



Construcción de cableado y manejo de redes en S.O.(Documentación)

1.-Objetivos:

El objetivo de esta experiencia es la de proporcionar al alumno la capacidad de construcción de cableado básico para redes LAN, así como, el manejo de los comandos adecuados para la configuración de el hardware, protocolos y software asociado a redes de computadoras en los sistemas operativos Linux y Windows

2.-Prerrequisitos :

Esta experiencia requiere del alumno un conocimiento básico de redes de computadores, obtenido en el ramo de Redes de Computadores (ELO-321). Además presume un conocimiento de sistemas Operativos Linux-Unix aportado por el ramo de Sistemas Operativos.

3.-Material para utilizar:

Estaciones de trabajo Windows-Linux.
Herramienta de presión RJ-45
Cable de red categoría 5
Conectores RJ-45 machos

4.-Conceptos básicos:

4.1 Construcción de Patch Cord.

4.1.1 Estándar regulador:

El estándar ANSI/EIA/TIA-568-A es el documento principal que regula todo lo concerniente a sistemas de cableado estructurado para edificios comerciales y el que nos ocupara por su competencia en esta experiencia.

El objetivo de la norma se describe en el mismo documento de la siguiente forma:

"Esta norma especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante. También proporciona directivas para el diseño de productos de telecomunicaciones para empresas comerciales.

El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la construcción o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado."

Alcance

La norma EIA/TIA 568-A especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. En ella se hacen recomendaciones para:

- ☞ Las topología
- ☞ La distancia máxima de los cables
- ☞ El rendimiento de los componentes
- ☞ Las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Las aplicaciones que emplean el sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

- ☞ Voz
- ☞ Datos
- ☞ Texto
- ☞ Video
- ☞ Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.

4.1.2 Descripción de materiales:

4.1.2.1 Cable UTP (par trenzado sin blindar) :

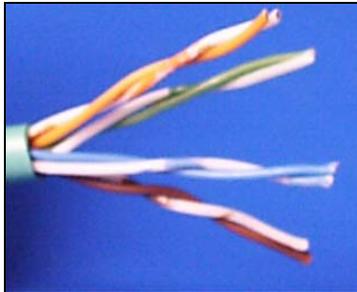


Figura 1. Cable UTP

Es el soporte físico más utilizado en las redes LAN, pues es barato y su instalación es barata y sencilla. Consiste en un conjunto de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la diafonía(interferencia respecto a los pares más cercanos). Un cable de par trenzado puede tener pocos o muchos pares; en aplicaciones de datos lo normal es que tengan 4 pares. Uno de sus inconvenientes es la alta sensibilidad que presenta ante interferencias electromagnéticas.

El cable UTP se clasifica según su categoría. Este cable UTP permite la transmisión de grandes volúmenes de información. Estas propiedades están dadas por varios factores: el cobre con que está fabricado el conductor, el material de recubrimiento, tanto de cada conductor como del cable total y finalmente en trenzado de cada par. Estas características hacen que el cable no requiera de blindaje para mantener la señal limpia y estable.

Categorías del cable UTP

Una categoría de cableado es un conjunto de parámetros de transmisión que garantizan un ancho de banda determinado en un canal de comunicaciones de cable de par trenzado. Las categorías de cableado definen el estándar que debe cumplirse en la construcción end to end del cableado estructurado.

A continuación se explicara las categorías de cableado estructurado pero referidas al cable de par trenzado utilizado en cada una de estas, las categorías son:

Categoría 1

La primera categoría responde al cable UTP Categoría 1, especialmente diseñado para redes telefónicas, el clásico cable empleado en teléfonos y dentro de las compañías telefónicas.

Categoría 2

El cable UTP Categoría 2 es también empleado para transmisión de voz y datos hasta 4Mbps

Categoría 3

La categoría 3 define los parámetros de transmisión hasta 16 MHz. Entre las principales aplicaciones de los cables de categoría 3 encontramos: voz, Ethernet 10Base-T y Token Ring. El largo máximo que puede alcanzar un tramo sin considerar los patch cord (chicotes) según el norma dictada por el EIA/TIA es de 90 metros, o sea, 90 metros desde el punto de la pared a el patch panel.

Categoría 4

El cable UTP Categoría 4 tiene la capacidad de soportar comunicaciones en redes de computadoras a velocidades de 20Mbps. El largo máximo al igual y bajo las mismas premisa que la categoría 3 es de 90 metros.

Categoría 5

El cable UTP categoría 5, es el más usado hoy en día en redes LAN, con la capacidad de sostener comunicaciones a 100Mbps, será en este en el que se hará mayor hincapié por ser el que se utilizará en el laboratorio.

La categoría 5 define los parámetros de transmisión hasta 100 MHz. Inicialmente, la categoría 5 sólo definía atenuación y NEXT como parámetros importantes en la medición de las características del canal. A raíz de los trabajos en Gigabit Ethernet se agregaron nuevos parámetros a la definición de esta categoría puesto que había que garantizar una transmisión por los cuatro pares de manera simultánea en ambas direcciones(full duplex).

Entre las principales aplicaciones de los cables de categoría 5 encontramos: voz, Ethernet 10Base-T, Token Ring, 100VG AnyLan, Fast Ethernet 100Base-TX, ATM 155 Mbps, ATM 622 Mbps y Gigabit Ethernet.

Parámetro de transmisión	Valor para el canal a 100 MHz
Atenuación	24 dB
NEXT	27.1 dB
Wiremap	N.A.
Length	90mtrs.

Tabla 1. Valores limites para las pruebas de certificación en categoría 5.

Categoría 5 mejorada(5E)

La categoría 5 enhance define los parámetros de transmisión hasta 100 MHz. La diferencia fundamental con la categoría 5 normal es el agregar nuevas pruebas de certificación de manera de asegurar el soporte directo de la tecnología Gigabit Ethernet. Estas nuevas pruebas son PowerSum NEXT (PSNEXT), PowerSum ELFEXT, PowerSum ACR, Return Loss, Delay y Delay Skew.

Entre las principales aplicaciones de los cables de categoría 5 mejorada encontramos: voz, Ethernet 10Base-T, Token Ring, 100VG AnyLan, Fast Ethernet 100Base-TX, ATM 155 Mbps, ATM 622 Mbps y Gigabit Ethernet.

Parámetro de transmisión	Valor para el canal a 100 MHz
Atenuación	24.0 dB
NEXT	30.1 dB
PSNEXT	27.1 dB
ACR	6.1 dB
PSACR	3.1 dB
ELFEXT	17.4 dB
PSELFEXT	14.4 dB
Return Loss	10.0 dB
Delay	548 n.s.
Delay Skew	50 n.s.

Tabla 2. Valores limites para las pruebas de certificación en categoría 5E.

Estos valores fueron publicados como la adición 5 de la norma TIA/EIA-568A.

Categoría 6

La categoría 6 ha sido liberada el reciente mes de junio del 2002 y define como pruebas de certificación las mismas que la categoría 5E pero siendo más estricta en sus valor limites, además por una petición de la IEEE las pruebas de aumentaron de 200Mhz que era la tasa de transmisión original a 250Mhz.

La categoría es tan estricta en sus pruebas que aun no hay soluciones para la construcción personal de patch cord los cuales solos pueden ser fabricados en laboratorios (fabricas) especializadas.

Categoría 7

La categoría 7 utiliza en su instalación cable par trenzado blindado, o sea, blindado esta categoría no es utilizada en sur y norte América si no más bien en Europa por lo cual no haremos mayor hincapié en ella.

Estructura del cable UTP

El cable UTP para redes actualmente usado es el de 8 hilos categoría 5, es decir cuatro partes trenzados formando una sola unidad. Estos cuatro pares vienen recubiertos por una tubo plástico que mantiene el grupo unido, mejorando la resistencia ante interferencias externas. Es importante notar que cada uno de los cuatro pares tiene un color diferente, pero a su vez, cada par tiene un cable de un color específico y otro blanco con algunas franjas del color de su par. Esta disposición de los cables permite una adecuada y fácil identificación de los mismos con el objeto de proceder a su instalación.

La norma define también el número identificador de cada par referente a su color como se muestra a continuación.

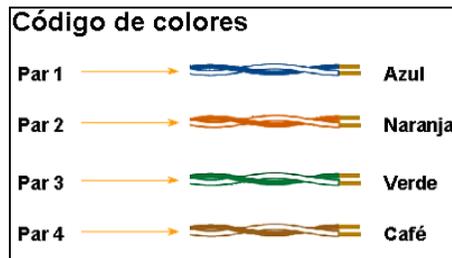


Figura 2. Código de colores.

Características del cable UTP:

Las características generales del cable no blindado son:

- ☞ **Tamaño:** El menor diámetro de los cables de par trenzado no blindado permite aprovechar más eficientemente las canalizaciones y los armarios de distribución
- ☞ **Peso:** El poco peso de este tipo de cable con respecto a los otros tipos de cable facilita el tendido.
- ☞ **Flexibilidad:** La facilidad para curvar y doblar este tipo de cables permite un tendido más rápido así como el conexionado de las rosetas y las regletas. El radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable. Para par trenzado de cuatro pares categoría 5 el radio mínimo de doblado es de 2.5 cm.
- ☞ **Impedancia característica:** La impedancia característica es igual 100 ohms + 15 % desde 1 Mhz hasta la frecuencia más elevada referida (16, 20 ó 100 Mhz). De una categoría particular.
- ☞ **Instalación:** Debido a la amplia difusión de este tipo de cables, existen una gran variedad de suministradores, instaladores y herramientas que abaratan la instalación y puesta en marcha.
- ☞ **Integración:** Los servicios soportados por este tipo de cable incluyen:
 - Red de Area Local ISO 8802.3 (Ethernet) y ISO 8802.5 (Token Ring)
 - Telefonía analógica
 - Telefonía digital
 - Terminales síncronos
 - Terminales asíncronos
 - Líneas de control y alarmas

- 🔗 **Facilidad de Uso:** Este cable viene marcado con números que representan la distancia en pies de cada tramo en forma correlativa con lo que se puede saber la longitud utilizada y la distancia que aun queda disponible en la caja con solo registrar estos números y realizar una simple resta.

Manejo del cable

El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm. para cables UTP categoría 5.

Para la construcción de patch cord se establece en la norma una distancia máxima de 3 metros en el cable UTP incluidos los conectores.

4.1.2.2 Conector RJ-45 (Plug 8P8C):

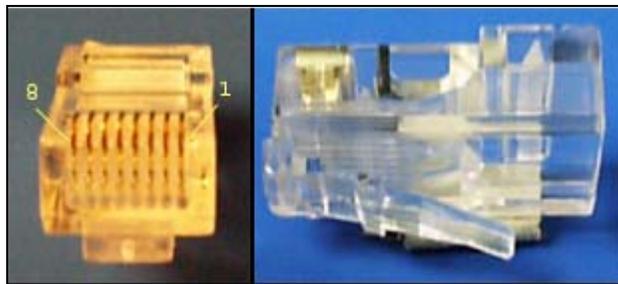


Figura 3. Plug RJ-45

Este conector es el que ha brindado un gran empuje a estas redes, pues es muy sencillo conectarlo a las tarjetas y a los hubs, además es seguro gracias a un mecanismo de enganche que posee, mismo que lo firmemente ajustado a otros dispositivos, no como en el cable coaxial donde permanentemente se presentan fallas en la conexión.

La figura muestra el conector RJ-45, con 8 contactos para los 8 hilos del cable UTP, tanto de perfil como una vista superior.

Un aspecto general a toda instalación de este tipo de cableado es que todos los elementos deben corresponder a la categoría 5, ya que esto asegura de que todos los elementos del cableado pueden soportar las mismas velocidades de transmisión, resistencia eléctrica, etc. El conector en este caso no es la excepción.



Figura 4. Terminal de Patch Cord.

Códigos de conexión para las tomas de información o jacks RJ 45

La norma EIA/TIA 568 especifica dos configuraciones de conexión para el cable UTP de 4 pares los códigos de conexión 568 A y 568 B las diferencias básicas entre uno y otro radican en que en el 568 A el par #2 del cable (naranja) termina en los contactos 3 y 6 y el par #3 del cable (verde) en los contactos 1 y 2 mientras que el 568 B solo intercambia estos dos pares. El par #1 y #4 no varían de una configuración a otra.

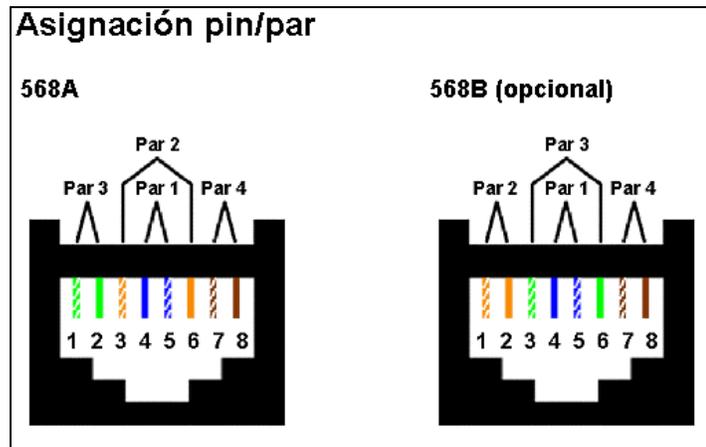


Figura 5. Diagrama de asignación de pares a pines.

4.1.2.3 Herramienta de presión RJ-45: llamada también herramienta de crimpear, permite cortar y pelar el cable, además, de apretar el conector para fijar los hilos del cable UTP a los contactos.

Por supuesto no hace falta pelar los cables. El conector se introduce en una ranura especial que posee un alicate fabricado precisamente para estos efectos.

Al imprimir presión sobre el alicate, este mecánicamente produce que los contactos del conector RJ-45 se aseguren firmemente contra cada uno de los cables en su interior.



Figura 6. Herramienta de presión.

4.1.3 Construcción del patch cord.

Antes de comenzar a trabajar asegúrese de tener a mano todos los elementos que necesitará.

☞ **Paso 1.**

Mida y corte un trozo de cable para la construcción de su patch cord



Figura 7. Construcción de Patch Cord paso 1.

☞ **Paso 2.**

Corte la cubierta protectora de manera de liberar los pares trenzados, lo suficiente para poder trabajar sin problemas.

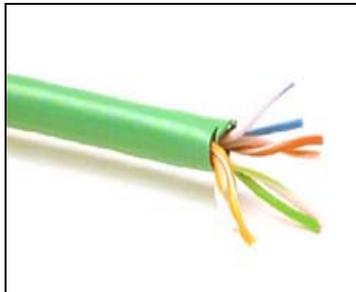


Figura 8. Construcción de Patch Cord paso 2.

☞ **Paso 3.**

Desarme el trenzado de los pares de manera de luego poder ordenarlos.

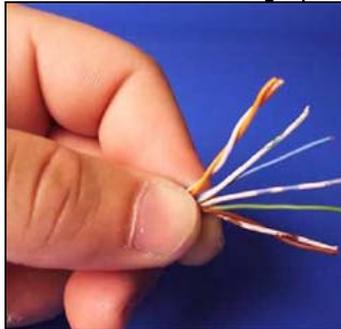


Figura 9. Construcción de Patch Cord paso 3.

🔧 **Paso 4**

Ordene los pares según la configuración elegida EIA/TIA, 568-A o 568-B.

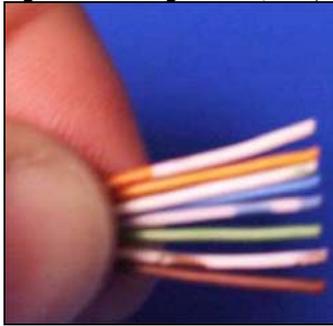


Figura 10. Construcción de Patch Cord paso 4.

🔧 **Paso 5**

Pruebe el largo de los cables insertándolos en el conector RJ-45 de manera de medir para cortar si es necesario, de manera que se cumpla la norma.

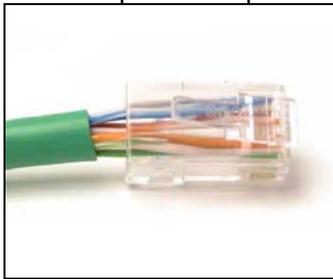


Figura 11. Construcción de Patch Cord paso 5.

🔧 **Paso 6**

Corte de manera que la cubierta del cable quede justo en la banda que lo presiona en el conector.

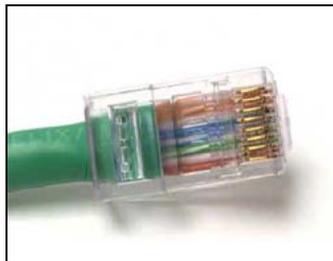


Figura 12. Construcción de Patch Cord paso 6.

🔧 **Paso 7**

Verifique que cada uno de los pares hayan sido introducidos de manera correcta a los conectores. Utilice la herramienta de presión para fijar el cable a el conector.



Figura 13. Construcción de Patch Cord paso 7.

🔧 **Paso 8**

Verifique la transmisión del cable con algún Aparato de testeo o certificador.



Figura 14. Construcción de Patch Cord paso 8.

4.2 Sistema Operativo Microsoft Windows.

4.2.1 Protocolo TCP-IP

4.2.1.1 Instalación del protocolo TCP/IP

Para poder instalar el protocolo TCP-IP siga los siguientes pasos:

1. En el menú Inicio seleccione Configuración y  Panel de control.
2. Dentro del Panel de control seleccione el icono  Red
3. Si la tarjeta de red ha sido correctamente instalada en la ventana de diálogo aparecerán los elementos  Cliente para redes Microsoft y el icono del  adaptador de red del que disponga.
4. Haga clic en el botón Agregar.
5. Seleccione la opción  Protocolo.
6. Seleccione Fabricante: Microsoft y Protocolo de red:  TCP/IP.
7. Inserte el disco de instalación de Windows 98 si es necesario.
8. Haga clic en Aceptar para terminar.

A final del proceso aparecerán tantos iconos de  TCP/IP como dispositivos capaces de soportarlo tenga instalados en la maquina. Por ejemplo, si el ordenador dispone de un módem y una tarjeta de red en la ventana aparecerán los iconos TCP/IP->Adaptador de acceso telefónico y TCP/IP-> (Su adaptador de red).

En otro caso sólo aparecería uno correspondiente al adaptador de red.

4.2.1.2 Configuración del protocolo TCP/IP

Una vez instalado el protocolo TCP/IP siga estos pasos para configurar sus parámetros de funcionamiento(IP, DNS, GATEWAY):

1. Si no está abierto, seleccione el icono  Red en el Panel de control.
2. En la ventana de diálogo seleccione el icono del protocolo  TCP/IP. Si hay más de uno seleccione el correspondiente al adaptador de red.
3. Haga clic en Propiedades. Aparecerá una ventana de diálogo con varias etiquetas
4. En la etiqueta Dirección IP active la opción Especificar una dirección IP.
5. En el recuadro Dirección IP introduzca la dirección, por ejemplo, 192.168.1.2.
6. Introduzca el valor correspondiente en Máscara de subred, por ejemplo 255.255.255.192
7. Haga clic en Aceptar.

4.2.1.3 Comprobación

Una vez instalado el protocolo en el cliente se puede comprobar el correcto funcionamiento de la red de la siguiente manera:

- 1.La primera prueba a realizar es ejecutar el comando Ping con su dirección IP como parámetro, una respuesta afirmativa le asegurara que su dispositivo esta correctamente configurado, por lo fallas de comunicación pueden ser atribuidas a otras partes de la red.

2. Al abrir el icono Entorno de Red en el escritorio aparecerán los nombres de los demás ordenadores conectados.

3. Compruebe si otras maquinas son accesibles mediante el comando PING.

Asociando un nombre a su IP

1. Editar el archivo hosts.sam que está en el directorio de Windows
2. Al final del archivo incorporar la dirección IP y el nombre del computador.
3. Asegurarse de que la dirección IP y el nombre coinciden con la dirección IP que se ha fijado en la configuración antes hecha.
4. Salvar el archivo con el nombre "hosts" (sin extensión) y reiniciar Windows '98

El sistema Windows98 provee la funcionalidad de reiniciar el sistema sin necesariamente reiniciar la máquina esto se logra manteniendo presionada la tecla Shift mientras se rebootea el computador, seleccionando reiniciar en la pantalla de salida, NO soltar la tecla Shift hasta que aparezca el mensaje "**Windows se esta reiniciando**".

Comprobación de la red

1. Abrir una sesión MS-DOS
2. Teclear "ping 'nombre del computador' "
3. Debería aparecer:

```
Pinging maquina [su_IP] with 32 bytes of data:  
Reply from su_IP: bytes=32 time=1ms TTL=32  
Reply from su_IP: bytes=32 time<10ms TTL=32  
Reply from su_IP: bytes=32 time<10ms TTL=32  
Reply from su_IP: bytes=32 time<10ms TTL=32
```

4. Teclear "tracert su_IP "
5. Debería aparecer:

```
Tracing route to su_IP over a maximum of 30 hops
```

```
1 <10 ms 1 ms <10 ms su_IP
```

```
Trace complete.
```

Si la respuesta a los comandos ha sido como se esperaba , el computador se encontrara en condiciones de funcionar como si estuviera en red.

Problemas más frecuentes

Los tres problemas más comunes que se pueden presentarse cuando intentemos comprobar el funcionamiento correcto de la red interna son:

Cuando hacemos "ping" obtenemos "Bad IP address 'nombre del computador' "

Intentar teclear "ping Su_Ip". Si ahora sí se obtiene respuesta, la causa del problema es que el archivo de host ha quedado mal configurado, para esto debe probar si la IP asociada al nombre es la correcta.

El programa cliente o el servidor fallan al intentar el "connect"

La causa podría estar en que se produzca un fallo por archivo no encontrado en el directorio Windows/System de las librerías WINSOCK.DLL o WSOCK32.DLL. Muchos programas que se utilizan en Internet reemplazan estos ficheros cuando se instalan. Asegurarse de que están estos ficheros y que son los originales que vienen con la distribución de Windows '98.

El programa servidor dice que no puede "bind" a un socket

Esto sucede porque tiene el DNS activado y no puede encontrar ese DNS o servidor de direcciones.

4.2.2 Comandos de Red Windows.

4.2.2.1 Ipconfig muestra la configuración de los dispositivos de red instalados en el sistema. Comando equivalente en linux "*Ifconfig*".

Modo de uso: *ipconfig [opciones]*

Opciones:

/ALL	Muestra información detallada.
/Batch [archivo]	Escribe en el archivo o en winipcfg.out.
/renew_all	Renueva la información de todos los adaptadores.
/release_all	Libera todos los adaptadores.
/renew N	Renueva el adaptador N.
/release N	Libera el adaptador N.
-h	Muestra la ayuda del comando.

Tabla 3. Opciones de ipconfig.

```

Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\>ipconfig

Configuración IP de Windows 2000

Ethernet adaptador Conexión de área local:

    Sufijo DNS específico de la conexión. :
    Dirección IP. . . . . : 192.168.1.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . :

Ethernet adaptador Conexión de área local 2:

    Sufijo DNS específico de la conexión. : vtr.net
    Dirección IP. . . . . : 200.83.223.86
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . : 200.83.220.1

C:\>_
  
```

Figura 15. Salida del comando Ipconfig.

Este comando tiene un equivalente grafico que puede ser visto en windows llamado "winipcfg"



Figura 16. Formato del programa winipcfg.

4.2.2.2 Tracert este comando permite trazar la ruta entre la computadora de ejecución y una de destino basado sobre 30 saltos máximo. Su funcionamiento se basa en el envío de mensajes ICMP. Su equivalente en Linux es el comando "*traceroute*"

Modo de uso: `tracert [-d] [-h máximo_de_saltos] [-j lista_de_hosts] [-w tiempo_de_espera] nombre_de_destino`

Opciones:

-d	No convierte direcciones en nombres de host.
-h número de saltos	Máximo cantidad de saltos en la búsqueda del objetivo.
-j lista de host	Enrutamiento relajado de origen en la lista de hosts.
-w tiempo de espera	Tiempo en milisegundos entre intentos.

```

Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\>tracert www.elo.utfsm.cl

Traza a la dirección vega.elo.utfsm.cl [200.1.17.31]
sobre un máximo de 30 saltos:

 1  10 ms  <10 ms  <10 ms  10.12.0.1
 2  10 ms   10 ms   10 ms  192.168.211.164
 3  10 ms   10 ms   10 ms  192.168.217.11
 4  <10 ms  10 ms   10 ms  192.168.217.33
 5  10 ms   10 ms   10 ms  fe-8-1-1-24.border2.telefoniamundo.cl [200.10.2
24.217]
 6  10 ms   10 ms   20 ms  customergw.reuna.cl [200.10.224.254]
 7  10 ms   10 ms   20 ms  ra-utfsm.reuna.cl [146.83.240.7]
 8  ra-utfsm.reuna.cl [146.83.240.7]  informes: Red de destino inaccesible.

Traza completa.

C:\>_

```

Figura 17. Salida del comando tracert.

4.2.2.3 Netstat permite visualizar estados de las conexiones, protocolos (rutas, estados de puertos , estadísticas) . Su equivalente en Linux es el comando "*netstat*"

Modo de uso: *netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]*

Opciones:

-a	Muestra todas las conexiones y puertos en estado listen.
-e	Muestra estadísticas Ethernet. Se puede combinar con -s.
-n	Muestra números de puertos y direcciones en formato numérico.
-s	Muestra estadísticas por protocolo. En forma predeterminada, se muestran para TCP, UDP e IP; se puede utilizar la opción -p para especificar un subconjunto de lo predeterminado.
-p proto	Muestra conexiones del protocolo especificado por proto; que puede ser tcp o udp. Si se usa con la opción -s para mostrar estadísticas por protocolo, proto puede ser TCP, UDP o IP.
-r	Muestra el contenido de la tabla de rutas.
intervalo	Vuelve a mostrar las estadísticas seleccionadas, haciendo pausas en el intervalo de segundos especificado entre cada muestra. Presione Ctrl+C para detener la actualización de estadísticas. Si se omite, netstat imprimirá la actual información de configuración una vez.
-h	Muestra la ayuda del comando.

Tabla 4. Opciones de netstat.

```

Seleccionar C:\WINNT\System32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\>netstat -r

Tabla de caminos
=====
Lista de interfaces
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 e0 7d 82 e4 ca ..... Realtek RTL8029(AS) Ethernet Adapt
0x3 ...00 80 ad e0 86 8b ..... Novell 2000 Adapter.
=====

Rutas activas:
Destino de red      Máscara de red   Puerta de acceso  Interfaz  Métrica
0.0.0.0             0.0.0.0         200.83.220.1     200.83.223.86  1
127.0.0.0          255.0.0.0       127.0.0.1        127.0.0.1      1
192.168.1.0        255.255.255.0   192.168.1.1     192.168.1.1    1
192.168.1.1        255.255.255.255 127.0.0.1        127.0.0.1      1
192.168.1.255     255.255.255.255 192.168.1.1     192.168.1.1    1
200.83.220.0       255.255.252.0   200.83.223.86   200.83.223.86  1
200.83.223.86     255.255.255.255 127.0.0.1        127.0.0.1      1
200.83.223.255    255.255.255.255 200.83.223.86   200.83.223.86  1
224.0.0.0          224.0.0.0       192.168.1.1     192.168.1.1    1
224.0.0.0          224.0.0.0       200.83.223.86   200.83.223.86  1
255.255.255.255   255.255.255.255 200.83.223.86   200.83.223.86  1
Puerta de enlace predeterminada: 200.83.220.1
=====

Rutas persistentes:
ninguno

C:\>

```

Figura 18. Salida del comando netstat -r.

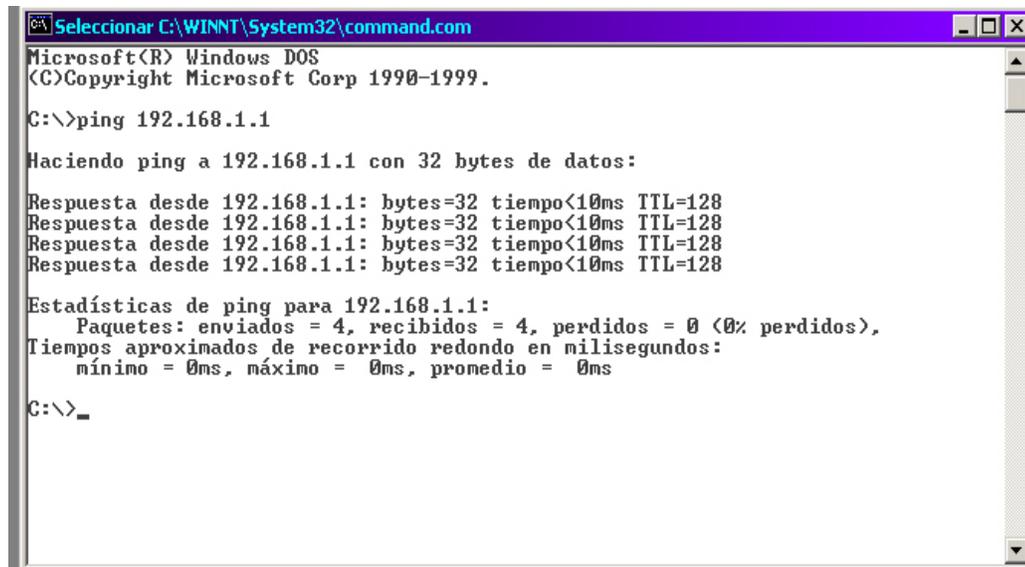
4.2.2.4 Ping este comando envia mensajes ICMP del tipo Echo_request y recibe mensajes Echo_response en respuesta. La información obtenida nos permitirá determinar el retardo entre la maquina de origen y destino. Su equivalente en Linux posee el mismo nombre.

Modo de uso: ping [-t] [-a] [-n cantidad] [-l tamaño] [-f] [-i TTL] [-v TOS] [-r cantidad] [-s cantidad] [[-j lista de host] | [-k lista de host]] [-w Tiempo de espera agotado] [-c contenido] lista de destino

Opciones:

-t	Solicita eco al host hasta ser interrumpido. Para ver estadísticas y continuar: presione <input type="checkbox"/> olic-Inter. Para interrumpir: presione <input type="checkbox"/> olic-C.
-a	Resuelve direcciones a nombres de host.
-n cantidad	Cantidad de <input type="checkbox"/> olicitudes de eco a enviar.
-l tamaño	Tamaño del búfer de envíos.
-f	No fragmentar el paquete.
-i TTL	Tiempo de vida.
-v TOS	Tipo de servicio.
-r cantidad	Registrar la ruta para esta cantidad de saltos.
-s cantidad	Registrar horarios para esta cantidad de saltos.
-j lista de host	Ruta origen variable en la lista de host.
-k lista de host	Ruta origen estricta en la lista de host.
-w Tiempo	Tiempo de espera agotado de respuesta en milisegundos.
-c contenido	Permite setear el contenido del paquete ICMP

Tabla 5. Opciones de Ping.



```
Seleccionar C:\WINNT\System32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

C:\>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta desde 192.168.1.1: bytes=32 tiempo<10ms TTL=128

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de recorrido redondo en milisegundos:
        mínimo = 0ms, máximo = 0ms, promedio = 0ms

C:\>_
```

Figura 19. Salida del comando Ping 127.0.0.1.

4.2.3 Archivos en windows.

4.2.3.1 Host.sam

El fichero host.sam sirve para la traducción de nombres a IP y viceversa de manera de poder ocupar estos atajos en la ejecución de comandos.

Una vez realizadas las entradas a este archivo debe ser renombrado a hosts y rebootear la maquina de manera que la configuración sea actualizada.

El fichero símil de este en plataformas linux es /etc/hosts.

A continuación se muestra el formato contenido por este archivo:

```
# Copyright (c) 1998 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP stack for Windows98
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com              # x client host

127.0.0.1        localhost
194.165.23.15   mimaquina          www.labredes.cl
```

Figura 20. Contenido de archivo hosts

4.3 Sistema Operativo Linux.

4.3.1 Archivos importantes para el manejo de redes:

4.3.1.1 /etc/protocols

El sistema de red de unix utiliza un número especial, denominado número de protocolo, para identificar el protocolo de transporte específico que la máquina recibe; esto permite al software de red decodificar correctamente la información recibida. En este archivo se pueden encontrar todos los protocolos de transporte reconocidos junto a su número de protocolo y sus alias.

Ej.

```
Ip      0      IP      #internet protocol, pseudo protocol number
Icmp    1      ICMP    #internet control message protocol
```

En forma normal este fichero no necesita ni debe ser editado, ya que el el software de red el que se encarga de administrarlo.

4.3.1.2 /etc/services

Este fichero contiene el nombre, número de puerto, protocolo utilizado y alias de todos los servicios de red existentes.

Ej.

```
Smtplib 25/tcp      mail
```

Este fichero es utilizado por los servidores y por los clientes para obtener el número de puerto en el que deben escuchar o al que se deben enviar las peticiones, de esta forma se puede cambiar un número de puerto sin afectar las aplicaciones que funcionan con él.

Se hace hincapié en no caer en el error de creer que al modificar este fichero se pueden habilitar o deshabilitar servicios de una máquina.

4.3.1.3 /etc/hosts

Este fichero se utiliza para establecer una relación entre un nombre de máquina y una dirección IP; en cada línea de /etc/hosts se especifica una dirección IP y los nombres de máquina que le corresponden. Normalmente se incluyen las direcciones y alias de los equipos pertenecientes a la red local de manera que la máquina no deba consultar al DNS. El formato de las líneas de este archivos es el siguiente:

```
IP      nombre      alias1      alias2
```

Ej.

```
192.168.1.2  juan  www.labredes.cl  labredes.
```

Una vez configurado este archivo no será necesario recordar la IP de una máquina si no tan solo su nombre o uno de sus alias.

4.3.1.4 /etc/ethers

Este fichero establece una correspondencia entre nombre de máquinas y sus direcciones ethernet (dirección MAC de la tarjeta). El formato de las líneas de este archivo es el siguiente:

```
Dirección ethernet      nombre máquina.
```

Ej.

```
02:AF:5C:23:00:C2      labredesPC1
```

este fichero aunque en desuso es interpretado por el sistema, no es usado hoy en día ya que las direcciones de hardware se obtienen por ARP.

4.3.1.6 /etc/inetd.conf

Este es el archivo de configuración del demonio inetd, conocido como el superservidor de red. Su correcta configuración es importante ya que es el demonio inetd el encargado de ofrecer la mayoría de los servicios de nuestra máquina. Cada línea del archivo (excepto los comentarios) le indica a inetd cómo se ha de comportar cuando recibe una petición en cierto puerto; en cada una de ellas existe al menos 6 campos cuyo significado es el siguiente:

- ☞ Servicio
Este campo indica el nombre del servicio asociado a la línea correspondiente, se hace notar que este servicio debe estar registrado en /etc/services.
- ☞ Socket
Aquí se indica el tipo de socket asociado a la conexión (EJ. TCP stream, UDP dgram).
- ☞ Protocolo
Aquí se define el protocolo asociado, el cual debe ser un protocolo definido en /etc/protocols.
- ☞ Concurrencia
Este campo es solo aplicable a sockets del tipo datagrama, aquí se especifica la forma en que se atenderá este servicio, liberando el socket cada vez para poder recibir peticiones intermedias (valor nowait) o no liberando el socket sino que esperando a que finalice la entrega (valor wait), en caso de no ser aplicable el campo toma un valor nowait.
- ☞ Usuario
Este campo indica el nombre de usuario bajo el cual se ha de ejecutar el programa que atiende el servicio.
- ☞ Programa
Por último en este campo se ha de indicar la ruta del programa encargado de servir cada petición que inetd recibe en un puerto determinado.

Ej.
telnet stream tcp nowait root /usr/sbin/in.telnetd

4.3.1.7 /etc/networks

Este fichero permite asignar un nombre simbólico a las redes, de forma similar a lo que /etc/hosts hace con las máquinas. En cada línea se especifica un nombre de red, su dirección y sus alias.

Ej.
Loopback 127.0.0.0

Cada día mas en desuso este fichero ha sido reemplazado por el uso de DNS.

4.3.2 Comandos de Red Linux.

4.3.2.1 Hostname

Muestra o setea el nombre de la máquina, este programa es usado por muchos programas de red para identificar la máquina.

Modo de uso: `hostname [-d] [-F nombre_archivo] [-f] [-h] [-s] [-v]`

Opciones:

-d	Muestra el nombre del dominio DNS.
-F nombre_archivo	Lee el nombre de máquina desde nombre_archivo.
-f	Muestra el FQDN. Un FQDN consiste de un nombre de máquina corto y el nombre del dominio DNS.
-h	Muestra la ayuda del comando.
-s	Muestra el nombre corto de la máquina.
-v	Muestra la información de versión y finaliza.

Tabla 6. Opciones de hostname.

4.3.2.2 Ifconfig

Configura una interfase de red. Si el comando es llamado sin parámetros entonces mostrara el estado actual de la configuración de las interfaces de red instalados.

Modo de uso: `ifconfig [interface]`
`ifconfig interface [atype] option | address`

Opciones:

Interface	El nombre de la interfase de red. Ej.eth0.
Up	El uso de este flag causa que la interfase sea activada.
Down	El uso de este flag causa que el driver para esta interfase sea desactivado.
[-]arp	Habilita o deshabilita el uso del protocolo ARP en esta interfase.
[-]allmulti	Habilita o deshabilita el modo promiscuo en esta interfase.
Mtu N	Este parámetro setea el valor del MTU para la interfase.
Netmask addr	Setea la mascara de red para esta interfase.
[-]broadcast [addr]	Setea la dirección broadcast para esta interfase.
Hw	Setea la dirección de hardware para este dispositivo, siempre y cuando el driver del dispositivo lo permita.
address	Setea la dirección IP asociada a esta interfase.

Tabla 7. Opciones de ifconfig.

4.3.2.3 Ping

El comando ping se utiliza normalmente para testar el aspectos de red, como comprobar que un sistema este encendido y conectado. Si bien pareciera un comando inofensivo puede ser utilizado como un arma efectiva de ataque a sistemas informaticos.

Modo de uso: `ping [-r] [-v] host [tamaño_paquete] [count]`

Opciones:

-r	Salta las tablas de ruteo normales y envia directamente a un host de una red local, si el host no esta en una red local un error es retornado.
-v	Modo verbose.

Tabla 8. Opciones de ping.

4.3.2.4 Netstat

Esta orden se utiliza para visualizar el estado de diversas estructuras de datos del sistema de red, desde las tablas de ruteo hasta el estadode todas las conexiones a y desde nuestra máquina, pasando por las tablas ARP, en función de los parámetros que reciba.

Modo de uso: `netstat [[-a | [-t | -u | -w]] [-n | -o] | -x [-c]`
`netstat -a [-c] [-n]`
`netstat -v`

Opciones:

-a	Muestra información de todos los sockets, incluyendo aquellos que solo están escuchando.
-c	Genera una lista continua del estado de la red.
-n	Causa que el comando no resuelva los hostname y servicios cuando muestra información de puertos y direcciones locales y remotas.
-o	Muestra el estado de los contadores, tiempos de expiración.
-r	Muestra la tabla de ruteo del kernel.
-t	Muestra la información solo de los sockets TCP, incluyendo los de estado listen.
-u	Muestra la información solo de los sockets UDP.
-v	Muestra la información de versión.
-w	Muestra la información de los sockets RAW.
-x	Muestra información sobre los sockets del dominio Unix.

Tabla 9. Opciones de netstat.

Significado de la información de estados de conexión mostrada por netstat.

FREE	El socket no esta ocupado.
LISTENING	El socket esta escuchando por una petición.
UNCONNECTED	El socket no esta conectado a otro.
CONNECTING	El socket esta estableciendo una conexión
DISCONNECTING	El socket esta desconectado.
UNKNOW	Este estado no debería aparecer nunca.

Tabla 10. Estados de conexión.

4.3.2.5 arp

Este comando permite gestionar las tablas de conversiones de direcciones ARP

Modo de uso: `arp [-v] [-t type] -a [hostname]`
`arp [-v] -d hostname ...`
`arp [-v] [-t type] -s hostname hw_addr`
`arp [-v] -f filename`

Opciones:

-v	Setea al comando a modo verbose.
-t type	Al setear o leer el cache ARP este parámetro le dice que tipo de entradas deberán ser chequeadas.
-a [hostname]	Muestra las entradas del hostname específico.
-d [hostname]	Borra las entradas del hostname específico.
-s hostname hw_addr	Crea una entrada al cache de forma manual asociando hostname con hw_addr.
-f filename	Identico a -s más los valores son tomados desde filename.

Tabla 11. Opciones de Arp.

4.3.2.6 Traceroute

Este comando es utilizado para imprimir la ruta que los paquetes siguen desde la máquina de ejecución a otra de destino; para ello utiliza el campo TTL del protocolo IP, inicializándolo con valores bajos y aumentándolo conforme va recibiendo tramas ICMP de tipo TIME_EXCEEDED. Un aspecto negativo del comando es la excesiva carga que impone en el sistema.

Modo de uso: `traceroute [-m max_ttl] [-p port] [-q nqueries]`
`[-r] [-s src_addr] [-t tos] [-w waittime] host [packetsize]`

Opciones:

-m max_ttl	Setea el maximo ttl usado por los paquetes de prueba salientes. El valor por defecto es de 30.
-p port	Setea el numero del puerto usado en las pruebas, por defecto es el puerto 333434
-q nqueries	Setea el numero de pruebas por ttl a nqueries, el valor por defecto es 3.
-r	Salta las tablas de ruteo normales y envía el paquete directamente a un host en la red local.
-s src_addr	Usa la siguiente Ip como dirección de fuente en los paquetes de prueba de salida.
-t tos	Setea el tipo de servicio en los paquetes de prueba a el siguiente valor el cual puede ser un entero entre 0 y 255, el valor por defecto es 0.
-v	Setea el comando a modo verbose.
-w	Setea el tiempo(en segundos) que se espera por una respuesta a una prueba, el valor por defecto es de 3 segundos.

Tabla 12. Opciones de traceroute.

4.3.2.7 Route

Este comando se utiliza para configurar las tablas de ruteo del kernel del sistema. Generalmente en todo equipo en una red local encontraremos al menos 3 rutas:

- ☞ La ruta de loopback, que utiliza el dispositivo de bucle interno (lo,lo0...).
- ☞ La de red local, que utiliza la tarjeta de red para comunicarse con equipos dentro del mismo segmento de red.
- ☞ La de default que también utiliza la tarjeta de red para enviar a un router o gateway paquetes que no son para equipos de nuestro segmento.

Si el comando es llamado sin parámetros este listara el estado actual de las tablas de ruteo.

Modo de uso: `route [-vn]`

```
route [ -v ] add [ -net | -host ] XXXX [gw GGGG] [metric
MMM] [netmask NNNN] [mss NNNN] [window NNNN] [dev DDDD]
route [ -v ] del XXXX
```

Opciones:

-n	Igual a no pasarle parámetros , pero muestra en cambio las direcciones numéricas.
-v	Setea el modo verbose (no es usado actualmente)
-del xxxx	Borra las rutas asociadas con la dirección de destino xxxx

Add [-net -host] xxxx [gw GGGG] [metric MMMM] [netmask NNNN] [dev DDDD]	Adhiere una ruta a la dirección IP xxxx. La ruta es una ruta de red si el parámetro -net es usado o xxxx se encuentra en xxxx. El argumento gw GGGG significa que algún paquete IP enviado a esta dirección debe ser ruteado al gateway específico. El parámetro metric MMMM no está implementado actualmente. El parámetro netmask NNNN especifica la máscara de red de la ruta a ser adherida. El parámetro dev DDDD fuerza la asociación entre la ruta y un dispositivo específico.
---	--

Tabla 13. Opciones de route.

Ej.

```
Route add -net 192.56.76.0 netmask 255.255.255.0 dev eth0
```

4.3.2.8 Telnet

Este programa al interfase de usuario para el protocolo telnet. El comando es de gran utilidad ya que nos permite la conexión a distintos servicios, en distintos puertos y la conversación con este, por medio del protocolo determinado.

Modo de uso `telnet [-d] [-a] [-n tracefile] [-e escapechar] [[-l user] host [port]]`

Opciones:

-d	Setea el valor inicial del modo de debug a verdadero.
-a	Este flag habilita el uso de auto login, utilizando el username almacenado en la variable de ambiente USER.
-n tracefile	Abre el archivo tracefile para recordar la información de trazado.
-e escapechar	Setea el carácter de escape para la sesión, si es omitido, se dice que el carácter de escape será el carácter de no escape.
-l user	Cuando conecta al sistema remoto toma user como el nombre de usuario para realizar la autenticación.
Host	Host de destino del llamado.
port	Indica el número de puerto al cual realizar la conexión, el puerto por defecto es el de telnet.

Tabla 14. Opciones de telnet.

Bibliografía.

Definiciones de puertos.

<http://www.iana.org/assignments/port-numbers>

CCNA. Cisco Primer Semestre.

CCNA. Cisco Segundo Semestre.

Linux Complete Reference Comand.

Guía del Administración de Linux.

Guía del Usuario de Linux.