UD1.- Caracterización de redes

Clasificación de redes. Topoloxías. Introdución aos Protocolos a ás arquitecturas de redes

Redes de ordenadores

Unha **rede de ordenadores** ou **rede informática** é un conxunto de equipos informáticos autónomos conectados entre si por medio de dispositivos físicos que envían e reciben impulsos eléctricos, ondas electromagnéticas ou calquera outro método para o transporte de datos coa finalidade de **compartir** información e recursos. Na rede de ordenadores tense en conta tamén aqueles medios técnicos que permiten compartir a información, tanto software como hardware.
O propósito das redes de equipos é **compartir**, xa que é a capacidade de **compartir** información de forma eficiente o que lles da ás redes de ordenadores a súa potencia e atractivo.
Deste xeito, as redes aumentan a eficiencia e reducen os custes. Os seus obxectivos son:

- **Compartir** información (datos, ficheiros)
- **Compartir** hardware e software.
- **Centralizando** a administración e o soporte.
- Permiten maior **confianza**, ao dispoñer de máis dunha fonte para os recursos.
- Permiten maior **escalabilidade** dos recursos (pode medrar sen perder calidade).

De todos os xeitos, os ordenadores dunha rede de ordenadores para ser considerada como tal teñen que ter dúas características importantes:

- ✔ Atoparse **interconectados** mediante algún medio de transmisión: poden intercambiar información.
- ✔ Son **autónomos**. Quere isto dicir que teñen certa potencia de cálculo independente.

Tipos de redes

Se nos fixamos en vez da titularidade no **tamaño** podemos clasificar unha rede nun dos seguintes grupos:

PAN (Personal Area Network ou Rede de Área Persoal)

Son as redes persoais que se están impoñendo nos fogares, para conectar teléfonos, portátiles, etc. Normalmente empregan conexións sen fíos ou WIFI.

LAN (Local Area Network ou Rede de Área Local)

Comunican un conxunto de equipos informáticos localizados nunha área xeográfica reducida (aulas, edificio), e deben depender (segundo o comité **IEEE 802**) dun canal físico de comunicacións cunha velocidade alta e que presente unha reducida taxa de erros na comunicación. Na súa construción úsanse liñas de comunicación propias.

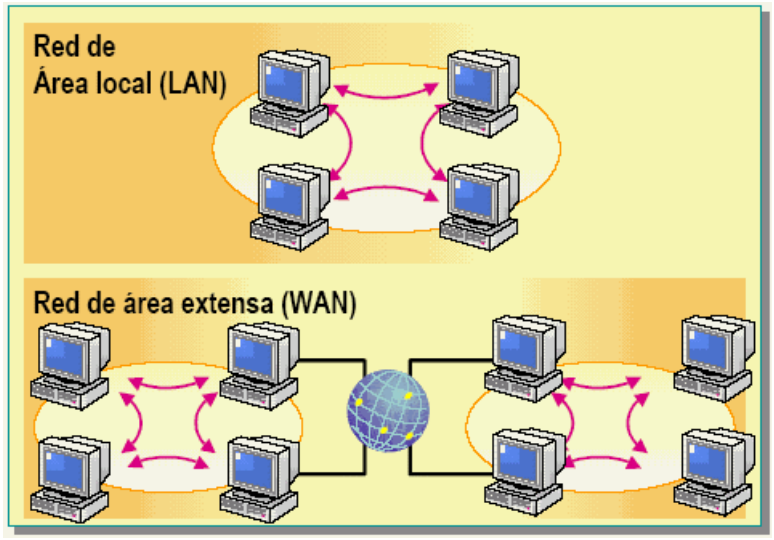
As velocidades de transmisión son altas, habitualmente de 100Mbps ou 1Gbps, podendo chegar ata 10Gbps, nas redes moi modernas.
A taxa de erro adoita ser mínima, da orde de 1 bit erróneo por cada 100 millóns de bits transmitidos.
Unha LAN pode constar de moi poucos equipos ou ben estar formado por un grande número de equipos e periféricos conectados.
Como veremos ao longo do curso, en todas as redes de área local nos atoparemos un modo de **transmisión/modulación** (banda ancha ou banda base), un **protocolo de acceso** (TDMA, CSMA/CD, Token Passing, FDDI), **un soporte físico** (cables de pares trenzados con ou sen apantallar, coaxiais ou fibra óptica), e finalmente unha **topoloxía** (bus, anel, estrela, malla)
A tendencia actual é empregar tamén enlaces de radio (WiFi) para facilitar a mobilidade dos usuarios, empregando para conectarse os chamados puntos de acceso ou "hotspots".

CAN (Campus Area Network ou Rede de Area de Campus)

Xurde da interconexión de distintas LAN, dun mesmo propietario (universidade, empresas, etc.) extendéndose nunha superficie como un campus, un polígono, etc

MAN (Metropolitan Area Network ou Rede de Area Metropolitana)

Abarcan unha área xeográfica restrinxida a unha cidade (unha rede intermedia entre unha LAN e unha WAN). Xeralmente unen varias LANs mediante liñas públicas ou privadas, como o sistema telefónico local, sistemas de microondas locais ou cables de fibra óptica soterrados.
Xeralmente está regulada por normas locais.



WAN (Wide Area Network ou Rede de Área Extensa)

Comunicará un conxunto de equipos informáticos situados en áreas xeográficas tan grandes como países, ou o planeta enteiro no caso de internet.
Usará liñas públicas de comunicación para a súa conexión.
Podemos entender internet como unha WAN extrema, conectando todas as redes WAN do mundo. Internet é unha rede de redes conectadas por enrutadores.

Topoloxías

As redes informáticas, para poder intercambiar información mediante a comunicación, precisan estar conectadas, e salvo as redes inalámbricas, a maioría das redes empregan cables para conectar todo o equipamento informático.

O termo **topoloxía da rede** fai referencia ao xeito no que se interconectan os diferentes nodos da rede. Indicaranos pois cal é o xeito de organización da rede, o deseño da mesma.

Podemos falar de dous tipos de topoloxías, a topoloxía física e a topoloxía lóxica:

Topoloxía física: Definirá a distribución física dos equipos na rede, ademais do tipo de cableado. Indicará o xeito real "físico" ou "presencial" de distribución da rede.

Topoloxía lóxica: Define o xeito empregado polos equipos para acceder ao medio para realizar a comunicación. Esta topoloxía lóxica da lugar á definición de protocolos empregados na comunicación. (ver vídeos). Os máis comúns son

- ✔ topoloxía *broadcast ou difusión (*cada equipo envía cara TODOS os demais equipos)
- ✔ *paso de testemuña* ou *paso de token (*a transmisión dun token controla o acceso á rede. Só o equipo que recibe o token ten a quenda para empregar a rede).

A selección da topoloxía empregada afectará ao tipo de equipamento que precisa a rede, as capacidades dos equipos, a capacidade de aumento do tamaño da rede, etc.

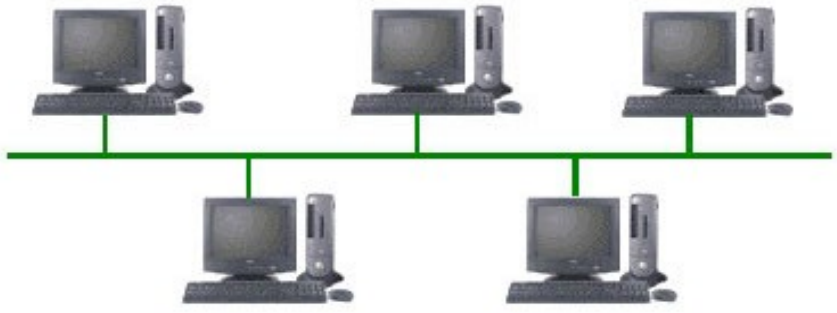
TOPOLOXÍAS FÍSICAS

Veremos as topoloxías físicas máis empregadas:

Topoloxía de bus

Esta topoloxía recibe tamén o nome de "bus lineal" porque os equipos están conectados nunha liña recta. E un dos métodos máis simple: consta dun segmento de cable central (*trunk*, *backbone* ou segmento) que conecta todos os equipos entre si, permitíndose a comunicación en ambos sentidos: todos os equipos comparten o medio e a información que circula polo medio de transmisión é recibida por todas as estacións.

Esta topoloxía era a que empregaba en redes LAN con cable coaxial fino, con conectores en T para os equipos. Na actualidade non se emprega nin se contempla nos estándares IEEE para as LAN.

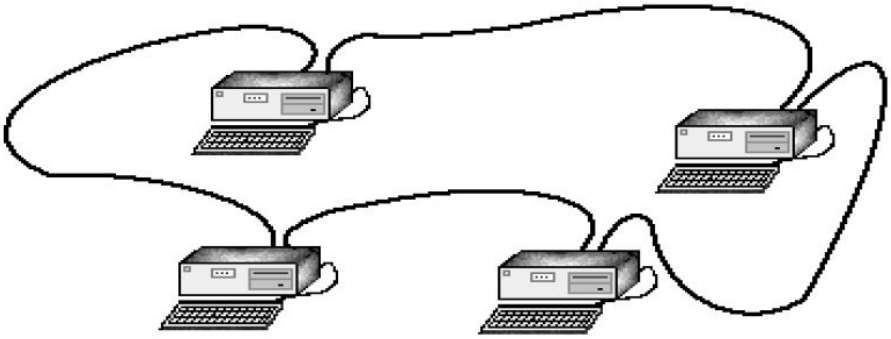


O inconveniente da topoloxía en bus era que calquera problema no cable ou nalgún terminal producía unha caída total da rede.

Topoloxía en anel

Nesta topoloxía os equipos conéctanse formando un bucle ou anel pechado. A información circula nunha única dirección ao longo do bucle, pasando de equipo en equipo ata chegar ao seu destinatario.

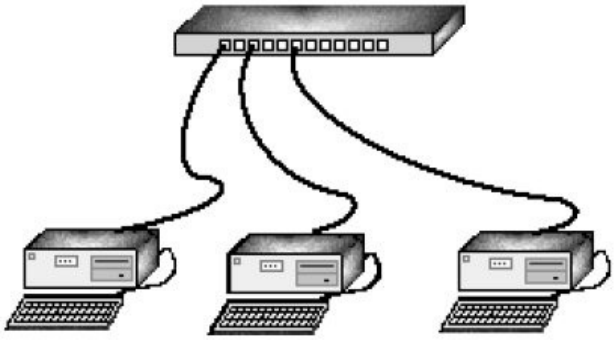
Do mesmo xeito que na topoloxía en bus, a avaría do cable ocasiona a caída da rede.



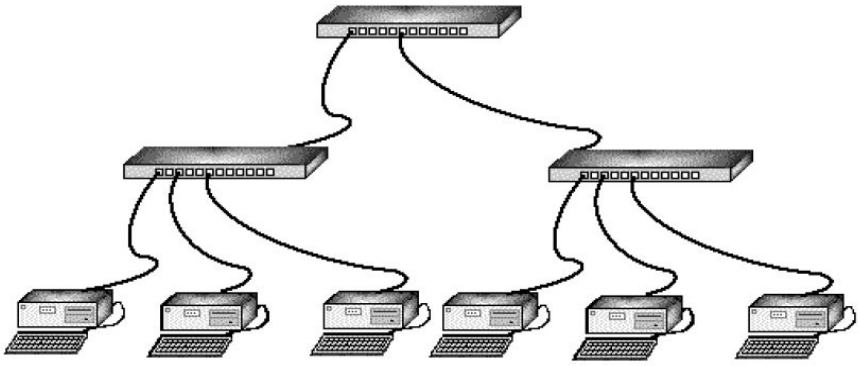
Esta tecnoloxía foi desenvolvida por IBM para redes LAN (denominada Token Ring, estándar IEEE 802.5), pero na actualidade non se emprega.
Unha variante é a do anel dobre, con 2 aneis concéntricos, que se emprega en tecnoloxía de fibra óptica **FDDI** (Interfaz de Datos Distribuida por Fibra, *Fiber Distributed Data Interface),* que non se empregan nas LAN, pero si en redes CAN.

Topoloxía en estrela

Na topoloxía en estrela, cada equipo informático está conectado a un elemento central polo que circulan todas as comunicacións entre os equipos. Normalmente, será un switch ou conmutador co que está unido cada un dos equipos. Isto fai que se requira máis cableado que nas anteriores. Se o controlador da rede deixa de funcionar, fallará todo o sistema, mentres que se calquera equipo individual ou cable falla a rede seguirá traballando normalmente.
Na actualidade esta é a única topoloxía física dos estándares do IEEE. O cable empregado é par trenzado UTP, con conectores RJ45, coas categorías 5e, e categoría 6, que permiten transmisións a 1Gb/seg. A categoría 6 é a recomendada para cableados novos.

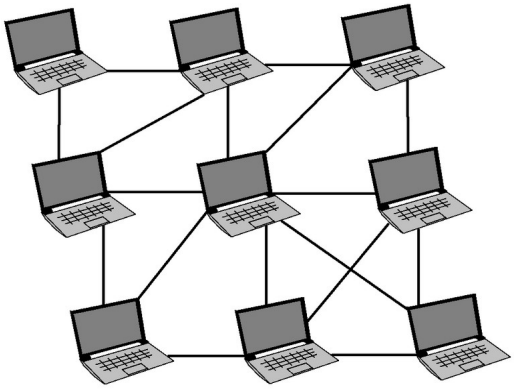


Poderemos combinar varias redes en estrela de xeito xerárquico, formando unha topoloxía en árbore.



Topoloxía en malla

Finalmente, a topoloxía en malla consiste en que cada equipo da rede está enlazado directamente varios dos outros equipos directamente por un cable. Deste xeito, existen camiños redundantes entre cada 2 equipos, e aínda que algún cable deixe de funcionar a rede seguiría traballando. O inconveniente deste tipo de topoloxía é a cantidade de cable empregado na súa instalación.



Existen tamén topoloxías físicas mixtas, combinacións das anteriores.

Introdución á arquitectura de redes e Protocolos

No inicio da informática o deseño dos ordenadores era tan complexo que non se reparaba na compatibilidade con outros modelos de ordenadores, chegaba con que o deseño fora correcto e eficiente. Por iso, era preciso crear para cada modelo de ordenador un sistema operativo, e tamén os programa eran específicos para cada modelo.

No ano 1964 IBM creou un novo modelo **Sistema/360** (ver imaxe), que realmente era unha familia de varios modelos cunha **arquitectura común**. Esta arquitectura establecía unhas especificacións comúns para facer compatibles os distintos modelos desa familia: conxuntos de instrucións, xeito de almacenar os datos, ... podendo utilizar os mesmos programas, sistema operativo, compiladores, etc. Isto era posible en todos os modelos desa familia, ordenadores de distinto prezo e diferentes potencias.

A arquitectura 360 foi evolucionando ata os nosos días (ESA/370, ESA/390, ..., zSeries e IBM-Z). Os grandes ordenadores (*mainframes*) da familia zSeries de IBM son empregados na actualidade en aplicacións críticas en empresas como bancos, liñas aéreas, etc.

Na actualidade, todos os fabricantes de ordenadores empregan unha ou varias arquitecturas como base para as liñas dos seus equipos.

Do mesmo xeito que os ordenadores, nas primeiras redes de ordenadores tanto as redes como os protocolos de comunicación eran deseñados pensando no *hardware* a utilizar en cada momento, sen pensar na futura evolución nin compatibilidades con outros equipos.

Segundo foi pasando o tempo e mellorando a tecnoloxía comezaron a aparecer os mesmos problemas que nos primeiros ordenadores: os programas de comunicacións (feitos con grandes esforzos de desenvolvemento) tiñan que ser **reescritos practicamente de cero** para adaptalos ao novo hardware, pois debido á pouca modularidade do código practicamente non se podía reutilizar nada.

O problema foi resolto do mesmo xeito que cos ordenadores. Cada fabricante elaboraba a súa propia **arquitectura de rede**, facéndoa independente do hardware concreto que utilizaba. Así, se se quería cambiar algún compoñente só tiñan que cambiar a función ou o módulo afectado.

Entendemos a **arquitectura de rede** como un **MODELO** organizado das funcións que realiza a rede.

As primeiras arquitectura de redes foron no 1974 a de IBM (SNA ou Systems Network Architecture) e a de DEC de 1975 (DNA ou DEC Network Arquitecture ou DECNET).

A arquitectura SNA baseábase na definición de 7 **niveis** ou **capas**, cada unha delas ofrecendo unha serie de **servizos** á seguinte. A seguinte capa baséase na capa anterior para levar a cabo os seus servizos, e así sucesivamente.

Cada unha destas capas pode ser realizada en hardware, software ou unha combinación de ambos. O módulo (hardware e/ou software) que implementa unha capa nun determinado elemento da rede debe poder substituírse sen afectar ao resto da rede, sempre e cando o protocolo empregado non se modifique. É dicir, SNA é unha arquitectura **estruturada** e **modular**.

Este modelo de capas foi a base de todas as arquitecturas empregadas actualmente, tanto as baseadas no **modelo OSI** (*Open Systems Interconnection* ou Interconexión de Sistemas Abertos) e o **TCP/IP** (*Transmission Control Protocol/Internet Protocol* ou Protocolo de Control da Transmisión/Protocolo de Internet), que veremos máis adiante polo miúdo.

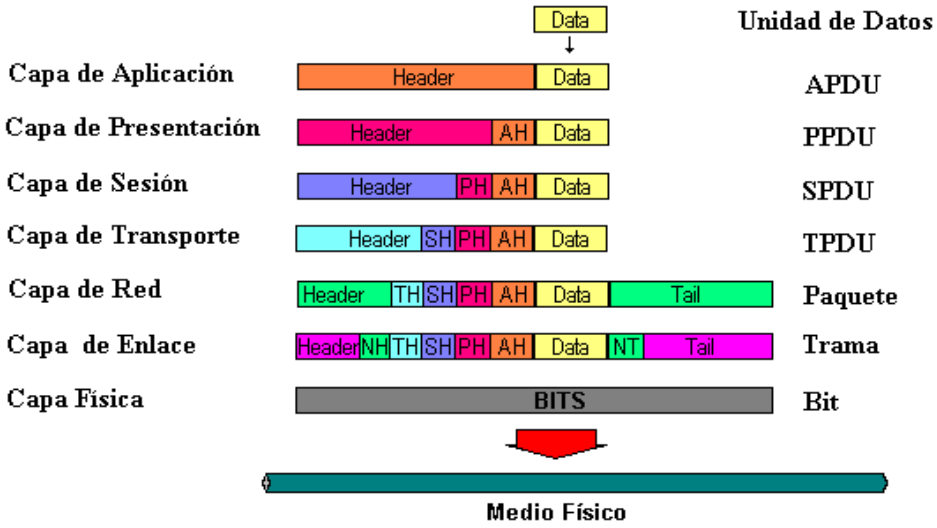


Figura do Modelo OSI

Vexamos como son as ideas básicas do modelo de capas:

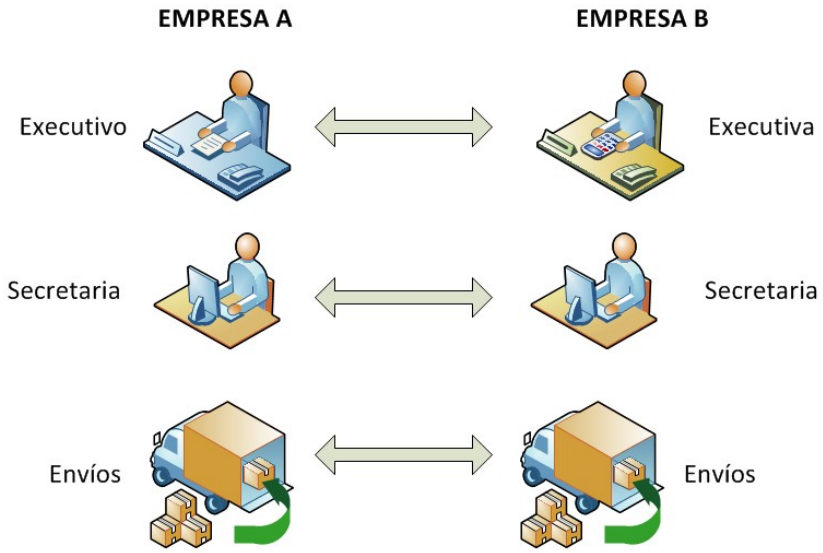
- A capa *n* ofrece unha serie de servizos á capa *n+1*.
- A capa *n* só ve os servizos que lle ofrece a capa *n-1*.
- A capa *n* nun sistema determinado só se comunica coa súa homóloga no sistema remoto (o que se coñece como comunicación entre iguais ou "peer-to-peer" ou *P2P*). Esta conversa efectúase cunha serie de regras coñecidas como "***protocolo da capa n***".

Podemos entender isto nun exemplo como poder ser o envío dunha carta. Dividimos o proceso en 3 niveis ou capas: o remitente da carta, a oficina de correos e o transporte.

A comunicación entre 2 capas adxacentes nun mesmo sistema realízase de acordo a unha **interfaz**.
OLLO: Esta **interfaz** é un xeito concreto de implementar un servizo

Así, a **arquitectura de rede** será a *descrición das capas que a compoñen, a súa funcionalidade, os servizos que empregan e os protocolos que utiliza para falar entre "iguais".* O conxunto de protocolos que emprega unha determinada arquitectura é coñecido como **pila de protocolos** ("protocol stack" en inglés). Fálase pois da **pila de protocolos** OSI, SNA, TCP/IP ou DECNET, por exemplo.

Para entender mellor o xeito de funcionar dun modelo de arquitectura de redes baseado en capas imos facer unha analoxía. Supoñamos que un executivo dunha empresa A quere enviar de xeito urxente un importante envío a unha executiva dunha empresa B. Para isto falará con ela avisándoa do envío, e a continuación pasará á súa secretaria o informe coas instrucións correspondentes.
A secretaria de A chamará á secretaria da empresa B para obter a dirección exacta, poñerá o envío nun paquete e chamará a un servizo de mensaxería, que enviará a un motorista para recoller o paquete e levalo ao aeroporto.
Cando o paquete chega ao aeroporto destino é recollido por outro motorista que o leva á oficina da empresa B, entregándollo á secretaria de B. Esta encargarase dos trámites administrativos (pagar a mensaxería, abrir o paquete, comprobar o contido, dar acuse de recibo á secretaria de A, etc.) e a continuación pasarllo á súa xefa. Finalmente, cando a executiva de B leve a cabo un estudo do recibido chamará ao executivo da empresa A.



Fíxate que no proceso anterior existen diferentes niveis diferenciados: os executivos, as secretarias, os motoristas, e por último a empresa de liñas aéreas que se ocupa do transporte físico da mercancía. En todos os niveis (menos no físico) hai 2 entidades, a transmisora (A) e a receptora (B). Se todo acontece como é debido cada entidade só terá que falar coa súa entidade correspondente no outro lado, e coas entidades veciñas, é dicir, o xefe de A só falará coa súa secretaría e coa xefa de B, a secretaria fala co seu xefe ou xefa, falará co motorista, e coa outra secretaria, etc. Fíxate que cada motorista só fala coa secretaria correspondente.

Non se precisa que a secretaria de A fale coa xefa de B, ou a secretaria de B co xefe de A. Deste xeito, se a secretaria de A é substituída por calquera motivo os procedementos seguirán funcionando se a nova secretaria leva a cabo a súa función. Deste xeito, as variacións de carácter interno só teñen que ser coñecidas polas entidades contiguas. Por exemplo, o motorista de B pode ser substituído por unha furgoneta de reparto e isto só sería coñecido pola secretaria de B. No modelo de capas simplifícase moito a tarefa de cada unha das entidades, que só se ten que ocupar dunha pequena parte de todo o mecanismo (o proceso vaise dividindo en moitas partes que se van asignando a distintas capas).

Nunha comunicación de datos, cando o sistema emisor desexa enviar unha mensaxe a un sistema remoto normalmente a información é xerada no nivel máis alto (por exemplo un navegador), e conforme vai descendo ata o nivel máis baixo prodúcense diversas transformacións, como poden ser adición de cabeceiras, de colas, de información de control, etc. Se a mensaxe é moi grande será dividida en moitos **paquetes**, etc.

Todas estas operacións son invertidas no sistema destino nas capas correspondentes: en cada capa reconstruirase unha mensaxe similar á orixinal.

Algúns elementos da arquitecturas de redes

Cando se deseña unha arquitectura de rede hai unha serie de aspectos e decisións fundamentais que condicionan o proceso da comunicación.

Entre elas está o ***direccionamento***: cada capa debe poder identificar as mensaxes que envía e recibe. Ás veces un mesmo ordenador pode ter varias instancias dunha mesma capa, polo que a identificación do ordenador pode non ser suficiente.
Calquera protocolo admite normalmente comunicación en ambos sentidos (**dúplex**), pero non sempre se permite que isto aconteza de xeito *simultáneo* (**full-dúplex**). Tamén haberá que determinar se hai que definir ***prioridades***, e cales son estas.
En calquera comunicación é preciso establecer un ***control de erros***, pois os canais de comunicación non son totalmente fiables. Haberá que decidir que código de detección se vai empregar, e en que capa se leva a cabo. Ademais, haberá que decidir se facemos ou non corrección de erros. A medida que os medios de transmisión melloran e as taxas de erros diminúen a detección/corrección vaise suprimindo das capas inferiores e se levan a cabo nas máis altas (a detección e corrección é un proceso que pode enlentecer apreciablemente a transmisión).

Por outra banda, débese ter en conta a posibilidade de que os paquetes cheguen ao seu destino en orde diferente ao seu envío.

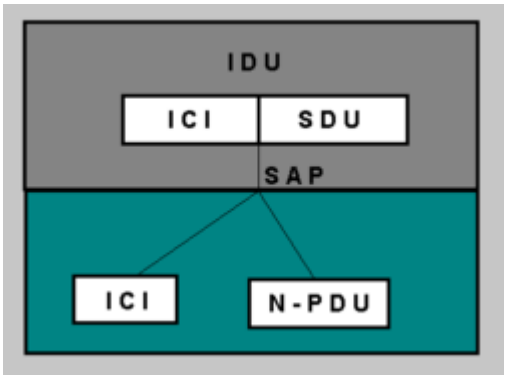
Hai que ter en conta a posibilidade que o receptor non sexa quen de “asimilar” a información enviada polo transmisor. Para isto é conveniente dispoñer dalgún ***mecanismo de control de fluxo*** e notificación para indicar a conxestión.
Normalmente os equipos funcionan de xeito óptimo cando o tamaño das mensaxes que se envían están en certo rango. Para evitar problemas que pode producir o envío de mensaxes moi grandes ou moi pequenas existirán tamén ***mecanismos de fragmentación*** e ***reagrupamento***.

Interfaces e servizos

As interfaces e os servizos son unha parte importante nos protocolos.

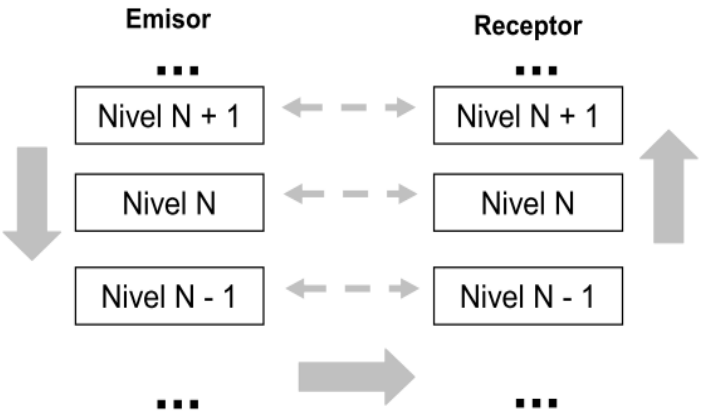
Chamamos **entidade** aos elementos activos en cada capa. Unha entidade pode ser un proceso, un compoñente hardware, ou unha combinación de ambos. Un ordenador pode ter unha ou varias entidades en cada capa (por exemplo un ordenador con 2 tarxetas de rede).
Chamaremos **entidades iguais** ou **entidades pares** ("*peer entities*" en inglés) a 2 entidades diferentes que pertencen á mesma capa. Xeralmente estarán en diferentes máquinas, pero poden estar na mesma.
As entidades da capa n executan os servizos que usa a capa n+1. Dise que a capa n actúa como o **provedor** do servizo e a capa n+1 é o **usuario** do servizo. O uso que a capa n faga dos servizos da capa n-1 é algo que nin afecta nin incumbe á capa n+1.

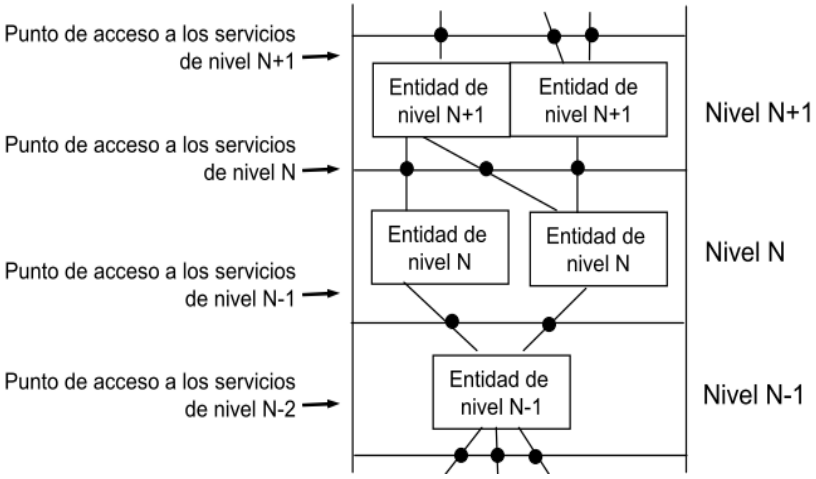
Denominamos **interfaz** ao conxunto de regras que gobernan o intercambio de información entre capas. Nunha comunicación a entidade da capa n+1 intercambia unha **IDU** (*Interface Data Unit* ou *Unidade de Dato do Interfaz*) coa entidade da capa n a través do **SAP** (*Service Acces Point*, ou *Punto de Acceso ao Servizo*).



Esta **IDU** estará formada por unha **SDU** (*Service Data Unit* ou *Unidade de Datos de Servizo*) e información de control da interfaz (**ICI** *ou Interfaz Control Information* ou *Información de Control de Interfaz*).
A **SDU** será o que se transmita á entidade equivalente (peer) no lado contrario da comunicación, e de alí á capa n+1 a través do seu **SAP**.
A información de control é precisa como o seu nome indica para que a interfaz faga correctamente o seu traballo, pero non forma parte dos datos mesmo. Na especificación da arquitectura só é preciso describir a estrutura da SDU, pero non a IDU (esta especifícase na interfaz, que pode ser distinta en cada especificación).
Para transferir a SDU a entidade da capa n constrúe o que se chama **PDUs** (*Protocol Data Unit),* que será o que se intercambia entre o emisor e receptor, polas entidades da capa n. No caso máis simple, a modificación que sofre a SDU é simplemente engadir un encabezamento. Se non:

- se se precisa, máis dunha SDU é combinada para formar a PDU, o que recibe o nome de ***concatenación***.
- se se realiza o proceso contrario, e unha SDU é dividida e cada fragmento forma unha SDU diferente, falamos de ***segmentación***.





Servizos orientados e non orientados a conexión

Nunha arquitectura de redes, como vimos na sección anterior, cada capa emprega os servizos da capa inmediatamente inferior para comunicar co correspondente no outro extremo. En función de como se estableza esa comunicación haberá 2 tipos de servizos: *orientados a conexión* e *non orientados a conexión:*

No servizo **orientado a conexión,** tamén chamado **CONS** (*Connection Oriented Network Service*), antes de iniciar a comunicación hai unha **negociación previa** entre as entidades (verifícanse determinados datos: dispoñibilidade, alcance, etc.) e se negocian unhas credenciais para facer a conexión máis segura e eficiente. Logo transmítense os datos, e finalmente péchase a conexión.
Nalgúns protocolos que empregan servizos orientados a conexión (ollo: **NON** en todos) a comunicación pode empregar o que se coñece como **circuíto virtual** ou VC. Unha vez establecido o VC o camiño físico que van seguir os datos está determinado: os paquetes deben ir todos por el desde a orixe ata o destino, e chegar coa mesma orde coa que foron enviados. Como o VC establece de xeito claro o destino, os paquetes non precisan conter a súa dirección.

No servizo **Non orientado a conexión**, tamén chamado **CLNS** (*ConnectionLess Network Service*) a comunicación establécese dun xeito menos formal: **NON existe negociación** previa á comunicación. Cando

unha entidade ten información que transmitir envíaa en forma de paquetes, confiando que estes chegaran ao seu destino. Tampouco se establece previamente un circuíto virtual nin outro tipo de canal de comunicación extremo a extremo: os paquetes poden ir por camiños físicos diversos, e deben incluír cada un a dirección de destino. Os paquetes poderán ser almacenados por nodos intermedios da rede, e reenviados máis tarde, podendo chegar nunha orde diferente á súa saída (aínda que non é frecuente). Os paquetes enviados nun servizo NON orientado a conexión reciben o nome de **datagramas**, cada parte é independente como un telegrama.

Unha analoxía sería entender o sistema telefónico como un sistema orientado a conexión, mentres que o correo pode entenderse como un servizo non orientado a conexión.
En redes de computadores a diferencia no tempo de entrega entre servizos CONS e CLNS non é tan grande como esta analoxía pode facer pensar.

En calquera dos tipos de servizos comentados é posible que se produza perda de información, pode acontecer tamén que o tempo de envío do paquete, chamado **retardo** ou **latencia** (*delay* ou *latency*) sexa moi grande ou varíe nun rango determinado debido á carga e conxestión da rede.

Nalgúns casos requírese unha entrega fiable, é dicir, que se garanta a entrega dos paquetes, pero podemos tolerar un retardo máis ou menos grande. Polo contrario, a voz ou o vídeo toleran unha pequena porcentaxe de perdas pero precisan dun retardo e flutuación do sinal reducidos.
Cando ao establecer unha comunicación se solicita un nivel mínimo para algún destes parámetros dise que se require unha **calidade de servizo** (chamado **QoS**, *Quality of Service*). A calidade de servizo estipula uns mínimos que a rede ten que satisfacer para efectuar a conexión, por exemplo “transmisión fiable cun retardo non superior a 100 mseg”. É posible que a rede non sexa quen de satisfacer a calidade solicitada, neste caso podería facer unha proposta alternativa (“o mínimo sería 250 mseg, estás conforme?”). Unha vez pactadas as condicións da comunicación estas actúan a modo de contrato que obriga á rede a dar a calidade de servizo prometida ao usuario.
Non todos os protocolos ou redes ofrecen a posibilidade de negociar calidades de servizo; nestes casos o protocolo simplemente aproveita os medios dispoñibles o mellor que pode, tentando evitar as conxestións e situacións críticas no posible, e repartir os recursos entre os usuarios de xeito máis ou menos equilibrado. Esta estratexia coñecese co nome de “mellor esforzo” (*best effort*). Como exemplo de redes con QoS citar a ATM, como exemplo de redes *best effort* podemos mencionar a internet empregando TCP/IP e Ethernet.