1-3-2017

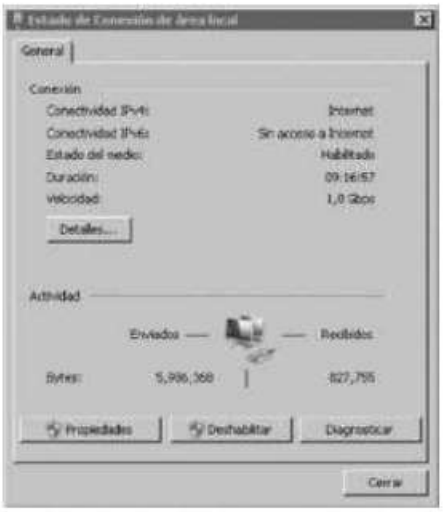
MODULO V / SUBMODULO 1

DOCUMENTO DE REDES LAN, PARCIAL DOS (No. A01)

CETis 115
ESPECIALIDAD DE TELECOMUNICACIONES 2017;
ING. CARLOS ALFONSO HERNÁNDEZ VILLANUEVA

Figura 1-10

Cuadro de diálogo Estado de Conexión de Área Local



Definiendo la Transferencia de Datos en una LAN

Generalmente, cuando la información es transferida en una LAN se envía de forma serial a través de cableado de par trenzado. La *Transferencia serial de datos* significa la transferencia de un bit a la vez, en otras palabras, transferir en una sola cadena de bits. Este es el formato regularmente utilizado para enviar información de un adaptador de red a otro. Ahora, discutiremos esta ordenación a mayor profundidad. Digamos que un usuario desea enviar un archivo de texto pequeño (tamaño de 10 bytes) a otro usuario en la red. Hay muchas formas de hacer esto, una forma sería mapear una unidad de red a otra computadora de usuario y simplemente copiar y pegar el archivo de texto al disco duro de la otra computadora. Cuando ocurre esto, suceden algunas cosas:

1. Primero, el archivo de texto se empaqueta por el sistema operativo. El paquete será ligeramente más grande que el archivo original. El paquete es entonces enviado al adaptador de red.
2. A continuación, el adaptador de red toma el paquete y lo ubica dentro de un frame, el cual es ligeramente más grande que un paquete, regularmente, éste será una frame Ethernet.
3. Ahora, se debe enviar el frame de información al medio físico, el cableado. Para hacer eso, el adaptador de red divide el frame de información en una cadena serial de datos que se envía un bit a la vez a través de los cables a la otra computadora.
4. La computadora receptora toma la cadena de bits y recrea el frame de datos. Después de analizar el frame y verificar que de hecho es el receptor destino, la computadora desmonta el frame de información para que sólo quede el paquete.
5. El paquete se envía al sistema operativo y finalmente, el archivo de texto aparece en el disco duro de la computadora, disponible para el usuario a través del explorador de Windows. Este es un ejemplo básico de transferencia de datos y lo ampliaremos en la Lección 2, "Definiendo redes con el Modelo OSI."

Regularmente, las LANs utilizan uno de varios estándares Ethernet. ***Ethernet*** es un conjunto de reglas que gobiernan la transmisión de datos entre adaptadores de red y varios dispositivos de conexión central. Todos los adaptadores de red y dispositivos de conexión central deben ser compatibles con Ethernet con el fin de comunicarse entre sí. Un tipo

común de Ethernet es conocido como 802.3u o Fast Ethernet y se ejecuta a 100 Mbps. Otro tipo común es 802.3ab o Gigabit Ethernet.

En este tipo de red cuando una computadora envía datos, éstos son transmitidos por defecto (broadcast) a cada uno de los hosts en la red. El problema con este método es que generalmente sólo hay un receptor destinado para la información, así que el resto de computadoras simplemente deshecha los paquetes de datos. Esto a su vez desperdicia ancho de banda de red. Para aligerar este problema, se desarrolló el switcheo Ethernet hace cerca de 15 años y aún es utilizado en la mayoría de redes hoy en día. El Switcheo o Switching tiene muchas ventajas, una de ellas es que el switch sólo envía tráfico unicast. ***Unicast*** describe la situación en la cual la información se envía a un solo host. Esto reduce el tráfico de red en gran medida y también ayuda con los paquetes perdidos y duplicados.

Hemos mencionado el tema de la velocidad de la red varias veces. Sin embargo, un término más preciso sería ***tasa de transferencia de datos***, conocido también como tasa de bits, la cual es el máximo de bits por segundo (bps) que pueden ser transmitidos por la red. Como se mencionó anteriormente, este valor es nominal en bits y se señala con una *b* minúscula (por ejemplo, 10 Mbps). La b minúscula ayuda a diferenciar esta cantidad de datos que son almacenados en un disco duro, el cual utiliza un B mayúscula que se coloca para bytes (por ejemplo 10 MB).

Por supuesto, todo esto no significa nada sin un sistema de direccionamiento. El tipo más común de dirección de red es la dirección de protocolo de internet o simplemente, dirección IP.

Configurando el Protocolo de Internet

El Protocolo de Internet o IP, es la parte de TCP/IP que, entre otras cosas, gobierna las direcciones IP. La ***dirección IP*** es la piedra angular de las redes porque define la computadora o host en la que usted está trabajando. Hoy en día, cada computadora y muchos otros dispositivos tienen esa dirección. Una dirección IP le permite a cada computadora enviar y recibir información de un lado a otro de una manera ordenada y eficiente. Las direcciones IP son parecidas a la dirección de su casa. Sin embargo, mientras que su dirección identifica el número de la casa y la calle en la que vive, una dirección IP identifica el número de computadora y la red en la que vive. Un ejemplo típico de una dirección IP seria 192.168.1.1.

Cada dirección IP se divide en dos partes: la porción de red (en este caso 192.168.1), la cual es la red en la que su computadora es miembro y la porción de host, el cual es el número individual de su computadora que diferencia su computadora de las demás en la red. En este caso, la porción de red es .1. ¿Cómo sabemos esto? La máscara de subred nos lo dice.

La máscara de subred es un grupo de cuatro números que define de cual red IP es miembro la computadora. Todos los 255 en una máscara de subred se refieren colectivamente a la porción de subred, mientras que los 0 se refieren a la porción de host. La Tabla 1-1 muestra una dirección IP de clase C típica y la máscara de subred correspondiente por defecto. Si fuera configurar la dirección IP de una computadora con Windows como 192.168.1.1. Windows automáticamente establecería por defecto la máscara de subred 255.255.255.0. si otras computadoras necesitan comunicarse con la suya, estas deben configurarse con el mismo número de red, sin embargo, cada computadora en la misma red necesita tener un numero diferente de host o podría suceder un conflicto de IP. Por supuesto, como un administrador capacitado, aprenderá cómo evitar conflictos de IP. Encontrará algunos consejos sobre cómo hacerlo en las lecciones 4 y 5.

Tabla 1-1

Una dirección IP y su máscara de subred correspondiente

Tipo de dirección	Primer Octeto	Segundo Octeto	Tercer Octeto	Cuarto Octeto
Dirección IP	192	168	1	1
Máscara de subred	255	255	255	0

Las direcciones IP son de hecho números de punto decimal de 32 bits. Si fuera a convertir una dirección IP de números decimales a binario, tendría un total de 32 bits. Una dirección IP se considera de punto porque cada número está separado por un punto. En total, cada dirección IP contiene cuatro números, cada uno de los cuales es un byte o un octeto. Así, en nuestro ejemplo, 192 es un octeto y su equivalente binario seria 11000000 los cuales son ocho bits. 168 también es un octeto, su equivalente binario es 10101000 y así sucesivamente. Agregando los cuatro octetos juntos nos da 32 bits.

Las direcciones IP se aplican generalmente al adaptador de su red pero también se pueden aplicar a otros dispositivos como switches, routers, etc. El hecho de que un dispositivo o computadora tenga una dirección IP es lo que lo hace un host. Configuremos direcciones IP en nuestro host con Windows 7. Recuerde que otras computadoras con Windows se configurarán de manera similar.

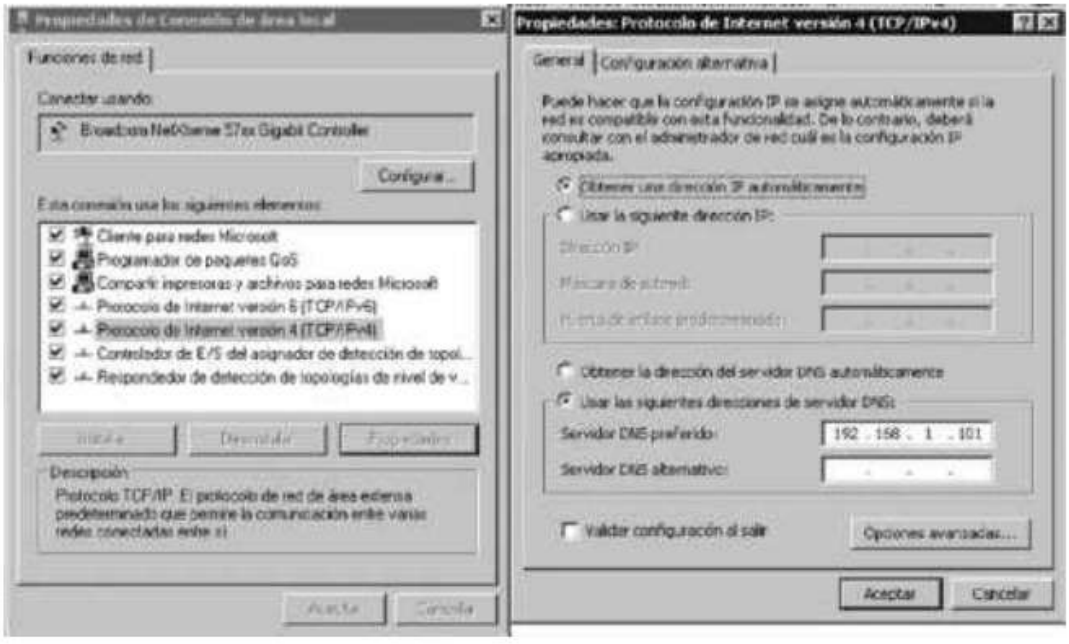
→ Configurar Direcciones IP

PREPÁRESE. Para configurar direcciones IP, desarrolle estos pasos:

1. Acceda al cuadro de diálogo Propiedades de Conexión de Área Local una vez más.
2. Haga clic en **Protocolo Internet Versión 4**, entonces dé clic en el botón de **Propiedades**.
3. Por defecto, las opciones del cuadro de diálogo estarán configuradas como "Obtener una dirección IP automáticamente" y "obtener la dirección del servidor DNS automáticamente", como se muestra en la Figura 1-11. Esto significa que el adaptador de red intentará obtener toda su información de IP de un servidor DHCP u otro dispositivo como un router SOHO de 4 puertos. Sin embargo, lo que queremos es configurar el adaptador de forma estática, así que continuemos.

Figura 1-11

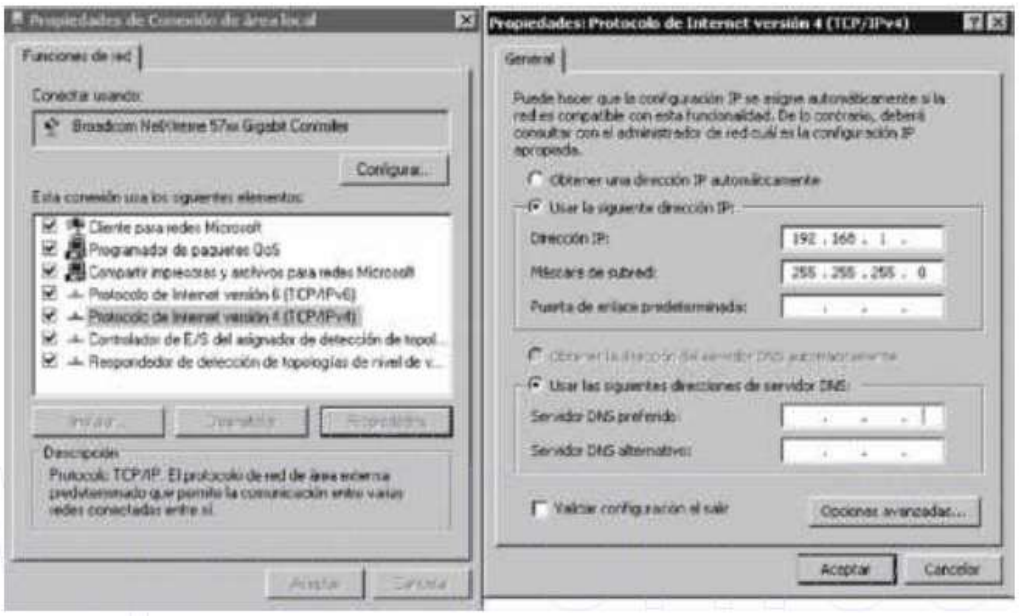
Cuadro de diálogo Propiedades de Protocolo de Internet Versión 4



4. Dé clic en el botón de radio **Usar la siguiente dirección IP**. Se habilitan los otros campos de forma que podrá introducir la información deseada. Ingrese lo siguiente:
   - Para dirección IP, introduzca 192.168.1.1.
   - Para la máscara de subred, introduzca 255.255.255.0.
   - Deje los campos de puerta de enlace predeterminada y el servidor DNS preferido en blanco.
   - Cuando termine, su cuadro de diálogo debe parecerse a al mostrado en la Figura 1-12.
   - Si tiene otras computadoras, trate de configurar sus direcciones IP también. Recuerde, la porción de host de la dirección IP debe ascender una vez para cada computadora, .1, .2, .3 y así sucesivamente.

Figura 1-12

Cuadro de diálogo Propiedades de Protocolo de Internet Versión 4 configurada estáticamente



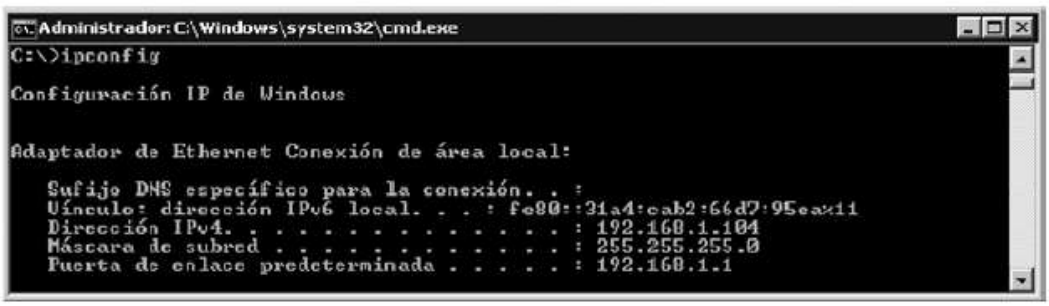
★ Tome Nota

Si está trabajando con otros durante este ejercicio, cada persona debe introducir una dirección IP diferente. Por ejemplo, la primera persona debe introducir 192.168.1.1, la segunda persona debe introducir 192.168.1.2, y así sucesivamente. Esto evitará cualquier posible conflicto de IP

5. Dé clic en **Aceptar**, luego en el cuadro de diálogo Propiedades de Conexión de Red Local y finalmente seleccione **Aceptar**. Se terminará y establecerá la configuración al adaptador de red.
6. Pruebe su configuración. Haremos esto de dos maneras, primero con el comando **ipconfig** y después con el comando **ping**.
   a. Abra el símbolo del sistema. Hágalo presionando las teclas **Windows+R** y escribiendo **cmd** en el campo abierto. Ahora, introduzca **ipconfig**. El resultado debe parecerse a Figura 1-13. Observe que el campo de dirección IPv4 está en los resultados y la dirección IP está enlistada. Esta debería ser la dirección IP que configuró previamente. Si no, regrese y revise su cuadro de diálogo Propiedades de Protocolo Internet.

Figura 1-13

Resultados de ipconfig



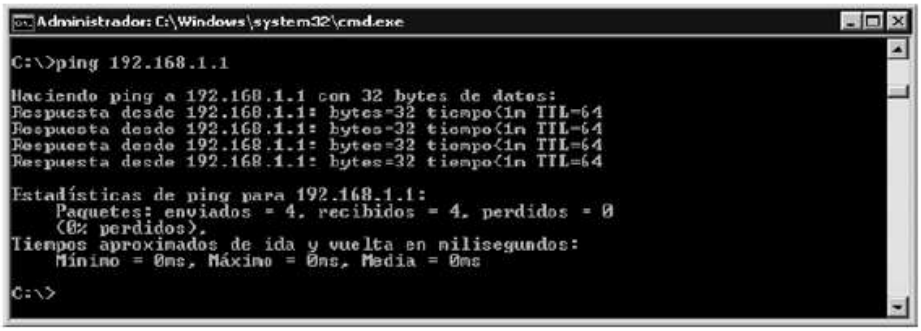
b. Dé un ping a una computadora en la misma red 192.168.1. Si no hay otras computadoras, de ping a su propia dirección IP. Por ejemplo, introduzca el siguiente comando:

ping 192.168.1.1

Este comando envía una petición a otra dirección IP. Si la otra computadora se está ejecutando y está configurada apropiadamente, deberá replicarlo de regreso. Un ping positivo debería ser similar a la Figura 1-14, en la cual se reciben cuatro respuestas en la computadora que envía el ping.

Figura 1-14

Resultados de Ping



Si por alguna razón no obtiene una respuesta u obtiene otro mensaje como "Tiempo de espera agotado para esta solicitud", deberá revisar la configuración IP otra vez para asegurarse que la otra computadora que está tratando de enviarle ping esté configurada apropiadamente. También asegúrese de que todas las computadoras involucradas estén cableadas a la red.

★ Tome Nota

Siempre pruebe sus configuraciones de red

También puede enviar un ping a su propia computadora utilizando la dirección de loopback. Cada computadora con Windows obtiene automáticamente esta dirección, que es 127.0.0.1. Esta dirección existe además de la dirección lógica que asignó anteriormente. Pruebe el comando **ping loopback** y revise sus resultados. También puede probar **ping localhost** y **ping 127.0.0.1**. Deberá obtener los resultados de127.0.0.1. Cuando se envía un ping a esta dirección, no ocurre ningún tráfico de red, ya que el adaptador de red solamente esta ciclando de regreso el ping al sistema operativo, este nunca ubica ningún paquete en la red. Por lo tanto, ésta es una manera confiable para probar si el TCP/IP está instalado correctamente en el adaptador de red. Aun si no está conectado físicamente a la red.

Cuando termine, regrese su computadora a su configuración regular de IP. Explicaremos más acerca de IPs en la Lección 5, "Comprendiendo el Protocolo de Internet".

► *Identificando Tipos de LANs*

Existen varios tipos de redes de área local a las que una computadora se puede conectar. Una organización debe elegir entre utilizar conexiones alámbricas, conexiones inalámbricas o una mezcla de las dos. También es posible tener LANs virtuales.

☑ Listo para la Certificación

¿Cómo identifica los diferentes tipos de LANs?—1.2

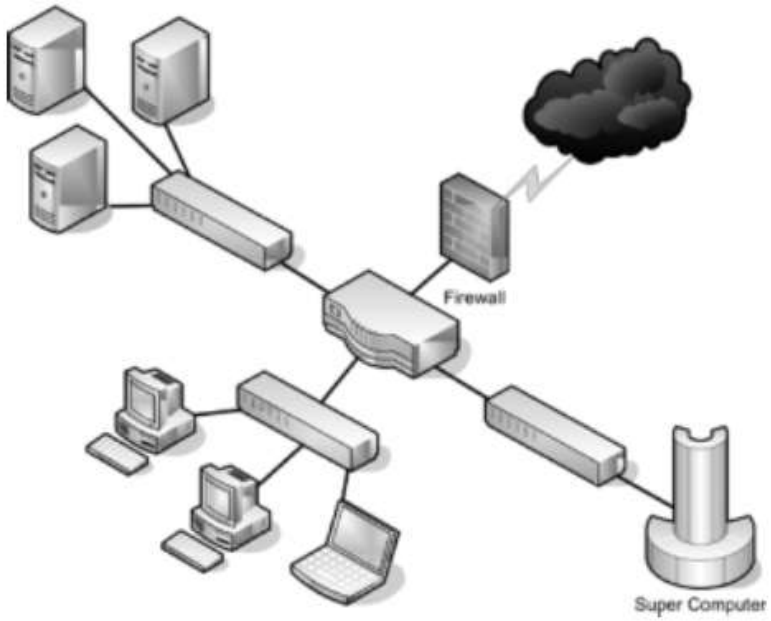
El primero y más común de los tipos de LAN es la alámbrica. Aquí, las computadoras y otros dispositivos están interconectados utilizando cables de par trenzado de cobre. Estos cables tienen un conector RJ45 en cada extremo, el cual es la conexión real a los puertos RJ45 que residen en el adaptador de red de la computadora y en los hubs, switches, o routers. (Por supuesto, probablemente haya algún otro cableado de equipos entre cada uno de ellos, pero lo cubriremos más profundamente en la Lección 3 "Comprendiendo redes alámbricas e inalámbricas.")

La Figura 1-15 tiene un nuevo diagrama, pero esta vez muestra tres LANs conectadas por un router. Algunos nuevos dispositivos que no hemos visto hasta ahora aparecen en la

figura, estos son firewalls, los cuales protegen la LAN (o LANs) del Internet y una súper computadora, la cual ocupa su propia pequeña LAN.

Figura 1-15

Documentación de LAN alámbrica



Generalmente, la conexión de las PCs a su switch será o de 100 Mbps o de 1 Gpbs. Cualquiera que sea la velocidad que decida utilizar debe ser soportada por cada puerto del switch, así como también por cada computadora. En este diagrama, la computadora está cableada al switch. Por lo tanto, para alcanzar la velocidad de red gigabit, los cables utilizados deberían ser Categoría 5e o mayor (profundizaremos sobre tipos de cableado en la Lección 3).

Sin embargo, la conexión de la granja de servidor al switch en la parte superior izquierda, así como a la súper computadora a su switch, debe ser más rápida que tu conexión PC promedio. Así, si las PCs en la LAN se conectaron a 100 Mbps, los servidores se podrían conectar a 1 Gbps; de manera similar, si las PCs se conectan a 1 Gbps, los servidores deberían conectarse a 10 Gbps. También se deben realizar conexiones de alta velocidad entre los tres switches y el router. Ahora estamos viendo una representación más precisa de una configuración de red de nuestra compañía ficticia. Sin embargo, nuestra documentación de red será mucho más detallada a medida que avancemos. Después de todo, sólo estamos en la Lección 1.

Históricamente, las redes alámbricas fueron significativamente más rápidas que las redes inalámbricas. Pero ahora, la diferencia de velocidad entre las dos es mucho más pequeña debido al hecho de que las tecnologías de redes inalámbricas han progresado a saltos agigantados desde la década pasada más o menos. Una ***Red de Área Local Inalámbrica*** (WLAN) tiene muchas ventajas, la más obvia es la movilidad. Una persona con una laptop, computadora portátil, PDA u otro dispositivo puede trabajar desde donde sea. Sin embargo, las LANs inalámbricas tienen muchos problemas de seguridad, y debido a esto, algunas compañías han optado no utilizarlas en sus oficinas principales. La Figura 1-16 ilustra algunos dispositivos inalámbricos.

Figura 1-16

Diagrama de LAN inalámbrica

El *punto de acceso inalámbrico* (WAP) actúa como el dispositivo de conexión central. Hoy en día, estas redes pueden consistir de muchos tipos de dispositivos que no sean PCs tradicionales, incluyendo teléfonos inteligentes, PDAs, computadora de tableta y micro computadoras. Sin mencionar el hecho de que las PCs y laptops equipadas con adaptadores de red inalámbrica pueden conectarse a esas redes también.

Las redes inalámbricas y redes alámbricas pueden coexistir. De hecho, en redes pequeñas, un solo dispositivo puede actuar como punto de acceso inalámbrico, switch, router y firewalls. Sin embargo, las redes más grandes generalmente tendrán uno o más puntos de acceso inalámbricos separados que se conecten de forma alámbrica a un switch de red. También, es importante notar que los puntos de acceso inalámbricos tiene un rango limitado. Por lo tanto, podría necesitar implementar múltiples WAPs dependiendo del tamaño del edificio y el área que requiera cubrir.

Referencia Cruzada

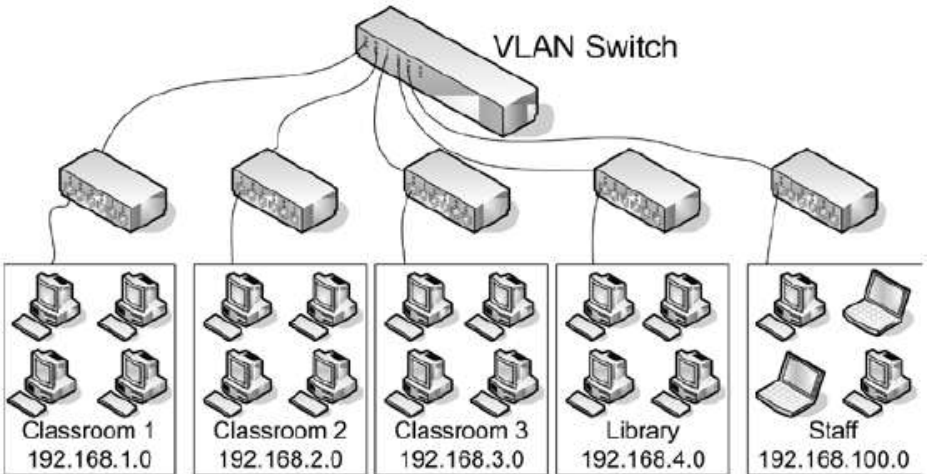
Para más información acerca de redes alámbricas e inalámbricas, referirse a la Lección 3

También existe otro tipo de LAN, la LAN Virtual o VLAN. Una ***LAN Virtual*** es un grupo de hosts con un conjunto común de requerimientos que se comunican como si estuvieran conectados de una manera normal en un switch, sin importar su localización física.

Una VLAN se implementa a un segmento de red, reduce colisiones, organiza la red, impulsa el desempeño e incrementa la seguridad. Generalmente los switches controlan la VLAN. Como subneteo, una VLAN segmenta a una red y puede aislar el tráfico. Pero a diferencia del subneteo, una VLAN puede establecerse de manera física, un ejemplo de esto sería la VLAN basada en puertos, como se muestra en la Figura 1-17. En este ejemplo, cada conjunto de computadoras (como "Salón de Clases 2") tiene su propia VLAN (la cual está dedicada a la red 192.168.2.0 en este caso); sin embargo, las computadoras en esa VLAN se pueden localizar en cualquier lugar de la red *física*. Como otro ejemplo, las computadoras dentro del "Staff" VLAN se pueden ubicar en algunas áreas físicas en el edificio, pero sin importar donde estén ubicadas, estarán asociadas con el Staff VLAN debido al puerto físico donde se conectan.

Figura 1-17

Ejemplo de una VLAN



También existen tipos lógicos de VLANs, como la VLAN basada en protocolo y la VLAN basada en dirección MAC, pero por mucho, el más común es la VLAN basada en puerto. El estándar más común asociado con VLANs es el IEEE 802.1Q, el cual modifica Frames Ethernet "etiquetándolos" con la información VLAN apropiada. Esta información de VLAN determina la VLAN a la cual dirigir el Frame Ethernet.

▶ *Introducción a las Redes Perimetrales*

Las Redes Perimetrales son pequeñas redes que generalmente consisten de sólo algunos servidores que son accesibles desde la Internet de alguna manera. Generalmente, el término "red perimetral" es sinónimo de zona desmilitarizada (DMZ). Usted debería ser capaz de identificar una DMZ y su propósito en la organización, así como también saber cómo implementar una DMZ básica.

☑ Listo para la Certificación

¿Cómo define a las redes perimetrales?—1.2

Una *red perimetral* (también conocida como una *zona desmilitarizada o DMZ*) es una red pequeña que se implementa separadamente de una LAN privada de la compañía y de la Internet. Se llama red perimetral debido a que generalmente se encuentra en la orilla de la LAN, pero la DMZ se ha convertido en un término mucho más popular. Una DMZ permite a los usuarios fuera de la compañía acceder a servicios específicos ubicados en la DMZ. Sin embargo, cuando se implementa apropiadamente una DMZ, a esos usuarios se les bloquea el acceso a la LAN de la compañía. Los usuarios en la LAN a menudo se conectan también a la DMZ, pero lo pueden hacer sin tener que preocuparse por atacantes externos que accedan a su LAN privada. Un DMZ puede alojar un switch con servidores conectados que ofrezcan Web, correo electrónico y otros servicios. Dos configuraciones comunes de las DMZs incluyen lo siguiente:

★ Tome Nota

Puede aprender más acerca de Microsoft ISA Server o Microsoft Forefront accediendo al enlace proporcionado en el sitio Web que acompaña a este libro

- **Configuración Back-to-back**: Involucra a una DMZ situada entre dos firewalls, los cuales pueden ser aplicaciones de caja negra o servidores de Aceleración y seguridad de Microsoft Internet (ISA), o tal vez dispositivos Microsoft Forefront. Una ilustración de esta implementación aparece en la Figura 1-18. En esta configuración, un atacante tendría que pasar por dos firewalls para ganar acceso a la LAN.
- **Configuración perimetral de 3 patas**: en este escenario, la DMZ generalmente se adjunta a una conexión separada del firewall de la compañía. Por lo tanto, el firewall podría tener tres conexiones: una para la LAN de la compañía, otra a la DMZ y otra a Internet, como se muestra en la Figura 1-19. Una vez más, esto se puede hacer con una aplicación de firewall o con un servidor de Microsoft ISA. En esta configuración, un atacante solo necesitaría atravesar un firewall para ganar acceso a la LAN. Aunque esto es una desventaja, las tecnologías como los sistemas de detección y prevención de intrusos de red pueden ayudar a aligerar la mayoría de las cuestiones de seguridad. Además, un sólo firewall significa menos administración.

Figura 1-18

Una configuración back-to-back de una DMZ

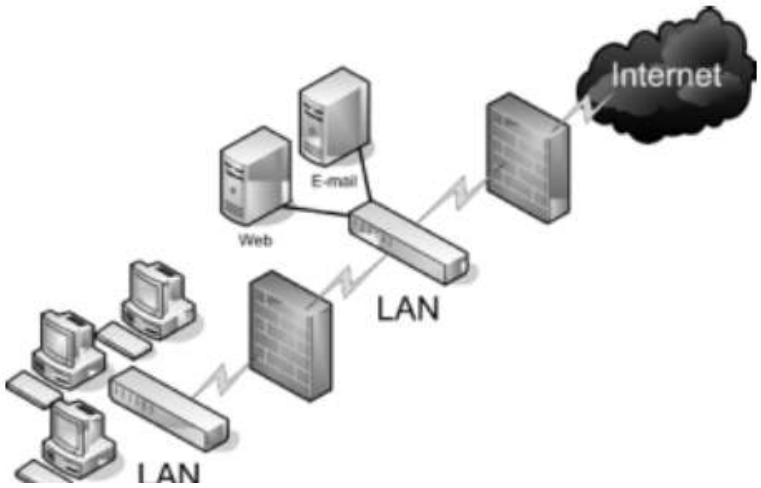
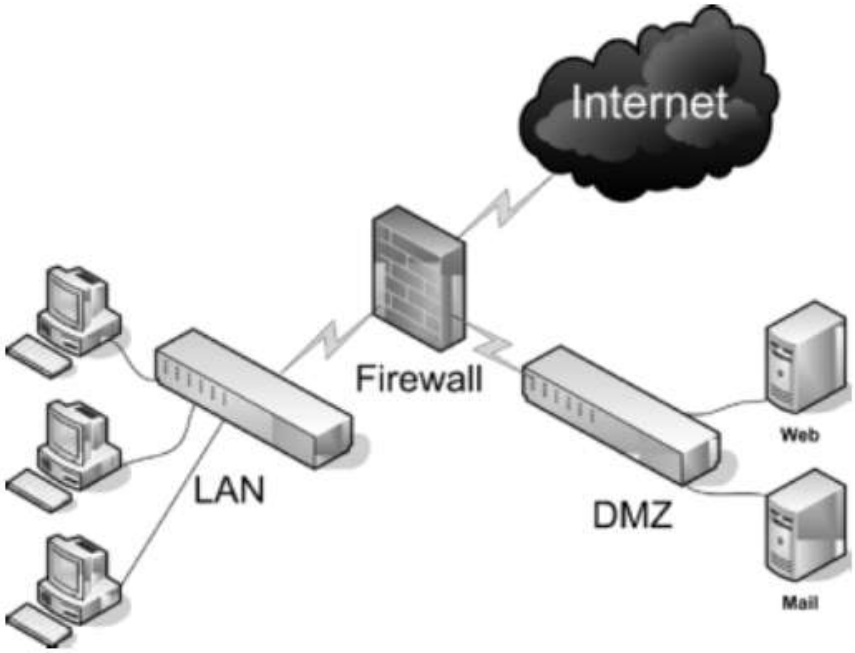


Figura 1-19

Una configuración perimetral de 3 patas de una DMZ



▪ Identificando Topologías de Red y Estándares

↓ EN RESUMEN

Las redes necesitan estar situadas de alguna manera que se facilite la transferencia de información. Las topologías son las colocaciones físicas de las computadoras en una LAN. Los métodos de acceso indican como las computadoras realmente envían datos, la más común de ellas es la configuración Ethernet basada en el cliente/servidor, aunque hay otras. Con el fin de construir una LAN, primero debe planear que topología (o topologías) serán utilizadas y qué tipo de métodos de acceso serán implementados. Los métodos tienden a ser un concepto menos tangible, así que empecemos con las topologías de red.

▶ *Identificando Topologías de Red*

Una ***topología de red*** define la conexión física de hosts en una red de computacional. Hay varios tipos de topologías físicas, incluyendo: bus, anillo, estrella, malla y árbol. Para el examen, deberá conocer las topologías de estrella, anillo y malla. Incluiremos la topología de árbol, también conocida como topología de estrella jerárquica, ya que muchas personas la consideran una extensión de la topología de estrella. También identificamos topologías lógicas, ya que tienen características diferentes a las topologías físicas.

☑ Listo para la certificación

¿Cómo define las topologías de red y los métodos de acceso?—1.5

En este ejercicio, examinaremos las siguientes topologías de red *físicas*:

- Estrella
- Malla
- Anillo

Por mucho, la topología más común es la ***topología de estrella***. Cuando se utilice una topología de estrella, cada computadora se cablea individualmente a un dispositivo de conexión central con cables de par trenzado. El dispositivo de conexión central podría ser un hub, un switch o un router SOHO. Este es el tipo de topología que se utiliza generalmente para implementar redes.

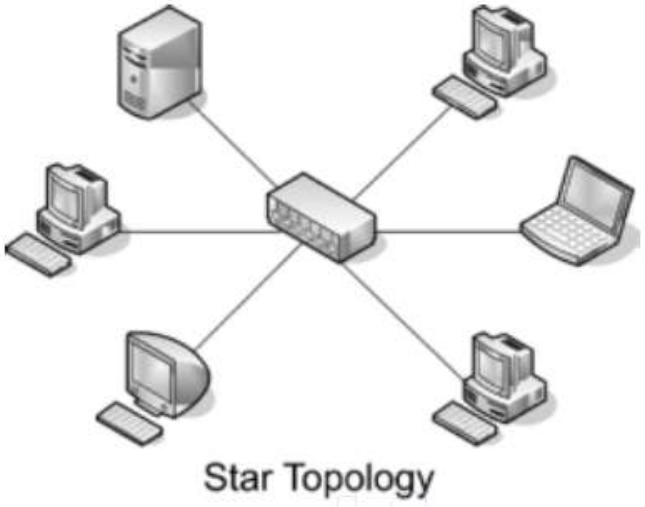
→ Identificando Topologías

PREPÁRESE. Para identificar topologías, desarrolle estos pasos:

1. Examine la Figura 1-20. Ésta ilustra una topología de estrella simple. Observará que esta imagen es similar a las Figuras 1-1 y 1-2 anteriores en esta lección. De hecho, esas otras figuras también ilustran topologías de estrella. Note que el hub en el centro de la figura conecta a cada computadora por un solo cable. De esta manera, si un cable es desconectado, el resto de la red puede seguir funcionando, este es la topología física estándar para una red Ethernet.

Figura 1-20

Topología de Estrella



2. Examine su propia red computacional. Revise si tiene las características de la topología de estrella: esto es decir, ¿cada computadora está conectada a un dispositivo de conexión central?, ¿las computadoras están cableadas individualmente al dispositivo?, si identifica su red como una topología de estrella, añada el hecho a su documentación de red.

   En los viejos tiempos, las redes a menudo utilizaban lo que se conoce como topología de bus. Con esa topología, todas las computadoras estaban conectadas a un solo cable de bus, por lo tanto, si una computadora fallaba, la red entera se venía abajo. A pesar de esta desventaja parte del concepto de la topología de bus pasó a la topología de estrella. Por ejemplo, dos redes en estrella individuales se pueden conectar (por medio de sus dispositivos de conexión central) para crear una topología de estrella-bus. Esto se hace conectando en serie (o apilando) uno o mas hubs o switches, regularmente por un puerto especial de ***Interfaz dependiente al medio (MDI)***, aquí es donde entra la parte de "bus" de una topología de estrella-bus.

Referencia Cruzada

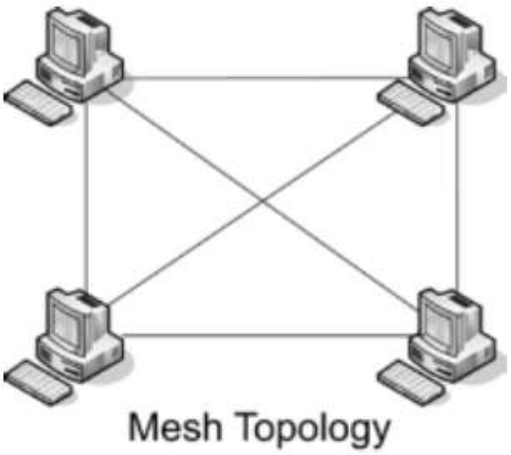
Estudiaremos más de cerca los puertos MDI en la Lección 3 "Comprendiendo redes alámbricas e inalámbricas"

   El problema de la topología de estrella-bus es que está basada en el concepto de apilamiento. Esto puede plantear problemas organizacionales y sobre el aprovechamiento del ancho de banda. Una mejor solución en la mayoría de los escenarios es utilizar la estrella jerárquica, mostrada en la Figura 1-3 anteriormente en esta lección.

3. En una ***topología de malla***, cada computadora se conecta con cada otra computadora, no se necesita un dispositivo de conexión central. Como se puede imaginar, una malla verdadera o "completa" requiere muchas conexiones, como se ilustra en la Figura 1-21. Examine la figura y calcule cuantas conexiones serian necesarias en cada computadora para asegurar una configuración de malla completa.

Figura 1-21

Topología de Malla

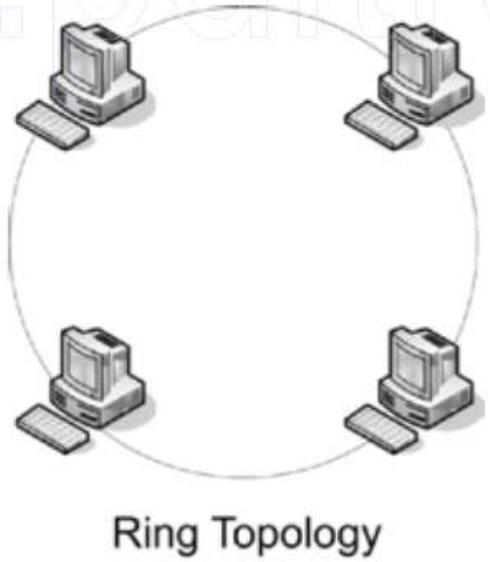


El número de conexiones de red que cada computadora necesitará es el número total de computadoras menos uno. Como se puede imaginar, este tipo de topología es raro, pero es necesario en algunas situaciones de laboratorio y escenarios con falta de tolerancia (donde la información necesita ser replicada a múltiples maquinas). Una versión menor de esta topología es la "malla parcial", en la cual sólo una o un par de las computadoras en la red tienen una segunda conexión. (Esto puede ser útil cuando necesita que una computadora replique una base de datos a otra computadora pero no quiere que la conexión sea molestada por cualquier otro tráfico). Una computadora con dos o más conexiones de red es conocida como computadora multi-homed.

4. Por último, tenemos la ***topología de anillo***. Observe la Figura 1-22. Esta ilustra cómo las computadoras se pueden conectar en forma de anillo. En una ambiente LAN, cada computadora se conecta a la red utilizando un circuito cerrado, históricamente, esto se realizaba con cable coaxial. Aplicado a las LANs de hoy en día es un concepto obsoleto, sin embargo, cuando se aplica a otros tipos de redes como Token Ring o Interfaz de Datos Distribuidos por Fibra, toma un significado diferente: el de una topología lógica.

Figura 1-22

Topología de Anillo



Una topología lógica se refiere a cómo la información es realmente enviada de una computadora a la siguiente. Token Ring y FDDI utilizan un sistema de paso de token. En lugar de transmitir información a todas las computadoras en la red Ethernet que utilizan topología de estrella, las computadoras Token Ring y FDDI esperan a obtener el token. El token se pasa de computadora en computadora. Recogiendo información y dejándola caer si es necesario. La mayoría de estas redes tienen un token, pero es posible tener dos en redes más grandes. La ventaja más grande de esta topología es que las colisiones no son un factor. Una colisión es cuando dos computadoras intentan enviar

colisión de información que hace que ambas piezas de datos sean irrecuperables. En redes Ethernet, las colisiones de datos son comunes dada la idea del broadcasting. En los sistemas basados en token, hay por lo menos un elemento volando al rededor de la red a alta velocidad, así que no tiene nada con que colisionar. Las desventajas de esta implementación incluyen el costo y mantenimiento. Además, el switcheo Ethernet y otras tecnologías Ethernet pueden tener una gran cantidad de colisiones que fueron la perdición de los ingenieros de redes hace 10 o 15 años.

Aunque las redes FDDI utilizan topología de anillo lógica y físicamente, las redes Token Ring difieren. Una red Token Ring envía información lógicamente en modo de anillo, lo que significa que un token va a cada computadora, una a la vez y continúa en ciclos. Sin embargo, las computadoras token ring se conectan físicamente en forma de estrella. Es decir, todas las computadoras en una red Token Ring están conectadas a un dispositivo de conexión central conocido como ***Unidad de Acceso multi estación (MAU*** o ***MSAU)***. Hablaremos más sobre Token Rings en la Lección 2, "Definiendo redes con el Modelo OSI."