Arquitecturas de protocolos

Sumario

- 1 Introdución
- 2 **INTERÉSACHE Organismos de estandarización**. No mundo das redes existen diversos organismos de estandarización, adicados a diferentes cuestións como a ITU (Unión Internacional de Telecomunicacións), a ISO (Organización Internacional de Normalización), ANSI (Instituto Americano de Normas Nacionais), o IEEE (Instituto de Enxeñeiros Eléctricos e Elctrncs.), o IAB (Consello de Arquitectura de Internet), etc.
- 3 As arquitecturas de protocolos
- 4 O modelo OSI
    - 4.1 Os protocolos
    - 4.2 Os servizos
    - 4.3 Os sete niveis do modelo OSI
- 5 TCP/IP, a pila de protocolos de Internet
    - 5.1 Orixes
- 6 **INTERÉSACHE** As versións 1, 2, 3 e 5 do IP non se utilizaron nunca. Internet, desde o seu inicio como ARPANET, adoptou a versión 4. Na actualidade, fálase da versión nova como a versión *next generation* (en honra á serie de televisión Star Trek: the next generation) en lugar de chamala versión 5, que sería o normal se non fose porque un documento confundiu a todo o mundo dicindo que a nova versión sería a 7. Sexa como sexa, os catro primeiros bits de todos os paquetes que circulan por Internet son 0100, é dicir, 4, para indicar a versión IP que os define. Os novos paquetes deberán empezar por catro bits diferentes, que obviamente non poden ser next generation. Estes catro bits iniciais serán 0110, é dicir, 6.
    - 6.1 Software libre e Internet
- 7 **INTERÉSACHE** A definición de software libre proposta pola Free Software Foundation baséase en catro liberdades básicas que calquera programa considerado libre debe proporcionar:
    1. Liberdade para utilizar o programa para calquera propósito.
    2. Liberdade para poder estudar como funciona o programa e adaptalo ás nosas necesidades.
    3. Liberdade para redistribuír o programa.
    4. Liberdade de mellorar o programa e facer públicas as melloras aos demais, de modo que toda a comunidade se beneficie. Implica o acceso ao código fonte deste.
    - 7.1 TCP/IP versus OSI
    - 7.2 Os protocolos de Internet
    - 7.3 Encapsulamento
- 8 Sniffers

Introdución

As primeiras redes estaban construídas por fabricantes que seguían as súas propias especificacións, é dicir, non había normas para conectar os dispositivos, nin especificacións de protocolos para transmitir a información. Isto supoñía un problema á hora de comunicar redes de distintos fabricantes xa que non eran compatibles entre si. Polo tanto era necesario un esforzo por parte da nacente industria para coordinar a todos os fabricantes mediante a estandarización.

Os **estándares**, no ámbito das redes, posibilitan a comunicación entre computadoras de distintos fabricantes. Tamén permiten que os produtos teñan menor custe e maior aceptación. Existen dous tipos de estándares:

- Estándares **de facto** (de feito): Apareceron e impuxéronse no mercado pola súa ampla utilización
- Estándares **de iure** (por lei): Foron acordados por algún organismo internacional de estandarización autorizado.

INTERÉSACHE

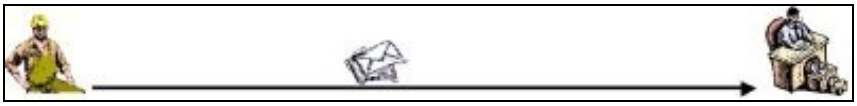
Organismos de estandarización. No mundo das redes existen diversos organismos de estandarización, adicados a diferentes cuestións como a ITU (Unión Internacional de Telecomunicacións), a ISO (Organización Internacional de Normalización), ANSI (Instituto Americano de Normas Nacionais), o IEEE (Instituto de Enxeñeiros Eléctricos e Elctrncs.), o IAB

(Consello de Arquitectura de Internet), etc.

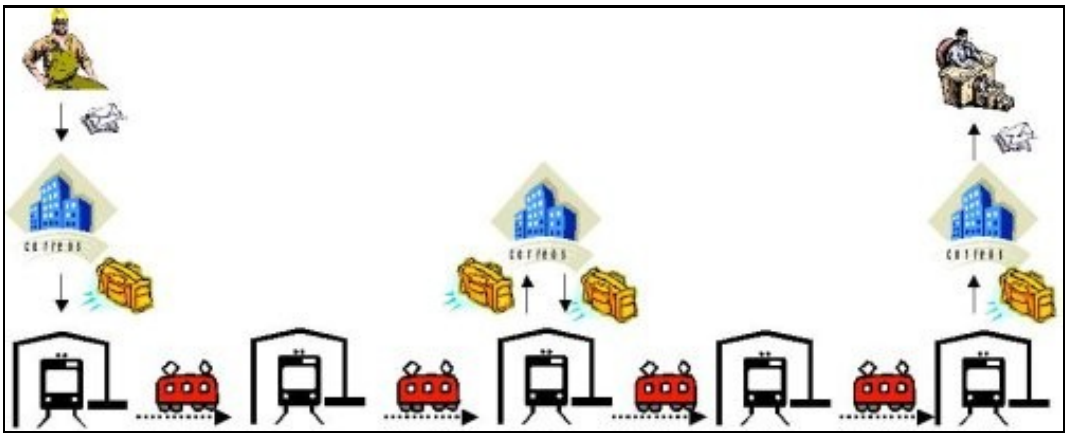
As arquitecturas de protocolos

As **arquitecturas ou pilas de protocolos** afrontan o problema das comunicacións de datos e as redes informáticas dividíndoo en niveis. Cada nivel desenvolve unha ou varias funcións especificadas previamente. Redúcese así a complexidade do deseño e permítese facer modificacións por bloques polo que o sistema é máis doado de manter, seguindo o principio *Divide et vinces* de Julio César. Algunha destas arquitecturas, como TCP/IP, é un estándar de facto e outra, como o modelo OSI, pretenderon ser un estándar de iure, aínda que quedou nun modelo de referencia académico, pero ámbalas dúas baséanse nese principio.

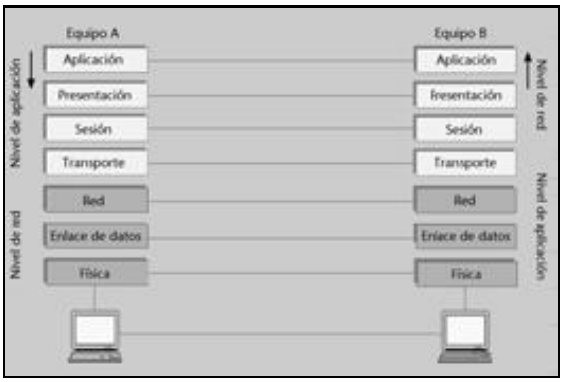
Para entender o funcionamento dunha pila de protocolos podemos facer unha analoxía co mundo real. Supoñamos que un amigo quere enviar unha carta a outro. Nesta comunicación hai un emisor (o amigo que escribe a carta), un receptor (quen a recibe), datos a transmitir (a carta) e un mecanismo de envío e recepción (o servizo de correos). O que sucede cando se mete a carta no sobre e se envía é transparente para eles como usuarios do servizo de correos. A imaxe que teñen do proceso é a seguinte:



Con todo, a realidade é outra moi distinta xa que cando o emisor deposita a carta en correos, a esta engádeselle información (por exemplo, dependendo de se é urxente, certificada, etc.), envíase por diversos medios dependendo da dirección de destino (tren, avión, etc.), pasa por diferentes sucursais de correos e un sen fin de procesos máis que os dous amigos, emisor e receptor, descoñecen por completo:

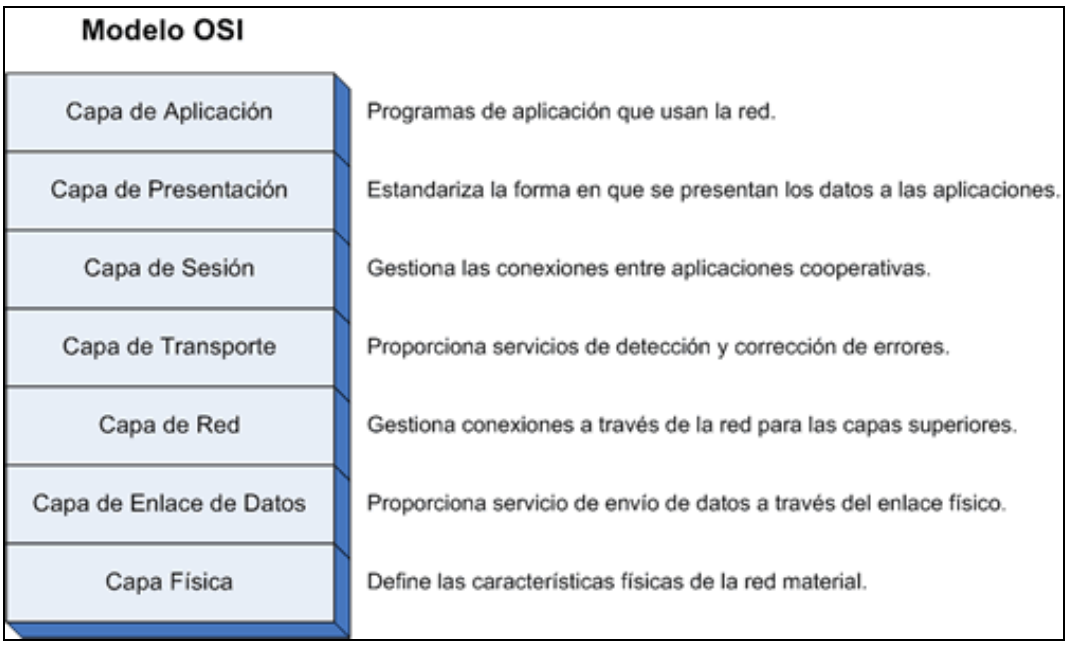


O funcionamento dunha pila de protocolos é similar a este exemplo como veremos máis adiante. En calquera caso, a pila de protocolos non deixa de ser software que normalmente está integrado no sistema operativo do dispositivo que se quere conectar á rede. Polo tanto, cada extremo da comunicación incorpora unha pila de protocolos igual á doutro extremo para poder "falar" entre eles.



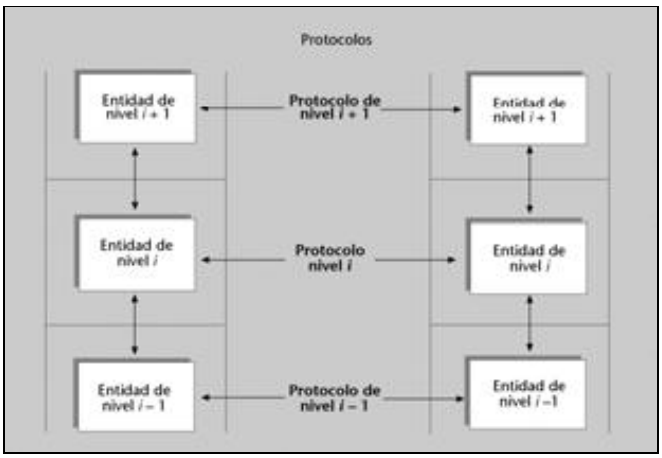
O modelo OSI

Seguindo os principios anteriores a ISO definiu o modelo OSI (*Open System Interconnection*) que é a súa pila de protocolos:



OSI é un modelo de referencia teórico moi útil dende o punto de vista docente pero a súa complexidade e detalle nas especificacións levouno a un marco meramente académico polo que non está implementado no mercado. Con todo, a pila TCP/IP está omnipresente como veremos en breve.

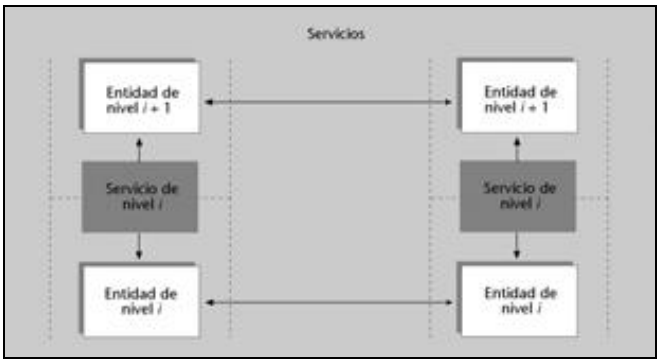
Os protocolos



Un protocolo é un conxunto de especificacións que permite a intercomunicación de entidades situadas en máquinas diferentes. A comunicación é horizontal, é dicir, dáse entre niveis homónimos e hai un protocolo por cada nivel da pila. Un protocolo de nivel i especifica o formato, o significado e a temporización da información para ese nivel.

A especificación dun protocolo debe levarse a cabo nun estándar claramente definido que permita a desenvolvedores distintos implementalo de xeito totalmente idéntico. A recepción dunha secuencia de bits nun momento inesperado pode facer que a entidade destinataria non reaccione correctamente e deixe o sistema nunha situación inestable.

Os servizos



Por servizo entendemos a comunicación que se produce entre niveis da pila de protocolos, sempre dentro dunha mesma máquina. A especificación dun servizo é menos estrita que a de un protocolo xa que a comunicación dáse na mesma máquina. Cada nivel da pila usa os servizos do nivel superior e proporciona servizos ao nivel inferior (exceptuando, claro está, o primeiro e último nivel da pila). Existe, polo tanto, unha comunicación vertical.

Os sete niveis do modelo OSI

A pila OSI define sete niveis e asigna diferentes funcións a cada un deles:

1. **Nivel físico**: é o encargado da transmisión física dos sinais eléctricos e define cuestións como, por exemplo, que voltaxe se usará para representar un 1 e un 0. Este nivel está moi vinculado ao de transmisión (cable coaxial, par trenzado, fibra óptica, radio, etc.).
2. **Nivel de enlace**: entre as súas funcións están a detección de erros, o control de fluxo, etc. Algúns exemplos reais de niveis de enlace son tecnoloxías como Ethernet, Frame Relay ou ATM.
3. **Nivel de rede**: encárgase da asignación de direccións (*addressing*), o encamiñamento de paquetes (*routing*), etc. Algúns exemplos reais de protocolos do nivel de rede son IP, IPX ou NetBEUI (estes dous últimos en desuso)
4. **Nivel de transporte**: garante as conexión extremo a extremo, xestiona o control de fluxo, etc. Algúns exemplos reais de protocolos deste nivel son TCP ou SPX.
5. **Nivel de sesión**: xestiona as conexión de longa duración. Un exemplo de protocolo deste nivel é NetBIOS.
6. **Nivel de presentación**: unifica a codificación da información. Neste nivel fálase máis de formatos que de protocolos. Algúns exemplos son ASN.1 e XML.
7. **Nivel de aplicación**: fálase de protocolos pero tamén de programas/servizos. Algúns exemplos son DNS, HTTP, FTP, SMTP, etc.

TCP/IP, a pila de protocolos de Internet

Orixes

TCP/IP é unha arquitectura de protocolos que inclúe catro capas, aínda que non coinciden exactamente coas do modelo OSI. É a pila de protocolos que usa Internet (actualmente tamén se usa nas redes locais) polo tanto as súas orixes están nos anos 70 cando o departamento de defensa americano encarga un proxecto de investigación, ARPANET, coa idea de crear unha rede tolerante a fallos ante posibles ataques externos.

Durante a primeira década de funcionamento ARPANET permitiu a un inxente conxunto de investigadores desenvolver e perfeccionar as técnicas para a xestión e o uso da rede. Cara ao ano 1979, a pila TCP/IP empézase a perfilar como o conxunto de protocolos de futuro da rede e ao final de 1982 todos os nodos de ARPANET xa adoptaran o TCP/IP. Co tempo, todas as redes académicas, en primeiro lugar as de Estados Unidos, despois as de Europa e máis tarde as do resto do mundo, acabaranse conectando a ARPANET (a rede militar segregaríase en MILNET).

A rede de redes, Internet ou a Rede como tamén se lle coñece, empezou o seu crecemento vertixinoso cara ao ano 1986. A principios dos anos noventa, as principais universidades xa formaban parte de Internet. É neste momento cando as empresas empezaron a ver o potencial da rede, en primeiro lugar como medio de interconexión e, un pouco máis tarde, como ferramenta de mercadotecnia. En 1993 aparece o HTTP - *Hypertext Transfer Protocol* -, ou protocolo da WWW - *World Wide Web* - que supón una fito na evolución da rede ao achegar os seus servizos aos usuarios non técnicos.

O crecemento actual de Internet mantense imparable e empezan a xurdir os primeiros problemas. A rede Internet sofre certas limitacións na súa especificación actual que poden facer que este crecemento deba deterse nun futuro non demasiado afastado se non se realizan cambios importantes. En particular, o protocolo IP na versión actual, a 4 (IPv4) limita o número de estacións que se poden conectar a Internet a 2^32 (uns 4.000 millóns de estacións). A maneira de asignar as direccións de Internet fai que haxa moitas direccións que, na práctica, sexan inutilizables. Na actualidade, considérase que a única solución a longo prazo será a actualización de todos os compoñentes da rede na versión nova, a 6 (IPv6 ou IPng, *IP next generation*).

INTERÉSACHE

As versións 1, 2, 3 e 5 do IP non se utilizaron nunca. Internet, desde o seu inicio como ARPANET, adoptou a versión 4. Na actualidade, fálase da versión nova como a versión *next generation* (en honra á serie de televisión Star Trek: the next generation) en lugar de chamala versión 5, que sería o normal se non fose porque un documento confundiu a todo o mundo dicindo que a nova versión sería a 7.

Sexa como sexa, os catro primeiros bits de todos os paquetes que circulan por Internet son 0100, é dicir, 4, para indicar a versión IP que os define. Os novos paquetes deberán empezar por catro bits diferentes, que obviamente non poden ser next generation. Estes catro bits iniciais serán 0110, é dicir, 6.

Software libre e Internet

O software libre tivo un papel fundamental no crecemento de Internet. De feito, podemos afirmar que se usas Internet, usas software libre porque a maior parte da infraestrutura de Internet baséase en protocolos abertos. Máis do 50% dos servidores web (setembro 2008) empregan Apache, outro gran número usan SendMail para xestionar o envío de correo electrónico e practicamente a totalidade dos servidores de nomes (DNS), esenciais no funcionamento da Rede, utilizan o programa BIND ou derivados do seu código fonte.

É indiscutible a importancia que tivo o software libre na extensión e no desenvolvemento de Internet dende os seus inicios. Sen a existencia do software libre Internet hoxe en día probabelmente non existiría. Foi igualmente importante o feito de que os protocolos que definen a arquitectura de Internet sexan abertos e que non sexan controlados por unha ou por varias empresas.

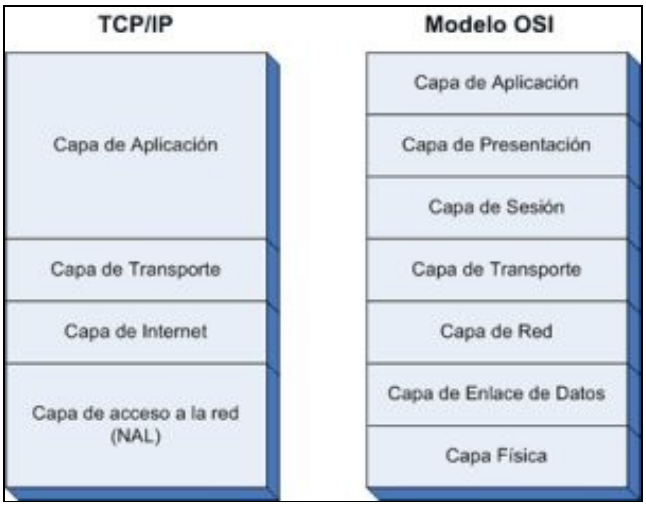
INTERÉSACHE

A definición de software libre proposta pola Free Software Foundation baséase en catro liberdades básicas que calquera programa considerado libre debe proporcionar:

1. Liberdade para utilizar o programa para calquera propósito.
2. Liberdade para poder estudar como funciona o programa e adaptalo ás nosas necesidades.
3. Liberdade para redistribuír o programa.
4. Liberdade de mellorar o programa e facer públicas as melloras aos demais, de modo que toda a comunidade se beneficie. Implica o acceso ao código fonte deste.

O software libre baséase na cooperación e na transparencia, e garántelle unha serie de liberdades aos usuarios. Estes aspectos, xunto co feito de que o seu desenvolvemento foi paralelo ao de Internet, provocaron que sexa abandeirado por un gran número de usuarios que teñen unha concepción libertaria do uso das novas tecnoloxías. Aos programas que non son libres chámaselles propietarios ou privativos. Por exemplo, todas as versións de Microsoft Windows ou Adobe Acrobat son exemplos de software propietario.

TCP/IP versus OSI



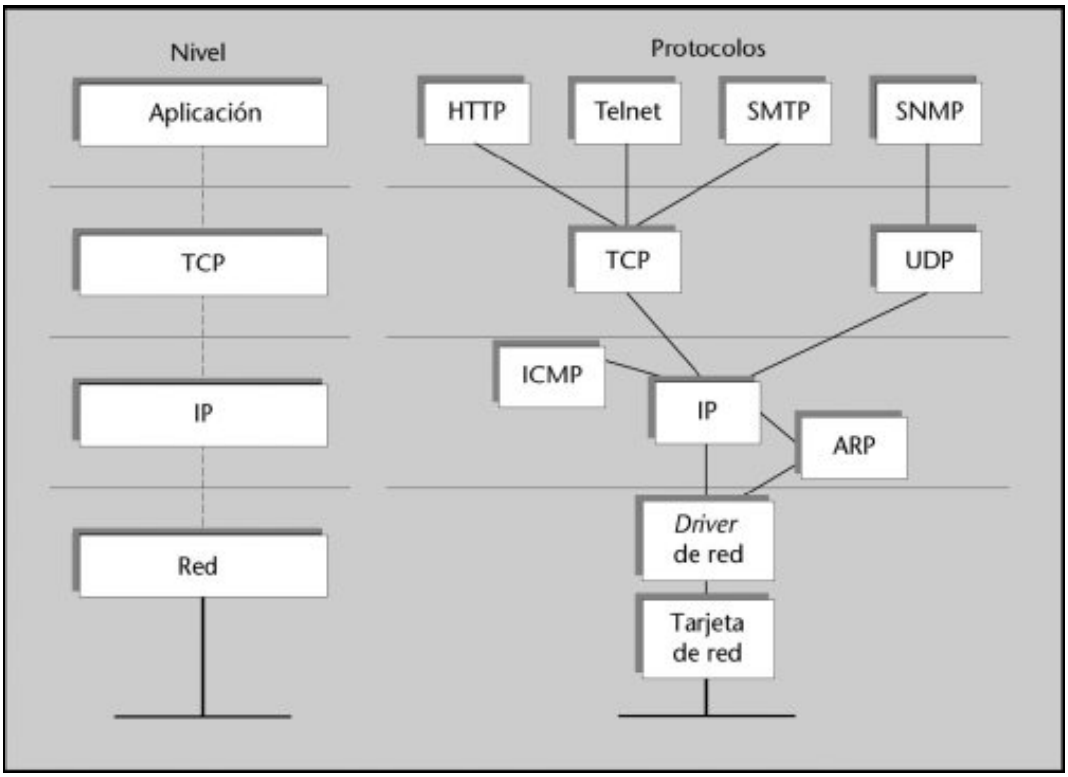
Os principios da expansión de TCP/IP son diversos. Quizais o máis importante é que especifica unha pila de protocolos simple, xa que con media ducia deles pode funcionar. De feito, elimina dúas capas que ten o modelo OSI, a de presentación e a de sesión, deixando as funcións destes niveis á capa de aplicación, é dicir, ao programador.

Ademais, TCP/IP apareceu antes que OSI razón que lle permitiu converterse nun estándar de facto nos anos 80 o que fai que TCP/IP sexa tamén independente dos fabricantes e das marcas comerciais, polo que soporta múltiples tecnoloxías distintas, e pode pode funcionar en máquinas pequenas e grandes. TCP/IP admite calquera tipo de tecnoloxía de rede sen depender do hardware.

Existen, ademais, outras arquitecturas de protocolos, aínda que a maior parte se atopan en desuso: SNA de IBM, IPX/SPX de Novell, NetBIOS sobre NetBEUI de Microsoft, etc.

Os protocolos de Internet

Seguindo o principio *Divide et vinces* de Julio César, a pila TCP/IP está estruturada en catro capas ou niveis, tal e como se ve na seguinte figura:



No nivel de aplicación da pila TCP/IP existen moitos protocolos e cada ano aparecen novos servizos ou aplicacións con novos protocolos.

O protocolo ARP (*Address Resolution Protocol*), definido no RFC 826, serve de ponte entre o nivel de rede e o nivel de enlace. É o encargado de averiguar a dirección física, ou dirección MAC (*Media Access Control*) dunha tarxeta de rede, a partir da dirección IP da máquina.

O protocolo ICMP (*Internet Control Messaging Protocol*), definido no RFC 792, permite aos encamiñadores ou nodos intermedios enviar mensaxes de control aos equipos que enviaron a información. Esencialmente, este protocolo responde ás cuestións ¿por que non se entregou un paquete? e ¿por onde acaba de pasar o noso paquete? ICMP só informa, non corrixe erros, polo que deberá ser o equipo orixe da transmisión o que corrixa ditos erros.

O protocolo IP (*Internet Protocol*), definido no RFC 791, é o encargado da comunicación de datos a través dunha rede de paquetes conmutados. É un protocolo **non orientado a conexión**, o que quere dicir que cada paquete que envíe non ten por que ir sempre polo mesmo camiño, xa que non se establece ningún circuíto permanente co destino. A unidade básica de transferencia do IP é o paquete que encapsula os datos que lle veñen do nivel superior (transporte). Como IP non garante a entrega de paquetes poden aparecer duplicados ou paquetes perdidos. Estas cuestións deléganse nos niveis superiores. Por todo isto, ao IP chámaselle protocolo de tipo *best-effort*, porque fai o mínimo para poder desempeñar as súas funcións.

O protocolo TCP (*Transmission Control Protocol*), definido no RFC 793, encárgase de aportar fiabilidade á comunicación, debido a que IP é un protocolo *best-effort*. Por iso TCP é un protocolo **orientado a conexión**, xa que establece unha conexión virtual ou lóxica (non física) co destinatario para cada aplicación que o solicite. Unha vez finalizada a transmisión, pechara a conexión previamente aberta. TCP pode ter varias conexións ao mesmo tempo con mesmo destinatario. Estas conexións identifícanse polo número de porto utilizado, o cal diferencia á aplicación que recollerá a mensaxe. Por exemplo: podemos estar conectados ao mesmo tempo a un servidor web no porto 80 e estar descargando un ficheiro polo porto 21 correspondente ao FTP. Desta forma non haberá dúbida sobre que paquete corresponde a cada aplicación.

O protocolo UDP (*User Datagram Protocol*), definido no RFC 768, é un protocolo non orientado a conexión. A súa utilización céntrase en obter maior velocidade e flexibilidade na comunicación, ademais de incorporar o mecanismo de identificación de aplicacións mediante portos.

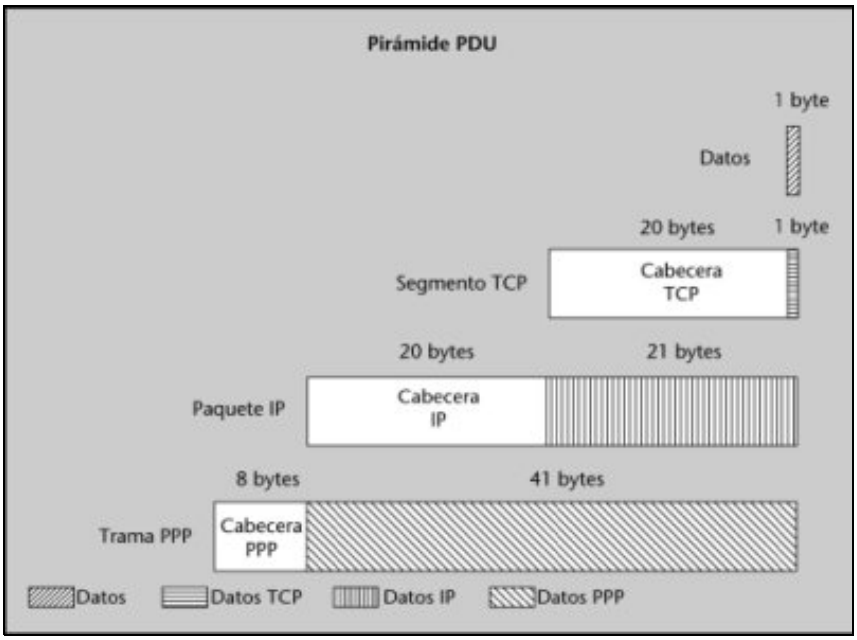
Encapsulamento

Cada protocolo funciona cunhas estruturas fundamentais que se chaman PDU (Unidade de Datos do Protocolo). En cada nivel da pila a PDU ten un nome distinto:

- Nivel de enlace/físico: **Tramas**
- Nivel de rede: **Paquetes**
- Nivel de transporte: **Segmentos (TCP) e datagramas (UDP)**
- Nivel de aplicación: **Mensaxes** ou **datos**

Os datos que xenere unha aplicación dividiranse en varios partes que se incluirán en segmentos (PDU do nivel de transporte) que á súa vez se dividirán en varios paquetes (nivel de rede), e estes, en varias tramas (nivel de enlace). Este mecanismo coñecese como **encapsulamento** ou empaquetado e é similar ao das famosas monecas rusas.

Polo tanto, cada nivel engade información do protocolo á PDU do nivel superior producíndose unha cascada de PDU que vai descendendo ata o nivel inferior, que finalmente é quen transmite fisicamente os bits en forma de impulsos eléctricos.



Sniffers

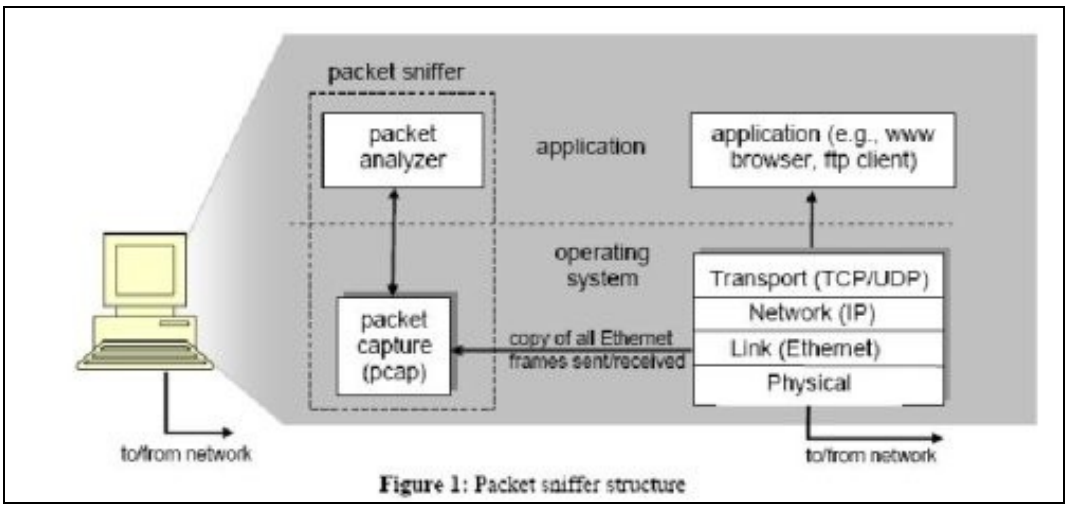


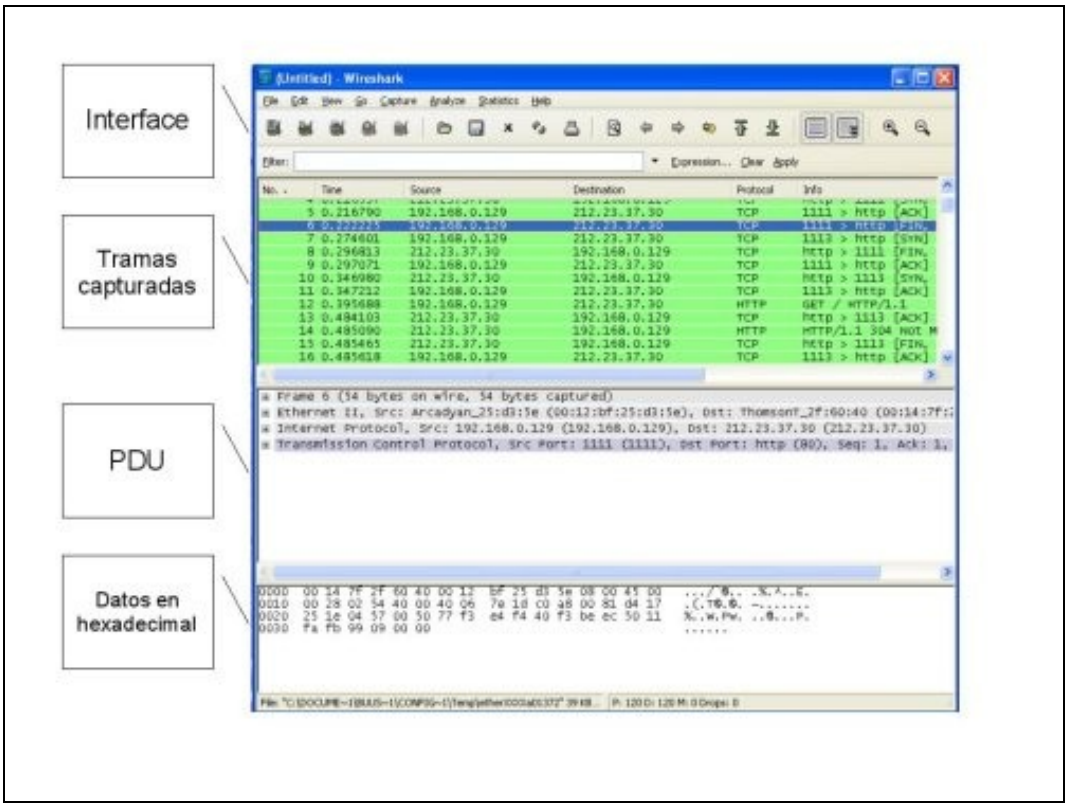
Figure 1: Packet sniffer structure

Un *sniffer* ou *packet sniffer* é unha ferramenta que captura os datos que chegan e/ou saen do noso computador. Permite observar as mensaxes intercambiadas entre as entidades de protocolo nunha rede, aínda que estas mensaxes non estean dirixidas a nós. Polo tanto, o que fai e capturar as PDU dos diferentes niveis da pila de protocolos (recorda a encapsulación).

Aos *sniffers* tamén se lles chama analizadores de tráfico e son elementos pasivos porque non envía paquetes de ningún tipo á rede, senón que recibe unha copia da trama que vai pola rede activando o modo promiscuo da tarxeta de rede (recorda o funcionamento dunha rede de difusión en medio compartido).

O *sniffer* coñece ás especificacións dos distintos protocolos, polo que pode analizar e amosar os paquetes á perfección. Coñece o formato dunha trama ethernet a partir da que se extrae o paquete IP que leva, á súa vez, un segmento TCP (ou UDP) e dentro os datos a transmitir xerados pola aplicación.

Un dos *sniffers* máis potentes do mercado é o Wireshark (anteriormente Ethereal). É un programa multiplataforma que funciona en GNU/Linux, Ms-Windows e MacOS. Soporta máis de 500 protocolos, é software libre e ten unha comunidade de desenvolvedores e usuarios moi importante. Ademais, ten abundante documentación na súa web polo que é moi recomendable para estudar o funcionamento dos protocolos e das pilas de protocolos.



--Arribi 12:00 6 oct 2009 (BST)