



**Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas**

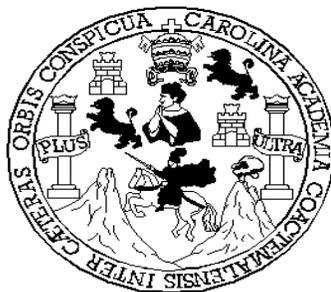
ANÁLISIS Y DIAGNÓSTICO DE REDES DE COMPUTADORAS

MARLON AUGUSTO MORÁN GONZÁLEZ

Asesorado por Ing. Caleb Rejopachi Carrera

Guatemala, septiembre de 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

ANÁLISIS Y DIAGNÓSTICO DE REDES DE COMPUTADORAS

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

MARLON AUGUSTO MORÁN GONZÁLEZ

ASESORADO POR EL ING. CALEB REJOPACHI CARRERA

AL CONFERÍRSE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, SEPTIEMBRE DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Bra. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivone Veliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
EXAMINADOR	Ing.. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. Luis Alberto Vettorazzi España
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS Y DIAGNÓSTICO DE REDES DE COMPUTADORAS,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha Junio de 2002.

Marlon Augusto Morán González

AGRADECIMIENTO

A:

DIOS

Por darme una vida tan llena de bendiciones,
por darme una excelente familia y unos
padres tan comprensibles;

MIS PADRES

Por su ayuda en todo momento, por sus
esfuerzos, su amor y su comprensión;

MI FAMILIA

Por su apoyo durante toda mi vida;

**MIS COMPAÑEROS
Y AMIGOS**

Por su ayuda, su amistad, apoyo, motivación
y enseñanzas;

**UNIVERSIDAD DE
SAN CARLOS**

Por la enseñanza recibida.

DEDICATORIA

A:

mis padres que son mi fuente de inspiración y que gracias, a su esfuerzo, trabajo, amor y comprensión, he logrado superar las más grandes dificultades que se me han presentado en la vida;

mis padres con mucho amor.

INDICE GENERAL

INDICE DE ILUSTRACIONES	iv
GLOSARIO	vii
RESUMEN	ix
OBJETIVOS	xi
INTRODUCCIÓN	xiii

1 CREACIÓN DE UNA RED

1.1. Componentes necesarios para crear su propia red	1
1.1.1 Servidor	1
1.1.2 Estación de trabajo	2
1.1.3 Cableado	3
1.1.4 Tarjeta de Red	3
1.1.5 Concentrador o centro de cableado (<i>HUB</i>)	3
1.1.6 Repetidores	5
1.2. Que debe saber acerca de una red	6
1.2.1 Usos	7
1.2.2 Topologías	8
1.2.2.a Topología de Bus	8
1.2.2.b Topología de Estrella	9
1.2.2.c Topología de Arbol	9
1.2.2.d Topología de Anillo	10
1.2.3 Protocolos	11
1.2.3.a Protocolo TCP / IP	11
1.2.3.b Protocolo OSI	12
1.2.4 Medios de transmisión	12
1.2.4.a Cable Par Trenzado	13
1.2.4.b Cable Par Paralelo	14
1.2.4.c Cable Coaxial	14
1.2.4.d Cable Fibra Optica	14

2 HERRAMIENTAS DE DIAGNOSTICO

2.1. Utilidades TCP/IP	17
------------------------------	----

2.1.1 Utilización del comando PING.....	17
2.1.2 Utilización del comando ARP	19
2.1.3 Utilización del comando NETSTAT	20
2.1.4 Utilización del comando NBTSTAT	21
2.1.5 Utilización del comando IPCONFIG	24
2.1.6 Utilización del comando TRACERT	25
2.1.7 Utilización del comando ROUTE	26
2.1.8 Utilización del comando NSLOOKUP	29
2.2. Utilidades de <i>Windows NT</i>	31
2.2.1 <i>Registry Editor</i>	32

3 TÉCNICAS PARA LA SOLUCIÓN DE PROBLEMAS

3.1 Protocolos de internet	35
3.1.1 Descripción general de los comandos y las respuestas de los protocolos	36
3.1.1.1 SMTP	37
3.1.1.2 POP3	37
3.1.1.3 IMAP4	37
3.1.1.4 NNTP.....	38
3.2 Comprobando <i>hardware</i>	39
3.2.1 Enrutador	39
3.2.1.1 El enrutador no puede arrancar desde la red con un servidor TFPT	41
3.2.1.2 El enrutador no puede arrancar desde la red con otro enrutador	41
3.2.1.3 Los tiempos de espera agotados y paquetes en desorden impiden el arranque desde la red	41
3.2.1.4 El cliente ARP indica tiempo de espera agotado durante el arranque desde la red	43
3.2.2 Cableado	45
3.2.2.1 Longitud	45
3.2.2.2 Atenuación	46
3.2.2.3 Retardo en modo diferencial	47
3.2.2.4 Fiabilidad	48
3.2.2.5 Velocidad	50
3.2.2.6 La colisión	51
3.2.2.7 Colisión Tardía	51

3.3 Mensajes comunes de errores en redes	52
3.4 Utilizando herramientas de diagnóstico	53
3.5 Modelo general para la resolución de problemas	54
3.6 Como prevenirse para una falla de red	56
4 HERRAMIENTAS PARA RESOLUCIÓN DE PROBLEMAS	
4.1 Lista de herramientas de análisis y diagnóstico	57
4.2 Herramientas de análisis y diagnóstico a nivel de <i>software</i>	59
4.2.1 <i>Link Analyst</i>	59
4.2.2 <i>RMON TrafficDirector</i>	62
4.2.3 <i>VlanDirector</i>	62
4.2.4 <i>MRTG: Multi Router Traffic Grapher</i>	63
4.2.5 <i>Microsoft Systems Management Server</i>	63
4.2.6 <i>Cisco Info Center</i>	65
4.2.7 <i>CiscoWorks</i>	67
4.2.8 Otras aplicaciones	68
4.3 Herramientas de análisis y diagnóstico a nivel de <i>hardware</i>	69
4.3.1 Medidores de voltaje y resistencia, multímetros digitales y probadores de cables	69
4.3.2 TDRs y OTDRs	70
4.3.3 Cajas de derivación, <i>fox boxes</i> y BERT/BLERT	71
4.3.4 Monitores de red	71
4.3.5 Analizadores de red	72
CONCLUSIONES	73
RECOMENDACIONES	75
BIBLIOGRAFÍA	77
APÉNDICES	79
Apéndice A – Información de soporte técnico	80
Apéndice B – Códigos de Error de <i>Windows</i>	83

INDICE DE ILUSTRACIONES

FIGURAS

1. Concentrador o centro de cableado (<i>hub</i>).....	4
2. Conexión de <i>hub</i> por medio de un cable UTP.....	5
3. Conexión de dos concentradores por medio de los conectores BNC.....	5
4. Conexión de una red utilizando un repetidor	6
5. Repetidor multipuertos	6
6. Topología de Bus.....	8
7. Topología de Estrella.....	9
8. Topología de Arbol.....	10
9. Topología de Anillo.....	11
10. Cable de par trenzado	14
11. Cable Coaxial	14
12. Cable Fibra Optica.....	15
13. Resolución de dirección de <i>hardware</i>	20
14. Resolución de nombres DNS.....	29
15. Editor de Registro.....	32
16. Claves del registro de <i>Windows</i>	33
17. Diagrama de resolución de problemas	54
18. Propiedades de los elementos	59
19. Mapeo de red	60
20. Reporte de servicios TCP/IP	60
21. Reporte de servicios IPX	61
22. Tiempo de respuesta.....	61
23. Registro.....	62

TABLAS

I. Descripción de rutas.....	28
II. Registro de <i>Windows</i>	33
III. Protocolos y los puertos que escuchan	35
IV. Comandos de SMTP.....	37
V. Comandos de POP3	37
VI. Comandos de IMAP4	38
VII. Comandos de NNTP	38
VIII. Distancia máxima promedio de los cables y sus conectores.	46
IX. Cables de fibra óptica, conectores y distancia máxima promedio	46
X. Ancho de banda de la fibra óptica	48
XI. Tecnologías de red y esquemas de codificación utilizado	50
XII. Equipo a conectar y conexiones aconsejadas.....	51
XIII. Herramientas de análisis y diagnóstico a nivel de <i>software</i>	58
XIV. Herramientas de análisis y diagnóstico a nivel de <i>hardware</i>	58

GLOSARIO

Ancho de banda	Volumen de información que puede circular por un medio físico de comunicación de datos, capacidad de conexión. A mayor capacidad mayor velocidad.
ATM, <i>Asynchronous Transmission Mode</i>	Sistema de transferencia de datos asíncrono que aprovecha al máximo la capacidad de una línea.
Bit, <i>Binary digit</i>, ó Dígito Binario.	Unidad mínima de información que puede ser tratada por un ordenador , en otras palabras, un 1 ó 0.
Byte	Conjunto de bits que representan un caracter.
DNS, <i>Domain Name System/Sever</i>, ó Servidor de nombres de dominios.	Sistema de computadoras y bases de datos distribuidas organizadas en forma jerárquica que se encarga de convertir, resolver, las direcciones de Internet en la dirección IP correspondiente y viceversa.
Host, sistema central.	Ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP.
Interface, interfaz, interfase.	Conexión entre dos componentes de hardware entre dos aplicaciones o entre un usuario y una aplicación.
Internet	Es la mayor red internet del mundo. Tiene una jerarquía de tres niveles formados por redes de eje central, "backbones" como, por ejemplo, NSFNET y MILNET, redes de nivel intermedio, y redes aisladas ("stub networks"). Internet es una red multiprotocolo.
IP	Dirección numérica y única de cada ordenador en Internet.

ISO , <i>International Standards Organization</i> , ó Organización Internacional para la Normalización.	Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones. Esta formada por las organizaciones de normalización de sus 89 países miembro.
OSI , <i>Open Systems Interconnection</i> , ó Interconexión de Sistemas Abiertos.	Conjunto de protocolos diseñados por comités ISO con el objetivo de convertirlos en estándares internacionales de arquitectura de redes de ordenadores.
Protocolo	Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes.
LAN , <i>Local Area Network</i> , ó Red de Área Local.	Grupo de equipos conectados en un mismo lugar.
Servidor	Equipo que controla el acceso de los usuarios a una red y les da servicio e información.
SMTP , <i>Simple Mail Transfer Protocol</i> , ó Protocolo Simple de Transferencia de Correo.	Se usa para transferir correo electrónico entre ordenadores.
Software	Programas, aplicaciones. Por extensión, todo lo que es "contenido", texto, imágenes, sonido, en contraste con lo material, hardware.
TCP/IP , <i>Transmission Control Protocol/Internet Protocol</i> , ó Protocolo de Control de Transmisión/Protocolo Internet.	Sistema de protocolos, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla, adecuadamente a través de la red.

RESUMEN

El presente trabajo consta de las cosas básicas a saber, al momento de querer determinar en dónde es posible que esté dando un error la red de computadoras que se tenga, o fácilmente puede dar una guía de donde es probablemente este error o simplemente ayudar a evitar un futuro error que se pueda dar.

El primer capítulo, consiste, únicamente, de facilitar una guía de los elementos que se tienen que tomar en cuenta, al momento de querer realizar una red, proporcionando, además información de para que sirve cada uno de los componentes que se mencionan. También, este mismo capítulo, contiene información de usos posibles que se le pueden dar a una red, lo que permite tener una idea previa respecto ventajas de las que se poseen al realizar una red de computadoras.

El segundo capítulo, está destinado a mostrar qué herramientas pueden ser utilizadas para determinar en dónde presenta errores la red y mostrar una utilidad propia del sistema operativo *Windows* que permite monitorear la red.

El tercer capítulo, está orientado, específicamente, a la solución de los problemas que se presentan, para ello, se especifica cuales son las principales partes a verificar en una red, es decir, qué es importante verificar primero, antes de determinar dónde se encuentra el error, tales como: el enrutador, el cableado, los mensajes presentados. Además, el capítulo presenta un modelo muy sencillo que se puede llevar a cabo al momento que se esté determinando en dónde se encuentran los problemas en la red de computadoras.

El cuarto y último capítulo, muestran información de algunas herramientas que son posibles soluciones a los dolores de cabeza al momento de analizar y diagnosticar una red de computadoras, ya que, éstas cuentan con las opciones necesarias para valuar partes importantes de la red y mostrar si éstas funcionan, adecuadamente. Las herramientas que se muestran están divididas en dos, unas que evalúan, específicamente, el *software* y la segunda de ellas evalúa el *hardware* de la red de computadoras.

OBJETIVOS

General

Dar a las personas una guía que le ayude a anticiparse a los errores o corregir posibles causas de errores que se presentan en el momento de estar administrando o trabajando con una red de computadoras.

Específicos

1. Dar a conocer cuales son los componentes básicos necesarios, *hardware* y *software*, en el momento de la creación de una red de computadoras.
2. Describir que cosas son las más comunes a revisar para detectar errores dentro de una red de computadoras.
3. Mostrar que existen varios comandos dentro de los sistemas operativos, específicamente: *Windows NT / Windows 2000 / Windows XP, Windows 2003*, que pueden ayudar a diagnosticar una red de computadoras.
4. Plantear posible soluciones a los errores que se presentan en las redes de computadoras.
5. Dar a conocer referencias de algunos programas de computadoras que pueden ayudar para detectar y solucionar los problemas de las redes de computadoras.

INTRODUCCIÓN

Este trabajo está orientado hacia aquellas personas que están interesadas conocer cómo detectar y solucionar problemas que se presentan en redes de computadoras, ya sea cuando se está creando un red cuando ya se tiene una creada.

El trabajo presenta varios comandos que pueden usarse para detectar si la red esta funcionando correctamente, así como, también, soluciones en el caso de que el comando que se ejecutó muestra que algún parámetro de la red no dió el resultado esperado.

En este trabajo, también, se encontrarán las cosas básicas que se deben conocer acerca de una red de computadoras, pero ya que el trabajo no pretende enseñar cómo crear una red, sino solucionar los problemas que en ella se presenten, sólo se mencionará lo más prescindible y no se entrará a explicar en detalle la creación de una red, los componentes con los que debe contar para armarla y qué debería de hacer para configurarla. Esto se hace con el fin de que las personas que nunca han hecho una red tengan nociones de con que cosas debe contar.

Se pretende que todas las personas tengan una guía que le enseñe cómo detectar si se cometió algún error al crear o configurar una red o si el error se está desarrollando debido a algún mal funcionamiento de alguno de los dispositivos de la red. También, se pretende mostrar cuáles son las posibles soluciones a los distintos errores que se presenten, para que el usuario pueda corregirlos, es más, un usuario podrá detectar cuáles son las causas del error en una red y, así, anticiparse a ellas.

Al final del trabajo, también, se hace referencia de algunas herramientas existentes en el mercado que pueden ser de mucha utilidad para diagnosticar redes de computadoras. Estas herramientas tienen, entre sus muchas opciones, la de detallar estadísticas del funcionamiento de la red, realizar ciertas acciones ante comportamientos detectados y la posibilidad de detectar errores.

1 CREACIÓN DE UNA RED

El presente capítulo trata de dar a conocer cuáles son los componentes básicos con los que debe contar, para que pueda crear una red de computadoras. En él se presentan desde los componentes físicos que componen una red de computadoras, hasta la topología, medios de transmisión y qué cosas son las que se deben configurar.

1.1 Componentes necesarios para crear su propia red

Antes de poder crear su propia red de computadoras, se debe saber cuáles son los componentes que se necesitarán para crearla, la topología, métodos de acceso y, sobre todo, se tiene que saber cuál es el objetivo por el cual la necesita.

Hay que tomar en cuenta que, dependiendo como uno configure su red, tendrá la posibilidad de compartir programas y archivos, compartir recursos de la red, compartir bases de datos, posibilidad de utilizar *software* de red, uso de correo electrónico, creación de grupos de trabajo, contar con cierta seguridad, acceso a más de un sistema operativo, tener mejoras en la organización de la empresa.

A continuación se muestra una lista de que componentes son necesarios.

- 1 Servidor
- 2 Estación de trabajo
- 3 Cableado, los conectores van a variar dependiendo del tipo de cableado a utilizar
- 4 Tarjetas de Red
- 5 Concentrador o centro de cableado
- 6 Repetidores

1.1.1 Servidor

Este es el que se encargará de proveer de todos los datos, programas o recursos que necesitan todas las estaciones de trabajo que están conectadas a esta red.

Algo que se debe tomar en cuenta, es que por ser la computadora que se encargará de prestar estos servicios a las estaciones de trabajo, debería de ser la computadora más poderosa dentro de la red, para que todos los servicios los realice de una forma eficiente y rápida.

Para poder decir que un servidor es poderoso, nosotros tendríamos que evaluar varios aspectos de este, tales como:

- 1 Memoria RAM
- 2 Microprocesador
- 3 Disco Duro
- 4 Arquitectura del Bus
- 5 Ranuras de expansión

Todos estos aspectos afectan directamente al desempeño de la red, pero también el *software* que se utiliza juega un papel muy importante, ya que con el se le puede sacar partido a las prestaciones del circuito integrado. Para que se obtenga un rendimiento significativo debe contarse con sistemas operativos de red que soporten la tecnología que se este utilizando y si es posible la tecnología que todavía no ha salido pero que se esta fabricando.

El que una computadora este como servidor, no quiere decir que no se pueda usar como una estación de trabajo, pero lo que si hay que tener muy claro es que si se utiliza como estación de trabajo también, no se podrá obtener de ésta la máxima velocidad y eficiencia en la red.

1.1.2 Estación de trabajo (o nodos de red)

Un usuario no necesita conocer mucho acerca de redes, ya que el solo tiene contacto con su estación de trabajo, que es donde el ejecuta sus aplicaciones, también le sirve para poder comunicarse no solo con el servidor, sino también con otras estaciones de trabajo que están en la misma red. Una estación de trabajo no necesita tantos requerimientos como los que se necesitan en el servidor, ya que en esta solo tendrá que tener lo necesario para ejecutar las aplicaciones con las que cuenta o con las que desea trabajar pero que son accedidas a través del servidor.

Un punto muy importante sobre lo que son las estaciones de trabajo, es que no necesariamente tienen que tener disco duro para funcionar, ya que estas pueden utilizar los recursos que tienen el servidor entre ellos el disco duro

1.1.3 Cableado

En una red el cableado es el que sirve para poder hacer la interconexión del servidor y las estaciones de trabajo, es decir, es el medio que sirve para que se comuniquen las computadoras (o medio de transmisión).

Existen varios tipos de cables utilizados para realizar las redes, entre los que se pueden contar por trenzado, cable coaxial y cable de fibra óptica. Cada cable tiene ciertas características que lo diferencian unos de otros tales como el costo, accesorios, ancho de banda. Susceptibilidad a interferencias magnéticas y emisiones eléctricas, etc.

1.1.4 Tarjetas de Red

El servidor y cada una de las estaciones de trabajo deben de tener por lo menos una tarjeta de red, que es donde el cableado es conectado. La tarjeta de interfaz de red también es llamada NIC. La *NIC* no es más que una tarjeta que inserta en alguno de los *slots* con los que cuentan las computadoras. La función principal que tiene es la de formar los paquetes de datos de la estación de trabajo (o el servidor) y transmitirlos a través del cableado. Otras de las funciones que realiza la tarjeta de red, es la de recibir paquetes para luego traducirlos a *bytes* que el CPU de la estación de trabajo pueda entender.

Los NIC que se encuentran en la actualidad, están equipados con un microprocesador o CPU, el cual les permite procesar cierta información sin que tenga que intervenir el CPU de la estación de trabajo. Esto permite quitarle cierta carga de trabajo al CPU de la computadora, lo cual ayuda a que el desempeño de la computadora se mejore.

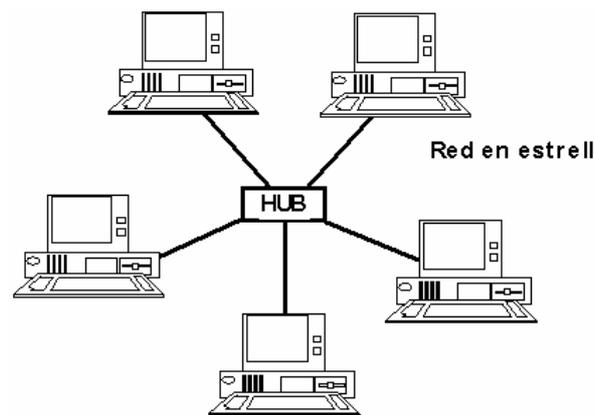
1.1.5 Concentrador o centro de cableado (HUB)

Según el tipo de topología que se este utilizando puede ser que necesite utilizar un concentrador (mejor conocido como HUB).

Normalmente un HUB es utilizado cuando no se pueden conectar todas las estaciones al servidor, es decir, que en el servidor no cuenta con el suficiente número de tarjetas de red como para conectar todos los cables que vienen desde varias estaciones de trabajo.

Un HUB es utilizado como el área central en donde las estaciones de trabajo y el servidor pueden comunicarse. Dentro del HUB se trata de encaminar los paquetes hacia su destino final.

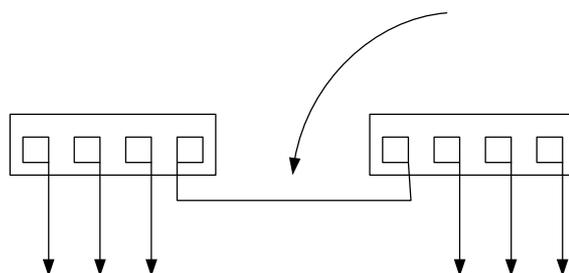
Figura 1. Concentrador o centro de cableado (*hub*).



Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología de estrella. El concentrador tiene varios puertos en la parte trasera de la tarjeta, a los que se conecta el cable de otros nodos de red.

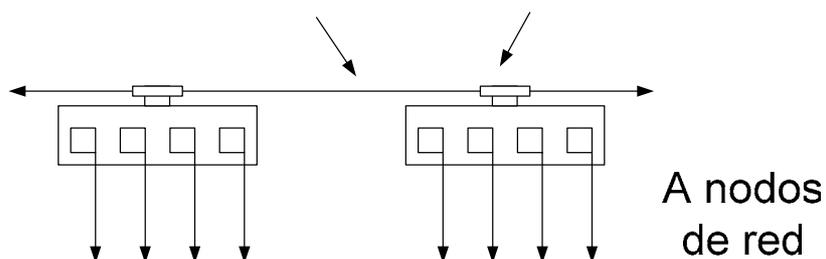
Los concentradores permiten el que se conecten otros concentradores, lo cual permite que se tengan más estaciones de trabajo adicionales. Se utiliza un puerto en cada concentrador para conectarse con el otro concentrador. El cable empleado para conectar a los Concentradores es el mismo que se usa entre el concentrador y las estaciones de trabajo, a excepción de que los alambres están traslapados entre los dos conectores a cada extremo.

Figura 2. Conexión de *hub* por medio de un cable UTP



Una de las características que tienen la mayoría de concentradores es que tienen un conector del tipo BNC que es distinto a los demás tipos de conectores que tiene, esto permite que se enlacen concentradores por medio de un cable coaxial *Thin Ethernet*.

Figura 3. Conexión de dos concentradores por medio de los conectores BNC.



1.1.6 Repetidores

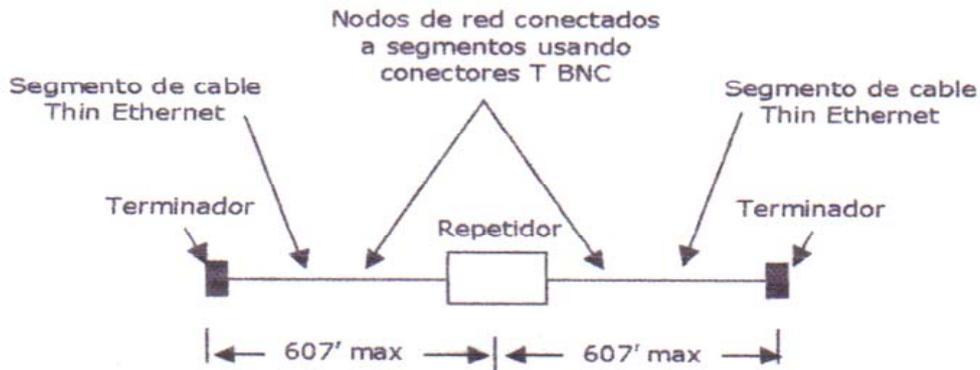
Son dispositivos que permiten el contar con una longitud mucho mayor a la que se tiene únicamente con el alcance que se tiene con el tipo de cableado utilizado, además permite ampliar la red y retransmitir la señal de la red.

Los repetidores hacen posible que se tengan tramos largos de cableado los que funcionan levantando la señal, amplificándola, limpiándola y enviándola a través de señales ópticas o eléctricas. Los repetidores son utilizados cuando una red debe exceder el máximo tamaño físico permitido por los estándares de ingeniería.

En la figura se muestra una conexión de red utilizando repetidores, tomando en cuenta que la longitud máxima de segmento de cable para *Thin Ethernet* es de 607 pies. **Cable Thinnet**

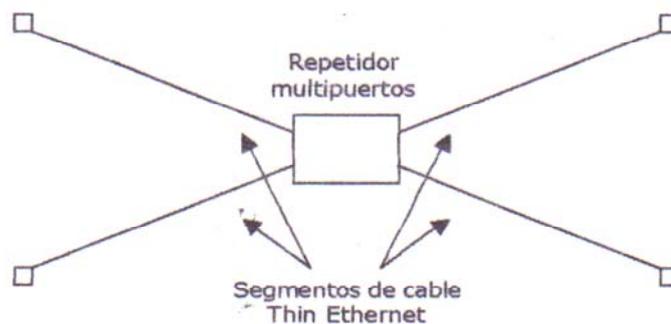
Si se coloca un repetidor al extremo del cable, se puede conectar otro segmento de cable *Thin Ethernet* de hasta 607 pies para dar un total de 1214 pies.

Figura 4. Conexión de una red utilizando un repetidor.



También se tiene la opción de utilizar repetidores múltiples, lo cual permite el conectar más de dos segmentos de cable de red. En la figura, con un repetidor multipuerto se pueden conectar varios segmentos de *Thinnet*. Es importante no olvidar que, aunque el repetidor multipuertos permite crear una topología física de estrella basada en varias topologías físicas de bus, el propósito principal de un repetidor es extender la longitud máxima permitida del cable de red.

Figura 5. Repetidor multipuertos.



1.2 Que debe saber acerca de una red

Una red de computadoras no es más que un conjunto de computadores autónomos interconectados entre si, con el fin de compartir información y recursos.

Entre las características con las que cuenta una red están:

- 1 Cobertura geográfica limitada
- 2 De docenas a cientos de dispositivos
- 3 Velocidad de transmisión
- 4 Medio de transmisión compartido

1.2.1 Usos

El uso que uno le da a una red depende de las necesidades que se tengan, aunque la idea principal de crear una red, es la de compartir dispositivos e información.

Algunos otros usos que se le dan a la red:

- 1 Un medio de comunicación a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. Las redes locales están contenidas en una reducida área física: un edificio, un campus, etc.
- 2 Transmisión de datos a velocidades máximas a las que se pueden comunicarse las estaciones de trabajo de la red.
- 3 Unir estaciones de trabajo que se encuentran a distancias cortas, entre unos metros y varios kilómetros.
- 4 Hacer que todos los dispositivos pueden comunicarse con el resto y algunos de ellos pueden funcionar independientemente.
- 5 Seguridad, contar con un sistema fiable, con un índice de errores muy bajo.
- 6 Flexibilidad, el usuario administra y controla su propio sistema.
- 7 Expansión, contar con la posibilidad de que el sistema reconozca requerimientos de expansión futuros.
- 8 Tener al alcance todos los recursos existentes dentro de la red.
- 9 Conectividad con distintos sistemas, pudiendo así eliminar las limitaciones de *hardware*.
- 10 Veracidad, contar con un sistema que sea digno de toda nuestra confianza.

Entre las aplicaciones que se le puede dar a una red están:

Compartir

- 1 Impresoras
- 2 Discos duros

- 3 *Drives*
- 4 Líneas telefónicas
- 5 Conexión con computadoras minis o *mainframes*

Comunicación entre grupos de trabajo

- 1 Correo electrónico
- 2 Compartir datos

Nuevas aplicaciones

- 1 Plantilla de grupo
- 2 Flujos de trabajo
- 3 Multimedia
- 4 Video Interactivo
- 5 Mensajería de voz

1.2.2 Topologías

1.2.2.a Topología de Bus

En este tipo de topología, se tiene un solo canal de transmisión, por donde se da una comunicación bidireccional, con sus puntos de terminación bien identificados. Una de las ventajas que se tiene es que al momento de que una estación de trabajo falle, no afectará esta a todo el sistema. Pero entre sus inconvenientes esta el que si el bus falla, ninguna estación de trabajo podría comunicarse. Otro problema que presenta es que se tiene una gran dificultad al querer detectar los errores que presenta.

Figura 6. Topología de Bus.



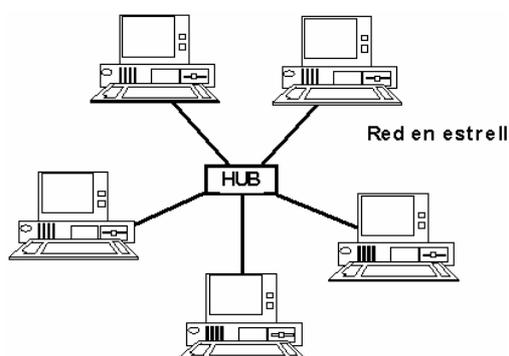
1.2.2.b Topología de Estrella

Esta topología consiste en un conjunto de estaciones de trabajo que tienen comunicación entre ellas a través de un dispositivo central conocido con el nombre de *Hub*, que se encarga de enlutar la información a la estación de trabajo indicada.

Se caracteriza por la centralización de las operaciones y comunicaciones. En este tipo de topología se tiene el inconveniente de que si se produce un fallo en el nodo central produce la caída de todo el sistema de red, aunque esto puede representar una ventaja para cuando se realiza una detección de fallos.

Entre las ventajas que presenta este tipo de topología están: fácil servicio; es fácil agregar una estación de trabajo; el esquema de la red es fácil de modificar; los diagnósticos se vuelven fáciles de realizar, por ejemplo cuando se daña un cable, fácilmente se detecta que cable es el que está dañado, ya que solo hay un cable que se conecta desde el *hub* hasta la estación de trabajo.

Figura 7. Topología de Estrella.



1.2.2.c Topología de Arbol

Este tipo de topología también recibe el nombre de estrella distribuida.

En esta topología se reúnen varias estaciones de trabajo en unos dispositivos conocidos como *Hub*, que a su vez se interconectan entre sí. Allí puede haber inicialmente un bus que es conectado a un *hub*, el cual divide aquel bus en dos o más buses, lo cual puede seguir dándose, creando más buses de las divisiones del bus original.

Esta topología es relacionada con un árbol por el hecho de tener varias ramificaciones, las cuales se van expandiendo como se expanden las ramas en los árboles.

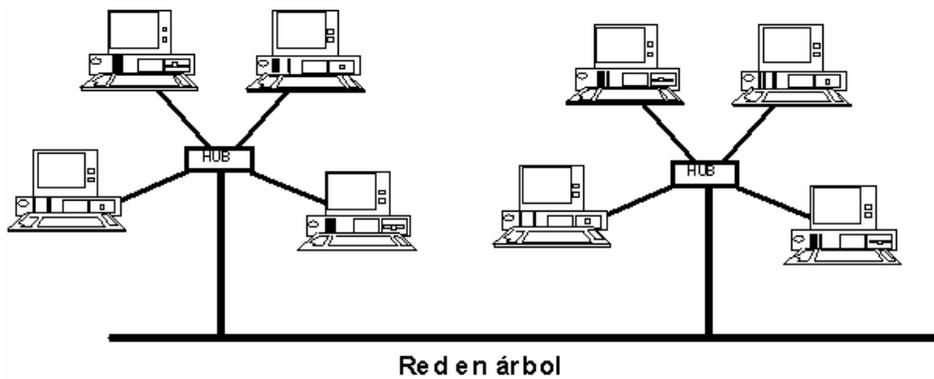
Entre las ventajas que se tienen están:

- 1 Se puede extender fácilmente
- 2 Facilidad para detectar y aislar fallas

Como todas las anteriores topologías, esta también tiene sus desventajas, tales como:

- 1) Si el bus que da origen a una ramificación falla, todas las estaciones que se encuentran en esta ramificación también fallan.

Figura 8, Topología de Arbol.



1.2.2.d Topología de Anillo

En este tipo de topología todas las estaciones de trabajo están conectadas por un solo medio de transmisión, el cual tiene una forma de anillo. En esta topología el medio de transmisión se define por un camino unidireccional cerrado que conecta todas las estaciones. Se puede notar que no existen finales para el cableado, ya que se forma un anillo completo.

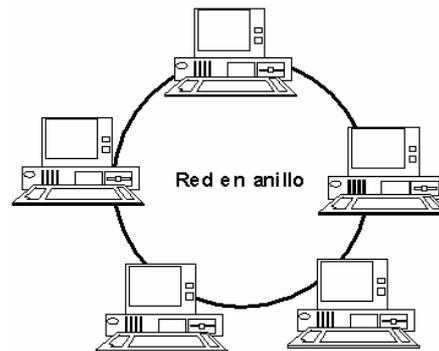
Los datos viajan alrededor del anillo en una única dirección y pasa a través de cada nodo. Cada una de las estaciones actúa como un repetidor.

Ventajas de una red de anillo:

- 2 La longitud del cableado es menor y por lo tanto un costo de cableado más bajo
- 3 No se requiere de un dispositivo extra

Entre las desventajas que se pueden detectar en este tipo de topología están: que si una de las estaciones de trabajo falla, la red completa fallaría, ya que cada una de las estaciones sirve como repetidoras, por lo que la siguiente estación no recibiría la información y no podría transmitirla; se hace difícil diagnosticar donde se encuentran las fallas; el querer cambiar o reconfigurar la red se hace muy difícil.

Figura 9. Topología de Anillo.



1.2.3 Protocolos

Para posibilitar la comunicación entre computadoras es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos.

Un protocolo es un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos.

1.2.3.a Protocolo TCP / IP

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos. El protocolo que más ampliamente es utilizado es el *Internet Protocol Suite*, comúnmente conocido como TCP / IP. El nombre TCP / IP Proviene de dos protocolos importantes de la familia, el *Transmission Control Protocol* (TCP) y el *Internet Protocol* (IP).

Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos.

La parte IP proporciona actualmente una de las mejores definiciones para la interconexión entre redes y está siendo usada en la Internet.

En términos generales, el *software TCP/IP* está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de *hardware*.

- 1 Aplicación
- 2 Transporte
- 3 Internet
- 4 Interfaz de Red
- 5 *Hardware*

1.2.3.b Protocolo OSI

Esta jerarquía está definida por la *International Organization for Standardization* (Organización para la Estandarización o ISO, por sus siglas en inglés), conocida como *Referencia Model of Open System Interconnection* (Modelo de referencia de interconexión de sistemas abiertos) de ISO, denominada frecuentemente modelo ISO.

Este protocolo suele ser usado como estándar para comparar otras jerarquías de protocolos. El modelo ISO contiene 7 capas conceptuales organizadas como se muestra a continuación: aplicación, presentación, sesión, transporte, red, enlace de datos, física.

El modelo ISO, elaborado para describir protocolos para una sola red, no contiene un nivel específico para el ruteo en el enlace de redes, como sucede con el protocolo TCP/IP.

1.2.4 Medios de transmisión

Para que pueda existir comunicación entre estaciones y servidores es necesario contar con un medio que sirva para transmitir la información que necesitamos enviar, es por ello que en la actualidad existe una variedad de medios de transmisión, entre los que se encuentran:

- 1 Par Trenzado
- 2 Par Paralelo
- 3 Cable Coaxial
- 4 Cable de Fibra Óptica

Todos ellos son medios confinados. Los factores que han de considerarse a la hora de la elección de un cable son preferentemente: impedancia característica, frecuencia de trabajo, atenuación máxima, coste por metro.

También se puede utilizar el medio inalámbrico que usa ondas de radio, microondas o infrarrojos, estos medios son más lentos que el cable o la fibra óptica. Las líneas de transmisión son las que conforman la espina dorsal de la red, por ellas se transmite toda la información que se quiera transmitir entre las distintas estaciones de trabajo.

1.2.4.a Cable Par Trenzado

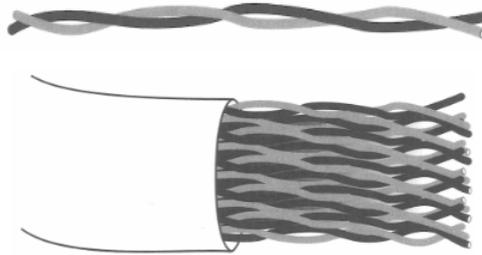
El par trenzado consta como mínimo de dos conductores aislados trenzados entre ellos y protegidos con una cubierta aislante. Un cable de este tipo contiene 2, 4 u 8 hilos.

Los diámetros del conductor en este tipo de cables pueden ser de 0'6 mm o de 1'2 mm. Se puede usar en dos modalidades, apantallado y no apantallado y principalmente en topologías estrella y *hub*. Una de las grandes ventajas que ofrece es que se pueden transmitir a la vez voz (telefonía) y datos. Además, se pueden eliminar los ruidos en las señales transmitidas restando las diferencias de la señal de tierra recibida con la enviada (supresión de modo común).

Como ventajas de este tipo de cable se pueden destacar, a parte de las ya comentadas, su bajo costo, fácil instalación, que permite ser configurado en diferentes topologías (bus o estrella), y que el mismo tipo de cable puede soportar diferentes tipos de redes.

Como desventajas las distancias que cubre son más limitadas que en los demás conductores, presenta mayor sensibilidad al ruido que el cable coaxial y no soporta grandes velocidades de transmisión de datos.

Figura 10. Cable de par trenzado.



1.2.4.b Cable Par Paralelo

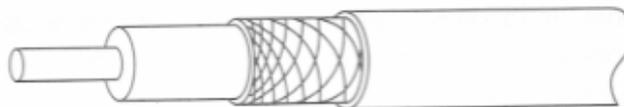
Este tipo de transmisión consta de dos cables de cobre aislados entre sí. No permite conexiones fiables (sin demasiada atenuación) de más de 50 metros. Tiene como principales inconvenientes los ruidos y acoplamientos que sufre por la mala calidad del aislante.

1.2.4.c Cable Coaxial

El cable coaxial consiste de dos conductores concéntricos, separados por un dieléctrico y protegido del exterior por un aislante (similar al de las antenas de TV).

Sobre el cable coaxial cabe destacar su gran inmunidad al ruido debido a su construcción. Estos medios tienen un gran ancho de banda, en función del diámetro del conductor, y una mejor respuesta en frecuencia que los cables anteriores. Por último, los cables coaxiales típicos utilizados en redes de área local son el RG-58 (*thin Ethernet*), el RG-11 (*thick Ethernet*) y el RG-62 (*ARCnet*).

Figura 11. Cable Coaxial.

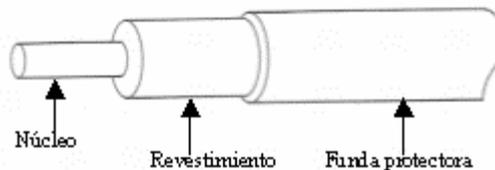


1.2.4.d Fibra óptica.

Es uno de los medios que da una velocidad de transmisión grande comparada con los demás medios de transmisión. Las señales de datos se transmiten a través de impulsos luminosos y pueden recorrer grandes distancias sin que se tenga que amplificar la señal.

Cabe destacar que los mejores resultados obtenidos en este tipo de medio alcanza frecuencias de hasta 1 GHz teniendo pérdidas despreciables por kilómetro, aunque también es más cara y difícil de acoplar, ya que el diámetro del núcleo de la fibra es del orden de la longitud de onda de la luz que por ella se transmite.

Figura 12. Cable Fibra Optica.



Otra de las ventajas que se puede dar de este tipo de medio es que por su naturaleza, este tipo de señal y cableado es inmune a las interferencias electromagnéticas y por su gran ancho de banda (velocidad de transferencia), permite transmitir grandes volúmenes de información a alta velocidad. Por lo que se puede considerar como una solución apta para redes donde se necesita alta velocidad a grandes distancias, con un cierto flujo de datos considerable.

Entre los inconvenientes que se tiene con este tipo de medio de transmisión están: que tiene un soporte físico muy caro, debido a el precio de los conectores y el equipo requerido para enviar y detectar las ondas y la necesidad de disponer de técnicos calificados para realizar la instalación y mantenimiento del sistema de cableado.

2 HERRAMIENTAS DE DIAGNOSTICO

2.1 Utilidades TCP/IP

En la actualidad existe una gran variedad de utilidades que pueden ayudar a diagnosticar nuestra red, aunque también contamos con las herramientas que proporcionan nuestro sistema operativo (*Windows NT*, 2000), entre las que tenemos:

- PING
- ARP
- NETSTAT
- NBTSTAT
- IPCONFIG
- TRACERT
- ROUTE
- NSLOOKUP

A continuación se dará una breve explicación de cómo es que podemos utilizar cada una de estas herramientas para poder realizar un buen diagnóstico de la red.

2.1.1 Utilización del comando PING

La instrucción “ping” es utilizada normalmente para asegurar que se puede llegar a establecer una conexión con otra estación de trabajo. Al ejecutar esta instrucción se muestra en pantalla si se ha recibido una respuesta del destino, además de mostrar cuanto tiempo se tardó en recibirla.

En caso de que no se haya recibido una respuesta, es decir, que los paquetes que se enviaron al destino no le llegaron o bien que los paquetes enviados por el destino no llegaron, el comando ping muestra un mensaje de error.

También podemos utilizar el comando para:

- Determinar si el TCP/IP está funcionando correctamente, para ello lo único que tendríamos que hacer es un ping al equipo con la dirección (no con el nombre del host), lo cual devolvería un error si en caso no estuviera funcionando.
- Determinar si el enrutador esta en ejecución, para lo que tendríamos que hacer un ping hacia la dirección de este.
- Puede servir para determinar si la conectividad hacia alguna de las direcciones que deseamos se encuentra bien, lo único que tendríamos que hacer es un ping hacia la dirección que queremos alcanzar.

Formato y parámetros a utilizar con el comando ping:

```
ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
[-r cuenta] [-s cuenta] [[-j lista-host] | [-k lista-host]]
[-w tiempo de espera] lista-destino
```

Descripción de los parámetros:

-t	Ping al <i>host</i> especificado hasta que lo hagamos parar. También puede servir para ver una serie de estadísticas del envío de paquetes.
-a	Resolver direcciones en nombres de <i>host</i> .
-n cuenta	Número de peticiones eco para enviar.
-l tamaño	Enviar tamaño del buffer.
-f	Establecer No fragmentar el indicador en paquetes.
-i TTL	Tiempo de vida.
-r cuenta	Ruta del registro para la cuenta de saltos.
-s <i>count</i>	Sello de hora para la cuenta de saltos.
-w tiempo de espera	Tiempo de espera en milisegundos para esperar cada respuesta.

Si al momento de ejecutar el comando ping obtenemos el mensaje "Red de destino inaccesible", quiere decir que no existe ninguna ruta que pueda seguir los paquetes hacia el destino, por lo que se tendría que comprobar la tabla de enrutamiento del enrutador.

Ahora bien si la respuesta que obtenemos es "Tiempo de espera agotado para esta solicitud", estará indicando que no se obtuvo ninguna respuesta al comando ping durante el período de tiempo predeterminado (1 segundo). Algo que se puede realizar en estos casos es comprobar lo siguiente:

- Hay algún enrutador inactivo. Para comprobar si hay algún enrutador que no este activo podemos utilizar el comando *tracert*, que mostrará la ruta que siguen los paquetes, con lo que podemos determinar cual es el último punto al que llegan.
- *Host* de destino inactivo. Para ello nosotros tendríamos que comprobar que el *host* está ejecutándose o comprobar la conectividad utilizando algún otro protocolo.
- No hay ruta de retorno al equipo. Si se tiene que el *host* de destino esta activo, tendríamos que revisar si tenemos alguna ruta de retorno, es decir, si tenemos alguna puerta de enlace (o *gateway*) predeterminada.

2.1.2 Utilizando el comando ARP

ARP no es más que un protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*). Este protocolo ayuda a resolver direcciones IP las cuales se utilizan para tener un control de acceso a medios.

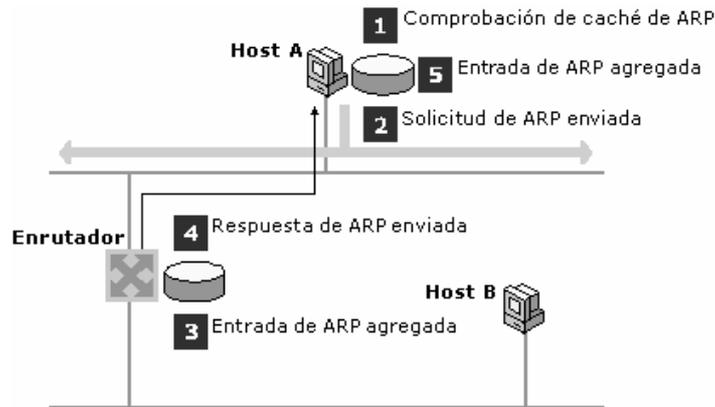
Que usos le podemos dar al protocolo ARP:

- Podemos llegar a determinar cual es la dirección de control de acceso a medios de un dispositivo configurado con una dirección IP.
- Registrar la dirección IP del solicitante de ARP, lo cual se realiza con el simple hecho de hacer una solicitud ARP, lo cual realiza un registro no solo de la dirección IP del solicitante, sino que también registra la dirección IP del remitente, esto lo guarda en la caché de ARP.

La dirección de control de acceso a medios, no es más que una dirección única que el fabricante programa en el dispositivo, esta dirección consta de tan solo 6 *bytes*, la cual esta programada en la memoria de sólo lectura de cada dispositivo.

En la siguiente figura se muestra la forma en que ARP resuelve las direcciones IP a direcciones de *hardware* dentro de la misma red local.

Figura 13. Resolución de dirección de *hardware*



En esta figura se muestra dos *hosts* que están en una misma red física. A tiene una dirección IP 10.0.0.99 y B la dirección IP 10.0.0.100.

Los pasos que sigue el ARP para resolver las direcciones son:

1. Determinar cual es la dirección de reenvío. Después, buscar en la propia caché de ARP del *host* A una dirección que coincida con la del *host* B
2. Si no se encuentra, envía una solicitud ARP a todos los *hosts*, donde solicita la dirección de *hardware* para 10.0.0.100.
3. Dentro de cada *hosts* que recibe la solicitud, se verifica si la dirección no es la suya, sino lo es, la descarta. El *host* que tiene esa dirección, agrega una dirección de *software* y *hardware* hacia el *host* A en su caché de ARP.
4. El *host* que tiene la dirección que coincide con la solicitada envía un mensaje de respuesta al *host* A, indicando en el su dirección de *hardware*.
5. Al momento en que el *host* A recibe el mensaje de respuesta, realiza el registro en la caché de ARP de la dirección de *hardware* y *software* del *host* B.

Luego de realizar todos estos pasos, ya puede existir una comunicación o tráfico *IP* entre ambos *hosts*.

Este comando más que todo tiene como finalidad la resolución de nombres.

2.1.3 Utilizando el comando NETSTAT

El comando `nbtstat` es utilizado para la resolución de nombres bajo NetBIOS en direcciones *IP*.

Otras opciones que se tienen para la resolución de nombres NetBIOS, son:

- Búsqueda en la caché local,
- Consultar los servidores *WINS* y *DNS*
- Buscar dentro de los archivos *Lmhosts* y *Hosts*.

Descripción de los parámetros:

- n Muestra los nombres NetBIOS que los programas registraron localmente.
- c Muestra la caché de nombres NetBIOS, que contiene asignaciones de nombres a direcciones para otros equipos.
- R Purgar los nombres que se encuentran en la caché y cargarlos nuevamente desde el archivo *Lmhosts*.
- RR Liberar los nombres NetBIOS que fueron registrados dentro de algún servidor *WINS* y después renovar el registro de los nombres.
- S Muestra las sesiones de NetBIOS actuales y su estado

2.1.4 Utilizando el comando NBTSTAT

Este comando es utilizar para mostrar estadísticas y el estado actual de las conexiones TCP/IP.

¿Que podemos llegar a determinar utilizando este comando?

- Si se están recibiendo o enviando paquetes.
- Si existen conexiones activas.
- Obtener estadísticas de nuestra IP.
- Podemos obtener una tabla que muestra todos los caminos que se tienen guardados.
- Obtener una lista de todos los puertos que se encuentran activos.

Formato y parámetros a utilizar con el comando ping:

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]

Descripción de los parámetros:

- a Muestra todas las conexiones y puertos escucha.

- e Muestra estadísticas *Ethernet*. Se puede combinar con la opción -s.
- n Muestra números de puertos y direcciones en formato numérico.
- r Muestra el contenido de la tabla de rutas.
- s Muestra estadísticas por protocolo.

C:\>netstat -e

Estadísticas de la interfaz

	Recibidos	Enviados
<i>Bytes</i>	3995837940	47224622
Paquetes unidifusión	120099	131015
Paquetes no unidifusión	7579544	3823
Descartados	0	0
Errores	0	0
Protocolos desconocidos	363054211	

C:\>netstat -a

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	CORP1:1572	172.16.48.10:nbsession	ESTABLISHED
TCP	CORP1:1589	172.16.48.10:nbsession	ESTABLISHED
TCP	CORP1:1606	172.16.105.245:nbsession	ESTABLISHED
TCP	CORP1:1632	172.16.48.213:nbsession	ESTABLISHED
TCP	CORP1:1659	172.16.48.169:nbsession	ESTABLISHED
TCP	CORP1:1714	172.16.48.203:nbsession	ESTABLISHED
TCP	CORP1:1719	172.16.48.36:nbsession	ESTABLISHED
TCP	CORP1:1241	172.16.48.101:nbsession	ESTABLISHED
UDP	CORP1:1025	*:*	
UDP	CORP1:snmp	*:*	
UDP	CORP1:nbname	*:*	
UDP	CORP1:nbdatagram	*:*	
UDP	CORP1:nbname	*:*	
UDP	CORP1:nbdatagram	*:*	

C:\>netstat -s

Estadísticas IP

Paquetes recibidos = 3907

Errores de encabezado recibidos	= 0
Errores de dirección recibidos	= 0
Datagramas reenviados	= 0
Protocolos desconocidos recibidos	= 0
Paquetes recibidos descartados	= 0
Paquetes recibidos procesados	= 3907
Solicitudes de salida	= 3907
Descartes de ruta	= 0
Paquetes de salida descartados	= 0
Paquetes de salida sin ruta	= 0
Reensambles requeridos	= 0
Reensambles correctos	= 0
Reensambles erróneos	= 0
Datagramas correctamente fragmentados	= 0
Datagramas mal fragmentados	= 0
Fragmentos creados	= 0

Estadísticas ICMP

	Recibidos	Enviados
Mensajes	582	582
Errores	0	0
Destino inaccesible	0	0
Tiempo agotado	0	0
Problemas de par metros	0	0
Paquetes de control de flujo	0	0
Redirecciones	0	0
Echos	291	291
Respuestas de eco	291	291
Fechas	0	0
Respuestas de fecha	0	0
Mascaras de direcciones	0	0
Mascaras de direcciones respondidas	0	0

Estadísticas de TCP

Activos abiertos	= 161
Pasivos abiertos	= 161
Intentos de conexión erróneos	= 0
Conexiones restablecidas	= 0
Conexiones actuales	= 17
Segmentos recibidos	= 3316
Segmentos enviados	= 3313
Segmentos retransmitidos	= 3

Estadísticas UDP

Datagramas recibidos	= 9
Sin puerto	= 291
Errores de recepción	= 0
Datagramas enviados	= 9

2.1.5 Utilizando el comando IPCONFIG

Con este comando, nosotros tenemos la posibilidad de revisar si nuestra dirección IP es la correcta, también tenemos la posibilidad de liberar la dirección para que cualquier otra computadora pueda tomar esa dirección, así como también podríamos desear cambiar la dirección que tenemos, por lo que podríamos solicitar otra dirección si es que estamos como cliente DHCP o bien nosotros mismos podremos indicarle que dirección va a tomar.

Formato y parámetros a utilizar con el comando ping:

```
ipconfig [/? | /all | /release [adapter] | /renew [adaptador]
| /flushdns | /registerdns
| /showclassid adaptador
| /setclassid adaptador [classidtoreset ]
```

Descripción de los parámetros:

<i>/all</i>	Muestra toda la información de configuración.
<i>/release</i>	Libera la dirección IP para el adaptador especificado.
<i>/renew</i>	Renueva la dirección IP para el adaptador especificado.

<code>/flushdns</code>	Purga la <i>cach</i> , de resolución de DNS.
<code>/registerdns</code>	Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS
<code>/displaydns</code>	Muestra el contenido de la <i>cach</i> , de resolución de DNS.
<code>/showclassid</code>	Muestra todos los Id. de clase DHCP permitidos para el adaptador.
<code>/setclassid</code>	Modifica el Id. de clase DHCP.

Cuando no se coloca ningún parámetro, la información que se muestra es la dirección IP, la máscara de subred y la puerta de enlace que se tiene por cada adaptador.

2.1.6 Utilizar el comando TRACERT

Con este comando podrá determinar cual es la ruta que sigue los paquetes que enviamos a una dirección destino. El comando muestra el conjunto de enrutadores IP por donde va pasando nuestro paquete por lo que podrá determinar si hay alguna estación intermedia dañada. Otra característica que tiene este comando es que muestra el tiempo que se tarda el paquete en cada uno de los enrutadores por donde va pasando. Si el paquete que se envió no llega al destino al que se quería enviar, por lo menos podemos ver cual fue el último enrutador al que llego, con lo que podemos identificar a que enrutador es al que no se pudo llegar o a partir de cual no se envió el paquete determinando donde se encuentran los posibles problemas para realizar la conexión con la estación que se quiere alcanzar.

Formato y parámetros a utilizar con el comando ping:

```
tracert [-d] [-h saltosMáximos] [-j listaDeHosts] [-w tiempoDeEspera]
nombreDeDestino
```

Descripción de los parámetros:

- d La ruta de acceso del enrutador se muestra más rápidamente, ya que no se intenta resolver los nombres de los enrutadores en la ruta de acceso.
- h *saltosMáximos* Le indica cual es el número de saltos máximos que se deben buscar para el destino

-j *listaDeHosts* Especifica la ruta de origen no estricta a lo largo de la lista de equipos.

-w *tiempoDeEspera* Sirve para indicarle cual será el número de milisegundos en cada respuesta.

nombreDeDestino Es el nombre o dirección IP de la estación destino.

La forma en que trabaja este comando es la siguiente:

1. Primero se envían una serie de paquetes de eco del Protocolo de control de mensajes Internet (ICMP, *Internet Control Message Protocol*) con valores variables de tiempo de vida IP (TTL) al destino.
2. Cada enrutador que se encuentra dentro de la ruta que sigue el mensaje disminuirá el valor TTL del paquete en al menos 1 antes de poder reenviarlo.
3. Al momento de que el valor de TTL del paquete llega a ser 0, el enrutador donde se encuentra ya no lo reenvía, sino que devuelve el mensaje ICMP "Tiempo agotado" al equipo de origen.

2.1.7 Utilizar el comando ROUTE

Con este comando podrá tener un control de la tabla de enrutamiento, por lo que podrá ver la tabla de enrutamiento, también podrá eliminar cualquiera de las rutas que existen en la tabla o si lo quiere podrá agregar una ruta a ella. Algo que hay que tomar muy en cuenta para poder utilizar este comando, es que solo funciona si tiene instalado el protocolo TCP/IP.

Formato y parámetros a utilizar con el comando ping:

route [-f] [-p] [*comando* [*destino*] [*mask* máscaraSubred] [*puertaDeEnlace*] [*metric métrica*]]

Descripción de los parámetros:

-f Borra las tablas de enrutamiento de todas las entradas de puerta de enlace o *gateway*. Si se utiliza junto con alguno de los comandos, las tablas se borrarán antes de la ejecución de éste.

-p Normalmente es utilizado junto con el parámetro *add*. El parámetro -p es utilizado para indicar que la ruta que se esta agregando es del tipo persistente, es decir que aunque se reinicie el sistema, esta ruta siempre aparecerá.

También se puede utilizar con el parámetro *print*, para mostrar la lista de rutas persistentes registradas.

comando

Comando	Propósito
<i>Print</i>	Imprime un camino
<i>Add</i>	Agrega un camino
<i>Delete</i>	Elimina un camino
<i>change</i>	Modifica el camino existente

destino Especifica el *host* al cual se enviará el comando. Se puede utilizar tanto el nombre de *host* como la dirección *IP*.

mask máscaraSubred Especifica una máscara de subred a asociar con esta entrada de camino. Si no se especifica, se utiliza 255.255.255.255.

puertaDeEnlace Especifica una dirección *IP* o nombre de *host*, el cual corresponde a el enrutador o puerta de enlace que se estará utilizando para el reenvío.

metric métrica Asigna una medida de costo (que va desde 1 hasta 9999) para utilizarla para calcular las rutas más rápidas, más confiables o menos costosas. Por *default* utiliza 1.

Ejemplo de cómo agregar una ruta estática:

Se tiene la red 192.168.10.0 con una máscara 255.0.0.0, y se tiene una puerta de enlace 10.0.0.1.

```
route add 192.168.10.0 mask 255.0.0.0 10.0.0.1
```

Ejemplo de cómo mostrar la tabla de enrutamiento:

Se tiene la siguiente configuración

- Dirección IP: 192.168.10.1
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada: 192.168.10.3

=====
ILista de interfaces

0x1 MS TCP Loopback interface

0x2...00 00 21 6a be 48 Realtek RTL8029(AS) Ethernet
 Adapt=====

Rutas activas:

Tabla I. Descripción de rutas.

Descripción	Destino de red	Máscara de red	Puerta de acceso	Interfaz	Métrica
Ruta predeterminada	0.0.0.0	0.0.0.0	192.168.10.3	192.168.10.1	1
Red de bucle invertido	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
Red local	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.1	1
Dirección IP local	192.168.10.1	255.255.255.255	127.0.0.1	127.0.0.1	1
	192.168.10.255	255.255.255.255	192.168.10.1	192.168.10.1	1
Direcciones de multidifusión	224.0.0.0	224.0.0.0	192.168.10.1	192.168.10.1	1
Dirección de difusión limitada	255.255.255.255	255.255.255.255	192.168.10.1	192.168.10.1	1

Puerta de enlace predeterminada: 192.168.10.3

Nota

- La primera columna no se muestra al momento de ejecutar la instrucción *route print*.

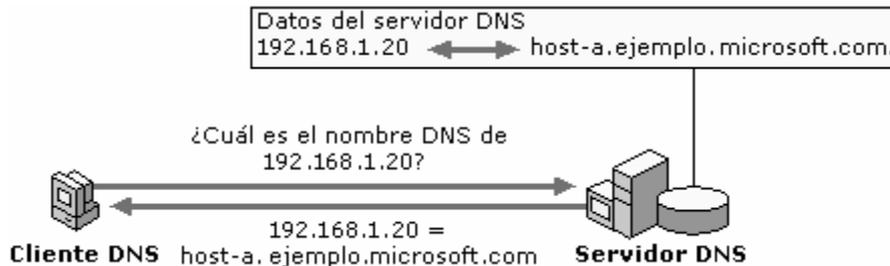
Cuando trata de comunicarse con un determinado *hosts*, el equipo busca dentro de la tabla de enrutamiento del equipo la dirección que más se le parezca a la dirección que especifiquemos, pero si no encuentra una ruta que coincida, esta dirección es enviada por la puerta de enlace predeterminada de un enrutador en la subred local.

Desde un enrutador se pueden enviar datagramas a otros enrutadores o a otras subredes, ya que en el se tiene información acerca de los identificadores de red de las demás subredes. El datagrama puede ir viajando de enrutador en enrutador hasta llegar finalmente a un enrutador que tenga comunicación con el *host* o subred de destino.

2.1.8 Utilizar el comando NSLOOKUP

El comando nslookup puede ayudarnos a comprobar que se puede obtener y resolver nombres *DNS*.

Figura 14. Resolución de nombres DNS



También podrá ver información de los servidores DNS (Sistema de nombres de dominio), tales como registros, alias y servicios.

Nslookup tiene dos modos: interactivo y no interactivo.

Cuando se trata de buscar solo un fragmento de datos, se debe utilizar el modo no interactivo, si en caso se deseará buscar más de un fragmento se utiliza el modo interactivo.

NSLOOKUP recibe dos argumentos, el primer argumento que recibe es el nombre o dirección IP del equipo a buscar; el segundo argumento que es opcional, es el nombre o dirección IP del servidor de nombres DNS, si no se coloca el segundo argumento se utiliza el servidor predeterminado.

Ejemplo:

```
C:\>nslookup libreria.com
Servidor: localhost
Address: 127.0.0.1
Nombre: libreria.com
Address: 192.168.10.1
```

Para utilizar el modo interactivo, se pueden utilizar los mismos dos argumentos del modo no interactivo, con la excepción que su uso puede ser opcionales, es decir, que se pueden omitir ambos.

Si se utiliza el primer argumento, se tiene que escribir un guión (-) antes del nombre o dirección IP del equipo a buscar. El segundo argumento también viene siendo opcional colocarlo, pero si se coloca también tendrá que llevar un guión antepuesto.

Formato y parámetros a utilizar con el comando *ping*:

nslookup [-*opción ...*] [*equipoBuscado* | - [*servidor*]]

Descripción de los parámetros:

-opción... Especifica uno o varios comandos nslookup como una opción de la línea de comandos. Cada opción consta de un guión (-) inmediatamente seguido del nombre del comando y, a veces, de un signo de igual (=) y después un valor.

Entre los comandos que se pueden utilizar están: *Help, exit, finger, ls, lserver, root, server, set, set all, set cl[ass], set view.*

equipoBuscado Mostrar información de *equipoBuscado* mediante el servidor predeterminado actual o mediante *servidor* si se especifica. Si lo que se desea es buscar un equipo que se encuentra fuera del dominio DNS actual, lo único que tendrá que hacer es anexar un punto al nombre.

Si escribe un guión (-) en lugar de *equipoBuscado*, el símbolo del sistema cambia al modo interactivo de nslookup.

servidor Sirve para indicar cual es nombre del servidor de nombres DNS.

También hay que tomar en cuenta que la línea de comandos no debe ser mayor de 256 caracteres.

A continuación se presentan varias cosas que se deben tomar en cuenta al momento de utilizar nslookup en modo interactivo.

1. Se debe presionar CTRL+B para interrumpir los comandos interactivos en cualquier momento.
2. Para salir se debe escribir *exit* .
3. La longitud máxima de la línea de comandos es 256 caracteres.
4. Cuando se esta utilizando un nombre de equipo que es igual a uno de los comandos que están integrados con el comando nslookup, se le debe anteponer el carácter (\).

5. Un comando no reconocido se interpreta como un nombre de equipo.

Entre los posibles errores que pueden presentarse al ejecutar el comando están:

- Tiempo de espera agotado

Se muestra cuando el tiempo que tiene especificado ha terminado y no recibió respuesta del servidor buscado. El tiempo se puede establecer utilizando en comando *set timeout=valor*.

- No hay respuesta del servidor

Indica que no existe ningún servidor DNS en el equipo o que el servidor DNS no se esta ejecutando.

- No hay registros

No se encontró ningún registro para ese equipo de lo que se esta solicitando en la consulta.

- Dominio inexistente

No existe el equipo o el nombre del dominio DNS.

- Conexión rechazada

No se puede establecer una comunicación con el servidor DNS o con el servidor *finger*.

Este error suele producirse en las peticiones *ls* y *finger*.

- Error del servidor

Se da cuando no se puede devolver una respuesta valida a causa de alguna incoherencia que exista en la base de datos.

- Rechazada

El servidor de nombres DNS no aceptó dar servicio a la petición.

- Error de formato

Esto se muestra a causa de alguna instrucción mal escrita o que no sigue el formato que se establece con el comando.

2.2 Utilidades de *Windows NT*

Entre las utilidades para diagnosticar nuestra red que proporcionan nuestro sistema operativo (*Windows NT*, 2000), están:

- *Registry Editor*
- *Network Monitor*

2.2.1 Utilizar el comando REGEDIT

Es una base de datos donde se almacena la configuración de *hardware* y *software* de la computadora actual, esta información es la utilizada para controlar el sistema operativo, provee la información de inicialización de aplicaciones y carga de componentes tales como *drivers* de dispositivos y protocolos de red.

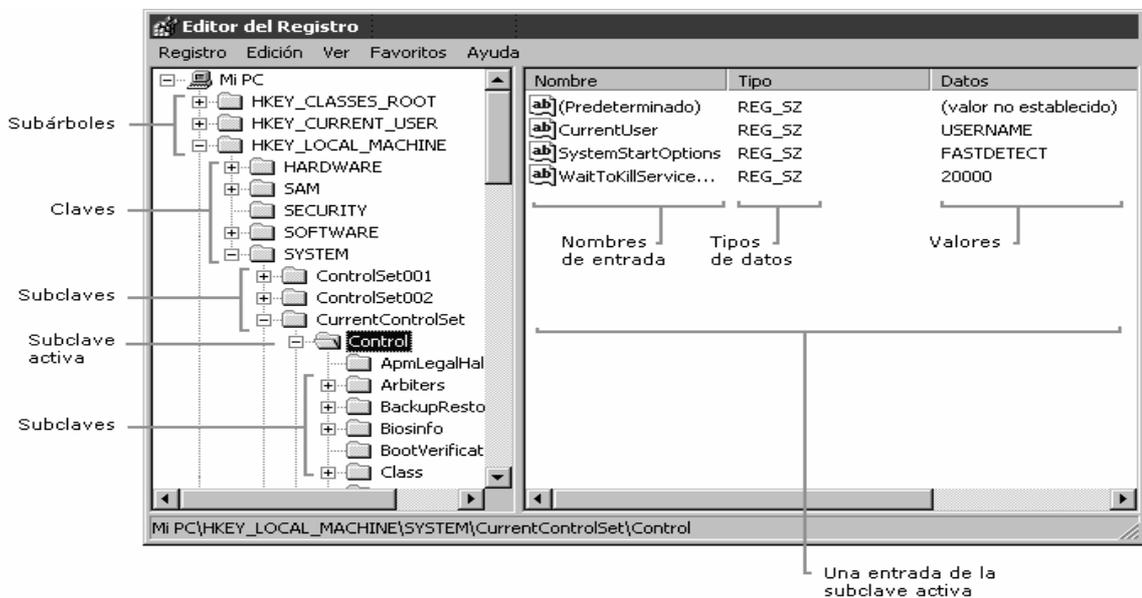
Entre la información contenida dentro del Registro están:

- Los perfiles de cada usuario.
- Los programas instalados en el equipo y los tipos de documento que puede crear cada programa.
- La configuración de propiedades de los iconos de carpetas y programas.
- El *hardware* presente en el sistema.
- Los puertos en uso.

El registro se encuentra organizado por niveles.

A continuación se muestra como esta organizado el registro.

Figura 15. Editor de Registro



Algunas claves son permanentes y otras se sobrescriben al momento de iniciar el sistema operativo.

A continuación se muestra la lista de subárboles que forman el registro:

Tabla II. Registro de *Windows*

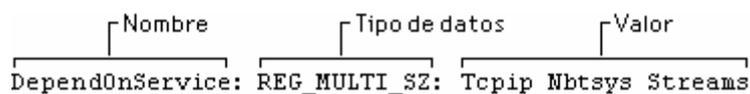
Nombre de la clave raíz	Descripción
HKEY_LOCAL_MACHINE	Contiene tiene la información acerca de la computadora local, esta información es usada por las aplicaciones, <i>drivers</i> y el sistema operativo para configurar la computadora.
HKEY_CLASSES_ROOT	Mantiene información acerca de la asociación de datos con los objetos COM.
HKEY_CURRENT_USER	Tiene toda la información del usuario logeado actualmente en el sistema. Se almacena una copia para cada usuario que se haya logeado en la computadora.
HKEY_USERS	Contiene información acerca de los perfiles de usuario activos cargados y del perfil predeterminado. Sus perfiles se cargan en el Registro de sus propios equipos.
HKEY_CURRENT_CONFIG	Contiene información sobre el perfil de <i>hardware</i> que utiliza el equipo local al iniciarse. Esta información se usa para configurar opciones tales como los controladores de dispositivo y la resolución de pantalla que se va a utilizar. Esta información es extraída de las llaves <i>software</i> y <i>system</i> del subárbol HKEY_LOCAL_MACHINE.

Entradas de valor de las claves de Registro

Una entrada de valor tiene tres partes: el nombre del valor, el tipo de datos del valor y el propio valor. Los datos que reciben las claves reciben el nombre de entradas de valor.

El orden que siguen las entradas de valor es la siguiente:

Figura 16. Claves del registro de *Windows*.



3 TÉCNICAS PARA LA SOLUCIÓN DE PROBLEMAS

En la actualidad ya existen una serie de herramientas que permiten determinar si existe algún problema en la red, pero muchas veces no se cuenta con el suficiente dinero para comprarlas, es por eso que algunas veces es mejor recurrir a los manuales o a la experiencia, para buscar donde se encuentran los errores e intentar resolverlos.

3.1 Protocolos de internet

Todos los protocolos controlan unas reglas que determinan como será que se realice la conexión de un *host* a otro, es decir, como será la conexión TCP a un puerto determinado del *host* receptor. Este tipo de conexión requiere que haya una sesión para poder transmitir y recibir datos, para posteriormente poder utilizar los comandos que ayudarán a enviar y recibir datos.

La siguiente tabla muestra una lista de protocolos con los puertos TCP que utilizan para escuchar.

Tabla III. Protocolos y los puertos que escuchan.

Protocolo	Puerto
<i>SMTP</i>	25
<i>HTTP</i>	80
<i>TNP</i>	119
<i>LDAP</i>	389
<i>POP3</i>	110
<i>IMAP4</i>	143

Primero que nada tendríamos que determinar si la conexión es correcta, esto lo podemos averiguar mediante el comando telnet hacia el puerto que queramos revisar. La sintaxis que utiliza telnet es la siguiente:

telnet direcciónIP puerto

Al ejecutar este comando hacia una dirección y puerto específico, se mostrará una ventana de Telnet y un mensaje indicando que la conexión es correcta, lo que indica que el *host* está escuchando por el puerto indicado y que podrá enviar mensajes al *host*, pero aquí no se acaba la revisión, ya que pueden existir problemas durante la utilización de alguno de los comandos utilizados, por lo que habría que revisar las respuestas recibidas al utilizar algunos comandos.

Para realizar esta prueba tendremos ejecutar los comandos hacia el *host*, por medio del comando telnet. Ahora se tiene el problema de que comandos son los que puedo enviar o que es lo que el programa cliente-servidor está intentando enviar. El problema es si es que no puede ver lo que el *host* está enviando, sino que solo ve las respuestas típicas.

Ejemplo 1: comprobando la conexión *SMTP* con un *host*.

A continuación se muestra un ejemplo de una sesión típica de Telnet para un *host SMTP* (telnet al puerto 25 del *host*).

```
telnet 10.10.1.1 25
```

1. Se ejecuta *HELO* y si el servidor responde, indica que comprende y acepta el comando.
2. *MAIL FROM* indica al *host* quién está enviando el mensaje. De nuevo, el servidor responde correctamente.
3. *RCPT TO* indica al *host* a quién debe entregar este mensaje.

Ejemplo 2: comprobando la conexión *POP3*.

- El comando *USER*, seguido del identificador de inicio de sesión, se utiliza para iniciar una sesión en el buzón de *POP3*.
- El comando *PASS* emite la contraseña para obtener acceso.
- *Exchange Server* devuelve "+OK User successfully logged on".

Si los siguientes pasos no devuelven ningún error, se puede decir que no se tienen problemas en esos protocolos de internet.

3.1.1 Descripción general de los comandos y las respuestas de los protocolos

La tabla que a continuación se muestra, tiene especificaciones de los comandos utilizados en telnet, así como la respuesta que deberían devolver.

3.1.1.1 SMTP

Tabla IV. Comandos de SMTP

Comandos	Respuesta esperada	Descripción
<i>HELO</i>	250 <i>OK</i>	Inicia la conversación entre los <i>hosts</i> .
<i>MAIL</i> FROM: <usuario@dominio.tld>	250 <i>OK</i>	Identifica quién envía el mensaje.
<i>RCPT</i> TO: <usuario@dominio.tld>	250 <i>OK</i>	Identifica a quién va dirigido el mensaje.
<i>DATA</i>	354 <i>Send Data</i>	Identifica el punto de inicio de los datos del mensaje.
. (un único punto)	250 <i>OK</i>	Identifica el punto de finalización de los datos del mensaje.
<i>QUIT</i>	221	Termina la sesión.

3.1.1.2 POP3

Tabla V. Comandos de POP3

Comandos	Respuesta esperada	Descripción
<i>USER</i> <i>dominioNT/cuentaNT/alias</i>	+ <i>OK</i>	Inicia el proceso de autenticación.
<i>PASS contraseñaNT</i>	+ <i>OK</i>	Especifica la contraseña para la cuenta de <i>Windows NT</i> .
<i>LIST</i>	+ <i>OK</i>	Enumera los mensajes disponibles para descargar.
<i>RETR mensajeNº</i>	Texto del mensaje	Recupera el texto del mensaje con ese número.
<i>DELE mensajeNº</i>	+ <i>OK</i>	Elimina el mensaje con ese número.
<i>QUIT</i>	+ <i>OK</i>	Termina la sesión.

3.1.1.3 IMAP4

Cuando se refiere al protocolo IMAP, este tiene que tener precedido un identificador de comando. Por ejemplo, cuando el cliente IMAP emite *local SELECT inbox*, el servidor responde con *local OK*.

Tabla VI. Comandos de IMAP4

Comandos	Respuesta esperada	Descripción
<i>LOGIN dominioNT/cuentaNT/alias contraseña</i>	<i>OK LOGIN</i>	Inicia una sesión en el buzón.
<i>SELECT carpeta</i>	Modo de carpeta y <i>OK SELECT</i>	Selecciona una carpeta para su presentación.
<i>FETCH mensajeNº</i>	Texto del mensaje y <i>OK FETCH</i>	Recupera el mensaje por <i>mensajeNº</i> .
<i>STORE indicadoresMensajes \indicador</i>	<i>OK STORE</i>	Marca un mensaje para su eliminación o como leído/no leído.
<i>EXPUNGE</i>	<i>OK</i>	Elimina todos los mensajes marcados.
<i>LOGOUT</i>	<i>OK</i>	Termina la sesión.

Cuando alguno de los comandos no es aceptado, la respuesta recibida es NO.

3.1.1.4 NNTP

Hay dos modos de acceso a NNTP: autenticado y anónimo. La autenticación requiere los dos primeros comandos enumerados.

Tabla VII. Comandos de NNTP

Comandos	Respuesta esperada	Descripción
<i>NEWGROUPS fecha hora</i>	Lista de grupos	Dame una lista de grupos de noticias después de fecha/hora.
<i>NEWGROUPS grupos fecha hora</i>	Lista de artículos	Dame una lista de artículos nuevos de los grupos especificados.
<i>POST</i>	340	Tengo un artículo para ti que se publico aquí.
<i>IHAVE id</i>	435 <i>Accepted.</i>	Tengo id de artículo ¿Lo quieres?
<i>AUTHINFO USER dominioNT/cuentaNT/nombreUsua rio</i>	381 <i>More Info Needed</i>	Proporciona información de autenticación.
<i>AUTHINFO PASS contraseña</i>	281 <i>Accepted.</i>	Proporciona la contraseña para la autenticación.
<i>LIST</i>	Lista de grupos	Enumera todos los grupos disponibles.
<i>GROUP grupo</i>	Especificaciones de grupo	Establece el grupo actual.
<i>ARTICLE id</i>	Texto del artículo	Recupera un artículo por <i>Nº</i> .
<i>QUIT</i>	205	Termina la sesión.

3.2 Comprobación de *hardware*:

En este capítulo se tratará de dar una referencia de algunas técnicas que podrán ser de mucha utilidad al momento de querer comprobar el funcionamiento de algunos componentes utilizados en la red.

3.2.1 Enrutador

Hay mucho que decir acerca de un enrutador y su forma de trabajar, pero en esta sección solo se mostrará problemas que se pueden presentar al momento de arrancarlo. Antes de mostrar algunos de los problemas que se pueden presentar, hay que mencionar que la mayoría de enrutadores tienen varias formas de arrancar, entre las que se encuentran:

- Arranque desde la red: un enrutador tiene la posibilidad de arrancar desde un servidor que utilice el TFPT (Protocolo Trivial de Transferencia de Archivos), MOP (Protocolo de Operación de Mantenimiento) DEC, o el RCP (Protocolo de Copia Remota) utilizando cualquiera de los medios que maneje (como *Ethernet*, *Token Ring*, *FDI*, *HSSI* y líneas seriales).
- Memoria Flash: la memoria es un medio de almacenamiento no volátil (que no se perderá al momento de que se apague), la cual puede ser borrada y reprogramada de manera eléctrica.
- ROM: la mayoría de enrutadores tienen un tipo de memoria que es solo de lectura (ROM), la cual le puede servir para arrancar su sistema.
- Tarjeta de memoria PC *Flash*: los enrutadores también tienen la opción de arrancar por medio de una tarjeta que puede ser removible, “Tarjeta de Memoria PC *Flash*”.

Para reducir el impacto de las fallas es recomendable que el enrutador tenga una secuencia de arranque, a continuación se presenta la secuencia que más se recomienda:

1. Arrancar una imagen desde la memoria *Flash*
2. Arrancar una imagen utilizando un arranque desde red
3. Arrancar desde una imagen ROM

Ahora, se preguntará como se hace esto, las líneas que abajo se presentan realizan esta secuencia de arranque.

```
goriot# configure terminal
```

Escriba los siguientes comandos, uno por línea. Termine con CTRL+Z

```
goriot(config)# boot system flash gsxx
```

```
goriot(config)# boot system gsxx 131.108.1.101
```

```
goriot(config)# boot system rom
```

```
goriot(config)# ^Z
```

```
goriot#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
goriot# copy running-running startup-config
```

```
[ok]
```

```
goriot#
```

De esta forma su enrutador tendrá tres fuentes desde las cuales podrá arrancar: memoria *Flash*, desde la red y ROM.

A continuación se presentan una serie de síntomas que ocurren con mayor probabilidad al arranque un enrutador:

- El enrutador no puede arrancar desde la red con un servidor TFTP
- El enrutador no puede arrancar desde la red con otro enrutador
- Los tiempos de espera agotados y paquetes en desorden impiden el arranque desde la red
- El cliente ARP indica tiempo de espera agotado durante el arranque desde la red

Resolución de problemas

Antes de comenzar a hablar acerca de soluciones, hay que recordar que es lo que debe de ocurrir al momento de encender un enrutador:

- Se debe de encender un *LED* y permanecer encendido mientras este recibiendo corriente.
- El ventilador interno del enrutador debe estar operando.
- Los *LEDs RSP* y Normal que se encuentran en la parte frontal tienen que estar encendidos durante la operación, el *LED CPU Halt* debe estar apagado.

- También debe encenderse el *LED Enabled* de cada procesador de interfaz, esto indica que *RSP* terminó la inicialización de dicho procesador.

A continuación se presentan una serie de posibles soluciones para los síntomas que se mencionaron anteriormente.

3.2.1.1 El enrutador no puede arrancar desde la red con un servidor TFTP

Este problema suele dar cuando se trata de arrancar desde una red.

La red está desconectada o aislada:

1. Trata de arrancar desde la ROM o desde la memoria *Flash*.
2. Ejecute el comando **ping 255.255.255.255**.
3. Si la ejecución del anterior comando no dio respuesta, entonces utilice el comando **show arp** para buscar en la tabla alguna entrada que esté asociada con el servidor.
4. Ejecute el comando **show ip route** para buscar alguna entrada de la red o subred del servidor.

Si existe alguna entrada del servidor, no se tiene el problema de una red desconectada. Por el contrario, sino existe dicha entrada, asegúrese de agregarla antes de volver a arrancar desde la red.

No está operando el servidor TFTP

1. Intente realizar una conexión TFTP desde el servidor de arranque hacia sí mismo, con el fin de determinar si el servidor TFTP está operando, por lo que se tendría éxito si esta operación da resultado.
2. Si la operación anterior no da resultado, inicialícelo.

Dirección de protocolo errónea

1. Revise la dirección *IP* del *host* dentro del archivo de configuración del servidor, para asegurarse que este bien.
2. Si la dirección no es correcta, cambie la configuración.

Especificación incorrecta del registro de configuración

Primero que nada se debe especificar la forma en que se quiere arrancar en el registro de configuración. La configuración para el arranque desde la red depende de la plataforma que se esté arrancando.

1. Revise la especificación de configuración de su sistema.

2. Especifique la forma en que desea arrancar, manual o automática con un servidor TFTP.

Cuando en el registro de configuración se establece 0x0, le estaremos diciendo que la forma en que queremos arrancar es de forma manual, en caso de no especificar esto, el sistema se arrancará utilizando el nombre de imagen predeterminado o la especificada por el comando *boot system*.

3.2.1.2 El enrutador no puede arrancar desde la red con otro enrutador

Falta o está incorrecto el comando de configuración tftp-server

1. Ejecute el comando *show running-config*, con lo que podrá observar si falta el comando *tftp-server system* o si esta especificado en forma errónea.
2. Agregue o modifique el comando de configuración en el servidor TFTP. Asegúrese de especificar el nombre de un archivo en la memoria Flash.

Imagen incompleta en la memoria Flash

Para determinar si la imagen esta incompleta se puede utilizar el comando *show flash*, este comando muestra información de si se elimino la imagen y la razones.

1. El mensaje que se muestra cuando el enrutador intenta arrancar y encuentra una imagen incorrecta es “*wrong system software*”. En este caso el enrutador se está arrancando desde el ROM.
2. Obtenga la imagen correcta. Para obtener una imagen correcta es mejor dirigirse con su representante de soporte técnico.
3. Luego de obtener la imagen correcta, el siguiente paso sería el de utilizar el comando *copy tftp flash* para recuperarla.

3.2.1.3 Los tiempos de espera agotados y paquetes en desorden impiden el arranque desde la red

Cuando sucede este error, se podría arrancar el enrutador cliente, pero si se presentan demasiados tiempos de espera agotados y paquetes en desorden, es probable que hay un problema en la red y el arranque podría ser inconsistente.

El enlace está saturado

1. Arranque desde la ROM y ejecute un ping hacia el servidor TFTP para determinar si aparecen tiempos de espera agotados y paquetes en desorden.
2. Revisar en los concentradores de red local si hay colisiones.
3. Utilice el comando ***show interface*** para buscar si hay paquetes descartados y errores de salida.
4. Si se da que 15% o más del tráfico esta siendo descartado o si ocurre cualquier error de salida, el problema podría ser el congestionamiento.
5. Antes de intentar arrancar el enrutador, espere a que se calmé el tráfico. Si se tiene que es grave el problema, una solución sería aumentar el ancho de banda o acercar el servidor al enrutador que está arrancando.

Se pierde el enlace

1. Utilice los comandos ping o trace para revisar la trayectoria de los paquetes desde el enrutador que está arrancando hacia el servidor de arranque.
2. Si se encuentra un problema, repare el enlace e intente de nuevo arrancar desde la red.

3.2.1.4 El cliente ARP indica tiempo de espera agotado durante el arranque desde la red

Cuando el enrutador no recibe una respuesta ARP, se muestra el mensaje “*Booting gs3-bfx.....[timed out]*”

Los enrutadores intermedios tienen activado un filtrado ARP

1. Arranque desde la ROM.
2. Pruebe hacer un **ping** hacia el servidor, asegurándose de que dio resultados correctos.
3. Pruebe la conectividad utilizando el comando ***copy running-running tftp***.

4. Si hasta el momento todos los comandos no le han dado errores, utilice el comando *show arp*, para revisar la configuración del enrutador intermedio.
5. Revise que se este generando respuestas *proxy* utilizando el comando *debug arp*.
6. Especifique una puerta de enlace predeterminada utilizando el comando *ip default-gateway*.

La tabla que se presenta a continuación presenta otras cosas que también deben ser tomadas muy en cuenta al momento de realizar un análisis acerca del funcionamiento de un enrutador.

Procesador

- Que este funcionando el ventilador y que estén encendidos los *LEDs* de los módulos del procesador.
- Interruptor encendido.
- El cable de corriente funcione correctamente.

Enfriamiento

- Que arranque el ventilador.
- Que se mantenga funcionando el ventilador mientras todo el proceso.
- Si el sistema no detectó sobrecalentamiento dentro del chasis.
- Que no este recibiendo aire caliente procedente de algún otro equipo.
- Que la tarjeta de control del ventilador esté insertada correctamente.

Red

- Si el sistema no reconoce alguna de las interfaces de red.
- La conexión de cable de la interfaz de red.
- El cable de conexión a la interfaz.

3.2.2 Cableado

En lo que respecta al cableado en redes de computadoras, simplemente se hablara de cómo es que afecta en la transmisión de la información y por que, sin adentrarse en como es que se debería de realizar las conexiones, dando además algunas características que ayudarán a determinar si el tipo de cable que estamos utilizando es correctas y adecuado para el tipo de red que tenemos.

Hay veces que la persona encargada del cableado, simplemente echan mano de los cables que tenga o los que sean más baratos, sin tomar en cuenta que esto le puede causar dificultades al momento de utilizar la red. Muchas de las veces se utiliza el cable sin tomar en cuenta que en algunos casos se necesita de mayor protección que en otros, o sin tomar en cuenta que los cables tienen un distancia a la que pueden llevar la los datos que queremos enviar.

También hay que tomar en cuenta que los cables trabajan por medio de variaciones de voltajes o corrientes, y que al momento de estar muy cerca de alguna fuente de energía, puede llegar a perder información.

Otra de las características que se tiene que revisar es la cantidad de nodos que pueden estar conectados, ya que si se excede de la cantidad limite que tiene cada cable, puede que la transmisión de la información no se realice de la mejor forma posible, y hasta puede llegarse a dar que la información sea inconsistente.

3.2.2.1. Longitud:

Para ayudar a determinar si el problema que se tiene es debido a la longitud de cable que se esta utilizando, a continuación se presenta una tabla que muestra distintos tipos de cables, los conectores que se deberían de utilizar con estos cables y la distancia máxima promedio que se puede utilizar, no queriendo decir con ello que estos cables tienen la limitante de que solo se pueden utilizar para cablear redes donde los nodos tienen que estar cerca, ya que aparatos que pueden retransmitir la señal que viene en cualquiera de estos cables.

Tabla VIII. Distancia máxima promedio de los cables y sus conectores.

Denominación	Cable	Pares	Duplex	Conectores	Distancia
10BASE5	Coaxial grueso	1	No	'N'	500 m
10BASE2	RG 58	1	No	BNC	185 m
10BASE-T	UTP cat. 3	2	Sí	RJ-45	100 m
10BASE-T	UTP cat. 5	2	Sí	RJ-45	150 m*
100BASE-TX	UTP cat. 5	2	Sí	RJ-45	100 m
100BASE-TX	STP	2	Sí	9 pin D sub.	100 m
100BASE-T4	UTP cat. 3	4	No	RJ-45	100 m
100BASE-T2	UTP cat. 3	2	Sí	RJ-45	100 m
1000BASE-CX	STP	2	Sí	8 pin SHCD o 9 pin D sub.	25 m
1000BASE-T (prev. mar.99)	UTP cat. 5	4	Sí	RJ-45	100 m

* La longitud máxima del cable UTP-5 según las normativas de cableado estructurado es 100 m, pero la norma 802.3 permite un alcance de 150 m cuando se utiliza 10BASE-T con cable categoría 5.

Una variante que se encuentra es al utilizar cables de Fibra Óptica, ya que este tipo de cable tiene un mejor desempeño que los cables de cobre, pero tiene la inconveniencia de ser más caro. La tabla siguiente resume las principales características de todos los medios de fibra óptica actualmente utilizados, y sus alcances.

Tabla IX. Cables de fibra óptica, conectores y distancia máxima promedio.

Medio	Ventana	Luz	Fibra	Conector	Distancia
10BASE-FL	1 ^a	Normal	62,5/125	ST	2 Km
100BASE-FX	2 ^a	Normal	62,5/125	SC	2 Km
100BASE-SX (propuesto)	1 ^a	Láser	62,5/125 50/125	SC o ST	500 m 500 m
1000BASE-SX	1 ^a	Láser	62,5/125 50/125	SC	275 m 550 m
1000BASE-LX	2 ^a	Láser	62,5/125 50/125 9/125	SC	550 m 550 m 5 Km

3.2.2.2. Atenuación

La atenuación no es más que pérdida de potencia conforme la señal se propaga hacia su destino. Este tipo de problema se puede dar debido a la utilización de conectores y empalmes.

3.2.2.3. Retardo en modo diferencial

Este problema se da cuando la fibra es apreciablemente más ancha que el haz láser que le esta llegando, por lo que la luz va “rebotando” por las paredes durante todo el trayecto. El ensanchamiento de la luz es mayor entre mayor es la distancia que va recorriendo; otro de los detalles que hay que tomar en cuenta es que a mayor velocidad de transmisión, menos ensanchamiento puede tolerarse, ya que el pulso se envolvería con el siguiente.

Este tipo de efecto viene siendo proporcional a la distancia inversamente proporcional a la frecuencia de los pulsos, es decir la velocidad de transmisión.

Un método que le puede ser de mucha utilidad para medir las limitantes de las fibras, es el que se conoce como ancho de banda modal o simplemente ancho de banda, el cual se mide en MHz*Km. Veamos un ejemplo, con un ancho de banda de 1000 MHz*Km podremos enviar como máximo 1 millón de pulsos por segundo a una distancia de 1 Km, o medio millón de pulsos a 2 Km o dos millones a 500 m.

Existen otros factores que influyen en el funcionamiento del ancho de banda de una fibra, estos son:

- Diámetro del núcleo
- Longitud de onda
- Calidad de la fibra

Diámetro del núcleo: entre mayor sea el núcleo, menor será el ancho de banda, esto se debe a que el pulso va más ancho y rebota más.

Longitud de onda: entre mayor sea la longitud de onda, mayor será nuestro ancho de banda, ya que el haz viaja de una forma más ajustada en la fibra.

Calidad de la fibra: las fibras construidas con mayores controles de calidad, tiene un ancho de banda mayor.

Existe un parámetro característico de las fibras que mide esta limitación, que se conoce como ancho de banda modal o simplemente ancho de banda, y se mide en MHz*Km.

Por ejemplo con un ancho de banda de 1000 MHz*Km podremos enviar como máximo 1 millón de pulsos por segundo a una distancia de 1 Km, o medio millón de pulsos a 2 Km o dos millones a 500 m.

Un buen consejo para la elección de un cable de fibra, es mejor escoger el que tenga el mayor ancho de banda posible, para lo cual podrá ver en los catálogos de los fabricantes las especificaciones de con que ancho de banda cuenta cada uno de los cables que venden. Esto puede hacer que aumente el costo, pero esto es despreciable comparándolo con el alcance que se tiene y que podremos usar emisores 100BASE-SX en mas situaciones.

La tabla que a continuación se muestra, contiene especificaciones tales como, el ancho de banda de fibra según los estándares EIA/TIA e ISO/IEC, así como los valores garantizados de algunas de las mejores fibras del mercado.

Tabla X. Ancho de banda de la fibra óptica.

Fibra o estándar	Diámetro (mm)	Ancho de banda 850 nm (MHz*km)	Ancho de banda 1300 nm (MHz*km)
EIA/TIA 568	62,5/125	160 (220m)	500(550 m)
ISO/IEC 11801	62,5/125	200(275 m)	500(550 m)
Alcatel GIGAlite	62,5/125	500	500
BRUGG FG6F	62,5/125	300	1200
ISO/IEC 11801	50/125	200 (275 m)	500 (550 m)
ISO/IEC 11801 (propuesto)	50/125	500 (550 m)	500 (550 m)
ANSI <i>Fibre Channel</i>	50/125	500 (550 m)	500 (550 m)
Alcatel GIGAlite	50/125	700	1200
BRUGG FG5F	50/125	600	1200

La distancia que se encuentra encerrada entre paréntesis, corresponde al alcance máximo en *Gigabit Ethernet*.

3.2.2.4. Fiabilidad

En la actualidad se tiene que una buena instalación de red, puede dar sin problemas una tasa de error de 10^{-12} , lo cual vendría a representar menos de un error por día en una red de 10Mb/s completamente saturada, por lo que los errores de CRC en una red (excepto las inalámbricas) no deberían de existir.

Lo máximo de datos que puede transmitirse por un cable viene determinado por tres factores:

- El ancho de banda del cable (en MHz*Km). En el caso de cable de cobre UTP la longitud máxima es siempre de 100m, por lo que el ancho de banda viene fijado por la frecuencia, es decir la categoría del cable. Por ejemplo el cable categoría 5 (100 MHz) tiene un ancho de banda de 10 MHz*Km.
- El esquema de codificación utilizado. Debido a que en las redes Ethernet, como en todas las redes locales, la transmisión se realiza de manera asíncrona, es decir no hay un reloj maestro que mantenga sincronizados todos los equipos, por este motivo se utiliza una sincronización mediante el uso de códigos que incorporan cierto nivel de redundancia, lo cual es llamado esquema de codificación.
- El número de pares empleados.

Ajustando adecuadamente estos tres parámetros es posible en teoría conseguir cualquier caudal de datos por un cable UTP, si se utilizara un código suficientemente rico. Lógicamente el uso de códigos mas ricos y con más posibles estados requiere una relación señal/ruido mayor, lo cual a su vez supone más silicio en el *transceiver* y un mayor costo de los equipos.

La tabla que se muestra a continuación muestra una serie de códigos utilizados en algunas de las tecnologías de red:

Tabla XI. Tecnologías de red y esquemas de codificación utilizado.

Tipo de red	Velocidad (Mb/s)	Esquema de codificación	Número de pares	Frecuencia Señalizac. (Mbaud.)	Categoría mínima de cable UTP
1BASE-5	1	Manchester	1	2	2
Token Ring	4	Manchester Diferencial	1	8	3
10BASE-T	10	Manchester	1	20	3
100BASE-T4	100	8B/6T	3	25	3
100BASE-T2	100	PAM 5x5	2	25	3
100VG-AnyLAN	100	5B/6B	4	30	3
Token Ring	16	Manchester Diferencial	1	32	3
ATM	25,6	4B/5B	1	32	3
FDDI, 100BASE-X	100	4B/5B	1	125	5
1000BASE-TX	1000	PAM 5x5	4	125	5
ATM	155,52	NRZ	1	155,52	5
1000BASE-X	1000	8B/10B	1	1250	-

Este cálculo se debería hacer para el par de estaciones más distante de la red. Generalmente será necesario hacerlo para varias parejas, ya que en una red compleja no suele ser evidente cual es la que está más distante.

3.2.2.5. Velocidad

El escoger la velocidad con la que se quiere trabajar, muchas veces depende del tipo de aplicaciones y de necesidades.

A nivel de consejo se presenta la siguiente tabla, la cual le ayudará a determinar cual tipo de conexión debería utilizar:

Tabla XII. Equipo a conectar y conexiones aconsejadas.

Equipo a conectar	Tipo de conexión aconsejada
Puesto de trabajo	10BASE-T conmutada <i>full duplex</i> 100BASE-TX conmutada <i>full duplex</i>
Servidor	100BASE-TX conmutada <i>full duplex</i> 2, 3 ó 4 100BASE-X conmutada <i>full duplex (etherchannel, 802.3ad)</i> 1000BASE-TX conmutada <i>full duplex con buffered repeater</i>
Backbone (conmutador- conmutador)	100BASE-X conmutada <i>full duplex</i> 2, 3 ó 4 100BASE-X conmutada <i>full duplex (etherchannel, 802.3ad)</i> 1000BASE-X conmutada <i>full duplex</i> 2, 3 ó 4 1000BASE-X conmutada <i>full duplex (etherchannel, 802.3ad)</i>

3.2.2.6. La colisión

Este tipo de problema se da cuando dos o más estaciones empiezan a enviar simultáneamente o más exactamente cuando lo hacen con una separación menor que el tiempo de ida y vuelta que los separa, en otras palabras se da cuando mas de una estación intenta transmitir al mismo tiempo sobre un mismo cable.

Al momento de que ocurran hasta un total de 16 colisiones sucesivas, el protocolo MAC abandona y reporta el fallo a los niveles superiores, los cuales tomarían la decisión de volver a enviar los datos o abandonar desistir de enviarlos. Cuando se tiene tráfico algo elevado y se transmiten tramas pequeñas, es normal tener cierta proporción de colisiones.

Cuando se dan 16 colisiones sucesivas, es síntoma claro de saturación o problemas físicos, por lo que sería conveniente revisar el cableado, tarjeta de red o el *transceiver* en caso de revisar las partes físicas; mejorar el reparto del tráfico (utilizando conmutadores por ejemplo).

3.2.2.7. Colisión Tardía

Una red *Ethernet* puede estar funcionando normalmente y tener decenas de colisiones por segundo, pero una sola colisión tardía es síntoma de un problema serio en la red que debe ser investigado.

Una colisión tardía se da cuando una estación transmitiendo y luego de los primeros 512 bits, comienza a transmitir una segunda estación, lo cual provocara una colisión, ya que a partir de los primeros 512 bits transmitidos por la primera estación, las demás estaciones tendrían que saber que hay una estación que esta transmitiendo y aquí no se da ese caso. El problema se da a causa de que la segunda estación que esta transmitiendo se encuentra a una distancia mayor a la permitida posiblemente por una topología inválida.

3.3 Mensajes comunes de errores en redes

a) **Alignment Error:** este mensaje puede aparecer al momento de existir una colisión en la red o también cuando hay averías en la interfaz de red. Más exactamente, cuando aparecen en exceso, es debido a que existe algún problema de hardware. A continuación se muestra una formula utilizada para determinar si puede ser problema de hardware.

$$\text{Alignment Errors/Good Frames} * 100 > 0.2\% \text{ problema de hardware}$$

b) **Inter Frame Gap Error:** este mensaje puede aparecer cuando ocurre una colisión, esto ocurre debido a que se tiene una red demasiado grande en cuando a longitud de cable o con demasiados repetidores o *hubs*, o posiblemente por un dispositivo en mal estado (tarjeta de red, repetidores o *hubs*).

c) **FCS Error:** el CRC (*cyclic redundancy check*) del paquete es erróneo. Un FCS (*Frame Check Sequence*) error suele indicar un error *hardware* en la red. La mayoría de las veces, este error proviene del puesto emisor del paquete erróneo o del *hub* dónde va conectado. La tasa de error de este tipo debe mantenerse por debajo del 1 % del total de paquetes buenos. A continuación se muestra la formula utilizada para comprobar la tasa de error de este tipo.

$$\text{FCS Errors/Good Frames} * 100 < 0.1\% \text{ de Good Frames}$$

d) **Data Rate Mismatch:** los datos entrantes no se encuentran en el intervalo de tolerancia de 10 Mhz + o - 0.01 %. Esto suele darse debido a un reloj (*Quarzo*) averiado en el interfaz de red del emisor, el repetidor o el *hub*. Este tipo de error suele desencadenar otros tales como, colisiones, errores CRC, etc. por lo cual es imprescindible sustituir el material averiado lo más pronto posible.

e) **Fragment:** un paquete con un tamaño de entre 2 *bytes* y 64 *bytes*. Tiene un SFD y un FCS erróneo (error CRC). Es generalmente producto de una colisión pero también puede ser producido por algún problema que se tenga en *hardware*. Suelen ocurrir pero no deben pasar del 0.2 % del total de paquetes buenos.

Formula : $\text{Fragments/Good Frames} * 100 < 0.2\%$ de la utilización total

f) **MAU Jabber Lockup Protection (MJLP):** la electrónica del repetidor del *hub* se encuentra bloqueada. El *Hub* no funciona correctamente. Según la norma IEEE 802.3, el *Hub* está diseñado para asegurar que un dispositivo (en este caso el *hub*) no puede enviar flujos de datos erróneos continuos a través de la red. Indica que el repetidor se ha desconectado el mismo de la red con el objetivo de cortar la emisión errónea.

3.4 Utilizando herramientas de diagnóstico

En la actualidad existen una serie de herramientas utilizadas para garantizar el funcionamiento del cableado utilizado en la red, estas herramientas no permiten determinar si existe algún problema en el cableado de una forma rápida y sencilla.

Estas herramientas permiten localizar problemas físicos en la red. Además de llevar a cabo una serie de pruebas a nivel físico, análisis y medidas para reducir el tiempo de inactividad y los gastos correspondientes.

Se ha comprobado a nivel estadístico que más del 80% de los problemas de comunicación provienen de errores en el cableado (conexiones sueltas, circuitos abiertos, cortocircuitos). Las herramientas que se encuentran en el mercado, comprueban los cables, busca posibles errores, muestra la distancia entre cada uno de ellos e identifica los terminadores de conectores que no se han conectado debidamente, además de medir la longitud total y el valor de terminación de la red (resistencia).

Antes resolver un problema de red era un proceso de ensayo y error. Ahora, se ofrece una solución rápida, precisa y económica que ahorra tiempo y problemas.

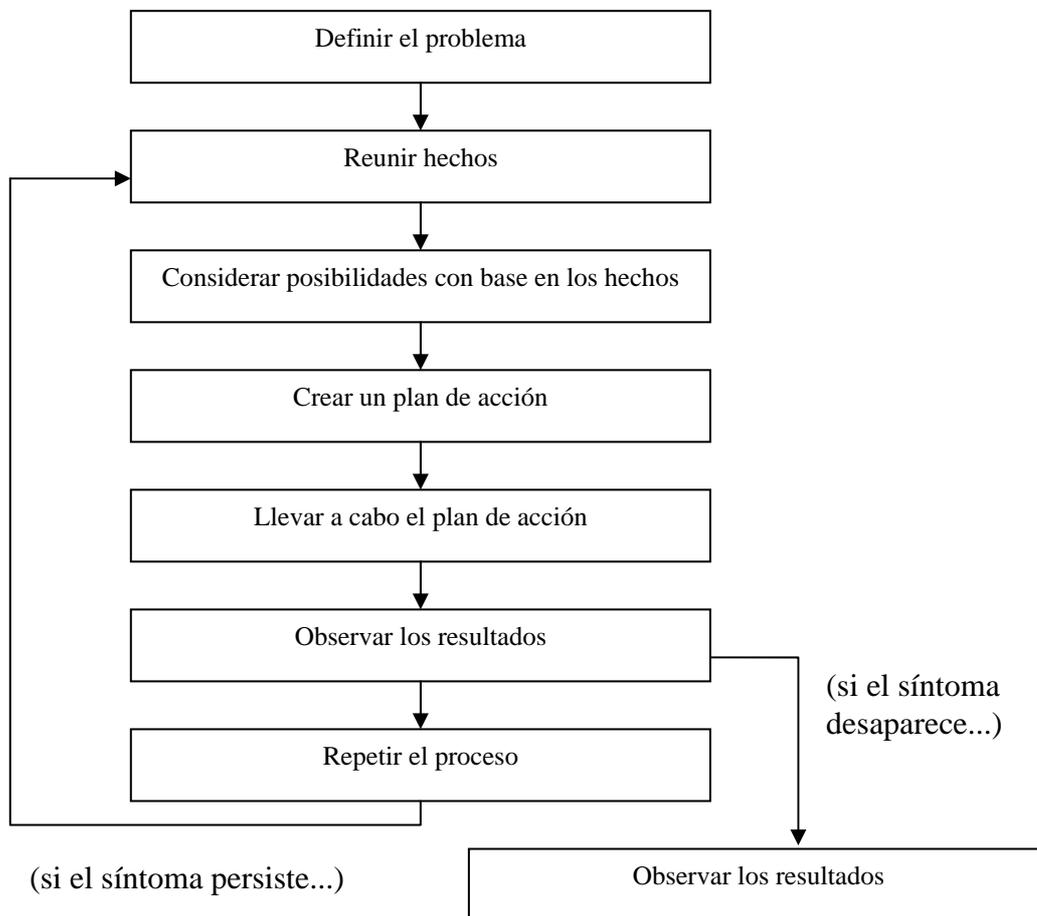
Por lo que ahora se tiene una opción más rápida y segura de encontrar errores, en vez de tener que determinar donde se encuentran estos por simple inspección, experiencia, o cualquier otra cosa.

3.5 Modelo general para la resolución de problemas

Cuando se encuentra solucionando problemas en un entorno de red, la mejor opción es emplear un enfoque sistemático. Defina los síntomas específicos, identifique todos los problemas potenciales que podrían estar causando tales síntomas y luego, elimine cada problema potencial (desde el más probable hasta el menos probable) hasta que desaparezcan los síntomas.

En la siguiente figura se muestra un flujo que no tiene que ser precisamente el que use, pero si que le ayudaría bastante al momento de querer resolver problemas de red.

Figura 17. Diagrama de resolución de problemas.



A continuación se da en una forma más detallada cada uno de los pasos que se mencionan en el diagrama de flujo.

- Paso 1** Al analizar un problema de red, construya un enunciado claro del problema. Debe definir dicho problema en términos de un conjunto de síntomas y causas potenciales.
- Para analizarlo en forma adecuada, identifique los síntomas generales y luego determine que tipo de problemas (causas) podrían dar lugar a esos síntomas.
- Paso 2** Reúna los hechos que necesita para aislar posibles causas.
- Formule preguntas a usuarios afectados, administradores de red, gerentes y otras personas clave. Reúna información de fuentes como los sistemas de administración de red, las indicaciones del analizador de protocolos, los resultados de la ejecución de comandos de diagnóstico del enrutador, o notas de la versión del *software*.
- Paso 3** Considere los posibles problemas con base en los hechos reunidos. Mediante el uso de éstos puede eliminar de su lista algunos de los problemas potenciales.
- Por ejemplo, dependiendo de los datos, podría eliminar el *hardware* como un problema, con el propósito de concentrarse en problemas de *software*. En cada oportunidad procure reducir el número de problemas potenciales a fin de crear un plan de acción eficiente.
- Paso 4** Cree un plan de acción basado en los problemas potenciales restantes. Comience por el más probable y conciba un plan en el que sólo se manipule una variable a la vez.
- Cambiar una variable a la vez le permite reproducir una solución dada a un problema específico. Si cambia al mismo tiempo más de una variable, podría resolver el problema, pero se volverá más difícil identificar el cambio específico que eliminó el síntoma y no le ayudará a solucionar el mismo problema si ocurre en el futuro.
- Paso 5** Ponga en marcha el plan de acción, realizando con cuidado cada paso al tiempo que comprueba si desaparece el síntoma.
- Paso 6** Siempre que cambie una variable, asegúrese de recopilar los resultados. En general, para reunir hechos debe emplear el mismo método que usó en el paso 2 (es decir, trabajar con las personas clave afectadas conjuntamente con el empleo de sus herramientas de diagnóstico).

Paso 7 Analice los resultados para determinar si se resolvió el problema. De ser así, entonces el proceso está concluido.

Paso 8 Si el problema no se resolvió, debe crear un plan de acción basado en el siguiente posible problema de su lista. Regrese al paso 4, cambie una variable a la vez y repita el proceso hasta que se resuelva el problema.

3.6 Como prevenirse para una falla de red

Siempre le será más fácil recuperarse de una falla de red si está prevenido. Posiblemente el requerimiento más importante en cualquier entorno de red sea tener disponible en todo momento, para el personal de soporte de la misma, la información actual y precisa acerca de la red. Sólo con información completa se pueden tomar decisiones inteligentes acerca de un cambio en la red, y sólo con la información completa puede efectuarse la resolución de problemas en la forma más rápida y sencilla posible. Durante el proceso se tiene que asegurar que la información este actualizada.

4 HERRAMIENTAS PARA RESOLUCIÓN DE PROBLEMAS

En este capítulo podrá encontrar herramientas que le podrán de ser de mucha utilidad para resolver problemas de redes, tanto a nivel de *software* como de *hardware*.

4.1 Lista de herramientas de análisis y diagnóstico

En esta sección podrá llegar a conocer una gran variedad de herramientas que pueden ser utilizadas para el análisis y diagnóstico de una red, con lo que podrá llegar a reconocer cual es la herramienta que le conviene comprar para tener una red robusta y segura, que realice las tareas que necesite y si en caso de algún problema, este pueda llegar a determinarse de forma rápida, para evitar contratiempos e incurrir en gastos como el buscar a un técnico para que determine donde se encuentra el error, lo cual le puede llegar a tomar horas, días o hasta meses, en buscar la posible solución del problema. Todo esto lo puede realizar de una manera más segura y fiable en tan solo unos segundos, utilizando herramientas que ya se encuentran en el mercado, y que tienen como finalidad el detectar errores dentro de la red, aunque también pueden servir para determinar como esta funcionando la red en ese momento y ver si es necesario mejorarla para posibles ampliaciones, o simplemente para crear una red con mejores capacidades.

Aparte de lo que se menciona anteriormente, también pueden servir para:

- Detección de cuellos de botella
- Colisiones
- Cargas de tráfico
- Simulaciones de carga
- Tratamiento y optimización de protocolos
- Resolución de problemas
- Diseño

A continuación se muestra una lista de algunas herramientas las muchas que hay, para análisis y diagnóstico de redes:

Tabla XIII. Herramientas de análisis y diagnóstico a nivel de *software*.

Herramienta	Funcionalidad
<i>Link Analyst</i>	Monitoreo, Mapeo, Análisis de servicios TCP y IPX, Detectar colisiones, Reportes.
<i>Microsoft Systems Management Server</i>	Inventario de <i>hardware</i> y <i>software</i> , Verificación de compatibilidad de <i>hardware</i> y <i>software</i> , Medición de <i>software</i> , Detección de topología de red, Reportes, Mapeo, Monitoreo, Diagnóstico remoto.
<i>MRTG: Multi Router Traffic Grapher</i>	Monitoreo de tráfico (entrante y saliente) con opción de especificar 4 niveles de monitoreo (diario, semanal, mensual, anual).
<i>Router-Stats</i>	Monitoreo de tráfico, Estadísticas.
<i>ACTRIZ</i>	Aislar problemas, Analizar los protocolos para acceso.
<i>LAN Wizard TNV</i>	Recolección de tráfico, Estadísticas de comportamiento.
<i>Cisco Info Center</i>	Diagnóstico, Monitorización de rendimiento y servicios, Aislamiento de problemas.
<i>Cisco Works</i>	Administración de redes.
<i>RMON TrafficDirector</i>	Monitoreo remoto de rendimiento, Detectar problemas potenciales.
<i>VlanDirector</i>	Administración de redes.

También existen las herramientas que permiten analizar los medios físicos (cables, conexiones, terminadores, cortocircuitos, etc), entre los que se encuentran:

Tabla XIV. Herramientas de análisis y diagnóstico a nivel de *hardware*.

Herramienta	Funcionalidad
<i>NetChecker</i>	Diagnóstico, Localizar cortocircuitos, Errores de terminación y Nodos defectuosos.
<i>MediaChecker</i>	Comprobar cables, Buscar posibles errores, Identificar los terminadores, Conexiones sueltas, Cortocircuitos, Circuitos abiertos.

4.2 Herramientas de análisis y diagnóstico a nivel de *software*

La mayoría de aplicaciones que analizan el comportamiento del tráfico de las redes, lo realizan por medio del protocolo *SNMP* (Protocolo Sencillo de Administración de Redes).

4.2.1 *Link Analyst*

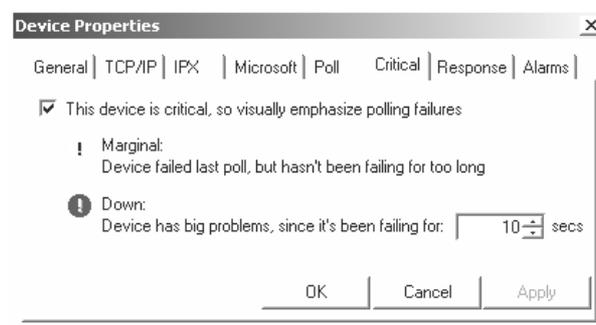
Esta herramienta permite tener información del comportamiento de nuestra red de una forma clara y fácil de entender, gracias a que tiene una interfaz donde se muestra la información de una forma clara y detallada.

Esta herramienta puede ayudar a identificar cual elemento de la red es el que esta fallando, por lo que dispone de un diagrama de todos los elementos que componen la red, en donde se visualiza fácilmente todos los elementos. La herramienta se encarga de hacer revisiones de cada uno de los componentes cada intervalo de tiempo, el cual puede ser especificado por el operario.

Otras de las características que se tiene es que los elementos que tienen algún problema son marcados con una etiqueta.

La herramienta presenta distintas etiquetas, unas de color amarillo para indicar que el elemento ha fallado pero no por mucho tiempo, esto con el fin de que tome precaución con este elemento. Las etiquetas de color rojo indican que el elemento tiene grande problemas, por lo que habrá que cambiarlo o revisar cual sea el problema que presenta.

Figura 18. Propiedades de los elementos.

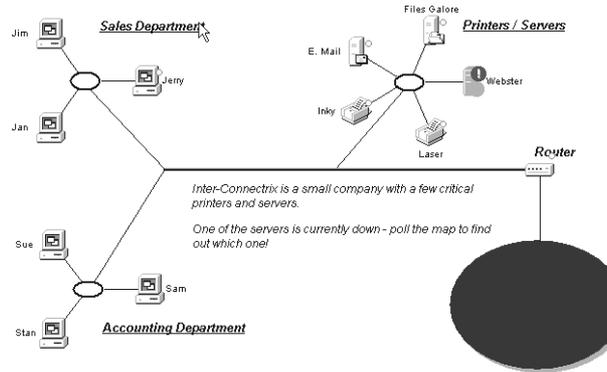


Entre los distintos reportes que presenta la herramienta están:

Mapa

Este reporte presenta en forma gráfica como es que se encuentra la red en ese momento. El reporte se está actualizando casi en tiempo real.

Figura 19. Mapeo de red



Servicios TCP/IP

Podrá obtener información de cómo es que se encuentran los servicios de TCP/IP que este utilizando. En la herramienta también se le puede especificar que información es la que quiere obtener, por ejemplo solo ciertos servicios de TCP/IP.

Dentro de el reporte también se presentan las etiquetas que indican si se tienen problemas con algún tipo de servicio, además se muestran marcados con otro tipo de etiqueta (🚩) cuales fueron los servicios que se tomaron para realizar el análisis.

Figura 20. Reporte de servicios TCP/IP

Name	DNS	FTP	HTTP	LPD	NNTP	POP3	SMTP	SNMP	TELNET
1 Jerry									
2 Jim									
3 Jan									
4 Sam									
5 Sue									
6 Stan									
7 Inky									
8 Laser									
9 Router									
10 Files Galore									
11 E. Mail									
12 Webster									
13 marlon.www.inpr...		🚩		🚩				🚩	

Servicios IPX

Este es otro tipo de reporte que muestra, dónde presenta información del comportamiento de los servicios IPX, al igual que el anterior reporte, también se tiene la opción de seleccionar cual servicio es el que quiere uno que se analice.

Figura 21. Reporte de servicios IPX

	Name	IPX/SPX	Router driver	LAN driver	Shell	VAP	Router	File server/route
1	Jerry							
2	Jim							
3	Jan							
4	Sam							
5	Sue							
6	Stan							
7	Inky							
8	Laser							
9	Router							
10	Files Galore							
11	E-Mail							
12	Webster							
13	marlon.www.impr...							

Tiempo de Respuesta

Podrá obtener un reporte detallado de cuanto es lo que se tardo en responder cada uno de los elementos de la red.

La herramienta realiza verificaciones cada cierto tiempo a cada uno de los elementos, lo que va registrando en un historial, para tener un promedio de respuestas, tiempos máximos y mínimo de respuesta, con lo que se podrá dar cuenta si hay alguno de los elementos que este fallando.

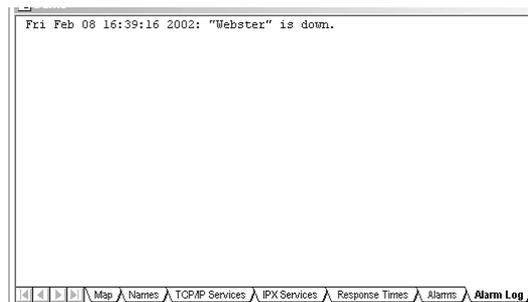
Figura 22. Tiempo de respuesta

	Name	Latest (ms)	Minimum (ms)	Maximum (ms)	Average (ms)	Good	Marginal	Poor
1	Jerry	40.5	0.3	49.5	24.0			
2	Jim	24.5	0.3	49.5	24.0			
3	Jan	40.0	0.3	49.0	25.8			
4	Sam	39.0	0.3	49.0	27.1			
5	Sue	38.0	0.3	49.5	24.8			
6	Stan	3.5	0.3	49.5	26.1			
7	Inky	35.0	0.5	49.5	27.3			
8	Laser	17.5	0.3	49.5	27.0			
9	Router	0.5	0.3	49.0	25.5			
10	Files Galore	13.5	0.5	49.5	26.9			
11	E-Mail	30.0	0.3	49.5	25.1			
12	Webster	NA	NA	NA	NA			
13	marlon.www.impr...	NA	NA	NA	NA			

Registro

Este reporte es el resumen de una serie de análisis realizado por la herramienta, ya que aquí se concentra el análisis de los elementos de la red que posiblemente son los que han estado causado problemas, con lo que solo tendrá que ir y revisar el elemento marcado y ver cual es la causa del problema.

Figura 23. Registro



4.2.2 RMON TrafficDirector

Con esta aplicación podrá monitorear el tráfico desde cualquier parte de la red, desde las capas de enlace, red, transporte o aplicación. Permite obtener una evaluación rápida de la carga de la red y de la distribución de los protocolos.

La aplicación también permite profundizar un poco más, pasando por segmentos, puertos de conmutadores o enlaces troncales específicos y aplicar herramientas de análisis y diagnóstico en tiempo real para ver *hosts*, conversaciones y captura de paquetes.

4.2.3 VlanDirector

Es una aplicación para la administración de conmutadores, permitiendo simplificar la asignación de los puertos, además de proporcionar otras capacidades de administración para las *VLANs*, proporciona otras características para los administradores de red, tales como:

- Una representación física de la red.
- Información de configuraciones de *VLAN*.
- Resolver problemas e identificar configuraciones de dispositivos individuales que tienen errores con la *VLANs* a nivel de sistema.
- Detección de cambios en el estado de la *VLAN* o puertos del conmutador.
- Autenticación de usuario.

4.2.4 MRTG: *Multi Router Traffic Grapher*

Es una aplicación que le permite ver en modo gráfico los datos que lee el protocolo SNMP. Esta aplicación crea páginas HTML con gráficos GIF sobre el tráfico entrante y saliente en los interfaces de red.

El paquete esta compuesto por un conjunto de utilidades que ayudan al proceso de analizar los interfaces de enlace, extraer sus características y generar los ficheros de configuración base, que luego se pueden modificar para adaptarlos a las necesidades concretas. Entre las características con que cuenta esta herramienta, se encuentra la cantidad de información que produce, permitiéndonos escoger cuatro niveles de detalle del tráfico que se tiene en cada *interface*: las últimas 24 horas, última semana, último mes y anual.

Guarda un historial de la información que se va obteniendo, pero además utiliza un algoritmo que no permite que los ficheros donde se guarda crezcan excesivamente.

Esta aplicación tiene la desventaja de que se tiene que estar ejecutando cada intervalo de tiempo, para que pueda recoger datos y generar los gráficos periódicamente, pero por ser una página HTML, también se le puede indicar que se este refrescando cada cierto tiempo.

4.2.5 *Microsoft Systems Management Server*

Esta tiene entre sus características el poder mostrar un inventario de *hardware*, medición y un inventario de *software*, elaboración de reportes. También puede ayudarnos a resolver problemas de forma remota. Todo esto permite llevar un mejor control de los cambios y configuraciones que se han realizado en la red, tomando en cuenta que solo trabaja en *Windows*.

Con esta herramienta se podrá administrar de una forma sencilla toda la red, exponer servicios e interfaces que las aplicaciones puedan usar.

Entre las ventajas que pueden proporcionar están:

- Proporciona el menor costo de administración por medio de herramientas de planeación, implementación y diagnóstico.
- Habilita las soluciones de administración más escalables, desde organizaciones pequeñas hasta ambientes empresariales.

Esta aplicación usa el formato CIM (*Common Information Model*) para la recolección de la información, es por eso que la información que se tiene del *hardware* (como lo es un inventario) es muy completa, basándose en los estándares para seleccionar que información es importante.

Para proporcionar un mejor inventario de *software*, lleva a cabo una búsqueda de recursos por versión en cada ejecutable de la máquina del cliente, en lugar de verificar contra una base de datos predefinida. Esto proporciona un mecanismo eficiente para obtener información detallada en cada aplicación de cada PC. Estas opciones de un inventario centralizado reducen la necesidad de los administradores de revisar cada computadora. También, los reportes que se presentan, pueden ayudarnos a tener en forma resumida y presentable los datos, lo que permite ahorrar tiempo

Una de las características más importantes con que cuenta esta herramienta, es la de poder rastrear y medir el uso de *software* por usuario, grupo, estación de trabajo, tiempo con el objetivo de reducir los costos asociados con el uso inapropiado. También proporciona nuevas herramientas sofisticadas de medición de *software* para analizar, monitorear y controlar el uso de las aplicaciones en servidores y estaciones de trabajo. El administrador tiene muchos niveles de control, desde simples señales de alerta hasta la suspensión de la ejecución de una aplicación.

Muchas veces es necesario que un ingeniero revise la computadora donde ha ocurrido algún problema, pero esto no siempre es posible, ahora bien con esta aplicación podrá tener un control de forma remota, con lo que podrá estar al tanto de donde ha ocurrido un problema y cuál es, sin necesidad de tener que estar en el lugar de los hechos. Todo esto se puede hacer gracias a que cuenta con un sistema de monitoreo remoto, donde se presenta información de la salud de la red. Esta aplicación se complementa con la utilidad HealthMon, la cual permite ver información gráfica en tiempo real sobre los recursos del servidor.

También se incluye la habilidad de monitorear servidores DHCP en mal estado o intentos de irrumpir en Internet. También ofrece una nueva herramienta de topología de definición de redes que pone al tanto de las actividades de administración de sistemas de la red.

Esta nueva función proporciona una gráfica de las rutas de la red entre los servidores dentro de un sitio, incluyendo la actividad de los dispositivos y el estado de los servicios en los servidores. Esto permite un análisis sencillo del éxito o fracaso de una acción como la distribución de *software* a una locación remota antes de liberarlo, reduciendo los costos asociados con las distribuciones fallidas de *software*.

La aplicación ha sido diseñada para reducir los costos asociados con el tráfico de WAN. Logra esto al proporcionar múltiples emisores de WAN, programación y aceleración de ancho de banda.

Systems Management Server permite delegar de una forma más sencilla y precisa las actividades, de modo que los administradores puedan contar con una herramienta de administración que corresponda exactamente a su trabajo.

4.2.6 Cisco Info Center

Cisco Info Center (CIC) permite obtener un control sobre fallas y rendimiento, gracias a que es una aplicación de diagnóstico y monitorización de alarmas a nivel de servicio. También permite el aislamiento de problemas de la red. Está diseñada para que las personas que operan y administran la red, se centren únicamente en las situaciones que más necesitan de atención en la red. La herramienta permite establecer una correlación entre la información de fallos de multitecnología, multifabricantes y plataformas, ayudándonos a resolver de forma eficaz y oportuna los problemas de la red y en consecuencia una reducción en el costo de las operaciones.

Con este tipo de herramienta uno puede ahorrarse el esfuerzo manual que se requiere diagnosticar y solucionar los problemas de la red.

Otra característica muy importante que se tiene, es la de poder autorizar a los operadores a interpretar datos, mientras que las acciones activadas por eventos pueden configurarse para responder automáticamente a determinados comportamientos, además de poderse agregar más reglas de automatización.

En vez de que el administrador tenga que analizar una gran cantidad de datos, esta aplicación se encarga de correlacionar la información y presentar los datos más importantes de los fallos de una manera que le sea fácil de interpretar.

CIC es capaz de recibir múltiples flujos de datos, independientes de la tecnología del elemento de la red, proporcionando un centro de gestión de fallos centralizado.

Entre las ventajas que presenta ésta herramienta están:

- Fácil manejo
- Arquitectura ampliable y de alta distribución
- Rentabilidad inmediata de su inversión
- Mejora de la oferta de servicios
- Potente interfaz administrativa
- Motor de correlación de eventos totalmente personalizable
- Sobrecarga de información
- Redes de varios proveedores
- Soporte para varias redes

Cisco Info Center es un conjunto de utilidades, entre las que se encuentran:

Info Server

Esta utilidad es el elemento central de CIC, ya que se encarga de recaudar la información de fallos y prepararla, esto lo realiza mediante fuentes como *Info Mediators* y otros *Info Servers*. La utilidad también utiliza una base de datos relacional para almacenar la información recabada, la información es obtenida monitorizando las actividades de la red en tiempo real.

IP VPN

La integración de esta utilidad permite relacionar la información de los fallos de la red con un análisis de impacto en el usuario final, todo esto de una forma automática.

Cisco Info Expert

Permite reducir de forma inteligente la cantidad de información que tenga que ver los fallos de la red, la cual será presentada al operador, todo con el fin de aislar los servicios afectados.

La utilidad ayuda a definir las reglas a utilizar para activar las acciones que se realizaran cuando se detecte cierto comportamiento, estas reglas estarán

definidas por el usuario. También se le puede incorporar procedimientos para la recuperación ante fallos, lo cual ayudara a la protección de los datos.

Cisco Info Expert permite enlazar multiples *Info Server*, de tal forma que se pueda informar a los operadores de diferentes áreas geográficas.

De esta forma los operadores que se encuentran a grandes distancias, pueden estar centrando su atención en aspectos como compartir información, también podrán ejecutar herramientas de diagnóstico basándose en el tipo de alarma que este recibiendo, con el fin de acelerar la identificación y resolución de los problemas.

Info Mediators

Recopila y analiza los eventos de CIC. Esta utilidad recoge los datos que estén relacionados con las fallas de los elementos de la red. Los mediadores de información son aplicaciones que recogen y procesan la información relativa a los eventos y a los fallos antes de enviarla al servidor de información. Pueden configurarse para filtrar y traducir cuando reciben determinados datos. Entre las acciones configurables se incluyen traducciones de identificadores de interrupción específicos o la introducción de información adicional sobre los eventos junto con un original mensaje de alarma.

Info Gateways

Los *Info Gateways* enlazan el *Info Server* con *Info Servers* u otros sistemas externos. Facilitan la propagación de información entre servidores, sistemas y el almacenamiento de datos. Una de las funciones más significativas de una *gateway* de información es su capacidad para admitir el filtro en tiempo real y la distribución de fallos y eventos. Las *gateways* de información llevan a cabo la propagación de alarmas y eventos.

4.2.7 CiscoWorks

Esta herramienta esta compuesta por una serie de aplicaciones, las cuales son útiles para la resolución de problemas, entre las que se encuentran:

- **Device Monitor:** esta aplicación permite seleccionar cual dispositivos de red es el que uno quiere monitorear, con lo que muestra información acerca del entorno de estos dispositivos, así como estadísticas de su comportamiento.
- **Healt Monitor:** con esta aplicación uno puede recibir información del estado de cualquiera de los dispositivos que forman la red, también podemos obtener información de los búferes, la carga de la CPU, la memoria disponible y los protocolos e interfaces que se están usando.
- **Show Commands:** permite monitorear las operaciones que se realizan en la red; permite detectar problemas en las interfaces, nodos, medios o aplicaciones; también ayuda a determinar cuando esta congestionada una red. Además podemos determinar el estado de los servidores.
- **Path Tool:** permite analizar y desplegar información de la ruta que existe entre dos dispositivos para recolectar datos sobre su uso y los errores.
- **Device Polling:** prueba los dispositivos de la red, obteniendo datos acerca de sus condiciones.
- **Cisco View:** proporciona monitoreo dinámico y funciones de resolución de problemas, incluyendo un despliega gráficos de dispositivos, estadísticas e información de configuraciones.
- **Offline Network Análisis:** realiza un análisis fuera de línea acerca de las tendencias de desempeño y patrones de tráfico, por lo que recolecta datos históricos para la realización de comparaciones con los datos presentes.
- **CiscoConnect:** permite que le proporcione a Cisco información sobre la depuración, configuraciones e información de topología para agilizar la resolución de problemas de red.

4.2.8 Otras aplicaciones

Hay otra categoría de *software* que ofrece una solución completa tanto para monitorizar como para configurar toda la red.

Este tipo de solución permite obtener una compleja representación gráfica de la red y observar fácilmente los nodos que la componen, verificando detalles de configuración específicos y otras cuestiones de interés.

Entre estas aplicaciones podemos mencionar: *HP-OpenView* y *SunNet Manager*. Cuentan con utilidades que le permiten localizar los nodos de la red en los que se están ejecutando agentes *SNMP*. Otra característica importante es la capacidad de integrar productos de otros fabricantes, como el *CiscoWork*.

4.3 Herramientas de análisis y diagnóstico a nivel de *hardware*

Algunas veces a parte de las herramientas *software*, también hace falta contar con alguna herramienta *hardware*, para poder detectar donde se encuentran los problemas en la red. Las siguientes son algunas herramientas típicas usadas en la resolución de problemas:

- Los medidores de voltaje y resistencia, los multímetros digitales y los probadores de cables son útiles para probar la conectividad física del tendido de cables.
- Los TDRs (reflectómetros de dominio de tiempo) y los OTDRs (reflectómetros ópticos de dominio de tiempo) son dispositivos que ayudan en la localización de rupturas de cables, falta de correspondencia de impedancias y otros problemas físicos del cableado.
- Las cajas de derivación y las *fox boxes* son útiles para la resolución de problemas en *interfaces* periféricas.
- Los analizadores de red, tales como *Network General Sniffer*, decodifican problemas en las siete capas OSI y pueden identificarlos automáticamente en tiempo real, proporcionando una visión clara de la actividad de la red y clasificando los problemas de acuerdo a su nivel crítico.

4.3.1 Medidores de voltaje y resistencia, multímetros digitales y probadores de cables

Muchas veces uno puede llegar a detectar que en cierta área de nuestra red es donde se está teniendo conflictos, por medio de herramientas de *software*, pero no podemos llegar a determinar con precisión si es por causa de algunos de los cables que se tienen, es más también el voltaje que se puede llegar a tener puede causar problemas.

Herramientas como los medidores de voltaje y resistencia, multímetros digitales y probadores de cables, pueden ser de mucha utilidad cuando tratamos de realizar pruebas de cables. Estos dispositivos miden parámetros tales como el voltaje *AC* y *DC*, corriente, resistencia, capacitancia y continuidad del cable. Son empleados para revisar la conectividad física.

Existen diferentes tipos de probadores de cables, los hay para los tipos de cable *STP* (par trenzado blindado), para *UTP* (par trenzado sin blindaje) y cables 10BaseT, coaxial y bicoaxial (twinax). Estos tipos de probadores de cables, tienen que ser capaz de realizar las siguientes funciones:

Probar y reportar las condiciones del cable, incluyendo diafonía cercana al extremo (*NEXT*), atenuación y ruido.

Realizar funciones de *TDR*, monitoreo de tráfico y mapa de asignación de terminales. Desplegar información de la capa *MAC* (Control de Acceso a Medios) acerca del tráfico de *LAN*, proporcionar estadísticas como el uso de la red y las tasas de error de paquetes y realizar pruebas de protocolo limitadas (por ejemplo, pruebas *TCP/IP* como ping).

Como es de esperarse, el tipo de cable de fibra óptica también cuenta con probadores, los cuales son similares a los probadores de los otros tipos de cable. Debido al alto costo de este tipo de cable y su instalación, debe probarse antes (pruebas en el carrete) y después de la instalación. La prueba de continuidad de la fibra requiere una fuente de luz visible o un reflectómetro. Las fuentes de luz se emplean con medidores de potencia que pueden medir las mismas longitudes de onda, probar la atenuación y devolver la pérdida de transmisión en la fibra.

4.3.2 TDRs y OTDRs

Con este tipo de herramienta uno puede llegar a encontrar donde se encuentran circuitos abiertos y en corto, ondulaciones, enroscaduras, dobleces agudos, falta de correspondencia de impedancia y otros defectos en cables metálicos.

Los *TDRs* funcionan midiendo la señal en el extremo del cable, basándose en las longitudes de señal que reflejan estos, ya que se ha determinado de que las roturas, cortos y otros problemas, devuelven diferentes longitudes de señales.

Un *TDR* mide qué tanto tiempo necesita la señal para reflejarse y calcula la distancia hacia la falla en el cable.

Otra de las características de este tipo de aparato, es que también puede ser empleado para medir las longitudes de los cables.

Para la medición de los cables de fibra óptica se utilizan los *OTDR*, los cuales pueden ayudar a medir con una gran precisión la longitud de estos, localizar rupturas, medir atenuación y las pérdidas de las uniones o conectores.

4.3.3 Cajas de derivación, fox boxes y BERT/BLERT

Estas herramientas no son más que probadores de tasa de error (*bit/bloque*). Son empleadas para medir las señales digitales que presentan las *PCs*, impresoras, módems, la *CSU/DSU* (Unidad de Servicio de Canal/Unidad de Servicio Digital), así como de otras interfaces periféricas.

Con todo esto tendrá la posibilidad de diagnosticar problemas comunes en los sistemas de comunicaciones de datos. También es posible examinar el tráfico de los equipos a través del *DCE* (equipo de comunicaciones de datos), con lo que se podrá aislar los problemas y asegurarse de que se haya instalado el cableado adecuado. Cabe mencionar que no son capaces de probar señales de medios tales como *Ethernet*, *Token Ring* o *FDDI*.

4.3.4 Monitores de red

Los monitores de red realizan un muestreo de todas las actividades que se están realizando en la red durante un periodo con el fin de establecer como es el desempeño normal de la red, esto le ayuda a obtener una línea base del comportamiento de la red.

Estas herramientas se encargan de recolectar información de la red, tales como el tamaño de los paquetes, la cantidad de paquetes, los paquetes con errores, el uso que se le este dando a las conexiones, la cantidad de *hosts* que se tienen y sus direcciones MAC. También permiten determinar como es la comunicación entre los *hosts* y los otros dispositivos.

Todo lo anterior puede ayudar a determinar como se comporta el tráfico de nuestra red y en consecuencia determinar si existe alguna sobrecarga de tráfico, además de ayudarnos a planear alguna expansión de la red, detectar intrusos, establecer el desempeño de la línea base y distribuir el tráfico de manera más eficiente.

4.3.5 Analizadores de red

Los analizadores de red decodifican las diversas capas de los protocolos en una trama de registro resumida y lo presenta de tal forma que sea fácil de comprender, detallando además cada una de las capas que se está involucrando (física, enlace de datos, etc.) y para que sirva cada *byte* o contenido de *byte*.

Los analizadores de red tienen que poder realizar las siguientes funciones:

- Filtrar tráfico que cumpla determinado criterio.
- Anotar la hora de los datos capturados.
- Presentar las capas de protocolos en forma fácilmente legible.
- Generar tramas y transmitir las en la red.
- Incorporar un sistema experto en donde el analizador utilice un conjunto de reglas, combinadas con información acerca de la configuración y operación de la red, para diagnosticar, resolver o proporcionar soluciones potenciales a los problemas de red.

CONCLUSIONES

- Existen varios factores que afectan el rendimiento de una red, tales como: el retardo, el número de estaciones, lo cual se puede evitar si se toman en cuenta las limitaciones de cada uno de los dispositivos que se usan para formar la red.
- La persona responsable de una red, tiene que estar realizando revisiones continuas de los procesos que se tienen en la red, con el fin de evitar saturaciones o mejorar el servicio que la red este prestando en ese momento. También, estar consciente de las normas a seguir, tales como: el no poner demasiados ordenadores en un cable, cuál es la distancia promedio de un cable, etc.
- Toda persona que tenga los conocimientos básicos de computación, puede llegar a detectar, diagnosticar y hasta resolver problemas de redes de computadoras, sin ser un experto en la materia.
- Un administrador de redes de computadoras tiene que saber en que momento es conveniente expandir de una red o simplemente seguir trabajando con la que ya se tiene, teniendo bajo la responsabilidad la optimización de los recursos de la red existente.

- Cuando se trabaja con redes muy complejas es muy difícil encontrar cuales son las causas que puedan o estén provocando problemas, por lo que muchas veces hace falta contar con alguna herramienta de respaldo para hallar las soluciones a posibles errores que se puedan dar o que se estén dando.
- Es una buena práctica el tomar nota de que métodos se usaron para resolver los problemas. Además, el tomar nota de la resolución de problemas puede ayudar a prevenir estos problemas en un futuro.

RECOMENDACIONES

- Si se posee la disponibilidad de utilizar una herramienta de diagnóstico, deberá hacerse, ya que, esto le ayudará a tener una mejor administración de la red, a parte de ahorrar tiempo y dinero para solucionar problemas que se puedan enfrentar.
- Antes de comprar una herramienta para diagnóstico de red, asegurarse que posea lo necesario para diagnosticar una red con las características que tenga la propia.
- Cuando se esté intentando resolver un problema, no es muy aconsejable que se realice el cambio de varias variables a la vez, ya que, será más difícil el saber cuál fue la variable que le ayudó a corregir el problema que se tenía. Cuando se realizan cambios de una sola variable a la vez, es fácil darse cuenta si ésta fue la que ayudó a corregir el problema.
- Trata de hacer revisiones periódicas para poder prevenir errores.
- Tomar nota del método utilizado para la solución de los problemas, ya que, esto puede ayudar en un futuro.

BIBLIOGRAFÍA

Herramientas *on-line* de *networking*. <http://www.canalti.com/magazine/canalcisco.cfm>. Julio 2001.

Introducción a los *Routers*.
<http://www.canalti.com/magazine/versecciones.cfm?seccion=Redes%20y%20Comunicaciones>. Septiembre 2001.

Componentes de una red. <http://www.angelfire.com/mi2/Redes/componentes.html>. Julio 2001.

Diagnóstico de una red TCP/IP.
<http://www.frc.utn.edu.ar/institucional/sistemasinformacion/laboratoriosistemas/Publicaciones/AdminTcp/diagnostico.html>. Julio 2001.

Protocolos y Arquitectura.
<http://www.geocities.com/elplanetamx/protocolosyarquitectura.htm>. Julio 2001.

Tecnologías LAN. <http://www.geocities.com/elplanetamx/tecnologiaslan.htm>. Julio 2001.

Medios de Transmisión.
<http://www.geocities.com/elplanetamx/mediosdetransmision.htm>. Julio 2001.

Tipos de redes y subredes, Protocolos, Enrutamiento. <http://www.solont.com>. Septiembre 2001.

Guía para la solución de problemas.
<http://www.microsoft.com/latam/technet/articulos/200010/art09/default.asp>. Agosto 2001

Familia de productos de "*appliances*" *NetCache*. <http://www-es.netapp.com/products/>. Agosto 2001.

Multi Router Traffic Grapher (MRTG).
<http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html>. Agosto 2001.

Router Stats. <http://www.scn.de/~iain/router-stats/> . Agosto 2001.

Software de gestión de red *SNMP*. <http://wwwsnmp.cs.utwente.nl/software/> . Agosto 2001.

Redes. http://www.unav.es/cti/manuales/Redes_Internet/indice.html. Agosto 2001.

Administración de Redes.

<http://www.geocities.com/SiliconValley/Circuit/3779/documentos/admredes.html>.

Agosto 2001.

Cisco Info Center. <http://www.cisco.com>. Diciembre 2001, Enero 2002.

NETWORK ROUTE MAPPING, DEVICE UPTIME TRACKING, RESPONSE MONITORING & ANALYSIS TOOL, Analisis de trafico y monitoreo de redes de datos, *Link Analyst*. <http://www.networkinstruments.com>. Enero 2002.

Microsoft Systems Management Server.

<http://www.microsoft.com/latam/sms/exec/default.asp>. Enero 2002.

Resuelva problemas de red a nivel físico de forma rápida y sencilla.

http://www.ab.com/controlnews/issue_2_00/spanish/page7.html. Enero 2002.

S. Tanenbaum, Andrew. **Redes de Computadoras**. Tercera edición. Pearson Educación. México. 1997.

Lew, H. Kim y colaboradores. **Interconectividad: Manual para resolución de problemas**. Primera edición. Pearson Educación. México. 2000.

Rejopachi Carrera, Caleb Rafael. **Tesis Fibra Óptica y Cableado Estructurado en el Diseño de Redes**. Guatemala. 1995.

APÉNDICES

A – Información de soporte técnico

B - Códigos de error de *windows*

APÉNDICE A

Información de soporte técnico

En esta sección se encontrara una serie de hojas de trabajo que le ayudarán a registrar los síntomas a dar soluciones a éstos.

Con las tablas que se presentan a continuación se podrá tomar un registro de los hechos relevantes, para poder aislar los posibles problemas, así, posteriormente, puedan ser resueltos.

Estas hojas de trabajo, simplemente son una guía de cómo se podrían registrar los problemas que han surgido y como se han resuelto, para que en el futuro pueda servir para resolver los mismos problemas o algunos otros.

1 Síntomas reportados:

2 Mapa de la topología de la red – adjunte hojas adicionales

3 Protocolos de red implementados:

4 Protocolos enrutados:

5 Protocolos punteados:

6 Puntos de contacto con redes externas:

7 Equipo de interred (incluyendo dirección de red, fabricante, modelo y función):

8 Nodos de sistemas finales y de interred sospechosos (incluyendo dirección de red, fabricante, modelo y función):

9 Aplicaciones usadas en la red (*FTP, sendmail, NFS, NetWare*, etcétera):

10 Síntomas y posibles problemas:

Síntomas	Posibles problemas

11 Plan de acción para cada problema:

Problema	Plan de acción

12 Resultados de las acciones:

Problema	Acción	Resultado

APÉNDICE B

Códigos de error de *windows*

En esta sección se encontrará una lista de errores que aparecen en *Windows*. La lista muestra un número de orden, un código que identifica al error y una breve explicación del error. Estos errores pueden surgir por algo indebido que hagamos o por que el ordenador detecto algo anormal.

Listado de Errores

- 0 0x0000 La operación se ha completado correctamente.
- 1 0x0001 Función incorrecta.
- 2 0x0002 El sistema no puede hallar el archivo especificado.
- 3 0x0003 El sistema no puede hallar la ruta especificada.
- 4 0x0004 El sistema no puede abrir el archivo.
- 5 0x0005 Acceso denegado.
- 6 0x0006 Controlador no válido.
- 7 0x0007 Los bloques de control de almacenamiento han sido destruidos.
- 8 0x0008 Espacio de almacenamiento insuficiente para procesar este comando.
- 9 0x0009 Dirección de bloque de control de almacenamiento no válida.
- 10 0x000A El entorno es incorrecto.
- 11 0x000B Se ha intentado cargar un programa con un formato incorrecto.
- 12 0x000C Código de acceso no válido.
- 13 0x000D Datos no válidos.
- 14 0x000E Espacio de almacenamiento insuficiente para completar esta operación.
- 15 0x000F El sistema no puede hallar el controlador especificado.
- 16 0x0010 No se puede quitar el directorio.
- 17 0x0011 El sistema no puede mover el archivo a otra unidad de disco.
- 18 0x0012 No hay más archivos.
- 19 0x0013 El medio está protegido contra escritura.
- 20 0x0014 El sistema no puede hallar el dispositivo especificado.
- 21 0x0015 El dispositivo no está listo.
- 22 0x0016 El dispositivo no reconoce el comando.
- 23 0x0017 Error de datos (comprobación de redundancia cíclica)
- 24 0x0018 El programa lanzó un comando pero la longitud del comando es incorrecta.
- 25 0x0019 La unidad no puede hallar un área o pista específica en el disco.
- 26 0x001A No se tiene acceso al disco o disquete especificados.
- 27 0x001B La unidad no puede hallar el sector requerido.
- 28 0x001C No queda papel en la impresora.

- 29 0x001D El sistema no puede escribir en el dispositivo especificado.
- 30 0x001E El sistema no puede leer desde el dispositivo especificado.
- 31 0x001F Uno de los dispositivos vinculados al sistema no funciona.
- 32 0x0020 El proceso no tiene acceso al archivo porque está siendo utilizado por otro proceso.
- 33 0x0021 El proceso no tiene acceso al archivo porque otro proceso tiene bloqueada una parte del archivo.
- 34 0x0022 El disco insertado en la unidad no es el correcto.
- 36 0x0024 Hay demasiados archivos abiertos para compartir.
- 38 0x0026 Alcanzado el final del archivo.
- 39 0x0027 El disco está lleno.
- 50 0x0032 La petición de red es incompatible.
- 51 0x0033 El equipo remoto no está disponible.
- 52 0x0034 Existe un nombre duplicado en la red.
- 53 0x0035 No se ha encontrado la ruta de acceso de la red.
- 54 0x0036 La red está ocupada.
- 55 0x0037 El recurso de red o el dispositivo especificados ya no se encuentran disponibles.
- 56 0x0038 Se ha alcanzado el límite de comandos BIOS de la red.
- 57 0x0039 Error *hardware* en el adaptador de red.
- 58 0x003A El servidor especificado no puede ejecutar la operación solicitada.
- 59 0x003B Error de red inesperado.
- 60 0x003C El adaptador remoto no es compatible.
- 61 0x003D La cola de impresión está llena.
- 62 0x003E El servidor no dispone de espacio para almacenar el archivo que se va a imprimir.
- 63 0x003F Eliminado el archivo que estaba esperando para imprimirse.
- 64 0x0040 El nombre de red especificado ya no está disponible.
- 65 0x0041 Acceso a la red denegado.
- 66 0x0042 El tipo de recurso de red no es correcto.
- 67 0x0043 No se encuentra el nombre de red especificado.
- 68 0x0044 Excedido el límite del nombre del adaptador de red local.
- 69 0x0045 Se ha superado el límite de sesiones BIOS de la red.
- 70 0x0046 El servidor remoto se ha parado o está en el proceso de reiniciarse.
- 71 0x0047 No se pueden realizar más conexiones a este equipo remoto en este momento ya que hay más de las que puede aceptar.
- 72 0x0048 Se ha detenido la impresora o dispositivo de disco especificado.
- 80 0x0050 Este archivo ya existe.
- 82 0x0052 No se puede crear el directorio o archivo.
- 83 0x0053 Error en INT 24
- 84 0x0054 No hay lugar disponible para procesar esta petición.
- 85 0x0055 Ya se está utilizando el nombre del dispositivo local.
- 86 0x0056 La contraseña de red especificada no es válida.

- 87 0x0057 El parámetro no es correcto.
- 88 0x0058 Error de escritura en la red.
- 89 0x0059 Es sistema no puede iniciar otro proceso en este momento.
- 100 0x0064 No se puede crear otro semáforo de sistema.
- 101 0x0065 Este semáforo exclusivo pertenece a otro proceso.
- 102 0x0066 Se ha fijado el semáforo y no se puede cerrar.
- 103 0x0067 No se puede volver a fijar el semáforo.
- 104 0x0068 No se puede pedir semáforos exclusivos durante la interrupción.
- 105 0x0069 Ha terminado la posesión anterior de este semáforo.
- 106 0x006A Introduzca el disco de la unidad %1.
- 107 0x006B El programa se ha detenido porque no se ha introducido el disco alternativo.
- 108 0x006C Ya hay otro proceso utilizando o bloqueando este disco.
- 109 0x006D Ha terminado la canalización.
- 110 0x006E El sistema no puede abrir el dispositivo o archivo especificado.
- 111 0x006F El nombre del archivo es demasiado largo.
- 112 0x0070 Espacio en disco insuficiente.
- 113 0x0071 No hay más identificadores de archivos internos disponibles.
- 114 0x0072 El identificador de archivo interno de destino no es correcto.
- 117 0x0075 La llamada a IOCTL efectuada por el programa no es válida.
- 118 0x0076 El valor del parámetro de "comprobar al escribir" no es válido.
- 119 0x0077 Este comando no es compatible con el sistema.
- 120 0x0078 Esta función sólo es válida en modo Win32.
- 121 0x0079 Ha terminado el intervalo de espera del semáforo.
- 122 0x007A El área de datos transferida a una llamada del sistema es demasiado pequeña.
- 123 0x007B El nombre de archivo, directorio o etiqueta del volumen no es válido.
- 124 0x007C El nivel de llamada del sistema no es válido.
- 125 0x007D El disco no tiene etiqueta de volumen.
- 126 0x007E No se puede encontrar el módulo especificado.
- 127 0x007F No se encontró el proceso especificado.
- 128 0x0080 No hay subprocesos a esperar.
- 129 0x0081 La aplicación %1 no se puede ejecutar en modo Win32.
- 130 0x0082 Se ha intentado usar un identificador de archivo con una partición de disco abierta para una operación distinta de una E/S de disco sin procesar.
- 131 0x0083 Se ha intentado mover el puntero del archivo más allá del inicio del archivo.
- 132 0x0084 El puntero del archivo no puede establecerse en el dispositivo o archivo especificado.
- 133 0x0085 No se puede utilizar un comando JOIN o SUBST para una unidad que contiene unidades unidas con anterioridad.
- 134 0x0086 Se ha intentado utilizar el comando JOIN o SUBST en una unidad que ya se estaba unida.
- 135 0x0087 Se ha intentado utilizar el comando JOIN o SUBST en una unidad que ya se había sustituido.

- 136 0x0088 El sistema ha intentado eliminar la unión de una unidad que no está unida.
- 137 0x0089 El sistema ha intentado eliminar la sustitución de una unidad sin sustituir.
- 138 0x008A El sistema ha intentado unir una unidad a un directorio de una unidad ya unida.
- 139 0x008B El sistema ha intentado sustituir una unidad por un directorio en una unidad sustituida.
- 140 0x008C El sistema ha intentado unir una unidad a un directorio de una unidad sustituida.
- 141 0x008D El sistema ha intentado sustituir una unidad por un directorio de una unidad ya unida.
- 142 0x008E El sistema no puede ejecutar JOIN o SUBST en este momento.
- 143 0x008F El sistema no puede unir o sustituir una unidad a o por un directorio en la misma unidad.
- 144 0x0090 El directorio no es un subdirectorio del directorio raíz.
- 145 0x0091 El directorio no está vacío.
- 146 0x0092 La ruta de acceso especificada se está usando en un sustituto.
- 147 0x0093 Recursos insuficientes para procesar este comando.
- 148 0x0094 No se puede usar la ruta de acceso en este momento.
- 149 0x0095 Se ha intentado unir o sustituir una unidad donde uno de los directorios de la unidad es el destino de una sustitución anterior.
- 150 0x0096 La información de seguimiento del sistema no se ha especificado en el archivo *CONFIG.SYS* o no se permite el seguimiento.
- 151 0x0097 El número de sucesos del semáforo especificados para *DosMuxSemWait* no es correcto.
- 152 0x0098 No se ha ejecutado *DosMuxSemWait*. Se han establecido demasiados semáforos.
- 153 0x0099 La lista de *DosMuxSemWait* no es válida.
- 154 0x009A El nombre del volumen introducido sobrepasa el límite de caracteres del sistema de archivos de destino.
- 155 0x009B No se puede crear otro subproceso.
- 156 0x009C El proceso receptor ha rechazado la señal.
- 157 0x009D Ya se ha rechazado el segmento y no se puede bloquear.
- 158 0x009E El segmento ya está desbloqueado.
- 159 0x009F La dirección del identificador del subproceso no es correcta.
- 160 0x00A0 La cadena de argumentos pasada a *DosExecPgm* no es correcta.
- 161 0x00A1 La ruta de acceso especificada no es válida.
- 162 0x00A2 Ya hay una señal pendiente.
- 164 0x00A4 No se pueden crear más subprocesos en el sistema.
- 167 0x00A7 No se puede bloquear una región de un archivo.
- 170 0x00AA Ya se está utilizando el recurso especificado.
- 173 0x00AD No había una petición de bloqueo pendiente para la región proporcionada.
- 174 0x00AE El sistema de archivos no admite cambios atómicos al tipo de bloqueo.
- 180 0x00B4 El sistema ha detectado un número de segmento incorrecto.
- 182 0x00B6 El sistema operativo no puede ejecutar %1.
- 183 0x00B7 No se puede crear un archivo que ya existe.
- 186 0x00BA El indicador que se ha pasado no es correcto.
- 187 0x00BB No se encontró el nombre del semáforo de sistema especificado.

- 188 0x00BC El sistema operativo no puede ejecutar %1.
- 189 0x00BD El sistema operativo no puede ejecutar %1.
- 190 0x00BE El sistema operativo no puede ejecutar %1.
- 191 0x00BF No se puede ejecutar %1 en modo Win32.
- 192 0x00C0 El sistema operativo no puede ejecutar %1.
- 193 0x00C1 %1 no es una aplicación Win32 válida.
- 194 0x00C2 El sistema operativo no puede ejecutar %1.
- 195 0x00C3 El sistema operativo no puede ejecutar %1.
- 196 0x00C4 El sistema operativo no puede ejecutar esta aplicación.
- 197 0x00C5 El sistema operativo no está configurado para ejecutar esta aplicación.
- 198 0x00C6 El sistema operativo no puede ejecutar %1.
- 199 0x00C7 El sistema operativo no puede ejecutar esta aplicación.
- 200 0x00C8 El segmento de código debe ser menor que 64 KB.
- 201 0x00C9 El sistema operativo no puede ejecutar %1.
- 202 0x00CA El sistema operativo no puede ejecutar %1.
- 203 0x00CB El sistema no encontró la opción de entorno que se había especificado.
- 205 0x00CD No hay ningún proceso en el subárbol de comandos que tenga un identificador de señales.
- 206 0x00CE El nombre del archivo o la extensión es demasiado largo.
- 207 0x00CF Se está usando la pila de anillo 2.
- 208 0x00D0 Los caracteres globales del nombre de archivo, * o ?, se han escrito incorrectamente, o bien se han especificado demasiados caracteres globales.
- 209 0x00D1 La señal fijada no es correcta.
- 210 0x00D2 No se puede establecer el identificador de señales.
- 212 0x00D4 El segmento está bloqueado y no se puede reasignar.
- 214 0x00D6 Hay demasiados módulos de vínculo dinámico anexados a este programa o módulo de vínculo dinámico.
- 215 0x00D7 No se pueden anidar las llamadas a *LoadModule*.
- 230 0x00E6 El estado de la canalización no es válido.
- 231 0x00E7 Todas las instancias de canalización están en uso.
- 232 0x00E8 Se está cerrando la canalización.
- 233 0x00E9 No hay ningún proceso en el otro extremo de la canalización.
- 234 0x00EA Hay más datos disponibles.
- 240 0x00F0 Se ha cancelado la sesión.
- 254 0x00FE El nombre del atributo extendido especificado no es válido.
- 255 0x00FF Los atributos extendidos no son consistentes.
- 259 0x0103 No se dispone de más datos.
- 266 0x010A No se puede utilizar la API de copia.
- 267 0x010B El nombre del directorio no es válido.
- 275 0x0113 No se pueden cargar los atributos extendidos en el búfer.

276 0x0114 El archivo de atributos extendidos en el sistema de archivos está dañado.

277 0x0115 El archivo de la tabla de atributos extendidos está llena.

278 0x0116 El identificador del atributo extendido no es válido.

282 0x011A El sistema de archivos no permite atributos extendidos.

288 0x0120 Se ha intentado liberar una exclusión mutua no perteneciente al proceso.

298 0x012A Se han realizado demasiados envíos a un semáforo.

299 0x012B Sólo se ha completado parte de la petición *Read/WriteProcessMemory*.

317 0x013D El sistema no ha encontrado el mensaje para el mensaje número 0x%1, en el archivo de mensajes, para %2.

487 0x01E7 Se ha intentado tener acceso a una dirección no válida.

534 0x0216 El resultado aritmético sobrepasa los 32 *bits*.

535 0x0217 Hay un proceso en el otro extremo de la canalización.

536 0x0218 Esperando a que un proceso abra el otro extremo de la canalización.

994 0x03E2 Denegado el acceso al atributo extendido.

995 0x03E3 La operación de E/S se ha anulado debido a una salida de subprocesso o a una petición de aplicación.

996 0x03E4 El suceso de E/S superpuesto no está en estado con señal.

997 0x03E5 Se está ejecutando la operación de E/S superpuesta.

998 0x03E6 El acceso a la dirección de memoria no es válido.

999 0x03E7 Error al ejecutar la operación de paginación.

1001 0x03E9 La recursividad tiene demasiados niveles; se ha desbordado la pila.

1002 0x03EA La ventana no puede manipular el mensaje enviado.

1003 0x03EB No se puede completar esta función.

1004 0x03EC Los indicadores no son válidos.

1005 0x03ED El volumen no contiene un sistema de archivos reconocible. Asegúrese de que estén cargados todos los controladores necesarios del sistema de archivos y de que el volumen no esté dañado.

1006 0x03EE Se ha alterado externamente el volumen de un archivo de tal forma que el archivo abierto ya no es válido.

1007 0x03EF Esta operación no se puede ejecutar en el modo de pantalla completa.

1008 0x03F0 Se ha intentado hacer referencia a un testigo que no existe.

1009 0x03F1 La base de datos del Registro de configuraciones está dañada.

1010 0x03F2 La clave del Registro de configuraciones no es válida.

1011 0x03F3 No se puede abrir la clave del Registro de configuraciones.

1012 0x03F4 No se puede leer la clave del Registro de configuraciones.

1013 0x03F5 No se puede escribir la clave del Registro de configuraciones.

1014 0x03F6 Se ha tenido que recuperar uno de los archivos del Registro usando un registro o copia alternativa. Se ha recuperado en su totalidad.

1015 0x03F7 El Registro de configuraciones está dañado. La estructura de uno de los archivos o la imagen del sistema del archivo en memoria están dañados, o el archivo no se puede recuperar debido a que falta la copia o está dañada.

- 1016 0x03F8 Error en una operación de E/S iniciada por el Registro. El Registro no puede leer, escribir o descargar uno de los archivo con la imagen de sistema del Registro.
- 1017 0x03F9 El sistema ha intentado cargar o restaurar un archivo en el Registro pero el archivo especificado no tiene el formato de un archivo de Registros.
- 1018 0x03FA Se ha intentado realizar una operación ilegal en una clave de Registro que ya estaba marcada para su eliminación.
- 1019 0x03FB El sistema no puede asignar el espacio necesario en un registro del Registro.
- 1020 0x03FC No se puede crear un vínculo simbólico en una clave del Registro que ya dispone de subclaves o valores.
- 1021 0x03FD No se puede crear una subclave estable en una clave primaria volátil.
- 1022 0x03FE Se está completando una solicitud de notificación de cambio y la información no está siendo devuelta al búfer del llamador. El llamador debe enumerar ahora los archivos para buscar los cambios.
- 1051 0x041B Se ha enviado un control de parada a un servicio del que dependen otros servicios en ejecución.
- 1052 0x041C El control requerido para este servicio no es válido
- 1053 0x041D El servicio no ha respondido a la petición o inicio del control en un tiempo adecuado.
- 1054 0x041E No se puede crear un subproceso para el servicio.
- 1055 0x041F La base de datos de servicios está bloqueada.
- 1056 0x0420 Ya se está ejecutando una instancia de este servicio.
- 1057 0x0421 El nombre de la cuenta no es válido o no existe.
- 1058 0x0422 El servicio especificado está desactivado y no se puede iniciar.
- 1059 0x0423 Se ha especificado una dependencia de servicio circular.
- 1060 0x0424 El servicio especificado no existe como servicio instalado.
- 1061 0x0425 El servicio no acepta mensajes de control en este momento.
- 1062 0x0426 No se ha iniciado el servicio.
- 1063 0x0427 El proceso del servicio no puede conectar con el controlador del servicio.
- 1064 0x0428 Error de excepción en el servicio al manipular la petición de control.
- 1065 0x0429 La base de datos especificada no existe.
- 1066 0x042A El servicio ha devuelto un error específico del servicio.
- 1067 0x042B El proceso ha terminado de forma inesperada.
- 1068 0x042C No se puede iniciar el servicio o grupo de dependencia.
- 1069 0x042D No se puede iniciar el servicio debido a un error en el inicio de sesión.
- 1070 0x042E Después de iniciarse, el servicio ha quedado en un estado pendiente de inicio.
- 1071 0x042F El bloqueo de la base de datos del servicio especificado no es válido.
- 1072 0x0430 El servicio especificado se ha marcado para ser eliminado.
- 1073 0x0431 El servicio especificado ya existe.
- 1074 0x0432 Se está ejecutando el sistema con la última configuración que se sabe que no tiene problemas.
- 1075 0x0433 El servicio de dependencia no existe o se ha marcado para ser eliminado.

- 1076 0x0434 Ya se ha aceptado la inicialización actual para usarse como el control de la última configuración que se sabe que no tiene problemas.
- 1077 0x0435 No se ha intentado iniciar el servicio desde la última inicialización.
- 1078 0x0436 El nombre ya es usado como nombre de servicio o como nombre de presentación de servicios.
- 1100 0x044C Se ha llegado al final de la cinta.
- 1101 0x044D Un acceso de cinta ha alcanzado una marca de archivo.
- 1102 0x044E Se ha encontrado el inicio de una cinta o de una partición.
- 1103 0x044F Un acceso de cinta alcanzó el final de un grupo de archivos.
- 1104 0x0450 No hay más datos en la cinta.
- 1105 0x0451 No se puede efectuar la partición de la cinta.
- 1106 0x0452 Al tener acceso a una nueva cinta de una partición multivolumen, el tamaño de bloque actual no es correcto.
- 1107 0x0453 No se ha encontrado la información de partición al cargar la cinta.
- 1108 0x0454 No se puede bloquear el mecanismo de expulsión de la cinta.
- 1109 0x0455 No se puede descargar el medio.
- 1110 0x0456 Puede que el medio en la unidad haya cambiado.
- 1111 0x0457 Se ha restablecido el bus de E/S.
- 1112 0x0458 La unidad está vacía.
- 1113 0x0459 No hay ninguna asignación en la página de códigos de múltiples *bytes* de destino para el carácter *Unicode*.
- 1114 0x045A Error en una rutina de inicialización de biblioteca de vínculos dinámicos (DLL).
- 1115 0x045B Se está cerrando el sistema.
- 1116 0x045C No se puede anular el apagado del sistema porque no se estaba apagando.
- 1117 0x045D No se puede ejecutar el proceso debido a un error del dispositivo de E/S.
- 1118 0x045E No se ha inicializado ningún dispositivo serie. Se descargará el controlador serie.
- 1119 0x045F No se puede abrir un dispositivo que compartía una IRQ con otros dispositivos. Hay al menos otro dispositivo abierto que utiliza ese IRQ.
- 1120 0x0460 Una operación serie de E/S fue realizada por otra escritura en el puerto serie. (El *IOCTL_SERIAL_XOFF_COUNTER* alcanzó cero.)
- 1121 0x0461 Se completó una operación de E/S a causa de la finalización del tiempo de espera. (El *IOCTL_SERIAL_XOFF_COUNTER* no alcanzó cero.)
- 1122 0x0462 No se ha encontrado una marca de identificador de dirección en el disco.
- 1123 0x0463 Existe una mala adaptación entre el campo del identificador del disco y la dirección de la pista del controlador del disco.
- 1124 0x0464 El controlador de disco ha enviado un error que el controlador de la unidad de disco no reconoce.
- 1125 0x0465 El controlador de discos ha devuelto resultados incoherentes en los registros.
- 1126 0x0466 Error en la operación de calibración mientras se tenía acceso al disco duro, incluso después de varios intentos.

- 1127 0x0467 Error en la operación de disco mientras se tenía acceso al disco duro, incluso después de varios intentos.
- 1128 0x0468 Fue preciso restablecer el controlador de disco mientras se tenía acceso al disco duro, pero también produjo un error.
- 1129 0x0469 Ha llegado al final de la cinta.
- 1130 0x046A Espacio de almacenamiento insuficiente en el servidor para procesar este comando.
- 1131 0x046B Se ha detectado una posibilidad de que ocurra un interbloqueo.
- 1132 0x046C La dirección base o el desajuste del archivo no tiene la alineación adecuada.
- 1140 0x0474 El intento de cambiar el estado de la energía fue impedido por otra aplicación o controlador.
- 1141 0x0475 El BIOS del sistema no puede cambiar el estado de energía del sistema.
- 1150 0x047E El programa especificado requiere una versión de *Windows* más reciente.
- 1151 0x047F El programa especificado no es un programa de *Windows* o de MS-DOS.
- 1152 0x0480 No se puede iniciar más de una instancia del programa especificado.
- 1153 0x0481 El programa especificado se escribió para una versión anterior de *Windows*.
- 1154 0x0482 Uno de los archivos de biblioteca necesario para ejecutar esta aplicación está dañado .
- 1155 0x0483 No hay ninguna aplicación asociada con el archivo especificado para esta operación.
- 1156 0x0484 Error al enviar el comando a la aplicación.
- 1157 0x0485 No se puede hallar uno de los archivos de biblioteca necesarios para ejecutar esta aplicación.
- 1200 0x04B0 El nombre del dispositivo no es válido.
- 1201 0x04B1 El dispositivo no está conectado pero es una conexión memorizada.
- 1202 0x04B2 Se ha intentado memorizar un dispositivo que ya había sido memorizado.
- 1203 0x04B3 Ningún proveedor de red ha aceptado la ruta de acceso de la red.
- 1204 0x04B4 El nombre del proveedor de red no es válido.
- 1205 0x04B5 No se puede abrir el perfil de conexión de red.
- 1206 0x04B6 El perfil de conexión de red está dañado.
- 1207 0x04B7 No se puede enumerar algo vacío.
- 1208 0x04B8 Error extendido.
- 1209 0x04B9 El formato del nombre de grupo especificado no es válido.
- 1210 0x04BA El formato del nombre de sistema especificado no es válido.
- 1211 0x04BB El formato del nombre de suceso especificado no es válido.
- 1212 0x04BC El formato del nombre de dominio especificado no es válido.
- 1213 0x04BD El formato del nombre de servicio especificado no es válido.
- 1214 0x04BE El formato del nombre de red especificado no es válido.
- 1215 0x04BF El formato del nombre de recurso compartido especificado no es válido.
- 1216 0x04C0 El formato del nombre de contraseña especificado no es válido.
- 1217 0x04C1 El formato del nombre de mensaje especificado no es válido.
- 1218 0x04C2 El formato del destino de mensaje especificado no es válido.
- 1219 0x04C3 Las credenciales suministradas entran en conflicto con un conjunto de credenciales

existentes.

- 1220 0x04C4 Se ha intentado establecer una sesión en un servidor de red pero ya se han establecido demasiadas sesiones en ese servidor.
- 1221 0x04C5 El nombre de dominio o grupo de trabajo ya está en uso por otro equipo en la red.
- 1222 0x04C6 Falta la red o bien no se ha iniciado.
- 1223 0x04C7 El usuario ha cancelado la operación.
- 1224 0x04C8 No se puede realizar la operación solicitada en un archivo con una sección asignada de usuario abierta.
- 1225 0x04C9 El sistema remoto ha rechazado la conexión de red.
- 1226 0x04CA La conexión de red se cerró correctamente.
- 1227 0x04CB El punto final del transporte de red ya tiene una dirección asociada con él.
- 1228 0x04CC Todavía no se ha asociado una dirección con el punto final de red.
- 1229 0x04CD Se ha intentado una operación en una conexión de red no existente.
- 1230 0x04CE Se ha intentado una operación no válida en una conexión de red activa.
- 1231 0x04CF El transporte no tiene acceso a la red remota.
- 1232 0x04D0 El transporte no tiene acceso al sistema remoto.
- 1233 0x04D1 El sistema remoto no es compatible con el protocolo de transporte.
- 1234 0x04D2 No hay ningún servicio operativo en el punto final de red destino en el sistema remoto.
- 1235 0x04D3 La petición ha sido cancelada.
- 1236 0x04D4 La conexión de red ha sido cancelada por el sistema local.
- 1237 0x04D5 No se puede completar la operación. Se debería volver a intentarlo.
- 1238 0x04D6 No se puede realizar una conexión con el servidor porque se ha alcanzado el número límite de conexiones concurrentes para esta cuenta.
- 1239 0x04D7 Se ha intentado iniciar la sesión durante una hora del día no autorizada para esta cuenta.
- 1240 0x04D8 La cuenta no está autorizada a iniciar la sesión desde esta estación.
- 1241 0x04D9 No se puede usar la dirección de red para la operación solicitada.
- 1242 0x04DA El servicio ya está registrado.
- 1243 0x04DB El servicio especificado no existe.
- 1244 0x04DC La operación requerida no se ha realizado porque no se ha reconocido al usuario.
- 1245 0x04DD La operación requerida no se ha realizado porque el usuario no ha iniciado sesión en la red. El servicio especificado no existe.
- 1246 0x04DE Indica que desea que quien llama continúe el trabajo en curso.
- 1247 0x04DF Se intentó efectuar una operación de inicialización cuando la inicialización ya había sido completada.
- 1248 0x04E0 No hay más dispositivos locales.
- 1300 0x0514 No todos los privilegios a los que se hace referencia son asignados al llamador.
- 1301 0x0515 No se han efectuado algunas asignaciones entre los nombres de cuenta y los identificadores de seguridad.
- 1302 0x0516 No se han especificado límites de cuota de sistema para esta cuenta.
- 1303 0x0517 Se ha devuelto una clave de cifrado ya conocida.

- 1304 0x0518 La contraseña de NT es demasiado compleja para convertirla a una de LAN Manager. La contraseña devuelta por LAN Manager es una cadena nula.
- 1305 0x0519 No se conoce el nivel de revisión.
- 1306 0x051A Indica que dos niveles de revisión son incompatibles.
- 1307 0x051B No se puede asignar este identificador de seguridad como propietario del objeto.
- 1308 0x051C No se puede asignar este identificador como el grupo primario de un objeto.
- 1309 0x051D Un subproceso ha intentado realizar una operación en una imitación de *token* cuando dicho subproceso no representa a un cliente.
- 1310 0x051E No se puede desactivar el grupo.
- 1311 0x051F No hay servidores de inicio de sesión disponibles para atender la petición de inicio de sesión.
- 1312 0x0520 La sesión de inicio especificada no existe. Puede que ya haya terminado.
- 1313 0x0521 No existe el privilegio especificado.
- 1314 0x0522 El cliente no dispone de un privilegio requerido.
- 1315 0x0523 El nombre proporcionado no es un nombre de cuenta con la estructura correcta.
- 1316 0x0524 El usuario especificado ya existe.
- 1317 0x0525 El usuario especificado no existe.
- 1318 0x0526 El grupo especificado ya existe.
- 1319 0x0527 El grupo especificado no existe.
- 1320 0x0528 La cuenta de usuario ya es miembro del grupo especificado o no se puede eliminar el grupo porque todavía contiene un miembro.
- 1321 0x0529 La cuenta de usuario especificada no es miembro de la cuenta de grupo indicada.
- 1322 0x052A No se puede desactivar o eliminar la última cuenta administrativa.
- 1323 0x052B No se puede actualizar la contraseña. La contraseña especificada como actual no es correcta.
- 1324 0x052C El valor de la nueva contraseña contiene valores que no se permiten en las contraseñas.
- 1325 0x052D No se puede actualizar la contraseña porque se han violado las normas del cambio de contraseña.
- 1326 0x052E Se desconoce el nombre de usuario o la contraseña no es correcta.
- 1327 0x052F Error de inicio de sesión: restricción en la cuenta de usuario.
- 1328 0x0530 Error de inicio de sesión: infracción en la restricción de la hora de inicio.
- 1329 0x0531 Error de inicio de sesión: el usuario no tiene permiso para tener acceso a este equipo.
- 1330 0x0532 Error de inicio de sesión: la contraseña ha caducado.
- 1331 0x0533 Error de inicio de sesión: la cuenta está desactivada.
- 1332 0x0534 No se ha efectuado ninguna asignación entre los nombres de cuenta y los identificadores de seguridad.
- 1333 0x0535 Se han pedido demasiados identificadores de usuario local (LUID) al mismo tiempo.
- 1334 0x0536 No hay más identificadores de usuario local (LUID) disponibles.
- 1335 0x0537 La parte de subautoridad del identificador de seguridad no es válida para este uso en particular.

- 1336 0x0538 La estructura de la lista de control de acceso (ACL) no es válida.
- 1337 0x0539 La estructura del identificador de seguridad no es válida.
- 1338 0x053A La estructura del descriptor de seguridad no es válida.
- 1340 0x053C No se puede construir la lista de control de acceso (ACL) o la entrada de control de acceso (ACE) heredada.
- 1341 0x053D El servidor está desactivado.
- 1342 0x053E El servidor está activado.
- 1343 0x053F El valor no es válido para una autoridad de identificación.
- 1344 0x0540 Memoria insuficiente para la actualización de la información de seguridad.
- 1345 0x0541 Los atributos especificados no son válidos o son incompatibles con los atributos del grupo en conjunto.
- 1346 0x0542 El nivel de representación no es válido.
- 1347 0x0543 No se puede abrir un testigo de seguridad de nivel anónimo.
- 1348 0x0544 La clase de información de validación solicitada no es válida.
- 1349 0x0545 El tipo de testigo no es apropiado para el uso que se ha intentado hacer de él.
- 1350 0x0546 No se puede ejecutar una operación de seguridad en un objeto que no tiene una seguridad asociada.
- 1351 0x0547 Indica que no se tiene acceso a un servidor *Windows* NT Server o que los objetos de ese dominio están protegidos de tal modo que no es posible recuperar la información necesaria.
- 1352 0x0548 El servidor de autoridad de seguridad local (LSA) o el administrador de cuentas de seguridad (SAM) no se encontraba en un estado adecuado para ejecutar la operación de seguridad.
- 1353 0x0549 El dominio no se encontraba en el estado adecuado para ejecutar la operación de seguridad.
- 1354 0x054A Sólo se permite esta operación al controlador principal de dominio del dominio.
- 1355 0x054B El dominio especificado no existe.
- 1356 0x054C El dominio especificado ya existe.
- 1357 0x054D Se ha intentado exceder el límite en el número de dominios por servidor.
- 1358 0x054E No se puede completar la operación porque se ha detectado un error grave del medio o daños en la estructura de datos del disco.
- 1359 0x054F La base de datos de la cuenta de seguridad contiene inconsistencias internas.
- 1360 0x0550 Se han detectado accesos de tipo genérico en una máscara de acceso que ya deberían haberse asignado a tipos no genéricos.
- 1361 0x0551 Un descriptor de seguridad no está en el formato correcto (absoluto o autorelativo).
- 1362 0x0552 Esta acción está restringida a su uso por procesos de inicio de sesión. El proceso no se ha registrado como un proceso de inicio de sesión.
- 1363 0x0553 No se puede iniciar un nuevo inicio de sesión con un identificador que ya está en uso.
- 1364 0x0554 No se conoce el paquete de autenticación especificado.
- 1365 0x0555 La sesión de inicio no es consistente con la operación solicitada.
- 1366 0x0556 Ya se está utilizando el identificador de inicio de sesión.
- 1367 0x0557 Una petición de inicio de sesión contenía un valor de tipo de inicio de sesión no válido.

- 1368 0x0558 No se puede representar vía una canalización con nombre hasta que se hayan leído los datos de esa canalización.
- 1369 0x0559 El estado de transacción de un subárbol del Registro no es compatible con la operación.
- 1370 0x055A Se han detectado daños en la base de datos de seguridad interna.
- 1371 0x055B No se puede ejecutar esta operación en las cuentas internas.
- 1372 0x055C No se puede ejecutar esta operación en este grupo especial incorporado.
- 1373 0x055D No se puede ejecutar esta operación en este usuario especial incorporado.
- 1374 0x055E No se puede quitar al usuario de un grupo porque es el grupo primario de este usuario.
- 1375 0x055F El testigo ya se está usando como testigo primario.
- 1376 0x0560 El grupo local especificado no existe.
- 1377 0x0561 El nombre de cuenta especificado no es miembro del grupo local.
- 1378 0x0562 El nombre de cuenta especificado ya es miembro del grupo local.
- 1379 0x0563 El grupo local especificado ya existe.
- 1380 0x0564 No se ha concedido al usuario este tipo de inicio de sesión en este equipo.
- 1381 0x0565 Se ha excedido el máximo número de secretos que se pueden guardar en un único sistema.
- 1382 0x0566 La longitud de un secreto excede la longitud máxima permitida.
- 1383 0x0567 Existe una inconsistencia en la base de datos de la autoridad de seguridad local.
- 1384 0x0568 Durante el inicio de sesión, el contexto de seguridad del usuario ha acumulado demasiados identificadores de seguridad.
- 1385 0x0569 Error de inicio de sesión: no se ha concedido al usuario este tipo de inicio de sesión en este equipo.
- 1386 0x056A Se necesita una contraseña con cifrado cruzado para cambiar una contraseña de usuario.
- 1387 0x056B No se puede agregar un nuevo miembro al grupo local porque el miembro no existe.
- 1388 0x056C No se puede agregar un nuevo miembro a un grupo local porque el miembro tiene un tipo de cuenta incorrecto.
- 1389 0x056D Se han especificado demasiados identificadores de seguridad.
- 1390 0x056E Para cambiar esta contraseña de usuario es necesario una contraseña con cifrado cruzado.
- 1391 0x056F Indica que una lista de control de acceso contiene componentes no hereditarios
- 1392 0x0570 El archivo o directorio está dañado y no se puede leer.
- 1393 0x0571 La estructura del disco está dañada y no se puede leer.
- 1394 0x0572 No existe una clave de sesión de usuario para el inicio de sesión especificado.
- 1395 0x0573 El servicio al que está intentando obtener acceso tiene licencia para un número concreto de conexiones. No se pueden establecer más conexiones ahora porque hay tantas conexiones como las que acepta el servicio.
- 1400 0x0578 El identificador de la ventana no es válido.
- 1401 0x0579 El identificador del menú no es válido.
- 1402 0x057A El identificador del cursor no es válido.
- 1403 0x057B El identificador de la tabla de aceleración no es válido.

- 1404 0x057C El identificador del enlace no es válido.
- 1405 0x057D El identificador de una estructura de posición de ventana múltiples no es válido.
- 1406 0x057E No se puede crear una ventana secundaria de primer nivel.
- 1407 0x057F No se ha encontrado la clase de ventana.
- 1408 0x0580 La ventana no es válida. Pertenece a otro subproceso.
- 1409 0x0581 Ya se ha registrado la tecla de acceso rápido.
- 1410 0x0582 Esta clase ya existe.
- 1411 0x0583 Esta clase no existe.
- 1412 0x0584 La clase todavía tiene ventanas abiertas.
- 1413 0x0585 El índice no es válido.
- 1414 0x0586 El identificador de icono no es válido.
- 1415 0x0587 Se están utilizando palabras privadas de ventana de diálogo.
- 1416 0x0588 No se ha encontrado el identificador del cuadro de listas.
- 1417 0x0589 No se han encontrado comodines.
- 1418 0x058A El subproceso no tiene abierto un Portapapeles.
- 1419 0x058B La tecla de aceleración no está registrada.
- 1420 0x058C Esta ventana no es una ventana de diálogo válida.
- 1421 0x058D No se ha encontrado el identificador de control.
- 1422 0x058E El mensaje no es válido porque el cuadro combinado no tiene un control de edición.
- 1423 0x058F La ventana no es un cuadro combinado.
- 1424 0x0590 El alto debe ser menor que 256.
- 1425 0x0591 El identificador del contexto de dispositivo (DC) no es válido.
- 1426 0x0592 El tipo de procedimiento de enlace no es válido.
- 1427 0x0593 El procedimiento de enlace no es válido.
- 1428 0x0594 No se puede establecer un enlace no local sin un identificador de módulo.
- 1429 0x0595 Este procedimiento de enlace sólo se puede establecer de forma global.
- 1430 0x0596 El procedimiento de enlace diario ya se ha instalado.
- 1431 0x0597 El procedimiento de enlace no se ha instalado.
- 1432 0x0598 El mensaje del cuadro de lista de selección única no es válido.
- 1433 0x0599 *LB_SETCOUNT* enviado a cuadro de lista de tipo *non-lazy*.
- 1434 0x059A El cuadro de lista no admite tabulaciones.
- 1435 0x059B No se puede destruir un objeto creado por otro subproceso.
- 1436 0x059C Las ventanas secundarias no pueden tener menús.
- 1437 0x059D La ventana no tiene un menú de sistema.
- 1438 0x059E El estilo del cuadro de mensaje no es válido.
- 1439 0x059F El parámetro (SPI_*) para todo el sistema no es válido.
- 1440 0x05A0 La pantalla ya está bloqueada.
- 1441 0x05A1 Todos los identificadores de ventana en una estructura de posición de ventanas múltiples deben tener el mismo predecesor.
- 1442 0x05A2 La ventana no es una ventana secundaria.

- 1443 0x05A3 Comando GW_* no válido.
- 1444 0x05A4 El identificador del subproceso no es válido.
- 1445 0x05A5 No se puede procesar un mensaje de una ventana que no sea una ventana de interfaz de múltiples documentos (MDI).
- 1446 0x05A6 El menú emergente ya está activo.
- 1447 0x05A7 La ventana no tiene barras de desplazamiento.
- 1448 0x05A8 El intervalo de las barras de desplazamiento no puede ser mayor que 0x7FFF.
- 1449 0x05A9 No se puede mostrar o quitar la ventana de la forma especificada.
- 1450 0x05AA Recursos insuficientes en el sistema para completar el servicio solicitado.
- 1451 0x05AB Recursos insuficientes en el sistema para completar el servicio solicitado.
- 1452 0x05AC Recursos insuficientes en el sistema para completar el servicio solicitado.
- 1453 0x05AD Cuota insuficiente para completar el servicio solicitado.
- 1454 0x05AE Cuota insuficiente para completar el servicio solicitado.
- 1455 0x05AF El archivo de paginación es demasiado pequeño para completar la operación.
- 1456 0x05B0 No se encontró un elemento de menú.
- 1500 0x05DC El archivo con el Registro de sucesos está dañado.
- 1501 0x05DD No se puede abrir el Registro de sucesos por lo que no se ha iniciado el servicio.
- 1502 0x05DE El archivo de Registros de sucesos está lleno.
- 1503 0x05DF El archivo de Registro de sucesos ha cambiado entre lecturas.
- 1700 0x06A4 El enlace de cadenas no es válido.
- 1701 0x06A5 El identificador de enlace no es del tipo adecuado.
- 1702 0x06A6 El identificador de enlace no es válido.
- 1703 0x06A7 Secuencia de protocolo RPC incompatible.
- 1704 0x06A8 Secuencia de protocolo RPC no válida.
- 1705 0x06A9 El identificador único universal (UUID) de cadena no es válido.
- 1706 0x06AA El formato del extremo no es válido.
- 1707 0x06AB La dirección de red no es válida.
- 1708 0x06AC No se ha encontrado ningún extremo.
- 1709 0x06AD El valor de tiempo de espera no es válido.
- 1710 0x06AE No se ha encontrado el identificador único universal (UUID) de objeto.
- 1711 0x06AF Ya se ha registrado el identificador único universal (UUID) de objeto.
- 1712 0x06B0 Ya se ha registrado el identificador único universal (UUID) de tipo.
- 1713 0x06B1 El servidor RPC ya está en línea.
- 1714 0x06B2 No se han registrado secuencias de protocolo.
- 1715 0x06B3 El servidor RPC no está en línea.
- 1716 0x06B4 Tipo de administrador desconocido.
- 1717 0x06B5 Interfaz desconocida.
- 1718 0x06B6 No hay enlaces.
- 1719 0x06B7 No hay secuencias de protocolo.
- 1720 0x06B8 No se puede crear el extremo.

- 1721 0x06B9 Recursos insuficientes para completar esta operación.
- 1722 0x06BA El servidor RPC no está disponible.
- 1723 0x06BB El servidor RPC está demasiado ocupado para completar esta operación.
- 1724 0x06BC Las opciones de red no son válidas.
- 1725 0x06BD No hay ninguna llamada a procedimiento remoto que esté activa en este subproceso.
- 1726 0x06BE Error en la llamada a procedimiento remoto.
- 1727 0x06BF Error en la llamada a procedimiento remoto y no se ha ejecutado.
- 1728 0x06C0 Error del protocolo de llamada a procedimiento remoto (RPC).
- 1730 0x06C2 La sintaxis de transferencia no es compatible con el servidor RPC.
- 1732 0x06C4 El tipo de identificador único universal (UUID) no está permitido.
- 1733 0x06C5 La etiqueta no es válida.
- 1734 0x06C6 Los límites de matriz no son válidos.
- 1735 0x06C7 El enlace no contiene ningún nombre de entrada.
- 1736 0x06C8 La sintaxis del nombre no es válida.
- 1737 0x06C9 La sintaxis del nombre no es compatible.
- 1739 0x06CB No hay ninguna dirección de red disponible para construir un identificador único universal (UUID).
- 1740 0x06CC El extremo es un duplicado.
- 1741 0x06CD Tipo de autenticación desconocido.
- 1742 0x06CE El número máximo de llamadas es demasiado pequeño.
- 1743 0x06CF La cadena es demasiado larga.
- 1744 0x06D0 No se ha encontrado la secuencia de protocolo RPC.
- 1745 0x06D1 El número de procedimiento está fuera del intervalo permitido.
- 1746 0x06D2 El enlace no contiene información de autenticación.
- 1747 0x06D3 Servicio de autorización desconocido.
- 1748 0x06D4 No se conoce el nivel de autenticación.
- 1749 0x06D5 El contexto de seguridad no es válido.
- 1750 0x06D6 No se conoce el servicio de autenticación.
- 1751 0x06D7 La entrada no es válida.
- 1752 0x06D8 El extremo de servidor no puede ejecutar la operación.
- 1753 0x06D9 No hay más extremos disponibles desde el asignador de extremos.
- 1754 0x06DA No se han exportado interfaces.
- 1755 0x06DB El nombre de la entrada está incompleto.
- 1756 0x06DC La opción de versión no es válida.
- 1757 0x06DD No hay más miembros.
- 1758 0x06DE No hay nada que pueda dejar de exportarse.
- 1759 0x06DF No se ha encontrado la interfaz.
- 1760 0x06E0 La entrada ya existe.
- 1761 0x06E1 No se ha encontrado la entrada.
- 1762 0x06E2 El servicio de nombres no está disponible.

- 1763 0x06E3 La familia de direcciones de red no es válida.
- 1764 0x06E4 Esta operación no es compatible.
- 1765 0x06E5 No hay contexto de seguridad disponible para permitir representaciones.
- 1766 0x06E6 Error interno en una llamada a procedimiento remoto (RPC).
- 1767 0x06E7 El servidor de RPC ha intentado una división entre cero.
- 1768 0x06E8 Error de direccionamiento en el servidor RPC.
- 1769 0x06E9 Una operación en punto flotante en el servidor de RPC ha causado una división entre cero.
- 1770 0x06EA Subdesbordamiento de punto flotante en el servidor de *RPC*.
- 1771 0x06EB Desbordamiento de punto flotante en el servidor de *RPC*.
- 1772 0x06EC Se ha agotado la lista de servidores *RPC* disponibles para el enlace de identificadores automáticos.
- 1773 0x06ED No se puede abrir el archivo con la tabla de traducción de caracteres.
- 1774 0x06EE El archivo con la tabla de traducción de caracteres tiene menos de 512 *bytes*.
- 1775 0x06EF Un identificador nulo de contexto se pasó del cliente al *host* durante una llamada a procedimiento remoto.
- 1777 0x06F1 El identificador de contexto ha cambiado durante una llamada de procedimiento remoto.
- 1778 0x06F2 Los manipuladores de enlace pasados a una llamada a procedimiento remoto no coinciden.
- 1779 0x06F3 La etiqueta no puede tener acceso al identificador de la llamada de procedimiento remoto.
- 1780 0x06F4 Se pasó un puntero de referencia nulo a la rutina con código no ejecutable.
- 1781 0x06F5 El valor de enumeración está fuera del intervalo permitido.
- 1782 0x06F6 El número de *bytes* es demasiado pequeño.
- 1783 0x06F7 El fragmento ha recibido datos incorrectos.
- 1784 0x06F8 El búfer del usuario no es válido para esta operación.
- 1785 0x06F9 El disco no es reconocido. Puede que no esté formateado.
- 1786 0x06FA La estación de trabajo no tiene un secreto de confianza.
- 1787 0x06FB La base de datos *SAM* en *Windows NT Server* no tiene una cuenta de equipo para la relación de confianza de esta estación de trabajo.
- 1788 0x06FC Error en la relación de confianza entre el dominio principal y el dominio en el que se confía.
- 1789 0x06FD Error en la relación de confianza entre la estación de trabajo y el dominio principal.
- 1790 0x06FE Error en el inicio de sesión de la red.
- 1791 0x06FF Ya hay una llamada a procedimiento remoto en curso para este subproceso.
- 1792 0x0700 Se ha intentado iniciar la sesión pero el servicio de inicio de sesión de la red no se ha iniciado.
- 1793 0x0701 La cuenta del usuario ha caducado.
- 1794 0x0702 Se está usando el redirector y no se puede descargar.
- 1795 0x0703 El controlador de impresora ya está instalado.

- 1796 0x0704 No se conoce el puerto especificado.
- 1797 0x0705 No se conoce el controlador de impresora.
- 1798 0x0706 No se conoce el procesador de impresora.
- 1799 0x0707 El archivo separador especificado no es válido.
- 1800 0x0708 La prioridad especificada no es válida.
- 1801 0x0709 El nombre de la impresora no es válido.
- 1802 0x070A Esta impresora ya existe.
- 1803 0x070B El comando de impresora no es válido.
- 1804 0x070C El tipo de dato especificado no es válido.
- 1805 0x070D El entorno especificado no es válido.
- 1806 0x070E No hay más enlaces.
- 1807 0x070F La cuenta usada es una cuenta de confianza entre dominios. Utilice su cuenta de usuario global o una cuenta de usuario local para tener acceso a este servidor.
- 1808 0x0710 La cuenta utilizada es una cuenta de equipo. Utilice su cuenta de usuario global o una cuenta de usuario local para tener acceso a este servidor.
- 1809 0x0711 La cuenta usada es una cuenta de confianza de servidor. Utilice su cuenta de usuario global o la cuenta de usuario local para tener acceso a este servidor.
- 1810 0x0712 El nombre o el identificador de seguridad (SID) del dominio no es consistente con la información de confianza para ese dominio.
- 1811 0x0713 Se está utilizando el servidor y no se puede descargar.
- 1812 0x0714 El archivo imagen no contenía sección de recursos.
- 1813 0x0715 No se puede encontrar el tipo de recurso en el archivo imagen.
- 1814 0x0716 No se ha encontrado el nombre de recurso en el archivo imagen.
- 1815 0x0717 No se puede encontrar el recurso de identificador de idioma en el archivo de imagen.
- 1816 0x0718 Cuota insuficiente para procesar este comando.
- 1817 0x0719 No se han registrado interfaces.
- 1818 0x071A El servidor ha sido alterado mientras se procesaba esta llamada.
- 1819 0x071B El manipulador de enlace no contiene toda la información requerida.
- 1820 0x071C Error de comunicación.
- 1821 0x071D El nivel de autenticación requerido no es compatible.
- 1822 0x071E No se ha registrado un nombre principal.
- 1823 0x071F El error especificado no es un error de código de *Windows* RPC válido.
- 1824 0x0720 Se ha asignado un UUID que es válido sólo en este equipo.
- 1825 0x0721 Error específico de paquete de seguridad.
- 1826 0x0722 El subproceso no está cancelado.
- 1827 0x0723 Operación no válida en el identificador de codificación/descodificación.
- 1828 0x0724 Versión incompatible del paquete de serialización.
- 1829 0x0725 Versión incompatible de la rutina auxiliar (*stub*) de *RPC*.
- 1898 0x076A No se ha encontrado el miembro del grupo.
- 1899 0x076B No se puede crear la base de datos del asignador de extremos.

1900	0x076C	El identificador exclusivo universal (<i>UUID</i>) de objeto es el <i>UUID</i> nulo.
1901	0x076D	La hora especificada no es válida.
1902	0x076E	El nombre del formato especificado no es válido.
1903	0x076F	El tamaño del formulario especificado no es válido
1904	0x0770	El identificador especificado de la impresora ya se ha atendido
1905	0x0771	Ya se ha eliminado la impresora especificada
1906	0x0772	El estado de la impresora no es válido
1907	0x0773	El usuario debe cambiar su contraseña antes de iniciar la sesión por primera vez.
1908	0x0774	No se puede encontrar el controlador de dominio para este dominio.
1909	0x0775	La cuenta a que se hace referencia está bloqueada y no se puede utilizar.
2000	0x07D0	El formato de píxel no es válido.
2001	0x07D1	El controlador especificado no es válido.
2002	0x07D2	El estilo de ventana o el atributo de clase no es válido para esta operación.
2003	0x07D3	La operación de metarchivo solicitada no es compatible.
2004	0x07D4	La operación de transformación solicitada no es compatible.
2005	0x07D5	La operación de copia de datos solicitada no es compatible.
2202	0x089A	El nombre de usuario no es válido.
2250	0x08CA	No existe esta conexión de red.
2401	0x0961	Esta conexión de red tiene archivos abiertos o peticiones pendientes.
2402	0x0962	Todavía existen conexiones activas.
2404	0x0964	Hay un proceso activo utilizando el dispositivo y no se puede desconectar.
3000	0x0BB8	El monitor de impresión especificado es desconocido.
3001	0x0BB9	El controlador de impresora especificado ya está en uso.
3002	0x0BBA	No se ha encontrado el archivo de cola de impresión.
3003	0x0BBB	No se realizó una llamada a <i>StartDocPrinter</i> .
3004	0x0BBC	No se ha generado una llamada a <i>AddJob</i> .
3005	0x0BBD	El procesador de impresión especificado ya ha sido instalado.
3006	0x0BBE	El monitor de impresión especificado ya ha sido instalado.
4000	0x0FA0	<i>WINS</i> encontró un error mientras procesaba el comando.
4001	0x0FA1	<i>WINS</i> local no puede ser eliminado.
4002	0x0FA2	Error al importar desde el archivo.
4003	0x0FA3	Error en la copia de seguridad.
4004	0x0FA4	Error en la copia de seguridad. Compruebe el directorio donde desea hacer la copia de la base de datos.
4005	0x0FA5	El nombre no existe en la base de datos de <i>WINS</i> .
4006	0x0FA6	No está permitida la duplicación con un interlocutor no configurado.
6118	0x17E6	No se dispone de la lista de servidores para este grupo de trabajo