

Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[prerrequisitos](#)

[Componentes Utilizados](#)

[¿Cuál es Windows Networking?](#)

[Dominios contra los grupos de trabajo](#)

[¿Qué protocolo utiliza?](#)

[IP dinámica dirigiendo](#)

[¿Cuál es DHCP?](#)

[Alcances de DHCP](#)

[Relé DHCP](#)

[Opciones de DHCP](#)

[Servidores del DHCP de Cisco](#)

[Resolución de nombre](#)

[Caché del nombre de NetBIOS](#)

[Broadcasts de la subred IP](#)

[LMHOSTS](#)

[Windows Internet Name Service](#)

[DN de Internetes](#)

[Orden de búsqueda de nombre](#)

[El navegador de los servicios LAN de Microsoft](#)

[Nombres de NETBIOS](#)

[El proceso de inicialización](#)

[Encontrar una Computadora](#)

[Ver la vecindad de la red](#)

[Subred que hojea](#)

[Broadcast que hojea a través de las subredes](#)

[Ojeada de cualquier dominio con los TRIUNFOS](#)

[El apagar transmite](#)

[Escalamiento a redes más grandes](#)

[Dominios confiables](#)

[Solo dominio](#)

[Global Trust](#)

[Dominio principal](#)

[Dominios maestros múltiples](#)

[Replicar los TRIUNFOS](#)

[Acceso por módem](#)

[Dial-On-Demand Routing](#)

[Acceso ISDN](#)

[Adtran](#)

[BitSURFR de Motorola](#)

[Software de cliente](#)

[CiscoRemote Lite](#)

[Ejemplos](#)

[Ejemplo 1](#)

[Configuración del Cisco 4700 Router](#)

[Configuración del Servidor de acceso Cisco 2511](#)

[‘Ejemplo 2’](#)

[Ejemplo 3](#)

[Ejemplo 4](#)

[Apéndice A: Apagar la resolución de nombre de broadcast](#)

[Al usar las ventanas para grupos de trabajo 3.11](#)

[Windows 95/98](#)

[Windows NT 3.51](#)

[Entradas de registro del Windows NT](#)

[Encontrar a los exploradores maestros de variación aleatoria](#)

[Apéndice B: Configurar la resolución de DNS de los nombres de los TRIUNFOS](#)

[El archivo del inicio DNS](#)

[El archivo DNS para domain.com](#)

[Información Relacionada](#)

[Introducción](#)

El término "networking" abarca una amplia gama de tecnologías que, combinadas, permiten a los ordenadores compartir información. Los componentes de networking se pueden dividir en aplicaciones de sistema final, sistemas operativos de red y equipo de networking.

Un sistema operativo de red es software funcionado con en todos los sistemas interconectados. Los ejemplos incluyen implementación NFS del Novell Netware, de Sun (sistema de archivos de red), de AppleShare, y de Microsoft de un Windows Networking comúnmente llamado del sistema operativo de red. El Windows Networking ahora se despliega extensivamente con millones de Nodos.

Esta guía de diseño explica los conceptos básicos de Windows Networking y proporciona la penetración en cómo diseñar las redes (los LAN y los WAN) al mejor utiliza este sistema operativo. La guía también explica los protocolos, el nombramiento, y los problemas de ampliación asociados al Windows Networking.

[Antes de comenzar](#)

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

[prerrequisitos](#)

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

¿Cuál es Windows Networking?

El Windows Networking refiere al sistema de interconexión de redes compartido por el software que viene con todos los sistemas operativos Microsoft o servidores siguientes:

- Administrador de LAN de Microsoft
- MS-DOS con el cliente del administrador de LAN
- Ventanas para grupos de trabajo
- Windows 95, 98, y YO
- Windows NT y 2000

No discuten el administrador de LAN de Microsoft, el cliente del administrador de LAN para MS-DOS, y el Windows NT 3.1 en este documento excepto en un contexto histórico.

Dominios contra los grupos de trabajo

El Windows Networking tiene tres conceptos de un grupo de grupos de trabajo relacionados de los ordenadores, de dominios y de una jerarquía del dominio. Los grupos de trabajo pueden ser cualquier recolección lógica de los ordenadores; cualquier ordenador en la red puede unirse a un grupo de trabajo existente o crear un nuevo. Un proceso del controlador de dominio primario (PDC) crean y son manejadas a más entidades formales, los dominios que se ejecuta en un Windows NT o Windows 2000 Server. Un dominio tiene la Seguridad y propiedades administrativas que no lo haga un grupo de trabajo. Cada dominio debe tener por lo menos un NT o 2000 servidores, que es responsable del proceso PDC, de la información de cuenta de usuario en el dominio, y de la Seguridad dentro del dominio. Los dominios de conexión en red de Windows no son lo mismo que los Domain Name de Internet según lo utilizado por el Domain Name System (DNS). Una jerarquía de la jerarquía del dominio o de Active Directory es un grupo de dominios ordenado en las relaciones controlante/subordinado. Este convenio, introducido con el Windows 2000, habilita una búsqueda más fácil a través de los dominios múltiples en una sola interrogación (entre otras cosas). Esto jerarquía se correlaciona estrechamente a un espacio de nombres DNS.

¿Qué protocolo utiliza?

Antes del Windows 2000, el Windows Networking utilizó el protocolo NetBIOS para la capacidad de compartir archivos, el USO compartido de impresora, la Mensajería, la autenticación, y la resolución de nombre. Una instalación pura del Windows 2000 requeriría el NetBios solamente

para la Interoperabilidad con las versiones anteriores del Windows Networking usando espacio de nombres plano de NetBIOS. El NetBios es un protocolo de capa de la sesión que puede ejecutarse en uno de los después de los protocolos de transporte:

- NetBEUI (NetBios sobre LLC2)
- NWLink (NetBios sobre el [IPX] del Internetwork Packet Exchange)
- NetBios sobre TCP (NBT)

Aunque Microsoft recomiende que los clientes utilizan solamente uno en un momento del Transport Protocol para el rendimiento máximo, esta configuración es solamente el valor por defecto para el Windows 2000. Usted debe escoger un protocolo para utilizar para su toda la red, preferiblemente TCP/IP, y después apaga los otros protocolos porque el servicio de nombre de NetBIOS mantiene la información sobre los nombres de computadora (un espacio para nombre) por separado para cada transporte. Los espacios para nombre no obran recíprocamente con uno a; cada transporte actúa como red separada.

El NetBEUI (NetBios sobre LLC2) es el menos scalable de los tres protocolos porque debe ser interligado. El NetBEUI se incluye para soportar solamente muy los viejos servicios (por ejemplo, las versiones antiguas del administrador de LAN). El NetBEUI no requiere ninguna configuración de la dirección del cliente. No hay límite fijo al número de clientes de Windows puede tener con el NetBEUI, pero es común para que esta solución se ejecute en los problemas de rendimiento pues el número de clientes en un grupo de un solo Bridge pasa por encima 50 a 100 usuarios. La topología plana y la confianza en los broadcasts no escala, especialmente cuando el tráfico debe atravesar un link PÁLIDO.

El NWLink se recomienda solamente para las redes que ejecutan ya el IPX que no se puede actualizar para utilizar el TCP/IP. Similar al NetBEUI, el NWLink no requiere ninguna configuración de la dirección del cliente. El NWLink utiliza los paquetes tipos 20 IPX para intercambiar el registro y la información de exploración. Para remitir los paquetes IPX tipos 20 a través de los routers Cisco, usted debe configurar **propagación tipo 20 de IPX** en cada interfaz en cada router en su red.

Se recomienda para utilizar el NetBios sobre TCP (NBT) para la mayoría de las redes, o siempre la red incluye WAN. Puesto que el NBT utiliza el TCP/IP, cada ordenador se debe configurar para utilizar un IP Address estático, o para traer una dirección IP dinámicamente con el Protocolo de configuración dinámica de host (DHCP). Para la facilidad de la Administración de red, se recomienda altamente para utilizar el DHCP; para el rendimiento óptimo de red, se recomienda altamente para utilizar el servidor de los TRIUNFOS a (Windows Internet Name Service) también. Un servidor de los TRIUNFOS permite que los clientes consigan la información de exploración sin tuvo que los pedidos de broadcast cada vez. Hay una correlación directa entre el número de broadcasts en una red y el rendimiento de la red; los broadcasts son necesarios para que una red funcione, pero la reducción al mínimo de ellos puede ser crítica.

Cisco recomienda que la mayoría de los clientes utilizan el TCP/IP para el Windows Networking. El bulto de esta guía de diseño se centra en los diseños usando el NBT.

[IP dinámica dirigiendo](#)

[¿Cuál es DHCP?](#)

Manualmente dirigirse a los clientes TCP/IP es largo y falible. Para solucionar este problema, la Fuerza de tareas de ingeniería en Internet (IETF) (IETF) desarrolló el DHCP, el Dynamic Host

Configuration Protocol. El DHCP se diseña para proporcionar automáticamente a los clientes con una información del IP Address válido y de configuración relacionada (véase las [opciones DHCP de la](#) sección abajo). Cada rango de direcciones que un servidor DHCP maneja se llama un alcance.

[Alcances de DHCP](#)

Usted debe configurar un rango de direcciones para cada subred IP donde los clientes pedirán un DHCP Address; cada rango de direcciones se llama un alcance de DHCP. Usted puede configurar a un servidor DHCP para servir varios alcances puesto que el servidor DHCP o los servidores no necesita ser conectado físicamente con la misma red que el cliente. Si el servidor DHCP está en una diversa subred IP del cliente, después usted necesita utilizar el relé DHCP para remitir los pedidos de DHCP a su servidor DHCP.

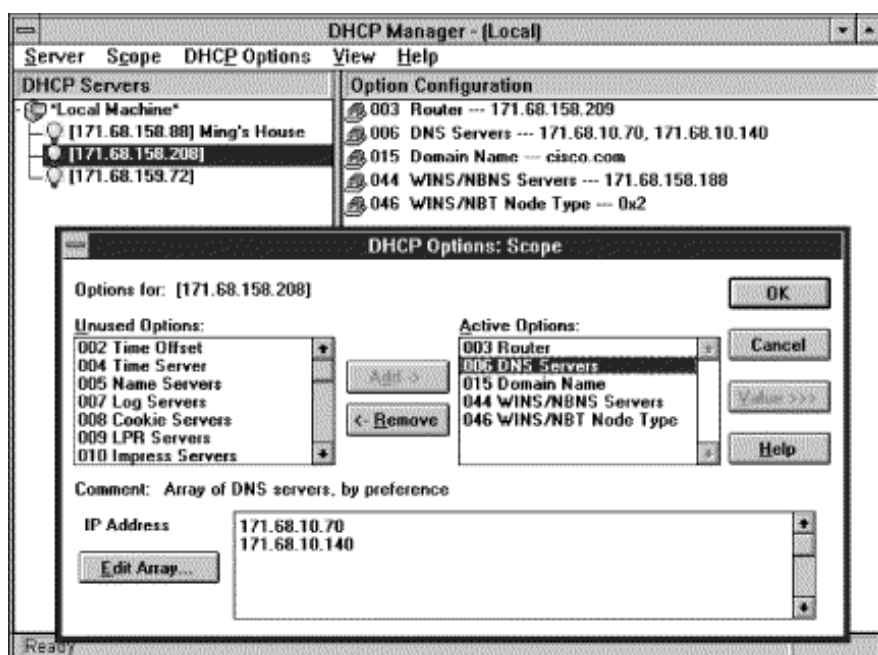
[Relé DHCP](#)

El relé DHCP se ejecuta típicamente en un router y el soporte de relay está disponible en la versión del servidor 4.0 del Windows NT y Windows 2000 Server. En los Cisco 700 Series Router, usted puede girar el relé DHCP con el **comando set dhcp relay**. Usted puede girar el relé DHCP en un router del Cisco IOS configurando el **ip helper-address** con el direccionamiento del servidor DHCP en cada interfaz que tenga los clientes DHCP. El **comando ip helper-address** adelante mucho el otro IP transmite, incluyendo los paquetes DNS, del Trivial File Transfer Protocol (TFTP), y del servicio de nombre de NetBIOS. Para remitir solamente los pedidos de DHCP, vea la configuración del siguiente ejemplo. Para más información, vea la sección "Configuración de manejo de broadcast" en los [Network Protocol guía de configuración, la parte I](#).

[Opciones de DHCP](#)

Además de su dirección IP, un Cliente de DHCP puede conseguir la otra información de la configuración TCP/IP de un servidor DHCP, incluyendo la máscara de subred, el default gateway, y la información DNS. Estas informaciones, llamadas las opciones DHCP, se pueden configurar en el administrador de DHCP en su servidor DHCP del Windows NT o del Windows 2000.

Figura 1: El administrador de DHCP de Microsoft



Si sus clientes están utilizando el Windows Internet Name Service (TRIUNFOS) para la resolución de nombre (discutida más adelante), usted debe configurar el direccionamiento del servidor de los TRIUNFOS y de los Tipos de nodo WIN. Una lista breve de tipos de nodo se incluye en el sección "Resolución de nombre". El p-nodo del tipo de nodo (**0x2**) se recomienda fuertemente.

[Servidores del DHCP de Cisco](#)

Cisco tiene actualmente un DHCP y un servidor DNS integrados para el Windows NT, el Windows 2000 y UNIX; el servidor tiene una interfaz gráfica, el soporte para el direccionamiento secundario, y muchas otras características para empresas. El Routers de los Cisco 700 Series Router (en la versión 4.1 y posterior) y del Cisco IOS (en la versión 11.2(7) F y posteriores) también incluye a un servidor DHCP que pueda asignar los direccionamientos en los segmentos de red local. Ambos estilos del router incluyen la traducción de la dirección de la red y del nivel de Puerto.

[Resolución de nombre](#)

La resolución de nombre es el proceso de asociar un nombre conveniente, tal como FRED o fred.domain.com, a una dirección de red (a menudo una dirección IP). Para los actuales propósitos, esta discusión se aplica a la manera que el Windows Networking resuelve un nombre único del puesto de trabajo del NetBios (descrito como *WORKSTATION<00>* en una sección posterior) a una dirección IP. Este proceso no se debe confundir con el relacionado sino el proceso diferente de la ojeada (que utiliza otros tipos de nombres de NETBIOS). A partir de la versión del Microsoft Windows 2000, los clientes del Windows Networking utilizan hasta cinco métodos de resolución de nombre:

- Caché del nombre de NetBIOS
- Broadcasts de la subred IP
- LMHOSTS
- GANA
- DN de Internetes

[Caché del nombre de NetBIOS](#)

El Windows Networking guarda un pequeño caché de los nombres de NETBIOS usados recientemente a las correspondencias de IP Address. Estas entradas se agregan después de la resolución de nombre acertada y después se quitan después de un cierto período de tiempo. Las entradas adicionales se pueden cargar en el inicio del sistema y la permanente hecha creando una entrada en el LMHOSTS para clasificar con la etiqueta #PRE (véase la sección [LMHOSTS](#) abajo).

[Broadcasts de la subred IP](#)

Los broadcasts de la subred IP se pueden utilizar para la resolución de nombre. Los broadcasts son recibidos por todos los ordenadores en una subred, requiriendo el tiempo de procesamiento en cada ordenador. El Windows Networking también mantiene un browse master señalado que mantiene una lista de todos los recursos disponibles en una subred. Un proceso de elección que utiliza los broadcasts determina este browse master porque los registros, las elecciones del buscador, y las consultas de nombre podrían todos generar los broadcasts, uso del método de la resolución de nombre de broadcast no se recomienda.

LMHOSTS

El Windows Networking puede consultar una tabla estática en un archivo llamado LMHOSTS. Para utilizar este método, el PDC debe mantener por lo menos una lista estática de todos los ordenadores y de sus IP Addresses en ese dominio y los nombres y dirección de los PDC para el resto de los dominios en la red. Todos los clientes deben entonces tener un archivo LMHOSTS con la dirección IP de su PDC y la trayectoria al archivo del master LMHOSTS en el PDC.

Windows Internet Name Service

Los TRIUNFOS fueron creados para permitir que los clientes en diversas subredes IP resuelvan dinámicamente los direccionamientos, registrarse, y hojear la red sin el envío transmite. Los clientes envían los paquetes de unidifusión al servidor de los TRIUNFOS en una dirección conocida. Para la compatibilidad con más viejos clientes de la interconexión de redes de Microsoft, sin embargo, todavía se gira la resolución de nombre de broadcast por abandono, incluso cuando los TRIUNFOS también se configuran.

Para relanzar qué fue expuesta arriba, se recomienda altamente para que el rendimiento óptimo de red utilice los TRIUNFOS. Una vez más hay una correlación directa entre el número de broadcasts en una red y el rendimiento de la red; los broadcasts son necesarios para que una red funcione, pero la reducción al mínimo de ellos puede ser crítica.

DN de Internetes

Cualquier servidor DNS puede ser configurado estáticamente para contestar a las interrogaciones para los ordenadores con los IP Address fijos. Este escenario es útil si los ordenadores en su red tienen IP Address fijos. Cuando los Sistemas Windows utilizan el DHCP para conseguir un IP Address y los TRIUNFOS para registrar un nombre de NETBIOS, usted puede configurar a un servidor DNS de Windows para preguntar un servidor de los TRIUNFOS para los nombres o los direccionamientos que no fueron ingresados estáticamente. En ambos casos, Windows y los sistemas distintos de Windows pueden resolver los IP Addresses correctamente.

Si un administrador configura cada servidor de red de Windows con un IP Address estático, puede ser conveniente ingresar cada servidor en el sistema DNS y utilizar el DNS para la resolución de nombre. (Por ejemplo, al usar a un enlace de marcado a pedido) es de vez en cuando conveniente registrar a los clientes con los TRIUNFOS y hacer las interrogaciones con el DNS. Microsoft NT 3.51 juegos de recursos, servidor y Windows 2000 todos del Windows NT 4.0 incluye a un servidor DNS que pueda contestar a las interrogaciones DNS preguntando un servidor de los TRIUNFOS en el fondo. Para más información sobre cómo configurar esta arquitectura, vea el [Apéndice A](#).

Con el Windows 2000, los servidores DNS pueden también ser configurados dinámicamente con el direccionamiento a las correlaciones de nombre. Los servidores de los clientes DHCP, de los servidores DHCP y de los dn dinámico funcionan juntos para poner al día el nombre a las correspondencias de direcciones en el servidor DNS. El servidor DHCP realizará esta actualización para el no Windows 2000 clientes DHCP.

Figura 2: Windows y los sistemas distintos de Windows ambos envían las búsquedas de DNS para un servidor del Windows NT nombrado Warthog. El servidor DNS no tiene una entrada para el facoquero, así que pregunta el servidor de los TRIUNFOS y vuelve la dirección IP.

Orden de búsqueda de nombre

Los componentes del Windows Networking envían las interrogaciones de la resolución de nombre en una diversa orden, dependiendo del tipo de nodo del NetBios. Si el sistema es Windows NT 4.0 y el nombre es más largo de 15 caracteres, después el Windows NT envía solamente una interrogación DNS. Otros componentes de interconexión de redes y servicios pueden también utilizar una diversa orden dependiendo del API llamado para realizar la resolución de nombre. Por ejemplo, una aplicación de los sockets que llama el `gethostbyname()` utilizará el DNS para la resolución de nombre primero. Si no la búsqueda de nombre se realiza en el siguiente orden:

- Marque Caché del nombre de NetBIOS.
- Envíe una interrogación del broadcast o un nombre de la interrogación de los TRIUNFOS, dependiendo del tipo de nodo actual del NetBios.
- Marque el archivo LMHOSTS.
- Marque el archivo de los HOST (si la “resolución usando el DNS” se marca).
- Envíe una interrogación de los DN de Internetes (si la resolución usando el DNS se marca).

Tabla 1: Los nombres de NETBIOS se buscan diferentemente basaron en el tipo de nodo del NetBios

Tipo de nodo del NetBIOS	Orden de búsqueda de nombre
B-nodo (0x1)	Broadcast solamente
p-nodo (0x2)	TRIUNFOS solamente
m-nodo (0x4)	Broadcast, entonces TRIUNFOS
h-nodo (0x8)	TRIUNFOS, entonces broadcast

El navegador de los servicios LAN de Microsoft

El Windows Networking fue diseñado originalmente para ejecutarse en un solo segmento LAN o una red interligada (del plano). En aquel momento, solamente el protocolo NetBEUI fue soportado.

Microsoft desarrolló el hojeador de los servicios LAN para permitir al usuario para hojear una lista de todos los ordenadores disponibles en la red. Cada cliente del Windows Networking registró su nombre de NETBIOS periódicamente enviando los broadcasts.

Cada ordenador también tuvo que enviar los broadcasts para elegir un browse master para la red. El browse master (y vario el respaldo hojea a los masters) mantuvo la lista de ordenadores y de sus direccionamientos. Cuando un usuario hojeó la red, el cliente envió un pedido de broadcast y uno de los masters de la ojeada respondió.

Eventual el apoyo añadido de Microsoft para el NetBios sobre el IPX y el NetBios sobre el TCP/IP, pero el Windows Networking todavía asumió que todos los clientes y servidores estaban en la misma red IPX o subred IP lógica---él todavía envió los broadcasts para registrar y para encontrar los ordenadores en la red.

Esta arquitectura, aunque sea simple implementar, genero una carga enorme en la red y en el

CPU de cada cliente en la red. Debido a estos problemas de ampliación, Microsoft comenzó a ofrecer otros métodos de ojeada y de resolución de nombre---maneras para que clientes asocien un nombre a la dirección IP de otros ordenadores en la red. Microsoft también proporcionó eventual a una manera de hojear y de resolver los nombres sin los broadcasts.

El resto de esta sección explica cómo la ojeada trabaja en los diversos entornos. La sección anterior explicada cómo se resuelven los nombres de NETBIOS individuales. Estas dos actividades son similares pero distintas. Los usuarios hojean la red al abrir la vecindad de la red, usando el comando net view, o la registración en a dominio de Windows NT en el lanzamiento. La resolución de nombre es el proceso de resolver los nombres sabidos previamente, o encontró al hojear. Observe por favor que esta discusión está sin relación a los buscadores Web.

Nombres de NETBIOS

Los nombres de NETBIOS son 15-character, los nombres mayúsculos que tienen un identificador especial agregado al décimosexto byte. También, los nombres de NETBIOS pueden aplicarse a una sola dirección IP (única), o a más de una (grupo). Algunos tipos del nombre pueden ser únicos o nombres del grupo. Algo del más común de estos caracteres más recientes se enumera como sigue (todos los valores están en el hexadecimal):

Tabla 2: Una tabla parcial de nombres de NETBIOS especiales y de sus descripciones

Nombres especiales registrados	Descripción
<i>Nombres de usuario</i>	
<USERNAME><00>	Utilizado para registrar el nombre del usuario actualmente abierto una sesión en la base de datos de los TRIUNFOS, de modo que los usuarios puedan recibir los comandos net send enviados a sus Nombres de usuario.
<i>Nombres de computadora</i>	
<COMPUTER><00>	Utilizado por los puestos de trabajo de la interconexión de redes de Microsoft para recibir los pedidos de slot para correo de la segunda clase. Todos los puestos de trabajo deben agregar este nombre para recibir los pedidos de slot para correo. Éste es el nombre de computadora registrado para los servicios del puesto de trabajo por un cliente de los TRIUNFOS.

<COMPUTER><03>	Utilizado como el nombre de computadora que se registra para el servicio de mensajero en un ordenador que sea un cliente de los TRIUNFOS.
<COMPUTER><20>	Utilizado como el nombre que se registra para el servicio del servidor de peer en un ordenador de Windows 95 (o el servicio de servidor en un ordenador del Windows NT) que sea un cliente de los TRIUNFOS.
<COMPUTER><Be>	Utilizado como el nombre único se registra que cuando el agente monitor de la red se comienza en el ordenador.
<COMPUTER><Bf>	Utilizado como el nombre del grupo se registra que cuando el agente monitor de la red se comienza en el ordenador. Si este nombre no es 15 caracteres de largo, se completa con (+) los símbolos más.
<COMPUTER><1f>	Utilizado como el nombre único que se registra para el intercambio de datos dinámico de la red (DDE) cuando el servicio de NetDDE se comienza en el ordenador.
<i>Nombres del grupo</i>	
<01><02>MSBROWSE<02><01>	Utilizado por los servidores buscadores maestros para anunciar periódicamente su dominio en una subred local. Este aviso contiene el Domain Name y el nombre del servidor buscador maestro para el dominio. Además, los servidores buscadores maestros reciben estos anuncios de dominio a

	<p>este nombre y los mantienen en su interno hojean la lista junto con el nombre de computadora del anunciador.</p>
<DOMAIN><00>	<p>Utilizado por los puestos de trabajo y los servidores a los avisos del servidor del proceso para apoyar al administrador de LAN de Microsoft. Los servidores que funcionan con Windows 95, el Windows NT, el servidor del Windows NT, y las ventanas para grupos de trabajo no transmiten este nombre a menos que la opción de LMAnnounce se habilite en las propiedades de servidor.</p>
<DOMAIN><1b>	<p>Utilizado para identificar el nombre del buscador maestro de dominio, que es un nombre único que solamente el controlador de dominio primario (PDC) puede agregar. El PDC procesa las peticiones de GetBrowserServerList en este nombre. Los TRIUNFOS asumen que el ordenador que registra un Domain Name con <1b> el carácter es el PDC.</p>
<DOMAIN><1c>	<p>Utilizado para el nombre de grupo de Internet, que los controladores de dominio registran. El nombre de grupo de Internet es una lista dinámica de hasta 25 ordenadores que han registrado el nombre. Éste es el nombre usado para encontrar un ordenador del Windows</p>

	NT para la autenticación del paso.
<DOMAIN><1d>	Utilizado para identificar a un buscador principal (no buscador maestro de dominio). El buscador principal agrega este nombre como nombre de NetBIOS único cuando comienza. Los puestos de trabajo anuncian que su presencia a este nombre de modo que los buscadores principales puedan construir su hojee la lista. Para los grupos de trabajo, este nombre tiene la forma <WORKGROUP><1d>.
<DOMAIN><1e>	Utilizado para todos los avisos del grupo de trabajo o del dominio de par en par por los servidores buscadores en un grupo de trabajo de la red de Windows o un dominio del servidor del Windows NT. Este nombre es agregado por todos los servidores buscadores y servidores potenciales en el grupo de trabajo o el dominio. Todos los paquetes de la elección del buscador se envían a este nombre. Para los grupos de trabajo, este nombre tiene la forma <WORKGROUP><1e>.

El proceso de inicialización

En el lanzamiento, cualquier sistema conectado en red envía una serie de paquetes para descubrir a las direcciones de red, para registrarse, para autenticarse, y para descubrir los servicios. Los sistemas del Windows Networking que registran en dominio de Windows NT deben entrar en contacto un controlador de dominio para autenticar. Este proceso utiliza la resolución de nombre y la ojeada.

Primero el sistema de inicio debe registrar un nombre de computadora (*WORKSTATION<00>*). Si el parámetro LMAnnounce está prendido (para la compatibilidad con los servidores del

administrador de LAN), después el sistema también registra el *DOMAIN<00>*. El sistema localiza después un controlador de dominio para el dominio del login intentando resolver el *DOMAIN<1C>*. Antes del Windows 2000, de éste trabajados solamente con los métodos del broadcast, de la resolución de nombre LMHOSTS, o de los TRIUNFOS. Con el Windows 2000, el DNS se intenta primero. Después, el sistema abre una sesión al controlador de dominio que usa los mensajes de mailslot NetBios-basados, que se envían en el puerto 138 del User Datagram Protocol (UDP). Finalmente, después de que el login sea acertado, el sistema registra al usuario que abrió una sesión (*USERNAME<03>*) así que el servicio de mensajero puede encontrar a ese usuario.

[Encontrar una Computadora](#)

Cuando peticiones del usuario un recurso en un ordenador por nombre (por ejemplo: `\neto \fred \someshare del uso`, o la FRED de los hallazgos), el sistema local intenta resolver el nombre de computadora. Esta interrogación está para un nombre de NetBIOS único del tipo `<00>`, o un DNS o RECIBE la entrada de archivo.

[Ver la vecindad de la red](#)

Cuando un usuario abre la vecindad de la red para pedir una lista de dominios, el sistema intentará conseguir una lista de buscadores de backup, con la difusión al nombre del buscador maestro, o directamente la conexión con el buscador maestro de dominio (o ambas). Una vez que una lista de buscadores de backup se extrae, el sistema elegirá a un buscador de backup, conecta con ese sistema y extrae la lista de dominios. Los pedidos posteriores para los servidores dentro de un dominio se remiten al mismo buscador de backup.

[Subred que hojea](#)

En los años 80, la mayoría de las redes eran “planas,” o tenían solamente algunas subredes. El NetBEUI y el NWLink utilizan este modelo, y los broadcasts IP se pueden interligar o ayudar a través de una pequeña cantidad de subredes. La discusión siguiente asume el caso de una red plana.

Cada subred tiene un buscador maestro de subred por el dominio o el grupo de trabajo y puede tener algunos buscadores de backup de la subred (también por el dominio o el grupo de trabajo). Después del bootup, los buscadores de backup y los nonbrowsers envían los anuncios de broadcast en los intervalos cada vez mayores de 1, 2, 4, y 8 minutos; ellos eventual anuncios de broadcast solamente cada 12 minutos. Los buscadores maestros de subred escuchan estos avisos para construir una lista de la ojeada.

Los buscadores maestros de subred y los buscadores de backup son responsables de la contestar hojean las interrogaciones de otros ordenadores. Los buscadores principales pueden contestar a estas peticiones directamente de la lista de la ojeada. Los buscadores de backup también guardan una lista de la ojeada, que preguntan el buscador maestro de subred cada 15 minutos.

[Broadcast que hojea a través de las subredes](#)

En la realidad, la mayoría de las redes tienen hoy varias subredes. De los dominios las subredes del palmo a menudo y las subredes contienen a veces los sistemas en más de un dominio. El software del buscador en algunos sistemas puede comunicar con un buscador maestro de dominio (generalmente el PDC) para intercambiar hojea las listas de muchas subredes, pero

necesita conocer a la dirección de Unicast del buscador maestro de dominio. Un buscador maestro de subred puede conseguir a la dirección de Unicast del PDC de un archivo LMHOSTS (para una descripción detallada, vea la sección de la [resolución de nombre](#)) o de los TRIUNFOS (véase la siguiente sección).

El LMHOSTS es un archivo de texto que el software del buscador puede leer para encontrar a la dirección de Unicast de un PDC. Una muestra sigue. Primero está el Unicast IP Address del PDC, después el nombre de NETBIOS del PDC (**ENG_PDC**), una etiqueta que salve esta línea en Caché del nombre de NetBIOS, (**#PRE**) y finalmente, una etiqueta que marque este sistema como controlador de dominio para el dominio Eng (**#DOM**).

Cuando un buscador maestro de subred conoce a la dirección de Unicast del buscador maestro de dominio, el intercambio de los navegadores hojea las listas cada 15 minutos (usando los paquetes de la unidifusión IP). Porque consultan a un buscador principal, los clientes pueden hojear solamente los dominios que tienen un sistema en la subred local (buscador maestro de subred). En la práctica, este escenario trabaja bastante bien para encontrar un servidor del login en el lanzamiento, pero no permite que los usuarios hojeen usando la vecindad de la red.

NOTA IMPORTANTE: Debido a un bug en algunas versiones de Windows para los grupos de trabajo 3.11 y Windows 95, estos sistemas no pueden funcionar como un buscador maestro de subred o un buscador de backup. El bug evita que el buscador de subred entre en contacto al buscador maestro de dominio. Este bug se ha reparado en Windows 95 OSR (versión) del servicio OEM 2. como consecuencia, la ojeada en la subred falla si hay Win31 o master o buscadores de backup de Win95 en la subred.

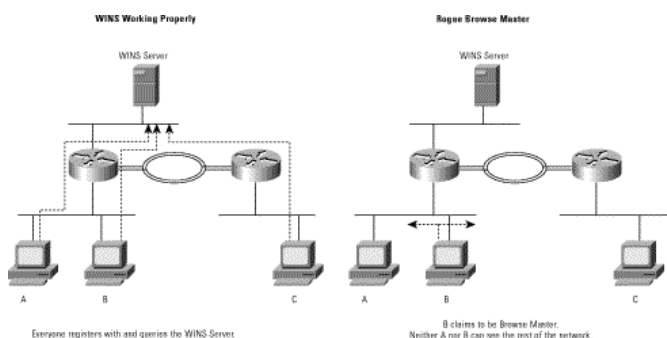
[Ojeada de cualquier dominio con los TRIUNFOS](#)

En una organización con varios dominios, no es razonable al arquitecto que una red basó en las restricciones delineó en la sección anterior. Cuando los TRIUNFOS se están ejecutando, el buscador de subred puede ser un cliente de los TRIUNFOS y puede conseguir el Unicast IP Address del buscador maestro de dominio (el PDC) para cualquier dominio. Sin embargo, los broadcasts todavía se envían con frecuencia y en varias ocasiones por abandono (véase la tabla el describir de los Tipos de nodo WIN en la sección siguiente) en la ocasión que puede haber clientes de algunos NON-TRIUNFOS en la subred. La mejor solución de la mayoría de las redes es apagar el broadcast que hojea.

[El apagar transmite](#)

El desafío más grande cuando apagar los broadcasts está evitando a los exploradores maestros de variación aleatoria, que causan el estrago en una subred porque interrumpen el proceso de la ojeada.

Figura 3: Explorador maestro de variación aleatoria



Usted puede inhabilitar la resolución de nombre de broadcast fijando la configuración de BrowserMaster inhabilitó. En las ventanas para grupos de trabajo 3.11, los broadcasts son apagados agregando un comando al archivo SYSTEM.INI. (Véase el [apéndice B](#) para los detalles.) En el Windows 95/98, la configuración de BrowserMaster en el archivo avanzado y la impresión que comparte las propiedades se deben fijar discapacitada. En el Windows NT, no es necesario dar vuelta apagado a la ojeada en la mayoría de los casos, aunque pueda ser deseable. En el Windows NT, fije el `Hkey_local_machine \ el sistema \ el CurrentControlSet \ los servicios \ clave de registro del navegador \ de los parámetros \ de MaintainServerList` no a los administradores puede controlar los broadcasts enviados por los clientes DHCP seleccionando los Tipos de nodo WIN apropiados (p-nodo: `0x2`). Una lista completa de Tipos de nodo WIN sigue.

Tabla 3: Lista de Tipos de nodo WIN

Tipos de nodo WIN	Orden de búsqueda de nombre
B-nodo (0x1)	Broadcast solamente
p-nodo (0x2)	TRIUNFOS solamente
m-nodo (0x4)	Broadcast, entonces TRIUNFOS
h-nodo (0x8)	TRIUNFOS, entonces broadcast

[Escalamiento a redes más grandes](#)

[Dominios confiables](#)

Al planear una red Windows, consideración de qué modelo del dominio es importante utilizar. Los párrafos siguientes discuten las ventajas y las desventajas de varios modelos del dominio. Si usted tiene varios dominios, usted quiere probablemente a los intercambiar datos con otros dominios en su red. Las relaciones de confianza son una manera de ganar o acceso de la concesión a un dominio sin tener que manejar a cada usuario individualmente. Cada relación permite la confianza en una dirección solamente. Para más información, vea a los *kit de recursos del servidor del Windows NT 4.0*, el volumen 2, el capítulo 4.

[Escoja el dominio](#)

Este modelo del dominio es el más simple---la red tiene solamente un dominio. Esta configuración trabaja para las instalaciones pequeñas o medianas sin WAN.

[Global Trust](#)

Se diseña para las compañías sin un administrativo central o la organización, el modelo del Global Trust es el más fácil de entender y el más difícil de manejar. Cada dominio confía en cada otro dominio.

[Dominio principal](#)

En este modelo, un dominio principal es confiado en por el resto de los dominios, pero el dominio principal confía en nadie. Esta opción es beneficiosa cuando los departamentos o las divisiones quieren el control administrativo sobre sus propios servicios, pero todavía quiere autenticar centralmente.

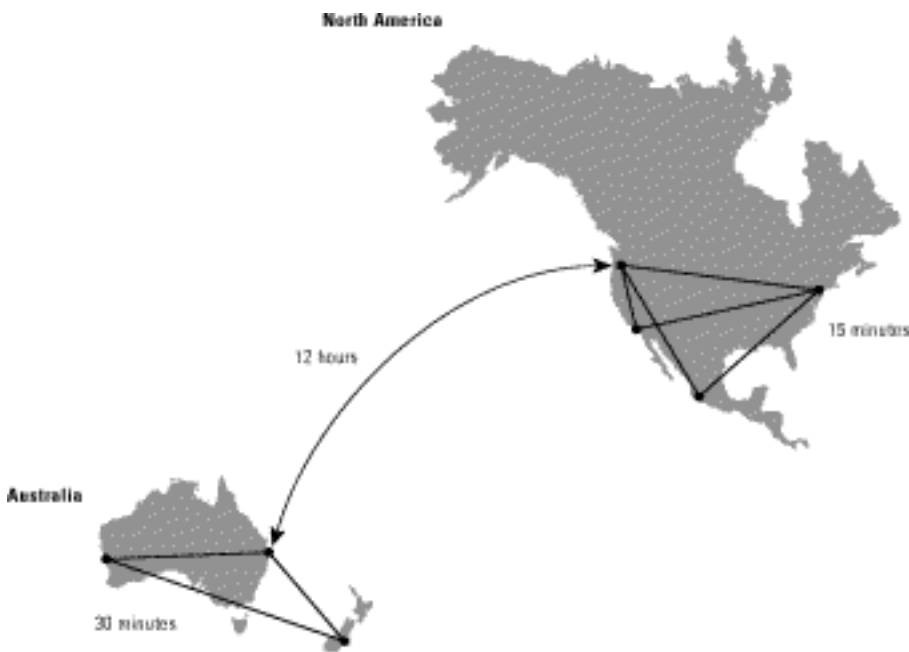
Dominios maestros múltiples

Este modelo se diseña para ser una versión más grande del modelo del dominio principal. Varios dominios principales toda la confianza, y cada uno de los dominios principales, a su vez, es confiados en por cada dominio departamental.

Replicar los TRIUNFOS

Para la Redundancia u optimizar el tráfico PÁLIDO, a veces teniendo varios servidores de los TRIUNFOS es deseable. Los servidores del Windows NT y del Windows 2000 pueden replegar o resincronizar las bases de datos de los TRIUNFOS en cualquiera o las ambas direcciones. En el cuadro 4, una empresa multinacional grande tiene varios servidores distribuidos de los TRIUNFOS, tan los TRIUNFOS que las interrogaciones no tienen que viajar a través de los continentes.

Figura 4: Ejemplo de una configuración para la copia de WINS para toda la empresa



Acceso por módem

El Windows NT y el Windows 2000 vienen con el Remote Access Server (RAS) de Microsoft, que utiliza el Point-to-Point Protocol (PPP). Los clientes pueden querer utilizar los Cisco Access Servers en vez de NT RAS para sus pools del dial-in debido a la mejores densidad y funcionamiento del dial-in disponibles en los Cisco Access Servers.

Windows soporta el TCP/IP, el IPX, y el NetBEUI (IP Control Protocol [IPCP], IPX Control Protocol [IPXCP], y del protocolo netbios frames control protocolos del control [NBFCP] para el PPP). El soporte del dial-in del NetBEUI fue agregado al Cisco IOS Software en la versión 11.1. Para el dial del NetBEUI adentro, utilice el **comando netbios nbf** (tal y como se muestra en del siguiente ejemplo) en cada interfaz asincrónica o en una interfaz asincrónica de grupo en el servidor de acceso.

interfaz Ethernet 0

nbf de NetBIOS

Interface Group-Async 0

group-range 1 16

nbf de NetBIOS

Para configurar el dial IPX adentro, utilice el **comando ipx ppp-client** (tal y como se muestra en el siguiente ejemplo) en cada interfaz asincrónica o en una interfaz asincrónica de grupo en el servidor de acceso. Este comando le requiere configurar un IPX Network Address en un Loopback Interface. Los clientes dial in no necesitan oír los mensajes del protocolo service advertisement (SAP), así que estos mensajes se deben apagar con el **comando ipx sap-interval 0**.

```
Interface loopback 0 ipx network <network number> interface group-async 0 group-range 1 16 ipx ppp-client loopback 0 ipx sap-interval 0
```

Para asignar los IP Addresses a los clientes dial in, los Cisco Access Servers pueden utilizar un pool de las direcciones locales o actuar como proxy para un servidor DHCP. El servidor de acceso pide un direccionamiento del servidor DHCP y las aplicaciones que dirigen durante la negociación PPP. El cliente puede también negociar el direccionamiento de su servidor de los TRIUNFOS.

```
ip dhcp-server n.n.n.n async-bootp nbns-server m.m.m.m async-bootp dns-server p.p.p.p ip address-pool dhcp-proxy-client! interface group-async 0 group-range 1 16 peer default ip address dhcp
```

Dial-On-Demand Routing

El Dial-on-Demand Routing (DDR) proporciona las conexiones de red a través del Public Switched Telephone Network (PSTN). Tradicionalmente, las conexiones WAN han sido líneas arrendadas dedicadas. El DDR proporciona las conexiones de red de poco volumen, periódicas, permitiendo los costos de la red a pedido de los servicios y de la disminución. El Integrated Services Digital Network (ISDN) es un Circuit-Switched Technology. Como la red de teléfono analógico, se hacen las conexiones ISDN solamente cuando hay una necesidad de comunicar.

Uso DDR de los routers Cisco de determinar cuando una conexión necesita ser hecha a otro sitio. Los paquetes se clasifican como interesante o sin interés, sobre la base de las Listas de acceso del protocolo específico y de las listas del dialer. Los paquetes no interesantes pueden viajar a través de un link DDR activo, pero no sacan a colación el link, ni guardan el link para arriba.

Los clientes de las ventanas para grupos de trabajo y del Windows 95/98 que la parte clasifica o las impresoras se registran con GANAN cada doce o quince minutos enviando un paquete de unidifusión al servidor de los TRIUNFOS (en el puerto del servicio de nombre de NetBIOS del puerto 137---the UDP).

Los sistemas del Windows NT pueden también enviar una variedad de otros paquetes periódicos, que pueden causar los altos costos PÁLIDOS. Estos paquetes periódicos incluyen la sincronización del buscador, la replicación de los TRIUNFOS, la replicación, la navegación de la impresora, y el DHCP SAM (base de datos de la cuenta de usuario). Muchos de estos servicios tienen claves de registro que se puedan ajustar para traer para arriba a la conexión de marcado a pedido menos con frecuencia. Para más información, vea el *Microsoft Knowledge Base*, artículo: Q134985. Las entradas de registro importantes incluyen:

Hkey_local_machine \ sistema \ CurrentControlSet \ servicios \ navegador \ parámetros \ MasterPeriodicity

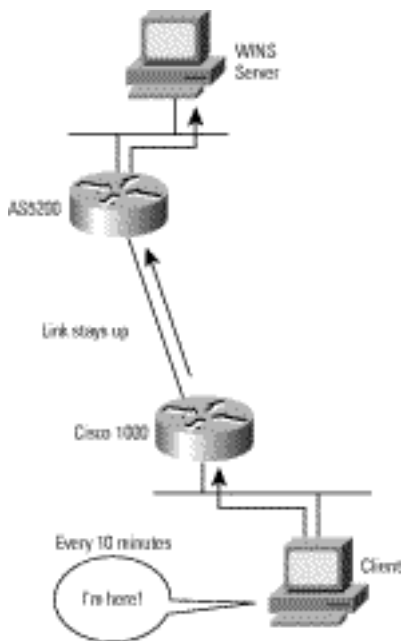
Hkey_local_machine \ sistema \ CurrentControlSet \ servicios \ navegador \ parámetros \ BackupPeriodicity

Hkey_local_machine \ sistema \ CurrentControlSet \ servicios \ Replicator \ intervalo

Hkey_local_machine \ sistema \ CurrentControlSet \ servicios \ Netlogon \ PulseMaximum

Hkey_local_machine \ sistema \ CurrentControlSet \ servicios \ control \ impresión \ DisableServerThread

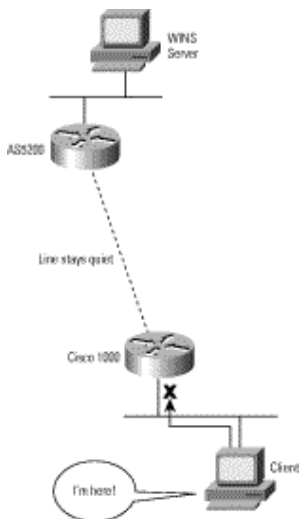
Figura 5: Enlace de marcado a pedido para arriba todo el tiempo



El envío de un paquete al servidor de los TRIUNFOS saca a colación normalmente al enlace de marcado a pedido. Si, sin embargo, este puerto se clasifica como sin interés al Cisco IOS Software, después el router ni saca a colación ni continúa el link.

```
Interface bri 0dialer-group 1!dialer-list 1 protocol ip list 101access-list 101 deny udp any any eq netbios-nsaccess-list 101 permit ip any any
```

Figura 6: El puerto 137 UDP es sin interés, link está abajo



Los filtros para las Cisco 700 Series están disponibles en la versión 4.1(2). Un filtro del ejemplo para hacer el tráfico del Windows NT SAM sin interés sigue:

```
SET netbsp OFFSET 2 FROM TCPHDR PATTERN 00 8b SET netbnsp OFFSET 2 FROM UDPHDR PATTERN 00 89 SET
netbdgp OFFSET 2 FROM UDPHDR PATTERN 00 8a SET refresh OFFSET 10 FROM UDPHDR PATTERN 40 00 SET
netbsm OFFSET 20 FROM TCPHDR PATTERN 00 SET smb OFFSET 24 FROM TCPHDR PATTERN ff 53 4d 42 SET
tcppat2 OFFSET 13 FROM TCPHDR PATTERN 02 SET netbsr OFFSET 20 FROM TCPHDR PATTERN 81 SET keepali
OFFSET 20 FROM TCPHDR PATTERN 85 SET tcpres OFFSET 13 FROM TCPHDR PATTERN 04 SET IP FILTER OUT
netbnsp refresh IGNORESET IP FILTER OUT netbdgp IGNORESET IP FILTER OUT netbsp netbsm smb
IGNORESET IP FILTER OUT netbsp tcppat2 IGNORESET IP FILTER OUT netbsp tcpres IGNORESET IP FILTER
OUT netbsp netbsr IGNORESET IP FILTER OUT netbsp keepali IGNORE
```

[Acceso ISDN](#)

Esta sección cubre los indicadores luminosos LED amarillo de la placa muestra gravedad menor y los adaptadores de terminal (TA) ISDN. Para la información sobre usar el Windows Networking con los routers ISDN, vea la sección anterior en el Dial-On-Demand Routing.

[Adtran](#)

Porque el Adtran y Cisco han trabajado de cerca durante la prueba de Interoperabilidad, el Adtran es un buen candidato a considerar para el externo TA. El Adtran TA soporta el multilink ppp (MP), el Challenge Handshake Authentication Protocol (CHAP), el protocolo password authentication (PAP), síncrono o las interfaces seriales asincrónicas, y la configuración del Automatic Service Profile Identifier (AutoSPID).

[BitSURFR de Motorola](#)

La manera más simple de hacer un BitSURFR conectado con un PC para interoperar con un router Cisco es girar el async/conversión sincronizada con el comando **AT%A2=95** (para más información, vea la página 7-1 del manual BitSURFR). Si usted está utilizando un Pro del BitSURFR y quiere utilizar ambos canales B, usted debe utilizar la autenticación PAP. El Pro del BitSURFR no puede contestar correctamente al desafío de la GRIETA enviado al sacar a colación el segundo canal B. Para poner una llamada usando dos canales B, usted debe ingresar el número de teléfono dos veces. Por ejemplo, si el número de teléfono es 555-1212, usted ingresaría el ATD555-1212&555-1212. La tabla siguiente enumera los comandos de ingresar para varios tipos de conexión:

Tabla 4: Comandos Configuration útiles para el BitSURFR de Motorola

Tipo de conexión	Comando
Conecte con el PPP	%A2=95
Utilice ambos canales B (el MP)	@B0=2
Utilizan la autenticación PAP	@M2=P
Velocidad del Data Termination Equipment (DTE) (puerto COM PC)	&M
Ponga las llamadas 64-kbps	%A4=0
Ponga las llamadas 56-kbps	%A4=1
Ponga las llamadas de voz	%A98

Software de cliente

CiscoRemote Lite

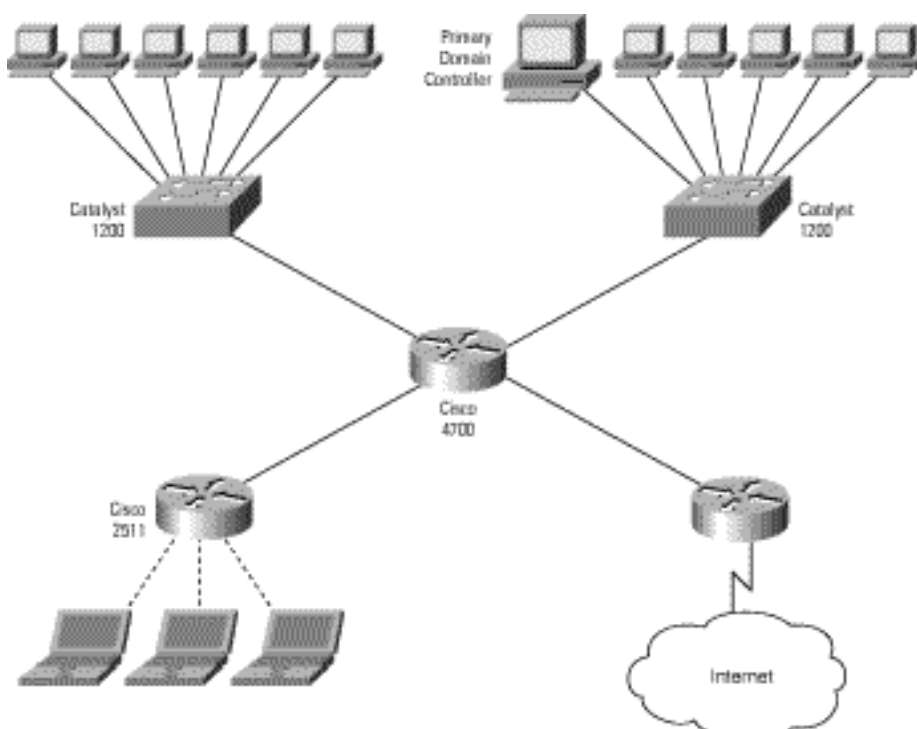
El CiscoRemote Lite es una aplicación libre de la pila de TCP/IP y del marcador para Windows 3.1 y las ventanas para grupos de trabajo. CiscoRemote soporta el PPP y los protocolos del protocolo serial line internet (SLIP).

Ejemplos

Ejemplo 1

El ejemplo 1 muestra un pequeño, red de un solo dominio usando el NWLink (NetBios sobre el IPX). El cuadro 7 muestra un gráfico de la configuración.

Figura 7: Pequeño, red de un solo dominio usando el NWLink



Configuración del Cisco 4700 Router

```
hostname 4700ipx routing!interface ethernet 0ipx network 50ipx type-20-propagationinterface ethernet 1ipx network 60ipx type-20-propagationinterface ethernet 2ipx network 7Bipx type-20-propagationinterface ethernet 3ipx network 95ipx type-20-propagation
```

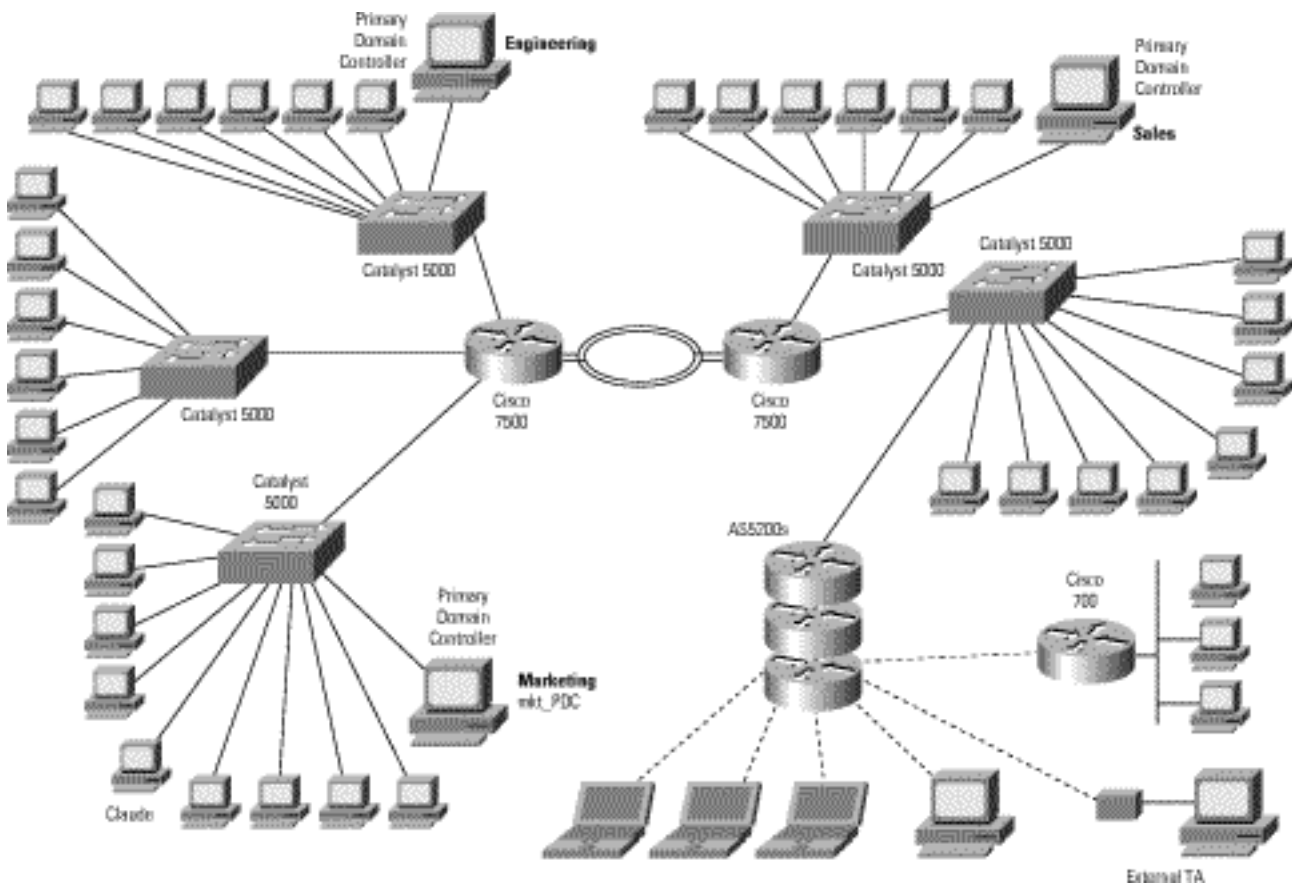
Configuración del Servidor de acceso Cisco 2511

```
hostname 2511ipx routing!interface ethernet 0ipx network 98interface loopback 0ipx network 163interface group-async 0group-member 1 16ipx ppp-client loopback 0ipx sap-interval 0encapsulation pppasync mode dedicated!line 1 16modem inoutspeed 115200flowcontrol hardware
```

'Ejemplo 2'

El ejemplo 2 muestra una red de tamaño medio usando NBT (NetBios sobre el TCP) y la resolución de nombre estática (LMHOSTS). El cuadro 8 muestra un gráfico de la configuración.

Figura 8: Red de tamaño medio usando el NBT y el LMHOSTS



Configuración LMHOSTS en Claude (cliente en el dominio de comercialización)

1.2.1.8	mkt_PDC	#PRE
1.2.7.3	mkt_BDC	#PRE
SUPLENTE #BEGIN		
\\\\ mkt_bdc \ público \ lmhosts del mkt_pdc #INCLUDE		
\ del público \ de los lmhosts #INCLUDE		
SUPLENTE #END		

Configuración LMHOSTS en el mkt_PDC (Primary Domain Controller para el dominio de

comercialización)

1.1.1.3	eng_PDC	#PRE #DOM: inglés
1.1.4.5	sales_PDC	#PRE #DOM: ventas
1.2.1.4	soñoliento	-
1.2.1.5	sneezy	-
1.2.6.2	Martin	-
1.2.6.78	Teresa	-
1.2.6.89	claude	-

Configuración del Cisco 7500 Router

```
hostname 7500ip forward-protocol udp bootpc!interface ethernet 0ip address 1.5.6.1
255.255.255.0ip helper-addressn.n.n.n...interface ethernet 23ip address 1.5.56.1 255.255.255.0ip
helper-addressn.n.n.n
```

Configuración de un AS5200 en un grupo de pila

```
hostname as5200-1!controller t1 0framing esflinecode b8zspri-groupcontroller t1 1framing
esflinecode b8zspri-group!sbgp group as5200ssbgp member as5200-2sbgp member as5200-3username
as5200s password stackpassword!ip dhcp-servern.n.n.nip wins-serverm.m.m.mip address-pool dhcp-
proxy-client!interface ethernet 0ip address 192.168.2.1 255.255.255.0!interface group-async
0group-member 1 48peer default ip address dhcp!interface serial 0:23dialer rotary-group 1isdn
incoming-voice modeminterface serial 1:23dialer rotary-group 1isdn incoming-voice modeminterface
dialer 1ip unnumbered ethernet 0encapsulation pppppp multilinkppp authentication chappppp use-
tacacsdialer-group 1!dialer-list 1 protocol ip permit!line 1 48modem inoutmodem autoconfigure
type microcom-hdmsspeed 115200flowcontrol hardware
```

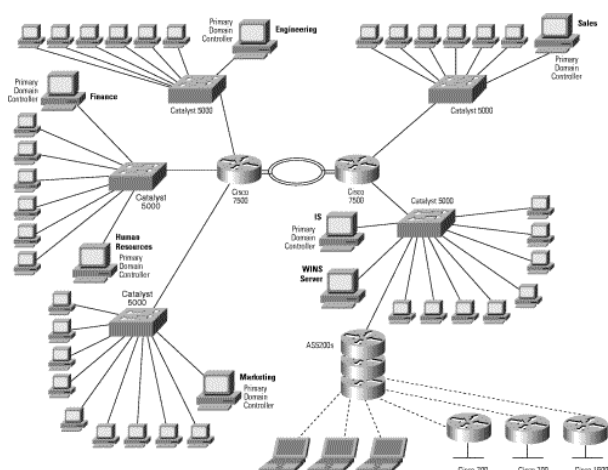
Configuración del Cisco 700 Router

```
set system 700cd LANset ip address 1.4.3.1set ip netmask 255.255.255.248set ip routing onset ip
rip update periodicCDset user as5200sset encapsulation pppset ip framing noneset ip routing
onset number 5551212set ip route destination 0.0.0.0/0 gateway 0.0.0.0CDset active as5200sset
bridging off
```

Ejemplo 3

El ejemplo 3 muestra una red de tamaño medio usando NBT (NetBios sobre el TCP) y un solo servidor de los TRIUNFOS. El cuadro 9 muestra un gráfico de la configuración.

Figura 9: Red de tamaño medio usando NBT (NetBios sobre el TCP) y un solo servidor de los TRIUNFOS



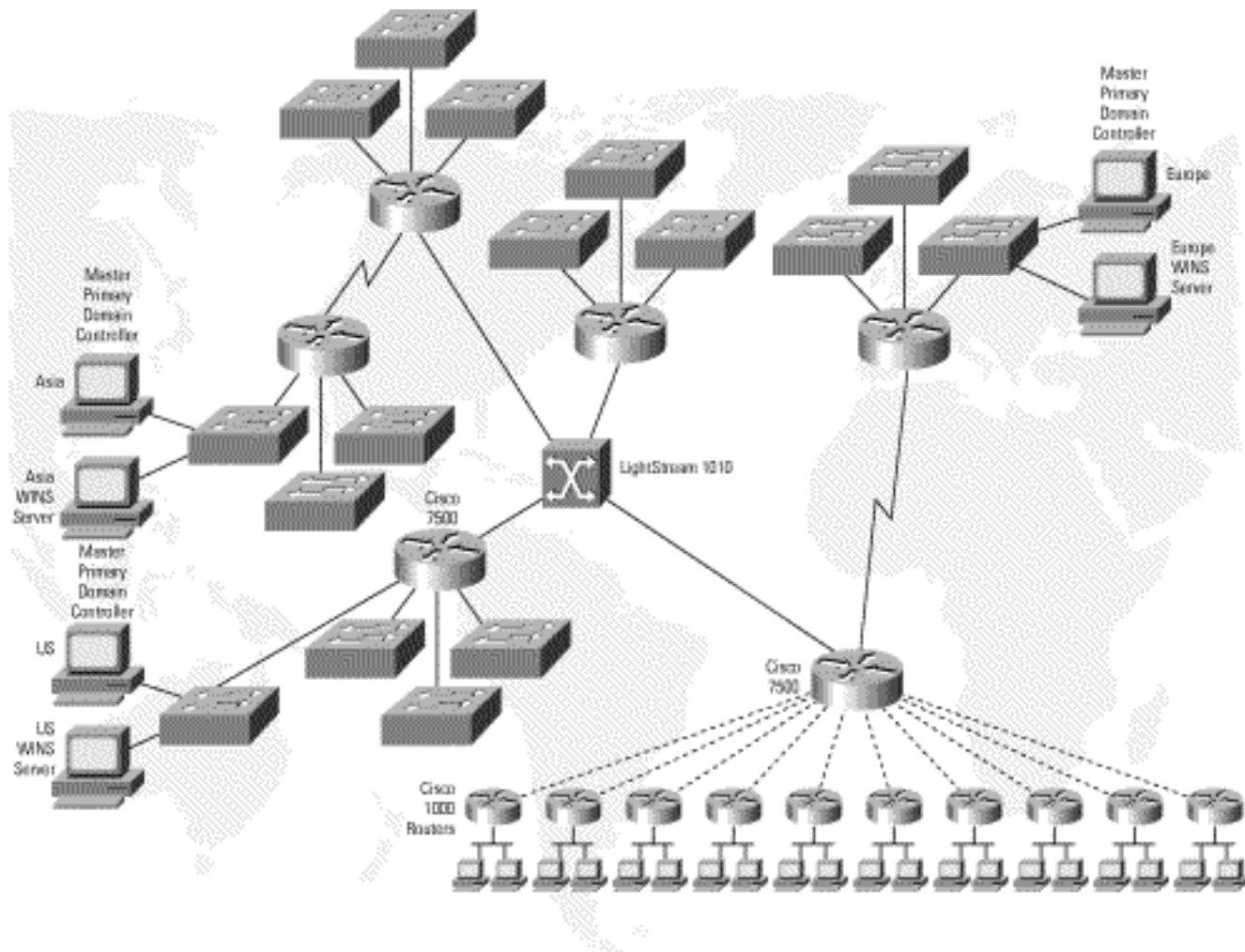
Configuración de un Cisco 1600

```
hostname 1600username as5200s password secret!interface ethernet 0ip address 1.4.3.1
255.255.255.248interface bri 0ip unnumbered ethernet 0encapsulation pppppp multilinkdialer
string 5551212dialer-group 1!dialer-list 1 protocol ip list 101access-list 101 deny udp any any
eq netbios-nsaccess-list 101 permit ip any any
```

Ejemplo 4

El cuadro 10 muestra una Red grande usando NBT (NetBios sobre el TCP) con los dominios maestros múltiples y los servidores replicados de los TRIUNFOS.

Figura 10: Red grande usando el NBT con los dominios maestros múltiples y los servidores replicados de los TRIUNFOS



Apéndice A: Apagar la resolución de nombre de broadcast

Al usar las ventanas para grupos de trabajo 3.11

Al usar las ventanas para grupos de trabajo 3.11, un nuevo archivo del navegador, el **VREDIR.386**, que se incluye con el Windows NT 3.5, se debe utilizar para permitir el hojear para trabajar correctamente. El Windows 95/98 incluye ya a este navegador modificado. El archivo VREDIR.386 se establece típicamente en el directorio de **C:\WINDOWS\SYSTEM**.

Los clientes de las ventanas para grupos de trabajo deben realizar el cambio siguiente al SYSTEM.INI clasificar:

; SYSTEM.INI

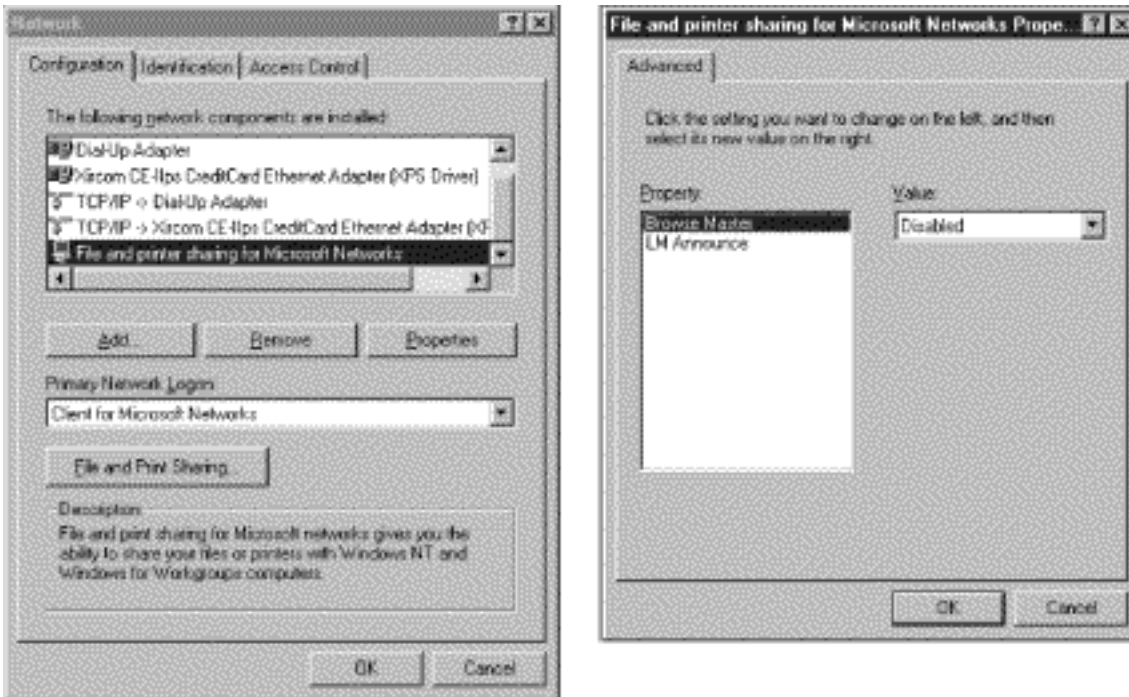
;

[network]

MaintainServerList=No

[Windows 95/98](#)

Cuadro 11: Apagar el browse master en el Windows 95/98



[Windows NT 3.51](#)

Los puestos de trabajo y los servidores del Windows NT 3.51 que se configuran para la resolución de nombre de los TRIUNFOS no envían los broadcasts a menos que otros ordenadores en el pedido de red una elección del buscador. No se requiere ninguna acción.

[Entradas de registro del Windows NT](#)

Estas entradas en el `hkey_local_machine \ el sistema \ el currentcontrolset \ los servicios \ navegador \ área de parámetros del registro` deben ser fijadas como sigue: `MaintainServerList` se debe fijar al sí, e `IsDomainMaster` se debe fijar a falso. Éstas son las configuraciones predeterminadas.

La configuración `MasterPeriodicity` (en los segundos) especifica cuantas veces la subred hojear los servidores pregunta al maestro del dominio para obtener una lista de la ojeada. Cuando la subred hojear los servidores y un link de poca velocidad separa al maestro del dominio o del carga-por-paquete, usted puede fijar esto a una hora o más.

[Encontrar a los exploradores maestros de variación aleatoria](#)

Los puestos de trabajo de Windows 3.1 y del Windows 95/98 no pueden funcionar como hojean los masters en una red del Windows NT porque no manejan el servidor NT y la información sobre el dominio. Desafortunadamente, por abandono, el Windows 95/98 intenta convertirse en un browse master. Una estación de trabajo única que demanda incorrectamente ser el browse master obstaculiza la ojeada para cada ordenador en esa subred completa. La prioridad para convertirse en un browse master es PDC, BDC, servidor NT, estación de trabajo NT, después el Windows 95/98, que deben evitar que ocurra esto.

Los kit de recursos del servidor del Windows NT 4.0 contienen una utilidad llamada **BROWSTAT**. La manera más fácil de encontrar un locutor rogue en una subred es ejecutar el BROWSTAT en un ordenador del Windows NT en la subred afectada.

[Apéndice B: Configurar la resolución de DNS de los nombres de los TRIUNFOS](#)

El servidor y el Windows 2000 ambos del Windows NT 4.0 incluyen a un servidor DNS que pueda contestar a las interrogaciones DNS preguntando un servidor de los TRIUNFOS en el fondo. El servidor DNS del Windows 2000 también soporta las actualizaciones dinámicas por el RFC 2136. El servidor de los TRIUNFOS y el servidor DNS no necesitan estar en la misma máquina de Windows Nt/2000. Todas las interrogaciones DNS a un subdomain (en este ejemplo, wins.cisco.com) se deben delegar al servidor DNS/WINS. Configurar a un servidor DNS de Windows Nt/2000 que usa un archivo del inicio no es necesario o recomendada por Microsoft. El administrador DNS proporciona una interfaz rica para el servicio.

[El archivo del inicio DNS](#)

; ARRANQUE	-	-
caché	.	CACHÉ
primario	domain.com	domain.dom
primario	8.17.1.in-addr.arpa	1-17-8.rev

[El archivo DNS para domain.com](#)

; domain.dom				
@	I N	SOA	ns.domain.com.	rohan.domain.com. (
			1	; Número de serie
			10800	; Restaure [3h]
			3600	; Revise [1h]
			604800	; Expiran [7d]
			86400)	; Mínimo [1d]
@	I N	GAN A 1.1.4.		

		6 1.2.7. 4		
triunfo- servidor	I N	1.1.4. 6		
wins-server2	I N	1.2.7. 4		

¹Albitz, Paul y grillo Liu. Sebastopol, CA: O'Reilly y socios, 1992.

[Información Relacionada](#)

- [Soporte Técnico - Cisco Systems](#)