REDES

Elementos e características dunha rede.

As redes son un mundo aparte por si só. Intentarei resumir moito os conceptos pero aínda así para profundar nelas, é necesario moito tempo, dedicación e esforzo.

- COMPOÑENTES DUNHA REDE -

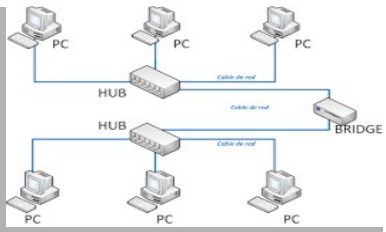
1. Compoñentes das redes

As redes permítennos intercambiar de forma rápida e económica información e recursos entre os equipos que están conectados por ela. Dentro da rede, podemos distinguir os seguintes compoñentes principais:

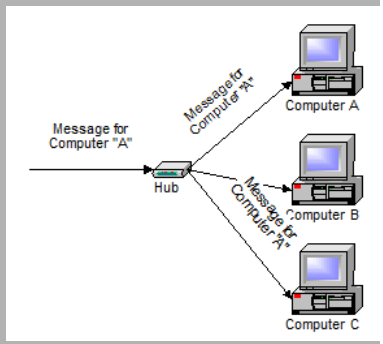
• ***Terminais***: Son os compoñentes que fan de fonte ou de destino de información. Englóbase todo tipo de dispositivos, que poden ser tanto un smartphone, unha impresora coma un potente ordenador. Cando un terminal inicia unha comunicación, usa a dirección do terminal destino para indicar onde vai a mensaxe.

• ***Dispositivos de rede intermedios:*** Estes dispositivos conectan os terminais á rede e distintas redes entre si. Dentro deste grupo podemos destacar os switchs, routers, puntos de acceso, firewalls de rede, etc.

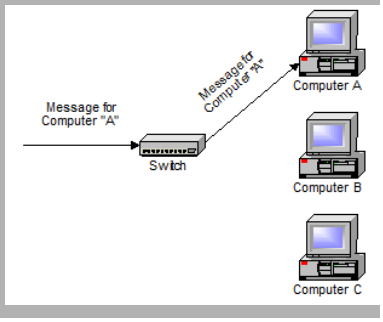
Elementos básicos que debedes coñecer:



- ✔ **Puente (Bridge):** Permite a conexión de dous segmentos de rede con iguais ou diferentes protocolos.



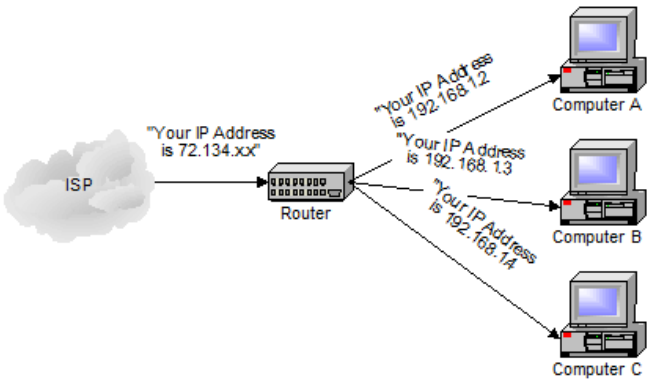
- ✔ **Hub (Concentrador):** É un dispositivo simple cunha única misión, a interconexión dos equipos dunha rede local. O seu funcionamento é sinxelo, cando algún dos ordenadores da rede local que están conectados a el envíalle datos, o hub replícaos e transmite instantaneamente ao resto de ordenadores desta rede local.



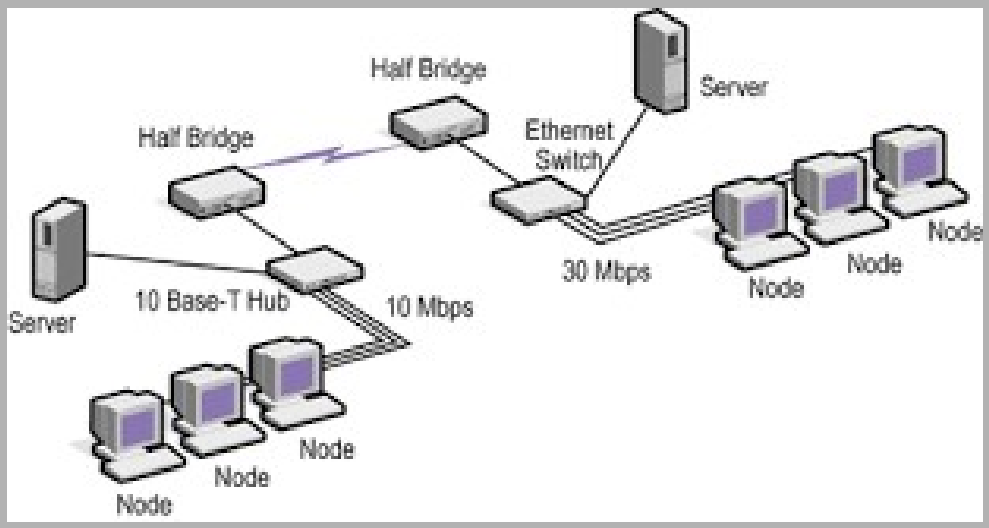
- ✔ **Switch (Conmutador):** Son os “irmáns listos” dos hub. A principal diferenza é que a través do switch, a información enviada polo equipo orixe vai directamente ao equipo destino sen replicarse ao resto de equipos que estén conectados. Este dispositivo creouse para traballar con redes con maior cantidade de quipos e facer que fose a comunicación máis fluída e con menos erros nas redes locales.

- ✔ **Router:** é o dispositivo que se encarga de reenviar os paquetes de información entre distintas redes. En xeral nunha rede local ou LAN e unha rede externa con porto WAN.

  Hoxe en día os routers poden cumplir funcións doutros dispositivos xa mencionados antes e incorporan outras tecnoloxías como un firewall basado en hardware ou servicios como NAT, servidor DHCP ou DNS.



Exemplo: equipos de interconexión dentro dunha rede.



• ***Liñas de comunicación:*** É o medio polo que viaxa a mensaxe, que ven caracterizado por un conxunto de parámetros, como a velocidade, etc. A calidade dunha liña está perfectamente caracterizada por normas internacionais.

2. Perturbacións nas transmisións

As transmisións de sinais están afectadas por unha serie de factores, que deforman ou alteran os sinais transmitidos, provocando que o sinal recibido non sexa exactamente igual que o emitido polo emisor. Estas contaminacións ou deformacións (que denominaremos perturbacións) poden conducir a perdas de información e a que as mensaxes non cheguen aos seus destinos con integridade. Podemos distinguir as seguintes perturbacións principais:

• ***Atenuación***: Perda de potencia do sinal a medida que aumenta a distancia de transmisión. Esta perda é debida á resistencia tanto da canle como do resto dos elementos que interveñen na transmisión. Este debilitamento provoca un descenso da amplitude do sinal transmitido. A atenuación mídese en decibelios (dB), e limita a distancia máxima pola que podemos enviar unha sinal polo medio, xa que chega un momento que se debilita demasiado.

• ***Distorsión:*** A distorsión consiste na deformación do sinal, producida normalmente porque a canle se comporta de modo distinto en distintas frecuencias. Os ecualizadores corrixen os efectos da distorsión dunha canle, potenciando a amplitude do sinal en aquelas frecuencias que se atenúan na transmisión.

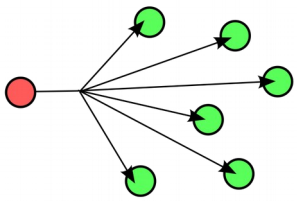
• ***Interferencias:*** O sinal recibido = sinal emitido + sinal emitido.

• ***Ruído:*** O sinal recibido = sinal emitido + sinais adicionais que se engadiron polo camiño. A diferenza coas interferencias é que no ruído se descoñecen a orixe das sinais adicionais, xa que son de natureza aleatoria.

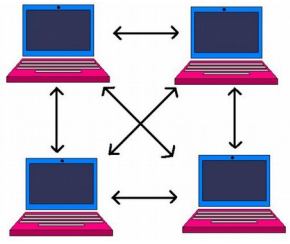
• ***Ecos:*** Reflexión do sinal no receptor co cal volve ó emisor. Apreciable no receptor se o retardo é superior a 10ms.

3. Tipos de transmisións

Redes punto a punto e multipunto



• **Rede Multipunto (Broadcast ou Redes de Difusión):** Todas as máquinas comparten unha soa canle de comunicación. Un paquete de datos mandado por algunha máquina é recibido por todas as outras.

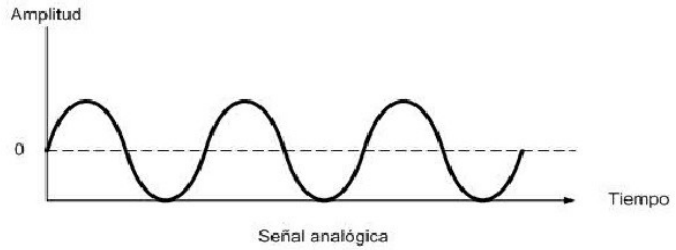


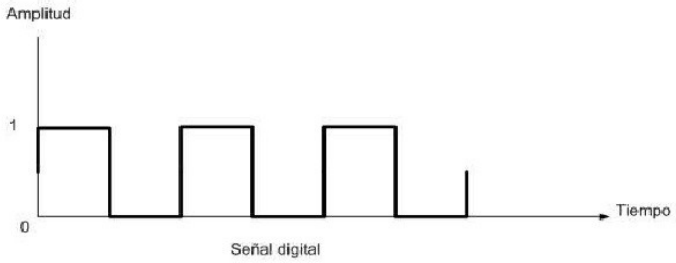
• **Rede Punto a punto (Point-to-Point):** Temos moitas conexións entre pares individuais de máquinas. Pode que nun momento dado os paquetes dunha máquina a outra teñan que atravesar máquinas intermedias, e entón precísase o enrutamento (routing) para dirixilos.

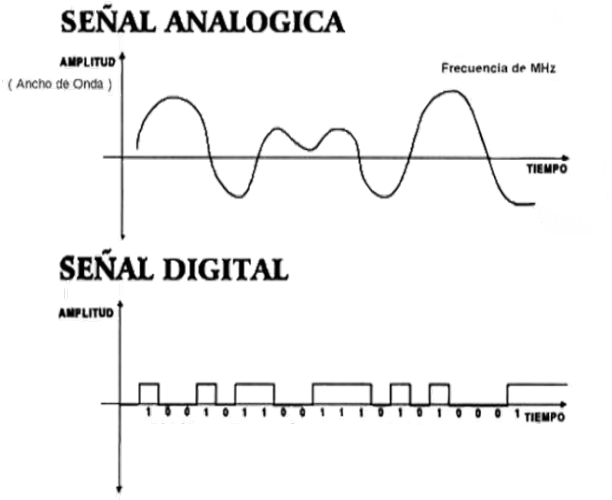
Transmisións analóxicas e dixitais

• **Sinal analóxico:** aquel que pode tomar calquera valor dentro dun rango determinado. A potencia do sinal analóxico recibido debe estar comprendido entre uns valores máximo e mínimo. A calidade depende non só da potencia recibida, senón tamén do ruído que a acompaña. Cando un sinal chega a un repetidor/amplificador este amplifica o sinal, co cal tamén amplifica o ruído que con ela chega.

• **Sinal discreto ou dixital:** aquel que só toma un número finito de valores dentro dun rango determinado. A potencia do sinal discreto recibido debe estar comprendido entre uns valores máximo e mínimo. Cando un sinal chega a un repetidor, este rexenera o sinal orixinal eliminando o ruído. Esta é a gran vantaxe das comunicacións dixitais, xa que son moito máis robustas ante o ruído que sempre aparece na transmisión.







Transmisión en serie e en paralelo

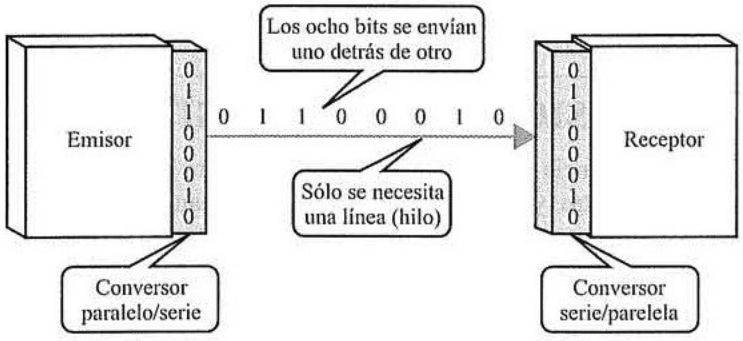
Neste caso distinguiremos dous tipos de secuenciamento dos bits transmitidos.

• **Serie:** Os bits dunha palabra envíanse consecutivamente un tras outro.

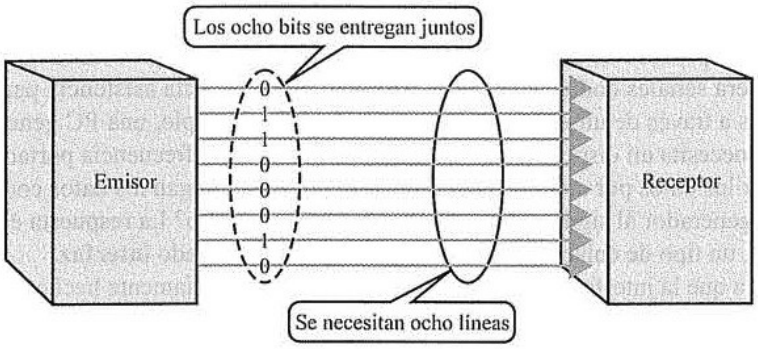
• **Paralela:** Os bits dunha palabra envíanse por diferentes circuítos/cables.

Aínda que o rendemento da transmisión en paralelo é maior que o da transmisión en serie, en grandes distancias o seu comportamento empeora polas interferencias que os distintos cables provocan entre si.

Serie



Paralela



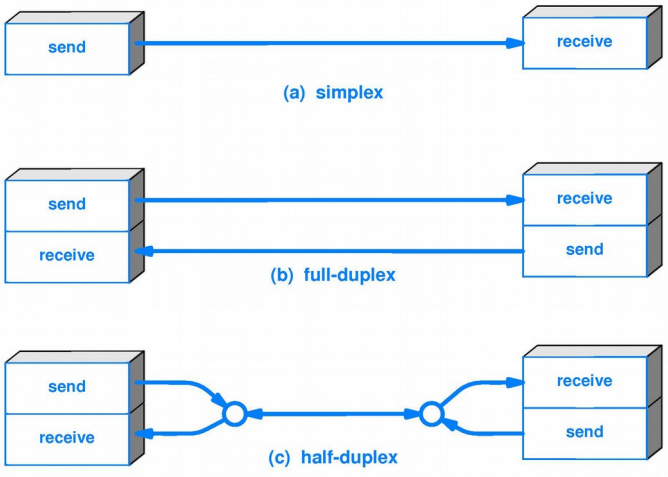
Comunicación símplex, dúplex e semidúplex

Neste caso podemos distinguir entre tres tipos de comunicacións nas redes segundo o fluxo de información entre o emisor e o receptor. As restricións no sentido da comunicación poden vir dadas tanto polos dispositivos emisores ou receptores como pola propia liña de comunicación.

• **Comunicación símplex:** Unha comunicación é símplex se están perfectamente definidas as funcións do emisor e receptor e a transmisión de datos sempre se efectúa exclusivamente nun sentido: de emisor a receptor. Dicimos que neste tipo de comunicación hai unha única canle física e unha única canle lóxica unidirecional.

• **Comunicación semidúplex ou half duplex:** A comunicación pode ser bidireccional, é dicir, emisor e receptor poderán intercambiar os seus papeis; sen embargo, esta bidirecionalidade non pode ser simultánea. Cando o emisor transmite, o receptor necesariamente recibe; despois, o receptor pode exercer como emisor coa condición de que o antigo emisor pase a ser receptor. Na comunicación semidúplex hai unha única canle física e unha canle lóxica bidirecional.

• **Comunicación dúplex ou full duplex:** Na comunicación dúplex a comunicación é bidireccional e ademais simultánea. O emisor e o receptor non están perfectamente definidos: Ambos terminais actúan como emisor e receptor indistintamente. Na comunicación dúplex hai unha canle física e dúas lóxicas. Os switches Ethernet operan por defecto neste modo.

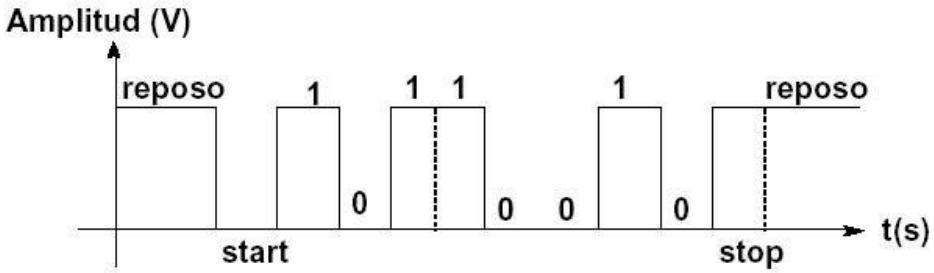


Transmisión síncrona e asíncrona

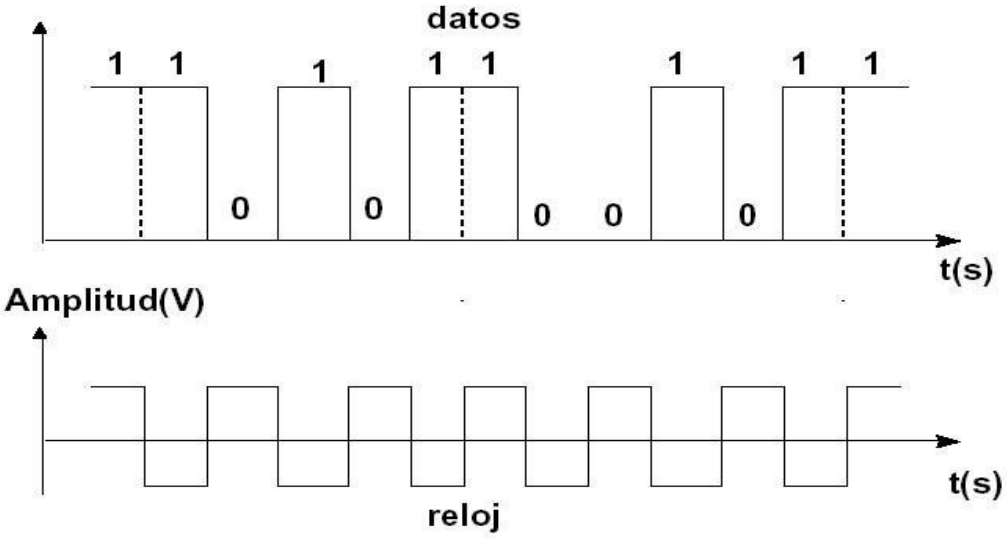
O sincronismo é o proceso polo que un emisor e un receptor se poñen de acordo sobre o instante preciso no que comeza ou remata unha información que se pon no medio de transmisión. Polo tanto, a sincronización require a definición dunha base de tempos sobre a que medir os distintos eventos que ocorren durante toda a comunicación. Un erro no sincronismo impedirá interpretar correctamente a información a partir dos sinais que viaxan polo medio.

Con respecto a técnica utilizada para conseguir o sincronismo na transmisión, podemos distinguir dous tipos de transmisións:

• **Transmisión asíncrona:** Unha transmisión é asíncrona cando o proceso de sincronización entre o emisor e o receptor realízase en cada palabra de código transmitida (unha *palabra* é conxunto de bits con algún significado, a unidade mínima de comunicación). Isto se leva a cabo a través duns bits especiais que axudan a definir o contorno de cada código. No seguinte exemplo, podemos ver unha liña cun estado de reposo (1), pola que se transmite unha palabra de 8 bits enmarcada entre un bit de start (0) e un bit de stop (1).



• **Transmisión síncrona:** A transmisión é síncrona cando se efectúa sen atender a palabras ou unidades de comunicación básicas. Por contra, nesta técnica os bits envíanse a unha cadencia constante un tras outro sen discriminar. Emisor e receptor sincronízanse a través dun sinal de reloxo que se envía paralelamente cos datos.



Nas transmisións síncronas sóense utilizar caracteres especiais para evitar os problemas de perdas de sincronía nos bits de información transmitidos, que poden producirse se o sinal de reloxo se desfasa. Por exemplo, o carácter SYN do código ASCII (0010110) é moi utilizado xa que é irrepetible polo desprazamento dos seus bits, e desta forma o receptor é capaz de darse conta de que houbo un desprazamento.

O modo de transmisión síncrona permite velocidades de transmisión maiores que a asíncrona, xa que obtén un mellor rendemento da liña de datos. Entendemos por rendemento dunha transmisión a relación entre os bits de información transmitidos e os bits totais transmitidos.

Hai que ter en conta que na transmisión síncrona non son precisos os bits de start e stop que acompañan a cada carácter na transmisión asíncrona. Por exemplo, se temos unha transmisión asíncrona cun bit de start e 2 de stop, obtemos un rendemento de:

Rendemento = 8/(8+1+2)*100 = 72,7%

Sen embargo, se supoñemos unha liña síncrona na que se envían 3 caracteres de SYN cada 256 bytes, o rendemento será:

Rendemento = 256/(256+3)*100 = 98,8%

4. Frecuencia e ancho de banda

A utilización de sistemas eficientes conduce a unha redución do tempo de transmisión, é dicir, que se transmite unha maior cantidade de información en menos tempo. Unha transmisión de información rápida conséguese empregando sinais que varían rapidamente co tempo.

O número de veces que o sinal varía por unidade de tempo é o que se coñece como frecuencia do sinal. A frecuencia mídese en Hz, e 1 Hz correspóndese cun ciclo por segundo. Desta forma, un sinal de 100 Mhz varía cunha velocidade de 100.000.000 ciclos por segundo.

Polo tanto, para transmitir a maior velocidade, só temos que aumentar a frecuencia do sinal transmitido. Pero estamos tratando cun sistema eléctrico, que conta con enerxía almacenada; e hai unha lei física que expresa que en todos os sistemas, excepto nos que non hai perdas, un cambio na enerxía almacenada require unha cantidade definida de tempo. Así, non podemos incrementar a velocidade do sinal de forma ilimitada, xa que a canle deixará de responder aos cambios do sinal.

A canle pola que transmitamos o sinal vainos a impoñer un rango de frecuencias mínima e máxima fora das cales os sinais transmitidos pola canle son fortemente distorsionados. A ese rango de frecuencias denomínaselle **ancho de banda** da canle. Canto maior sexa o ancho de banda da canle, mais amplo é o rango de frecuencias que permite transmitir e polo tanto maior cantidade de información poderemos transmitir por ela nunha unidade de tempo.

5. Clases de liñas de comunicación

En función do propietario das liñas que permiten a conexión dunha rede, podemos falar de tres tipos de liñas:

• ***Liñas privadas***: Dise que unha liña é privada cando ten un propietario e só son utilizadas polo seu propietario. As liñas utilizadas nas redes de área local son privadas, xa que todo o seu percorrido é propiedade do dono da rede.

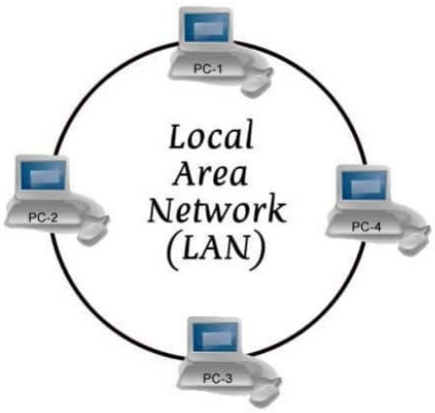
• ***Liñas públicas:*** Normalmente están en poder das compañías telefónicas e, polo tanto, teñen un ámbito de actuación nacional ou supranacional. O usuario dunha liña pública contrata os servizos de comunicacións coa compañía que lle subministra a liña en réxime de alugueiro.

• ***Liñas adicadas:*** Unha liña pode ser pública, pero iso non significa que sexa exclusiva para quen a aluga. Nunha liña pública mestúranse datos de diferentes usuarios, aínda que a rede se encargue de que cada dato chegue ó seu destino correcto. En ocasións interesa que a liña de datos pública só poida ser utilizada con exclusividade por dous usuarios ou por dous equipos concretos. Dise entón que a liña de comunicacións é adicada.

6. Clases de redes segundo o seu tamaño

En función do tamaño dunha rede, podemos clasificala nun dos seguintes grupos:

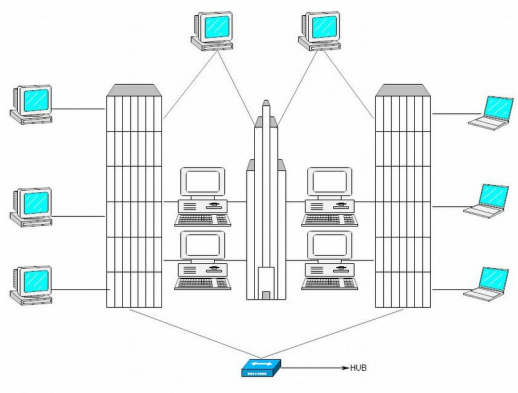
• **PAN** *(rede de área persoal ou personal area network):* Comunican dispositivos do ordenador, como o teclado ou o rato, ata teléfonos móbiles ou PDAs. Cobren só uns poucos metros, e aínda que poden ser redes conectadas con cable (por exemplo, USB), as máis interesantes para nós son as que non usan fíos (utilizan tecnoloxías como bluetooth).



• **LAN** *(rede de área local ou local area network):* Comunican un conxunto de ordenadores colocados nunha área xeográfica reducida (aulas, edificios, campus). Na súa construción úsanse liñas de comunicación privadas. Dado que o seu tamaño é restrinxido, o tempo de transmisión no peor dos casos é coñecido. As velocidades de transmisión que proporcionan son elevadas, xa que o máis habitual é que sexan de 100 Mbps (megabits por segundo), aínda que se poden atopar velocidades dende 10 Mbps (en redes antigas) ata 1Gbps ou 10Gbps (en redes modernas de altas prestacións).

Unha LAN pode ser moi simple (dous equipos conectados cun cable) ou complexa (centos de equipos e periféricos conectados dentro dunha grande empresa).

• **MAN** *(rede de área metropolitana ou metropolitan area network):* Cobren un área xeográfica restrinxida a unha cidade. Xeralmente unen varias LANs mediante liñas públicas ou privadas.



• **WAN** *(rede de área extensa ou wide area network):* Abarcan áreas xeográficas tan grandes coma un país ou como o mundo enteiro (Internet). Usan liñas públicas para a súa conexión. Unha WAN consta de varias LANs e ordenadores interconectados. Podemos ver Internet como a WAN suprema. Unha internet é unha rede de redes vinculadas por enrutadores (Internet é un exemplo dunha internet).

7. Medios de transmisión das redes de datos con fíos.

O medio de transmisión é o soporte físico que facilita o transporte da información. A calidade da transmisión dependerá, en gran parte, das súas características. A meirande parte das redes están conectadas por algún tipo de cableado, que actúa como medio de transmisión por onde pasan os sinais entre os equipos.

Hai dispoñibles unha grande cantidade de tipos de cables para cubrir as necesidades e tamaños das diferentes redes, dende as mais pequenas ás mais grandes. Podemos distinguir tres tipos fundamentais de cables:

• Cable de par trenzado

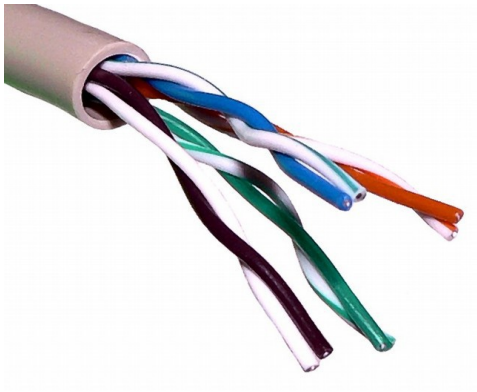
• Cable coaxial

• Fibra óptica

Estes medios de transmisións denomínanse medios guiados, xa que os sinais que se transmiten por eles seguen un camiño marcado polo cableado.

Sen embargo, o cable non é o único medio de transmisión das redes. O aire tamén é un medio de transmisión moi utilizando nas redes de comunicacións, utilizando ondas de distintas frecuencias. O aire é un exemplo dun medio de transmisión non guiado, xa que as ondas viaxan libres polo aire, sen ir confinadas por un conduto delimitado. Ata fai pouco tempo, o uso das transmisións sen fíos estaba restrinxido ás redes WAN e liñas de alta capacidades, sen embargo, hoxe en día a súa expansión nas LAN é cada vez maior, debido a súa flexibilidade e facilidade de instalación.

7.1 Cable de par trenzado.



Características do cable de par trenzado.

O cable de pares:

• É similar ao do teléfono.

• É o medio de transmisión máis simple e económico.

• Componse dunha serie de pares de fíos polos que se transmiten distintos sinais.

Algúns inconvenientes deste cable son:

• Presenta unha resistencia eléctrica bastante elevada, o que provoca o debilitamento do sinal se se sobrepasan determinadas lonxitudes. Isto obrigará a rexenerar o sinal para que poida ser recibida correctamente.

• O condutor de cobre que utiliza é moi sensible ás interferencias que se producen entre uns cables e outros.

Un modo de subsanar estas interferencias consiste en *trenzar os pares*, xa que así se consegue que que unhas perturbacións anulen ás outras. É por iso que falamos do cable de par trenzado, xa que os fíos van trenzados entre eles e se encerran nun recubrimento protector para formar un cable.

Canto máis trenzados estean os fíos maior inmunidade ao ruído, pero pola contra menor lonxitude pode ter o cable, pois ao ter maior lonxitude de fíos prodúcese maior atenuación, por iso hai que tomar un punto medio onde os pros e os contras se compensen.

7.1.1 Conectores do cable de par trenzado.

Os fíos do cable teñen unha cor que os identifica. Os pares que van trenzados son os dunha cor cos que son brancos e desa mesma cor:

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

O cable de par trenzado utiliza conectores telefónicos RJ-45 para conectarse a un equipo. Son similares aos conectores telefónicos RJ11, aínda que hai diferencias entre eles, e o seu tamaño non coincide. O conector RJ-45 contén oito conexións de cable, mentres que o RJ-11 só contén catro.

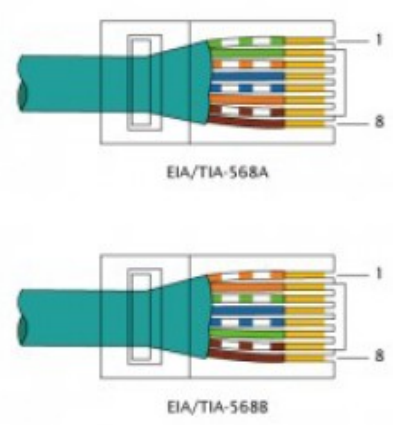
A tarxeta de rede transmite e recibe a información polo seu conector RJ-45 femia. Para a transmisión que actualmente se utiliza de 100 Mbps, os pins que usa para tal fin son:

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

Polo tanto os pins 1 e 2 do cable transmiten e o 3 e 6 reciben. Porén, hai que ter en conta que se quixeramos transmitir a 1 Gbps a tarxeta de rede faría uso dos 8 pins.

7.1.2 Códigos de conexión.

Se atendemos as consideracións de que os pares trenzados son máis inmunes as interferencias, temos que se no pin 1 do conector RJ-45 macho poñemos un cabliño con cor Marrón no pin 2 teremos que poñer o cabliño con cor Branco-Marrón, para que así se anulen as interferencias entre eles. O mesmo deberemos facer cos pins 3 e 6.



Tendo en conta estas consideracións, existen dúas combinacións convencionais de cables. Non teñen explicación técnica, simplemente son convenios adoptados para utilizar sempre a mesma orde nos cables nos conectores nunha rede.

PIN/Patilla	Código A	Código B
1	Branco-Verde	Branco-Laranxa
2	Verde	Laranxa
3	Branco-Laranxa	Branco-Verde
4	Azul	Azul
5	Branco-Azul	Branco-Azul
6	Laranxa	Verde
7	Branco-Marrón	Branco-Marrón
8	Marrón	Marrón

7.2 Cable coaxial.

É un cable moi similar ao que coñecemos da televisión. Houbo un tempo no que o cable coaxial foi o mais utilizado, xa que era barato e fácil de manexar; sen embargo hoxe en día está en desuso, xa que foi substituído polo cable de par trenzado.

Un cable coaxial consta dun núcleo de fío de cobre rodeado por un illante, un apantallamento de metal trenzado e unha cuberta externa.

• O **núcleo do cable** coaxial transporta os sinais electrónicos que forman os datos. Este núcleo pode ser sólido ou de fíos. Se o núcleo é sólido, normalmente é de cobre.

• Rodeando ao núcleo hai una **capa illante** dieléctrica que o separa da malla de fío.

• A **malla de fío trenzada** actúa como masa, e protexe ó núcleo do ruído eléctrico e das interferencias. O núcleo de condución e a malla de fíos deben estar separados un do outro. Se chegaran a tocarse, o cable sufriría un curtocircuíto, e o ruído ou os sinais que se atopen perdidas na malla circularían polo fío de cobre.

• O **apantallamento** protexe máis os datos transmitidos absorbendo os sinais de ruído, de forma que non pasan polo cable e non distorsionan os datos. Ao cable que contén unha lámina illante e unha capa de apantallamento de metal trenzado se lle denomina cable apantallado dobre. Para contornos que están sometidos a grandes interferencias, hai un apantallamento cuádruplo, con dúas láminas illantes e dúas capas de apantallamento de metal trenzado.

• Unha **cuberta exterior** non condutora (normalmente de goma, teflón ou plástico) rodea todo o cable.

Toda a protección que inclúe o cable coaxial faino máis resistente a interferencias e atenuación que o cable de par trenzado, permitindo chegar a frecuencias de 500 MHz.

7.3 Fibra óptica.

No cable de fibra óptica transpórtanse sinais dixitais de datos en forma de pulsos modulados de luz. Esta é unha forma moi segura de enviar datos debido a que, a diferencia dos cables de cobre que levan os datos en forma de sinais electrónicos, os cables de fibra óptica transportan impulsos non eléctricos. Isto significa en primeiro lugar que o cable de fibra óptica non se pode pinchar e os seus datos non se poden roubar, pero ademais que a transmisión é insensible a interferencias electromagnéticas externas.

Un sistema de transmisión óptico ten tres compoñentes:

• A **fonte de luz**: Encárgase de converter un sinal dixital eléctrico nun sinal óptico. Xeralmente utilízase un pulso de luz para representar un "1" e a ausencia de luz para representar un "0". Esta fonte pode ser un díodo láser (emite un onda láser) ou un díodo LED.

• O **medio de transmisión**: Trátase dunha fibra de vidro ultradelgada, que transporta os pulsos de luz.

• O **detector**: Encárgase de xerar un pulso eléctrico no momento no que a luz incide sobre el. O cable de fibra óptica é apropiado para transmitir datos a velocidades moi altas (ata 370 Thz) e con grandes capacidades debido á carencia de atenuación do sinal e a súa pureza.

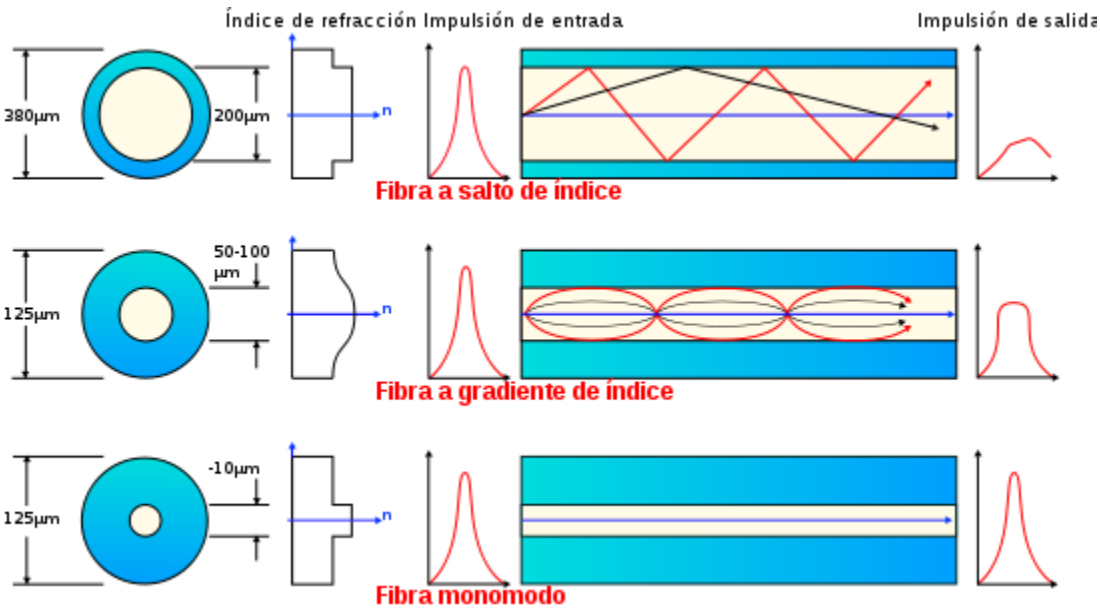
Unha fibra óptica consta dun cilindro de vidro extremadamente delgado, denominado núcleo, recuberto por unha capa de vidro concéntrica, coñecida como revestimento (Ás veces en lugar de vidro tamén pódese usar plástico que é máis fácil de instalar, pero non pode levar os pulsos de luz a distancias tan grandes como o vidro). Na transmisión, o sinal é conducido polo interior do núcleo, sen poder escapar del debido ás reflexións internas totais que se producen, impedindo tanto o escape de enerxía cara o exterior coma a adición de novas sinais externas. Varios cables de fibra poden agruparse en feixes utilizando unha funda exterior.

7.3.1 Tipos de cables de fibra óptica.

Actualmente utilízanse dous tipos de fibra óptica para a transmisión de datos:

• **Fibra monomodo ou de modo único**: Potencialmente, este é o tipo de fibra que ofrece maior capacidade de transmisión. O seu nome ven dado porque os raios de luz transmitidos só seguen unha traxectoria, seguindo practicamente o eixe da fibra. Isto conséguese con un núcleo dun diámetro moi pequeno (da orde de millonésimas de metro). Son, pola contra, difíciles de manexar e instalar.

• **Fibra multimodo**: Por ela os raios de luz non seguen a dirección do eixe da fibra, senón que forman un ángulo e rebotan no extremos. Desta forma permiten distintos camiños de luz sobre a mesma fibra, e polo tanto pódense facer varias transmisións simultáneas (utilizando a multiplexación por lonxitude de onda). Coa fibra multimodo, a distancia máxima de transmisión do cable é menor.

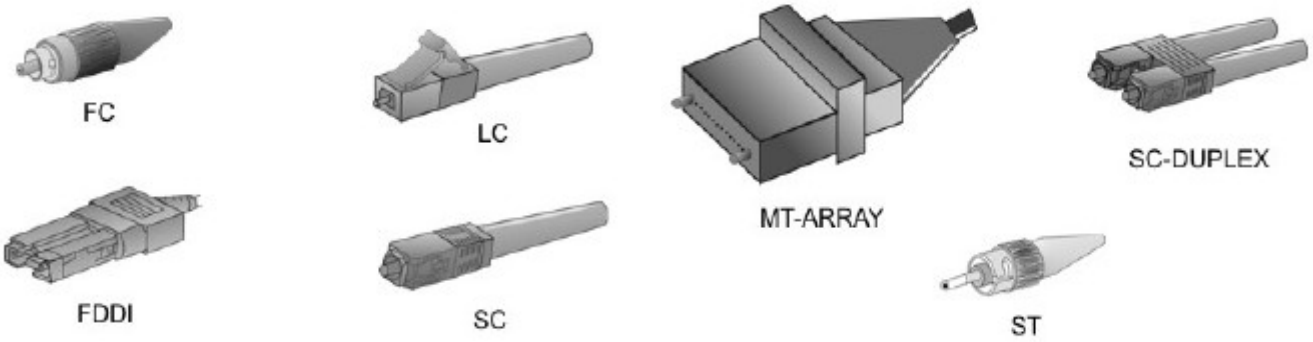


7.3.2 Aplicacións do cable de fibra óptica.

Podemos ver na seguinte táboa as aplicacións e características dos distintos tipo de fibra:

Tipo de fibra	Km	Aplicacións
Monomodo	>10000	Cables submarinos, cables interurbanos a 140 e 565 Mb/s
Multimodo I.G.	400 - 1500	Rotas urbanas ou provinciais ata 140 Mb/s, transmisións de TV dixital
Multimodo S.I con revestimento de vidro	100 - 400	Redes de abonado distribución de TV, redes locais
Multimodo S.I con revestimento plástico	15-20 / 5-10	Transmisión de datos, redes locais e punto a punto, aplicacións militares

7.3.3 Conectores de fibra óptica.



8. Transmisión sen fíos.

Podemos distinguir os seguintes tipos de redes sen fíos en base ao seu alcance:

• **WPAN** (Wireless Personal Area Network–Rede Sen Fíos de Ámbito Persoal)

• **WLAN** (Wireless Local Area Network–Rede Sen Fíos de Área Local)

• **WMAN** (Wireless Metropolitan Area Network–Rede Sen Fíos de Área Metropolitana)

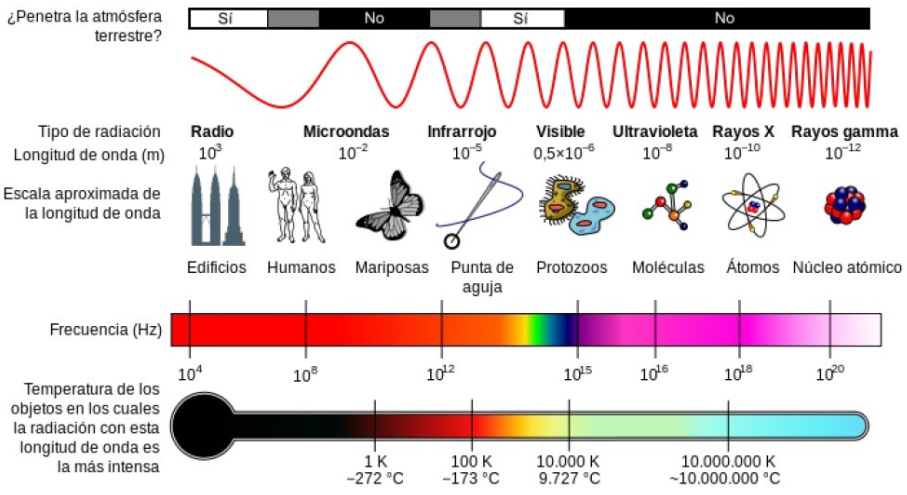
• **WWAN** (Wireless Wide Area Network–Rede Sen Fíos de Área Extensa)

8.1 Redes WPAN

Estas redes están pensadas para cubrir unha áreas do tamaño dunha habitación e a súa finalidade é a da conexión de dispositivos diversos, como o teléfono móbil, unha axenda electrónica (PDA), etc. Nas WPAN utilízanse as seguintes tecnoloxías:

• ***Transmisión infravermella***: Utilizan un raio de luz infravermella para levar os datos entre os dispositivos (Frecuencias de 300 GHz a 384 THz). Estes sistemas precisan xerar sinais moi fortes, porque os sinais débiles son susceptibles a interferencias dende fontes de luz. Este método pode transmitir sinais a altas velocidades debido ao grande ancho de banda da luz infravermella. Unha rede infravermella normalmente pode transmitir a 10 Mbps. As transmisións por infravermellos teñen unha serie de inconvenientes importantes, que impiden utilizalas en redes máis extensas. En primeiro lugar, aínda que hai distintos tipos de redes infravermellas, a maioría delas requiren que os equipos teñan alcance visual para poder comunicarse. Ademais, os infravermellos teñen dificultade para transmitir a distancias maiores de 30,5 metros. Por último, están supeditados a interferencias da forte luz ambiental que se atopa nos contornos comerciais.

• ***Transmisión por radio de amplo espectro***: Esta técnica utiliza ondas de radio (2,4 Ghz) para a transmisión do sinal polo aire. A radio de amplo espectro transmite sinais dentro dun rango de frecuencias. As frecuencias dispoñibles divídense en canles, coñecidos como hops ou saltos. A tecnoloxía bluetooth utiliza este tipo de transmisión, e define unha canle de comunicación dun máximo de 3 Mbps cunha distancia óptima de 10 m podendo chegar ata 100m en función da potencia de emisión. Vemos polo tanto que proporciona un ancho de banda menor que a transmisión por infravermellos, pero ten a vantaxe de poder atravesar obxectos sólidos, e non obrigar polo tanto a que os dispositivos teñan contacto visual.



8.2 Redes WLAN

Son as redes que cobren o ámbito dunha casa, unha oficina ou o dun edificio dunha empresa, unindo os distintos equipos da mesma.
Excepto polo medio utilizado, estas redes sen fíos operan de forma similar a unha LAN cableada: en cada un dos equipos instálase unha tarxeta de rede sen fíos cun transceptor, e os usuarios comunícanse coa rede como se estiveran utilizando equipos con cables.
Outro transceptor, tamén chamado ***punto de aceso***, transmite e recibe sinais dos equipos circundantes e pasa datos entre os equipos sen fíos e a rede cableada. Estas LAN sen fíos utilizan pequenos transceptores fixados na parede para conectarse á rede con fíos. Estes transceptores establecen contacto por radio cos dispositivos de rede.
Unha das tecnoloxías deste tipo máis utilizadas na actualidade para as WLAN é a tecnoloxía ***WI-FI***, que permite velocidades de 11 ata 9600 Mbps (nas versións máis recentes), utilizando ondas de radio 2,4 e 5 GHz, e de 1 a 6 GHz na última versión.

Podemos distinguir dous tipos de arquitecturas para as WLAN:
• **Modo equipo-equipo ou ad-hoc**: Simplemente se dota a cada equipo dunha tarxeta de rede sen fíos para que todos se comuniquen con todos.
• **Modo infraestrutura**: Introducindo unha unidade base, permite conectar a rede sen fíos a unha rede cableada.

8.3 Redes WMAN

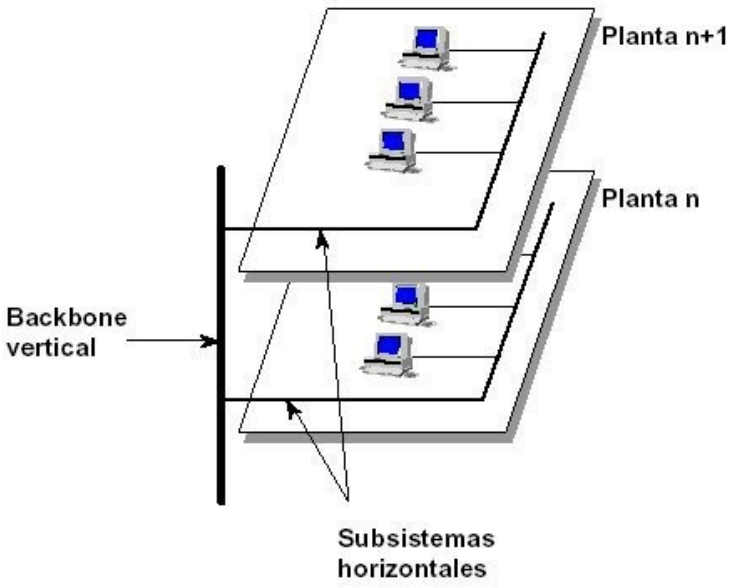
Para redes de área metropolitana destacan as tecnoloxías baseadas en ***WiMAX*** (Worldwide Interoperability for Microwave Access, é dicir, Interoperabilidade Mundial para Acceso con Microondas), un estándar de comunicación sen fíos baseado en la norma IEEE 802.16.
En comparación con Wi-Fi, WiMAX ofrece máis cobertura e ancho de banda. Tamén podemos atopar outros sistemas de comunicación como ***LMDS*** (Local Multipoint Distribution Service).

8.4 Redes WWAN

Son as redes que abarcan áreas máis amplas, como unha cidade, un país, etc. Dentro deste tipo de redes destacan as tecnoloxías de telefonía móbil, como ***GSM, GPRS, UMTS*** (que mellora a velocidade ata case 2 Mpbs), ***HSDPA*** (que pode chegar a 14 Mbps), ***HSPA+*** (ata 84Mbps) e ***LTE*** (coñecido como 4G, con capacidade máxima de ata 1Gbps).
Pero as redes de ordenadores tamén utilizan en moitos casos conexións sen fíos en redes de área extensa, ben entre edificios ou en conexións vía satélite. Nas redes WWAN utilízase a transmisión por enlaces de microondas (ondas electromagnéticas de alta frecuencia que poden ir de 1 GHz a 300 GHz), que poden utilizarse para conectar dous puntos a longa distancia sempre que sexan visibles un co outro. Utilízanse en casos como:
• Enlaces de satélite (situado nunha órbita xeoestacionaria a 36.000km de altura) a terra.
• Entre dous edificios.
• A través de grandes áreas uniformes e abertas, como extensións de auga ou desertos.

9. Elementos do cableado estruturado.

As normas definidas para o cableado definen unha serie de categorías de cable que garanten unhas determinadas prestacións nas transmisións no mesmo. Desta maneira defínense as bases do ***cableado estruturado***, establecendo os tipos de cable que se utilizarán nas distintas liñas de comunicación da rede.
Ademais, o cableado estruturado define a organización que se debe seguir á hora de cablear un edificio. Cando o número de dispositivos que utilizamos e a cantidade de cable é grande, é moi importante seguir estas normas para conseguir unha boa organización e estrutura física da rede.
O cableado estruturado, para comezar, distingue entre o ***cableado horizontal***, que une os equipos dunha planta na rede, e o ***cableado vertical ou backbone,*** que une as distintas plantas do edificio.



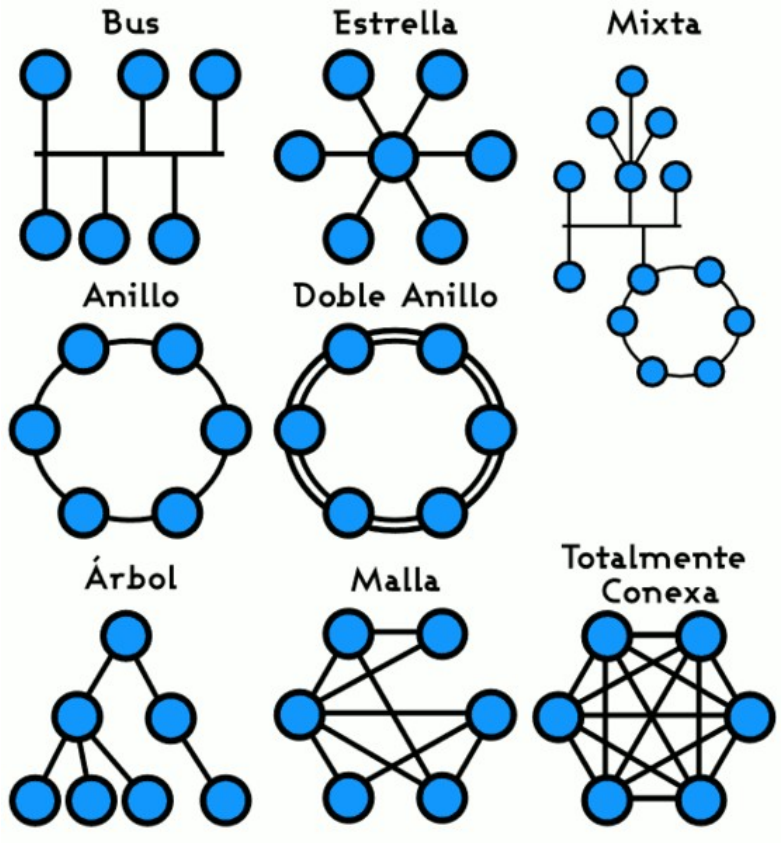
Mediante esta división, establécese unha plataforma estandarizada e aberta para a distribución do cableado co obxectivo de obter as mellores prestacións da rede. Ademais, o cableado estruturado incorpora unha serie de elementos que mellora a organización e o funcionamento da rede, como son:

- **Armarios ou racks de distribución** : Os armarios ou racks de distribución poden crear máis sitio para os cables naqueles lugares onde non hai moito espazo libre no chan. O seu uso axuda a organizar unha rede que ten moitas conexións.
- **Paneis de conexións ou de parcheo:** Colocados dentro dos armarios de distribución, serven para organizar mellor o cableado que vai conectarse nos dispositivos de interconexión.
- **Canaletas:** Son estruturas normalmente de plástico que se unen á parede ou ao chan e recollen o cableado no seu interior. As canaletas tabicadas inclúen unha separación interior para separar os cables de datos dos cables de alimentación.
- **Bridas, tubos corrugados e etiquetas identificativas:** Elementos plásticos que permiten agrupar e identificar os distintos cables.
- **Rosetas:** Estes conectores RJ-45 dobres ou simples conéctanse en paneis de conexións e placas de parede.
- **POP (Point of Presence):** Lugar onde a operadora de telecomunicacións instala o seu punto de acceso.
- **IDF/MDF (Intermediate/Main Distribution Facility):** Son os lugares onde se sitúan os equipos: racks de distribución, concentradores, conmutadores, enrutadores, servidores.

10. A topoloxía da rede

10.1 Qué é a topoloxía da rede

Antes de que os equipos poidan compartir recursos ou realizar outras tarefas de comunicacións, necesitan estar conectados. Na maioría das redes utilízanse cables para conectar un equipo a outro (excepto nas redes sen fíos).
Sen embargo, crear unha rede non é tan simple como conectar a un equipo un cable que está conectado a outros equipos. Os distintos tipos de cable (combinados cos distintos tipos de tarxetas de rede, sistemas operativos de rede e outros compoñentes) requiren distintos tipos de organizacións.
O termo ***topoloxía***, ou máis especificamente, topoloxía de rede, refírese á organización ou distribución dos equipos, cables e outros compoñentes da rede. Topoloxía é o termo estándar que utilizaremos cando nos refiramos ó deseño básico da rede.



10.2 Tipos de topoloxías

Debemos distinguir nunha rede dous tipos de topoloxías:

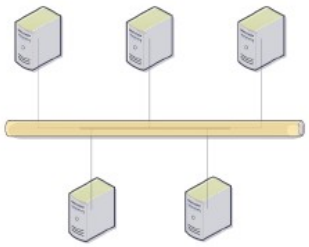
• ***Topoloxía física***: Define o cable así como a disposición física da rede, é dicir, a maneira na que os nodos están conectados uns cos outros. Por exemplo, unha topoloxía particular pode determinar non só o tipo de cable usado, senón, ademais, por onde pasa o cable.

• ***Topoloxía lóxica***: É a forma na que se transmiten os sinais polo cable, isto é, o método que usa un nodo para comunicarse cos demais, e a rota que toman os datos da redes entre os diferentes nodos da mesma. A topoloxía lóxica define o camiño lóxico que os datos toman para ir dun equipo a outro.

A topoloxía lóxica pode coincidir ou non coa topoloxía física.

10.2.1 Topoloxías físicas

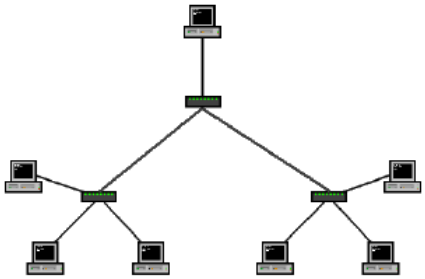
- A **topoloxía en bus**, a miúdo, recibe o nome de “bus liñal”, porque os equipos conéctanse en liña recta. Este é o método máis simple e común utilizado nas redes de equipos. Consta dun único cable chamado segmento central (trunk; tamén chamado backbone ou segmento) que conecta todos os equipos da rede nunha única liña.



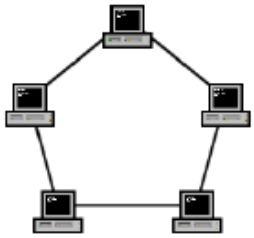
- Na **topoloxía en estrela**, os segmentos de cable de cada equipo están conectados a un compoñente centralizado, como por exemplo un hub. Os sinais son transmitidos desde o equipo emisor a través do hub a todos os equipos da rede. Esta topoloxía utilizouse xa nos inicios da informática, cando se conectaban equipos a un gran equipo central ou mainframe.

A rede en estrela ofrece a vantaxe de centralizar os recursos e a xestión. Sen embargo, como cada equipo está conectado a un punto central, esta topoloxía require unha grande cantidade de cables na instalación da rede. Ademais, se o punto central falla, cae toda a rede.
Nunha rede en estrela, se falla un equipo (ou o cable que o conecta ó nodo central), o equipo afectado será ó único que non poderá enviar ou recibir datos da rede. O resto da rede continuará funcionando normalmente.

- Podemos combinar varias redes en estrela de forma xerárquica. Formaremos así unha **topoloxía de estrela estendida ou árbore**, como podemos ver na seguinte figura:

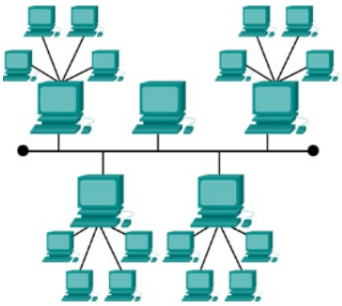


- A **topoloxía en anel** conecta equipos nun único círculo pechado de cable. A diferencia da topoloxía en bus, non existen finais con terminadores. O sinal viaxa a través do bucle nunha dirección, e pasa a través de cada equipo que pode actuar como repetidor para amplificar o sinal e envialo ó seguinte equipo. O fallo dun equipo pode ter impacto sobre toda a rede.



- A **topoloxía de malla ou interconexión total** ofrece unha redundancia e fiabilidade superiores. Cada equipo está conectado a todos os demais equipos mediante cables separados. Esta configuración ofrece camiños redundantes por toda a rede, de modo que se falla un cable, outro se fará cargo do tráfico.
  Aínda que a facilidade de solución de problemas e o aumento da fiabilidade son vantaxes moi interesantes, estas redes resultan caras de instalar, xa que utilizan moito cableado. En moitas ocasións, a topoloxía en malla utilízase xunto con outras topoloxías para formar unha topoloxía híbrida.

- A **topoloxía híbrida** combina dúas ou mais topoloxías de rede básicas. A vantaxe é que se pode implementar en diferentes entornos de rede. O inconveniente é que é complexa de configurar e manter.



10.2.2 Topoloxías lóxicas

¿Que é? A topoloxía lóxica define a forma na que os sinais se transmiten a través do medio. Pode coincidir ou non coa topoloxía física.
Está fortemente relacionada co mecanismo utilizado para administrar a forma na que os equipos acceden á rede. Dado que un cable nunha rede só pode atender a un equipo á vez, é necesario ter procedementos para administrar o acceso á rede, de forma tal que todas as estacións teñan acceso sen que existan conflitos entre elas. Estes procedementos chámanse métodos de control de acceso ao medio. Existen dúas topoloxías lóxicas fundamentais: en bus e en anel.

Nota: para non extender este apartado máis, déixovos uns enlaces para que ampliedes información.
- Redesbasico150. Topologías lógicas.
- Tema2. Redes de comunicación: Topología y enlaces. Universidad de Valencia. [PDF]

- ARQUITECTURA DE REDE -

1. Estándares e protocolos.

Moitos fabricantes de software e hardware proporcionan produtos para a conexión de equipos en rede. Fundamentalmente, as redes son un medio de comunicación, de aí que a necesidade dos fabricantes de tomar medidas para asegurar que os seus produtos puideran interactuar foi xa prematura no desenvolvemento das tecnoloxías de redes.
Como as redes e os provedores de produtos para redes están estendidos por todo o mundo, a necesidade dunha estandarización increméntase. Para dirixir os aspectos que atinxen á estandarización, varias organizacións independentes crean especificacións estándares de deseño para os produtos de redes de equipos. Cando se manteñen estes estándares, é posible a comunicación entre produtos hardware e software de diversos vendedores.
Estes estándares definen fundamentalmente unha serie de **protocolos**. Os protocolos son regras e procedementos para a comunicación. O termo protocolo utilízase en distintos contextos. Estes protocolos, ou regras de comportamento, son **especificacións estándar** para dar formato aos datos e transferilos. Algúns dos organismos mais coñecidos: IEEE, ISO, TIA, ANSI, IETF, SANS, W3C, ICANN, ...

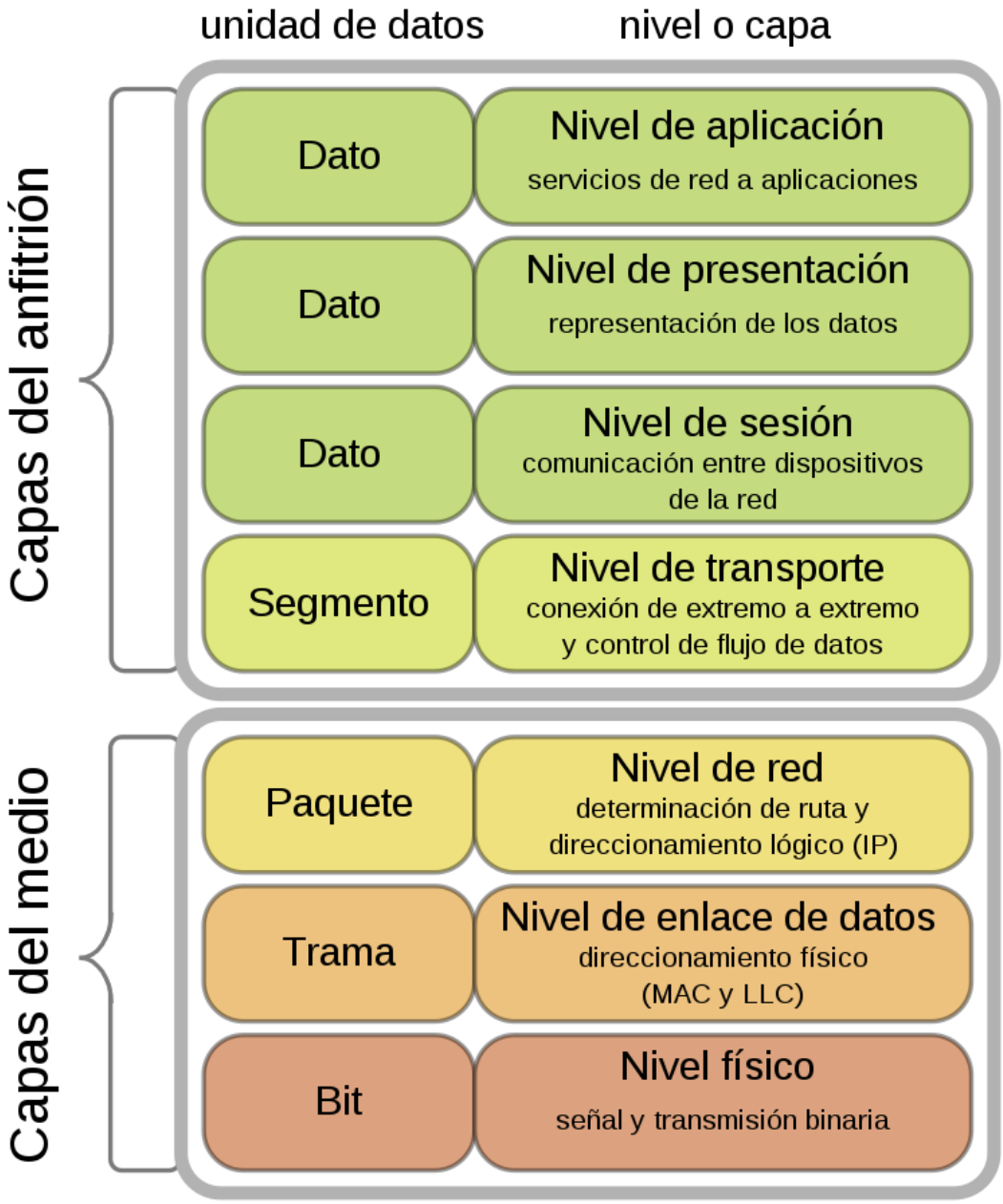
2. Modelo OSI.

2.1 Historia do modelo OSI

En 1978, a International Standards Organization, ISO (Organización internacional de estándares) divulgou un conxunto de especificacións que describían a arquitectura de rede para a conexión de dispositivos diferentes. O documento orixinal aplicouse a sistemas que eran abertos entre si, debido a que todos eles podían utilizar os mesmos protocolos e estándares para intercambiar información.
En 1984, a ISO presentou unha revisión deste modelo e o chamou modelo de referencia de Interconexión de Sistemas Abertos (OSI) que se converteu nun estándar internacional e se utiliza como guía deseñar e estudar a estrutura para as redes.
O modelo OSI é a guía mellor coñecida e máis amplamente utilizada para a visualización de contornos de rede. Os fabricantes axústanse ó modelo OSI cando deseñan o seus produtos para rede.
Este ofrece unha descrición do funcionamento conxunto de hardware e software de rede por niveis para posibilitar as comunicacións. O modelo tamén axuda a localizar problemas proporcionando un marco de referencia que describe o suposto funcionamento dos compoñentes.

2.2 Características do modelo OSI

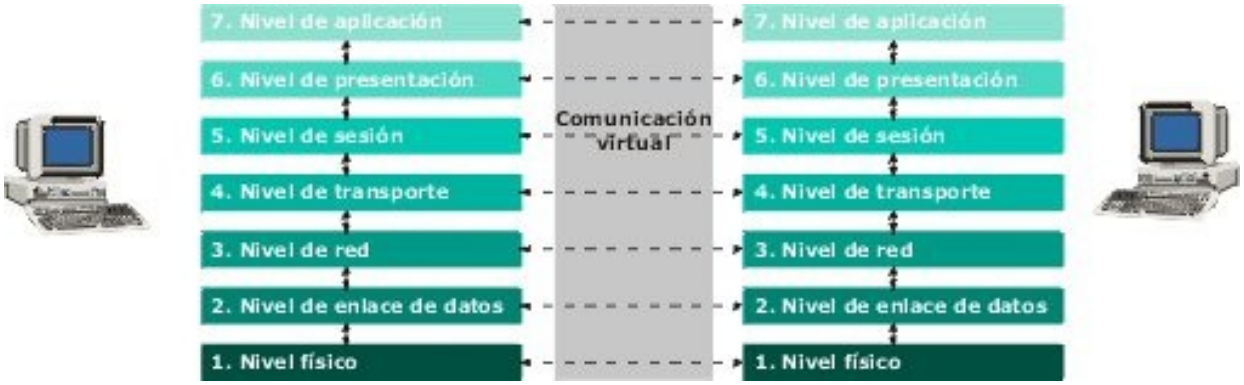
O modelo OSI representa sete niveis de proceso mediante o cal os datos empaquétanse e transmítense dende unha aplicación emisora a través de cables físicos cara a aplicación receptora.



Cada nivel cobre diferentes actividades, equipos ou protocolos de rede. O modelo OSI define como se comunica e traballa cada nivel cos niveis inmediatamente superior e inferior. Por exemplo, o nivel de sesión comunícase e traballa cos niveis de presentación e de transporte.

Dúas razóns fundamentais son as que levan a dividir a arquitectura das redes en niveis:
• As redes de ordenadores son sistemas complexos, que son máis fáciles de construír e manexar se se dividen e subsistemas máis simples.
• As tecnoloxías das redes cambian con moita rapidez, de forma que é de vital importancia conseguir que os distintos subsistemas sexan independentes entre si.

Cada nivel proporciona servizos ao nivel inmediatamente superior que o protexe dos detalles de implementación dos servizos dos niveis inferiores. Ao mesmo tempo, a cada nivel lle parece estar en comunicación directa co seu nivel asociado do outro equipo. Ás entidades de niveis correspondentes de máquinas distintas se lles chama **entidades pares**. Isto proporciona unha comunicación lóxica, ou virtual, entre niveis análogos.

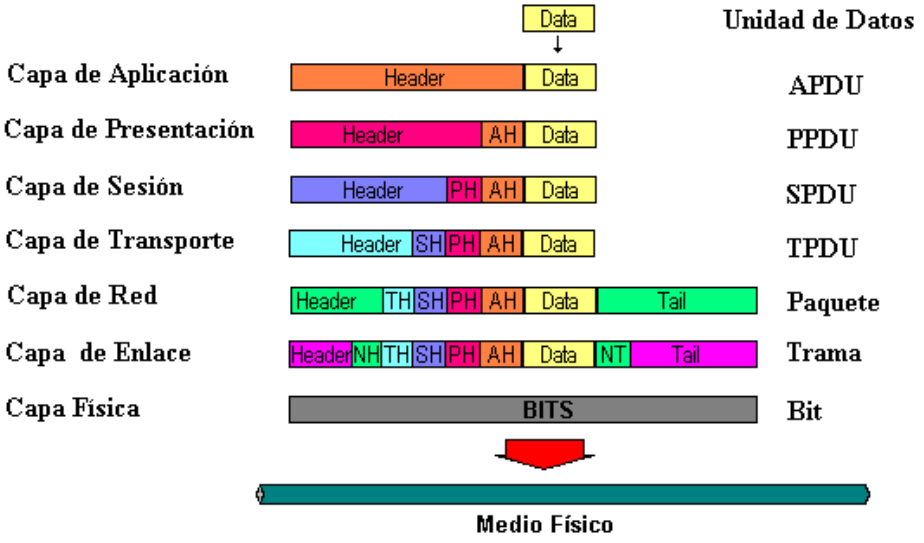


En cada nivel, o software implementa as funcións de rede de acordo con un conxunto de protocolos.

2.3 Os paquetes de datos

O proceso de creación de paquetes iníciase no nivel de aplicación do modelo OSI, onde se crean os datos. A información a enviar a través da rede comeza no nivel de aplicación e descende ó longo dos sete niveis.
En cada nivel, agrégase ós datos información relevante dese nivel. Esta información é utilizada polo correspondente nivel do equipo receptor. O nivel de enlace de datos do equipo receptor, por exemplo, lerá a información agregada no nivel de enlace de datos do equipo emisor.
No nivel de transporte, o bloque de datos orixinal divídese nos paquetes reais. O protocolo define a estrutura dos paquetes utilizados polos dous equipos.
Cando o paquete alcanza o nivel de transporte, agrégase unha secuencia de información que guía ao equipo receptor na desagrupación dos datos dos paquetes.

Cando, finalmente, os paquetes pasan a través do nivel físico ao cable, conteñen información de cada un dos outros seis niveis.



3. A pila de protocolos TCP/IP

3.1 Características de TCP/IP

O **Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP)** é un conxunto de protocolos aceptados pola industria que permiten a comunicación nun contorno heteroxéneo (formado por elementos diferentes). Ademais, TCP/IP proporciona un protocolo de rede encamiñable e permite acceder a Internet e ós seus recursos. Debido á súa popularidade, TCP/IP converteuse no estándar de facto (aceptado polos fabricantes) no que se coñece como interconexión de redes, a intercomunicación nunha rede que está formada por redes máis pequenas.

TCP/IP converteuse no protocolo estándar para a interoperabilidade entre distintos tipos de equipos. A interoperabilidade é a principal vantaxe de TCP/IP. A maioría das redes permiten TCP/IP como protocolo. TCP/IP tamén permite o encamiñamento e soese utilizar como un protocolo de interconexión de redes.

Deseñado para ser encamiñable, robusto e funcionalmente eficiente, TCP/IP foi desenvolvido polo Departamento de Defensa de Estados Unidos como un conxunto de protocolos para redes de área extensa (WAN). O seu propósito era o de manter enlaces de comunicación entre sitios no caso dunha guerra nuclear. Actualmente, a responsabilidade do desenvolvemento de TCP/IP reside na propia comunidade de Internet.

3.2 Vantaxes de TCP/IP

A utilización de TCP/IP ofrece varias vantaxes:

• É un **estándar na industria**: Como un estándar da industria, é un protocolo aberto. Isto quere dicir que non está controlado por unha única compañía, e está menos suxeito a cuestións de compatibilidade. É o protocolo, de feito, de Internet.

• **Contén un conxunto de utilidades para a conexión de sistemas operativos diferentes**: A conectividade entre un equipo e outro non depende do sistema operativo de rede que estea utilizando cada equipo.

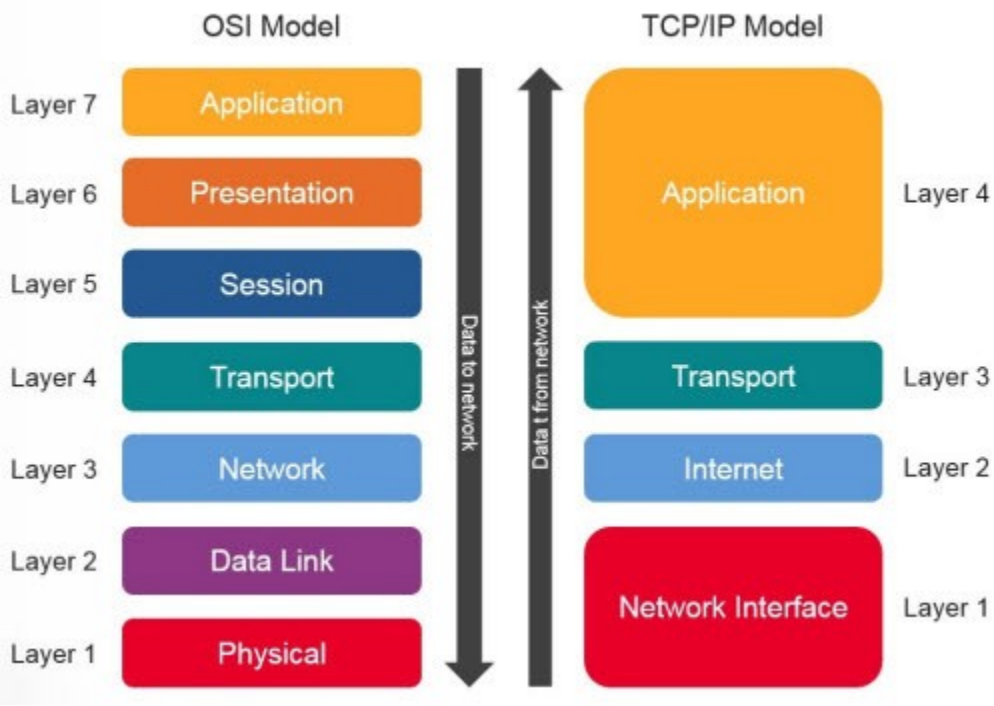
• **Utiliza unha arquitectura escalable, cliente/servidor**: TCP/IP pode ampliarse (ou reducirse) para axustarse ás necesidades e circunstancias futuras. Utiliza sockets para facer que o sistema operativo sexa algo transparente. Un socket é un identificador para un servizo concreto nun nodo concreto da rede. O socket consta dunha dirección de nodo e dun número de porto que identifica ao servizo.

3.3 Os niveis de TCP/IP

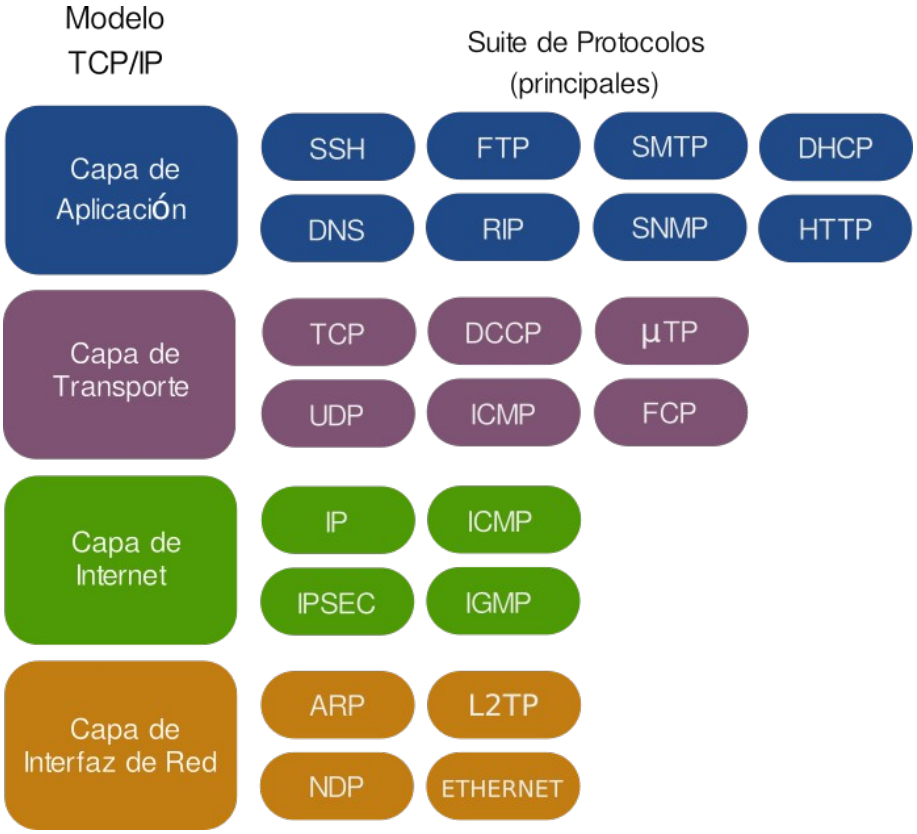
O protocolo TCP/IP non se corresponde exactamente co modelo OSI.

En vez de ter sete niveis, só utiliza catro. Normalmente coñecido como conxunto de protocolos de Internet, TCP/IP divídese en catro niveis, correspondéndose cada un con un ou máis niveis do modelo OSI.

Comparación co modelo OSI



3.4 Protocolos utilizados en cada nivel



Podemos concluír que OSI é un bo modelo de arquitectura de redes aínda que TCP/IP ofrece, sen embargo, unha boa implementación dun conxunto de protocolos, sendo ademais a arquitectura mais amplamente extendida na actualidade.

En moitos casos úsase un conxunto de niveis que combina as dúas arquitecturas:

• Nivel de aplicación

• Nivel de transporte

• Nivel de rede

• Nivel de enlace

• Nivel físico

- DIRECCIONAMENTO EN IPv4 -

1. Descrición do protocolo IP

- O protocolo a nivel de rede máis utilizado nas redes de ordenadores é o protocolo IP (Internet Protocol o Protocolo de Interrede). Este protocolo, que forma parte da pila de protocolos de TCP/IP, popularizouse enormemente debido ao grande éxito deste modelo e da rede Internet, que utiliza estes protocolos.
- IP prove un servizo de datagramas non fiable, xa que non ofrece ningún mecanismo para determinar se un paquete alcanza ou non o seu destino e tampouco realiza ningún tipo de control de erros nos datos transmitidos (protocolo de menor esforzo ou best-effort). Deste xeito, o paquete transmitido podería chegar danado, noutra orde con respecto a outros paquetes, duplicado ou simplemente non chegar.
- O protocolo IP define unha estrutura de paquete formada por unha cabeceira cun mínimo de 20 bytes e unha cola, nas que se inclúe información como dirección de orixe, dirección de destino, comprobación de erros, etc:

Formato da Cabeceira IP (Versión 4)

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabeceira	Tipo de Servizo	Lonxitude Total	
Identificador			Flags	Posición de Fragmento
Time To Live		Protocolo	Suma de Control de Cabeceira	
Dirección IP de Orixe				
Dirección IP de Destino				
Opcións				Recheo

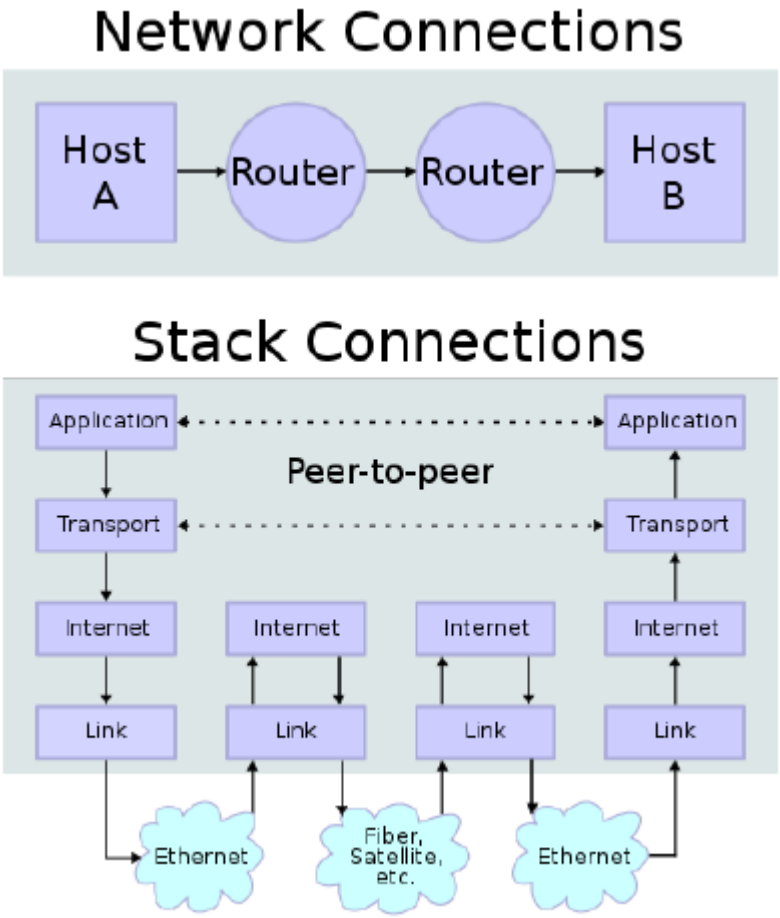
2. Routers e hosts.

No nivel de rede, podemos distinguir dous tipos de equipos dependendo da súa función:

• **Os equipos finais ou hosts,** que son aqueles equipos que envían ou reciben información na rede. Por exemplo, o noso ordenador persoal ou teléfono móbil, ou o servidor web ao que nos conectamos para consultar unha páxina, serían exemplos de hosts.

• **Os encamiñadores ou routers**, que son aqueles equipos intermedios na transmisión dunha mensaxe, xa que a súa función básica é a de dirixir os paquetes que recibe cara o destino. Para facelo, ao recibir un paquete, o router debe extraer deste a dirección de rede do destinatario e decidir cal é a mellor ruta, a partir do algoritmo e táboa de encamiñamento que utilice. Ademais, cada encamiñador ten as súas propias direccións a nivel de rede.

A figura mostra o esquema dunha conexión entre dous equipos finais pasando por dous routers intermedios. Nela podemos observar que mentres os equipos finais implementan os cinco niveis da arquitectura de rede, os router só implementan ata o nivel de rede:



Para realizar o encamiñamento do paquete, o router terá en conta información como número de saltos ou nodos intermedios ata o destino, velocidade de transmisión máxima dos enlaces, custo das transmisións e condicións do tráfico entre os enlaces.

Un router proporciona os seguintes servizos na rede:

✔ Seguridade a través de filtros de paquetes como por exemplo ACLs (Listas de Control de Acceso)

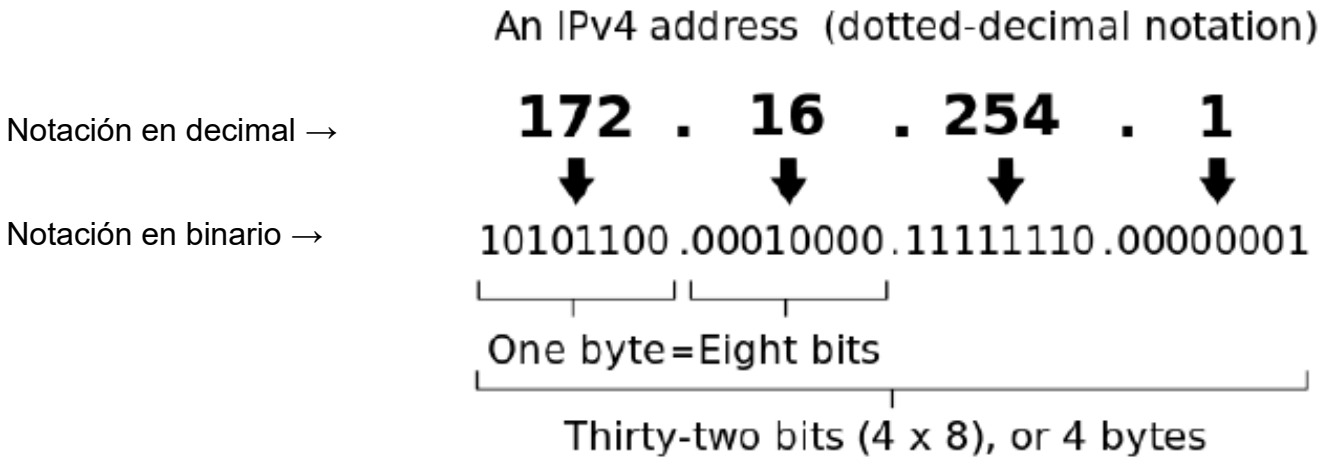
✔ Pode integrar diferentes tecnoloxías de enlace de datos (Ethernet, Token Ring, Conexión sen fíos, etc.)

✔ Permite a existencia de diferentes rutas alternativas contra conxestións e fallos nas comunicacións.

3. Direccións IP. Clases.

IP utiliza as **direccións IP** dun tamaño fixo de **32 bits** (na versión 4 do protocolo) para os equipos da rede.

Estas direccións almacénanse en binario e se poderían especificar en binario, pero é moito máis cómodo usar a notación decimal separada por puntos. Para pasar unha dirección de binario a decimal, só hai que converter os números tomando os bits de 8 en 8 díxitos; despois separamos cada número decimal, que terá un valor entre 0 e 255, por puntos.

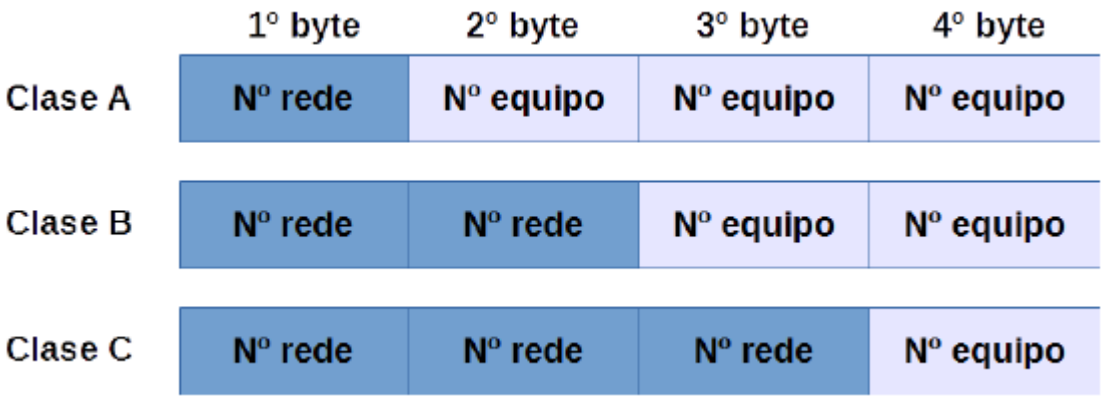


4. Clases de direccións IP

A nivel de rede, as máquinas organízanse en redes independentes que se conectan entre si. Dentro da dirección IP, os números indican en primeiro lugar ***número de rede*** e despois un ***número de equipo*** dentro desa rede.

Cando se deseñou o protocolo IP, o problema era decidir cantos bits reservar para o número de rede e cantos para o número de equipo. Se se puñan moitos bits para as redes, podían definirse moitas redes, pero moi poucos equipos, e o mesmo á inversa.

Por iso optouse por unha solución que permite ter distintos tipos de direccións con diferentes tamaños para os dous campos. Concretamente, definíronse as seguintes clases de direccións:



En cada clase repártense os bytes da dirección IP de forma diferente. A clase da dirección ven indicada polo valor dos primeiros bits da mesma (que sempre forman parte do número de rede e coñécense como ***identificador de clase***).

Polo tanto, temos estas clases de redes que se completan coas clases D e E que teñen un uso específico. Na seguinte táboa de cada clase de rede podemos ver:

• Cales son os bits de comezo que identifican ás direccións desa clase.

• O rango das direccións que pertencen a ela.

• O número de bits que forman o número de rede, excluíndo os do identificador da clase.

• O número de redes distintas que existen desa clase ($2^{\text{bits nº rede}}$).

• O número de bits que forman o número de equipo.

• O número de direccións IP distintas que hai en cada rede desa clase ($2^{\text{bits nº equipo}}$).

Clase IP	Id	Rango	Bits nº rede	Nº redes	Bits nº equipo	Nº IPs por rede
A	0	1.0.0.0 – 127.255.255.255	7 bits	127	24 bits	16777216
B	10	128.0.0.0 – 191.255.255.255	14 bits	16384	16 bits	65536
C	110	192.0.0.0 – 223.255.255.255	21 bits	2097152	8 bits	256
D	1110	224.0.0.0 – 239.255.255.255	28 bits	Reservadas para *multicast*		
E	11110	240.0.0.0 – 247.255.255.255	27 bits	Reservadas para usos futuros		

As direccións de clase D están reservadas para mensaxes de multidifusión ou multicast, que son mensaxes dirixidos a un conxunto de varios equipos. As direccións de clase E están reservadas para usos futuros e só se utilizan experimentalmente.

5. Direccións IP públicas e privadas.

As direccións IP configúranse por parte do usuario, pero non se poden utilizar as direccións que se queiran, xa que entón podería haber moitos equipos coa mesma dirección.

Por iso, existe un organismo chamado ICANN encargado de asignar direccións de Internet para impedir duplicados. Este organismo só asigna unha clase e número de rede, e despois o administrador da rede é o que debe asignar os números para cada estación da mesma.

Sen embargo, non sempre necesitamos reservar direccións únicas para todos os equipos do mundo. Non pode haber dous equipos en Internet que teñan a mesma dirección IP, pero si

pode haber equipos con direccións IPs repetidas sempre que non estean conectados na mesma rede. É por iso que existen unhas direccións IPs determinadas reservadas para o uso privado, e que se poden asignar a equipos que non están conectados a Internet (a lo menos directamente, como veremos máis adiante), e que non é necesario reservar xa que se poden repetir. Estas direccións se coñecen como **direccións IP privadas**, en contraposición ás direccións únicas asignadas por ICANN que se coñecen como **direccións públicas**.

As direccións IP privadas posibles son:
• Para unha rede de clase A: A rede 10.0.0.0.
• Para redes de clase B: As direccións de 172.16.0.0 a 172.31.0.0 (16 redes clase B)
• Para redes de clase C: As direccións de 192.168.0.0 a 192.168.255.0 (256 redes clase C)

6. Asignación de direccións IP nunha rede.

Por exemplo, se solicitamos unha dirección de clase C para unha rede que vai a ter menos de 200 equipos, poderíasenos asignar a dirección 192.118.64.0.
Con isto temos 256 direccións distintas (dende 0 a 255) e poderiamos pensar que podemos polo tanto asignar direccións a 256 máquinas, pero isto non é así.

IMPORTANTE: Existen algunhas direccións do rango que non se poden asignar a equipos, xa que:

• A dirección co nº de equipo con todos os bits a 0 utilízase para identificar a rede (**dirección de rede**), utilizada nos mecanismos de direccionamento.

• A dirección co nº de equipo con todos os bits a 1 utilízase para enviar unha mensaxe a todos os equipos da rede; é o que se denomina mensaxe de **broadcast**.

Polo tanto, neste caso a rede tería un número máximo de equipos de 254, e non 256.

IMPORTANTE: Ademais, tamén existen unha serie de direccións non utilizadas por estar reservadas para fins específicos:

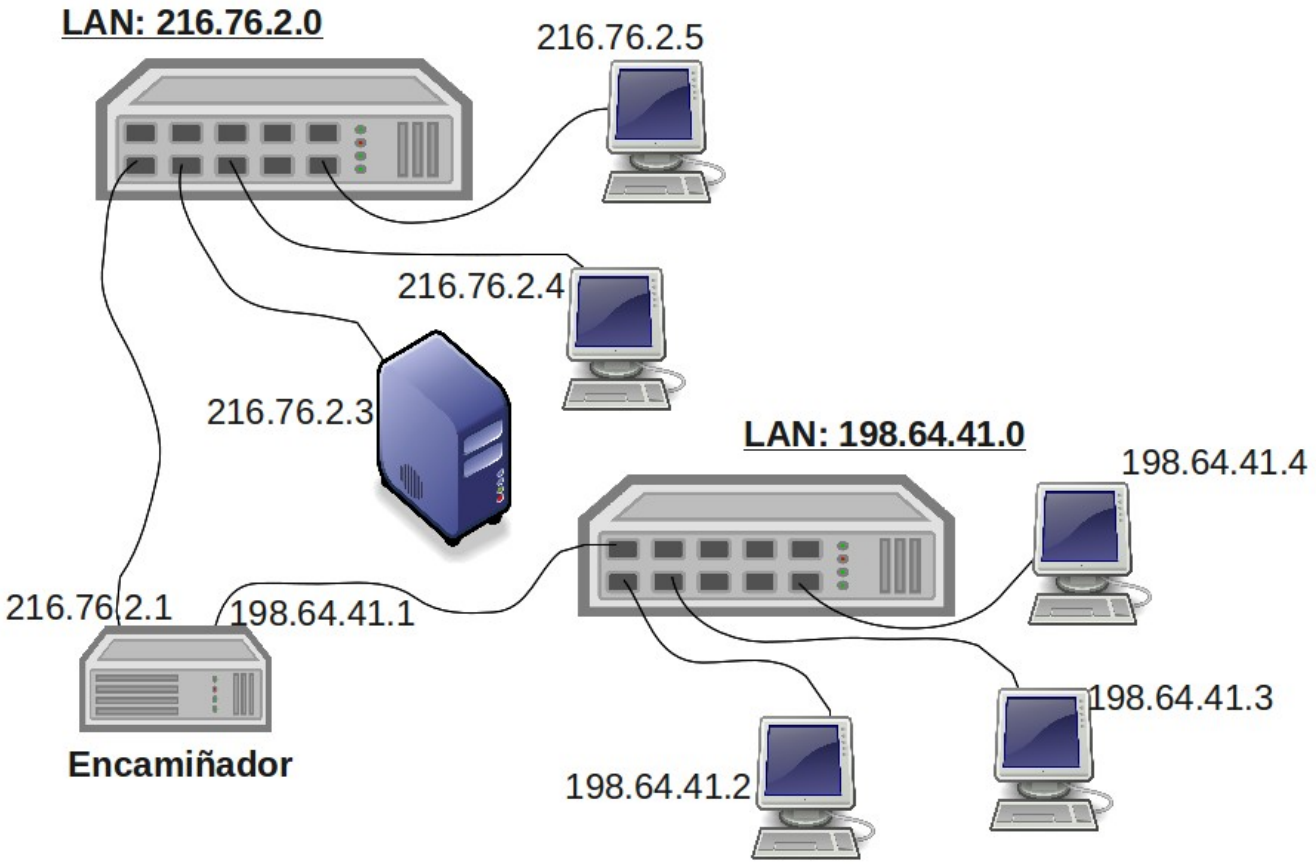
• A dirección 0.0.0.0 úsase por equipos sen disco duro cando arrancan durante a carga do sistema operativo.

• A dirección 127.0.0.1 úsase para especificar un enlace co propio equipo, de forma que sempre en calquera ordenador (aínda que non dispoña de tarxeta de rede) poderemos establecer unha conexión coa propia máquina local usando esta dirección IP. Recibe o nome de **dirección de bucle local ou loopback**. En realidade, están reservadas para este uso as direccións dende a 127.0.0.1 á 172.255.255.254.
RECORDADE: isto vímolo cando traballabamos cos comandos ifconfig, ip ad ou ipconfig (en Linux e Windows).

• As direccións de 169.254.0.1 a 169.254.255.254, coñecidas como direccións IP privadas automáticas (APIPA) están reservadas para o seu uso nos equipos Windows cando están configuradas para tomar a configuración IP de forma automática e non atopan ningún servidor DHCP que lles poida asignar esta configuración.

6.1 Exemplo básico de asignación de direccións IP

A asignación de direccións IP aos distintos equipos dunha rede é un paso importante dentro do deseño da mesma, e no que haberá que ter en conta todos estes factores. No caso dos encamiñadores, deberán ter unha dirección IP por cada conector de rede (ou porto, ou boca) que incorpore.
A cada equipo da rede asignarémoslle unha dirección IP que non sexa a *dirección de rede* nin a de *broadcast*, normalmente de forma correlativa para levar un control das direccións que xa temos asignadas e as que temos libres. É habitual que o router que conecta unha rede co exterior se lle asigne a primeira dirección IP da rede, aínda que non é obrigatorio facelo así.
Por exemplo, na seguinte figura podemos ver dúas redes LAN coas direccións IP dos distintos equipos conectadas por un encamiñador:



7. A máscara de rede.

7.1 Estrutura das máscaras de rede.

Aínda que nun principio a clase da dirección IP determina qué parte da dirección IP é o número de rede e qué parte é o número de equipo dentro da rede, en realidade os equipos utilizan para iso a máscara de rede (ou subrede, como xa veremos máis adiante).

A máscara de rede é unha dirección IP (xa que é un conxunto de 32 bits) que ten todo 1's na parte de dirección de rede e todo ceros na parte de dirección de equipo. Polo tanto, unha máscara de rede ten que ser obrigatoriamente unha sucesión correlativa de un ou varios uns seguida de unha sucesión de cero ou varios ceros correlativos.

A continuación vemos unha serie de exemplos de máscaras de rede:

Rede	Clase	Máscara	Máscara en binario
216.89.3.0	C	255.255.255.0	11111111.11111111.11111111.00000000
198.64.126.0	C	255.255.255.0	11111111.11111111.11111111.00000000
188.119.0.0	B	255.255.0.0	11111111.11111111.00000000.00000000
23.0.0.0	A	255.0.0.0	11111111.00000000.00000000.00000000

Así, a máscara da primeira fila (255.255.255.0) ven a indicar que os 24 primeiros bits da dirección IP son o número de rede, mentres que os 8 últimos son o número de equipo dentro da rede. Isto é o que se corresponde coas redes de clase C.

7.1.1 Formatos de representación das máscaras de rede.

As máscaras pódense representar en 3 formatos diferentes:
- Binario
`11111111.00000000.00000000.00000000`

- Notación decimal punteada ou Dotted-decimal notation (DDN)
`255.0.0.0`

- Prefijo (classless interdomain routing [CIDR]): É dicir, o número de bits da máscara que están a 1 antecedido por unha barra lateral.
`/8`

NOTA: Nos 3 exemplos indícase a mesma máscara.

Para facer os cálculos hai que ter en conta a conversión de binario a decimal e viceversa que vimos no principio de curso.

Se nos dan unha máscara poderemos transformala en calquera notación, como se pode ver nos seguintes exemplos:

7.2 O uso da máscara de rede.

Grazas á máscara de rede, un equipo pode saber a partir da súa dirección IP cal é a dirección da rede á que pertence, simplemente poñendo a cero todos os bits da dirección IP que se corresponden co número de equipo. Para facelo, aplica o operador lóxico AND (Y) a nivel de bit entre a súa dirección IP e a máscara de rede.

O funcionamento do operador AND entre dous bits é o seguinte:

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Polo que o resultado do AND só é 1 se os dous bits son 1, e 0 en calquera outro caso.
Podemos equiparar a operación AND entre bits á multiplicación, xa que calquera bit AND 0 da como resultado 0, mentres que calquera bit AND 1 da ese bit.

Desta maneira, ao aplicar a operación AND entre unha dirección IP e unha máscara, o que vai pasar é que todos aqueles bits da dirección IP que se correspondan con uns na máscara quedarán co mesmo valor, mentres que os que se correspondan ceros quedarán postos a cero.
Así obteremos a dirección da rede, que é aquela que mantén o número de rede e ten todos os bits correspondentes co número de equipo a cero.

8. Subdivisión de redes.

Algunhas veces é necesario facer subdivisións de rede para poder conseguir adaptar a rede ás características propias do contexto en que nos encontramos por iso é bo coñecer tamén como facer ditas subdivisións. Para iso utilizaremos tanto as clases como as direccións de rede proporcionada e a máscara de rede asociada. Veremos proximamente un exemplo pero antes é interesante coñecer uns conceptos básicos.

¿Para qué é necesario subidividir redes?

A segmentación das redes en outras mais pequenas de dispositivos e servizos é para conseguir:
- Controlar o tráfico mediante a contención do tráfico de broadcast dentro da subrede.
- Reducir o tráfico xeral da rede e mellorar o rendemento desta.

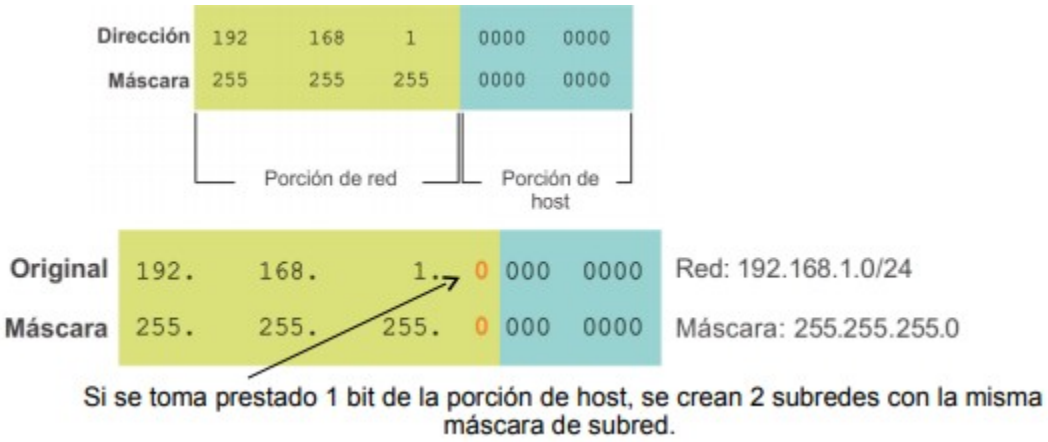
Comunicación entre as subredes.

É necesario un router para que os dispositivos que estean en diferentes redes e subredes podan comunicarse entre eles. Ademais cada interfaz do router debe ter unha dirección de host IPv4 que pertenza á rede ou subrede á cal se conecta a interfaz do router.
Os dispositivos dunha rede ou subrede utilizan esa interfaz do router conectada á súa LAN como ***gateway*** (recordade que falamos del como a primeira porta de saída fóra da rede) predeterminado.

División básica en subredes.

Exemplo e imaxes sacadas de:
Cisco Networking Academy. Introducción a redes. Capítulo 9: División de redes IP en subredes. Ing. Aníbal Coto Cortés

Para a subdivisión dunha rede é necesario o préstamo de bits da parte de host para a creación destas subredes.
Por exemplo, temos a IP 192.168.1.0 con máscara /24, se se toma 1 bit prestado da parte de hosts (sempre empezando pola parte esquerda) conseguimos 2^1= 2 subredes como está indicado ao final da seguinte imaxe.



Subred 0

Red 192.168.1.0-127/25

Máscara: 255.255.255.128

Subred 1

Red 192.168.1.128-255/25

Máscara: 255.255.255.128

✔ A máscara suma 1 bit mais de 1's, entón a máscara pasa a ser /25, é dicir 255.255.255.128

✔ A primeira subrede será a 192.168.1.0/25 e a segunda subrede será a 192.168.1.128/25

Rango de direccións para a subrede 192.168.1.0/25

Dirección de red

192.	168.	1.	0	000 0000	= 192.168.1.0

Primera dirección de host

192.	168.	1.	0	000 0001	= 192.168.1.1

Última dirección de host

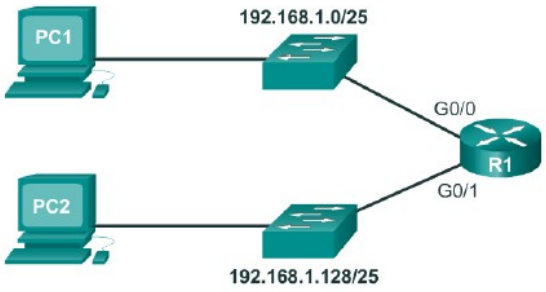
192.	168.	1.	0	111 1110	= 192.168.1.126

Dirección de broadcast

192.	168.	1.	0	111 1111	= 192.168.1.127

Subred 0

Red 192.168.1.0-127/25



Subred 1

Red 192.168.1.128-255/25

Rango de direccións para a subrede 192.168.1.128/25

Dirección de red

192.	168.	1.	1	000 0000	= 192.168.1.128

Primera dirección de host

192.	168.	1.	1	000 0001	= 192.168.1.129

Última dirección de host

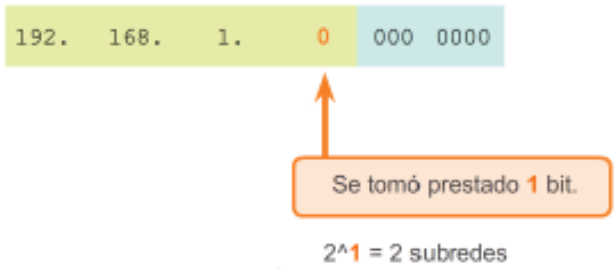
192.	168.	1.	1	111 1110	= 192.168.1.254

Dirección de broadcast

192.	168.	1.	1	111 1111	= 192.168.1.255

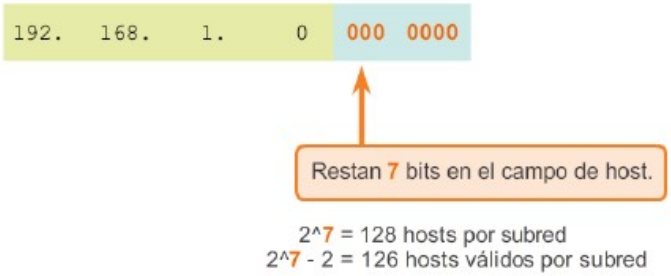
Para o cálculo da cantidade de subredes

Subredes = 2^n
onde n é a cantidade de bits que se "toman prestados" para as subredes.



Para o cálculo de número de hosts

Hosts = 2^n
onde n é o número de bits de host restantes

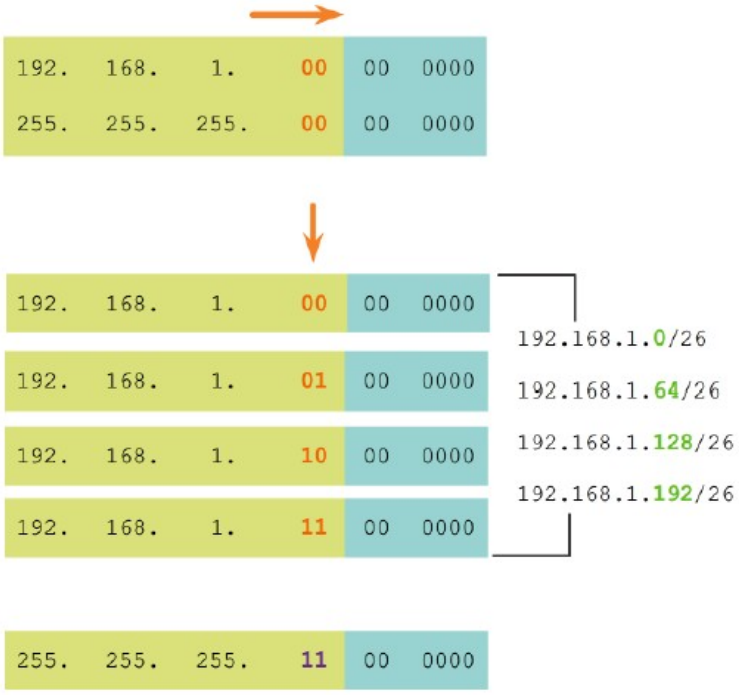


Ollo, a primeira dirección de host é para a dirección de rede e a última para a dirección de broadcast. Son dúas direccións IP que non se poden utilizar. Isto fai que o número de hosts válidos sexa: 2^n - 2
Os hosts válidos son realmente o número de IP's dispoñibles/utilizables para asignar a equipos. E esta información hai que tela en conta por se se pide unha restricción de hosts por rede.

Variantes do exercicio anterior.

- ¿E se queremos dividir a rede, en vez de en dúas subredes, en 4?

Temos que buscar o "n" que en 2^n nos 4 ou un número maior (xa que polo menos teremos 4 subredes). Neste caso $2^2 = 4$. Con 2 bits temos xusto para facer as 4 subredes.

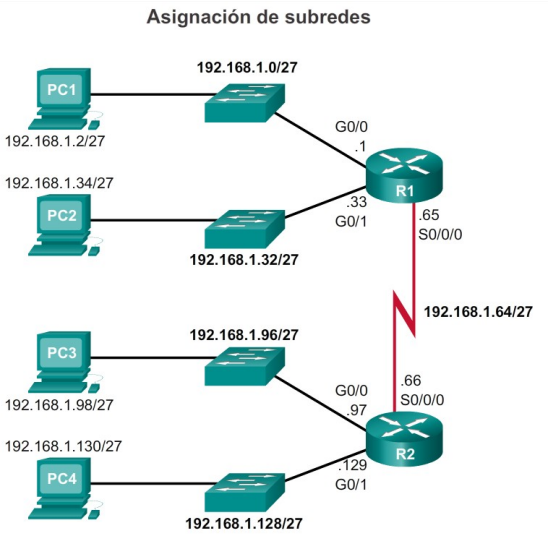


Estas serán as 4 subredes con máscara con dous bits mais, polo tanto /26.

- ¿E se queremos dividir a rede, en vez de en dúas subredes, en 8?

Seguirá o mesmo principio pero en vez de 2 bits necesitaremos 3 para engadir á máscara.

Red 0	Red	192.	168.	1.	000	0	0000	192.168.1.0
	Primero	192.	168.	1.	000	0	0001	192.168.1.1
	Última	192.	168.	1.	000	1	1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1	1111	192.168.1.31
Red 1	Red	192.	168.	1.	001	0	0000	192.168.1.32
	Primero	192.	168.	1.	001	0	0001	192.168.1.33
	Última	192.	168.	1.	001	1	1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1	1111	192.168.1.63
Red 2	Red	192.	168.	1.	010	0	0000	192.168.1.64
	Primero	192.	168.	1.	010	0	0001	192.168.1.65
	Última	192.	168.	1.	010	1	1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1	1111	192.168.1.95
Red 3	Red	192.	168.	1.	011	0	0000	192.168.1.96
	Primero	192.	168.	1.	011	0	0001	192.168.1.97
	Última	192.	168.	1.	011	1	1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1	1111	192.168.1.127
Red 4	Red	192.	168.	1.	100	0	0000	192.168.1.128
	Primero	192.	168.	1.	100	0	0001	192.168.1.129
	Última	192.	168.	1.	100	1	1110	192.168.1.158
	Broadcast	192.	168.	1.	100	1	1111	192.168.1.159
Red 5	Red	192.	168.	1.	101	0	0000	192.168.1.160
	Primero	192.	168.	1.	101	0	0001	192.168.1.161
	Última	192.	168.	1.	101	1	1110	192.168.1.190
	Broadcast	192.	168.	1.	101	1	1111	192.168.1.191
Red 6	Red	192.	168.	1.	110	0	0000	192.168.1.192
	Primero	192.	168.	1.	110	0	0001	192.168.1.193
	Última	192.	168.	1.	110	1	1110	192.168.1.222
	Broadcast	192.	168.	1.	110	1	1111	192.168.1.223
Red 7	Red	192.	168.	1.	111	0	0000	192.168.1.224
	Primero	192.	168.	1.	111	0	0001	192.168.1.225
	Última	192.	168.	1.	111	1	1110	192.168.1.254
	Broadcast	192.	168.	1.	111	1	1111	192.168.1.255



No exemplo da imaxe superior están establecidas 5 das 8 direccións de subrede pero poderiamos ter as 8. É dicir, como máximo poderiamos dividir con esta máscara ata 8 subredes.

Cumprimento dos requisitos dunha rede.

É importante lograr un equilibrio entre a cantidade de subredes necesarias e a cantidade de hosts que se requiren para a subrede mais grande. Moitas veces imos ter que ver a cantidade de hosts que son necesarios nunha rede (últimos bits da subrede).
Deberiamos:
- Deseñar o esquema de direccionamento para poder admitir a cantidade máxima de hosts para cada subrede.
- Deixar espazo para o crecemento en cada subrede.

Para unha subdivisión de subredes máis eficiente das direccións poderemos utilizar **máscaras de subrede de lonxitude variable** (**VLSM**). Non o veremos neste resumo pero podedes buscar información sobre isto.

8.1 Exemplo de exercicio de subredes explicado.

Enunciado: Unha empresa ten unha rede de clase C 195.100.205.0 e quérea dividir en 4 subredes.

Solución:

1. ¿Cal será a máscara de subrede?

195.100.205.0 → Clase C → 1 byte para identificar os host, é dicir, podemos coller ata 8 bits para subredes (dentro dos bits de host) e engadirllos á máscara de rede para conseguir as subredes.

195.100.205.X = 195.100.205.xxxxxxxx

2. ¿Cántas subredes necesitamos?
4 Subredes → Coller 2 bits da parte ID del host

Agora debemos controlar ben o paso a binario e a utilización do AND lóxico.
1a Subred: 195.100.205.**00**000000 = 195.100.205.0
2a Subred: 195.100.205.**01**00000 = 195.100.205.64
3a Subred: 195.100.205.**10**000000 = 195.100.205.128
4a Subred: 195.100.205.**11**000000 = 195.100.205.192

3. ¿Qué modificación da máscara por defecto deberemos utilizar?

Máscara de subred → /26

255.255.255.192 =1111111.11111111.11111111.11000000

9. Protocolos en redes.

9.1 O protocolo ARP

O protocolo IP é o encargado de decidir cal debe ser o seguinte destino dun paquete no seguinte salto para conseguir chegar ó destino final. Para iso, o protocolo baséase nas direccións IP dos equipos/dispositivos intermedios. Esas direccións IP son totalmente independentes das direccións utilizadas a nivel de enlace (dirección MAC).

O protocolo ARP (Address Resolution Protocol ou Protocolo de Resolución de Direccións) funciona na capa de enlace e é o responsable de encontrar a dirección MAC que corresponde con unha dirección IP. Para isto enviar paquetes ARP Request á dirección de broadcast da rede que contén a dirección IP pola que pregunta e espera que unha máquina lle responda (ARP Replay) coa dirección IP correspondente.

✔ As **direccións IP** identifican univocamente a todos os equipos e dispositivos conectados a unha rede. É un número que identifica a cada dispositivo.
✔ A **dirección MAC** está presente en todos os dispositivos que contan cunha tarxeta de rede. Tamén é un identificador único. É un número que cada fabricante asigna a un dispositivo en concreto. Por esta razón pode ser que un equipo teña varias direccións MAC. Por exemplo, un ordenador pode ter unha tarxeta de rede para conectarnos por cable e outra para conectarnos por WIFI e cada unha delas ten unha dirección MAC.

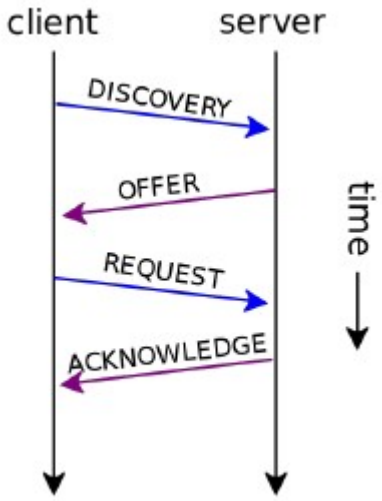
Para saber mais sobre este protocolo:

- Wikipedia. Protocolo de resolución de direcciones.
- Redes locales y globales. Protocolo ARP (Adress Resolution Protocol)
- AprendeDeRedes. ARP: Adress Resolution Protocol
- Tamén é interesante buscar información sobre "*suplantación de ARP ou ARP Spoofing*".

9.2 Asignación dinámica de direccións. Protocolo DHCP

O protocolo DHCP (Dynamic Host Configuration Protocol ou Protocolo de Configuración Dinámica de Estación) permite ás estacións da rede que se lles asigne unha dirección IP automaticamente cando se conectan á rede. Así, as direccións IP permanecen libres mentres non se necesitan.
Para iso, un dispositivo solicita unha dirección enviando unha mensaxe de broadcast, que é procesado por unha estación da rede que actúa como servidor DHCP (por exemplo un router). Este equipo servidor mantén unha táboa de direccións libres e asignadas na rede. Unha vez que o cliente recibe a dirección, confirma ao servidor DHCP cal é a IP tomada. Así o servidor ten constancia de que esa dirección xa está asignada.
Esta opción de direccionamento dinámico é moi utilizada tanto en Internet, co obxectivo de poder facer uso de menos direccións IP e repartilas así só entre os equipos conectados en cada momento á rede; e nas redes de área local, co obxectivo de simplificar a administración dos equipos, xa que a configuración de direccións IPs está centralizada no servidor.

Ademais, o servidor DCHP permite normalmente opcións avanzadas para, por exemplo, poder reservar unha dirección IP para unha dirección MAC determinada, de forma que sempre se lle asigne a mesma. Desta forma temos unha dirección IP fixa para o equipo establecida dinamicamente. Tamén é posible asignarlle ao cliente máis información que a dirección IP que ten que utilizar, como a porta de enlace, o servidor de DNS, etc.



Para saber mais sobre este protocolo:

- OpenWebinars. Qué es un servidor DHCP
- Medium.com ¿Qué es la inspección DHCP (DHCP Snooping) y cómo funciona?

9.3 O protocolo ICMP

O protocolo ICMP (Internet Control Message Protocol ou Protocolo para o Control de Mensaxes en Internet) é utilizado conxuntamente con IP, xa que realmente é unha parte integrante de IP e utiliza os mesmos paquetes e direccións.
Sen embargo, o obxectivo concreto deste protocolo é o de informar de erros no procesamento de paquetes. Existen varias situacións nas que os equipos envían notificacións mediante paquetes ICMP, como por exemplo:
• Cando un paquete non se puido enviar ao destino.
• Cando un equipo non ten suficiente capacidade de almacenamento temporal para procesar e reenviar unidades de datos.
• Cando existen rutas máis curtas para chegar ao nodo de destino.

A aplicación de rede **ping** (que permite testar se hai conexión con outro equipo) está baseada no protocolo ICMP.

9.4 O protocolo DNS

O protocolo DNS (Domain Name System, Sistema de Nomes de Dominio ou Resolución de Nomes de Dominio) forma parte dos protolos de capa de aplicación e asocia/traduce nomes de dominio á súa IP e viceversa para localizar e direccionar equipos mundialmente.

Un servidor DNS utiliza unha base de datos que é capaz de asociar diferentes tipos de información a cada nome de dominio. Por exemplo, se a dirección IP do servidor Google é 216.58.210.163, a maioría da xente chega a este equipo utilizando www.google.com e non pola IP. Isto además de ser mais fácil de recordar é mais fiable xa que a dirección numérica podería cambiar por moitas razóns, sen que teña que cambiar o nome do sitio web.

Para mais información:

- Digital Guide IONOS. Cambiar el servidor DNS: cómo modificar las entradas DNS.
- Wikipedia. Sistema de nombres de dominio.
- RedesZone. Los principales tipos de ataques DNS y cómo prevenirlos.
- Tips tecnológicos. Windows Server: Instalar y configurar un servidor DNS en Windows Server 2019.
- Instalación de servicios en redes locales. Instalación de un servidor DNS en Ubuntu.

10. Exercicios para practicar.

NOTA: as solucións están ao final deste boletín nun anexo.

EX1) Converte as seguintes direccións IP a formato binario e identifica a súa clase:
a) 192.16.2.80
b) 145.32.59.24
c) 200.42.129.16

EX2) Converte as seguintes direccións IP a formato decimal con puntos e identifica a súa clase.
a) 00011010101011110001100010100000
b) 11100101000011111111000000000001

EX3) Disponse da seguinte rede de clase B: 172.16.0.0 con máscara 255.255.192.0. Determina a dirección de cada unha das 4 subredes que queremos conseguir ademais do rango de direccións que queremos asignar a cada unha delas.

EX4) Dadas as direccións IP de clase C 192.168.100.40 e 192.168.100.51 e a máscara de subrede 255.255.255.240, indica se é necesario ou non un router entre elas para comunicarse.

EX5) Dada a dirección de rede de clase B 156.35.0.0 e a máscara 255.255.252.0, obtén o número máximo de subredes que se poden formar e o número máximo de equipos que poden conter.

EX6) Indica se as seguintes máscaras de subrede son correctas.
a) 255.255.194.0
b) 255.255.240.0

- DIRECCIONAMENTO EN IPv6 -

1. Esgotamento das direccións IP

A versión 4 do protocolo IP, que é a máis utilizada na actualidade, presenta un grave problema: Dada a expansión que tivo Internet, as direccións IP dispoñibles resultan insuficientes para o número de equipos actuais.

Cando se deseñou o protocolo IP (anos 80 do século pasado), pensouse que as direccións de 32 bits serían suficientes, xa que con elas se podería asignar direccións a 2^{32}=4.294.967.296 máquinas.

Iso era naquel momento máis que a poboación mundial, e resultaba impensable que se puidese a precisar máis dunha dirección IP por persoa.

Moitos foron os factores que fixeron que isto non fose así, entre os que podemos destacar:

- *Explosión demográfica de Internet*: Aínda no ano 1990, tan só unha mínima cantidade de fogares tiñan acceso a Internet. Hoxe en día, ao aumento da poboación mundial hai que sumarlle o aumento exponencial na conexión a Internet, sobre todo en países asiáticos de gran poboación como India ou China.
- *Uso ineficiente das direccións*: Organizar o espazo de direccións por clases e as direccións reservadas desperdicia millóns de direccións, polo que realmente non asignamos aos equipos todas as direccións IP dispoñibles.
- *Conexións always-on*: Unha solución que se utilizou para paliar o problema do esgotamento das direccións IP foi usar o protocolo DHCP para asignar unha dirección dinámica no momento no que un usuario establece unha conexión, de forma que esta dirección queda liberada cando o usuario se desconecta e pode ser usada por outro usuario. Porén, hoxe en día o habitual é contar con dispositivos permanentemente conectados, o que reduce enormemente o beneficio da re utilización das direccións.
- *Dispositivos móbiles:* A enorme expansión de dispositivos móbiles con acceso a Internet (smartphones, tablets, etc.) incrementou enormemente o número de equipos conectados á rede.
- *A Internet das cousas (IoT)*: Espérase que no futuro haxa moitas máis cousas (obxectos de todo tipo: electrodomésticos, lámpadas, dispositivos do fogar, automóbiles, etc.) conectadas a Internet que persoas. A idea é que desta maneira poderemos monitorizar e xestionar todos estes dispositivos a través da rede. Existen estimacións que calculan que no ano 2021 haberá arredor de 26 mil millóns de dispositivos conectados.

Debido a todo isto, xa dende os anos 90 se comprendeu que o número de direccións dispoñibles no protocolo IPv4 non ía ser suficiente para satisfacer a demanda de conexións.

Pese a que o uso de NAT e DHCP paliou en gran medida este problema de escaseza de direccións, o 3 de febreiro de 2011 a IANA asignou os últimos bloques de direccións IPv4 libres, esgotando efectivamente as direccións IPv4 dispoñibles.

A solución definitiva pasa polo cambio da versión protocolo IP a outra versión que utilice direccións mais grandes (e polo tanto permita ter un maior número de direccións distintas): esta versión é o **protocolo IP versión 6**, máis coñecido como **IPv6 ou IPng** (Internet Protocol Next Generation).

2. Características de IPv6.

• ***Utiliza direccións de 16 bytes (128 bits)***, co cal se dispón de 2128 direccións (340 sextillóns de direccións, o que supón preto de 670 mil billóns de direccións por cada milímetro cadrado da superficie da Terra).

- Isto ademais de dar solución ao problema de esgotamento das direccións en IPv4 supón un cambio total na filosofía da asignación das direccións IP, xa que o protocolo está deseñado para o desperdicio de direccións IP.

- Como mostra disto, pensemos que a cada usuario doméstico que teña conexión a Internet en IPv6 asignaráselle unha subrede que terá como mínimo máscara /64 (polo tanto terá como mínimo 264 direccións), o que suporá un tamaño moito maior que todo o espazo de direccionamento dispoñible en IPv4.

• ***Autoconfiguración***: Tendo en conta a lonxitude que teñen as direccións en IPv6 e polo tanto a dificultade para escribilas de forma manual, a intención do protocolo é que na meirande parte dos casos os equipos se configuren de forma automática sen intervención do administrador. Só os routers ou servidores terán de forma xeral direccións manuais.

• ***Uso intensivo de multicast***: Mentres que en IPv4 o uso de multicast é opcional, en IPv6 forma parte intrínseca do protocolo. De feito, en IPv6 non se implementan as direccións de broadcast, xa que son substituídas por direccións multicast. A última dirección da rede que en IPv4 é a dirección de broadcast, é unha dirección normal en IPv4.

• ***Mellora na seguridade das comunicacións***, ao integrar de forma nativa o protocolo IPSec (Internet Protocolo Security) que permite cifrar as comunicacións.

• ***Maior velocidade no enrutamento dos paquetes***, xa que o formato do paquete está optimizado para procesadores de 64 bits e só ten 7 campos na cabeceira, en lugar dos 13 da versión 4.

• ***Permite o uso de jumbogramas***: Mentres en IPv4 o tamaño máximo dos paquetes é de 64KiB, IPv6 soporta que os paquetes superen ese límite. Estes paquetes, chamados jumbrogramas (jumboframes) poden ser de ata 4GiB, o que pode mellorar a eficiencia na transmisión de ficheiros de gran tamaño en redes con baixas taxa de erros.

• ***É compatible coa versión 4 do protocolo*** (utilizando protocolos de tradución de direccións), polo que os dous protocolos poden coexistir durante a implantación da nova versión.

3. Representación de direccións IPv6.

A forma de representar as direccións IPv6 é diferente á IPv4. Unha dirección IPv6 represéntase por 8 números de 4 cifras escritos en hexadecimal (xa que cada número se corresponde con 16 bits), separados por ":".

A seguinte táboa mostra unha dirección IPv6 coa súa representación en hexadecimal:

Dirección IPv6 binaria	00100000 00000001	00001101 10111000	10000101 00111010	00000000 00000000	00000000 00000000	01001010 00101110	00000011 01110000	01110011 00110100
Dirección IPv6 hexadecimal	2001	0db8	853a	0000	0000	8a2e	0370	7334
Dirección IPv6 hexadecimal	2001:0db8:853a:0000:0000:8a2e:0370:7334							

Para reducir a lonxitude da dirección IPv6, podemos comprimila do seguinte xeito:

• Omitindo os ceros á esquerda en cada número hexadecimal.

• Substituíndo un grupo de números consecutivos a cero por "::".

• Esta substitución só se pode facer unha vez na dirección, xa que de facelo varias veces non poderíamos saber cantos números se corresponden con cada "::".

• En caso de que a dirección teña varios grupos de números consecutivos a cero, escolleremos o maior, xa que así comprimiremos máis a dirección.

Aplicando estas operacións sobre a dirección IPv6 do exemplo, obteríamos o seguinte:

Dirección IPv6 sen comprimir	2001:0db8:853a:0000:0000:8a2e:0370:7334
Dirección IPv6 omitindo os ceros á esquerda	2001:**db8**:853a:0000:0000:8a2e:**370**:7334
Dirección IPv6 comprimida ao máximo	2001:**db8**:853a**::**8a2e:**370**:7334

4. Exercicios para practicar.

EX7) Escribe a dirección 2800:0000:0000:00b2:0000:0000:0000:1ef5 comprimida ao máximo

EX8) Descomprime ao máximo a dirección 2001:db8:1::2:

Anexo (Solucións de exercicios)

EX1)

a) 11000000000010000000000001001010000 Clase C

b) 10010001001000000011101100011000 Clase B

c) 11001000001010101000000100010000 Clase C

EX2)

a) 26.175.24.160 Clase A

b) 229.15.240.1 Clase D

EX3)

Clase B - > 2 bytes para identificar o host

172.16.y.z= 172.16.xxxxxxxx.xxxxxxxx

Máscara de subrede → 4 subredes → + 2 bits

255.255.192.0 =1111111.11111111.**11**000000.00000000

4 Subredes → Coller 2 bit da parte ID do host (variacións con eses bits) → 00, 01, 10,11.

1a) Subrede: 172.16.**00**000000.00000000 = 172.16.0.0

2a) Subrede: 172.16.**01**000000.00000000 = 172.16.64.0

3a) Subrede: 172.16.**10**000000.00000000 = 172.16.128.0

4a) Subrede: 172.16.**11**000000.00000000 = 172.16.192.0

Rango de direccións IP para a 1a subrede:

10101100.00010000.00000000.00000001 172.16.0.1 ...

10101100.00010000.00111111.11111110 172.16.63.254

Rango de direccións IP para a 2a subrede:

10101100.00010000.01000000.00000001 172.16.64.1 …

10101100.00010000.01111111.11111110 172.16.127.254

Rango de direccións IP para a 3a subrede:

10101100.00010000.10000000.00000001 172.16.128.1 …

10101100.00010000.10111111.11111110 172.16.191.254

Rango de direccións IP para a 4a subrede:

10101100.00010000.11000000.00000001 172.16.192.1 …

10101100.00010000.11111111.11111110 172.16.255.254

EX4)

Máscara de subred:

255.255.255.240 = 1111111.11111111.11111111.11110000

Obter a dirección de rede para cada IP aplicando a máscara:

- 192.168.100.40:

  192.168.100.**00101000** && (AND)

  255.255.255.**11110000**

  = 192.168.100.00100000 ou 192.168.100.32 (Dirección Subrede)

- 192.168.100.51:

  192.168.100.00110011 &&

  255.255.255.11110000

  = 192.168.100.00110000 ou 192.168.100.48 (Dirección subrede)

As direccións de rede son distintas polo que os equipos pertencen a subredes diferentes e polo tanto necesitan un router para comunicalas.

EX5)

Máscara de subred → 255.255.252.0 = 1111111.11111111.**111111**00.00000000

Na máscara destínanse 6 bits para crear subredes e 10 bits para identificar os equipos das subredes.

Número máximo de subredes: 2^6 = 64 subredes

Número máximo de equipos/subrede: 2^{10} - 2 = 1022 equipos

EX 6)

Para comprobar se son correctas hai que pasalas a formato binario:

a) 255.255.194.0 → 11111111111111111100001000000000

Non é unha máscara correcta porque conten 1's despois dos 0's.

b) 255.255.240.0 → 11111111111111111111111111110000

Sí é correcta a máscara de rede.

EX7)

2800:0:0:b2::1ef5

EX8)

2001:0db8:0001:0000:0000:0000:0000:0002