0, que tampouco coincide co destino.
- Pasamos á terceira fila, na que o resultado do AND coa máscara será 167.98.0.0, que tampouco coincide co destino.

- Polo tanto, chegamos á entrada “default” que si coincide con calquera destino e aplicámola, polo que o router reenviará o paquete ao router coa dirección IP 195.3.2.1.

5.10.4 O encamiñamento nos hosts

No que respecta aos nodos finais (hosts), cada equipo da rede tamén dispón dunha pequena táboa de encamiñamento, que especifica que direccións están na mesma rede e cales están accesibles a través de encamiñadores.

Estas táboas de encamiñamento serán construídas automaticamente polo sistema operativo ao configurar a dirección IP, máscara e porta de enlace predeterminada do equipo.

Por exemplo, na figura anterior, o equipo coa 141.10.0.10 tería a seguinte táboa:

Rede destino	Máscara	Seguinte
141.10.0.0	255.255.0.0	141.10.0.10
default	*	141.10.0.1

O que lle indicará que se o destino o paquete está dentro da rede 141.10.0.0 (é dicir, é da forma 14.10.*.*), ese paquete debe ser entregado directamente pola interface que ten a dirección IP 141.10.0.10, e en calquera outro caso o paquete debe ser enviado ao router coa dirección IP 141.10.0.1.

Como se pode ver, a función e a forma de aplicar a táboa de encamiñamento é exactamente igual nos hosts que nos routers; a única diferenza é que as táboas dos hosts serán habitualmente moito más simples.

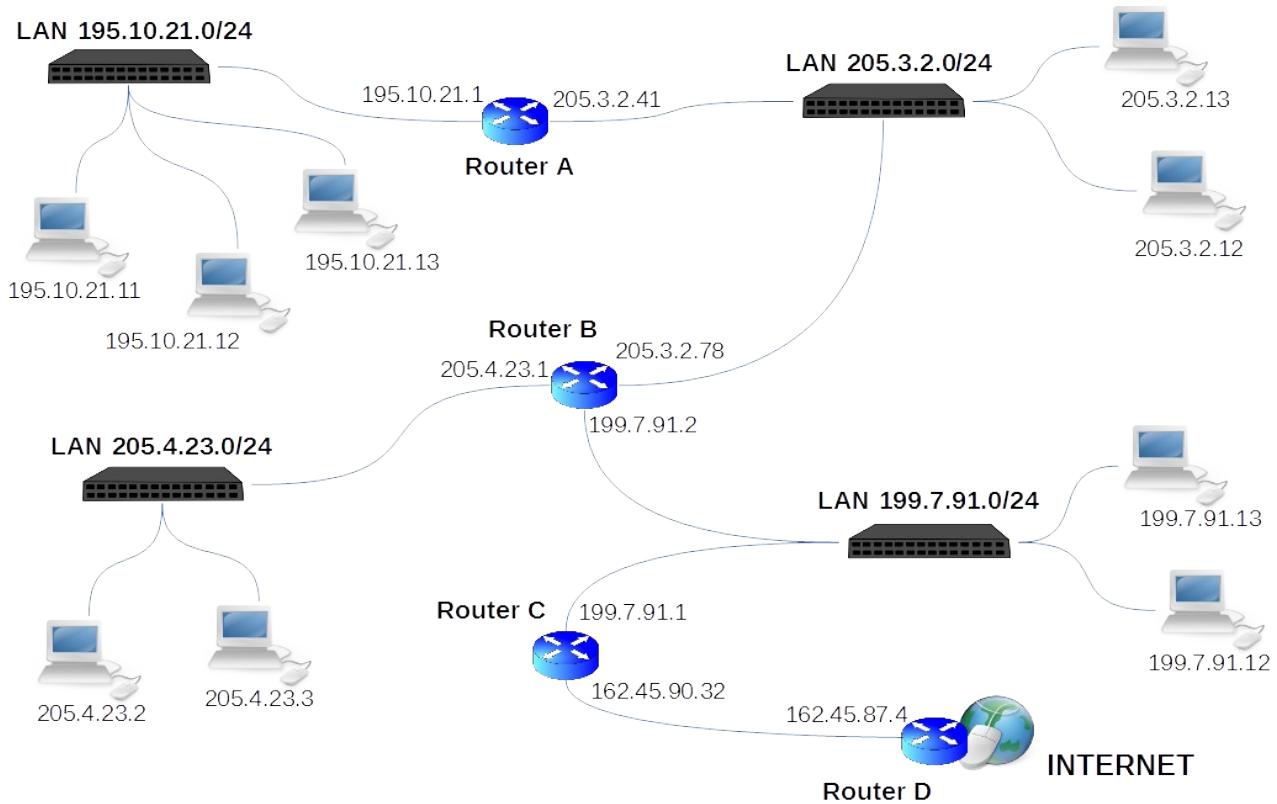
5.11 Efecto das subredes nos routers externos

Cando dividimos unha rede en subredes, só os routers e equipos que están dentro da rede deben coñecer a existencia das subredes e facer uso da máscara axeitada para o funcionamento das mesmas.

Os routers externos, que non pertencen á rede que dividimos, non teñen por que coñecer a existencia das subredes e poden ver a rede como un único ente sen dividir. Isto simplifica as táboas de encamiñamento destes routers, xa que en lugar de ter unha entrada por cada subrede poden ter unha única entrada para toda a rede.

5.11.1 Esquema de exemplo sen subredes

Para clarificar todo isto, imos ver un exemplo concreto. Supoñamos o seguinte esquema, formado por varias redes de clase C:

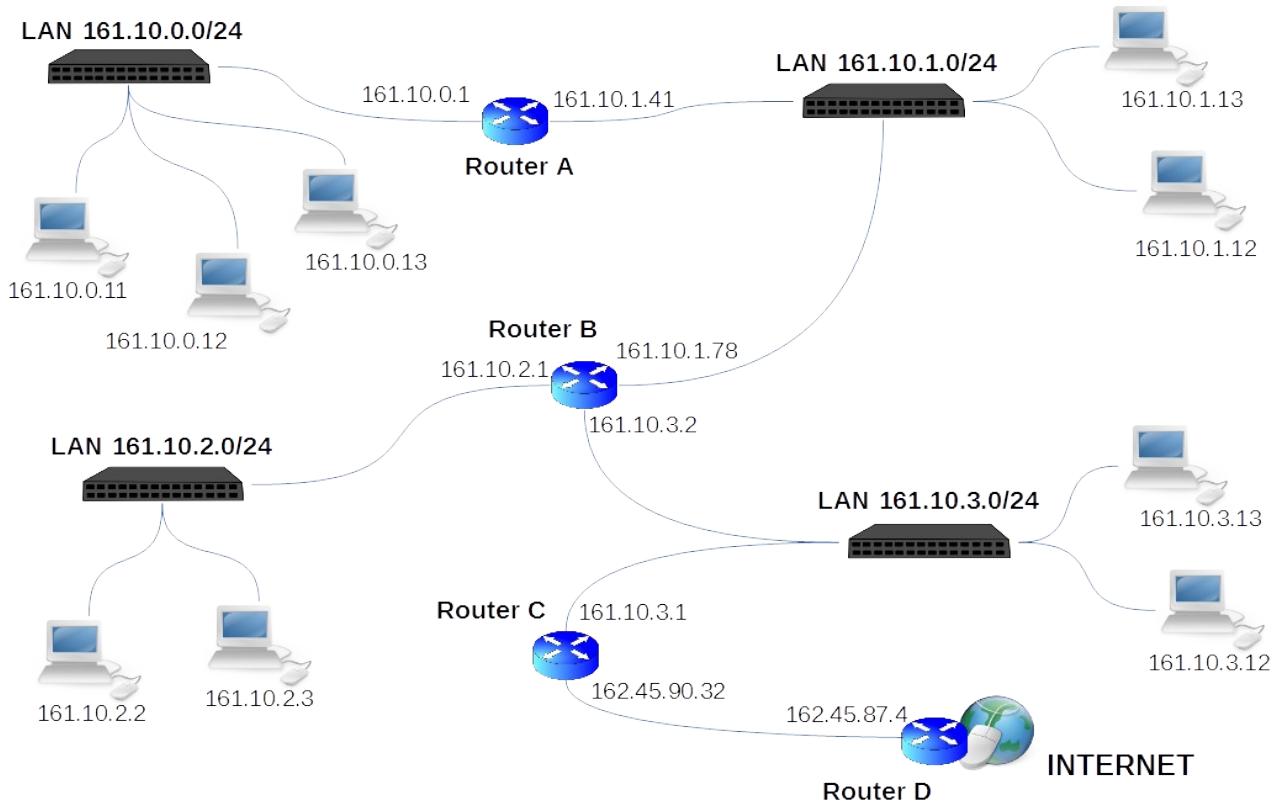


O router D tería que ter na súa táboa de encamiñamento as seguintes entradas:

Rede destino	Máscara	Seguinte	Métrica
...
195.10.21.0	255.255.255.0	162.45.90.32	3
205.3.2.0	255.255.255.0	162.45.90.32	2
205.4.23.0	255.255.255.0	162.45.90.32	2
199.7.91.0	255.255.255.0	162.45.90.32	1
...

5.11.2 Esquema de exemplo con subredes

Sen embargo, se a mesma rede se estrutura como unha rede de clase B con subredes deixando 8 bits para número de subrede, podería quedar do seguinte xeito:



E as entradas da táboa de encamiñamento do router D serían substituídas por unha única entrada á rede 161.10.0.0/16, como a seguinte:

Rede destino	Máscara	Seguinte	Métrica
...
161.10.0.0	255.255.0.0	162.45.90.32	1
...

Desta maneira, este router ve as catro subredes como unha única rede de clase B, e podemos simplificar a súa táboa de encamiñamento.

Debemos ter en conta que cuntas menos entradas teña un router na súa táboa de encamiñamento máis rápido será no proceso de enrutamento, xa que menor será o número de comparacións que terá que facer coa dirección IP de destino dos paquetes para determinar por onde deben ser reenviados.

En cambio, os encamiñadores internos da rede (A, B e C) utilizarán para as direccións da rede a máscara das redes tipo C (255.255.255.0), distinguindo así as catro subredes diferentes (161.10.0.0, 161.10.1.0, 161.10.2.0 e 161.10.3.0).

5.11.3 Seguridade na arquitectura de rede

Se poñemos todos os equipos na mesma rede e prodúcese un ataque de seguridade entón toda a rede verase comprometida. As arquitecturas de seguridade utilizanse para que no caso de que haxa unha intrusión, poidase limitar o acceso do intruso. Existen

varias arquitecturas de rede, desde a más sinxela, que utiliza simplemente un router, ata outras más complexas, baseadas en varios routers, proxys e redes perimetrais (ou zonas neutras).

Antes de entrar en detalle coas arquitecturas de devasas, van describir tres elementos básicos que interveñen nela:

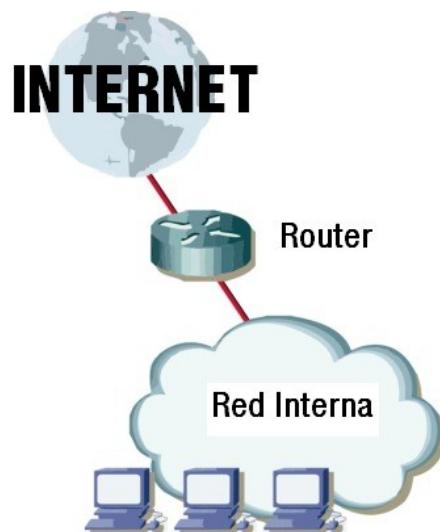
- Router. Equipo que permite ou denega as comunicacións entre dúas ou máis redes. Ao ser o intermediario entre varias redes debe estar especialmente protexido, co encamiñamento, xa que pode ser obxecto dun ataque.
- Rede interna. É a rede interna da empresa e, por tanto, é onde se atopan os equipos e servidores internos. Dependendo do nivel de seguridade que necesite a rede interna pódese dividir en varias redes para permitir ou denegar o tráfico dunha rede a outra.
- Zona neutra (ou rede perimetral). Rede engadida entre dúas redes para proporcionar maior protección a unha delas. Nesta rede adoitan estar situados os servidores da empresa. O seu principal obxectivo é que ante unha posible intrusión nuns dos servidores, íllese a intrusión e non se permita o acceso á rede interna da empresa.

A continuación móstranse varios esquemas, comezando polos más simples.

5.11.3.1 Esquema de rede básico

É a configuración máis simple e consiste no emprego dun router para comunicar a rede interna da empresa con Internet. Como o router é o encargado de comunicar ambas as redes é ideal para permitir ou denegar o tráfico.

Ilustración que mostra arquitectura básica dunha rede utilizando un router



Imaxe obtida de materiais orixinais de FP a Distancia

Esta arquitectura de rede, aínda que é a más sinxela de configurar é a más insegura de todas xa que toda a seguridade reside nun único punto: o router. No caso de que se produza un fallo de seguridade no router o atacante ten acceso a toda a rede interna.

Esta arquitectura é a usual nos domicilios e en pequenas empresas.

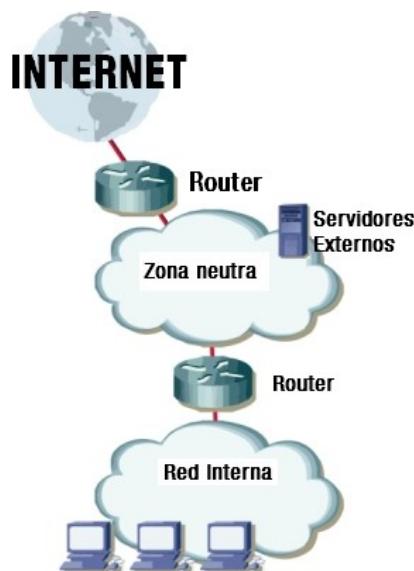
5.11.3.2 Esquema de rede cunha zona neutra

No anterior esquema, se se desexa ter un servidor que ofrece servizos a Internet hai que situalo na rede interna. É perigoso poñer o servidor na rede interna xa que o router permite o tráfico ao servidor e, no caso de que se produza un fallo de seguridade o atacante ten acceso completo á rede interna. Para solucionar este problema engádese unha nova rede á empresa que se denomina zona neutra ou zona desmilitarizada.

Esta arquitectura utiliza dúas routers que permiten crear un perímetro de seguridade (rede perimetral ou zona neutra), na que se poden situar os servidores accesibles desde o exterior, protexendo así á rede local dos atacantes externos.

Na imaxe móstrase un esquema de rede cunha zona neutra e unha rede interna utilizando dúas routers.

Ilustración que mostra esquema de rede cunha zona neutra e unha rede interna utilizando dúas routers.

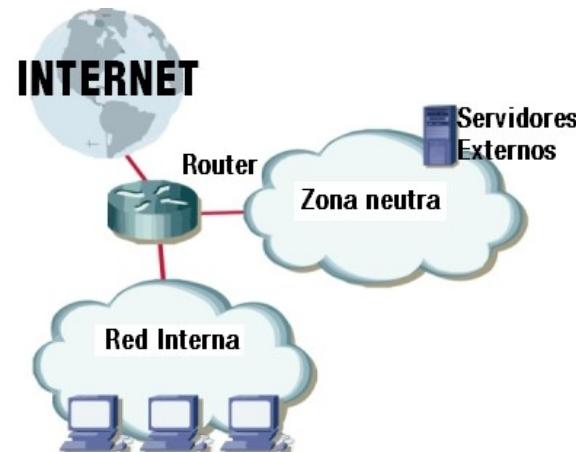


Imaxe obtida de materiais orixinais de FP a Distancia

Neste esquema o router exterior está configurado para permitir o acceso desde Internet aos servidores da zona neutra, especificando os portos utilizados, mentres que o router interior permite unicamente o tráfico saínte da rede interna ao exterior. Desta forma se se produce un fallo de seguridade e accédese aos servidores da zona neutra, o atacante nunca poderá ter acceso á rede interna da empresa.

Pódense realizar outras configuracións con zona neutra. Pódese crear unha zona neutra utilizando un único router con tres interfaces (que unha tres redes, ten que ser un router profesional, non valen os routers dos operadores telefónicos que só unen dúas redes)

Esquema de rede cunha zona neutra e unha rede interna utilizando un único router con tres interfaces.

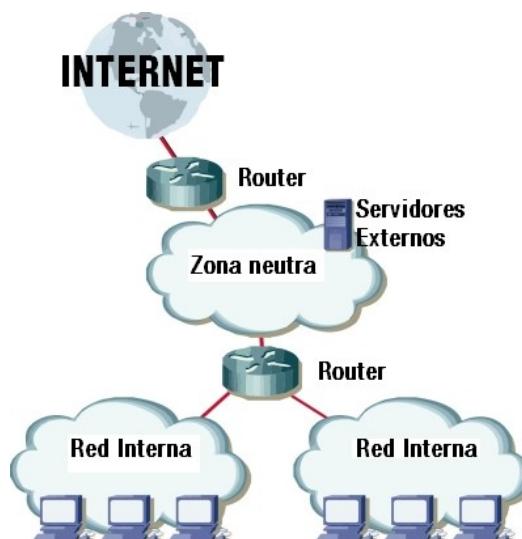


Imaxe obtida de materiais orixinais de FP a Distancia

Aínda que este esquema non é tan fiable como o anterior resulta máis aconsellable que o modelo básico que non ten ningunha zona neutra.

Estes esquemas permiten distintas modificacións. Por exemplo na imaxe móstrase un esquema onde hai 2 routers con zona neutra e varias redes internas. Neste caso increméntase a seguridade entre as propias redes internas da empresa.

Ilustración de rede cunha zona neutra e unha rede interna utilizando dúas routers, un deles con tres interfaces.



Imaxe obtida de materiais orixinais de FP a Distancia

5.12 Administración de redes Windows

5.12.1 Configuración de rede en Microsoft Windows

Administrar unha rede consiste en aplicar unha serie de técnicas que a manteñan sempre operativa, de forma óptima e segura, para xestionar o uso eficiente dos seus recursos e garantir a calidade dos servizos que ofrece.

Grupo de traballo (Workgroups)

Por defecto, os computadores que forman parte do mesmo grupo aparecen xuntos cando se exploran en “Os meus sitios de Rede” ou en “Rede” no explorador de Windows. A administración de cada computador é local e independente. Un computador, exporta ou comparte recursos concretos, e o usuario remoto ten que dispoñer dunha conta e permisos suficientes. Esta é a forma que se vai a traballar nesta unidade. Imos ter 2 equipos, cada un cos seus usuarios e password. Tamén recibe tradicionalmente o nome de rede punto a punto (peer to peer) na que cada usuario, para conectarse a calquera equipo ten que ter unha conta dese equipo.

Imaxinemos, unha empresa con 10 computadores e os seus traballadores, se queremos que un traballador, poidase poñer en calquera posto, teremos que crear unha conta para ese traballador en cada equipo. Esta organización, segundo faise a empresa grande faise complicada.

Dominio

É a forma habitual de traballar nunha empresa grande, hai 1 computador principal con sistema operativo Windows Server, no que se instala un controlador de dominio. Despois, introdúcese ao resto dos equipos nese dominio. As contas de usuarios que se crean no controlador, serven para iniciar sesión en calquera equipo do dominio.

No exemplo anterior, o traballador poderá iniciar sesión en calquera equipo, só con ter unha conta creada no equipo controlador de dominio.

No controlador de dominio centralízase as contas de usuarios, grupos, equipos, directivas de seguridade, recursos compartidos.

Non é necesario que os computadores que forman un dominio atópense fisicamente próximos, poden estar en distintas sedes xeográficas. Para crear un dominio, é necesario que polo menos un dos servidores Windows Server da rede convértase nun DC. Para iso, débese executar un asistente denominado dcpromo.

Os contidos de dominios non forman parte da materia de Sistemas Informáticos, polo que nesta unidade só se vai a traballar en grupo de traballo.

5.12.2 Exercicio configuración Rede. Instalación de 2 máquinas Windows en Rede en grupo de traballo

O primeiro que se vai a realizar é configurar 2 máquinas virtuais Microsoft Windows na mesma rede.

Paso 1. Clonar unha máquina Windows

Clonar con VirtualBox a máquina virtual Windows10.

Ao clonar, ter especial coidado en marcar “Reiniciar MAC”, senón facémolo as 2 tarxetas de rede terían a mesma dirección física, e tal como díxose na unidade 8, toda tarxeta de rede ten unha dirección única no mundo, polo que non poderá funcionar a rede.

Paso 2. Configurar nomes das máquinas e grupo de traballo

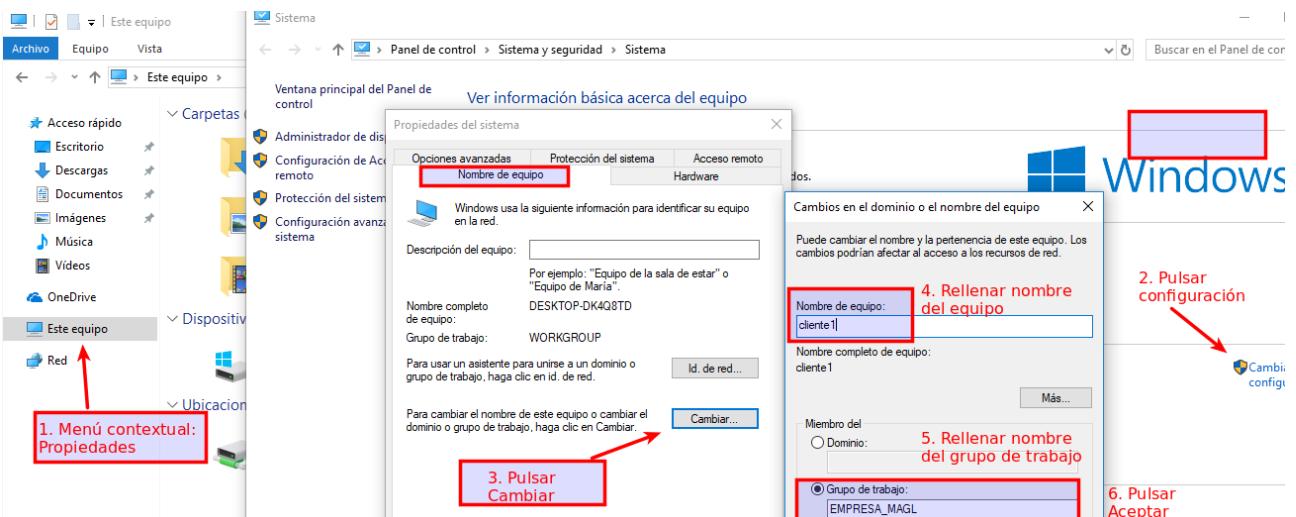
As 2 máquinas van introducir no mesmo grupo de traballo.

Para iso, seguir os pasos seguintes (segundo imaxe):

- Ir ao Menú contextual de Equipo e pulsar Propiedades.
- Pulsar en “Cambiar configuración” e seleccionar Lapela “Nombre de equipo”
- Pulsar o botón “Cambiar”.
- Nesta última xanela que aparece, configúrase Nome de Equipo e Nome do Grupo de Traballo.
- Poñer ás dúas máquinas o nome: cliente1 e cliente2
- Introducir a ambas as máquinas no mesmo grupo de traballo: “Empresa_InicialesApellidoNombreAlumno”

Unha vez recheos os datos, pulsar Aceptar. Ao pulsar Aceptar, hai que reiniciar a máquina para que os cambios teñan efecto.

Ilustración de Configurar nome de equipo e grupo de traballo.



Miguel Angel García Lara (CC BY-NC-SA)

Paso 3. Crear 2 usuarios, un administrador e outro normal en cada máquina.

Crear en cada máquina dous usuarios, un administrador e outro pertencente ao grupo usuario. Utilizar os nomes e password especificados nas táboas:

Usuarios en cliente1

Nombre usuario	Password	Único grupo al que pertenecen
Supervisor	Administradores	empleado1
super1	Empleado	Usuarios

Usuarios en cliente2

Nombre usuario	Password	Único grupo al que pertenecen
Supervisor	Administradores	empleado2
super2	Empleado	Usuarios

Paso 4. Configuración da rede por defecto en VirtualBox

Por defecto, VirtualBox ten configuradas as máquinas en NAT, desta forma saen a Internet, pois a máquina anfitrión realiza ponte coa hóspede. Para comprobalo e entendelo realizanse os pasos seguintes:

- Comprobar que ambas as máquinas teñen Internet. Para iso, executar en terminal: ping www.google.es
- Envíanse paquetes á páxina de google e devólvese o tempo de resposta.
- Comprobar que ambas as máquinas teñen a mesma dirección IP na tarxeta de rede Ethernet. Para iso, executar ipconfig. Con todo, conéctanse a Internet sen problemas estando as dúas máquinas acesas (o que demostra que non están na mesma rede, porque dentro da mesma rede dúas máquinas non poden ter a mesma IP)

Na imaxe seguinte móstrase a execución de ambos os comandos.

Ilustración de Execución ping e ipconfig.

```

C:\ Administrador: Símbolo del sistema
C:\Windows\system32>ping www.google.es

Haciendo ping a www.google.es [216.58.201.163] con 32 bytes de datos:
Respuesta desde 216.58.201.163: bytes=32 tiempo=5ms TTL=127
Respuesta desde 216.58.201.163: bytes=32 tiempo=6ms TTL=127
Respuesta desde 216.58.201.163: bytes=32 tiempo=5ms TTL=127
Respuesta desde 216.58.201.163: bytes=32 tiempo=8ms TTL=127
ping correcto
Tenemos conexión con google

Estadísticas de ping para 216.58.201.163:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 5ms, Máximo = 8ms, Media = 6ms
ping incorrecto
No hay conexión con googleee.es

C:\Windows\system32>ping www.googleee.es
La solicitud de ping no pudo encontrar el host www.googleee.es. Compruebe el nombre y
vuelva a intentarlo.

C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet: Tarjeta de red Ethernet
de la máquina virtual Windows10Siste
Sufijo DNS específico para la conexión. . . : Home
Vínculo: dirección IPv6 local. . . : fe80::5d05:ad0c:2420:f52a%2
Dirección IPv4. . . . . : 10.0.2.15
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 10.0.2.2
IP 10.0.2.15

```

Miguel Angel García Lara (CC BY-NC-SA)

Paso 5. Configuración dos 2 equipos en rede interna en VirtualBox.

Apagar as 2 máquinas e en VirtualBox, en Configuración / Rede cambiar “NAT” a “Rede interna”.

Isto equivale a conectar as 2 máquinas fisicamente no mesmo switch. Desta forma, ambas as máquinas están na mesma rede física, pero falta o direccionamento IP para que se poidan conectar entre elas.

Paso 6. Comprobar que agora non hai conexión a Internet.

Agora as máquinas xa non saen a Internet, nin sequera teñen rede local pois non teñen asignada IP. Ao executar os mesmos comandos que en paso 4 obsérvanse as diferencias seguintes: o ping non responde (os paquetes pérdense) e en ipconfig, vese a conexión de rede desactivada (sen dirección IP)

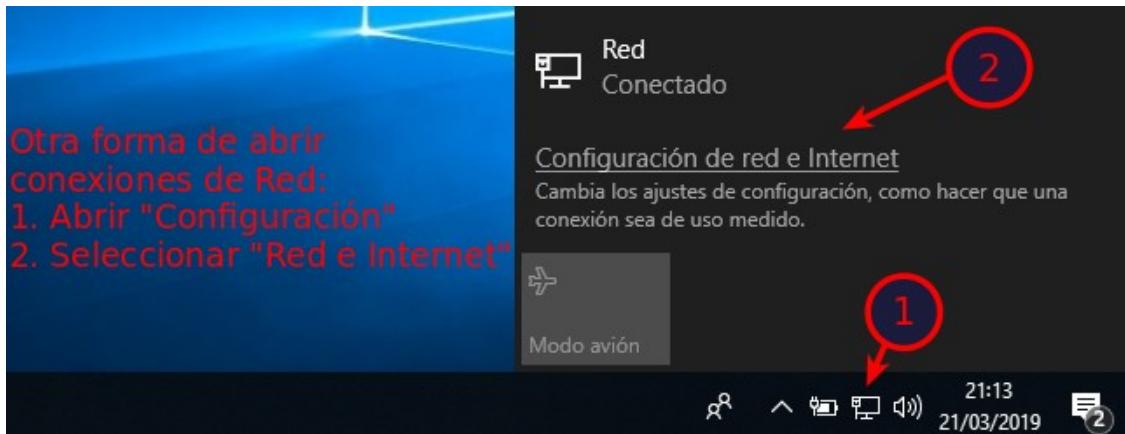
Paso 7. Configurar a rede local, asignando dirección IP estática a ambas as máquinas.

Neste paso configúranse as direccións IP en ambas as máquinas. As direccións para configurar son as da táboa. Para a configuración, seguir as capturas.

Direccións de rede

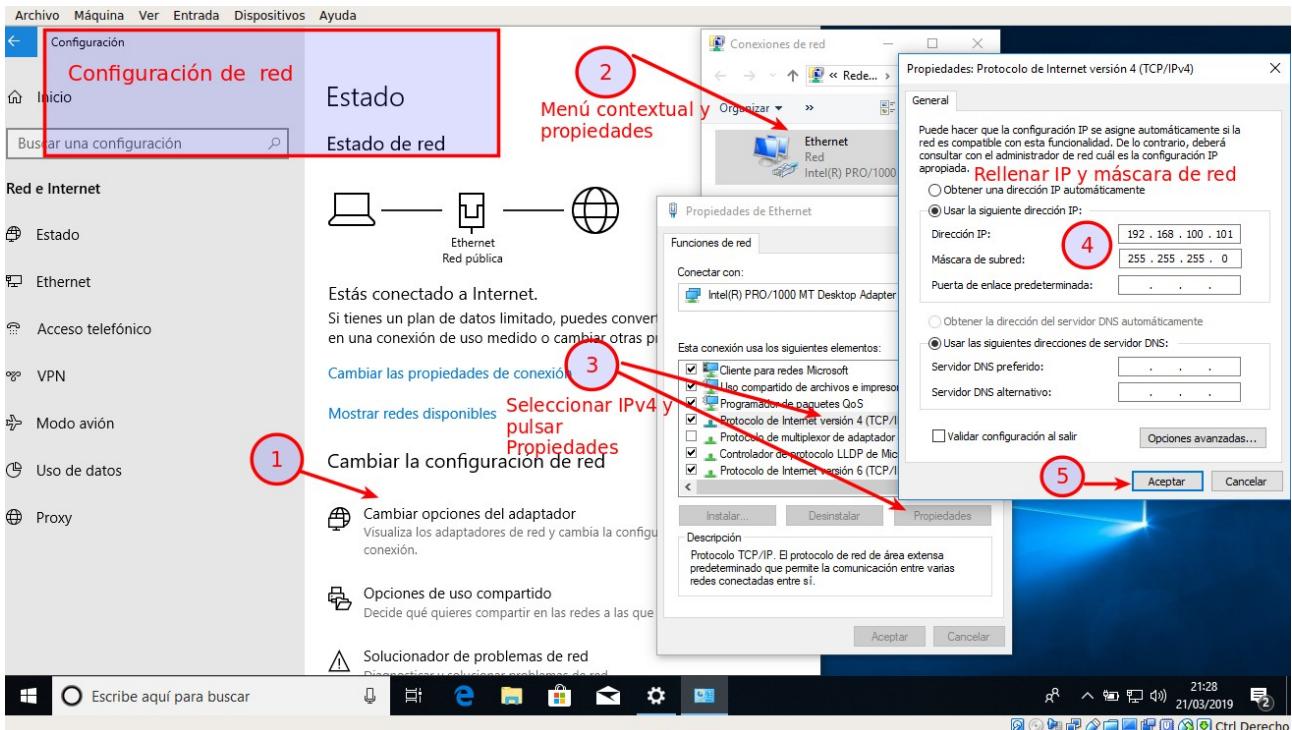
Nombre máquina	IP	Máscara de red
cliente1	192.168.100.101	255.255.255.0
cliente2	192.168.100.102	255.255.255.0

Ilustración de Abrir configuración de rede.



Miguel Angel García Lara (CC BY-NC-SA)

Ilustración de Configurar IP e máscara de rede.



Miguel Angel García Lara (CC BY-NC-SA)

Segundo direccionamiento IP estudiado, estamos a configurar ambas as máquinas na mesma rede con dirección 192.168.100.0/24 (rede de clase C con máscara de 24 bits)

Non configuramos porta de ligazón nin DNS. Imos ter as 2 máquinas na mesma rede local, pero non van saír a Internet. Para saír a Internet, teríamos que ter un router que conecte a nosa rede con Internet. A dirección interna do router sería a porta de ligazón. O

servidor DNS é un equipo da internet que se utiliza para a resolución de nomes (direccións web) en IP, como de momento non saímos a Internet non nos fai falta.

Paso 8. Executar ipconfig para comprobar IP asignadas.

Imos comprobar a conexión á outra máquina con ping.

Para iso, en cliente 1 executamos ping 192.168.100.102 e en cliente 2 executamos ping 192.168.100.101.

Resulta que non responden os ping, pois por defecto, o firewall de Windows non admite ping. Hai que bloquear o firewall nas máquinas ou crear unha regra de exclusión.

Na imaxe, execútase na máquina cliente2 o comando ipconfig, onde se ve o IP ben configurada, pero con todo non responde o ping á máquina cliente1.

Ilustración de Non responde ping polo firewall de Windows.

```
C:\Windows\system32>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::99af:b84d:e817:3c30%2
    Dirección IPv4. . . . . : 192.168.100.102 IP 19.168.100.102
    Máscara de subred . . . . . : 255.255.255.0 configurada en cliente2
    Puerta de enlace predeterminada . . . . . :
C:\Windows\system32>ping 192.168.100.101
Haciendo ping a 192.168.100.101 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.100.102: Host de destino inaccesible.

Estadísticas de ping para 192.168.100.101:
```

ping a máquina cliente1 con IP 192.168.100.101 no responde

Miguel Angel García Lara (CC BY-NC-SA)

Crear regras de exclusión no firewall para permitir ping nas máquinas

Pasos:

En máquina cliente1, abrir “Windows Defender Firewall de Windows con seguridade avanzada:

- Seleccionar “Regras de entrada” e á dereita en “Nova Regra”
- Seleccionar “Personalizada” e pulsar Seguinte.
- Seleccionar “Todos os programas” e pulsar Seguinte.
- Seleccionar “Tipo de protocolo ICMPv4” e pulsar en Configuración de ICMP “Personalizada”

- Pulsar en “Tipos de ICMP específicos” e activar “Petición de eco”. Pulsar en Aceptar e Seguinte varias veces, ata que se solicita o nome da regra. Encher como nome “Permitir ping”

Unha vez engadida a regra na máquina “cliente1”, cliente2 executa ping 192.168.100.101 con resposta satisfactoria.

Ilustración de Máquina cliente1 responde ping a cliente2.

```
C:\Windows\system32>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Vínculo: dirección IPv6 local. . . : fe80::99af:b84d:e817:3c30%2
  Dirección IPv4. . . . . : 192.168.100.102 IP 19.168.100.102
  Máscara de subred . . . . . : 255.255.255.0 configurada en cliente2
  Puerta de enlace predeterminada . . . . . :

C:\Windows\system32>ping 192.168.100.101
Haciendo ping a 192.168.100.101 con 32 bytes de datos:
Respueta desde 192.168.100.101: bytes=32 tiempo<1m TTL=128
Estadísticas de ping para 192.168.100.101:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
```

ping a máquina clientel con
IP 192.168.100.101 responde

Miguel Angel García Lara (CC BY-NC-SA)

Por último, crear a regra na máquina cliente2 e comprobar ping contrario.

5.12.3 Compartir recursos na Rede

Cando falamos de recursos compartidos en rede estamos a tratar de cartafoles, de ficheiros e de dispositivos que se haxan nun equipo, pero que dalgunha maneira, pónense ao dispor de todos aqueles que se conectan a el a través dunha rede, ou só ao dispor dalgúns deles dependendo da forma de compartirlos. E todo iso facéndose extensivo a cada un dos equipos que forman parte da devandita rede.

Para facer que un recurso sexa compartido hai que poñelo accesible a través a rede, e unha vez que esta compartido, os usuarios, cos permisos adecuados, poderán acceder ao seu contido xa sexan aplicacións ou datos, ou utilizalo remotamente se se trata dun dispositivo, tal como unha impresora.

Nunha contorna de rede é preciso definir permisos de acceso e privilexios de uso sobre os recursos que se comparten, para manter certo nivel de seguridade e asegurar que o compartido só poida ser utilizado por quen teña dereito, e baixo as condicións de uso fixadas sobre o recurso, mentres que se bloquea o acceso a usuarios non autorizados.

5.12.3.1 Solapa Compartir

Se pulsamos menú contextual nun cartafol e propiedades, temos as lapelas Compartir e Seguridade. Na unidade 4, vimos a lapela “Seguridade” onde se dixo que representaba a seguridade local no equipo, coñecidos como permisos NTFS.

Neste libro estúdase a lapela “Compartir”, que serve para configurar os permisos cando accedemos a un equipo desde a rede.

Comézase con varias particularidades cando se comparte:

- Pódense compartir cartafoles e impresoras. Non se poden compartir archivos de forma individual. Chámase recurso ao cartafol ou impresora compartida.
- Cando se comparte un recurso, pónselle un nome que pode ser distinto ao nome do cartafol ou impresora.
- Un cartafol compartido adóitase distinguir no Explorador de Windows por unha icona dunha man que sostén un cartafol.
- Cando se comparte un cartafol, concédese un permiso de lectura ao grupo Todos de forma predeterminada. Pódense cambiar os permisos por defecto e agregar ou eliminar a usuarios e grupos.
- Un cartafol compartido, non se pode mover, se se move deixa de ser compartido o recurso.
- Un recurso ten un roteiro UNC, este roteiro está formada por \\NombreEquipo\NombreRecurso
- Este roteiro UNC é unha forma rápida de acceder ao recurso, pois se pode escribir directamente no explorador de Windows ou en Executar.
- Pódese ocultar un recurso, para iso engádese un signo de dólar (\$) ao final do nome do recurso. Desta forma non se ve no explorador de Windows cando se explora a rede, aínda que se se ten acceso a través do seu roteiro UNC \\NombreEquipo\NombreRecurso\$
- Límite de usuarios: Indica o número de usuarios que poden conectarse simultaneamente ao cartafol compartido. Por defecto son 20, que é o máximo permitido en Windows 10.

Tipos de permisos ao compartir

Cando se comparte un recurso, pódese compartir a usuarios ou grupos e existen 3 tipos de permisos:

- Lectura, cambio e control total
 - O permiso de lectura permite:
 - Ver os nomes de archivos e de subcarpetas
 - Percorrer as subcarpetas

- Ver os datos dos arquivos
- Executar arquivos de programa
- O permiso de cambio proporciona todos os permisos de lectura, así como:
 - Agregar arquivos e subcarpetas
 - Cambiar datos en arquivos
 - Eliminar subcarpetas e arquivos
- O permiso de control total proporciona todos os permisos de lectura e de cambio, así como:
 - Cambiar permisos
 - Tomar posesión

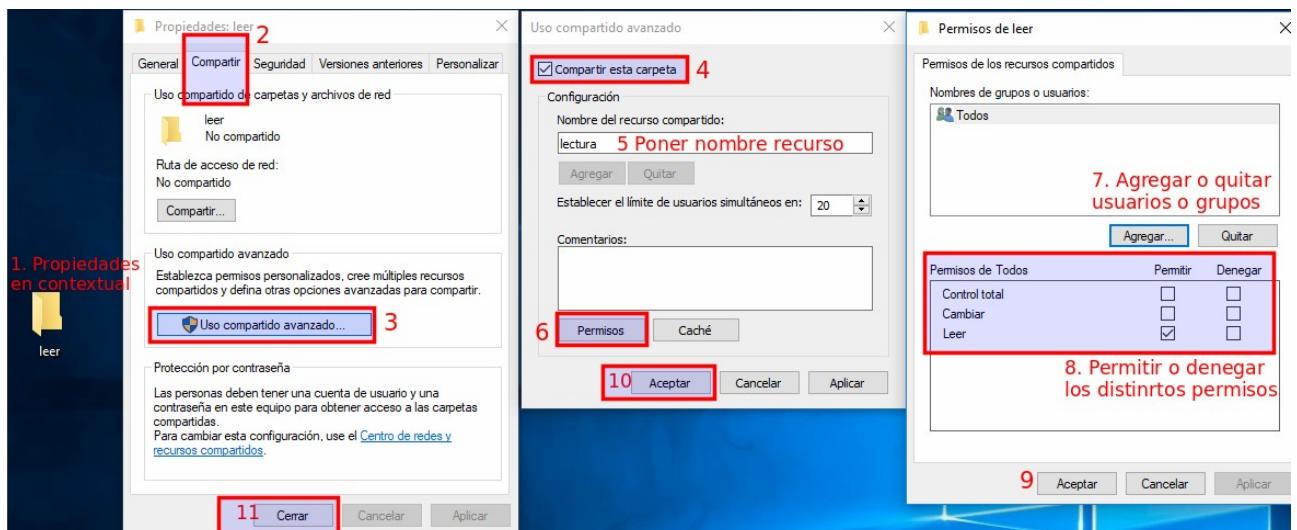
Como compartir un recurso?

A forma más habitual de compartir un recurso é mediante o Explorador de Windows, pulsando en menú contextual en propiedades / Lapela Compartir / Uso compartido avanzado.

A lapela Compartir funciona dunha forma moi similar á lapela Seguridade.

Na imaxe móstrase como se comparte un cartafol chamado “Ler” co nome de recurso “Lectura” e a “Todos” os usuarios co permiso Lectura.

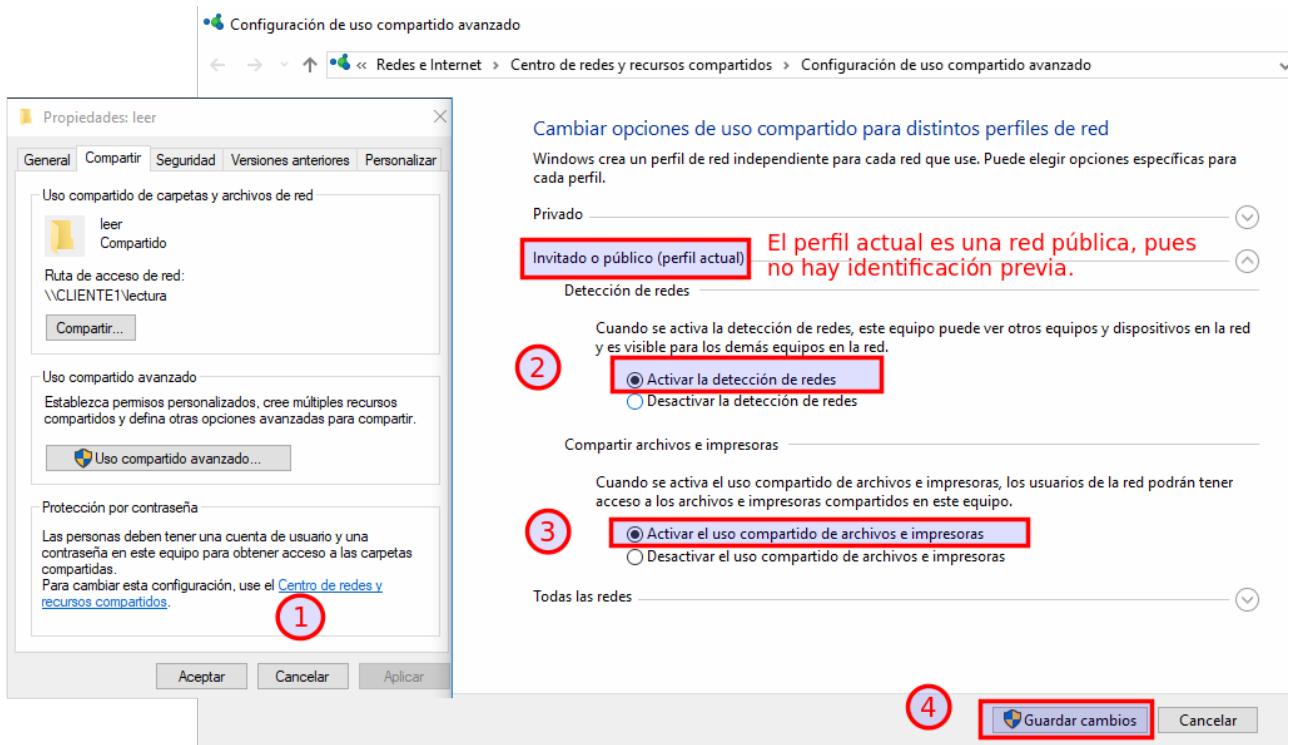
Ilustración de Compartir un cartafol.



Miguel Ángel García Lara (CC BY-NC-SA)

A primeira vez que se comparten recursos, é necesario “Activar detección de redes e uso compartido de archivos”. Se non se activa esta opción, non se poderá acceder aos equipos na rede, aínda que se compartiron recursos.

Ilustración de Activar detección de redes.



Miguel Ángel García Lara (CC BY-NC-SA)

Como acceder aos cartafoles compartidos noutro equipo

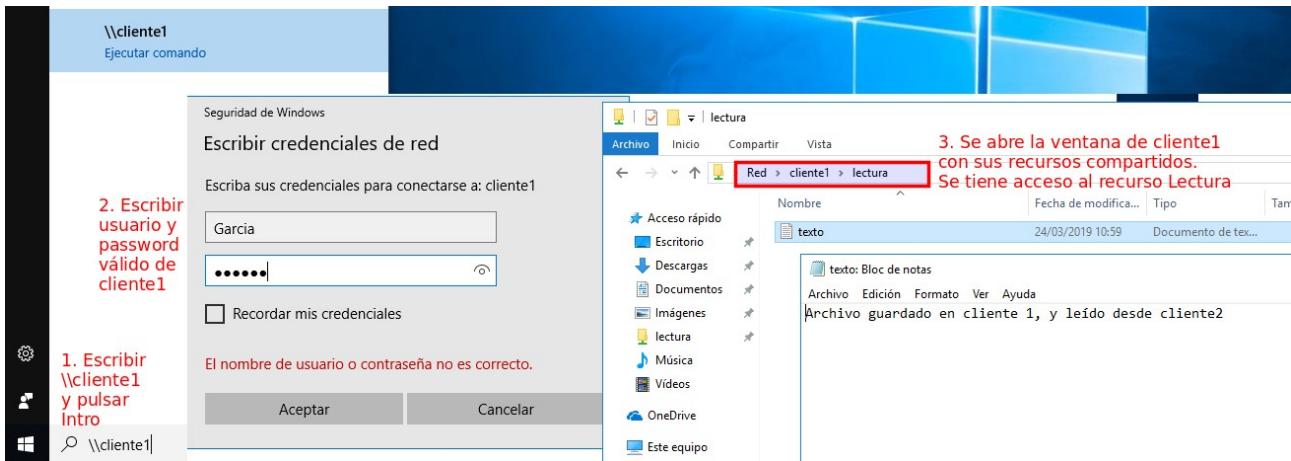
Desde un computador da rede, pódese acceder a un recurso doutro computador das formas seguintes:

- Executando directamente o roteiro UNC: \\nombreEquipo\nombreRecurso
- A través do explorador de Windows, pulsando en Rede.

Móstrase unha captura utilizando roteiro UNC con acceso desde cliente2 a cliente1. En cliente2 iniciouse sesión con supervisor, ao acceder a \\cliente1 e cliente1, pregunta unha identificación válida. Para realizar a conexión, hai que utilizar os datos dun usuario e password de cliente1.

É importante observar que se supervisor tivese o mesmo password nos 2 equipos, accedeuse directamente. Por ese motivo, configúronse distintas password para cada máquina, para maior comprensión didáctica dos exemplos.

Ilustración de Acceso a recurso con roteiro UNC.



Miguel Ángel García Lara (CC BY-NC-SA)

Calcular os permisos ao compartir

O algoritmo baséase nas dúas normas seguintes:

- Os permisos compartidos son acumulativos.
- Denegar prevalece sobre outros permisos.

Exemplos:

- Un usuario ten permiso de lectura nun cartafol compartido, e o usuario pertence a un grupo que ten control total.
 - Resposta.- O usuario conectarase con control Total
- Un usuario pertence a 3 grupos: un deles non ten permiso explícito, outro ten permiso lectura e outro ten permiso Cambiar.
 - Resposta.- O usuario conéctase con Cambio
- Un usuario pertence a 3 grupos: un deles ten lectura denegada, outro ten permiso lectura e outro ten permiso Cambiar.
 - Resposta.- O usuario non ten ningún permiso.

Observacións:

Do mesmo xeito que na configuración dos permisos locais, **debemos denegar permisos de forma coidadosa** ao compartir.

Combinación de permisos nas lapelas Compartir e Seguridade

Unha das primeiras preguntas que nos debemos fazer, é como se combinan os permisos de compartir en Rede e a seguridade local NTFS.

Nun recurso compartido, o usuario terá permisos de lectura, cambio, control total ou ningún permiso. O usuario conéctase desde a rede, e obterá devandito permiso.

Pero, que ocorre coa seguridade local?

- Se a partición é FAT 32, os permisos obtidos ao conectar ao recurso son os mesmos en todas as subcarpetas e ficheiros do recurso. (Pois FAT 32, non ten seguridade local)
- Se a partición é NTFS, os permisos obtidos ao conectar ao recurso ven afectados polos permisos NTFS LOCAIS. Desa forma, é posible que nalgúnsas subcarpetas podamos realizar cambios e noutras non.

Pódese resumir que cando un usuario conecta desde a rede, os permisos que ten son os más restritivos das lapelas Compartir e Seguridade (é dicir a intersección)

Exemplo: Un usuario ten nun recurso o permiso de cambio, e de forma local ten o permiso lectura. Que permiso ten o usuario cando acceda desde a rede?

Resposta: O usuario só terá lectura.

Recomendación final sobre seguridade local e compartir recursos.

Víronse dúas formas de poñer permisos, unha de forma local e outra na rede. Hai que ser moi ordenado na administración de permisos, pois se ha visto que cando se accede desde a rede, téñense en conta ambos.

Por este motivo danse 2 recomendacións conxuntas para facilitar a administración, e evitar conflitos:

- Administrar toda a seguridade cos permisos NTFS.
- Compartir o recurso a Todos os usuarios e con control total.

Este punto de vista explícarse da seguinte forma, se configuramos moi ben o equipo desde a seguridade local, xa non nos importa compartir con control total a Todos, pois a seguridade local impoñerase por ser más restritiva.

5.12.4 Servizos de redes

Os servizos en rede son importantes en toda infraestrutura de rede, xa que grazas a eles os diferentes computadores podes comunicarse, e o sistema informático é más potente.

Dentro dos servizos de rede verás como xestionalos e que portos están relacionados cos mesmos. Posteriormente estudas a configuración e xestión básica dalgúns servidores importantes, tales como os servidores de arquivos, de impresión e de aplicacións. Para finalmente mostrarche como controlar estes servizos.

5.12.4.1 Arquitectura cliente-servidor

Os servizos son procesos, programas en execución, que adoitan executarse de forma transparente ao usuario. Moitos se activan de forma automática ao comezo do sistema

operativo, ou tras unha petición do usuario, en función do rendemento do equipo, do tráfico da rede, etc.

O estudo vai centrar nos servizos de rede.

A arquitectura cliente-servidor é un modelo de aplicación distribuída no que as tarefas se reparten entre os provedores de recursos ou servizos, coñecidos como servidores, e os solicitantes destes, que son os clientes. Un cliente realiza peticións a outro programa, o servidor, que atende ditas peticións dando resposta.

A separación entre cliente e servidor é unha separación de tipo lóxico, onde o servidor non se executa necesariamente sobre unha soa máquina, nin é necesariamente un só programa.

Viuse en anterior unidade, que todos os equipos conectados a unha rede teñen unha dirección IP que os identifica, xa sexan ordenadores cliente ou servidores.

Portos

Cada sistema operativo posúe uns portos virtuais ou lóxicos. Isto significa que, ao contrario que os portos físicos (USB, Firewire, DVI, HDMI, etc.) só existen virtualmente para o computador. Os sistemas operativos contan con máis de 65.000 portos virtuais dispoñibles para abrir conexións, e cédenllas aos programas para que envorquen os seus datos na rede. Os programas solicítanos e o sistema operativo xestionaos para poder utilizalos e establecer unha conexión lóxica. Isto permite que poidan comunicarse con outro ordenador "punto a punto". Finalmente, toda comunicación entre dous dispositivos na internet tradúcese nun fluxo de datos entre dous portos virtuais abertos por alguma aplicación, entre unha parte cliente e unha servidora.

Os programas que comezan a comunicación nun porto chámanse clientes e os programas que están sempre usando un porto esperando que os clientes se conecten a el, chámanse servidores, dise que os servidores están a escoitar.

Por exemplo, un servidor web, está sempre esperando que un cliente (o navegador) conéctese para mostrarlle o contido da páxina web. O servidor web adoita utilizar permanentemente o porto 80 para esperar conexións entrantes e os navegadores adoitan usar un porto calquera dos 65.000 para establecer o fluxo de comunicación. O feito de que se utilice o porto 80 para ofrecer páxinas web é unha convención histórica, pero en realidade podería utilizarse calquera outro. Para enviar e recibir correo, por exemplo, utilízase o 25.

O número de portos codifícase con 16 bits, o que significa que hai $2^{16} = 65536$ posibles portos.

Os portos do 0 ao 1023 son os "portos coñecidos" ou reservados. Están reservados para os servidores. Con todo, un administrador de rede pode conectar servizos con portos da súa elección.

Os portos do 1024 ao 49151 son os "portos rexistrados". Os programadores, cando programan un servizo adoitan utilizar os portos rexistrados.

Os portos do 49152 ao 65535 son os "portos dinámicos e/ou privados". Utilízanse para comunicacións moi curtas, de aí o nome de dinámico.

Ao lado do cliente, o sistema operativo elixe o porto entre os disponibles de forma aleatoria, nunca entre os portos 0 e 1023 por ser os reservados para os servidores.

Reflíctese a continuación unha lista dos portos reservados para os servizos más importantes:

A continuación, indícanse algúns dos portos coñecidos máis utilizados:

Portos coñecidos asociados a servizos ou aplicacións

Puerto	Servicio o aplicación
21 (control), 20 (datos)	FTP
23	Telnet
25	 SMTP
53	DNS
80	 HTTP
110	 POP3
143	 IMAP
119	 NNTP

Monitoraxe de rede.

En ocasións, a velocidade da rede decrece, sendo necesario pescudar o motivo: hai algún usuario alleo á rede que está a se aproveitar do ancho de banda? Está a serse vítimas doutro tipo de ataque: sniffing, spoofin IP, DOUS?

A solución é incrementar o control sobre a rede utilizando ferramentas de análises de rede. Estas ferramentas realizan un estudo detallado e pormenorizado do tráfico que circula pola rede.

A monitoraxe considérase, tamén, unha tarefa de mantemento preventivo, tanto a nivel de seguridade como de dimensionamiento de rede: pode ocorrer que o ancho de banda sexa insuficiente ou pola contra estea sobredimensionado.

Algunhas das ferramentas de monitoraxe de redes más coñecidas:

Wireshark

É un analizador de protocolos utilizado para realizar análises e solucionar problemas en redes de comunicacóns. Ten unha interface gráfica, e moitas opcións de organización e filtrado de información. Así, permite ver todo o tráfico que pasa a través dunha rede establecendo a configuración en modo promiscuo.

Wireshark inclúe unha completa linguaxe para filtrar o que queremos ver e a habilidade de mostrar o fluxo reconstruído dunha sesión de TCP. Wireshark é software libre e execútase sobre a maioría de sistemas operativos Unix, Linux, Mac VOS X e Microsoft Windows.

Nmap

É un programa de código aberto que serve para efectuar rastrexo de portos. Nmap é difficilmente detectable, foi creado para evadir os Sistema de detección de intrusos (IDS) e interfere o menos posible coas operacións normais das redes e das computadoras que son analizadas.

Nagios

Software libre para Linux, permite monitorar a rede, permitindo ao administrador configurar advertencias.

Estas ferramentas de monitoraxe darán información sobre:

- Número de equipos conectados e as súas direccións IP.
- Tipo de tráfico predominante.
- Que portos están abertos.
- Que conexións establecidas hai.
- Algúns programas permiten a realización de inventarios dos equipos da rede (puntos de rede, segmentos, cableado, switches, routers, PC, etc.)

5.12.4.2 Servizos de infraestrutura de rede

Existen moitos servizos, algúns deles necesarios para crear unha infraestrutura de rede. Entre eles:

- **Encamiñamento:** permite a un servidor actuar como router para permitir a comunicación entre dúas ou más redes. No libro 9.A.1. configuramos as IP, dos equipos cliente1 e cliente2, pero non se puxo porta de ligazón. A porta de ligazón será normalmente a dirección do router, polo que sairemos a Internet.
- **Servidor DHCP.** Permite asignar automaticamente a configuración IP dos equipos clientes da rede. Este servizo é moi importante xa que facilita a conexión dos equipos á rede. Por exemplo, cando conectamos un computador en casa, non é necesario configurar a dirección IP como se fixo no libro A.1. Iso débese, a que os routers das compañías telefónicas adoitan ter instalado o servidor DHCP, de forma que cando se conecta un computador á devandita rede, o servidor DHCP facilita unha IP ao computador.

- **Servidor DNS.** Un servidor DNS é un equipo na internet que facilita a navegación web, pois traduce as direccións web, que se utilizan na navegadores web ás direccións IP correspondentes. Son como un dicionario con 2 columnas: direccións web e direccións IP. Nos computadores dos domicilios particulares, non adoita ser necesario especificar a dirección IP do servidor DNS, pois adoita estar indicado nos routers.

Profundouse o encamiñamento na unidade 8, agora vaise a profundar nos servizos DHCP e DNS.

1. Servizo DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración de equipo dinámica)

O mantenemento e a configuración da rede dos equipos dunha rede pequena é relativamente fácil. Con todo, se a rede é grande, calquera cambio na configuración de rede: dirección IP, porta de ligazón, DNS conleva un excesivo tempo para executar a tarefa.

Por outra banda, utilizar IP estáticas (IP fixas) pode obter un mal aproveitamento das direccións IP da rede. Por exemplo, nunha clase C só pódense ter 254 equipos. De forma estática só pódense ter esos equipos, pero se se configuran de forma dinámica, pódense reutilizar as direccións IP noutros equipos. Podemos ter nunha empresa con bastantes computadores portátiles, máis de 254, que cando se acandan, o servidor DHCP asígnalles unha dirección IP e ao apagar o equipo, queda libre para outro computador.

Os datos mínimos que un servidor de DHCP proporciona a un cliente son:

- Dirección IP.
- Máscara de rede.
- Porta de ligazón ou gateway.
- Dirección IP do servidor DNS.

O protocolo DHCP inclúe dous métodos de asignación de direccións IP:

Asignación dinámica. Asigna direccións IPs libres dun rango de direccións establecido polo administrador.

Reserva por dirección IP. Consiste en asignar sempre a mesma IP a un equipo concreto. Para iso utilízase a dirección MAC. Por exemplo, é desexable que unha impresora en rede teña sempre a mesma dirección IP xa que se cambia de dirección IP deberemos configurar novamente a impresora en todos os equipos clientes que a utilicen.

2. Servizo DNS (Domain Name System, Sistema de nomes de dominio)

Se executamos ping a www.educa.madrid.org vemos que responde o equipo 213.229.137.36, que é a súa dirección IP correspondente.

Para navegar é más fácil memorizar a páxina www.educa.madrid.org que o seu IP, ademais ofrece máis flexibilidade; pois se cambia o aloxamento da páxina web, cambia a

dirección IP, pero os clientes non notan ningún cambio, pois se segue navegando na páxina web coa dirección web.

Inicialmente a asociación de nomes coa súa respectiva dirección IP realizábase nos propios computadores a través dun ficheiro (\winnt\system32\driver\etc\hosts en Windows ou /etc/hosts en Linux). Esta opción presentaba o problema que calquera cambio, significaba cambiar o ficheiro en todos os computadores da rede.

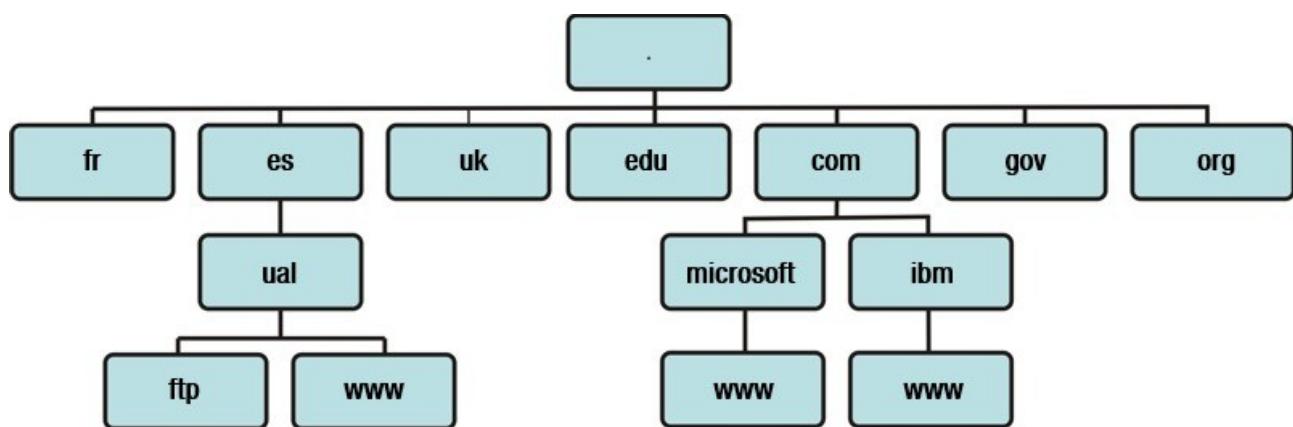
De aí ideouse o sistema de resolución de nomes (DNS) baseado en dominios, no que se dispón dun ou máis servidores encargados de resolver os nomes dos equipos pertenecentes ao seu ámbito, conseguindo a centralización necesaria para a correcta sincronización dos equipos e un sistema xerárquico que permite unha administración focalizada e descentralizada.

2.1. Espazo de nomes de dominio

Do mesmo xeito que os ficheiros dos sistemas operativos organízanse en árbores xerárquicas, o sistema de nomes de dominios tamén se estrutura cunha árbore xerárquica no que as distintas ramas que atopamos reciben o nome de dominio e o nome completo dun equipo (o equivalente ao nome dun ficheiro) ou FQDN (path absoluto) é o nome resultante de percorrer todos os dominios polos que pasamos, desde as follas ata a raíz da árbore utilizando, neste caso, o carácter '.' (punto) como separador.

Na imaxe móstrase un exemplo de xerarquía dos dominios da internet.

Imaxe de árbore dominios.



Imaxe dos materiais orixinais de FP a Distancia (CC BY-NC-SA)

Dependendo da profundidade da árbore, falarase de dominios de primeiro, segundo ou terceiro nivel.

Como exemplo na imaxe obtense o dominio de terceiro nivel www.microsoft.com

No primeiro nivel da árbore atopamos que os nomes dos nodos xa están establecidos de antemán, existindo dous tipos de divisións: xeográfica e organizativa.

División xeográfica: distínguese unha rama -dominio- por país:

- Para España .es
- Para Gran Bretaña, .uk
- Para Alemaña, .de.

División organizativa:

- Para empresas .com, independentemente do país no que se atopen.
- Para organizacións establecidas mediante tratados internacionais .int
- Para organizacións non gobernamentais .org
- Organizacións educativas .edu, do goberno .gov e do exército de EE.UU. .mil

Posteriormente, introducíronse novos dominios de primeiro nivel como .name para nomes de persoas; .info para provedores de servizos de información; .web para empresas relativas a servizos web; etcétera.

Cada rama da árbore xerárquica recibe o nome de dominio e a asignación de nomes delegase nun responsable. Para España, a rama .es mantén a empresa pública REDES, que á súa vez poderá delegar a resolución de nomes das distintas ramas nas que se divide, noutras corporacións.

Unha característica crucial é a máxima dispoñibilidade do servizo DNS. Para iso, existen varios servidores capaces de realizar o mesmo servizo aínda que a autoridade de resolución de nomes de zona siga recaendo nun servidor principal. Estes servidores con autoridade reciben o nome de servidores primarios e o resto servidores secundarios.

Para que non existan problemas de sincronización cada vez que se modifique un dato do servidor primario debe transmitirse a todos os secundarios para o correcto funcionamento do sistema.

2.2. Rexistrar un dominio

Calquera persoa física con residencia en España, así como empresas constituídas segundo a legislación española, pode solicitar o rexistro de dominios a través da páxina estatal nic.es ou ben, por medio dos axentes rexistradores acreditados. Os nomes de dominio débense, segundo a regulamentación española, corresponder con:

- Nome (ou abreviatura) dunha empresa que a identifique de forma inequívoca.
- Nomes comerciais ou de marcas.
- Nome de persoas tal e como aparecen no seu DNI, cun máximo de 60 caracteres.
- Nomes de profesións e o apellido ou nome do profesional que se dedica ao devandita labor ou do nome do establecemento.

5.12.4.3 Servizo FTP (File Transfer Protocol, Protocolos de transferencia de ficheiros).

As redes de computadores ideáronse para o intercambio de información e a compartición de ficheiros. Temos dúas opcións, a través dun servidor de arquivos, ou mediante o uso dun servidor FTP.

Un servidor de arquivos ou ficheiros permítenos compartir recursos, dentro de una mesma rede local como se viu no libro B ao compartir recursos en Windows. Ou como se estudará na unidade 10 en Linux, ao utilizar os servizos NFS e Samba.

Doutra banda, o servizo FTP permite conectarse a un equipo (o servidor FTP) e transferir ficheiros desde este cara a o equipo do cliente (cliente FTP) e en sentido inverso.

O protocolo FTP establece unha dobre conexión TCP entre o cliente e o servidor:

- **Conexión de control:** adoita empregarse o porto 21 do servidor e serve para indicarlle a este as operacións que se queren levar a cabo.
- **Conexión de datos:** úsase normalmente o porto 20 do servidor e é a que se serve para a transferencia de ficheiros cara a ou desde o servidor.

Cando un cliente FTP quérrese conectar ao servidor FTP, existen dous tipos de autenticación:

- **Anónimo.** A comunicación realizase sen ningún tipo de identificación e, por tanto o usuario terá moi poucos privilexios no servidor. Neste caso, o usuario estará confinado nun directorio público onde pode descargar os arquivos alí situados pero sen posibilidade de escribir ou modificar ningún ficheiro. O directorio público adoita chamarse pub.
- **Acceso autorizado.** O usuario establece a comunicación cunha conta de usuario. Tras identificarse, confínase ao usuario ao seu directorio predeterminado desde onde pode descargar ficheiros e, se a política implantada permíteo, tamén escribir. Esta opción é amplamente utilizada para que os usuarios poidan acceder aos seus ficheiros ou para poder actualizar de forma remota o seu portal web.

Estes parámetros (**o tipo de autenticación e os permisos**) estableceranse na configuración do sitio FTP no equipo servidor.

Como exemplo, o servidor (nome do dominio) ftp de Educamadrid chámase [ftp.educa.madrid.org](ftp://ftp.educa.madrid.org), que permite o acceso anónimo. Para iso, abrimos a navegador web e escribimos <ftp://ftp.educa.madrid.org>. Ao pulsar intro no navegador, entramos como usuario anónimo ao servidor ftp de Educamadrid (ver imaxe)

Cando na navegador web escríbese <ftp://> significa que a comunicación se realiza co protocolo ftp, a diferenza de cando se escribe <http://> que a comunicación se realiza co protocolo http.

Ilustración de Servidor [ftp.educa.madrid.org](ftp://ftp.educa.madrid.org).

Índice de ftp://ftp.educa.madrid.org/

Subir al directorio superior.

Nombre	Tamaño	Última modificación
MD	26/5/17	0:00:00 CEST
incoming	24/12/04	0:00:00 CET
mirror	24/12/04	0:00:00 CET
mirror2.0	21/11/05	0:00:00 CET
pub	7/11/17	0:00:00 CET

Miguel Ángel García Lara (CC BY-NC)

Servidores FTP

Os servidores FTP más utilizados son IIS (Internet Information Server) nos equipos Windows, Filezilla Server (para Windows e Linux) e vsftpd (para servidores Linux)

Clients FTP

Os clientes FTP son o software que utilizamos para conectar ao servidor FTP.

Os clientes FTP más utilizados son Filezilla, cuteftp, vsftp e os propios navegadores web.

As propias terminais de comandos, tanto de Windows como GNU-Linux inclúen un cliente ftp. Para conectarnos escríbese ftp nome_servidor.

Para explorar o servidor e realizar a transferencia de ficheiros utilízanse os comandos ftp.

5.12.4.4 Servizo Web. Protocolo HTTP (*Hipertext Transfer Protocol, Protocolo de transferencia de hipertexto*)

Coñecido coas súas siglas www (World Wide Web) que aparecen no nome de praticamente todos os servidores web, o servizo web é o servizo más utilizado dos que se ofrecen na internet.

Un servidor web encárgase de aloxar e proporcionar as páxinas web solicitadas polos clientes desde os seus navegadores. Un servidor web manexa o protocolo HTTP. Cando o servidor web recibe unha petición HTTP, leste responde cunha resposta HTTP, normalmente unha páxina HTML. O servidor Web pode responder cunha páxina HTML estática, unha imaxe, enviando unha redirección, ou delegando a xeración dinámica da resposta a algúun outro programa, por exemplo algúun script CGI, JSP (JavaServer Pages), Servlets, ASP (ActiveServer Pages), PHP, este tipo de programas ao lado do servidor dise que xeran unha páxina dinámica ao lado servidor, enviando a páxina resultante en HTML, para que poida ser vista na navegador web do usuario.

A variante segura de HTTP é o protocolo HTTPS onde a S significa Secure. O protocolo HTTPS protexe a integridade e confidencialidade dos datos entre o cliente e servidor.

A integridade refírese a que a páxina recibida no cliente sexa a realente enviada polo servidor.

A confidencialidade a que os datos enviados na comunicación non poidan ser interceptados por viaxar cifrados.

Servidor web

Os servidores web más coñecidos son:

- Apache: software libre multiplataforma para Windows, Linux e MacOS (40.20% de cota de mercado).
- Nginx, tamén software libre multiplataforma. (27.67% de cota de mercado)
- IIS - Internet Information Server, servizo de Microsoft para os sistemas operativos Windows. (11.08% de cota de mercado)

Cliente web

Os clientes son a navegadores web como Mozilla Firefox, Google Chrome, Internet Explorer, Safari, etcétera.

As principais diferenzas entre os clientes web residen no número e importancia de vulnerabilidades que presentan así como en diferentes matizácións que existen en canto á interpretación do código HTML e que pode impedir a correcta visualización dalgunhas páxinas en determinados clientes. Tamén inclúen a interpretación de scripts ao lado cliente como Javascript.

5.12.4.5 Servizo de correo electrónico

O sistema de correo electrónico é xunto ao servizo web, os servizos da internet más utilizados a nivel de usuarios.

Este servizo é un sistema para a transferencia de mensaxes, rápido e eficiente, ideado baixo a arquitectura cliente-servidor típica da internet.

Servidor de correo

O servidor ten os seguintes componentes, traballando con varios protocolos:

Servidor de correo saínte O cliente envía o email ao servidor, e á súa vez o servidor envía o correo ao servidor do destinatario. Utiliza o protocolo SMTP.

Servidor de correo entrante Almacena os correos electrónicos recibidos nas caixas de correos dos usuarios. Cando o cliente conéctase, envíanselle os correos electrónicos que recibiu. Utiliza os protocolos POP e IMAP.

Clientes de correo

Na actualidade utilízase o correo web de forma masiva, pero nas empresas o correo electrónico adóitase utilizar con clienes de correo.

Cando se envía unha mensaxe, esta mensaxe envíase ao servidor. Despois, segundo o tipo de correo que se utilice, o servidor envía ao destinatario a mensaxe, ou o solicita o destinatario ao servidor.

Isto dá lugar a 2 tipos de software de correo:

Correo web: o máis utilizado na actualidade a nivel particular. O usuario conéctase ao servidor de correo cunha navegador web. O usuario ten acceso a todo o seu correo e administración: pode crear mensaxes, borrar, organizar en bandexas e administrar os contactos. A información sempre está no servidor, polo que o usuario pódese conectar desde calquera computador con Internet.

Clientes de correo: instálase software de correo no computador, e o cliente conecta ao servidor, descargándose todos os correos no propio equipo. A bandexa de entrada, saída, contactos, tenen o usuario no propio equipo.

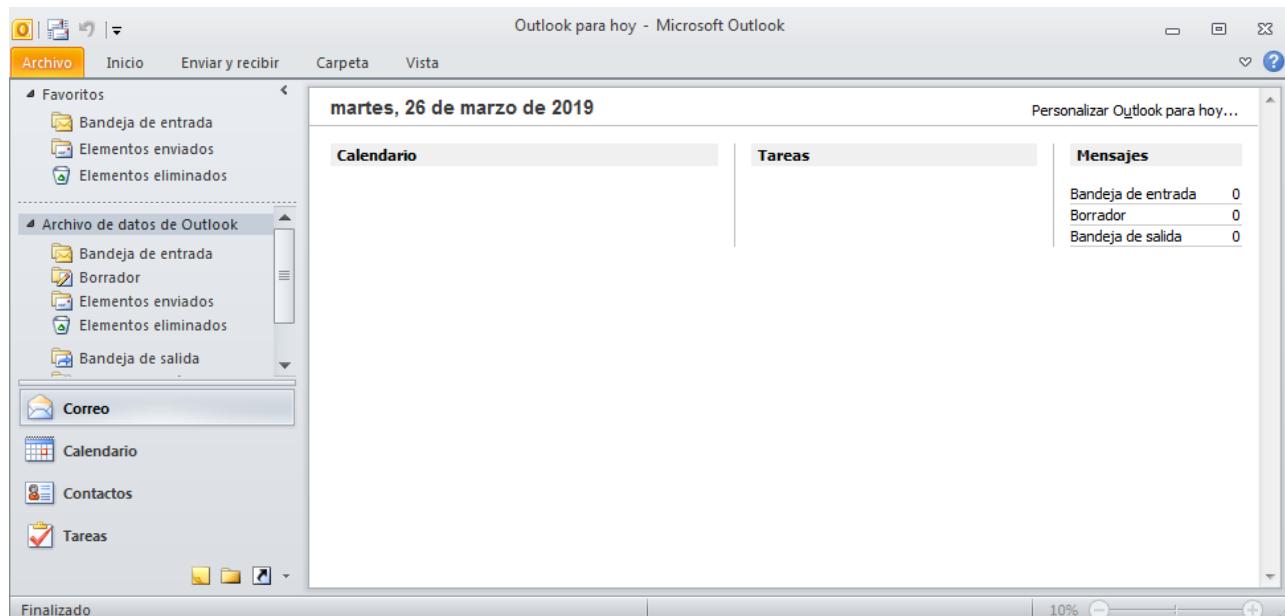
Entre os clientes de correo más coñecidos atópanse Evolution, Microsoft Outlook e Mozilla Thunderbird.

Esta é a forma máis habitual na conexión nas empresas. O usuario ten no seu equipo todas as mensaxes e contactos anteriores, sen necesidade de conectarse a Internet.

Todos eles presentan funcións similares: recepción, composición e ordenación mediante cartafolios e subcarpetas do correo electrónico.

Inclúese unha imaxe do cliente Microsoft Outlook:

Ilustración de Cliente correo Microsoft Outlook.



Miguel Ángel García Lara (CC BY-NC-SA)

5.12.4.6 Acceso remoto

Os servizos de acceso remoto, permiten controlar e administrar outro computador a través da rede. Así por exemplo, desde un equipo en casa pódese conectar ao equipo do traballo, e pódense usar todos os seus programas, arquivos e recursos de rede como se estivésese fisicamente no equipo da oficina.

Para realizar a conexión, nas distintas aplicacións, é necesario instalar o software servidor no equipo que se quere controlar, e o programa chamado cliente na máquina desde a que se vai a levar o control.

Especifícanse varios servizos de acceso remoto clasificados pola súa interface de texto ou interface gráfica:

Acceso remoto en modo terminal.

En modo terminal, utilizanse como accesos remotos os servizos Telnet e SSH.

Telnet é unha aplicación TCP/IP e utilízase tanto en Windows como Linux, incluída nas terminais de Windows e GNU-Linux. Pero na actualidade utilízase moi pouco por ser inseguro, pois o envío da información realiza en texto plano sen cifrar.

SSH ten a mesma funcionalidade que Telnet, e igualmente é o nome dun protocolo e dun programa, pero engadíronse: o cifrado das conexións para evitar que os datos sexan interceptados. Ademais emprega mecanismos de autenticación más seguros para os usuarios que se conectan. O servizo ssh é software libre e utilizado inicialmente en GNU-Linux, estendeuse o seu uso a Windows.

A vantaxe dos accesos remotos por terminal, é a fluidez na comunicación, pois necesitan pouco ancho de banda ao incorporar só texto na comunicación.

Acceso remoto en modo gráfico.

En modo gráfico as aplicacións más coñecidas son:

- Escritorio remoto e Terminal Server aplicacións incluídas nas versións más completas de Microsoft Windows.
- VNC (Visual Network Control), software libre utilizado en máquinas Windows e Linux.
- Teamviewer, aplicación externa de Windows, que adoitan utilizar os servizos técnicos telefónicos para a solución de problemas.

Exemplo. Instalación e configuración dun servidor FTP en “Internet Information Service” en Windows 10.

Neste tutorial vai instalar e configurar o servidor FTP que vén con Windows 10.

Este tutorial corresponde a un exercicio da tarefa.

Crearase un servidor FTP con nome ‘ftp.empresa_inicialesAlumno.es’ que esixa autenticación aos usuarios e onde estes teñan permisos para baixar e subir arquivos. Ademais, verase como se conecta un cliente ao servizo FTP.

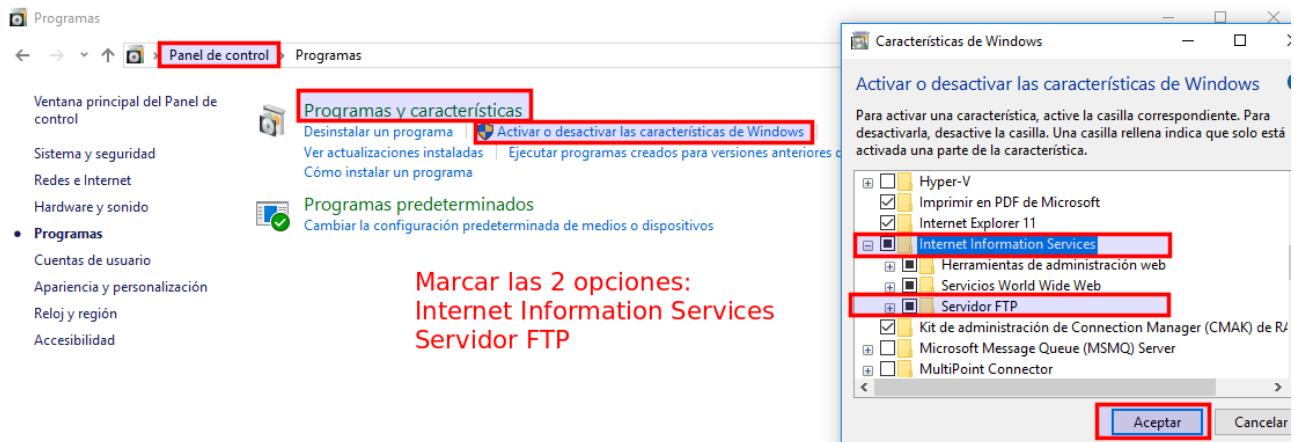
O servizo IIS (Internet Information Service) incluído nos sistemas operativos Windows, inclúe o servidor web e o servidor FTP de Microsoft. Microsoft denomina aos servidores web e ftp, como os meus “sitios web” e “sitios ftp”.

Paso 1. Instalar IIS co servidor FTP.

Instalar IIS e o servidor FTP de Windows. Para iso, ir a Panel de control / Programas / Engadir características de Windows /

Marcamos as opcións de engadir “Internet Information Services” e “Servizo FTP”, tal como vese na captura.

Ilustración de Instalar IIS e servidor FTP.



Miguel Ángel García Lara (CC BY-NC-SA)

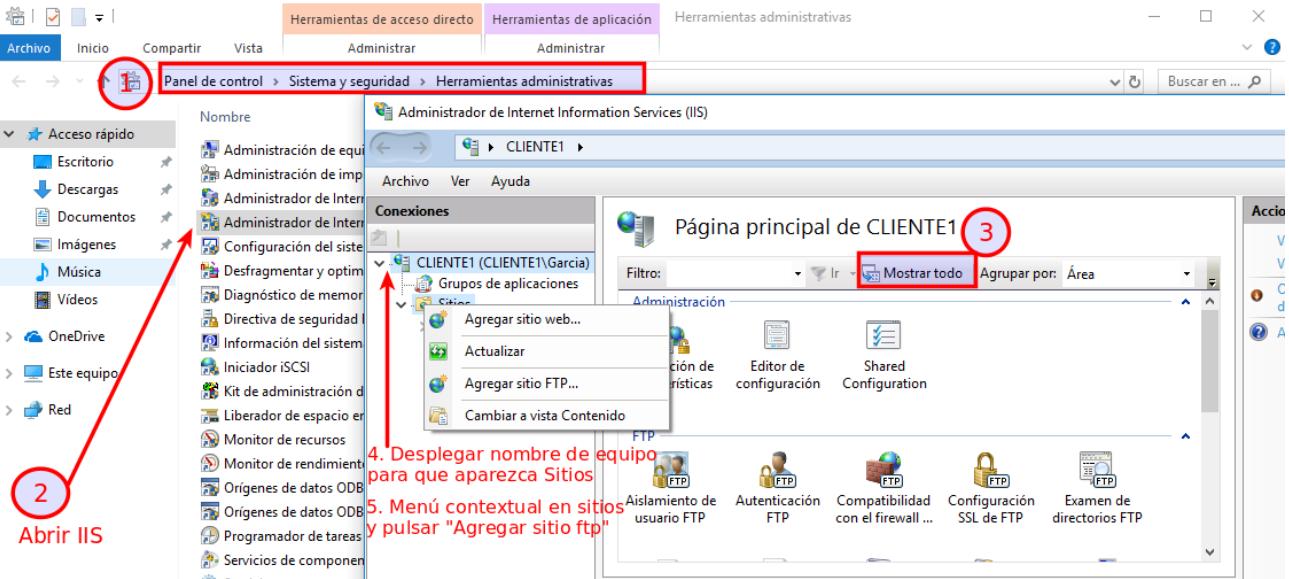
Cando se pulsa Aceptar, instálase o servidor.

Paso 2. Crear novo servidor FTP

Para configurar o servizo FTP regresamos de novo ao Panel de control – Sistema e seguridade - Ferramentas Administrativas e facemos clic sobre “Administrador da internet Information Service (IIS)”.

Seguimos os pasos da imaxe para engadir o sitio FTP: Pulsar mostrar todo. Menú contextual en nome de equipo para que aparezca “Os meus sitios” e menú contextual para seleccionar “Agregar sitio FTP”.

Ilustración de Consola de IIS: agregar sitio FTP.



Miguel Ángel García Lara (CC BY-NC-SA)

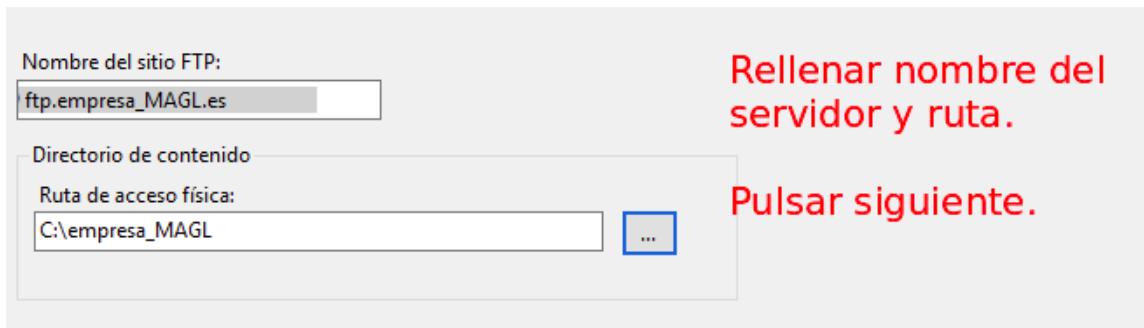
Paso 3. Encher nome do novo sitio FTP e roteiro

Escríbese os campos na xanela que aparece (ver captura):

Nome do sitio FTP: Encher con ftp.empresa_InicialesAlumno.es

Roteiro de acceso física: introdúcese o roteiro do cartafol onde se van a aloxar os ficheiros do sitio FTP. Crear a cartafol empresa_InicialesAlumno en C, e encher "C:/empresa_InicialesAlumno".

Ilustración Encher nome sitio FTP e roteiro cartafol.

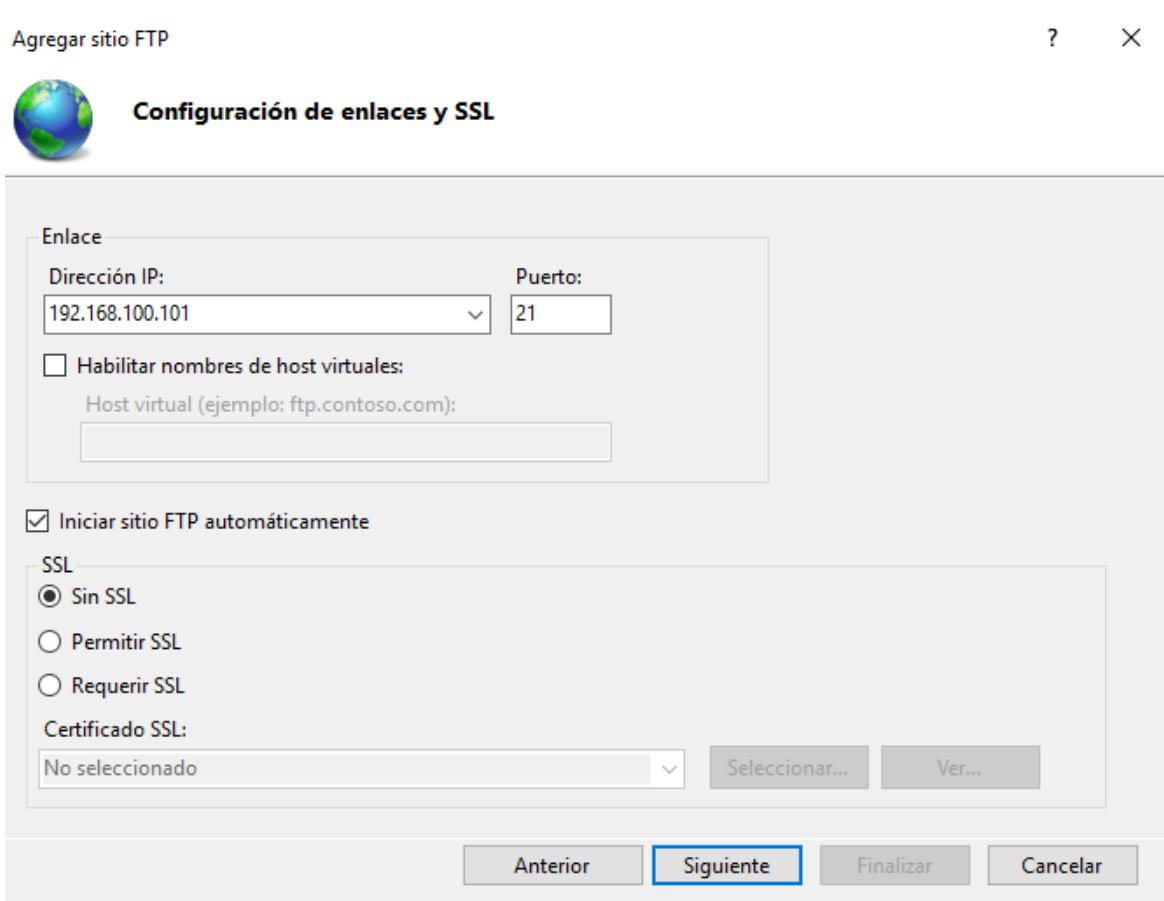


Miguel Ángel García Lara (CC BY-NC-SA)

Paso 4. Xanela “Configuración de ligazóns e SSL”

Ábrese esta xanela, enchemos cos datos da captura.

Ilustración Configurar IP e sen SSL.



Miguel Ángel García Lara (CC BY-NC-SA)

Explicación de cada opción:

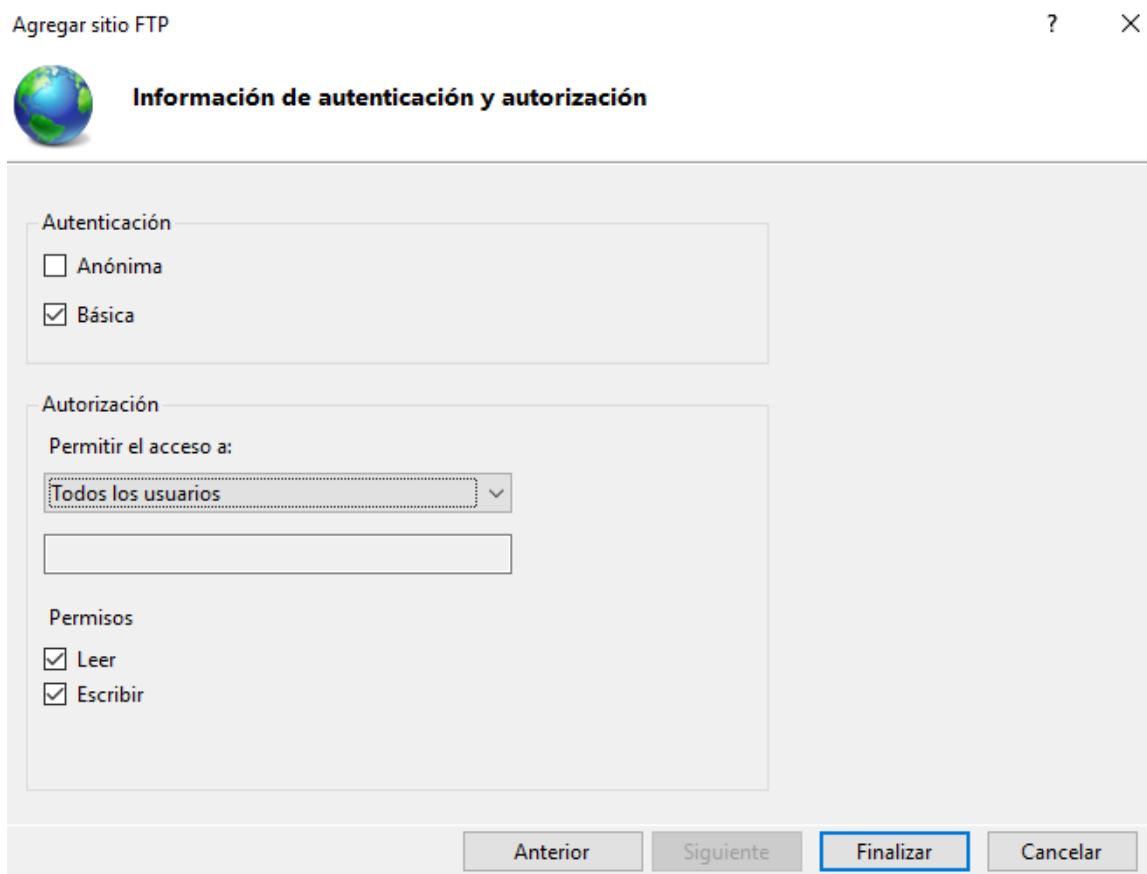
- Enlace - Dirección IP: neste campo pódese indicar que dirección IP asignaráselle a este sitio FTP, xa que o equipo pode ter varias direccións IP (varias interfaces de rede). Por defecto queda seleccionado “Todas as non asignadas”. Se temos varios sitios FTP e queremos que sexan accesibles desde fóra do equipo, poderemos indicar que dirección IP asignaráselle a cada sitio FTP.
- Habilitar nomes de host virtuais: se queremos ter varios sitios FTP nun equipo cunha soa dirección IP e queremos que sexan accesibles desde fóra do equipo (LAN ou Internet) poderemos marcar esta opción de “Habilitar nomes de host virtuais” e indicar o nome do sitio ftp que queiramos establecer. É dicir, pódense ter 2 servidores virtuais (de aí o seu nome) nun único servidor, utilizando nomes distintos: ftp.empres1.es e ftp.empres2.es
- Iniciar sitio FTP automaticamente: deixando marcada a opción o servizo do sitio FTP iniciase automaticamente ao arrincar o equipo.
- SSL, permite 3 opcións:

- Sen SSL: seleccionando esta opción de Secure Sockets Layer (Protocolo de Capa de Conexión Segura) desactívase este protocolo.
- Permitir: con esta opción o usuario pódese conectar con SSL e sen SSL.
- Requerir SSL: o usuario só pódese conectar usando SSL.
- No noso caso, ao non ter instalado ningún certificado de seguridade, hai que marcar “Sen SSL”

Paso 5. Xanela “Información de autenticación e autorización”

Ábrese esta xanela e enchemos cos datos da captura. Ao pulsar “Finalizar”, quedou creado o sitio web.

Ilustración de Configurar autenticación básica, todos e ler e escribir.



Miguel Ángel García Lara (CC BY-NC-SA)

Explicación das distintas opcións:

Nesta xanela configúrase se se permite o acceso anónimo ou baseado en “autenticación básica” onde os usuarios teñen que proporcionar un nome de usuario e contrasinal

válidos de Windows. É importante saber que a autenticación básica transmite contrasinais non cifrados pola rede, de aí, que nunha contorna profesional é obligatoria utilizar SSL.

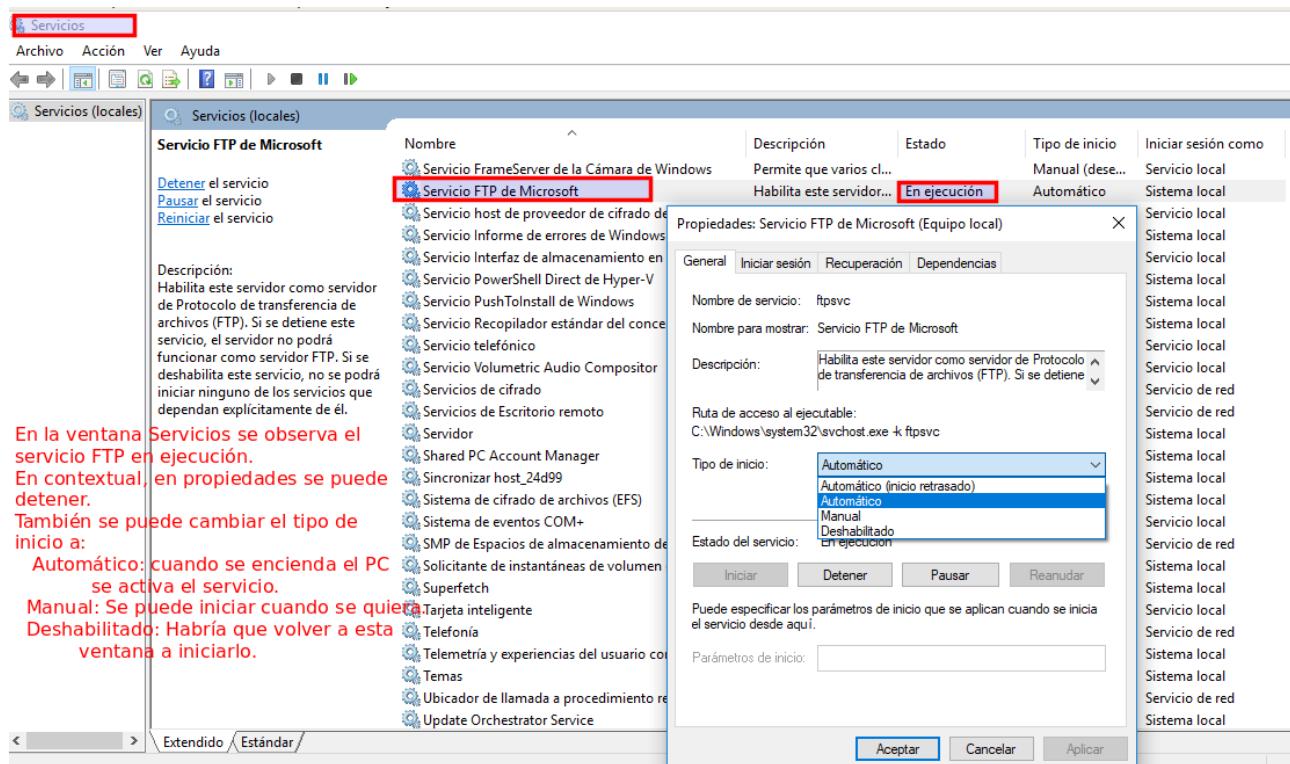
Marcada a autorización básica, pódese seleccionar a “Todos os usuarios” ou a usuarios ou grupos concretos.

Paso 6. Xanela servizos en Windows.

Compróbase que o servizo Ftp está activo en Windows, para iso, ábrese a xanela servizos e compróbase que o “Servizo FTP” atópase en execución, tal como móstrase na captura. Nesta xanela de Windows inicianse ou deteñen todos os servizos. Así mesmo, pulsando en propiedades no nome de cada servizo temos as opcións de seleccionar en “Tipo de inicio”:

- Automático: sempre que se inicie o computador, iníciase o servizo.
- Manual: hai que iniciar o servizo manualmente.
- Deshabilitado: non se pode iniciar o servizo.

Ilustración de Xanela servizos de Windows.



Miguel Ángel García Lara (CC BY-NC-SA)

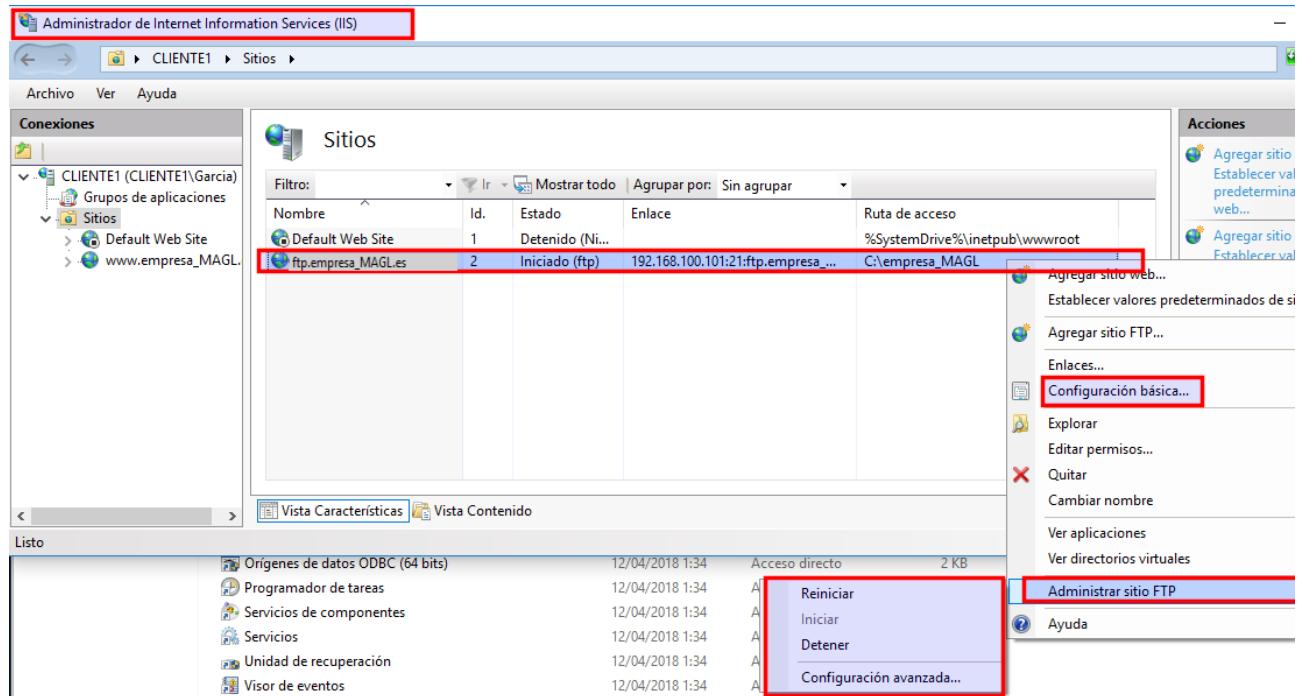
Paso 7. Configuración e control do sitio FTP.

En Servizos pódese deter ou iniciar o servizo FTP, pero habemos visto que se poden configurar varios “sitios FTP”. Se se queren ter uns activos e outros detidos, configúrarse na consola de “Internet Information Services”

Ao pulsar menú contextual no sitio, pódese Iniciar e Deter. E tamén configurar en “Configuración básica” e “Configuración avanzada”.

Mesmo, vemos as opcións para agregar un novo “sitio ftp” e un “sitio web”

Ilustración de Consola de IIS: Iniciar, deter, configuración.



Miguel Ángel García Lara (CC BY-NC-SA)

Conexión de clientes ao servizo FTP.

Neste exemplo vai realizar a conexión coa terminal de Windows. No equipo cliente2 ábrese a terminal e escríbese:

ftp 192.168.100.101

Pídenos usuario e contrasinal. Unha vez dentro, pódense utilizar os comandos de ftp. (Anexo da unidade)

Na captura, realizase unha conexión desde cliente2 ao servidor ftp e sóbese un ficheiro desde cliente2 a cliente1.

Ilustración Conexión cliente2 a servidor FTP de cliente1 con cmd.

```

C:\ Administrador: Símbolo del sistema

c:\Users\Garcia>echo hola > archivo.txt      Se crea archivo.txt en máquina local 192.168.100.102

c:\Users\Garcia>ftp 192.168.100.101          Se conecta al servidor ftp 192.168.100.101
Conectado a 192.168.100.101.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Usuario (192.168.100.101:(none)): supervisor
331 Password required
Contraseña:                                         Autenticación: Usuario supervisor
                                                       Password: super1
230 User logged in.

ftp> ls                                           Listado en servidor: vacío
00 PORT command successful.
25 Data connection already open; Transfer starting.
26 Transfer complete.

ftp> put archivo.txt                            Se sube archivo.txt al servidor
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
Ftp: 7 bytes enviados en 0.07segundos 0.10a KB/s.

ftp> ls                                           Listado en servidor: archivo.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
archivo.txt
226 Transfer complete.
Ftp: 16 bytes recibidos en 0.00segundos 16000.00a KB/s.

ftp> bye                                         Salir del servidor con bye. Vuelve la shell de Windows.

221 Goodbye.

c:\Users\Garcia>

```

Miguel Ángel García Lara (CC BY-NC-SA)

Observación final:

A conexión con nome do dominio realizaríase escribindo:

ftp ftp.empresa_MAGL.es

No exemplo visto aquí, non funciona se escribimos esta dirección. Por que?, porque non temos un servidor DNS que diga que ftp.empresa_MAGL.es corresponde á IP 192.168.100.101

5.12.5 Comandos de rede

5.12.5.1 Comandos TCP/IP en Windows.

O protocolo TCP/IP, facilita distintas utilidades para monitorar a rede, polo que estes comandos témolos tanto en Windows como en Linux, con pequenas diferenzas nos seus nomes ou execución.

Móstranse a continuación os de Windows con exemplos de execución.

Comando ipconfig

Devolve a configuración das distintas tarxetas de rede, coa súa dirección IP, máscara e porta de ligazón.

Coa opción /all devolve unha información más completa, entre ela, a dirección física (MAC) das distintas conexións.

Ilustración comando ipconfig.

```
C:\> Administrador: C:\Windows\System32\cmd.exe
C:\> Windows\system32>ipconfig
Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:
  Sufijo DNS específico para la conexión. . . : Home
  Vínculo: dirección IPv6 local. . . : fe80::29c0:57d8:6e5d:19ba%10
  Dirección IPv4. . . . . : 10.0.2.15
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : 10.0.2.2

Adaptador de túnel isatap.Home:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . : Home

Adaptador de túnel Teredo Tunneling Pseudo-Interface:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :
```

Miguel Ángel García Lara (CC BY-NC-SA)

Comando ping

Serve para ver se temos conexión con calquera equipo, podemos utilizar tanto a dirección web, como o seu IP. No exemplo realizaase ping con éxito a www.elpais.es

Ilustración do comando ping.

```
C:\> Administrador: C:\Windows\System32\cmd.exe
C:\> Windows\system32>ping www.elpais.es
Haciendo ping a a1749.g.akamai.net [212.106.208.40] con 32 bytes de datos:
Respuesta desde 212.106.208.40: bytes=32 tiempo=7ms TTL=127
Respuesta desde 212.106.208.40: bytes=32 tiempo=4ms TTL=127
Respuesta desde 212.106.208.40: bytes=32 tiempo=5ms TTL=127
Respuesta desde 212.106.208.40: bytes=32 tiempo=7ms TTL=127

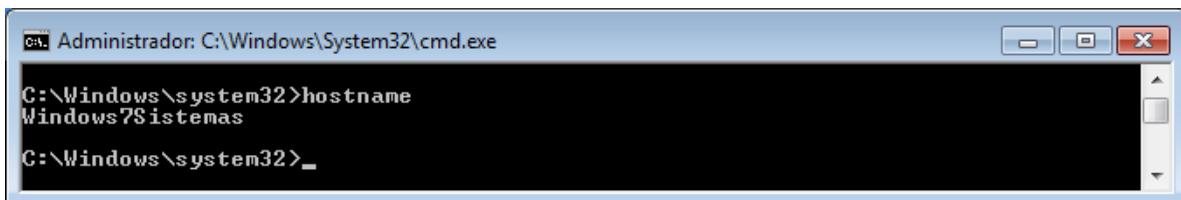
Estadísticas de ping para 212.106.208.40:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 4ms, Máximo = 7ms, Media = 5ms
C:\> Windows\system32>
```

Miguel Ángel García Lara (CC BY-NC-SA)

Comando hostname

Devolve o nome do equipo

Ilustración Comando hostname.



```
C:\ Administrador: C:\Windows\System32\cmd.exe
C:\Windows\system32>hostname
Windows7Sistemas
C:\Windows\system32>_
```

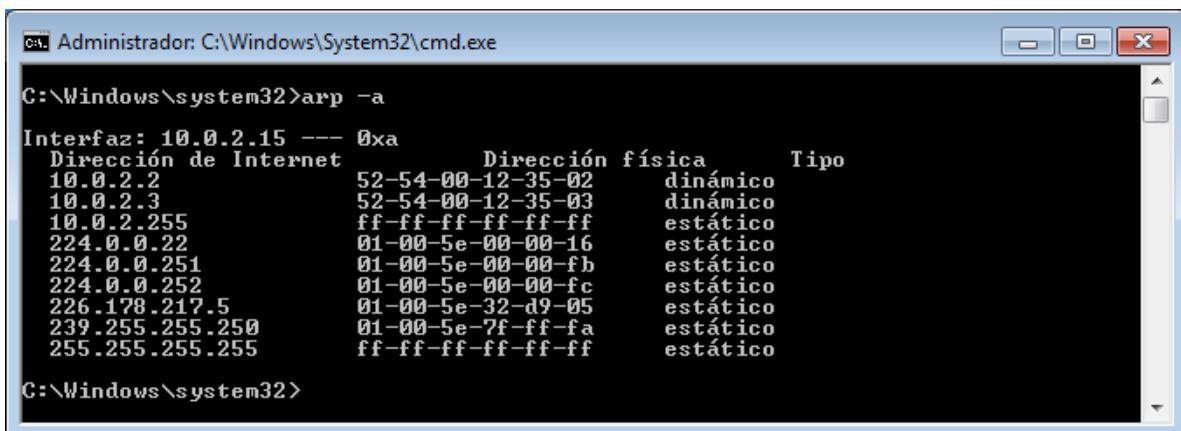
Miguel Ángel García Lara (CC BY-NC-SA)

Comando arp

Na unidade anterior estudouse que os protocolos arp e rarp traducen IP en direccións físicas e viceversa. O comando arp –a mostra relaciónelas IP e MAC coñecidas neste momento.

Con outras opcións, pódense engadir datos.

Ilustración Comando arp.



```
C:\ Administrador: C:\Windows\System32\cmd.exe
C:\Windows\system32>arp -a
Interfaz: 10.0.2.15 --- 0xa
          Dirección de Internet   Dirección física      Tipo
 10.0.2.2           52-54-00-12-35-02    dinámico
 10.0.2.3           52-54-00-12-35-03    dinámico
 10.0.2.255         ff-ff-ff-ff-ff-ff    estático
 224.0.0.22          01-00-5e-00-00-16    estático
 224.0.0.251         01-00-5e-00-00-fb    estático
 224.0.0.252         01-00-5e-00-00-fc    estático
 226.178.217.5       01-00-5e-32-d9-05    estático
 239.255.255.250     01-00-5e-7f-ff-fa    estático
 255.255.255.255     ff-ff-ff-ff-ff-ff    estático
C:\Windows\system32>
```

Miguel Ángel García Lara (CC BY-NC-SA)

Comando tracert

O comando tracert (vén de traceroute) devolve por todos os equipos que pasan as tramas para chegar do PC actual a un PC destino. Algunas datos non se mostran, porque os router bloquean estas peticións (tamén pasa moitas veces co comando ping)

Ilustración Comando tracert.

```

Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>tracert www.elpais.es
Traza a la dirección elpais.es.edgesuite.net [212.106.219.176]
sobre un máximo de 30 saltos:
  1   6 ms    <1 ms    <1 ms  10.0.2.2
  2   5 ms    1 ms    1 ms  SMBSHARE [192.168.1.1]
  3   *        *        *        Tiempo de espera agotado para esta solicitud.
  4   *        *        *        Tiempo de espera agotado para esta solicitud.
  5   *        *        *        Tiempo de espera agotado para esta solicitud.
  6   4 ms    4 ms    4 ms  74.217.106.212.static.jazztel.es [212.106.217.74]
  7   5 ms    4 ms    5 ms  253.216.106.212.static.jazztel.es [212.106.216.253]
  8   4 ms    4 ms    4 ms  176.219.106.212.static.jazztel.es [212.106.219.176]

Traza completa.

```

Miguel Ángel García Lara (CC BY-NC-SA)

Comando netstat

Netstat mostra todas as conexións activas no noso equipo e con que dirección remota están establecidas.

Coa opción –a, ademais das conexións establecidas, daríanos todos os portos que están abertos, escouitando (todas as portas abertas ao noso equipo), esperando peticións remotas.

Lembrar que cando por exemplo no navegador poñemos <http://www.elpais.es> estamos a utilizar o protocolo http que utiliza por defecto o porto 80. O que quere dicir que nos conectamos ao computador www.elpais.es polo porto 80. De feito, podíamos escribir no navegador: <http://www.elpais.es:80>

Ilustración Comando netstat.

```

Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>netstat
Conexiones activas

  Proto  Dirección local        Dirección remota      Estado
  TCP    10.0.2.15:49340       104.244.42.136:https ESTABLISHED
  TCP    10.0.2.15:49355       mad06s10-in-f170:https ESTABLISHED
  TCP    10.0.2.15:49357       68.232.35.172:https ESTABLISHED
  TCP    10.0.2.15:49361       90:http                ESTABLISHED
  TCP    10.0.2.15:49362       mad06s10-in-f14:https ESTABLISHED
  TCP    127.0.0.1:49360        www:21322             TIME_WAIT

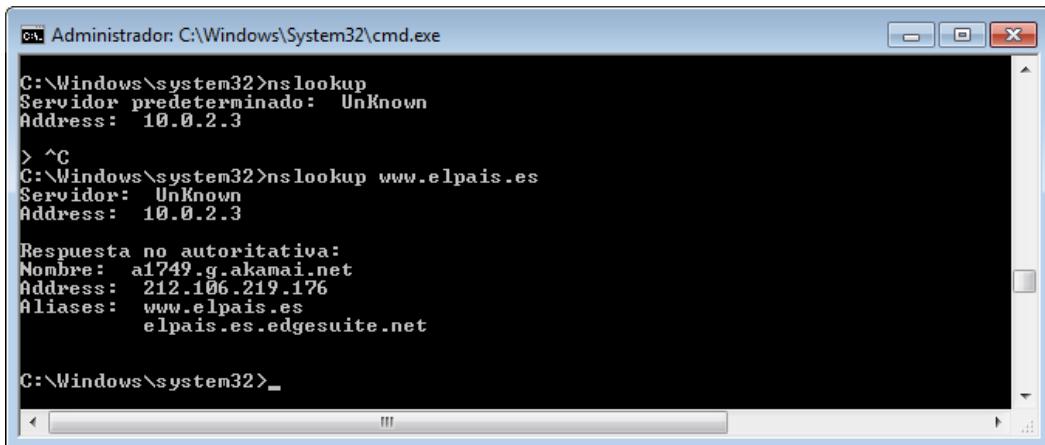
```

Miguel Ángel García Lara (CC BY-NC-SA)

Comando nslookup

O comando nslookup sen ningunha opción, devólvenos a dirección IP do noso servidor DNS. Tamén podemos pescudar a dirección IP de calquera páxina web. (ver captura).

Ilustración Comando nslookup



```
C:\Windows\system32>nslookup
Servidor predeterminado: Unknown
Address: 10.0.2.3

> ^C
C:\Windows\system32>nslookup www.elpais.es
Servidor: Unknown
Address: 10.0.2.3

Respuesta no autoritativa:
Nombre: a1749.g.akamai.net
Address: 212.106.219.176
Aliases: www.elpais.es
          elpais.es.edgesuite.net

C:\Windows\system32>
```

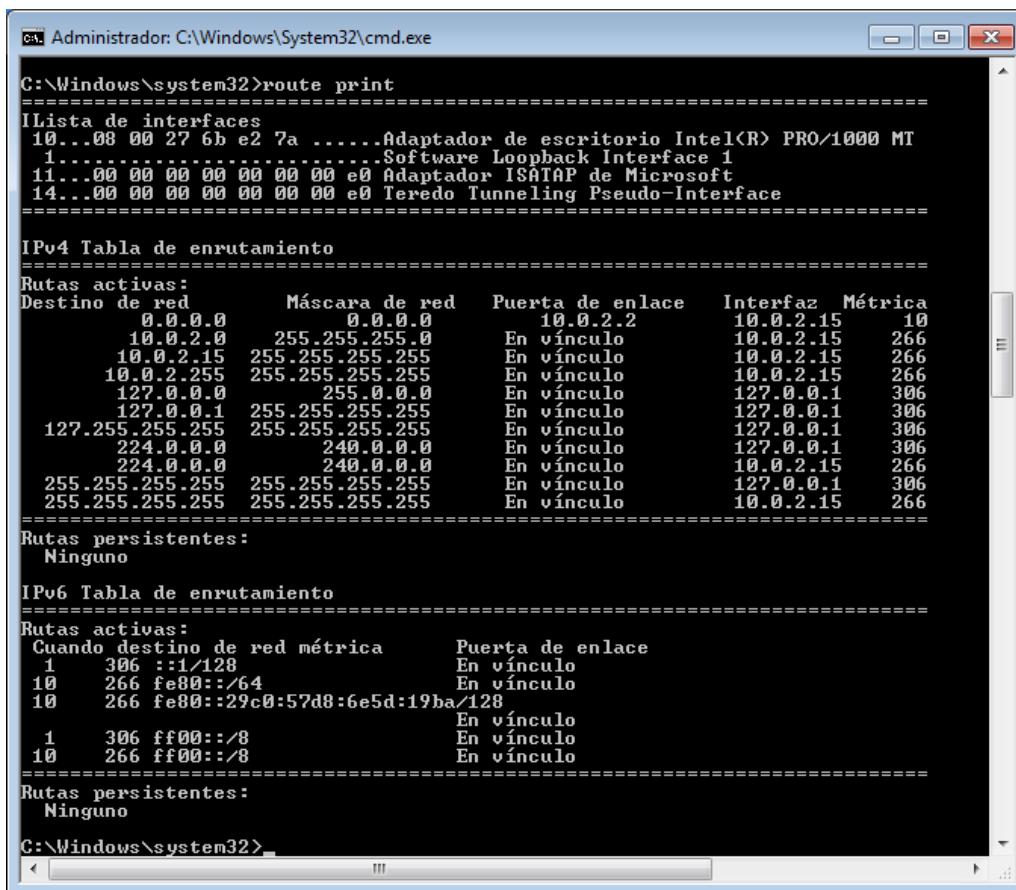
Miguel Ángel García Lara (CC BY-NC-SA)

Comando route

O comando route coa opción print, mostra a táboa de encamiñamento actual.

Con outras opcións, serve para configurar roteiros.

Ilustración de Comando route.



```
C:\Windows\system32>route print
=====
ILista de interfaces
10...00 00 27 6b e2 7a .....Adaptador de escritorio Intel(R) PRO/1000 MT
 1.....Software Loopback Interface 1
11...00 00 00 00 00 00 e0 Adaptador ISATAP de Microsoft
14...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red     Puerta de enlace   Interfaz   Métrica
          0.0.0.0          0.0.0.0        10.0.2.2       10.0.2.15    10
          10.0.2.0        255.255.255.255  En vínculo      10.0.2.15    266
          10.0.2.15       255.255.255.255  En vínculo      10.0.2.15    266
          10.0.2.255      255.255.255.255  En vínculo      10.0.2.15    266
          127.0.0.0        255.0.0.0       En vínculo      127.0.0.1    306
          127.0.0.1        255.255.255.255  En vínculo      127.0.0.1    306
          127.255.255.255 255.255.255.255  En vínculo      127.0.0.1    306
          224.0.0.0         240.0.0.0       En vínculo      127.0.0.1    306
          224.0.0.0         240.0.0.0       En vínculo      10.0.2.15    266
          255.255.255.255 255.255.255.255  En vínculo      127.0.0.1    306
          255.255.255.255 255.255.255.255  En vínculo      10.0.2.15    266
=====
Rutas persistentes:
  Ninguno

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica     Puerta de enlace
  1    306 ::1/128                 En vínculo
  10   266 fe80:::/64              En vínculo
  10   266 fe80::29c0:57d8:6e5d:19ba/128
                                En vínculo
  1    306 ff00::/8                En vínculo
  10   266 ff00::/8                En vínculo
=====
Rutas persistentes:
  Ninguno

C:\Windows\system32>
```

Miguel Ángel García Lara (CC BY-NC-SA)

5.13 Administración de redes GNU-Linux

5.13.1 Configuración de rede e router en Linux.

A unidade comeza coa configuración de 2 máquinas Linux en rede; configuraranse na mesma rede interna que as dúas máquinas de Windows.

Na primeira máquina Linux poñeránse dúas tarxetas de rede, unha en NAT coa máquina anfitrión pola que sae a Internet, e a outra en rede interna coas outras 3 máquinas. Esta máquina Linux realizará as funcións de router, de forma que as outras 3 máquinas tamén sairán a Internet.

No resto da unidade, estúdanse os distintos servizos de forma que nesta máquina router instalaranse distintos servizos: samba, nfs, ssh,...

Configuración de 2 máquinas Linux en Rede.

Este apartado é o primeiro exercicio da tarefa da unidade.

Paso 1. Clonar a máquina Linux utilizada en anteriores unidades

- Clonar con VirtualBox a máquina Linux utilizada en unidades anteriores. Realizar unha clonación completa e reiniciando a dirección MAC.
- Na máquina clonada, poñer como nome de máquina clienteLinux. Para iso, utilizar nano ou direccionamiento:
`root@sistemasubuntu:# echo clienteLinux > /etc/hostname`
- Editar o arquivo /etc/hosts e cambiar o nome da máquina (onde aparece SistemasUbuntu, cambialo por clienteLinux)

Observación: o arquivo /etc/hosts serve para configurar un DNS básico na rede local.

Paso 2. Configuración de rede en máquina Linux servidor.

A máquina orixinal Linux vai ter 2 tarxetas de rede para configurar un router:

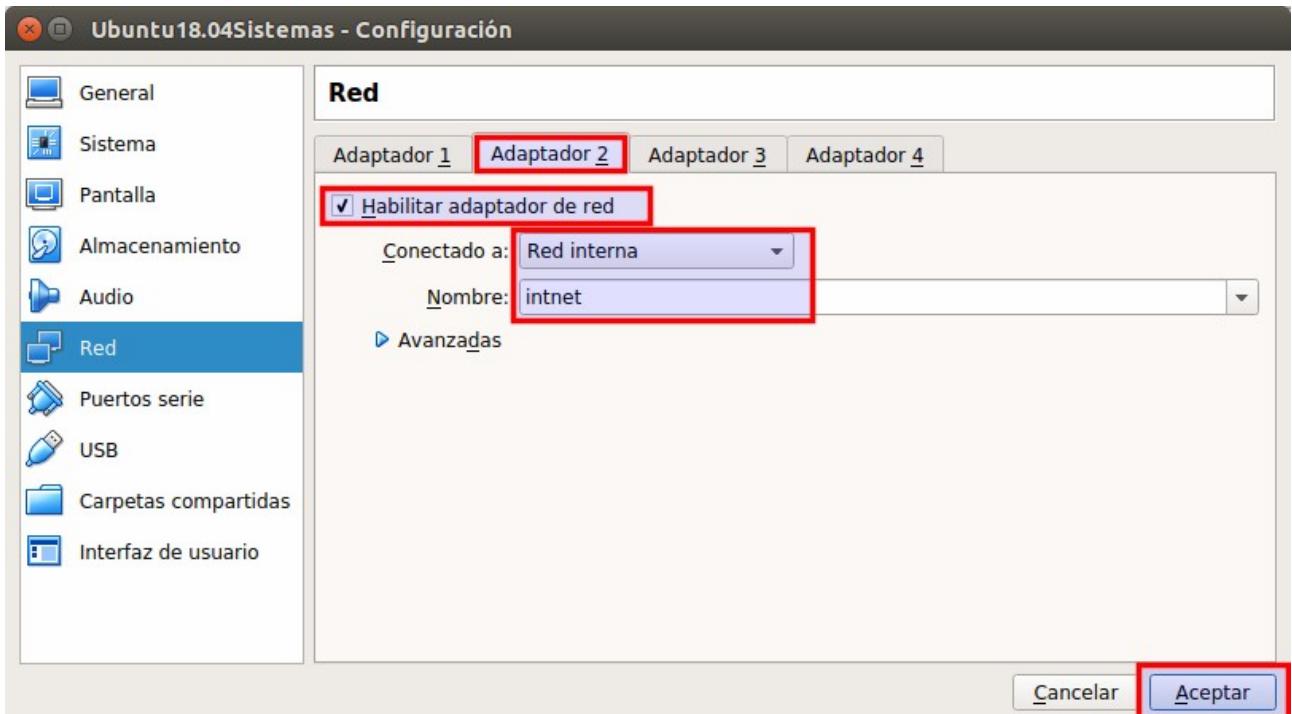
- A primeira tarxeta de rede, segue como ata o de agora, en NAT coa máquina anfitrión, saíndo a Internet a través dela.
- A segunda tarxeta de rede, poñerémola en rede interna para comunicarse coa outra máquina Linux.

1. Engadir segunda tarxeta de rede á máquina

En VirtualBox en configuración de Rede, habilitar adaptador 2 (pestana adaptador 2) e poñelo en rede interna, tal como aparece na imaxe.

Con esta operación, esta máquina xa se atopa na mesma rede física que as 2 máquinas Windows, (están no mesmo switch), pois o nome da rede interna non o cambiamos. Cando configuremos a IP configurarase de forma que esteán na mesma rede lóxica.

Ilustración que mostra como engadir unha segunda tarxeta de rede



Miguel Ángel García Lara (CC BY-NC-SA)

2. Nomes das tarxetas de rede en Linux. Comando ifconfig

Ao executar ifconfig ven os nomes asignados por Ubuntu ás tarxetas de rede e as súas direccións IP asignadas. Na captura que hai a continuación visualízase:

- Tarxeta enp0s3 (tarxeta de rede en NAT con maquina anfitrión) coa dirección IP 10.0.2.15
- Tarxeta enp0s8 (tarxeta de rede en rede interna, que comunicará con todas as máquinas restantes) sen dirección IP de momento.

Ilustración que mostra o comando ifconfig na máquina servidor

```
miguel@SistemasUbuntu:~
```

```
Archivo Editar Ver Buscar Terminal Ayuda
miguel@SistemasUbuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
          inet6 fe80::8fe6:b274:f65b:9eec prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:ff:a4:27 txqueuelen 1000 (Ethernet)
              RX packets 1197 bytes 1352426 (1.3 MB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 599 bytes 62488 (62.4 KB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet6 fe80::81c3:3f47:9cd4:3ff9 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:43:9a:4b txqueuelen 1000 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 216 bytes 35581 (35.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
```

Miguel Ángel García Lara (CC BY-NC-SA)

Observación: o comando ifconfig pode non estar instalado

A primeira vez que se executa ifconfig, en Ubuntu 18.04 di que non está instalado e que hai que instalar net-tools:

```
miguel@sistemasubuntu:$ ifconfig
```

Non se atopou a orde «ifconfig», pero pódese instalar con:

```
sudo apt install net-tools
```

```
miguel@sistemasubuntu:$ sudo apt install net-tools
```

....

Configurando net-tools (1.60+git20161116.90dá8a0-1ubuntu1)

```
miguel@sistemasubuntu:$
```

É posible, que mesmo dalgún erro ao instalar net-tools, porque non se actualizou nada no noso Ubuntu. Nese caso será necesario actualizar os paquetes instalados previamente. Executar os 2 comandos seguintes:

- Actualizar lista paquetes: #apt update
- Actualizar paquetes instalados: #apt upgrade

3. Configurar IP da segunda tarxeta de rede

A configuración das tarxetas de rede en Ubuntu atópase no directorio /etc/network.

O ficheiro para configurar as direccións IP chámase interfaces. A continuación, engádese a configuración IP da tarxeta de rede enp0s8 en rede interna.

```
root@sistemasubuntu:# nano /etc/network/interfaces
```

```
# interfaces(5) file used by ifup(8) and ifdown(8)
```

```
auto o
```

```
iface o inet loopback
```

Engadir as liñas seguintes no arquivo:

```
#ip estática en enp0s8
```

```
auto enp0s8
```

```
iface enp0s8 inet static
```

```
address 192.168.100.103
```

```
netmask 255.255.255.0
```

```
network 192.168.100.0
```

```
broadcast 192.168.100.255
```

Reiniciar a rede e comprobar que funciona enps08

Para que teña efecto o cambio, reiníciase o servizo de rede.

```
root@sistemasubuntu:# service networking restart
```

```
root@sistemasubuntu:# ifconfig #vemos que enp0s8 ten a nova dirección IP asignada
```

```
root@sistemasubuntu:# ping 192.168.100.103
```

#debe responder afirmativamente comprobando que hai conectividade de rede no propio equipo.

```
root@sistemasubuntu:# ping 8.8.8.8
```

#responde pois, temos conexión a Internet e esta dirección IP existe. Esta dirección IP corresponde ao servidor DNS de Google.

Paso 3. Configuración en máquina clienteLinux

Esta máquina só ten unha tarxeta de rede. Configurar en VirtualBox a tarxeta en rede interna.

Ao executar ifconfig obsérvase que só hai unha interface de rede co nome enps03. Configúrase a dirección IP no arquivo interfaces:

```
root@clientelinux:# nano /etc/netwok/interfaces
```

.....

#Engádense as liñas seguintes ao final do arquivo:

```
#ip estática en enp0s3
auto enp0s3
iface enp0s3 inet static
address 192.168.100.104
netmask 255.255.255.0
network 192.168.100.0
broadcast 192.168.100.255
gateway 192.168.100.103
```

Lembrar que a porta de ligazón ou gateway é a dirección IP pola que nos comunicamos con outras redes. Na primeira máquina Linux non había que engadir porta de ligazón, pois sae a Internet directamente. Pero esta segunda máquina Linux, sairá a Internet a través da primeira, configurando como porta de ligazón (gateway) a súa dirección IP.

Para que teña efecto o cambio, reiníciase o servizo de rede:

```
root@clientelinux:# service networking restart
```

Ademais, a primeira máquina Linux ten outra tarxeta de rede, con IP 10.0.2.15 que sae a Internet. No seguinte apartado, configúrase para que esta máquina sexa un router; de forma que todas estas máquinas poidan saír a Internet a través da máquina SistemasUbuntu.

Comprobacións de que a nova conexión funciona:

```
root@clientelinux:# ifconfig #vemos que enp0s3 funciona con nova ip
```

```
root@clientelinux:# ping 192.168.100.104
```

#nosa propia ip responde ao ping.

```
root@clientelinux:# ping 192.168.100.103 #responde a outra máquina linux
```

root@clientelinux:# ping 8.8.8.8 #non responde, pois aínda que se configurou a porta de ligazón, a primeira máquina aínda non está configurada como router, polo que non comunica as 2 redes.

Observación

Agora hai 4 máquinas na mesma rede:

As 2 máquinas Windows con IP 192.168.100.101 e 192.168.100.102

As 2 máquinas Linux con IP 192.168.100.103 e 192.168.100.104

Todas coa máscara 255.255.255.0

Configuración de rede en Ubuntu 18.04

Na versión Ubuntu 18.04, a empresa Canonical introduciu un servizo de rede networkd cuxo obxectivo é xestionar a rede con scripts (versión Ubuntu 18.04 Server) ou gráficamente (network-manager, en versión Ubuntu 18.04 Desktop).

Neste libro, utilizouse a configuración tradicional baseada en arquivo /etc/network/interfaces para a configuración das distintas tarxetas e o arquivo /etc/resolv.conf para os servidores DNS.

Resumo de parámetros da rede

- Arquivo con nome do equipo: /etc/hostname
- Arquivo de configuración das conexións: /etc/network/interfaces
- Arquivo onde se configura DNS: /etc/resolv.conf
- Arquivo para establecer DNS local: /etc/hosts

5.13.2 Encamiñamento en Linux

Neste apartado vai habilitar o encamiñamento na máquina SistemasUbuntu. Activarase regra iptables para permitir o tráfico, de forma que o resto das máquinas saian a Internet a través do router SistemasUbuntu.

Este contido é o exercicio 2 da tarefa.

Paso 1. Habilitar router en máquina SistemasUbuntu.

En primeiro lugar actívase o servizo de encamiñamento de Linux. Para iso actívase ip_forward da forma seguinte:

```
root@sistemasubuntu:# cat /proc/sys/net/ipv4/ip_forward
```

```
0
```

```
root@sistemasubuntu:# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Co comando echo, substituímos un 0 por 1 dentro do arquivo. Desta forma, dicimos á máquina que vai a enrutar.

En segundo lugar actívase unha regra iptables, servizo de devasa de Linux, que diga que deixa pasar todo o tráfico.

```
root@sistemasubuntu:# iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -d 0/0 -j  
MASQUERADE
```

Con esta regra, non hai restrición de tráfico. Se quixésemos restriccións de tráfico, teríamos que habilitar más regras iptables.

Paso 2. Comprobar encamiñamento en máquina clienteLinux

Para comprobar que a máquina SistemasUbuntu xa está enrutando, execútase ping na máquina clienteLinux cara ao exterior:

```
root@clientelinux:# ping 8.8.8.8 #Responde, xa hai comunicación con Internet
```

```
root@clientelinux:# ping www.elpais.es #Non responde, pois non se configurou a dirección IP do servidor DNS.
```

#Non hai ningún equipo na nosa rede que traduza www.elpais.es á IP concreta.

Configurar DNS en máquinas Linux

Cando se utilizan direccións IP estáticas, ademais da máscara de rede, débese configurar a porta de ligazón e os servidores DNS a utilizar. Neste caso, decidiuse configurar como DNS os propios servidores DNS de Google con direccións IP 8.8.8.8 (DNS primario) e IP 8.8.4.4 (DNS secundario). Sempre se configuran 2 servidores DNS por se o primeiro falla na conexión.

Para realizalo, executar:

```
root@clientelinux:# mv /etc/resolv.conf /etc/resolv.conf.old
```

#Gardamos o arquivo resolv.conf orixinal con outro nome, por se nun futuro queremos ter o arquivo orixinal. A continuación insérense os 2 DNS no arquivo.

```
root@clientelinux:# echo nameserver 8.8.8.8 > /etc/resolv.conf
```

```
root@clientelinux:# echo nameserver 8.8.4.4 >> /etc/resolv.conf
```

```
root@clientelinux:# cat /etc/resolv.conf
```

nameserver 8.8.8.8

nameserver 8.8.4.4

```
root@clientelinux:# ping www.elpais.es #xa responde afirmativamente, pois o servidor DNS sabe que IP ten o servidor www.elpais.es
```

Paso 3. Realizar un script con inicio automático, para que o encamiñamento inície sempre.

Se reiniciamos a máquina SistemasUbuntu, xa non enrutará. É dicir, a máquina clienteLinux xa non responde afirmativamente a ping 8.8.8.8.

Como solucionalo?

Crear un script cos comandos do paso 1. Este script executarase sempre que se inicie o equipo de forma automática.

En Ubuntu o arquivo /etc/rc.local execútase sempre que se inicia GNU-Linux.

En Ubuntu 18.04 este arquivo non existe, pero creámolo e introducimos os comandos vistos:

```
root@sistemasubuntu:# nano /etc/rc.local
```

#Escríbense as 4 liñas seguintes:

```
#!/bin/bash
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -d 0/0 -j MASQUERADE
```

```
exit 0 #Sempre debe ser a última liña do script rc.local
```

```
root@sistemasubuntu:# chmod +x /etc/rc.local
```

#Cámbiase permisos ao arquivo para que sexa executable.

```
root@sistemasubuntu:# reboot
```

#Ao reiniciar o equipo, execútase rc.local, de forma que esta máquina xa enruta en todo momento. Comprobar que clienteLinux responde ben a ping www.elpais.es

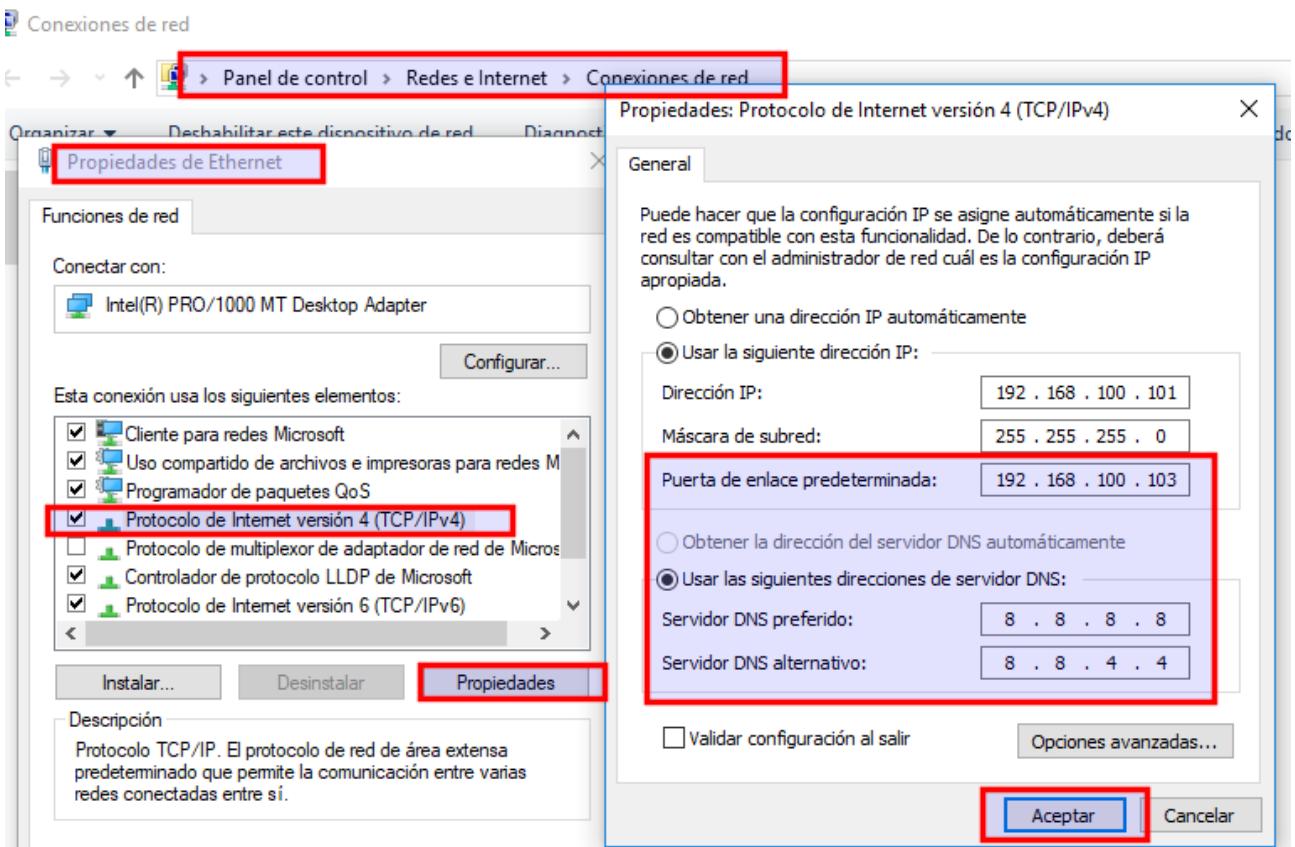
Paso 4. Saída a Internet de máquinas Windows cliente1 e cliente2

Para que as máquinas Windows da unidade 9 saian a Internet, só falta configurar nelas a porta de ligazón e o servidor DNS que no seu momento deixámos en branco segundo captura.

Configurar como porta de ligazón a máquina SistemasUbuntu: 192.168.100.103

Configurar como DNS os servidores de Google, 8.8.8.8 e 8.8.4.4.

Ilustración que mostra como se configura porta de ligazón e DNS



Miguel Ángel García Lara (CC BY-NC-SA)

Ter en conta que segundo a memoria RAM da máquina anfitrión é posible que só se poidan ter 2 ou 3 máquinas virtuais acesas. Reconfigurar se é necesaria a memoria de cada máquina en VirtualBox. Se as máquinas son de 64 bits, deixar 1600 MB en cada unha. Se son de 32 bits, só 1024 MB.

Nesta unidade, para realizar as prácticas sempre terá que estar acendida a máquina SistemasUbuntu, e algunha máis como mínimo.

5.13.3 Servizos e comandos TCP/IP en GNU-Linux.

Servizos en GNU-Linux

Os servizos en Linux configúranse cun arquivo de texto, normalmente con extensión "conf". Así, unha vez instalado o servizo web Apache configúrase no arquivo /etc/apache2/apache2.conf

Os servizos en Linux pódense parar e iniciar co comando service. Hai 4 opcións: stop, start, restart, status.

Como exemplo, para o servizo networking (servizo de rede) pódese executar:

```
# service networking start #iniciar servizo de rede  
# service networking stop #parar servizo de rede  
# service networking restart #reiniciar servizo de rede
```

service networking status #informa se o servizo está a executarse ou está parado. Cando se está executando, aparece a palabra running (en cor verde).

Comandos TCP/IP en Linux

Os comandos TCP/IP como din o seu nome, non son exclusivos de Windows ou Linux, senón do protocolo TCP. Por iso é polo que os comandos realizan a mesma acción e só cambia o nome algúns lixeiramente. A relación en Linux son:

- ifconfig /all (equivale a ipconfig en Windows)
- ping
- hostname
- arp
- traceroute (equivale a tracert en Windows)
- netstat
- nslookup
- route

5.13.4 Servizo SAMBA

O servizo SAMBA serve para compartir recursos entre máquinas Windows e Linux, para iso utilizase o protocolo SMB, que é o que se encarga de compartir recursos en Windows. Se só compártense recursos entre máquinas Linux, o servizo nativo para ese fin é o servizo NFS que se verá en libro seguinte desta mesma unidade.

Características do servizo Samba

- Utilízanse os portos 137, 138, 139 e 443. Portos 137 e 138 con protocolo UDP e 139 e 443 con protocolo TCP.
- Os servizos en Linux, configúranse nun arquivo. No caso de Samba o arquivo de configuración é /etc/samba/smb.conf
- Cando se teña o recurso compartido, desde un cliente Linux, poderemos acceder ao recurso co comando mount e sistema de ficheiros cifs; desde un cliente Windows, a través do explorador en Rede ou co roteiro UNC.

O servizo Samba instálase e configura no exercicio 3 da tarefa.

Paso 1. Instalación do servidor Samba. En máquina router.

Instalar SAMBA, cos 2 paquetes seguintes (vai instalar a versión 4.3 que se atopa en repositorios de Ubuntu 18.04):

```
root@sistemasubuntu:# apt-get install samba samba-common-bin
```

Comprobar se está activo SAMBA. Para iso, hai que saber que SAMBA está composto de 2 demos: smbd e nmbd. Comprobamos con service que están a correr. Verase running en verde:

```
root@sistemasubuntu:# service smbd status
```

- nmbd.service - LSB: start Samba NetBIOS nameserver (nmbd)

```
Loaded: loaded (/etc/init.d/nmbd; bad; vendor preset: enabled)
```

```
Active: active (running) since dom 2018-04-22 23:30:15 CEST; 2s ago
```

```
..... (para saír pulsar q)
```

```
root@sistemasubuntu:# service nmbd status
```

Paso 2. Configuración do arquivo /etc/samba/smb.conf

Editar o arquivo smb.conf e onde aparece workgroup, encher o nome do grupo de traballo das túas máquinas windows da unidade 9. (Se aparecese a liña comentada habería que descomentárla)

workgroup = Nome_GRUPO_TRABALLO

Para este exemplo, van compartir 2 recursos. Un cartafol público para todos os usuarios, con permisos de só lectura e outra privada para algúns usuarios, con permisos de lectura e escritura. Para iso, **engadir ao final de arquivo smb.conf**:

```
[publico]
```

```
path = /samba/lectura
```

```
browsable = yes
```

```
guest ok = yes
```

```
read only = yes
```

```
[escritura]
```

```
path = /samba/escritura
```

browseable = yes

guest ok = non

writeable = yes

valid users = @samba

Significado das distintas etiquetas:

- A etiqueta browseable = yes, serve para que os usuarios conectados, poidan ver no explorador o recurso, senón é un recurso secreto.
- No recurso lectura permitiuase o acceso a invitados (guest ok = yes), con todo, no recurso escritura non (guest ok = non)
- En escritura, permitiuase o acceso aos usuarios que pertenzan ao grupo samba do noso Linux (valid users = @samba). Tamén se podería poñer usuarios concretos, sen utilizar @. Por exemplo para permitir acceso a juan e aos usuarios do grupo samba especificase:
- valid users = juan, @samba

Paso 3. Creación de usuario, grupos, cartafoles e permisos na máquina servidor.

Imos crear o grupo samba, e introducir no devandito grupo aos usuarios juan e juana. (juan é un usuario novo, e juana un usuario dos creados na práctica da unidade 9)

```
root@sistemasubuntu:# adduser juan
```

```
root@sistemasubuntu:# addgroup samba
```

```
root@sistemasubuntu:# adduser juan samba
```

```
root@sistemasubuntu:# adduser juana samba
```

#Creamos a cartafol samba e subcarpetas lectura e escritura. Cambiamos a propiedade do cartafol ao grupo samba, e os seus permisos, de forma que poidan gardar cambios todos os usuarios do grupo.

```
root@sistemasubuntu:# mkdir /samba
```

```
root@sistemasubuntu:# mkdir /samba/lectura
```

```
root@sistemasubuntu:# mkdir /samba/escritura
```

```
root@sistemasubuntu:# chgrp samba -R /samba
```

```
root@sistemasubuntu:# chmod 770 -R /samba
```

Todos estes comandos son comandos de administración de Linux explicados nas unidades 5 e 6. Agora, utilizanxe comandos específicos de Samba, para engadir aos usuarios juan e juana como usuarios do servizo samba. Para iso:

```
root@sistemasubuntu:# smbpasswd -a juan
root@sistemasubuntu:# smbpasswd -a juana
```

Unha vez realizados cambios nos arquivos de configuración de calquera servizo, hai que reinicialo para que produzan efecto os cambios. No caso de Samba, reiniciamos os 2 demos:

```
root@sistemasubuntu:# service smbd restart
root@sistemasubuntu:# service nmbd restart
```

5.13.5 Conexión desde máquinas cliente

Conexión desde máquinas clientes Windows

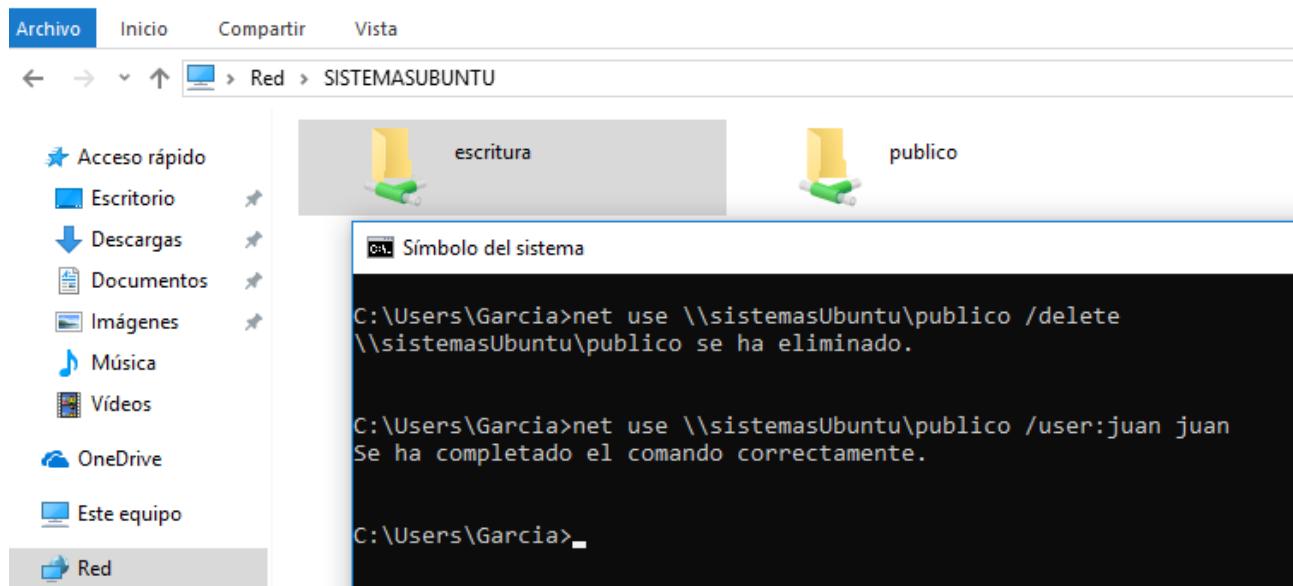
Iniciar máquina cliente1 da unidade 9. Lembra, que configuramos en arquivo de samba, o nome do grupo de traballo. Conectar á máquina a traves do explorador con Rede ou co roteiro UNC \\SistemasUbuntu. Abrirase a xanela cos recursos compartidos lectura e escritura.

Ao pulsar dobre clic para realizar a conexión solicítase usuario, conectar con juan.

Se sae a mensaxe de que non se ten acceso, executar os 2 comandos que ven na captura.

A continuación accédese a ambos os cartafoles, cos permisos correctos.

Ilustracion que mostra o acceso cliente Samba en Windows



Miguel Ángel García Lara (CC BY-NC-SA)

Conexión desde máquinas clientes Linux

Para realizar a conexión desde a máquina “clienteLinux” seguir os pasos seguintes:

Instalar software para o cliente:

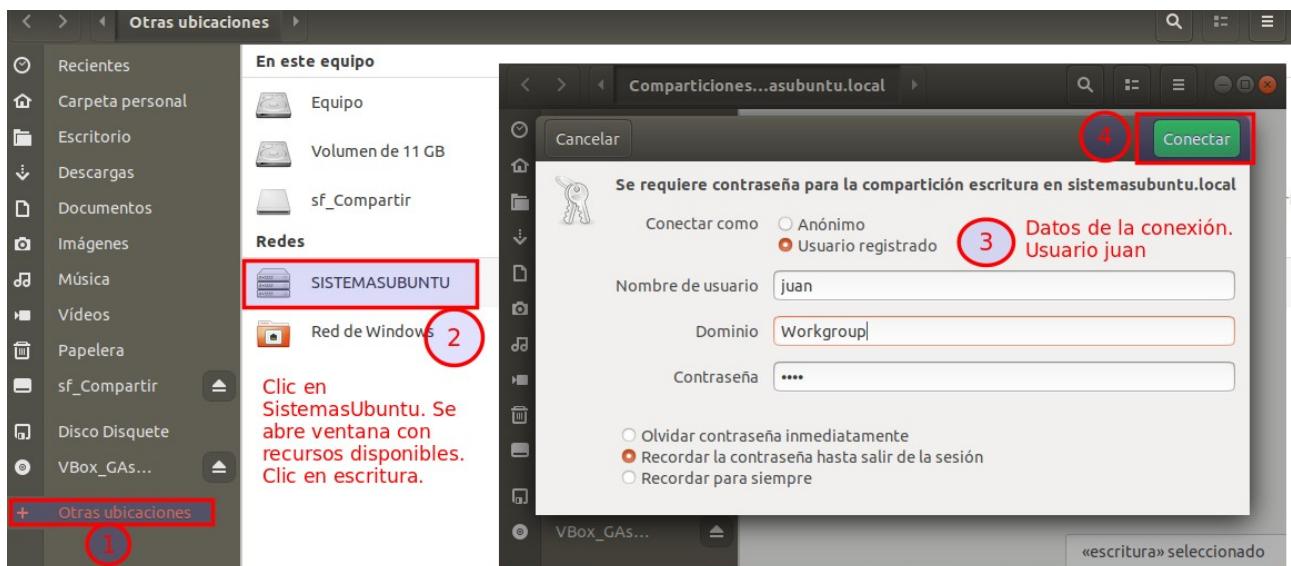
```
root@clientelinux:# apt install samba-common-bin
```

```
root@clientelinux:# apt install cifs-utils
```

Realizar conexión gráfica

Desde o explorador de archivos Nautilus, se pulsamos en REDE, xa se ve a máquina SistemasUbuntu. Na captura realizase unha conexión ao recurso escritura co usuario juan.

Ilustración que mostra como se accede desde un cliente a samba



Miguel Ángel García Lara (CC BY-NC-SA)

Realizar conexión desde terminal. Comando mount:

```
root@clientelinux:# mkdir /mnt/escritura
```

#Utilízase o comando mount, con sistema de ficheiros cifs e usuario juan.

```
root@clientelinux:# mount -t cifs -ou user=juan,pass=clave //192.168.100.103/escritura /mnt/escritura
```

```
root@clientelinux:# mkdir /mnt/escritura/cartafol2
```

#Creouse cartafol2 en servidor Linux

Que facer para que o usuario non teña que utilizar o comando mount cada vez que se conecte?

Engádese en /etc/fstab a liña de montaxe automática (na unidade 6)

```
root@clientlinux:# nano /etc/fstab
```

#Engadir ao final do arquivo a liña seguinte:

```
//192.168.100.103/escritura /mnt/escritura cifs rw,username=juan 0 0
```

#Ao iniciar o equipo, antes de comenzar sesión en GNU-Linux pregúntase usuario de acceso aos recursos de Samba.

5.13.6 Servizo NFS.

Instalación e configuración do servidor NFS

O servizo NFS comparte recursos entre máquinas Linux, sen ser compatible con máquinas Windows. O servizo NFS é más seguro que Samba.

Unha vez instalado o servizo, configuraranse os cartafolos para compartir no arquivo de configuración /etc(exports. A continuación reiníciase o servizo.

Para a conexión dos clientes utilízase o comando mount.

O servizo NFS instálase e configura no exercicio 4 da tarefa.

Paso 1. Instalar servidor NFS

```
root@sistemasubuntu:# apt install nfs-kernel-server
```

Paso 2. Configurar que recursos se comparten no arquivo /etc/exports

```
root@sistemasubuntu:# nano /etc/exports
```

#Engadir ao final do ficheiro as 2 liñas seguintes:

```
/nfs/escritura 192.168.100.104(rw)
```

```
/nfs/lectura 192.168.100.0/24(ro)
```

#A primeira liña comparte con escritura (read write) exclusivamente ao equipo 192.168.100.104.

#A segunda liña comparte só lectura (read only) a todos os equipos da nosa rede (observa que queda totalmente definida, pois se pon a dirección de rede e os bits da máscara).

Paso 3. Créanse os cartafolos e cámbianse os propietarios ao usuario nobody e grupo nogroup

```
root@sistemasubuntu:# sudo mkdir /nfs
root@sistemasubuntu:# sudo mkdir /nfs/lectura
root@sistemasubuntu:# sudo mkdir /nfs/escritura
#Para que non haxa problema de acceso, o cartafol ten que pertencer ao usuario nobody
e ao grupo nogroup (usuario e grupo xenéricos de Linux para servizos)
root@sistemasubuntu:# sudo chown -R nobody /nfs
root@sistemasubuntu:# sudo chgrp -R nogroup /nfs
#Créase un arquivo na cartafol lectura
root@sistemasubuntu:# echo ola > /nfs/lectura/saúdo.txt
#Cámbianse os permisos, de forma que poidan realizar todos os cambios no cartafol o
usuario e grupos propietarios:
root@sistemasubuntu:# chmod -R 770 /nfs
# Reiníciase o servidor, desa forma lese o arquivo /etc(exports e comproba a existencia
dos directorios compartidos.
root@sistemasubuntu:# service nfs-kernel-server restart
```

5.13.7 Cliente NFS

Instalar cliente NFS en equipo clienteLinux e montar recurso con mount

Instalar cliente NFS

```
root@clientelinux:# apt install nfs-common
```

Crear as cartafol onde se van a montar os recursos

```
root@clientelinux:# mkdir /mnt/nfs
root@clientelinux:# mkdir /mnt/nfs/lectura
root@clientelinux:# mkdir /mnt/nfs/escritura
```

Montar o recurso de lectura. Comprobar que se ten lectura e non escritura

```
root@clientelinux:# mount -t nfs 192.168.100.103:/nfs/lectura /mnt/nfs/lectura
# Compróbase que se pode ler o arquivo saúdo.txt creado no servidor
root@clientelinux:# ls -l /mnt/nfs/lectura
total 4
```

```
-rw-r--r-- 1 root root 5 abr 23 11:56 saúdo.txt
root@clientelinux:# cat /mnt/nfs/lectura/saúdo.txt
ola
# Compróbase que non se pode escribir:
root@clientelinux:# echo soyCliente > /mnt/nfs/lectura/cliente.txt
bash: /mnt/nfs/lectura/cliente.txt: Sistema de archivos de sólo lectura
```

Montar o recurso de escritura. Compróbase que se pode escribir

```
root@clientelinux:# mount -t nfs 192.168.100.103:/nfs/escritura /mnt/nfs/escritura
root@clientelinux:# echo soyCliente > /mnt/nfs/escritura/cliente.txt
```

Arquivo /etc/fstab liñas para non montar cada vez que se inicia o PC

Para non ter que utilizar o comando mount en cada sesión, engádense as liñas correspondentes no arquivo /etc/fstab

```
root@clientelinux:# sudo nano /etc/fstab
```

#Engadir as 2 liñas seguintes:

192.168.100.103:/nfs/lectura	/mnt/nfs/lectura	nfs	ro,intr,x-gvfs-show	0
0				
192.168.100.103:/nfs/escritura	/mnt/nfs/escritura	nfs	rw,intr,x-gvfs-show	0
0				

Observacións sobre as opcións:

Móntase con sistema nfs, e as opcións son:

ro/rw (read only/ read write segundo permiso en cartafol de servidor)

intr: evita bloqueo en caso de erro

x-gvfs-show: que se monte gráficamente, ademais de terminal

Ao iniciar o equipo, ademais de ter acceso en terminal, no explorador de arquivos Nautilus, haberá un acceso directo aos 2 cartafoles.

5.13.8 Servizo ssh

Accesos remotos

O servizo acceso remoto consiste en acceder desde un equipo a outro da rede, e traballar coma se fisicamente estivésese nel. Os servizos más utilizados para acceder de forma remota a un sistema GNU/Linux son:

- Telnet. Permite acceder ao sistema de forma remota por terminal, pero dunha maneira non segura.
- Open SSH. Permite acceder ao sistema por terminal, pero de forma segura xa que se cifran as comunicacóns. Ademais, permite transferir arquivos.
- VNC. Mientras que os servizos telnet e SSH permiten conectarse ao servidor por medio dun terminal, o servidor VNC permite utilizar o servidor utilizando o escritorio instalado no sistema: GNOME ou KDE.

Parámetros de ssh e instalación

- O servizo ssh pódese instalar tanto en Windows como en Linux. Igualmente pódese acceder con clientes de ambos os sistemas.
- O servizo ssh utiliza o porto 22.
- Os usuarios de conexión, son os propios da máquina Linux onde está instalado o servidor.
- O servizo ssh ten dúas vantaxes moi importantes con respecto ao servizo Telnet:
 - O servizo ssh é seguro a diferenza de telnet.
 - O servizo ssh ademais de acceso remoto permite a transferencia de ficheiros coa utilidade scp.

Para instalar o servidor ssh execútase na máquina servidor:

```
root@sistemasubuntu:# apt install ssh  
#Comprobamos que xa se está executando  
root@sistemasubuntu:# service ssh status
```

No **arquivo de configuración /etc/ssh/sshd_config** configúranse usuarios e/ou equipos cliente que se lles permite conectar.

Neste caso, non lle imos a configurar. Por defecto permítense conectar desde toda a rede e todos os usuarios do equipo.

Conexión desde equipos cliente

No cliente non hai que instalar nada, simplemente conectarse con:

```
$ ssh user@ip
```

```
$ ssh user@nombre_Equipo
```

Está a utilizarse acceso remoto, de forma que fisicamente vaise a traballar na máquina clienteLinux, pero controlando a máquina servidor SistemasUbuntu. Polo que teremos que conectarnos cun usuario da máquina servidor. Se nos conectamos cun usuario e password configurado en ambas as máquinas, bastará para realizar a conexión con: \$ ssh IP

Exemplo de conexión

```
miguel@clientelinux:$ ssh 192.168.100.103
```

```
#conectar ao servidor como miguel
```

```
.....  
miguel@192.168.100.103's password:
```

```
.....  
miguel@sistemasubuntu:$ exit
```

#obsérvase que a propia shell di que a máquina actual é SistemasUbuntu. Pódese executar calquera comando coma se estivésese fisicamente en SistemasUbuntu.

```
#Ao escribir exit, sáese da sesión, e vólvese ao equipo cliente.
```

```
logout
```

```
Connection to 192.168.100.103 closed.
```

```
miguel@clientelinux:$ ssh juan@192.168.100.103
```

#Volve realizar conexión ao servidor, agora como juan. O usuario juan existe na máquina servidor, pero non na máquina cliente.

```
juan@192.168.100.103's password:
```

```
.....  
#Pregúntase quen está conectado (who). Devolve o usuario miguel na propia máquina SistemasUbuntu e o usuario juan, desde a rede, desde a máquina 192.168.100.104
```

```
juan@sistemasubuntu:$ who
```

```
miguel :0 2019-04-16 20:21 (:0)
```

```
juan pts/1 2019-04-17 22:52 (192.168.100.104)
```

```
juan@sistemasubuntu:$ exit #Saír de ssh
```

```
logout
```

```
Connection to 192.168.100.103 closed.
```

Transferir arquivos con comando scp.

O servizo ssh, incorpora o comando scp para copiar ficheiros da máquina servidor á máquina cliente, ou viceversa. Dito doutra forma, o servizo ssh incorpora co comando scp un servizo ftp que ademais é seguro e coñécese como sftp.

Observación

O comando scp utilízase sen necesidade de realizar unha conexión previa ao servidor.

Sintaxe

scp [-r] [orixe] [destino]

onde, orixe ou destino fórmano: [usuario@maquina:arquivo]

A opción –r é de recursiva para enviar ou recibir un cartafol completo.

Exemplo para enviar:

```
$ scp practica.odt juan@192.168.100.103:/home/juan/practica.odt
```

Envíase o arquivo practica.odt ao servidor ssh 192.168.100.103

Exemplo para recibir

```
$ scp juan@192.168.100.103:/home/juan/practica.odt nome.odt
```

Recíbese o arquivo practica.odt desde o servidor ssh 192.168.100.103

5.13.9 Servizo Web: Apache

Instalación e configuración do servizo web Apache

Neste apartado vai explicar a configuración do servidor web Apache. Apache pódese instalar tanto en Windows como en Linux. Na tarefa non se incluíu ningún exercicio relacionado con Apache, non pola súa pouca importancia, senón por instalar xa un servizo web en Windows.

Hai 20 anos creouse o "Apache Software Foundation". Esta fundación fórmana desarrolladores de software onde cada un realiza os seus propios proxectos de código aberto.

Páxina de Apache: <http://www.apache.org/>

Páxina da fundación de software de Apache:

https://es.wikipedia.org/wiki/Apache_Software_Foundation

Para instalar Apache en GNU-Linux: # **apt-get install apache2**

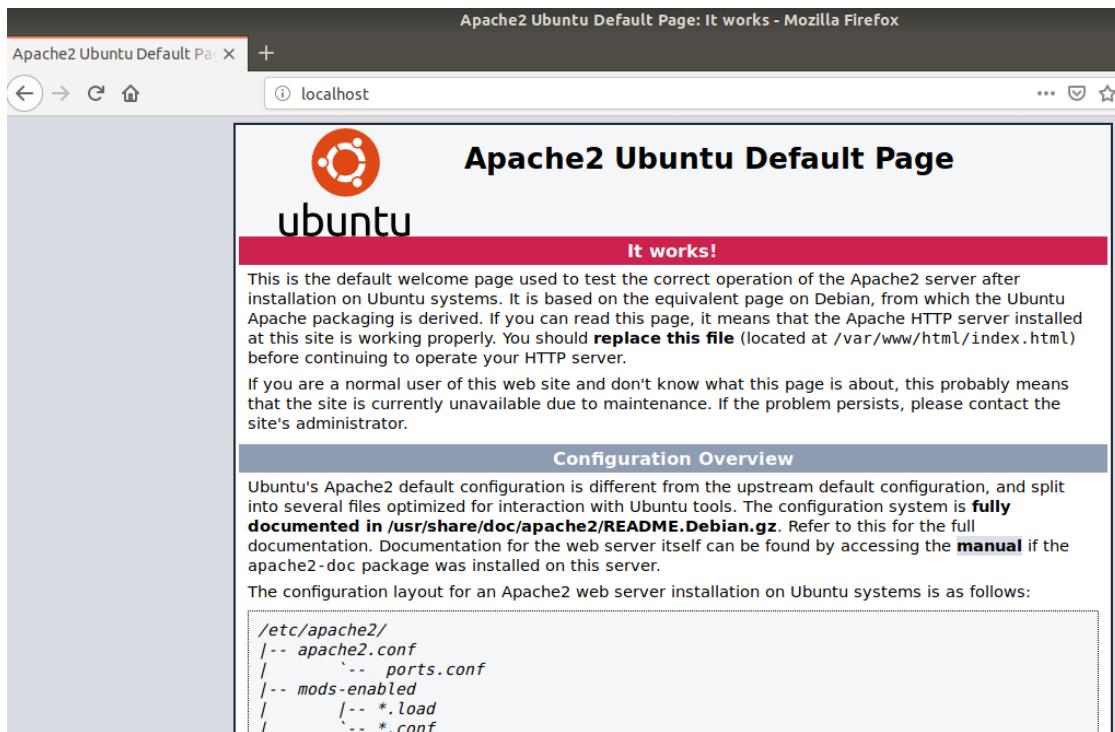
Unha vez instalado, xa está a funcionar Apache. Para comprobalo, executar: #**service apache2 status**

Xa se pode navegar e ver a páxina por defecto do servidor web Apache:

- Desde o equipo servidor, escribir no navegador: `http://localhost`
- Desde outra máquina, escribir no navegador: `http://IP_servidor`

Apache devolve a páxina por defecto `index.html` aloxada no directorio `/var/www/html`

Ilustración que mostra a páxina por defecto de Apache



Miguel Ángel García Lara (CC BY-NC-SA)

Configuración do servidor Apache

A configuración de apache almacénase no **directorio de configuración /etc/apache2**.

A continuación ven as **opcións de configuración** más importantes:

- O arquivo `/etc/apache2/apache2.conf` ten a configuración global do servidor.
- O arquivo `/etc/apache2/ports.conf` Permite establecer os portos de escoita de Apache, por defecto porto 80 para http e porto 443 para https.

`Listen *:80`

`Listen *:443`

- O * significa que pode realizar a petición calquera computador.

No mesmo servidor pódense ter varios sitios web, para iso, na cartafol `/etc/apache2/sites-available` se garda a configuración de cada un nun arquivo. Por defecto atopanse os sitios default e default-ssl. Cada sitio (ou arquivo) ten a seguinte estrutura:

```

<VirtualHost *:80>
    ServerAdmin servermaster@localhost
    Servername www.miempresa.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html default.html
</VirtualHost>

```

Onde o significado destas 4 directivas é o seguinte:

- ServerAdmin é o correo electrónico do administrador do sitio web.
- Servername é o nome FQDN do sitio web. Para o dominio por defecto (arquivo default) non se indica ningún nome, polo que a liña déixase comentada. Pero para outros dominios (por exemplo, www.miempresa.com) si se debe establecer.
- DocumentRoot. Indica a localización onde se atopa as páxinas web do sitio.
- DirectoryIndex. Indica o nome dos ficheiros que envía por defecto o servidor web. No exemplo, significa, que cando no navegador escribase http://IP_servidor devólvese a páxina /var/www/html/index.html

Exemplo de creación dun novo sitio web

Nun servidor web Apache pódense aloxar distintas páxinas web ou sitios web. Por defecto o servidor web publica o directorio /var/www/html para todos os dominios pero é posible personalizar de forma independente cada dominio.

- Para engadir o dominio www.miempresa.com que se aloxe na cartafol /portais/miempresa hai que crear o ficheiro /etc/apache2/sites-available/miempresa.com co seguinte contido:

```

<virtualhost *:80>
    ServerName www.miempresa.com
    DocumentRoot /portais/miempresa
    DirectoryIndex index.html index.htm
</virtualhost>

```

- Activar o sitio

```
# a2ensite miempresa.com
```

- Reiniciar o servidor web

```
# service apache2 restart
```

Páxina de inicio do servidor https

Co auxe dos negocios na internet popularizouse o uso de comunicacóns cifradas entre os clientes e o servidor Web, sendo a tecnoloxía de encriptación máis utilizada o Security Socket Layer (SSL).

Por defecto vén instalado en Apache, polo que para utilizar unha páxina segura baixo https en Apache só hai que:

- Activar o módulo ssl
- Activar o sitio default-ssl
- Reiniciar o servidor web

Unha vez reiniciado o servidor, accédese desde o navegador coa dirección https://IP_Servidor.

Pódese xerar certificado de seguridade utilizando o comando open-ssl.

5.13.10 Apache con PHP

Páxinas web dinámicas lado servidor con PHP

PHP é unha linguaxe de programación utilizado para crear páxinas web dinámicas ao lado servidor. Nas páxinas hai scripts de php para distintos fins. Como exemplo de utilización, supoñer que se solicita usuario e contrasinal ao usuario da navegador web, o código php accede á base de datos gardada no servidor, comprobando se o usuario ten acceso e devolvendo os datos requiridos.

Para instalar php no noso servidor web Apache executar:

```
# apt install php
```

En Ubuntu 18.04 instálase a versión 7.2 de php. Para comprobar que PHP se instalou con éxito pódese crear un ficheiro php e situalo no directorio raíz do servidor web.

Exemplo: Crear script de inicio info.php

- Editar o ficheiro /var/www/html/info.php.

```
# nano /var/www/html/info.php # Escribir o contido seguinte
```

```
<?php
```

```
boto "A información do meu servidor:<p />";
```

```
phpinfo();
```

```
?> #Gardar arquivo
```

- Agora, na navegador web escríbese na barra de direccións `http://localhost/info.php`. Esta páxina devolve a información do servidor utilizado (instrución `phpinfo`).

Observar que agora habemos tecleado o nome do arquivo, pois por defecto devolvería `index.html` (ao ser o indicado na directiva `DirectoryIndex`)

Ilustración que mostra PHP funcionando

System	Linux SistemasUbuntu 4.15.0-47-generic #50-Ubuntu SMP Wed Mar 13 10:44:52 UTC 2019 x86_64
Build Date	Mar 22 2019 17:05:14
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS

Miguel Ángel García Lara (CC BY-NC-SA)

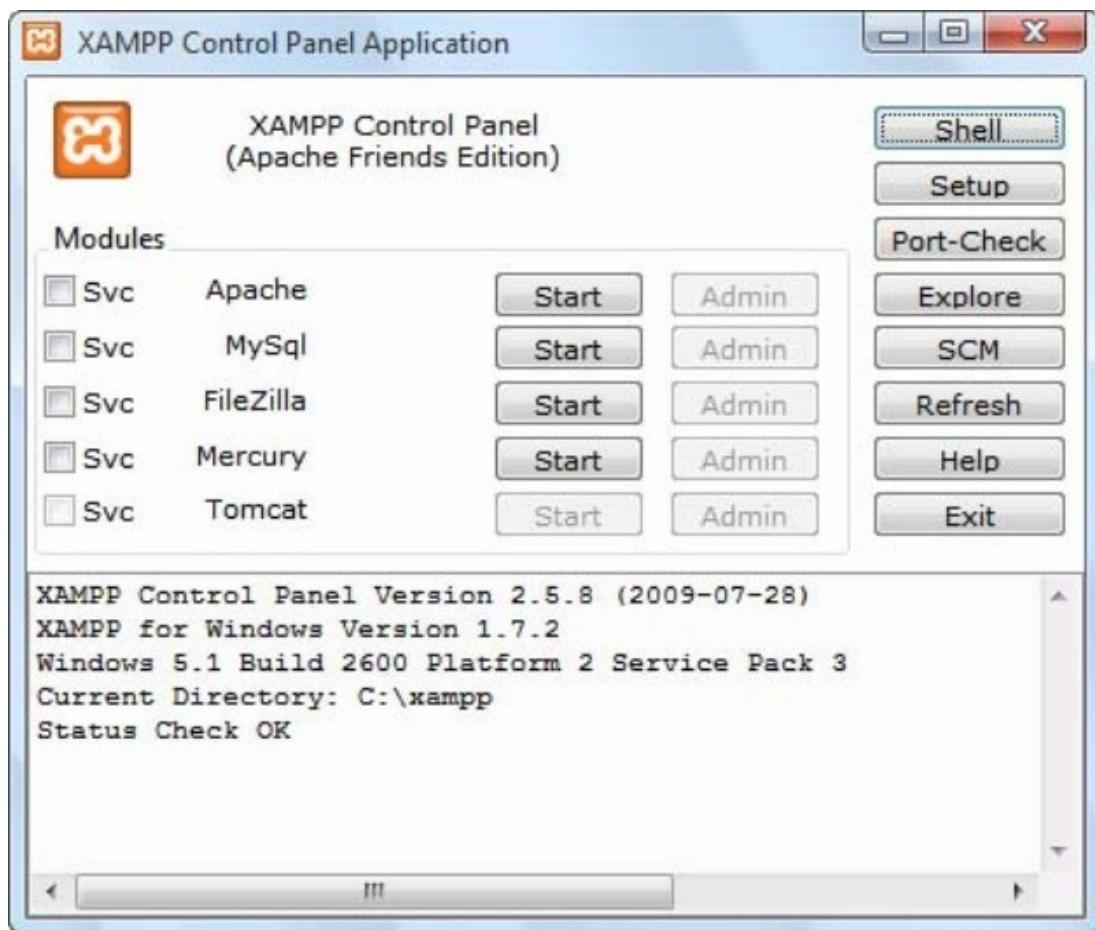
XAMPP

XAMPP é un paquete que aglutina varios servizos e programas: o servidor web Apache, o xestor de bases de datos MySQL e os intérpretes de linguaxe de scripts PHP e Perl. Desa forma, os programadores de páxinas dinámicas utilizan este software, como unha opción simple para ter todos os servizos instalados nun único proceso e cunha configuración sinxela.

XAMPP pódese instalar tanto en GNU-Linux como en Windows.

Unha vez instalado, hai un panel de control para iniciar ou deter cada servizo (ver imaxe)

Ilustración que mostra o panel de control de Apache



Materiais FP a Distancia do MEC (Dominio público)

Unha vez instalado e iniciado Apache, xa se pode visualizar no navegador a páxina de inicio de XAMPP escribindo no navegador `http://localhost`. Esta páxina de inicio está gardada no directorio de publicación do servidor web Apache por defecto, que no caso de Windows é `C:\xampp\htdocs`. Xa se pode gardar nese cartafol calquera páxina web estática (html) ou páxina dinámica (php)

5.13.10.1 Servizo FTP: vsftpd

Configuración

O servizo ftp utiliza os portos 20 e 21.

O servizo ftp máis utilizado en Linux chámase **vsftpd** (Very Secure FTP) é un servidor FTP moi pequeno e seguro.

Para instalalo: # **apt install vsftpd**

Unha vez instalado e comprobado que está a funcionar, xa se pode conectar o navegador. As conexións faranse cos mesmos clientes ftp que os vistos na unidade 9: terminal, filezilla, navegadores web.

O arquivo de configuración chámase **/etc/vsftpd.conf**

Neste arquivo configúrase os usuarios permitidos, se se permite usuario anónimo ou non, como o cartafol de descarga do servidor.

Por defecto, non se permite o acceso ao usuario anónimo. Os usuarios permitidos son os propios do sistema, e o seu directorio de conexión é a súa \$HOME. É dicir, se se conecta o usuario luís ao servidor ftp, o directorio onde se conecta é /home/luís.

Ademais configúrase se os usuarios quedan engaiolados no seu directorio, este concepto é importante. Supoñamos que o directorio de conexión ftp dun usuario é /home/luís é importante asegurarse que non vai poder saír ao directorio pai co comando cd ..

De feito, por defecto os usuarios non están engaiolados. Ver captura.

Ilustración que mostra a conexión a un servidor ftp en linux

miguel@clienteLinux: ~

Archivo Editar Ver Buscar Terminal Ayuda

miguel@clienteLinux:~\$ ftp 192.168.100.103
Connected to 192.168.100.103.
220 (vsFTPd 3.0.3)
Name (192.168.100.103:miguel): luis
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

Luis conectado se encuentra en su \$HOME. Con ls se ve sus archivos.

ftp> ls -l
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.

drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	Descargas	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	Documentos	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	Escritorio	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	Im??genes	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	M??sica	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	Plantillas	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	P??blico	
drwxr-xr-x	2 1002 1002	4096	Jan 03	14:17	V??deos	
-rw-r--r--	1 1002 1002	8980	Jan 03	14:16	examples.desktop	
drwxr-xr-x	2 1002 1002	4096	Apr 17	23:16	homeDeJuana	
drwxr-xr-x	2 1002 1002	4096	Apr 17	23:16	usuariosCliente	

226 Directory send OK.

Luis descarga el archivo examples.desktop

ftp> get examples.desktop
Local: examples.desktop remote: examples.desktop
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for examples.desktop (8980 bytes).
226 Transfer complete.
3980 bytes received in 0.00 secs (3.5199 MB/s)

ftp> cd ..
250 Directory successfully changed.

ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.

drwxr-xr-x	4 1001 1001	4096	Jan 09	12:32	alumno
drwxr-xr-x	4 1003 1003	4096	Apr 17	23:10	juan
drwxr-xr-x	4 1004 1005	4096	Apr 17	23:11	juana
drwxr-xr-x	16 1002 1002	4096	Apr 17	23:16	luis
drwxr-xr-x	18 1000 1000	4096	Apr 20	12:30	miguel

226 Directory send OK.

PELIGRO!!! El usuario no está enjaulado. Al ejecutar cd .. lo permite. De forma que al listar ls se ve el \$HOME de todos los usuarios

ftp> ■

Miguel Ángel García Lara (CC BY-NC-SA)

5.13.11 Configuración de parámetros de rede

ip addr #Listar interfaces activas

ip addr show #Equivale ao comando anterior.

ip addr show eth0 #Listar a configuración da interface eth0

ip link set eth0 up #Activar interface eth0

ip link set eth0 down #Deshabilitar interface eth0

ip address add 192.168.100.100/24 broadcast 192.168.100.255 dev eth0 #Configuración de rede para a interface eth0: IP=192.168.100.100, MS=255.255.255.0

ip address del 192.168.100.101/24 dev eth0 #Eliminar esa configuración IP na interface eth0. Neste caso esa configuración corresponden co alias eth0:0, polo que elimina ese alias da configuración de rede.

ip address del 192.168.100.102/24 dev eth0:web #Eliminar o alias eth0:web

ip route #Listar táboa de enrutamento

ip route show #Equivale ao comando anterior

ip route add default via 192.168.100.1

ip route del default via 192.168.100.1

ip route add 192.168.200.0/24 dev eth0 #Engadir regra de enrutamento para a rede 192.168.200.0 na interface eth0

ip route delete 192.168.200.0/24 dev eth #Eliminar regra de enrutamento para a rede 192.168.200.0 na interface eth0