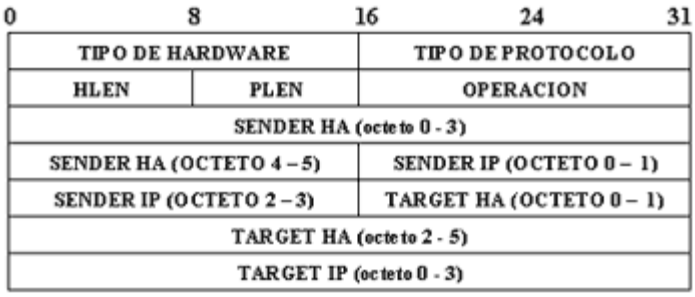
El Protocolo ARP

Es un protocolo de nivel de red cuya función es asociar a la dirección IP su correspondiente dirección de red mac. El método utilizado para la obtención de la IP es mediante peticiones de ARP. Cuando se quiere obtener la dirección mac se envía un paquete ARP request a la dirección de multififusion de red con la IP por la que se pregunta y espera obtener un paquete ARP request de otra maquina con la dirección mac de esa dirección IP. Para optimizar esto cada maquina mantiene una cache con las direcciones traducidas esto lo llamaremos tablas ARP.

Si queremos enviar un paquete de “A” a “B” que se encuentra en la misma red lo primero que hace “A” es comprobar en su tabla ARP si se encuentra la dirección MAC de “B” si es así se utiliza si no se enviara el correspondiente paquete broadcast esperando la respuesta de la maquina cuya dirección IP corresponda con la preguntada añadiendo un nuevo registro a la tabla. Estas entradas se borran cada cierto tiempo.

En un segundo caso si “A” quiere enviar un paquete a “B” que no esta en su misma red lo que hace “A” es enviarlo a través de la dirección física de su router de salida, para ello consulta la tabla ARP realizando el correspondiente intercambio de mensajes si dicha entrada no se encuentra en la tabla. Una vez en el router este consulta su tabla de encaminamiento enviando el paquete al próximo nodo y así sucesivamente hasta que le paquete llega a un router de la red en la que se encuentre la IP destino. Una vez allí el router se encarga de averiguar la dirección física consultando su tabla ARP o preguntando con mensajes correspondientes.



Lo podemos ubicar en el nivel tres (3) del modelo OSI.

Campos en los datagramas ARP:

- **Hardware protocol** : 16bits. Tecnología de red empleada por debajo de TCP/IP.
- **Network protocol** : 16 bits. Tipo de protocolo empleado a nivel 3.
- **Hardware address length** : 8 bits. Longitud de la dirección de red de hardware.
- **Network address length** : 8 bits. Longitud de la dirección de red IP.
- **Operación** : 16 bits. Tipo de operación que nos da información sobre si se trata de una petición o de una respuesta ARP.
- **Sender hardware address** : 48 bits. Dirección física MAC. de la interfaz de red del emisor.
- **Sender network address** : 32 bits. Dirección IP del emisor.
- **Target hardware address** : 48 bits. Dirección física mace e la interfaz de red del receptor.
- **Target network address** : 32 bits. La dirección IP del receptor.

El Protocolo ICMP

Es utilizado por el protocolo IP para diagnostico y notificación de errores. Su propósito no esta en el transporte de los datos, si no en controlar si un paquete no puede llegar a su destino si su ttl ha expirado, si el encabezamiento lleva un valor no permitido, etc… emitiendo un mensaje de error o control a la fuente que emitio los datos para que evite o corrija el problema detectado..

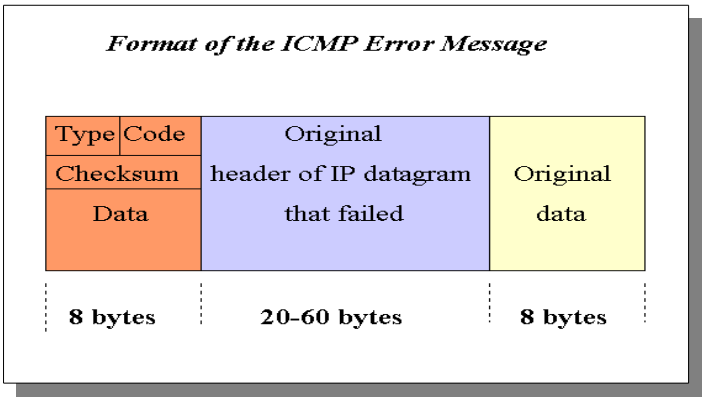
Este protocolo solo es informativo pero no toma decisiones, además estos mensajes icmp son construidos a nivel de la capa de red.

Existen 4 diferentes paquetes icmp.

- **Echo request** : Es el que usa el comando ping para comprobar si existe conectividad entre dos maquinas, petición de eco.
- **Echo replay** : La respuesta al eco request.
- **Timestamp request** : Este ha quedado obsoleto.
- **Information request** : Este ha quedado obsoleto.
- **Address mask request** : No se suelen utilizar a menudo pero a veces pueden resultar bastante utiles.

Lo podemos ubicar en el nivel tres (3) del modelo OSI.

Campos en los datagramas ICMP



- **Type 8 bits** **:** Identifica el tipo especifico de mensaje icmp puede tener 15 valores posibles.
- **Code 8 bits** : Se especifican las condiciones diferentes.
- **Cheksum 16 bits** : Campo de comprobación de integridad para el total del mensaje icmp.
- **Contents** : De longitud variable, depende del tipo de mensaje.

Tabla con el uso de los campos type y code y el mensaje que esta reportando:

Tipo	Codigo	Descripción
0	0	Echo reply
3	0	Network unrecheable
3	1	Host unrecheable
3	2	Protocol unreachable
3	3	Port unreachable
3	4	Fragmentacion deeded

3	5	Source routing failed
3	6	Destination network unknown
3	7	Destination host unknown
3	8	Source host isolated
3	9	Administratively prohibited
3	11	Network unreachable TOS
3	12	Host unreachable TOS
3	13	Prohibited by filtering
3	14	Host violation
3	15	Cutoff in effect
4	0	Source quench
5	0	Redirect for network
5	1	Redirect for host
5	2	Redirect for TOS and network
5	3	Redirect for tos and host
8	0	Echo request
9	0	Router advertisement
10	0	Router solicitation
11	0	TTL equals 0 during transit
11	1	TTL equals 0 during reassembly
12	0	Ip header bad
12	1	Required options missing
13	0	Timestamp request obsolete
14	0	Timestamp reply obsolete
15	0	Information request obsolete
16	0	Information reply obsolete
17	0	Address mask request
18	0	Address mask reply

Telnet

Telnet (Telecommunication Network1) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Funcionamiento

Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero es una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenga. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.

Aparte de estos usos, en general telnet se ha utilizado (y aún hoy se puede utilizar en su variante SSH) para abrir una sesión con una máquina UNIX, de modo que múltiples usuarios con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina. Es una forma muy usual de trabajar con sistemas UNIX.

Problemas de seguridad y SSH

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas. Por esta razón dejó de usarse, casi totalmente, hace unos años, cuando apareció y se popularizó el SSH, que puede describirse como una versión cifrada de telnet -actualmente se puede cifrar toda la comunicación del protocolo durante el establecimiento de sesión (RFC correspondiente, en inglés- si cliente y servidor lo permiten, aunque no se tienen ciertas funcionalidad extra disponibles en SSH).

Manejo básico de telnet

Para iniciar una sesión con un intérprete de comandos de otro ordenador, puede emplear el comando telnet seguido del nombre o la dirección IP de la máquina en la que desea trabajar, por ejemplo si desea conectarse a la máquina servidor.universidad.edu.co deberá teclear :

telnet servidor.universidad.edu.co

y para conectarse con la dirección IP 1.2.3.4 deberá utilizar :

telnet 1.2.3.4.

Una vez conectado, podrá ingresar el nombre de usuario y contraseña remoto para iniciar una sesión en modo texto a modo de consola virtual (ver Lectura Sistema de usuarios y manejo de clave). La información que transmita (incluyendo su clave) no será protegida o cifrada y podría ser vista en otros computadores por los que se transite la información (la captura de estos datos se realiza con un packet sniffer).

Una alternativa más segura para telnet, pero que requiere más recursos del computador, es SSH. Este cifra la información antes de transmitirla, autentica la máquina a la cual se conecta y puede emplear mecanismos de autenticación de usuarios más seguros.

Actualmente hay sitios para hackers en los que se entra por telnet y se van sacando las password para ir pasando de nivel, ese uso de telnet aún es vigente.

Seguridad

Hay 3 razones principales por las que el telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

- Los dominios de uso general del telnet tienen varias vulnerabilidades descubiertas a lo largo de los años, y varias más que podrían aún existir.
- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.
- Telnet carece de un esquema de autentificación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

En ambientes donde es importante la seguridad, por ejemplo en el Internet público, telnet no debe ser utilizado. Las sesiones de telnet no son cifradas. Esto significa que cualquiera que tiene acceso a cualquier router, switch, o gateway localizado en la red entre los dos anfitriones donde se está utilizando telnet puede interceptar los paquetes de telnet que pasan cerca y obtener fácilmente la información de la conexión y de la contraseña (y cualquier otra cosa que se mecanografía) con cualesquiera de varias utilidades comunes como tcpdump y Wireshark.

Estos defectos han causado el abandono y despreciación del protocolo telnet rápidamente, a favor de un protocolo más seguro y más funcional llamado SSH, lanzado en 1995. SSH provee de toda la funcionalidad presente en telnet, la adición del cifrado fuerte para evitar que los datos sensibles tales como contraseñas sean

interceptados, y de la autentificación mediante llave pública, para asegurarse de que el computador remoto es realmente quién dice ser.

Los expertos en seguridad computacional, tal como el instituto de SANS, y los miembros del newsgroup de comp.os.linux.security recomiendan que el uso del telnet para las conexiones remotas debería ser descontinuado bajo cualquier circunstancia normal.

Cuando el telnet fue desarrollado inicialmente en 1969, la mayoría de los usuarios de computadoras en red estaban en los servicios informáticos de instituciones académicas, o en grandes instalaciones de investigación privadas y del gobierno. En este ambiente, la seguridad no era una preocupación y solo se convirtió en una preocupación después de la explosión del ancho de banda de los años 90. Con la subida exponencial del número de gente con el acceso al Internet, y por la extensión, el número de gente que procura crackear los servidores de otra gente, telnet podría no ser recomendado para ser utilizado en redes con conectividad a Internet.

Fuente Wikipedia

Ejemplo enviando un correo :

- telnet mail.server.com 25 El puerto 25 generalmente es el puerto de correo electrónico en la mayoría de los servidores, pero algunos administradores de redes han cambiado ese puerto por otro diferente, como 465 (puerto seguro) o 587 (usuarios de Microsoft Outlook)[3]. Pregúntale a tu administrador cuál es el puerto correcto (o verifícalo en la información de la cuenta).
- HELO tudominio.com
- mail from: tu@servidor.com
- rcpt to: amigo@dominiodetuamigo.com
- Escribe data y presiona ↵ Enter.
- En la siguiente línea, escribe subject: prueba y presiona ↵ Enter dos veces. Reemplaza "prueba" por el asunto que quieras.
- Escribe tu mensaje. Cuando termines, presiona ↵ Enter.
- Escribe un solo un . para finalizar el mensaje. Luego presiona ↵ Enter. Deberá aparecer un mensaje confirmando si el correo se aceptó o se agregó a la cola. Este mensaje varía según el servidor.
- Si ves algún mensaje de error, anótalo y ponte en contacto con tu proveedor de correo electrónico.
- quit