Los protocolos de comunicaciones

Protocolos

Lista de protocolos de comunicaciones que se utilizan en la Internet/Intranet.

Protocolo	Descripción	Propósito
ARP	Address Resolution Protocol	Mapea direcciones IP con direcciones MAC. Es el encargado de asociar direcciones de red con direcciones físicas.
BGP	Border Gateway Protocol	Se usa para intercambiar información de encaminamiento entre sistemas autónomos, de tal manera que se conozcan las diferentes redes que son alcanzables dentro de cada sistema. Este protocolo es similar a EGP.
BOOTP	Bootstrap Protocol	Protocolo utilizado principalmente en redes TCP/IP para configurar estaciones de trabajo sin disco. Este protocolo se define en los documentos RFC-951 y RFC-1542.
CHAP	Challenge Handshake Authentication Protocol	The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses the industry-standard Message Digest 5 (MD5) hashing scheme to encrypt the response.
CLNP	Connectionless Network Protocol	Protocolo de red no orientado a conexión. Es un protocolo para la transmisión de datagramas y que proporciona mecanismos de fragmentación identificando los datos de manera completa o parcial.
CSLIP	Compressed SLIP	Muy similar a SLIP pero las cabeceras están comprimidas.
CSMA/CD	Carrier Sense Medium Access/Colission Detection	Acceso múltiple con escucha de portadora y con detección de colisión. Es un método de control de acceso al medio muy utilizado en los comienzos de la tecnología ethernet para

		redes de área local.
DHCP	Dynamic Host Configuration Protocol	Is a client-server technology that allows DHCP servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients.
DNS	Domain Name System/Service	Mapea las direcciones IP con los nombres de equipos.
DVMRP	Distance-Vector Multicast Routing Protocol	Es un protocolo de enrutamiento multidifusión haciendo uso del algoritmo vector-distancia. Se utiliza en equipos conmutadores (switchs) del rango empresarial.
EGP	Exterior Gateway Protocol	La información del protocolo EGP se intercambia entre los denominados encaminadores vecinos. Dos encaminadores se considerarán vecinos si están conectados a la misma red o están conectados por un enlace punto a punto. Este protocolo es similar a BGP.
FINGER	Servicio basado en el documento RFC1196	Ofrece la posibilidad de obtener información sobre un usuario en particular de un equipo local o de un servidor remoto. Se basa en TCP, usa el puerto 79.
FTP	File Transfer Protocol	Permite la transferencia de ficheros entre dos equipos de la red. El protocolo diferencia entre una conexión de control y otra conexión de datos. Se basa en TCP y usa el puerto 21.
HELLO	Routing protocol	Protocolo de enrutamiento muy utilizado en los comienzos de la era internet (a principios de los 80). Este protocolo está definido en el documento RFC-891.
HMP	Host Monitoring Protocol	Protocolo para controlar a un equipo informático que es miembro de una red informática. Protocolo en desuso. Este protocolo está definido en el documento RFC-869.
HTTP	HyperText Transfer Protocol	Protocolo utilizado para la transmisión de información organizada de forma hipertextual con vínculos internos y/o externos hacia otras fuentes con información. Utiliza el puerto TCP:80.

		Este protocolo se define en los documentos RFC-1945, RFC-2616, RFC-2774 y RFC-7540.
ICMP	Internet Control Message Protocol	Ofrece la posibilidad de que un dispositivo destino conectado a la red comunique al dispositivo origen, también conectado a la red, que ha habido algún problema con el datagrama que ha enviado.
IDENTD	Identification Daemon	El protocolo de identificación permite conocer la identidad del usuario que ha establecido cierta conexión TCP.
IDRP	Interdomain Routing Protocol	Protocolo para el intercambio de información de enrutamiento entre dominios. Es un protocolo de enrutamiento por vector de distancia diseñado para conectar dominios de enrutamiento OSI.
IGMP	Internet Group Management Protocol	Protocolo de gestión de grupos de internet. Este protocolo de red se utiliza para intercambiar información acerca del estado de pertenencia entre los enrutadores IP que admiten la multidifusión y los miembros de grupos de multidifusión. Este protocolo se define en el documento RFC-3376.
IGP	Interior Gateway Protocol	Protocolo de Pasarela Interna o Interior. Hace referencia a los protocolos usados dentro de un sistema autónomo.
IMAP	Internet Message Access Protocol	Protocolo para el acceso a los mensajes de la internet. Mediante este protocolo se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Este protocolo se define en el documento RFC-3501.
IP	Internet Protocol	Diseñado para interconectar sistemas basados en redes de intercambio de paquetes. Permite el intercambio de bloques datos, denominados datagramas, entre dispositivos conectados a una red y cada uno de ellos tiene una dirección única llamada dirección IP.
IRC	Internet Relay Chat	Es un protocolo de comunicación en tiempo real basado en texto,

		que permite la charla entre dos o más personas. Hace uso del puerto de comunicación TCP:6667 y TCP:194.
IRDP	ICMP Router Discovery Protocol	Es un protocolo que usa mensajes ICMP entre los enrutadores para descubrirse la dirección IP de ellos. Este protocolo se define en el documento RFC-1256.
IS-IS	Intermediate System to Intermediate System Protocol	Es un protocolo de enrutamiento diseñado para mover información de manera eficiente dentro de una red de computadoras, un grupo de computadoras conectadas físicamente o dispositivos similares. Lo logra determinando la mejor ruta para los datos a través de una red de conmutación de paquetes.
LCP	Link Control Protocol	Protocolo para el control de enlace. Los paquetes LCP están incrustados sobre los paquetes PPP. El protocolo LCP comprueba la identidad del dispositivo vinculado y acepta o rechaza el dispositivo, determina el tamaño del paquete aceptable para la transmisión, busca errores en la configuración y puede terminar el enlace si los requisitos exceden los parámetros.
LDAP	Lightweight Directory Access Protocol	Es un protocolo de acceso unificado a un conjunto de información sobre una red. Permite el acceso a un servicio de directorio con información precisa sobre la autenticación de los usuarios y otros recursos de red. Hace uso del puerto de comunicación TCP:389.
LLMNR	Link-Local Multicast Name Resolution	La resolución de nombres de multidifusión local de enlace es un protocolo basado en el formato de paquete del sistema de nombres de dominio que permite que los equipos IPv4 e Ipv6 realicen la resolución de nombres para los equipos en el mismo enlace local.
MOSPF	Multicast Extensions to Open Shortest Path First	Extensiones de multidifusión para primero abrir el camino más corto. Es una extensión del protocolo OSPF que facilita la interoperabilidad entre enrutadores tipo unidifusión y multidifusión.
MTPROTO	Mobil Protocol	Protocolo móvil de Telegram Messenger.

		El protocolo está diseñado para acceder a una API de servidor desde aplicaciones que se ejecutan en dispositivos móviles. Utiliza además otros protocolos: HTTP, HTTPS, TCP y Websocket. Hace uso del puerto de comunicación TCP:80 y HTTP:80.
NBNS	NetBIOS Name Service	Hace uso del puerto de comunicación TCP:137 y UDP:137.
NBSS	NetBIOS Session Service	Hace uso del puerto de comunicación TCP:139.
NCP	Network Control Protocol	Está conformado por un conjunto de otros protocolos tales como PPP, LCP, AP y otros más. Se utiliza para transmitir datos multiprotocolos entre dos equipos informáticos.
NFS	Network File System	Hace uso del puerto de comunicación UDP:2049.
NNTP	Network News Transfer Protocol	Hace uso del puerto de comunicación TCP:119.
NTLM	NT Lan Manager	Es un conjunto de protocolos de seguridad de Microsoft destinados a proporcionar autenticación, integridad y confidencialidad a los usuarios. NTLM es el sucesor del protocolo de autenticación en Microsoft LAN Manager (LANMAN).
NTP	Network Time Protocol	Tiene como objetivo facilitar la sincronización horaria entre los equipos de una red con una precisión de 1 a 50 ms. respecto a una hora oficial establecida.
OSPF	Open Shortest Path First	Es un protocolo de red para encaminamiento jerárquico de pasarela interior (IGP). Usa un algoritmo para calcular la ruta más corta entre dos equipos informáticos.
PAP	Password Authentication Protocol	Es un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. Este protocolo es un subprotocolo utilizado por la autenticación del protocolo PPP (Protocolo de punto a punto), validando a un usuario que accede a ciertos recursos.
PIM	Protocol Independent Multicast	Es un protocolo de encaminamiento que crea una estructura de

		árbol de distribución entre los clientes de multidifusión formando dominios.
POP3	Post Office Protocol	Es utilizado para transferir correo desde un servidor hasta una estación de trabajo. Usa el puerto TCP:110. El cliente y el servidor POP3 inician una negociación que consiste en una serie de comandos y respuestas hasta que la conexión finaliza de manera ordenada o es abortada por alguno de ellos.
PPP	Point-to-Point Protocol	Protocolo punto a punto. Es utilizado para interconectar directamente entre dos equipos físicos de una red. Se corrigen todas las deficiencias que tiene SLIP. Consta de tres partes: datagramas IP, un protocolo para negociar diferentes opciones (LCP) y un protocolo de control de red (NCP).
PPPoE	PPP over Ethernet	Protocolo punto a punto sobre Ethernet. Este encapsula los paquetes PPP sobre la capa Ethernet a los efectos de proveer conexión de banda ancha en cablemódems y en xDSL.
RARP	Reverse Address Resolution Protocol	Su función es permitir a una estación de red obtener su dirección IP conociendo únicamente su dirección física (MAC).
RIP	Routing Information Protocol	Fue diseñado para realizar el intercambio de información de encaminamiento entre los ruteadores y equipos de una red.
RTP	Real-time Transport Protocol	Protocolo de transporte en tiempo real. Es utilizado en las aplicaciones que ofrecen servicios de videoconferencias para la transmisión de audio y video en vivo.
RTCP	Real-time Control Protocol	Protocolo de control en tiempo real. Proporciona información de control sobre un flujo de datos asociado a las aplicaciones multimediales a los efectos de ofrecer una buena calidad de servicio para la transmisión de audio y video en vivo.
SLIP	Serial Line Internet Protocol	Encapsula datagramas IP sobre una línea serial.

SMB	Server Message Block	Es un protocolo que permite compartir ficheros, directorios e impresoras en un entorno de red Windows o también en Linux.
SMTP	Simple Mail Transfer Protocol	Su función es enviar correo de una manera fiable y eficiente. Es independiente del sistema de transmisión y únicamente requiere un canal de envío de datos. Usa el puerto TCP:25. El envío se hace desde una estación de trabajo hacia un servidor.
SNMP	Simple Network Management Protocol	Permite la gestión de los recursos que están disponibles en una red. Este protocolo consta de los siguientes elementos: agente de gestión, gestor, objeto gestionado y protocolo de gestión.
SSDP	Simple Service Discovery Protocol	Se utiliza este protocolo para la búsqueda de dispositivos UPnP conectados en un entorno de red. Hace uso de los puertos TCP:1900 y UDP:1900.
SSH	Secure Shell Protocol	También conocido como 'SSH Remote Login Protocol'. Permite el acceso remoto a un servidor por medio de un canal seguro de comunicaciones sobre la cual toda la info. está encriptada. Hace uso del puerto de comunicación TCP:22.
TCP	Transmission Control Protocol	Es un protocolo orientado a conexión que genera un circuito virtual entre dos entidades de red y que proporciona fiabilidad extremo a extremo. Utiliza una técnica conocida como acuse de recibo para garantizar la llegada de los datos a la entidad remota.
TFTP	Trivial File Transfer Protocol	Es una simplificación del protocolo FTP para la transferencia de ficheros. Debido a su sencillez hace uso de UDP en el nivel de transporte. Las capacidades de TFTP se limitan al envío y recepción de ficheros y carece de opciones típicas de FTP como la autentificación de usuarios o el listado de directorios.
Telnet	Telecommunications Network Protocol	Su propósito es proporcionar la facilidad bidireccional necesaria para que diferentes computadoras puedan acceder a cualquier tipo de equipo dentro de una red.

		Se basa en TCP para llevar a cabo el intercambio de datos y usa el puerto 23. Cuando la conexión se establece cada extremo de la misma se denomina terminal virtual de red.
UDP	User Datagram Protocol	Es un protocolo no orientado a conexión, que transporta un flujo de bytes, conocidos como datagrama, desde un equipo origen hasta otro equipo destino. No es un protocolo fiable, debido a que no garantiza la llegada de los mensajes ni la retransmisión de los mismos.
UUCP	Unix to Unix Copy Protocol	Ofrece servicios para copiar ficheros entre equipos locales y remotos.
VoIP	Voice over IP	Este protocolo hace posible que la señal de voz sea transmitida en forma digital a internet empleando el protocolo IP.
XMPP	Extensible Messaging and Presence Protocol	Es un protocolo abierto y extensible basado en XML para el intercambio de datos, ideado para mensajería instantánea. La compañía de comunicaciones WhatsApp Inc. lo utiliza en sus productos de telefonía móvil. Hace uso de los siguientes puertos de comunicaciones: TCP:5222;5223;5269. Para más info. leer el siguiente doc. RFC-6120 en tools.ietf.org/html/rfc6120 y también en www.rfc-editor.org/info/rfc6120.

El significado de...

MAC: es 'Media Access Control' que equivale en castellano a Control de Acceso al Medio. Identifica unívocamente mediante un número de 48 bits a un dispositivo físico/lógico de comunicación por ejemplo una tarjeta de red. Este dispositivo también puede ser virtual en un sistema operativo con un número MAC ficticio.
RFC: es 'Request For Comments' que equivale en castellano a Petición De Comentarios.
OSI: es 'Open System Interconnection' que equivale en castellano a Interconexión de Sistemas Abiertos.
UPnP: es 'Universal Plug and Play' que equivale en castellano a Enchufe y Uso Universal.

Dispositivos de comunicaciones

Enrutadores (routers)

In TCP/IP networking, routers are used to interconnect hardware and software used on different physical network segments called subnets and forward IP packets between each of the subnets.

Placas de redes

Fabricante: Atheros Communications Inc.
Descripción: Atheros AR9485WB-EG Wireless Network Adapter
Dirección física: 94-DB-C9-B5-3C-44

Fabricante: Atheros Communications Inc.
Descripción: Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20)
Dirección física: 10-BF-48-28-34-39

Fabricante: Realtek Semiconductor Corp.
Descripción: NIC PCI-E de LAN inalámbrica 802.11n Realtek RTL8192CE
Dirección física: FC-8F-C4-04-05-08

Fabricante: Realtek Semiconductor Corp.
Descripción: Controladora Realtek PCIe FE Family
Dirección física: 00-30-67-0A-D3-33

Comando NET SEND en Windows Server 2003, Enterprise Edition

Uso

Transmite mensajes del servicio de alertas y del comando 'net send' entre clientes y servidores. Puede encontrar más info en 'Servicios'. Para utilizar este comando debe estar habilitado el servicio Messenger.
Ir a Inicio/Todos los programas/Herramientas administrativas/Servicios y activar el servicio Messenger de forma automática.
Desde cmd.exe, también puede usarse el comando 'net start messenger' para iniciar y 'net stop messenger' para detener el servicio.
Para acceder a "Administración de equipos" desde cmd.exe ejecute el comando 'compmgmt.msc', luego seleccione 'Servicios y Aplicaciones/Servicios' y en el panel derecho aparecen todos los servicios que dispone el sistema operativo.

Sintaxis

NET SEND {nombre | * | /DOMAIN[:nombre] | /USERS} mensaje

Ejemplo

C:\>net send Administrador "te tengo en la mira..."

Aparece el cuadro de diálogo Messenger Service que dice:
'Mensaje de MAQUINA a ADMINISTRADOR el 08/01/2009 20:40:20

te tengo en la mira...'

Comando NET SEND en Windows XP, Service Pack 2, español

Cuando se pide una ayuda: 'net send /?' muestra incorrectamente la información solicitada. El modo de utilizar este comando en Windows XP es muy similar en Windows 2003. Se debe habilitar primero el servicio 'Mensajero (Messenger)' para usar este comando.

```
-----------------------------------------------
Comando NET en Windows Server 2012 R2, Standard
-----------------------------------------------

La sintaxis de este comando es:

NET HELP comando
     -o-
NET comando /HELP

Estos son los comandos disponibles:

  NET ACCOUNTS             NET HELPMSG              NET STATISTICS
  NET COMPUTER             NET LOCALGROUP           NET STOP
  NET CONFIG               NET PAUSE                NET TIME
  NET CONTINUE             NET SESSION              NET USE
  NET FILE                 NET SHARE                NET USER
  NET GROUP                NET START                NET VIEW
  NET HELP

NET HELP NAMES explica los diferentes tipos de nombres usados en las líneas de sintaxis de NET HELP.
NET HELP SERVICES muestra algunos de los servicios que se pueden iniciar.
NET HELP SYNTAX explica cómo leer las líneas de sintaxis de NET HELP.
NET HELP comando | MORE muestra la Ayuda en una pantalla a la vez.

-------------------------------------------------------
Comando NET HELP NAMES en Windows Server 2012 R2, Standard
-------------------------------------------------------

La sintaxis de este comando es:

NAMES
The following types of names are used with Windows:

Computername      A unique name that identifies a computer on
                  the local-area network.

Devicename        The name by which Windows identifies a disk resource
                  or printer. A disk resource is identified by a drive
```

	letter followed by a colon (for example, D:). A printer is identified by a port name followed by a colon (for example, LPT1:).
Workgroup	A group of computers on the network. Each workgroup has a unique name.
Localgroup	A group of names in a Workgroup that are granted the same rights.
Domain	A group of Windows Servers, Windows Workstations and other computers on the network. A domain has a unique name. Usually, you must log on in a domain to gain access to the network. Domains are created and managed with Windows Server.
Global group	A group of names in a domain that are granted the same rights.
Filename	The name of a file. Under the file allocation table (FAT) file system, a filename can have as many as eight characters, followed by a period (.) and an extension of as many as three characters. Under NTFS and HPFS, a filename can have as many as 254 characters.
Network path	A description of the location of a shared resource, consisting of a computer's computername followed by the sharename of the resource. The computername is preceded by two backslashes, and the sharename is preceded by one backslash (for example, \\SERVER1\RESOURCE).
Path	The location of a directory. A path can consist of a devicename and one or more directory names. A backslash (\) precedes each directory name (for example, C:\CUSTOMER\CORP\ACCT).
Pathname	A path and a filename. The filename is preceded by a backslash (\) (for example, C:\CUSTOMER\CORP\REPORT.DOC).

```
Sharename          A name that identifies a shared resource on a computer. A
                   sharename is used with the computer's computername to form
                   a network path (as in \\SERVER\RESOURCE).

Username           The name a person supplies when logging on at
                   a computer.

To view these definitions one screen at a time, type NET HELP NAMES | MORE.
```

Comando NET HELP SERVICES en Windows Server 2012 R2, Standard

---

La sintaxis de este comando es:

```
SERVICES
NET START se puede usar para iniciar servicios, incluidos:

   NET START BROWSER
   NET START DHCP CLIENT
   NET START EVENTLOG
   NET START FILE REPLICATION
   NET START NETLOGON
   NET START PLUG AND PLAY
   NET START REMOTE ACCESS CONNECTION MANAGER
   NET START ROUTING AND REMOTE ACCESS
   NET START RPCSS
   NET START SCHEDULE
   NET START SERVER
   NET START SPOOLER
   NET START TCP/IP NETBIOS HELPER
   NET START UPS
   NET START WORKSTATION

Cuando se escriben en el símbolo del sistema, los nombres de servicio de dos o más palabras deben estar entre comillas.
Por ejemplo, NET START "DHCP Client" inicia el servicio DHCP Client.
```

```
------------------------------------------------------------
Comando NET HELP SYNTAX en Windows Server 2012 R2, Standard
------------------------------------------------------------

La sintaxis de este comando es:

SYNTAX
Las siguientes convenciones se usan para indicar la sintaxis de comandos:

-  Las mayúsculas representan las palabras que se deben escribir como se
   muestran. Las minúsculas representan los nombres de elementos variables,
   como nombres de archivo.

-  Los elementos opcionales que se pueden proporcionar con el comando
   se indican entre los caracteres [ y ].

-  Las listas de elementos se indican entre los caracteres { y }.
   Proporcione uno de los elementos junto con el comando.

-  Los elementos de una lista se separan con |. Proporcione solo uno
   de los elementos.

   Por ejemplo, en la siguiente sintaxis, debe escribir NET COMMAND y
   SWITCH1 o SWITCH2. La especificación de un nombre es opcional.
       NET COMMAND [nombre] {SWITCH1 | SWITCH2}

-  Los puntos suspensivos [...] indican que se puede repetir el elemento
   anterior. Separe los elementos con espacios.

-  Los caracteres [,...] indican que se puede repetir el elemento anterior,
   pero los elementos se deben separar con comas o punto y coma, no con
   espacios.

-  Escriba los nombres de servicio con más de una palabra entre comillas
   en el símbolo del sistema. Por ejemplo, NET START "COMPUTER BROWSER"
   inicia el servicio Explorador de equipos.
```

Comandos de Windows

Esta es una breve descripción de los comandos que utilizan la pila de protocolos TCP/IP en Windows Server 2022, 2019, 2016, 2012, 2008, 2003, Windows XP, Vista, 7, 8, 10, 11 y otros Windows que andan dando vuelta por la Internet.

arp Muestra y modifica entradas en la caché de Protocolo de resolución de direcciones (ARP), que contiene una o varias tablas utilizadas para almacenar direcciones IP y sus direcciones físicas Ethernet o Token Ring resueltas. Existe una tabla independiente para cada adaptador de red Ethernet o Token Ring instalados en el equipo. Si no se utilizan parámetros, el comando arp muestra una ayuda.

finger Muestra información acerca de uno o varios usuarios en un equipo remoto especificado (generalmente, un equipo LINUX/UNIX) que ejecuta el servicio o demonio finger. El equipo remoto especifica el formato y la salida de la información que se muestra acerca del usuario. Si se utiliza sin parámetros, el comando finger muestra una ayuda. Los resultados obtenidos varían según el sistema remoto.

ftp Transfiere archivos en equipos que ejecutan un servicio del servidor del Protocolo de transferencia de archivos (FTP, File Transfer Protocol) como, por ejemplo los Servicios de Internet Information Server. Ftp se puede usar interactivamente o en modo por lotes al procesar archivos de texto ASCII.

getmac Muestra la dirección física (MAC) del dispositivo de comunicación conectado a la computadora.
Este comando debe ser invocado por el administrador del sistema.

nbtstat Muestra estadísticas del protocolo NetBIOS sobre TCP/IP (NetBT), las tablas de nombres NetBIOS para el equipo local y el remoto, y la caché de nombres NetBIOS. Nbtstat permite actualizar la caché de nombres NetBIOS y los nombres registrados con el servicio WINS. Cuando se usa sin parámetros, nbtstat muestra una ayuda.

net Se utiliza básicamente para administrar una red local.

netdom Es un comando con funciones similares a **net** pero más orientado a un ambiente de red corporativo.
Este comando debe ser invocado por el administrador del sistema.

netsh Su función es similar al comando **net** pero con opciones más avanzadas.
Este comando debe ser invocado por el administrador del sistema.

netstat Muestra las conexiones de TCP activas, los puertos en que el equipo escucha, las estadísticas de Ethernet, la tabla de enrutamiento IP, las estadísticas de IPv4 (para los protocolos IP, ICMP, TCP y UDP) y las estadísticas de IPv6 (para los protocolos IPv6, ICMPv6, TCP sobre IPv6 y UDP sobre IPv6). Cuando se utiliza sin parámetros, netstat muestra las

conexiones de TCP activas.

nslookup Se utiliza para consultar un nombre DNS o una dirección IP en algún servidor DNS de la red local o en la internet.

ipconfig Muestra los valores actuales de la configuración de la red TCP/IP y actualiza la configuración de DHCP (Protocolo de configuración dinámica de host) y DNS (Sistema de nombres de dominio). Si se utiliza sin parámetros, ipconfig muestra las direcciones IPv6 o la dirección IPv4, la máscara de subred y la puerta de enlace predeterminada de todos los adaptadores.

pathping Comando que combina la funcionalidad de **ping** con la de **tracert**.

ping Comprueba la conectividad de nivel IP en otro equipo TCP/IP al enviar mensajes de solicitud de eco de ICMP (Protocolo de mensajes de control Internet). Se muestra la recepción de los mensajes de solicitud de eco correspondientes, junto con sus tiempos de ida y vuelta. Ping es el principal comando de TCP/IP que se utiliza para solucionar problemas de conectividad, accesibilidad y resolución de nombres. Cuando se usa sin parámetros, ping muestra una ayuda.

route Muestra y modifica las entradas de la tabla de rutas IP local. Si se utiliza sin parámetros, route muestra su ayuda.

rpcping Comprueba la conectividad entre el equipo local y el equipo remoto mediante los protocolos RPC y HTTP.

telnet Administra un equipo local o remoto que ejecuta el servidor Telnet.

tlnadmn Comando relacionado al servicio Telnet. Se encuentra en Windows Server 2003 y posteriores.
Puede utilizar el comando tlntadmn para administrar equipos locales o remotos que ejecuten el servidor Telnet.
Este comando es nuevo en Windows XP y la familia Windows Server 2003.

tracert Determina la ruta tomada hacia un destino mediante el envío de mensajes ICMPv6 o de petición de eco del Protocolo de mensajes de control de Internet (ICMP) al destino con valores de campo de tiempo de vida (TTL, Time to Live) que crecen de forma gradual. La ruta mostrada es la lista de interfaces de enrutador casi al lado de los enrutadores en la ruta entre el host de origen y un destino. La interfaz casi al lado es la interfaz del enrutador que se encuentra más cercano al host emisor en la ruta. Cuando se utiliza sin parámetros, el comando tracert muestra una ayuda.

trcdlc Este comando se encuentra en Windows 95/98/Me.

whoami Devuelve el nombre de dominio, el nombre de equipo, el nombre de usuario, los nombres de grupo, el identificador de inicio de sesión y los privilegios del usuario que actualmente ha iniciado la sesión en el equipo.

winipcfg Este comando es similar a ipconfig. Se encuentra en Windows 95/98/Me.

Gran parte de estos comandos cuentan con una ayuda en pantalla si escribe la opción /? a continuación del nombre del comando.
Por ejemplo: netsh /?

En Windows se encuentra el intérprete de comandos cmd.exe y su antecesor command.com que sirven para comunicarse con el sistema mediante comandos, por ejemplo dir, echo, type, copy, cls, etc., son sencillos en su uso y en su cometido pero (siempre hay un pero) pueden ser "incorrectamente" usados con fines "dudosos".
Mire este ejemplo:

C:\WINDOWS>echo 255 >> explorer.exe

¡¡¡ Qué sorpresa verdad !!!
El programa explorer acaba de aumentar su tamaño en 6 bytes más porque se le inyectó 2+5+5+CR+LF+SPC al final del mismo. Que tal.
Entonces surge una pregunta entre tantas otras que nos podemos hacer como administradores de sistemas ¿ cómo podemos controlar la integridad de los archivos y de los directorios ?
En GNU/Linux se tiene el comando /usr/bin/stat que, básicamente, muestra todas las propiedades y permisos que tiene un fichero.
Pero en Windows este comando no está incluido. ¿ Porqué ?. No sé.
Pruebe a ejecutar el siguiente ejemplo:

```
          [root@localhost ~]# stat /boot/vmlinuz-2.6.22.14-72.fc6PAE
(linea 1)     File: «/boot/vmlinuz-2.6.22.14-72.fc6PAE»
(linea 2)     Size: 2062772         Blocks: 4040       IO Block: 4096   fichero regular
(linea 3)   Device: 302h/770d       Inode: 1114139     Links: 1
(linea 4)   Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
(linea 5)   Access: 2010-10-10 00:14:30.000000000 -0300
(linea 6)   Modify: 2007-11-21 17:02:20.000000000 -0300
(linea 7)   Change: 2010-08-10 19:32:09.000000000 -0300
```

Los resultados obtenidos de este comando fueron tomados de Fedora Core 6 con núcleo 2.6.22.14-72. Puede que en su sistema GNU/Linux tenga otra versión de núcleo.
En la línea 1 aparece el nombre completo del fichero a examinar.
En la línea 2 aparece entre otras cosas el tamaño del fichero expresado en bytes: 2062772.
En la línea 3 aparece el código del dispositivo en hexadecimal/decimal que contiene a este fichero examinado: 302h/770d.
En la línea 4 aparecen modo de acceso, identificador del usuario propietario e identificador del grupo.
Y por último y lo más destacable los tres tiempos que registran la actividad del fichero: tiempo de acceso, tiempo de modificación y tiempo de cambio de modo. Estos tiempos nos van a dar la pauta si el fichero fue alterado en su integridad lógica por algún usuario o aplicación malintencionado.
Si quiere conocer más detalles sobre stat, ejecute así:

```
[root@localhost ~]# stat --help
```

Se obtiene en pantalla todas las opciones disponibles que acepta este comando.

```
[root@localhost ~]# man stat
```

O también:

```
[root@localhost ~]# info stat
```

Se accede a las páginas del manual de stat.

Biometría

La biometría es una técnica para identificar personas mediante una característica física única, como una huella digital, un ojo o un rostro. Los dispositivos biométricos comprueban la identidad de alguien mediante la comparación de una medida guardada de una característica física específica con una medida actual. El dispositivo biométrico más común es el lector de huellas digitales.
Un lector de huellas digitales es un dispositivo que usa la huella digital para identificarle.
Funciona tomando una imagen de su huella digital y guardando una copia de ella. Cuando necesita identificarse, como al iniciar la sesión en un sitio web o en Windows, el lector de huellas digitales escanea su huella digital y la compara con la versión guardada.
Puede usar un equipo portátil con un lector de huellas digitales integrado o comprar un lector de huellas digitales externo y conectarlo al equipo.

Salida del comando netstat en Fedora Core 6

 # netstat -l

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:swat                      *:*                         LISTEN
tcp        0      0 *:netbios-ssn               *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:telnet                    *:*                         LISTEN
tcp        0      0 localhost.localdomain:ipp   *:*                         LISTEN
tcp        0      0 localhost.localdomain:smtp  *:*                         LISTEN
tcp        0      0 *:microsoft-ds              *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
udp        0      0 *:filenet-tms               *:*
udp        0      0 straton.linu:netbios-ns     *:*
udp        0      0 *:netbios-ns                *:*
udp        0      0 straton.lin:netbios-dgm     *:*
udp        0      0 *:netbios-dgm               *:*
udp        0      0 *:mdns                      *:*
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:ipp                       *:*
udp        0      0 *:filenet-rpc               *:*
udp        0      0 *:mdns                      *:*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     7077   @/var/run/hald/dbus-xExCVDhOTi
unix  2      [ ACC ]     STREAM     LISTENING     6290   /var/run/audit_events
unix  2      [ ACC ]     STREAM     LISTENING     6365   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     6448   /var/run/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     6516   /var/run/nscd/socket
unix  2      [ ACC ]     STREAM     LISTENING     6683   /var/run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     7076   @/var/run/hald/dbus-aDlnpIT8QX
unix  2      [ ACC ]     STREAM     LISTENING     6934   /tmp/.font-unix/fs7100
unix  2      [ ACC ]     STREAM     LISTENING     6872   /dev/gpmctl
unix  2      [ ACC ]     STREAM     LISTENING     7047   /var/run/avahi-daemon/socket
```

 # netstat -ln

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:901                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:139                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:23                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:445                 0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
udp        0      0 0.0.0.0:32768               0.0.0.0:*
udp        0      0 155.95.86.70:137            0.0.0.0:*
udp        0      0 0.0.0.0:137                 0.0.0.0:*
udp        0      0 155.95.86.70:138            0.0.0.0:*
udp        0      0 0.0.0.0:138                 0.0.0.0:*
udp        0      0 0.0.0.0:5353                0.0.0.0:*
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 :::32769                    :::*
udp        0      0 :::5353                     :::*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     7077   @/var/run/hald/dbus-xExCVDhOTi
unix  2      [ ACC ]     STREAM     LISTENING     6290   /var/run/audit_events
unix  2      [ ACC ]     STREAM     LISTENING     6365   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     6448   /var/run/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     6516   /var/run/nscd/socket
unix  2      [ ACC ]     STREAM     LISTENING     6683   /var/run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     7076   @/var/run/hald/dbus-aDlnpIT8QX
unix  2      [ ACC ]     STREAM     LISTENING     6934   /tmp/.font-unix/fs7100
unix  2      [ ACC ]     STREAM     LISTENING     6872   /dev/gpmctl
unix  2      [ ACC ]     STREAM     LISTENING     7047   /var/run/avahi-daemon/socket
```

Salida del comando netstat en Windows Server 2003

C:\>netstat -a

```
Conexiones activas

  Proto  Direcci¢n local        Direcci¢n remota       Estado
  TCP    tonomac:epmap          tonomac.windows.net:0  LISTENING
  TCP    tonomac:microsoft-ds   tonomac.windows.net:0  LISTENING
  TCP    tonomac:blackjack      tonomac.windows.net:0  LISTENING
  TCP    tonomac:cap            tonomac.windows.net:0  LISTENING
  TCP    tonomac:exlm-agent     tonomac.windows.net:0  LISTENING
  TCP    tonomac:cgms           tonomac.windows.net:0  LISTENING
  TCP    tonomac:csoftragent    tonomac.windows.net:0  LISTENING
  TCP    tonomac:netbios-ssn    tonomac.windows.net:0  LISTENING
  UDP    tonomac:epmap          *:*
  UDP    tonomac:microsoft-ds   *:*
  UDP    tonomac:isakmp         *:*
  UDP    tonomac:redwood-broker  *:*
  UDP    tonomac:ipsec-msft     *:*
  UDP    tonomac:ntp            *:*
  UDP    tonomac:ntp            *:*
  UDP    tonomac:netbios-ns     *:*
  UDP    tonomac:netbios-dgm    *:*
```

C:\>netstat -an

```
Conexiones activas

  Proto  Direcci¢n local        Direcci¢n remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3002         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3003         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3004         0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
```

```
  UDP    0.0.0.0:3001           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    192.168.56.1:123       *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
```

Salida del comando finger en Windows XP, Service Pack 2, español

---

C:\>finger root@192.168.56.101

```
[192.168.56.101]
Login: root                             Name: Administrador del sistema.
Directory: /root                        Shell: /bin/bash
Office: Marité, +1-921-685-6101         Home Phone: 155958672
On since Sun Oct 24 16:26 (ART) on tty1   13 minutes 20 seconds idle
On since Sun Oct 24 16:35 (ART) on tty2   5 minutes 32 seconds idle
No mail.
No Plan.
```

En este ejemplo, se solicita información sobre el usuario 'root' en el equipo terminal cuya dirección IP es 192.168.56.101.
Si en caso de no encontrar la cuenta del usuario, el servidor devolvería la siguiente respuesta:

C:\>finger root@192.168.56.101

```
[192.168.56.101]
finger: root: no such user.
```

En 192.168.56.101 debería estar corriendo el servidor finger para aceptar las peticiones de los equipos clientes.
En GNU/Linux trae un programa cliente (finger) y un programa servidor (fingerd) mientras que en Windows XP sólo trae la parte cliente (finger.exe).

Salida del comando ipconfig en Windows Server 2012 R2 Standard, español

---

C:\>ipconfig /displaydns

```
Configuración IP de Windows

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
----------------------------------------
Nombre de registro  . : 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa.
Tipo de registro  . . : 12
Período de vida . . . : 86400
Longitud de datos . . : 4
Sección . . . . . : respuesta
Registro PTR. . . . . : localhost


1.0.0.127.in-addr.arpa
----------------------------------------
Nombre de registro  . : 1.0.0.127.in-addr.arpa.
Tipo de registro  . . : 12
Período de vida . . . : 86400
Longitud de datos . . : 4
Sección . . . . . : respuesta
Registro PTR. . . . . : localhost


apis.google.com
----------------------------------------
Nombre de registro  . : apis.google.com
Tipo de registro  . . : 5
Período de vida . . . : 26
Longitud de datos . . : 4
Sección . . . . . : respuesta
Registro CNAME. . . . : plus.l.google.com


isatap
----------------------------------------
No existe el nombre.


sc1.rules.mailshell.net
```

```
---------------------------------------
Nombre de registro  . : sc1.rules.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 2426
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 83.94.215.46


sc19.rules.mailshell.net
---------------------------------------
Nombre de registro  . : sc19.rules.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 2064
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 75.107.121.181


msbogusdomain7-90.com.dnsbl7.mailshell.net
---------------------------------------
Nombre de registro  . : msbogusdomain7-90.com.dnsbl7.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 1632
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 127.0.0.90


sc17.rules.mailshell.net
---------------------------------------
Nombre de registro  . : sc17.rules.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 1817
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 83.95.190.173
```

```
sc21.rules.mailshell.net
----------------------------------------
Nombre de registro  . : sc21.rules.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 2511
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 83.94.225.223


7.0.0.223.lbl7.mailshell.net
----------------------------------------
Nombre de registro  . : 7.0.0.223.lbl7.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 58
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 127.0.0.188


sc2.rules.mailshell.net
----------------------------------------
Nombre de registro  . : sc2.rules.mailshell.net
Tipo de registro  . . : 1
Período de vida . . . : 2042
Longitud de datos . . : 4
Sección . . . . . . . : respuesta
Un registro (host). . : 66.12.56.29


vbox.linux.gnu
----------------------------------------
No existe el nombre.


sc18.rules.mailshell.net
----------------------------------------
Nombre de registro  . : sc18.rules.mailshell.net
Tipo de registro  . . : 1
```

```
    Período de vida . . . : 2328
    Longitud de datos . . : 4
    Sección . . . . . : respuesta
    Un registro (host). . : 83.90.39.128


    localhost
    ---------------------------------------
    Nombre de registro  . : localhost
    Tipo de registro  . . : 1
    Período de vida . . . : 86400
    Longitud de datos . . : 4
    Sección . . . . . : respuesta
    Un registro (host). . : 127.0.0.1


    localhost
    ---------------------------------------
    Nombre de registro  . : localhost
    Tipo de registro  . . : 28
    Período de vida . . . : 86400
    Longitud de datos . . : 16
    Sección . . . . . : respuesta
    Registro AAAA . . . . : ::1

------------------------------------------------------------------------
Salida del comando nslookup en Windows Server 2012 R2 Standard, español
------------------------------------------------------------------------

    C:\>nslookup www.google.com

    DNS request timed out.
        timeout was 2 seconds.
    Servidor:  UnKnown
    Address:  192.168.43.1

    Nombre:  www.google.com
    Addresses:  2800:3f0:4003:800::1014
            74.125.21.103
```

```
            74.125.21.147
            74.125.21.99
            74.125.21.105
            74.125.21.104
            74.125.21.106

-------------------------------------------------------
Salida del comando netsh en Windows 7 Home Basic, español
-------------------------------------------------------

C:\Users\Administrador> netsh wlan show settings

Configuración de LAN inalámbrica
--------------------------------
    Mostrar redes bloqueadas en la lista de redes visibles: No

    Usar solo perfiles GP en redes configuradas con GP: No

    Modo de red hospedada permitido en el servicio WLAN: sí

    Permitir credenciales de usuario compartidas para la autenticación de red: Sí

    Período de bloqueo: no configurado.

    La lógica de configuración automática está habilitada en la interfaz "Conexión de red inalámbrica"

-----------------------------------------------------
El cortafuegos de Windows XP, Service Pack 2, español
-----------------------------------------------------

Este es un contenido típico del fichero pfirewall.log de la aplicación Firewall de Windows:

#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2010-10-25 22:41:45 OPEN-INBOUND TCP 192.168.56.101 192.168.56.1 32777 80 - - - - - - - - -
2010-10-25 22:43:59 CLOSE TCP 192.168.56.1 192.168.56.101 80 32777 - - - - - - - - -
```

```
2010-10-25 23:03:26 DROP ICMP 192.168.56.1 192.168.56.101 - - 56 - - - - 5 1 - SEND
2010-10-26 00:24:40 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2010-10-26 00:24:40 DROP UDP 0.0.0.0 255.255.255.255 68 67 576 - - - - - - - RECEIVE
2010-10-26 00:24:40 DROP UDP 0.0.0.0 255.255.255.255 68 67 576 - - - - - - - RECEIVE
2010-10-26 00:38:05 OPEN TCP 192.168.56.1 192.168.56.101 1150 79 - - - - - - - - -
2010-10-26 00:38:52 CLOSE TCP 192.168.56.1 192.168.56.101 1150 79 - - - - - - - - -
2010-11-03 00:22:07 DROP TCP 192.168.56.101 192.168.56.1 32770 23 60 S 2396361311 0 5840 - - - RECEIVE
2010-11-03 00:22:10 DROP TCP 192.168.56.101 192.168.56.1 32770 23 60 S 2396361311 0 5840 - - - RECEIVE
2010-11-03 00:22:16 DROP TCP 192.168.56.101 192.168.56.1 32770 23 60 S 2396361311 0 5840 - - - RECEIVE
2010-11-03 00:22:28 DROP TCP 192.168.56.101 192.168.56.1 32770 23 60 S 2396361311 0 5840 - - - RECEIVE
2010-11-03 00:22:48 DROP TCP 192.168.56.101 192.168.56.1 32771 21 60 S 2440287478 0 5840 - - - RECEIVE
2010-11-03 00:22:51 DROP TCP 192.168.56.101 192.168.56.1 32771 21 60 S 2440287478 0 5840 - - - RECEIVE
2010-11-03 00:22:57 DROP TCP 192.168.56.101 192.168.56.1 32771 21 60 S 2440287478 0 5840 - - - RECEIVE
2010-11-03 00:22:57 OPEN UDP 192.168.56.1 192.168.56.101 137 137 - - - - - - - - -
2010-11-03 00:23:09 DROP TCP 192.168.56.101 192.168.56.1 32771 21 60 S 2440287478 0 5840 - - - RECEIVE
2010-11-03 00:37:07 OPEN TCP 192.168.56.1 192.168.56.101 1064 79 - - - - - - - - -
2010-11-03 00:37:07 CLOSE TCP 192.168.56.1 192.168.56.101 1064 79 - - - - - - - - -
2010-11-03 00:40:37 OPEN TCP 192.168.56.1 192.168.56.101 1067 79 - - - - - - - - -
2010-11-03 00:40:37 CLOSE TCP 192.168.56.1 192.168.56.101 1067 79 - - - - - - - - -
2010-11-03 00:44:17 CLOSE TCP 192.168.56.1 192.168.56.101 1070 25 - - - - - - - - -
2010-11-03 00:44:16 OPEN TCP 192.168.56.1 192.168.56.101 1070 25 - - - - - - - - -
```

La aplicación cURL

Su pronunciación en inglés es "see URL".
Consta de un programa que se utiliza desde la línea de comandos (bash, cmd, etc.) y de una biblioteca de funciones para la transferencias de ficheros mediante el uso de los protocolos que conforman la pila TCP/IP (ftp, http y otros más).
Por ejemplo, se puede peticionar la cabecera HTTP de un servidor de páginas web para verificar su correcto funcionamiento.
cURL está disponible en GitHub para ser descargado y usarlo en su sistema informático (GNU/Linux, IBM/AIX, Android, Windows, etc.).
Dirigirse a este enlace para descargar su código fuente: https://github.com/curl/curl
Si desea conocer más acerca de su uso diríjase a la fuente de documentación: https://curl.haxx.se/docs

La aplicación ComprobarEnlace

Se trata de una aplicación que corre en el modo consola del S.O. Windows y Linux.
Sirve para comprobar si hay enlace de comunicación entre el equipo local y el equipo remoto.
La comprobación se realiza mediante los comandos: ping, pathping, nslookup, getmac, ipconfig y curl.

Ejemplos:

```
C:\Usuarios\Administrador>ComprobarEnlace 8.8.8.8
C:\Usuarios\Administrador>ComprobarEnlace -dns 8.8.8.8
C:\Usuarios\Administrador>ComprobarEnlace www.falklands.gov.fk
C:\Usuarios\Administrador>ComprobarEnlace www.antartida.gov.ar
```

Visite la página https://www.lawebdelprogramador.com/codigo/C-Visual-C/5341-Comprobar-enlace-de-comunicacion.html
para descargar el programa para Windows y para Linux.

Recursos en la red mundial

Aplicación	Propósito	URL
Free Network Analyzer	Monitorea y analiza el flujo de datos en una red.	https://freenetworkanalyzer.com/
Horde	Sistema de correo electrónico basado en http.	http://www.horde.org
LibPCAP	Librería para capturar paquetes con el fin de monitorear el tráfico de una red.	http://www.tcpdump.org
NePED	Detector de intrusos en una red.	http://www.apostols.org https://securiteam.com/tools/2GUQ8QAQOU/
NMAP	Analizador/explorador de puertos.	http://www.insecure.org

OUI	El listado público de la IEEE de los códigos de los vendedores de tarjetas de red (Organizationally Unique Identifier).	http://standards.ieee.org/regauth/oui/oui.txt http://standards-oui.ieee.org/oui/oui.txt https://linuxnet.ca/ieee/oui/
Dude	Sistema de administración y monitoreo de redes.	http://www.mikrotik.com/dude/ https://mikrotik.com/thedude

Referencias

1) Documento tcpip.pdf: TCP/IP Illustrated, Volume 1, The Protocols
W. Richard Stevens, rstevens@noao.edu, http://www.noao.edu/~rstevens
http://freecomputerbooks.com/TCP-IP-Illustrated-Vol-1-The-Protocols.html

2) Protocolos de INTERNET, diseño e implementación en sistemas UNIX
A. López y A. Novo, Ed. Alfaomega grupo editor
http://www.smartec.es/LibroProtocolos

3) WiFi Alliance: http://www.wi-fi.org

4) Centro de ayuda y soporte técnico de Microsoft Windows Server 2019/2016/2012/2008/2003, Microsoft Windows XP Professional, Microsoft Windows Vista Ultimate, Microsoft Windows 7/8 Professional y Microsoft Windows 10 Home/Professional.
https://support.microsoft.com/es-es

5) Las páginas del manual (manpages) del sistema GNU/Linux: http://man.he.net/

6) Comando pathping en Wikipedia: https://en.wikipedia.org/wiki/PathPing

7) El protocolo HELLO: http://www.tcpipguide.com/free/t_TheHELLOProtocolHELLO.htm

8) Un Tutorial de TCP/IP: https://www.rfc-es.org/rfc/rfc1180-es.txt

9) Las referencias a diversos protocolos que se usan en internet: https://wiki.wireshark.org/ProtocolReference

10) The TCP/IP Guide: http://www.tcpipguide.com/free/index.htm

11) El protocolo NCP: https://www.tutorialspoint.com/network-control-protocol-ncp

12) El protocolo de Telegram Mssenger: https://core.telegram.org/mtproto

Autor de este documento

Eugenio H. Martínez, torrentelinux@gmail.com, Tucumán, Argentina.

Marco legal

Ediciones

Ultima edición >>- 11:47 p.m. lunes, 21 de marzo de 2022
Primera edición >>- 20:16 Sábado, 29 de Agosto de 2009