UNIVERSIDAD LASALLISTA BENAVENTE

ESCUELA DE INGENIERIA EN COMPUTACION

Con estudios incorporados a la
Universidad Nacional Autónoma de México
CLAVE: 8793-16

"CONFIGURACIÓN DE PC'S, LAN Y WAN PARA SERVICIOS DE ACCESO REMOTO"

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

PRESENTA:

Felipe Camargo Zamudio

Asesor: Ing. Maya Gicela Villagómez Torres

Celaya, Gto. **Mayo de 2007**

AGRADECIMIENTOS:

- ***A mis Papas:***
  Por haber confiado siempre en mi y apoyarme en cualquier momento.

- ***A mis Hermanos:***
  Por haberme apoyado siempre.

- ***A mi Novia:***
  Por apoyarme siempre.

INDICE

CAPÍTULO CUARTO

REDES DE COMUNICACIÓN

CAPÍTULO QUINTO

SEGURIDAD EN SERVIDORES DE ACCESO REMOTO

CAPÍTULO SEXTO

TERMINAL SERVER Y ESCRITORIO REMOTO PARA LA ADMINISTRACIÓN

CAPÍTULO SÉPTIMO

APLICACIÓN PARA ESTABLECER UNA CONEXIÓN REMOTA A UNA PC, LAN Y WAN Y SU GESTION REMOTA

INTRODUCCION

Las características de acceso remoto de la familia Microsoft Windows permiten a los usuarios móviles o remotos que utilizan vínculos de comunicaciones de acceso telefónico tener acceso a las redes corporativas como si estuvieran conectados directamente. El acceso remoto proporciona también servicios de red privada virtual (VPN), de forma que los usuarios pueden obtener acceso a las redes corporativas a través de Internet.

Si se configura Enrutamiento y acceso remoto para que actúe como un servidor de acceso remoto, se pueden conectar usuarios remotos o móviles a redes de organizaciones. Los usuarios con acceso remoto pueden trabajar como si sus equipos estuvieran conectados físicamente a la red.

Los usuarios ejecutan software de acceso remoto ya sea (Terminal Server o conexión a escritorio remoto) e inician una conexión con el servidor de acceso remoto. El servidor de acceso remoto, un servidor que ejecuta Enrutamiento y acceso remoto de Terminal Server , autentica sesiones de servicios y usuarios hasta que el administrador de redes o el usuario las termina. Todos los servicios que están habitualmente disponibles para un usuario conectado a una LAN (incluido el uso compartido de archivos e impresoras, el acceso al servidor Web y la mensajería) están habilitados por medio de la conexión de acceso remoto.

Los clientes de acceso remoto utilizan herramientas estándar para tener acceso a los recursos. Por ejemplo, en un servidor donde se ejecuta Enrutamiento y acceso remoto, los clientes pueden utilizar el Explorador de Windows para establecer conexiones a unidades y a impresoras. Las conexiones son persistentes: los usuarios no necesitan volver a conectarse a los recursos de la red durante sus sesiones remotas. Puesto que el acceso remoto admite por completo las letras de las unidades y la Convención de nomenclatura universal (UNC), la mayor parte de las aplicaciones comerciales y personalizadas funcionan sin necesidad de realizar ninguna modificación.

Un servidor que ejecuta Enrutamiento y acceso remoto ofrece dos tipos distintos de conectividad de acceso remoto:

1. Acceso telefónico a redes

El acceso telefónico a redes es una conexión de acceso telefónico no permanente, realizada por un cliente de acceso remoto, a un puerto físico de un servidor de acceso remoto mediante el servicio de un proveedor de telecomunicaciones como un teléfono analógico, ISDN (RDSI) o X.25. El mejor ejemplo de un acceso telefónico a redes es el de un cliente de acceso telefónico a redes que marca el número de teléfono de uno de los puertos de un servidor de acceso remoto.

Un acceso telefónico a redes a través de un teléfono analógico o ISDN (RDSI) es una conexión física directa entre el cliente y el servidor de acceso telefónico a redes. Puede cifrar los datos enviados a través de la conexión, pero no es necesario.

2. Redes privadas virtuales

La interconexión de redes privadas virtuales es la creación de conexiones seguras de punto a punto a través de una red privada o una red pública como Internet. Un cliente de rede privada virtual utiliza protocolos especiales basados en TCP/IP, denominados protocolos de túnel, para realizar una llamada virtual a un puerto virtual de un servidor de red privada virtual. El mejor ejemplo de red privada virtual es el cliente de red privada virtual que establece una conexión de red privada virtual a un servidor de acceso remoto conectado a Internet. El servidor de acceso remoto responde a la llamada virtual, autentica al que llama y transfiere datos entre el cliente de la red privada virtual y la red corporativa.

A diferencia del acceso telefónico a redes, la red privada virtual siempre es una conexión lógica e indirecta entre el cliente y el servidor de red privada virtual a través de una red pública como Internet. Para garantizar la privacidad, debe cifrar los datos enviados a través de la conexión.

CAPÍTULO PRIMERO

ANTECEDENTES

EVOLUCIÓN DE LAS REDES

En los 70 aparecen redes de acceso múltiple. Los nodos de la red comparten un canal común Ejemplos: ethernet, token ring, Aloha .Influencia de las redes de telefonía; Módems: transferencia de hasta 56 Kbps. RDSI: dos canales de 64 Kbps y uno de control de 16 Kbps, ADSL: hasta 2 Mbps de bajada

1.1CONCEPTOS BÁSICOS

Mainframe: Pc de gran capacidad de procesamiento, potente y costoso usado principalmente por una gran compañía para el procesamiento de una gran cantidad de datos; por ejemplo, para el procesamiento de transacciones bancarias.

Terminal: Dispositivo para dialogar con una pc. Puede ser local o remoto. Controlador de comunicación es: pc dedicada a comunicaciones Multiplexores, concentradores.

UNC: Convención de Nomenclatura Universal.

UTP: (Unshielded Twisted Pair) Par Trenzado Sin Apantallar, par trenzado sin blindar.

ISDN(RDSI) ó x.25: Red Digital de Servicios Integrados (RDSI o ISDN en inglés) es una red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados. Es una tecnología que utiliza la línea telefónica.

VPN: Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

Ras: Servicio de Acceso Remoto.

Terminal Server: Servidor Terminal. Una computadora específica que permite conectar varios módems y/o una conexión a una red de otro lado.

IPsec: (La abreviatura de Internet Protocol security) es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo.

Frame Relay: Se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2.048 Mbps. Trabaja en el nivel de enlace de datos del modelo OSI, aunque también posee funcionalidad de nivel de red. Es utilizado para conectar distintas LANs entre si de una manera rapida y eficiente.

ATM: Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Broadcast: (O en castellano "difusiones"), se producen cuando una fuente envía datos a todos los dispositivos de una red.

En la tecnología Ethernet el broadcast se realiza enviando tramas con dirección MAC de destino FF.FF.FF.FF.FF.FF.

En el protocolo IP se realiza enviando datos a una dirección de difusión, aquella dirección IP que tiene todos y cada uno de los bits de host con valor 1. Cuando se envían datos a esta dirección de difusión IP éstos son recibidos por todos los nodos.

MMDS: Servicio de Distribución Multicanal Multipunto o Mutichannel Multipoint Distribution Service utiliza tecnología inalámbrica para distribuir servicios de video/televisión sobre frecuencias de microondas en la banda de 2.600 a 2700 MHz.

Bluetooth: Es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos - Eliminar cables y conectores entre éstos.

Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales

El sistema de transmisión no es un medio sólido, tienen un gran auge en la ciudad PC's portátiles, teléfonos móviles, redes LAN inalámbricas. La tecnología empleada para estas redes son: Wavelan (IEEE 802.11),GSM, GPRS, UMTS, BlueTooth.

1.2 COMUNICACIÓN

Una red de comunicación es un conjunto de dispositivos hardware y software que permiten al usuario intercambiar información, es Conjunto de nodos interconectados para permitir el intercambio de información. En las figuras 1.1, 1.2 y 1.3 se muestran algunos modelos de comunicación.

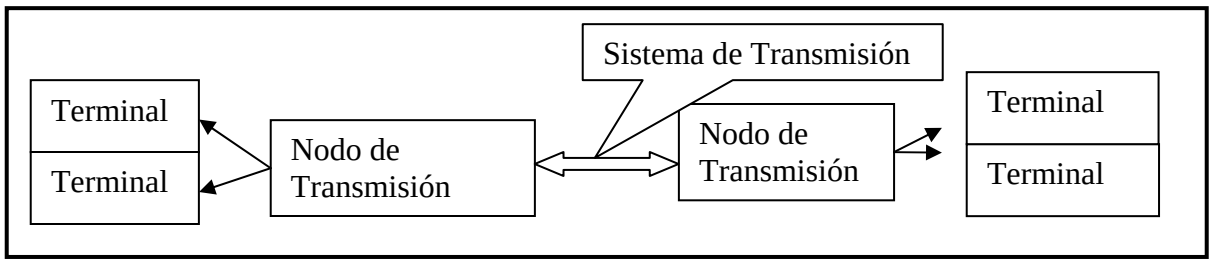


Fig. Num. 1.1

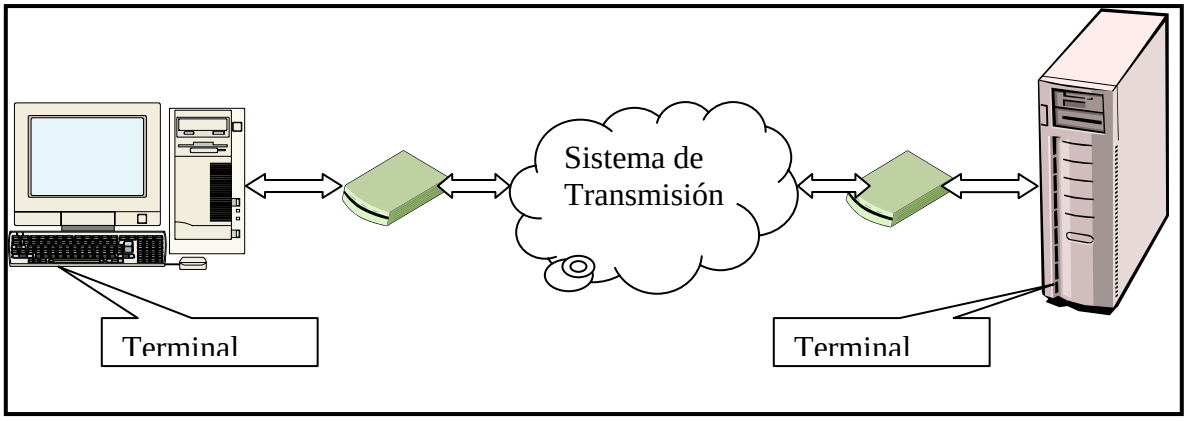


Fig. Num. 1.2

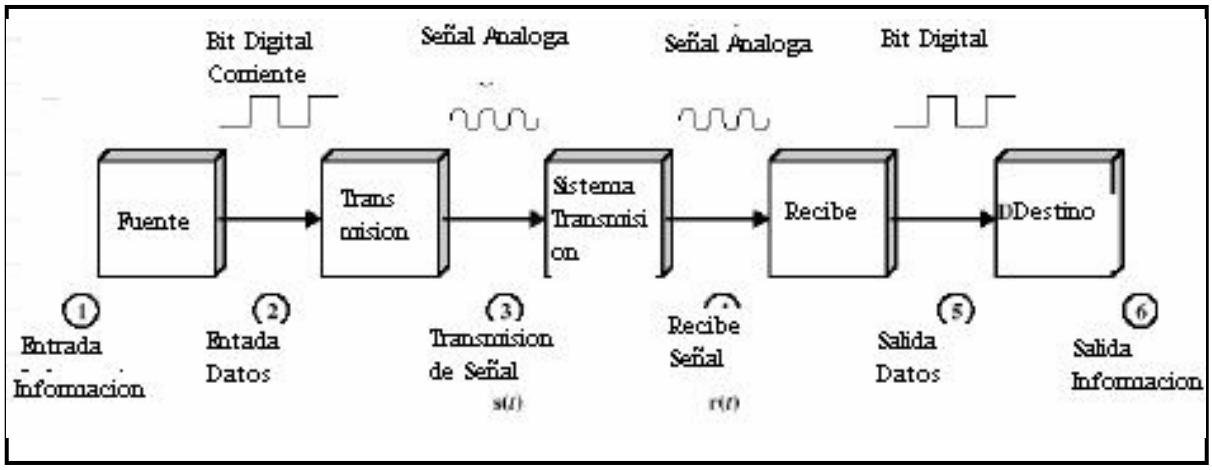


Fig. Num. 1.3

1.3 COMUNICACIÓN ENTRE EQUIPOS

La comunicación entre equipos puede ser de las siguientes formas:

A) Comunicación de dos PC's a través del puerto paralelo. Cuando se realiza una conexión directa entre dos PC's, la solución más simple, desde el punto de vista técnico y económico, es la conexión directa mediante un cable. Para ello puede emplearse un puerto serie o un puerto paralelo y un cable de conexión especial.

B) Comunicación de dos PC's a través de un cable Ethernet cruzado[1]. Es posible conectar directamente dos PC's empleando un cable Ethernet cruzado (los hilos están conectado de forma diferente que en el cable habitual). [2]

C) Desconectar los cables de red de los dos PC's (cliente y la PC servidor) y conectarlos a través del cable cruzado. Si el cable es correcto, verá como se encienden los LEDs de las dos tarjetas de red.

D) Haga un "ping" desde una de las PC's al otro y compruebe que la conexión es correcta.

E) Conéctese desde la PC multimedia a los recursos compartidos de la PC inestable. Verá como puede acceder a la carpeta documentos compartidos del equipo servidor.

F) Compartición de una conexión de red. En muchas ocasiones, es necesario conectar a Internet todos los equipos de una pequeña empresa o de un laboratorio, pero sólo uno de ellos dispone de una conexión apropiada. Windows Xp proporciona herramientas sencillas que permiten compartir la conexión a Internet de un equipo con otros de su misma subred de forma sencilla.

G) Apagar y desconectar de la red eléctrica el equipo, e instalar en él una tarjeta de red adicional. Arrancar de nuevo el equipo y conectar el cable cruzado, a la tarjeta de red del equipo

H) Configurar la tarjeta recién instalada en el equipo (denominada Conexión de área local 2) con la dirección IP 192.168.0.1, la máscara de subred 255.255.255.0 y dejar en blanco la puerta de enlace predeterminada. Configurar (apuntar previamente la configuración antigua) la red del equipo de

[1] En el capítulo cuarto se muestra como configurar un cable cruzado y preparar una red
[2] http://www.lcc.uma.es/~antonio/Ficheros/Docencia/id/Tema%201/ID.%20Tema%201.1T.pdf

forma que tenga la dirección IP 192.168.0.2, la máscara de subred 255.255.255.0 y configurar el equipo servidor como su puerta de enlace predeterminada.

I) Hacer un ping a otro equipo empleando su dirección física, por ejemplo, el equipo 156.35.151.120.

J) Para tratar de averiguar lo que ocurre, ejecute desde una interfaz de comandos la utilidad *"tracert.exe"* usando como destino la dirección anterior. Esto permitirá ver la ruta seguida hasta llegar al equipo destino.

K) Configurar la conexión a la red del laboratorio del equipo (la primera conexión de área local), activando la opción Habilitar conexión compartida a Internet para esta conexión.

CAPÍTULO SEGUNDO

LÍNEAS DE TRANSMISIÓN

2.1 LÍNEAS DE TRANSMISIÓN

Al nivel más bajo todas las comunicaciones de computadora comprenden la codificación de datos en una forma de energía y el envío de esa energía por un medio de transmisión. Por ejemplo, puede usarse corriente eléctrica para transferir datos por un alambre, u ondas magnéticas para transportar datos por el aire. Dado que los dispositivos de hardware conectados a una computadora se encargan de la codificación y la descodificación de datos, los programadores y usuarios no necesitan conocer los detalles de la transmisión. Sin embargo, ya que una función importante de software de comunicación es el manejo de errores y de fallas que se presentan en el hardware, entender tal software requiere del conocimiento de algunos conceptos básicos de transmisión de datos.

Algunos ejemplos de medios de transmisión:

A) Alambres de cobre. Las redes de cómputo convencionales usan alambres como medio primario de conexión dado que es un material barato y fácil de instalar. Aunque los alambres pueden fabricarse de varios metales, muchas redes utilizan cobre, debido a que su baja resistencia a la corriente eléctrica significa que las señales pueden viajar más lejos. El alambrado en las redes de cómputo se selecciona para reducir al mínimo la interferencia que se presenta por una señal eléctrica que viaja por un alambre y actúa como una estación de radio en miniatura.

El alambre emite una pequeña cantidad de energía electromagnética que puede viajar por el aire. Es más, cuando encuentra otro alambre, la onda electromagnética genera una pequeña corriente eléctrica. La cantidad de corriente

generada depende de la fuerza de la onda electromagnética y de la posición física del alambre. Por lo general, los alambres no se acercan lo suficiente para generar un problema de interferencia. Por ejemplo, si dos alambres se acercan a un ángulo recto y pasa una señal por medio de ellos, la corriente generada en el otro casi es indetectable. Sin embargo, al colocarse dos alambres cercanos y en paralelo, una señal intensa enviada por uno de ellos generará una señal similar en el otro ya que las computadoras no pueden distinguir entre las señales generadas de manera accidental y en las de transmisión normal la corriente generada puede ser bastante intensa como para alterar o evitar la comunicación normal. Por desgracia el problema de la interferencia es grave, pues los alambres que componen una red de datos con frecuencia se colocan paralelos a muchos otros alambres. Por ejemplo, como los alambres de una computadora pueden estar juntos a los de otras computadoras o de otras redes.

Para producir al mínimo la interferencia, las redes usan dos tipos básicos de alambrado que son:

- Par trenzado[3]
- Cable coaxial

El término se deriva de que cada alambre se recubre de un material aislante (por ejemplo, plástico) y se trenza con otro alambre igual, como se muestra en la Fig. Num 2.1 en la siguiente paguina.

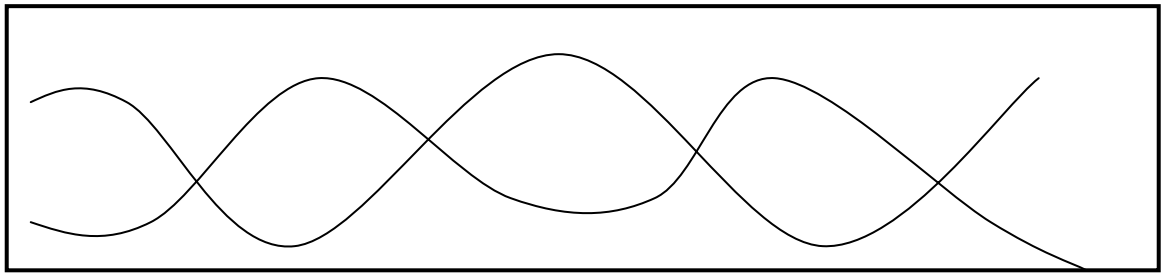


Fig. Num 2.1

[3] El alambrado de par trenzado también se utiliza en el sistema telefónico.

el simple trenzado cambia las propiedades eléctricas del alambre y ayuda a hacer lo adecuado para las redes. Primero, como limita la energía electromagnética emitida por el alambre, el trenzado evita que las corrientes eléctricas irradien energía que podría interferir con otros alambres.

Segundo, puesto que hace que el par de alambres sea menos susceptible a la energía electromagnética, el trenzado evita que las señales de otros alambres interfieran con el par.

El segundo tipo de alambrado de cobre que se usa en las redes es el cable coaxial, el mismo tipo de alambrado empleado para la televisión por cable. El coaxial da mayor protección contra interferencias que el par trenzado. En lugar de trenzar cables para limitarla, el cable coaxial consiste en un alambre rodeado de un blindaje de un metal más grueso como se muestra en la Fig. Num.2.2

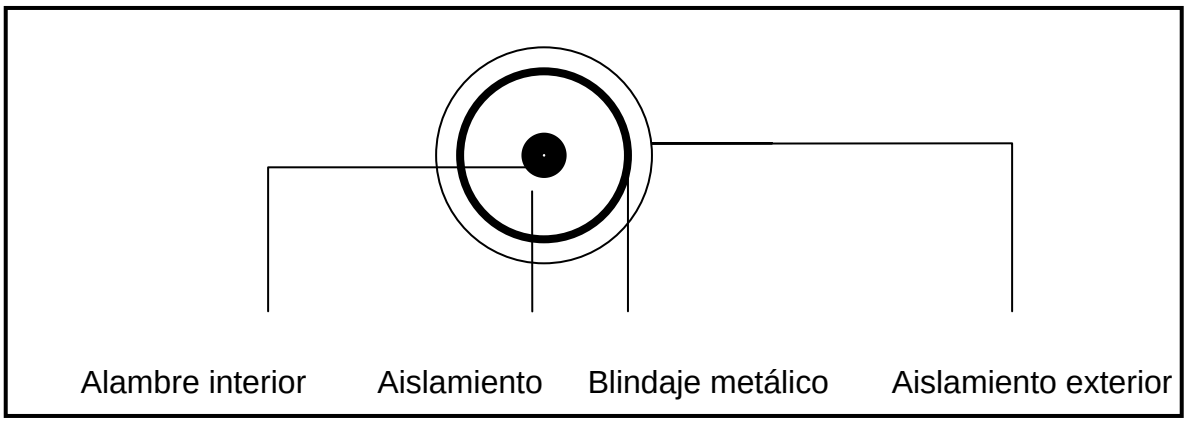


Fig. Num. 2.2

El blindaje del cable coaxial es cilíndrico metálico flexible alrededor del alambre interior que forma una barrera contra la radiación electromagnética. La barrera aísla el alambre interior de dos maneras: lo protege de la energía electromagnética entrante que causaría interferencia y evita que las señales del alambre interior irradien energía electromagnética que podría afectar a otros alambres. Ya que rodea de manera uniforme el alambre central, el blindaje del cable coaxial es muy efectivo. El cable puede colocarse en paralelo con otros cables o doblarse en las esquinas. El blindaje siempre se queda en su lugar.

El concepto de blindaje para proteger los alambres también se ha aplicado al par trenzado. El cable de par trenzado blindado consiste de un par de alambres rodeados de un blindaje metálico. Cada alambre se recubre con material aislante, de modo que el metal de un alambre no toque el del otro; el blindaje simplemente forma un abarrera que evita la entrada o salida de radiación electromagnética. El blindaje adicional que brinda el cable coaxial o el par trenzado blindado se usa con frecuencia cuando los alambres de una red pasan cerca del equipo que genera fuertes campos magnéticos o electromagnéticos (por ejemplo, un equipo de aire acondicionado).

B) Fibras de vidrio. Las redes también utilizan fibra de vidrio delgada para la transmisión de datos, conocida como fibra óptica, el medio usa luz para transportar los datos. La fibra de vidrio en miniatura se encapsula en un forro de plástico que permite doblarla sin romperla. El transmisor de un extremo de la fibra emplea un diodo emisor de luz (LED) o un láser para enviar pulsos de luz por ella. El receptor del otro extremo tiene un transistor sensible a la luz para detectar los pulsos. Las fibras ópticas tienen cuatro ventajas principales sobre los alambres. Primero, como usan luz no pueden provocar interferencia eléctrica en otros cables ni son susceptibles a ella. Segundo, dado que la fibra de vidrio se fabrica para reflejar hacia el interior casi toda la luz, las fibras pueden transportar los pulsos luminosos a mayor distancia que los alambres las señales. Tercero, dado que la luz puede codificar más información que las señales eléctricas, la fibra óptica puede cargar más información que los alambres. Cuarto, a diferencia de la electricidad que siempre requiere un par de alambres para completar el circuito, la luz puede viajar entre computadoras a lo largo de una sola fibra.

A pesar de sus ventajas, la fibra óptica tiene unos inconvenientes que son los siguientes:

1.- Su instalación requiere equipo especial para pulir los extremos y permitir el paso de luz.

2.- Si la fibra se rompe dentro del forro de plástico (al doblarse en ángulo recto), resultará difícil la localización del problema.

3.- La reparación de la fibra rota se dificulta debido a la necesidad de equipo especial para empalmar las fibras de modo que pueda pasar la luz por medio de la unión.

4.- La fibra óptica en la implantación de una red resulta ser de un costo más elevado.

C) Radio. Además de su uso en la difusión pública de programas de radio y televisión y en la comunicación privada mediante teléfonos portátiles y otros dispositivos, la radiación electromagnética puede servir para la transmisión de datos. Informalmente, se dice que una red que se vale de ondas electromagnéticas de radio opera a una radiofrecuencia y la transmisión se conoce como transmisión de RF. A diferencia de las redes que emplean alambre o fibra óptica, las redes que usan transmisión de RF no requieren una conexión física directa entre las computadoras, sino que cada computadora se conecta a una antena que puede transmitir y recibir RF.

En cuanto a su tamaño las antenas utilizadas en las redes de RF pueden ser grandes o pequeñas dependiendo de la esfera de acción deseada. Ejemplo, una antena diseñada para propagar señales a varios kilómetros, de lado a lado de la ciudad puede consistir en un poste metálico de unos dos metros montado verticalmente sobre un edificio. Una antena para comunicación dentro de un edificio puede ser lo bastante pequeña para caber en una computadora portátil. Como se muestra en la Fig. Num 2.3[4]

[4] Aunque las transmisiones de radio no siguen la curvatura de la superficie terrestre, la tecnología de RF puede combinarse con satélites para comunicar entre grandes distancias.

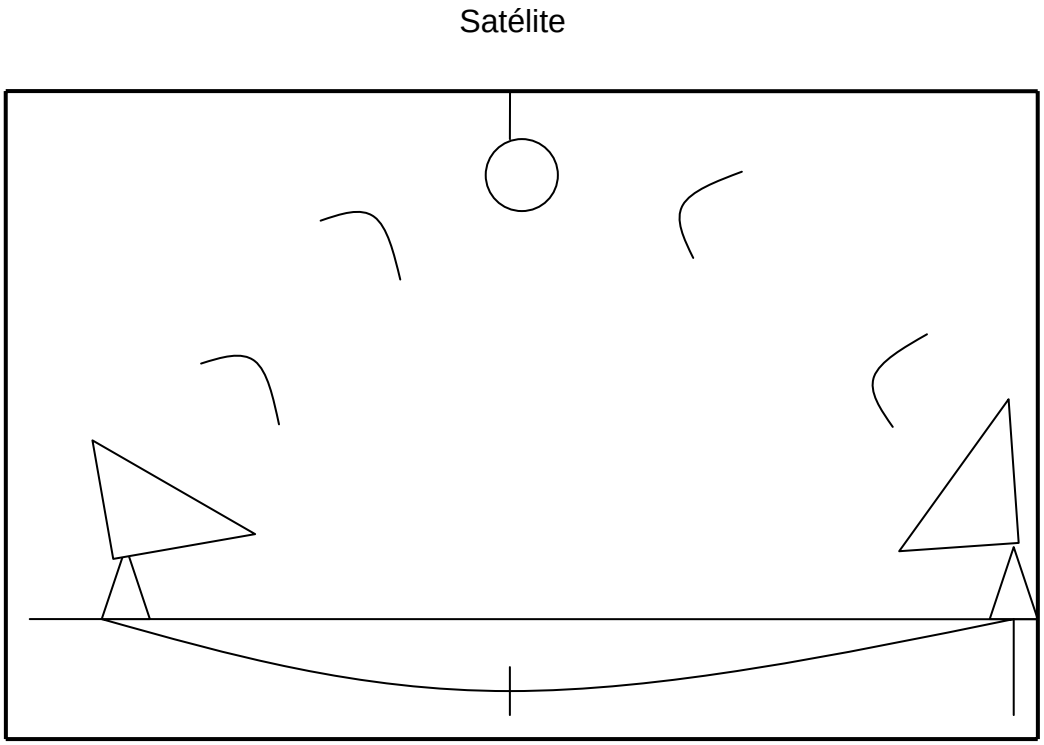


Fig. Num. 2.3

Figura 2.3. Ilustración del uso de un satélite para establecer comunicaciones de un lado al otro del océano. El satélite recibe las señales de radio de una estación de tierra y las retransmite a otra.

Aunque las microondas simplemente son una versión de mayor frecuencia de las ondas de radio, su comportamiento es diferente. En lugar de difundirse en todas las direcciones, la transmisión de microondas puede dirigirse, lo que impide que otros intercepten la señal. Además, la transmisión de microondas puede transportar más información que las transmisiones de RF. Sin embargo, ya que las microondas no pueden penetrar estructuras metálicas, esta transmisión funciona mejor si hay una trayectoria libre entre el transmisor y un receptor. Como resultado, la mayor parte de las estaciones de microondas consta de dos torres más altas de los edificios y la vegetación circundantes, ambas con un transmisor de microondas dirigido directamente al receptor de la otra.

D) Infrarrojo. Los controles remotos inalámbricos que usan los aparatos televisores y de estéreo se comunican mediante transmisión infrarroja. El infrarrojo se limita a un área pequeña (ejemplo, una habitación), generalmente requiere apuntar el transmisor al receptor. El hardware del infrarrojo es económico en comparación con otros mecanismos y no requiere una antena.

Las redes pueden usar tecnología infrarroja para la comunicación de datos. Ejemplo, es posible equipar un departamento grande con una conexión infrarroja que permita acceso de red a todas las computadoras del departamento.

E) Láser. Ya se ha mencionado que la luz puede utilizarse para la comunicación por medio de fibra óptica. También puede usarse un haz de luz para conducir datos por el aire. Al igual que el sistema de comunicación por microondas, el enlace que emplee la luz conste en dos instalaciones con transmisor y receptor. El equipo se monta en posición fija, frecuentemente en torres, y se alinea de manera que el transmisor de una localidad envíe su haz de luz al receptor de la otra. El transmisor usa un láser para generar el haz de luz, pues un haz láser se mantiene enfocado a grandes distancias. Como viaja en línea recta, por lo tanto no debe tener obstáculos al igual que la transmisión de microondas. Por desgracia, el haz del láser no puede penetrar la vegetación ni la nieve, neblina y condiciones ambientales similares.

2.2 TIPOS DE LÍNEAS DE CONEXIÓN

Existen dos tipos básicos de líneas de conexión para conectar dispositivos de comunicaciones, estas conexiones se hacen por medio de líneas arrendadas, conmutadas.

Líneas arrendadas. Una línea arrendada (leased line), también llamada comúnmente línea privada o dedicada, se obtiene de una compañía de comunicaciones para proveer un medio de comunicación entre dos instalaciones que pueden estar en edificios separados en una misma ciudad o en ciudades distantes. Aparte de un cobro por la instalación o contratación [pago único], la

compañía proveedora de servicios le cobrará al usuario un pago mensual por uso de la línea, el cual se basará en la distancia entre las localidades conectadas.

Este tipo de líneas tienen gran uso cuando se requiere cursar:

- Una cantidad enorme de tráfico
- Cuando este tráfico es continúo.
- Es muy utilizado este tipo de líneas por bancos, industrias, instituciones académicas, etc.

Las ventajas de las líneas arrendadas son:

- Existe un gran ancho de banda disponible (desde 64 Kbps hasta decenas de Mbps)
- Ofrecen mucha privacidad a la información
- La cuota mensual es fija, aún cuando está se sobreutilize.
- La línea es dedicada las 24 hrs.
- No se requiere marcar ningún número telefónico para lograr el acceso.

Las desventajas:

- El costo mensual es relativamente costoso.
- No todas las áreas están cableadas con este tipo de líneas.
- Se necesita una línea privada para cada punto que se requiera interconectar.
- El costo mensual dependerá de la distancia entre cada punto a interconectar.

Este tipo de líneas son proporcionadas por cualquier compañía de comunicaciones; los costos involucrados incluyen un contrato inicial, el costo de los equipos terminales (DTU, Data Terminal Unit) y de una mensualidad fija.

Líneas conmutadas. Una línea conmutada (switch o dial-up line) permite la comunicación con todas las partes que tengan acceso a la red telefónica pública conmutada (e.g. TELNOR, TELMEX, Alestra (AT&T), Avantel(MCI), etc.). Si el operador de un dispositivo terminal quiere acceso a una computadora, éste debe marcar el número de algún teléfono a través de un modem. Al usar transmisiones por este tipo de líneas, las centrales de conmutación de la compañía telefónica establecen la conexión entre el llamante y la parte marcada para que se lleve a cabo la comunicación entre ambas partes. Una vez que concluye la comunicación, la central desconecta la trayectoria que fue establecida para la conexión y reestablece todas las trayectorias usadas tal que queden libres para otras conexiones.

Este tipo de líneas tienen gran uso cuando se requiere cursar:

- Una cantidad pequeña de tráfico y
- Cuando éste tráfico es esporádico.

Es muy utilizada este tipo de líneas por bancos, industrias, instituciones académicas, y usuarios en general, etc.

Las ventajas de las líneas conmutadas:

- La comunicación con este tipo de líneas es muy amplia debido a que existen mundialmente más de 600 millones de subscriptores.
- El costo de contratación es relativamente barato.
- No se necesita ningún equipo especial, solo un modem y una computadora.
- El costo depende del tiempo que se use (tiempo medido), el numero de llamadas y de la larga distancia.

Las desventajas:

- No ofrecen mucha privacidad a la información.

- Se requiere marcar un número telefónico para lograr el acceso.
- La comunicación se puede interrumpir en cualquier momento.
- El ancho de banda es limitado (en el orden de Kbps)
- La conexión entre ambas depende de que la parte marcada no esté ocupada su línea y también de que el número de circuitos tanto para la comunicación local como nacional sean los suficientes.

Este tipo de líneas también se contrata ante una compañía telefónica, los incluyen una contratación de la línea el costo dependerá si ésta línea es residencial o comercial, una pequeña renta mensual y el servicio medido, más los costos de la larga distancia, en caso de que se utilice.

2.3 MODOS DE TRANSMISIÓN

Un método de caracterizar líneas, dispositivos terminales, computadoras y módems es por su modo de transmisión o de comunicación. Las tres clases de modos de transmisión son simplex, half-duplex y full-duplex.

2.3.1 Transmisión Simplex. La transmisión simplex o unidireccional es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción humano-máquina. La transmisión de datos se produce en un solo sentido, siempre existen un nodo emisor y un nodo receptor que no cambian sus funciones.

Ejemplos de transmisión simplex son: La radiodifusión (broadcast) de TV y radio, el paging unidireccional, etc.

En la sig pagina, La Fig. Num. 2.4 muestra una transmisión simplex.

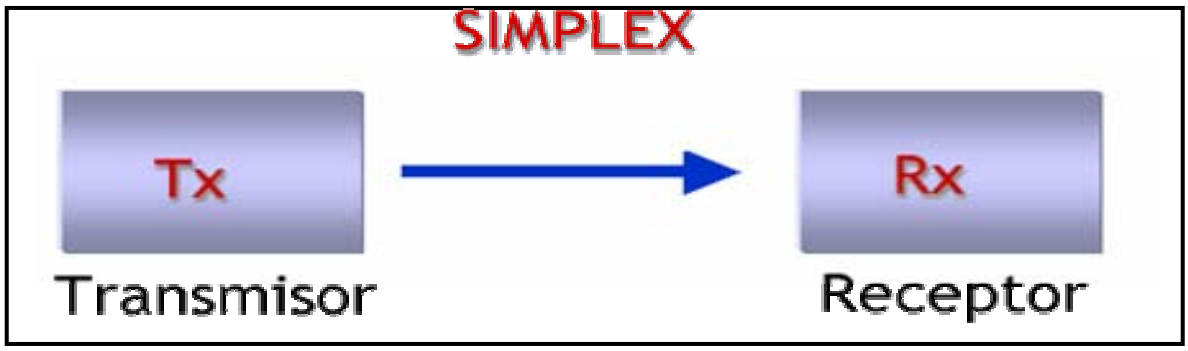


Fig. Num 2.4

2.3.2 Transmisión Half-Duplex. La transmisión half-duplex permite transmitir en ambas direcciones; sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez, Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo típico de half-duplex es el radio de banda civil donde el operador puede transmitir o recibir, pero no puede realizar ambas funciones simultáneamente por el mismo canal. Cuando el operador ha completado la transmisión, la otra parte debe ser avisada que puede empezar a transmitir, observe la Fig. Num. 2.5.

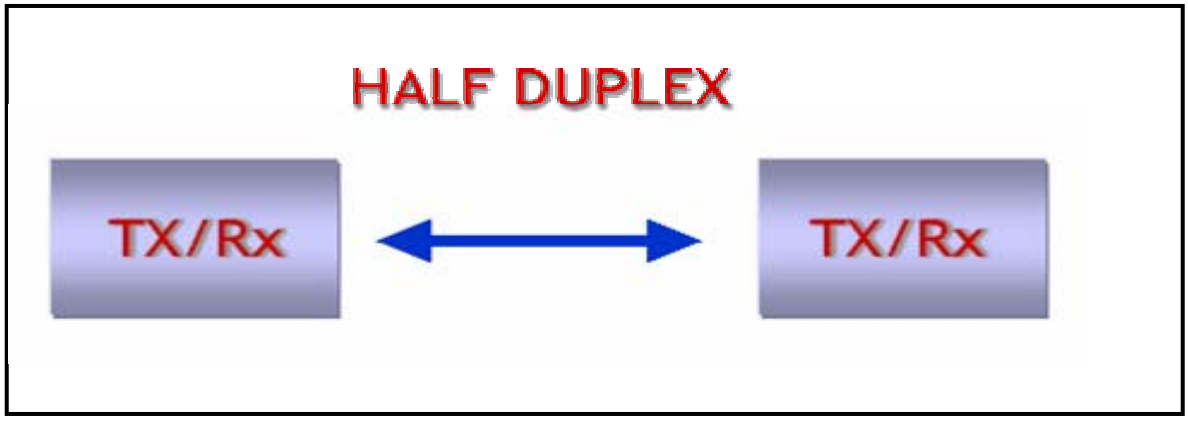


Fig. Num. 2.5

2.3.3 Transmisión Full-Duplex. La transmisión full-duplex permite transmitir en ambas dirección, simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir. Ejemplos de este tipo abundan en el terreno de las telecomunicaciones, el caso más típico es la telefonía, donde el transmisor y el receptor se comunican simultáneamente utilizando el mismo canal, pero usando dos frecuencias. Fig. Num 2.6

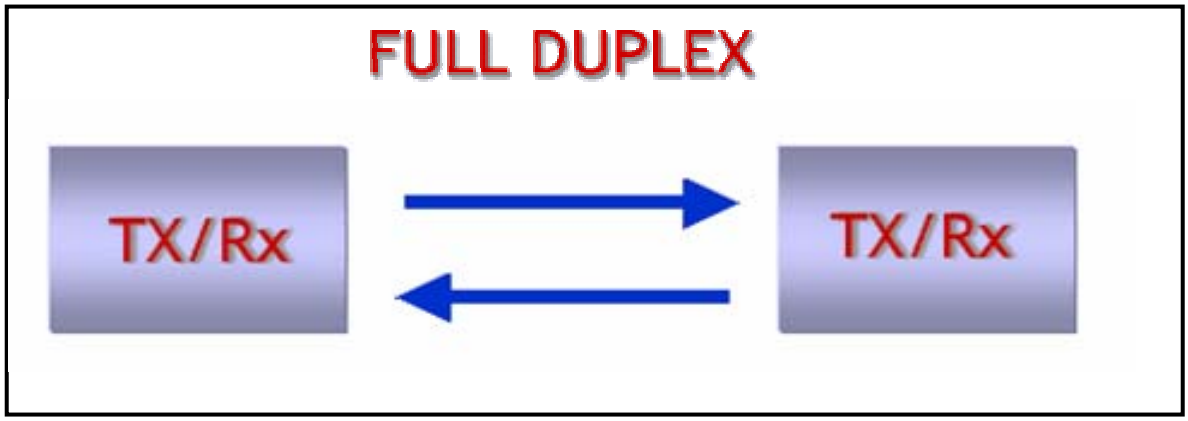


Fig. Num 2.6[5]

2.4 TÉCNICAS DE TRANSMISIÓN

2.4.1 Transmisión Asíncrona. La transmisión asíncrona es aquella que se transmite o se recibe un carácter, bit por bit añadiéndole bits de inicio, y bits que indican el término de un paquete de datos, para separar así los paquetes que se van enviando/recibiendo para sincronizar el receptor con el transmisor. El bit de inicio le indica al dispositivo receptor que sigue un caracter de datos; similarmente el bit de término indica que el caracter o paquete ha sido completado. Se muestra en la Fig. Num 2.7.

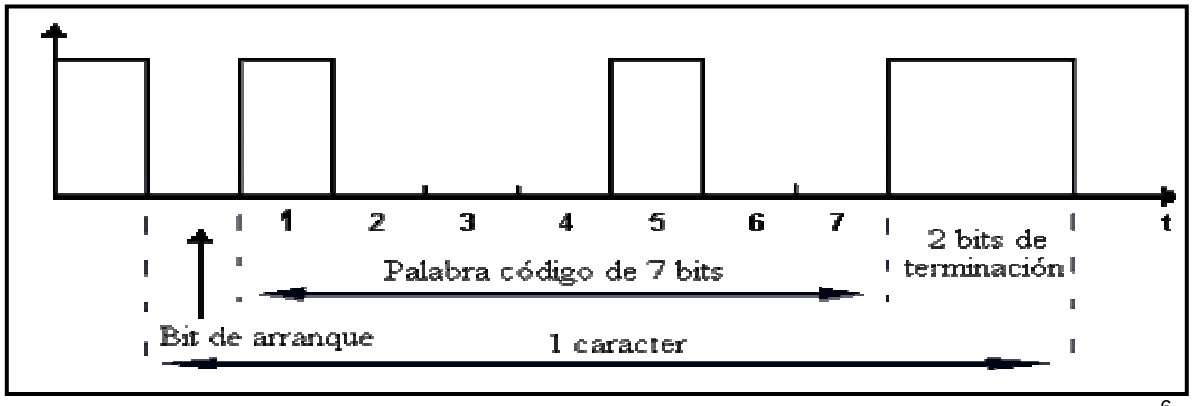


Fig. Num. 2.7[6]

Algunas de las características de la transmisión asíncrona son:

[5] Ejem. Un teléfono local
[6] Fuente: http://es.wikipedia.org/wiki/Transmisi%C3%B3n_as%C3%ADncrona

- Los equipos terminales que funcionan en modo asíncrono, se denominan también "terminales en modo carácter".

- La transmisión asíncrona también se le denomina arrítmica o de "start-stop".

La transmisión asíncrona es usada en velocidades de modulación de hasta 1,200 baudios.

El rendimiento de usar un bit de arranque y dos de parada, en una señal que use código de 7 bits más uno de paridad (8 bits sobre 11 transmitidos) es del 72 por 100.

Ventajas y desventajas del modo asíncrono:

- En caso de errores se pierde siempre una cantidad pequeña de caracteres, pues éstos se sincronizan y se transmiten de uno en uno.

- Bajo rendimiento de transmisión, dada la proporción de bits útiles y de bits de sincronismo, que hay que transmitir por cada carácter.

- Es un procedimiento que permite el uso de equipamiento más económico y de tecnología menos sofisticada.

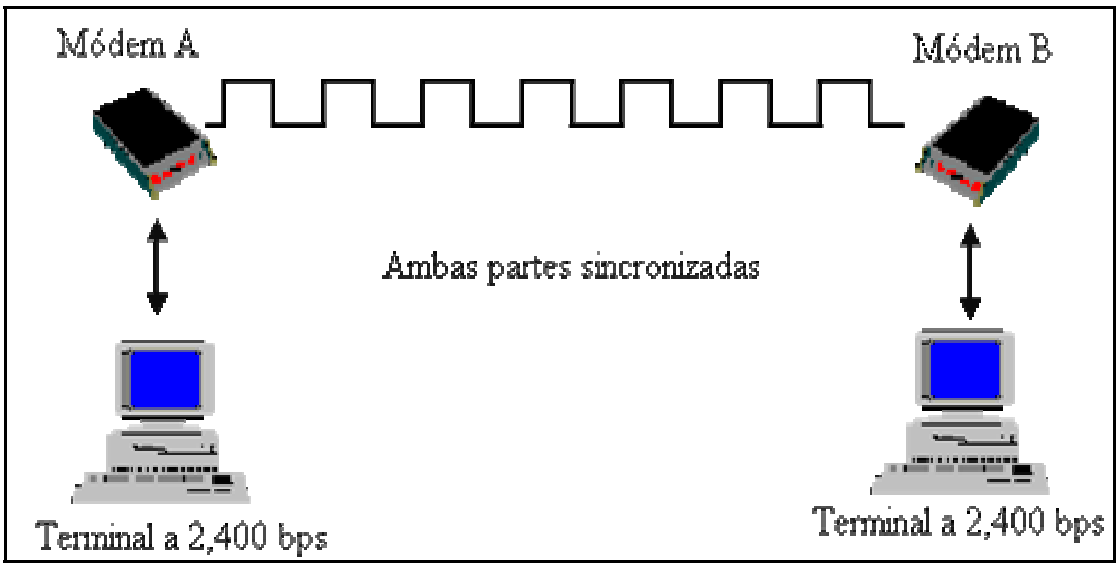
- Se adecua más fácilmente en aplicaciones, donde el flujo transmitido es más irregular.

- Son especialmente aptos, cuando no se necesitan lograr altas velocidades.

2.4.2 Transmisión Síncrona. Este tipo de transmisión el envío de un grupo de caracteres en un flujo continuo de bits. Para lograr la sincronización de ambos dispositivos (receptor y transmisor) ambos dispositivos proveen una señal de reloj que se usa para establecer la velocidad de transmisión de datos y para habilitar los dispositivos conectados a los módems para identificar los caracteres apropiados mientras estos son transmitidos o recibidos. Antes de iniciar la comunicación ambos dispositivos deben de establecer una sincronización entre

ellos. Para esto, antes de enviar los datos se envían un grupo de caracteres especiales de sincronía. Una vez que se logra la sincronía, se pueden empezar a transmitir datos.

En la Fig. Num. 2.8 se muestra la transmisión sincronía;



Transmisión Síncrona. Fig Num 2.8

Algunas de las características de la transmisión síncrona son:

- Los bloques a ser transmitidos tienen un tamaño que oscila entre 128 y 1,024 bytes.
- La señal de sincronismo en el extremo fuente, puede ser generada por el equipo terminal de datos o por el módem.
- El rendimiento de la transmisión síncrona, cuando se transmiten bloques de 1,024 bytes y se usan no más de 10 bytes de cabecera y terminación, supera el 99 %.

Ventajas y desventajas de la transmisión síncrona:

- Posee un alto rendimiento en la transmisión.

- Los equipamientos necesarios son de tecnología más completa y de costos más altos.

- Son especialmente aptos para ser usados en transmisiones de altas velocidades (iguales o mayores a 1,200 baudios de velocidad de modulación).

- El flujo de datos es más regular.

2.5 TIPOS DE CONEXIÓN

La distribución geográfica de dispositivos terminales y la distancia entre cada dispositivo y el dispositivo al que se transmite son parámetros importantes que deben ser considerados cuando se desarrolla la configuración de una red. Los dos tipos de conexiones utilizados en redes son punto a punto[7] y multipunto.

Las líneas de conexión que solo conectan dos puntos son punto a punto. Cuando dos o más localidades terminales comparten porciones de una línea común, la línea es multipunto. Aunque no es posible que dos dispositivos en una de estas líneas transmita al mismo tiempo, dos o más dispositivos pueden recibir un mensaje al mismo tiempo. En algunos sistemas una dirección de difusión (broadcast) permite a todos los dispositivos conectados a la misma línea multipunto recibir un mensaje al mismo tiempo. Cuando se emplean líneas multipunto, se pueden reducir los costos globales puesto que porciones comunes de la línea son compartidos para uso de todos los dispositivos conectados a la línea. Para prevenir que los datos transmitidos de un dispositivo interfieran con los datos transmitidos por otro, se debe establecer una disciplina o control sobre el enlace.

[7] Ver Fig. Num. 2.9

Cuando se diseña una red local de datos se pueden mezclar tanto líneas punto a punto como multipunto observe la Fig. Num. 2.9 , y la transmisión se puede efectuar en modo simplex, half-duplex o full-duplex.[8]

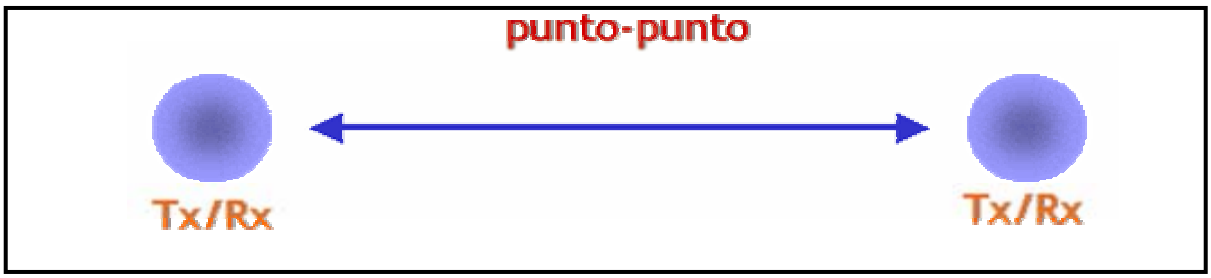


Fig. Num. 2.9

2.5.1 El radio modem. Cualquier tipo de módem (MOdulador/DEModulador) se encarga de convertir un flujo de datos digitales banda base en una señal analógica apropiada para ser transmitida sobre el medio, y viceversa. La principal diferencia entre un radio módem y un módem de cable se refiere a la aplicación a la que se destina. De este modo, los módems de cable están preparados para conectarse a redes de cable como pueda ser la red telefónica conmutada. Por su parte, los radio módems están destinados a aplicaciones en las cuales sea necesario transmitir la señal vía radio, como por ejemplo interconexión de ordenadores a través de LAN o MAN inalámbricas, sistemas MMDS (Servicio de Distribución Multicanal Multipunto), envío y recepción de mensajes o faxes a través de GSM, (Sistema Global para las comunicaciones Móviles), localización automática de vehículos, vending, etc. En la Fig. Num. 2.10 (Sig. Pág.), se muestra una aplicación típica de acceso a Internet a través del sistema MMDS.

[8] Fuente: www.eveliux.com/fundatel/linconex.html

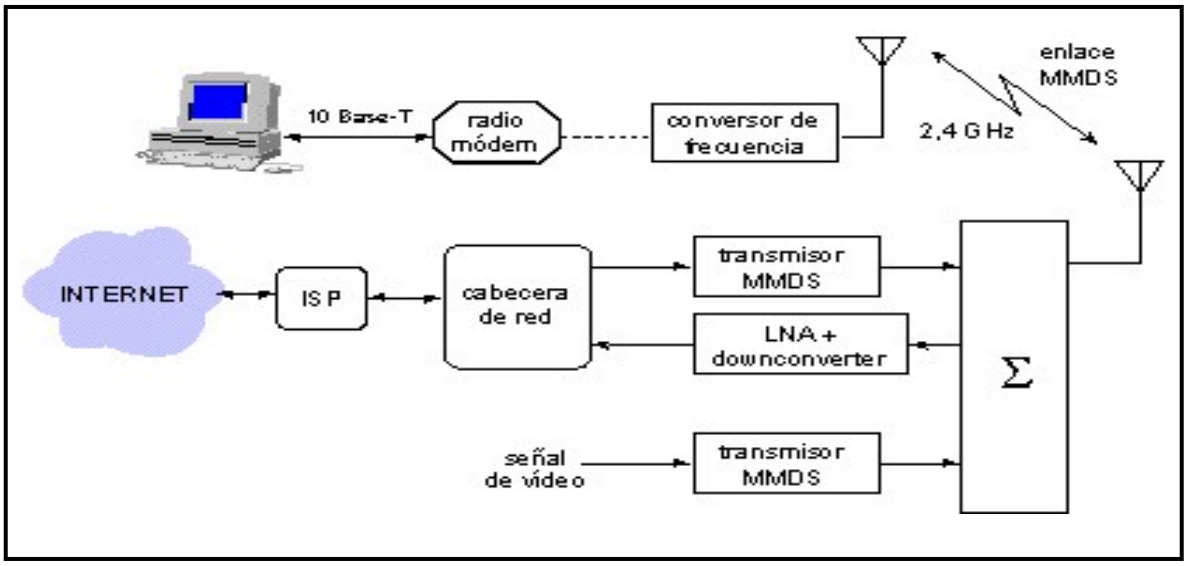


Fig. Num. 2.10

Así pues, los radio módems deben estar preparados para transmitir sobre un entorno más hostil que el cable, a menudo sujeto a desvanecimientos, propagación multicamino (multipath) o interferencias. Esto obliga a emplear mecanismos de modulación distintos a los empleados en los módems de cable. Al mismo tiempo, dado que en algunos casos es necesario dotar de movilidad al dispositivo, aparecen nuevos problemas como el tamaño o la autonomía del dispositivo.

Funcionamiento. Los módems de cable tienen su propio estándar, DOCSIS (Data Over Cable Service Interface Specification), pero éste no incluye a los sistemas inalámbricos. Los radio módems requieren una serie de modificaciones y mejoras para que puedan funcionar correctamente. A continuación se comentan algunas

A) Bandas con frecuencia. Los módems típicos para transmitir sobre el par telefónico utilizan portadoras que se acomodan dentro de los 4 kHz de ancho de banda telefónico, si exceptuamos los modernos módems ADSL. Los módems de cable, por su parte, utilizan frecuencias que se solapan con los canales VHF y UHF de difusión de televisión. Sin embargo, los radio módems suelen utilizar frecuencias superiores que gozan de licencia para transmisiones inalámbricas. En la figura 2.11 se muestran precisamente cuáles son estas bandas de frecuencia. Normalmente, se emplea un conversor de frecuencia para colocar los canales de FI del radio módem en estas bandas. Además, son típicos esquemas de

multiplexación de forma similar a como se realiza en el sistema de telefonía celular GSM para compartir de forma eficiente el espectro radioeléctrico entre un conjunto de usuarios.

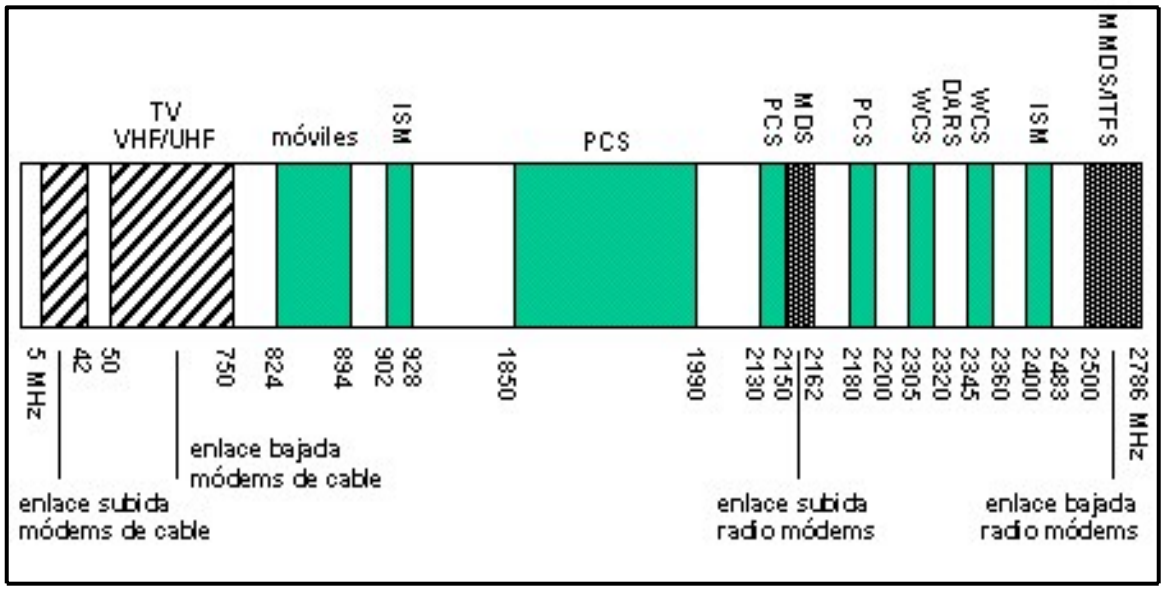


Fig. 2.11[9]

B) Tolerancia de frecuencia y seguimiento de la portadora. En un sistema de cable, la frecuencia de la señal del módem de cable es idéntica a la que debe demodularse en la cabecera de red. Si se produce una desviación de frecuencia de 30 ppm, lo cual supone 600 Hz para una portadora de 20 MHz, la señal todavía se encuentra lo suficientemente centrada y puede demodularse correctamente. Sin embargo, en un sistema inalámbrico las frecuencias se convierten a las bandas MDS, y una tolerancia de 30 ppm se traduce en un desplazamiento de hasta 64 kHz. Un modulador típico tendría dificultades para recuperar la señal, ya que el estándar DOCSIS especifica que la portadora debe encontrarse dentro de un ancho de banda de 30 kHz.

Para corregir este problema, los radio módems implementan un mecanismo de búsqueda y seguimiento de la portadora por medio de bucles de enganche de

[9] Fig.2.11 Bandas de frecuencia de sistemas inalámbricos

fase, comúnmente conocidos como PLLs, y que siguen la señal en rangos de 30 a150kHz.

C) Potencia transmitida y margen dinámico. Cualquier demodulador posee un margen dinámico limitado en el que puede funcionar correctamente. La señal del enlace de subida debe estar contenida dentro del margen dinámico del demodulador de cabecera. Esto incluye variaciones en el nivel de potencia de la señal debidas a la ganancia de las antenas, desvanecimientos por vegetación o precipitaciones y efecto multicamino. Los módems DOCSIS se especifican con un rango de 12 dB de tolerancia, mientras que los radio módems poseen un margen superior: típicamente 20 dB.

Adicionalmente, es necesario ejecutar un algoritmo inicial para que el radio módem localice el nivel de potencia adecuado para comenzar a funcionar. Téngase en cuenta que este nivel es muy dependiente de las características del entorno.

D) Ecualización. Como ya se ha comentado con anterioridad, durante la propagación, la señal radio sufre variaciones de amplitud y de fase que es necesario corregir en el receptor. Estos cambios deben corregirse y compensarse dinámicamente. Es por ello que los radio módems disponen de ecualizadores en tiempo real que modifican su ganancia o introducen retardos de forma dinámica en función de las condiciones del medio. Normalmente se implementan por medio de procesadores digitales de señal (DSPs). Para realizar las correcciones, es necesario disponer de alguna señal de referencia en el receptor. En el caso del estándar GSM, se transmite periódicamente una secuencia de bits conocida que se utiliza para calcular los coeficientes del filtro adaptativo del ecualizador.

E) Efecto multicamino. La propagación multicamino no existe en los sistemas de cable, sin embargo, en los sistemas de radiocomunicaciones se convierte en uno de los principales problemas. Se produce como consecuencia de reflexiones de la señal que se combinan a la entrada de la antena y que dan lugar a degradaciones en el nivel de potencia o distorsión de la señal. En particular, un camino secundario de la señal ligeramente mayor puede ocasionar la cancelación

completa del trayecto principal. En los radio módems aun es más perjudicial, puesto que como suelen disponer de movilidad, es posible que en ciertas posiciones se produzca la reflexión en algún obstáculo inesperado.

F) Esquemas de modulación. Además de las distintas características mencionadas anteriormente, la principal diferencia de los radio módems se refiere a los esquemas y velocidades de modulación utilizados. Normalmente, se utiliza modulación QPSK para el enlace de subida y modulaciones 16QAM o 64QAM para el enlace de bajada. Conforme disminuye la complejidad de la modulación, se consigue una mayor inmunidad frente a desvanecimientos y efecto multicamino, aunque a costa de reducirse la tasa de transmisión. Lo mismo ocurre con la velocidad de modulación. Además, menores velocidades suponen anchos de banda inferiores, lo cual afecta a la sensibilidad de la cabecera y, por lo tanto, al alcance del sistema. En particular, las modulaciones de fase son más adecuadas para la propagación de señales sobre entornos radio. La modulación QPSK es la más robusta, necesitando únicamente de una relación señal a ruido de 13 dB. Por otro lado, la modulación 64QAM consigue una eficiencia espectral tres veces superior, aunque a costa de necesitar una relación señal a ruido de 27 dB para conseguir la misma probabilidad de error (BER). En la figura 14 se representan las constelaciones de las técnicas de modulación QPSK y 16QAM, junto con la codificación que corresponde a cada símbolo transmitido. Obsérvese que conforme aumenta el número de símbolos para una misma potencia transmitida, aumenta la probabilidad de error como consecuencia de que se encuentran más próximos entre sí y son más difíciles de discernir en presencia de ruido. Ver Fig. Num. 2.12

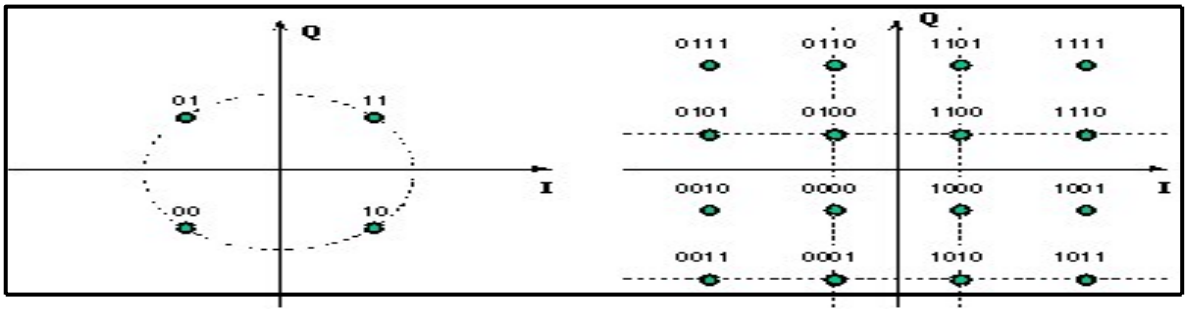


Fig. Num. 2.12

La técnica de espectro ensanchado (spread-spectrum) consiste en la transformación reversible de una señal de forma que su energía se disperse entre una banda de frecuencias mayor que la que ocupaba en un principio. Este tipo de transformación se aplica en sistemas de comunicaciones que requieren determinadas características, y los radio módems son uno de ellos. En la técnica de espectro ensanchado, el ancho de banda utilizado en la transmisión es mucho mayor que el necesario para una transmisión convencional. El ensanchamiento de la banda se realiza a partir de una señal pseudoaleatoria, es decir, con una apariencia de ruido. La señal transmitida tendrá, por lo tanto, características pseudoaleatorias, y sólo podrá ser demodulada si se es capaz de generar la misma señal pseudoaleatoria utilizada por el transmisor. Las características que proporciona el ensanchamiento del espectro de la señal transmitida son las siguientes:

- La transmisión es mucho más resistente frente a interferencias de banda estrecha.

- La señal es difícilmente detectable, ya que su nivel de potencia queda muy reducido por su dispersión espectral. Sólo tras la transformación de desensanchado, ésta recupera la relación señal a ruido suficiente para su demodulación.

- Además, en el caso de que se detecte la señal, la transmisión es ininteligible para quien no conozca la señal pseudoaleatoria utilizada para el ensanchado del espectro.

- La transmisión es resistente a las interferencias por multicamino, porque aunque se trate de una interferencia de la señal sobre sí misma, tiene consecuencias parecidas a cualquier otra interferencia de banda estrecha. Debe tenerse en cuenta que, al aplicar el desensanchado en el receptor, el retardo que ha sufrido la señal multicamino reduce la eficiencia de la interferencia.

- Es posible la transmisión simultánea de varios usuarios sobre el mismo medio, ya que si se emplean secuencias pseudoaleatorias diferentes y que cumplan ciertas condiciones (códigos ortogonales), la transmisión es resistente a las interferencias de unos canales sobre otros. Esto da lugar a la técnica de acceso múltiple por división de código (CDMA).

En la Fig. Num. 2.13 se resumen de forma esquemática algunos de los puntos anteriormente comentados que hacen a la técnica de espectro ensanchado muy apropiada para sistemas de comunicaciones inalámbricos.

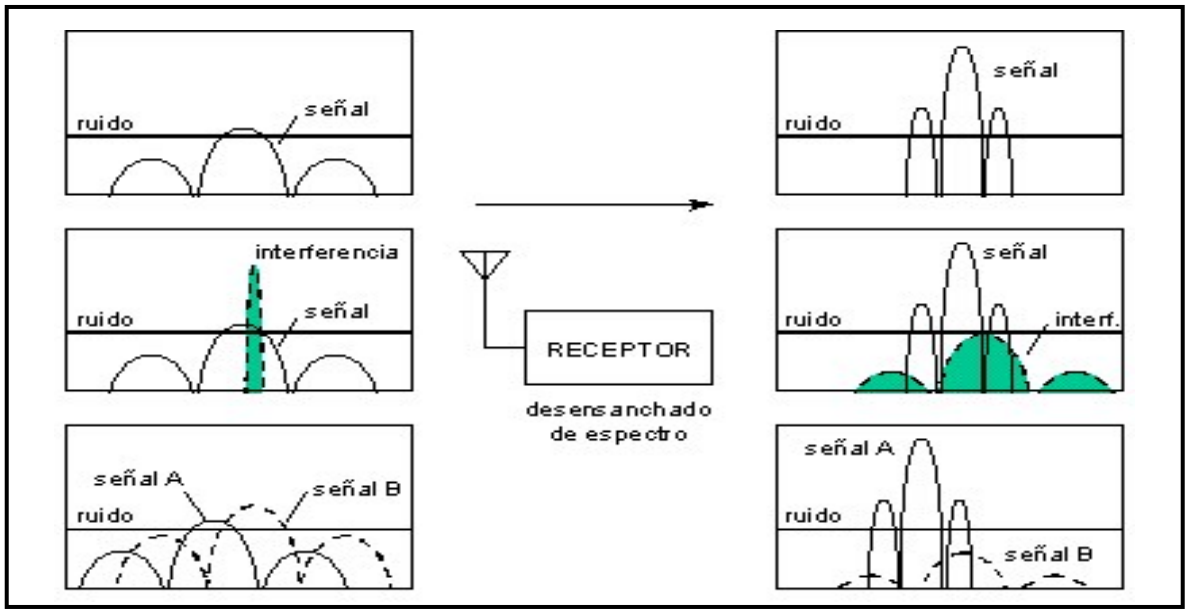


Fig. Num. 2.13

Existen principalmente dos técnicas: espectro ensanchado por secuencia directa (direct sequence) y espectro ensanchado por saltos de frecuencia (frequency hopping). En la primera de ellas, la secuencia pseudoaleatoria se utiliza para generar una señal discreta formada por pulsos que a su vez modula directamente la señal paso-banda. Con la particularidad de que el bloque ensanchador realiza una modulación del mismo tipo que la realizada por el bloque modulador previo, esta vez con la señal pseudoaleatoria. Para realizar el desensanchado de la señal previo a la demodulación en el receptor, es necesario disponer de una réplica exacta de la secuencia pseudoaleatoria y perfectamente sincronizada con la de la señal recibida. El proceso de sincronización consta de dos fases conocidas como

adquisición y seguimiento. En la fase de adquisición, la señal pseudoaleatoria generada en el receptor se desplaza en el tiempo hasta que se sincronice aproximadamente con la ensanchadora de la señal recibida. Esto se realiza calculando la correlación de la señal generada con la señal recibida. Una vez realizada la adquisición, se lleva a cabo la operación de seguimiento, la cual consiste en ajustar de forma continua la secuencia generada. El seguimiento tiene como finalidad alcanzar una sincronización más exacta, así como corregir en todo momento las derivas en los relojes de transmisión y recepción o las derivas en frecuencia por efecto Doppler debidas al movimiento relativo entre el transmisor y receptor.

En cuanto a la técnica de saltos de frecuencia, ésta consiste en realizar cambios periódicos del conjunto de frecuencias asociado a la transmisión. Estos cambios se realizan de acuerdo con una secuencia pseudoaleatoria generada de la misma forma que en los sistemas de secuencia directa. La señal ensanchadora, en este caso, es la salida de un sintetizador de frecuencias, y consiste en un tono que cambia de frecuencia con cada período de pulso de la señal pseudoaleatoria. Si el período de pulso de la señal pseudoaleatoria es mayor que el período de pulso de la señal moduladora, entonces se habla de saltos lentos (SFH, slow frequency hopping). En caso contrario, se denominan saltos rápidos (FFH, fast frequency hopping). El conjunto de frecuencias generado por el sintetizador da lugar al correspondiente conjunto de canales de frecuencia, es decir, bandas del espectro donde se va a localizar la señal transmitida en un momento dado. Al igual que en el caso de secuencia directa, en el receptor también se realizan procedimientos de adquisición y seguimiento similares antes de poder realizarse la demodulación.

Normalmente, las unidades utilizan técnicas de conmutación de paquetes para realizar la transmisión, de tal modo que los mensajes se fragmentan en paquetes que son transmitidos secuencialmente sobre el medio compartido.

Esta técnica conduce a una transmisión 100% libre de errores con un throughput efectivo de hasta 38,4 Kbit/s.

Cada paquete se comprueba en el receptor y, en caso de recepción incorrecta, se retransmite.

La conexión con el radio módem se realiza a través del puerto serie de un PC, desde el cual se puede configurar en cuál de los 3 canales debe operar. Además, es posible realizar transmisiones punto a multipunto en el modo Maestro/Esclavo. Cada vez que el Maestro envía datos, los reciben el resto de unidades. Mientras que cuando un Esclavo transmite, sólo recibe los datos el Maestro. Esta configuración emula lo que se conoce como red "multi-drop RS232".

Por último, el equipo puede disponer de antena interna o de un conector externo para que podamos instalar la antena que deseemos. De entre los distintos modelos, existen antenas omnidireccionales, antenas Yagi o monopolos, todas ellas para la banda de 900 MHz.

2.5.2 Routers. Routers ADSL sobre ISDN (RDSI) para oficinas pequeñas, oficinas en casa y telé trabajadores Cisco 677i y Cisco 677i-DIR Los routers de línea digital asimétrica de abonado (ADSL a través de ISDN) Cisco 677 para telé trabajadores y oficinas pequeñas/oficinas en casa se han diseñado para ofrecer servicios rentables de alta velocidad a oficinas pequeñas y telé trabajadores. Los routers Cisco 677i y 677i-DIR presentan un diseño compacto y proporcionan una solución de bajo costo no desmontable. Forman parte de la arquitectura líder de Cisco que ofrece una ruta hacia servicios de vanguardia. Estos routers proporcionan acceso seguro y de alta velocidad a servicios empresariales e Internet a través de un potente enrutamiento, una derivación transparente y un conjunto de características del protocolo punto a punto (PPP)/ATM.

Características y funcionamiento. ISDN (RDSI). Los modelos Cisco 677i y 677i-DIR son compatibles con las implementaciones ISDN (RDSI) 2B1Q y 4B3T. Ambos modelos proporcionan una interfaz 10/100BaseT para las conexiones a una LAN pequeña o con un único PC equipado con Ethernet. Admiten un potente conjunto de características de enrutamiento para así poder integrarse perfectamente con el servicio ADSL a través de ISDN (RDSI) en LAN y WAN

empresariales y domésticas. Un servidor integrado DHCP (Dynamic Host Configuration Protocol) asigna automáticamente direcciones IP a los PC de la LAN y mediante la conversión de direcciones de puerto (PAT) estos PC pueden compartir una sola dirección IP.

Hay dos versiones del router ADSL sobre ISDN, 677i y 677i-DIR.[10] La primera se utiliza en las líneas con tráfico ISDN (RDSI) Se conecta a la línea a través de un discriminador de equipo terminal de abonado. El router Cisco 677i-DIR se utiliza en líneas dedicadas sin tráfico ISDN (RDSI). Se conecta a la línea directamente sin discriminadores. En cuanto al espectro, es compatible con las implementaciones ISDN (RDSI).

Características

- Compatibilidad con rutas rápidas e intercaladas
- Codificación Trellis y alineación extensa de bits/bytes ATM
- Interfaz Ethernet 10BaseT o 100BaseTX con negociación automática

[10] Fuente;
http://www.tecnologiayredes.com.ar/viewtopic.php?p=41&sid=5d2e398cdef015116c9ee532419f01a5

CAPÍTULO TERCERO

REDES DE COMUNICACIÓN

3.1 REDES DE COMUNICACIÓN:

A) **LAN.** (Local Area Network) Redes de área local Cobertura uno o varios edificios. Sus características son:

Compuestas por varios segmentos, que se interconectan mediante conmutadores (switches) o concentradores (hubs). Topología: Bus: Ethernet (IEEE 802.3) Anillo: Token ring (IEEE 802.5), estrella

2. MAN. (Metropolitan Area Network). Redes de área metropolitana, Cobertura: una ciudad, Usan redes de cable de fibra óptica de instalación reciente en las ciudades, Aprovechan el ancho de banda de los cables de par trenzado de las redes de telefonía (xDSL) las tecnologías aplicadas se basan en LAN Pero existe un estándar para MAN: DQDB (IEEE802.6).

3. WAN (Wide Area Network). Redes de área extensa, su cobertura es de varias ciudades al mundo entero. Sus características son:

Compuestas por varias subredes, conectadas por enrutadores (routers) o pasarelas (gateways) requieren atravesar rutas de acceso público y circuitos proporcionados por una entidad de telecomunicación su tecnología se basa en conmutación de paquetes, conmutación de circuitos, ATM, Frame Relay

Cuando deseo enlazar mis oficinas centrales con alguna sucursal u oficina remota. (MODEM) Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

4. **VPN'S.** Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas[11] a varios kilómetros de distancia.

La VPN. Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. Ver fig. Num. 3.1. Una de sus características es que los costos son bajos porque solo se realiza llamadas locales, además de tener la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

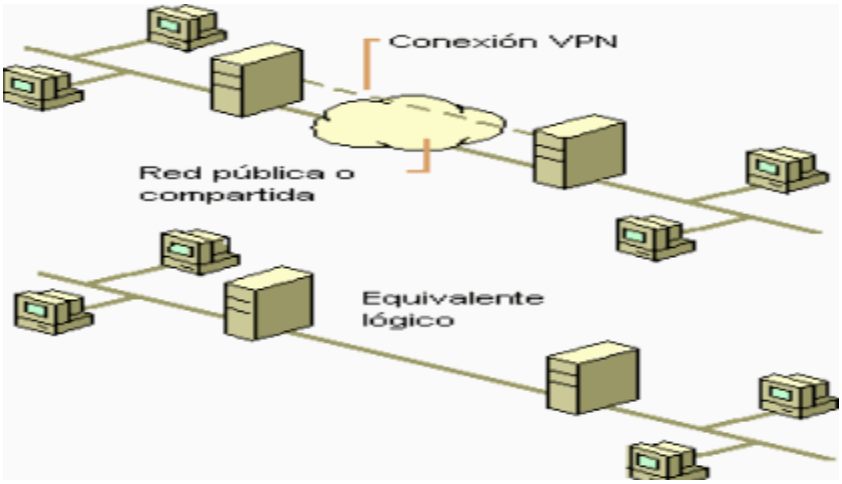


Fig. Num. 3.1

En la figura Num. 3.2 se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para

[11] El mejor ejemplo de un acceso remoto son las redes inalámbricas

nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado lleguen a su vez al firewall remoto y terminen en el servidor remoto.

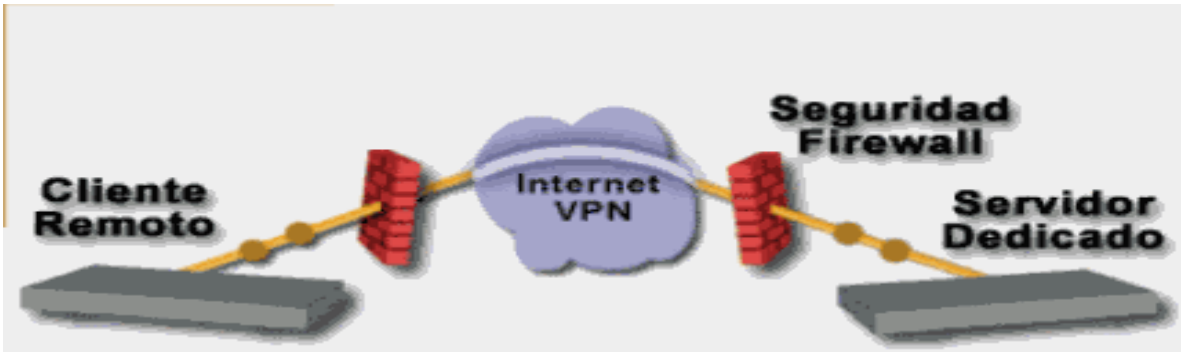


Fig. Num. 3.2

Las VPN pueden enlazar las oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet IP, Ipsec, Frame Relay, ATM como lo muestra la Fig. Num. 3.3

Fig. Num. 3.3

3.2 TECNOLOGÍA DE TÚNEL

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación. Además los paquetes van encriptados de forma que los datos son ilegibles para los extraños. Ver Fig. Num. 3.4

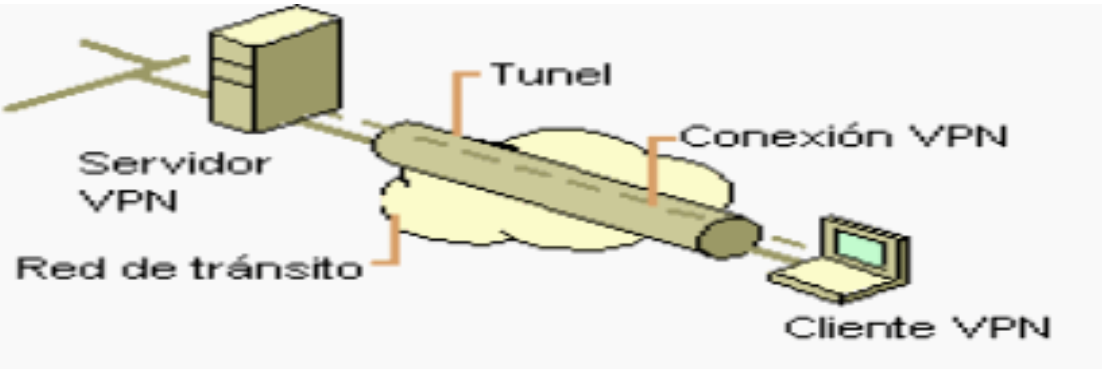


Fig. Num. 3.4[12]

3.3 REQUERIMIENTOS BÁSICOS DE UN ACCESO REMOTO

Por lo general cuando se desea acceder remotamente a un Servidor de Acceso Remoto que será el que nos conecte a una VPN hay que asegurarse de que proporcione:

El servidor debe ser capaz de verificar la identidad de los usuarios y restringir el acceso aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones. El servidor debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos. Los datos que se van a transmitir a traves de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves. El servidor debe generar y renovar las claves de codificación para el cliente y el servidor.

---

[12] Fuente: http://www.monografias.com/

Soporte a protocolos múltiples. El servidor debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

3.4 HERRAMIENTAS INDISPENSABLES PARA EL ARMADO DE UNA RED CON ACCESO REMOTO

Software. Hay una variedad de software utilizado para acceso remoto, uno de los mas comerciales que se puede usar en plataforma Windows es; el escritorio remoto o el cliente de Terminal Server.

Firewall. Un firewall es un sistema diseñado para prevenir acceso no autorizado hacia o desde una red privada. Provee un punto de defensa entre dos redes, protege una red de otra. Usualmente, un firewall protege la red privada de una empresa de las redes públicas o compartidas a las que se conecta. Un firewall puede ser tan simple como un ruteador que filtra paquetes o tan complejo como varias computadoras o varios ruteadores que combinan el filtrado de paquetes con *servicios proxy* a nivel aplicación.

Cualquier firewall puede clasificarse dentro de uno de los tipos siguientes[13];

Firewall de capa de red. El primero funciona al nivel de la red de la pila de protocolos (TCP/IP) como filtro de paquetes IP, no permitiendo que estos pasen el firewall a menos que se atengan a las reglas definidas por el administrador del firewall o aplicadas por defecto como en algunos sistemas inflexibles de firewall. Una disposición más permisiva podría dejar que cualquier paquete pase el filtro mientras que no cumpla con ninguna regla negativa de rechazo.
El cometido de los filtros (Packet Filters) consiste en filtrar paquetes dejando pasar por el tamiz únicamente cierto tipo de tráfico. Estos filtros pueden implementarse a partir de routers.

[13] Fuente: http://www.dric.com.mx/seguridad/firewall/firewall1.php?cat=4&scat=3

Firewall de capa de aplicación. El segundo trabaja en el nivel de aplicación, todo el tráfico de HTTP, (u otro protocolo), puede interceptar todos los paquetes que llegan o salen de una aplicación. Se bloquean otros paquetes (generalmente sin avisar al remitente). En principio, los firewall de aplicación pueden evitar que todo el tráfico externo indeseado alcance las máquinas protegidas.
Las pasarelas a nivel de aplicación (Application Gateway) se ocupan de comprobar que los protocolos a nivel de aplicación (ftp,http,etc...) se están utilizando de forma correcta sin tratar de explotar algunos problemas que pudiese tener el software de red.

CAPÍTULO CUARTO

PREPARACIÓN DE LA RED PARA ACCESO REMOTO

4.1 INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR DE ACCESO REMOTO PARA LOS SISTEMAS OPERATIVOS WINDOWS 2003 SERVER

La configuración del servidor de RAS (Remote Access Service), Servicio de Acceso Remoto, es distinta a la de los clientes de Acceso telefónico a redes. Aunque los clientes de Acceso telefónico a redes se configuran principalmente para tener acceso mediante marcado a redes remotas, los servidores de Acceso Remoto se configuran para proporcionar acceso a los servicios de red para esos clientes. La configuración de dicho servidor incluye la configuración de los puertos de comunicaciones, los protocolos de red (como NetBEUI, TCP/IP e IPX).

4.2 CONFIGURACIÓN Y ARMADO DE LA RED

4.2.1 Preparar el Sistema de Cableado. El funcionamiento del sistema cableado deberá ser considerado no sólo cuando se están apoyando necesidades actuales sino también cuando se anticipan necesidades futuras. Hacer esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones de sistema de cableado. Los cables son el componente básico de todo sistema de cableado. Existen diferentes tipos de cables, la elección de uno respecto a otro depende del ancho de banda necesario, las distancias existentes y el coste del medio, de acuerdo a lo visto en el capítulo segundo.

En este caso emplearemos el cable UTP ya que es el mas comercial y accesible en cuestión de presupuesto y para esto emplearemos un conector RJ-45 en la fig. Sig. Se muestra la configuración dependiendo de la norma 568 A – B. Que es el estándar que define un sistema genérico de cableado de telecomunicaciones para edificios que puedan soportar un ambiente de productos y proveedores múltiples.

Normativa 568-A[14]		Normativa 568-B[15]	
Conector 1	**Conector 2**	**Conector 1**	**Conector 2**
1- Blanco Naranja	1- Blanco Naranja	1- Blanco Verde	1- Blanco Verde
2- Naranja	2- Naranja	2- Verde	2- Verde
3- Blanco Verde	3- Blanco Verde	3- Blanco Naranja	3- Blanco Naranja
4- Azul	4- Azul	4- Azul	4- Azul
5- Blanco Azul	5- Blanco Azul	5- Blanco Azul	5- Blanco Azul
6- Verde	6- Verde	6- Naranja	6- Naranja
7- Blanco Marrón	7- Blanco Marrón	7- Blanco Marrón	7- Blanco Marrón
8- Marrón	8- Marrón	8- Marrón	8- Marrón

ya teniendo los cables armados el siguiente hardware que debemos tener son tarjetas de red integradas a las tarjetas madre de la PC o tarjetas PCI un Swicht o Router, un moden con servicio de Internet y por supuesto un firewall para asegurar nuestra información ya que a nuestra red se conectaran clientes externos.

4.2.2 Configuración del AP o Router. Lo primero que hay que configurar es la tarjeta de red. Asegurar de que el Router está conectado a la tarjeta de red mediante el cable UTP y el conector RJ45. Entramos al Panel de control -> Conexiones de red y damos un click derecho en la Conexión de área local y entramos a propiedades. Ahora seleccionamos el protocolo TCP/IP y entramos nuevamente a Propiedades. Hay que configurar lo siguiente; Dirección IP: Aquí pondremos la dirección del PC (cada PC de la red tendrá una dirección IP distinta, siendo siempre del mismo rango. Por ejemplo, si ponemos 192.168.110.1, los demás PCs de la red serán siempre 192.168.110.xxx). Se puede poner la dirección IP que quieras, siempre que los dos primeros grupos de dígitos sean 192.168 y los siguientes se encuentren entre 0 y 254. recomiendo que pongas IPs altas (192.168.110.xxx y no 192.168.1.xxx),ya que da más

[14] Fuente: http://www.tele-centros.org/tc-toolkit2.0/fuente/redes/prin_redes2.htm
[15] Fuente: http://www.tele-centros.org/tc-toolkit2.0/fuente/redes/prin_redes2.htm

seguridad.

Máscara de subred: Tiene que ser la misma en todos los PC's de la red (ahora no cambia el último grupo de números). Por ejemplo, si ponemos 255.0.0.0, los demás PC's de la red serán siempre 255.0.0.0. Como se muestra en la Fig Num 4.1

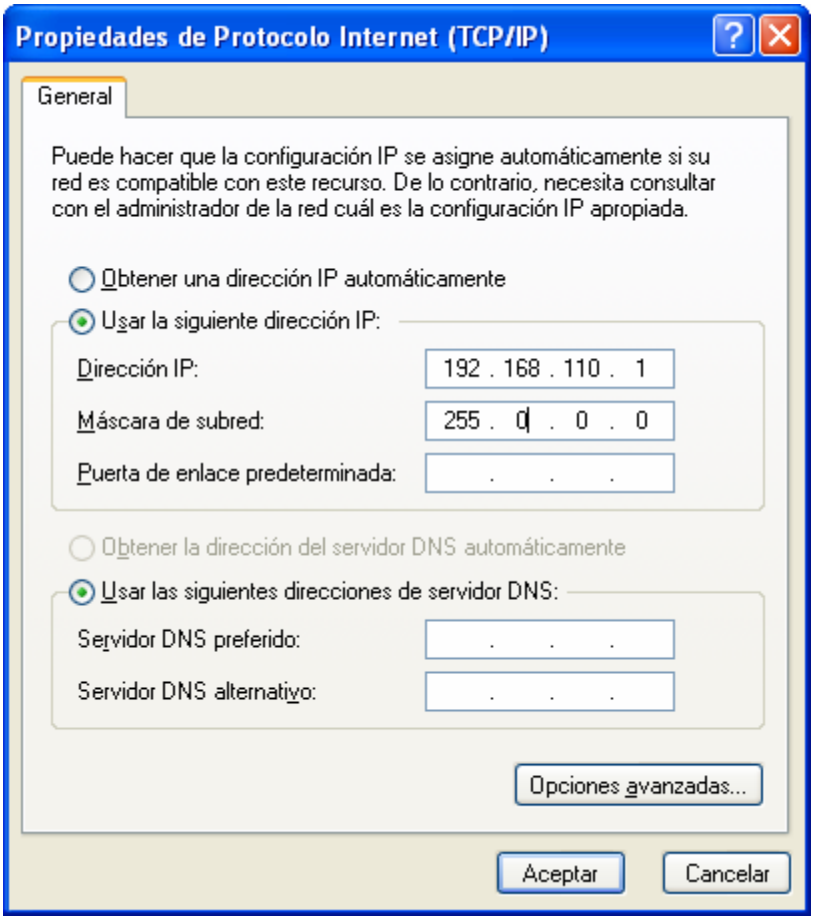


Fig. Num. 4.1

Ahora tenemos que incluirla al mismo grupo de trabajo y darle un nombre a la PC en la Red siguiendo estos pasos:

Damos un clic derecho sobre el icono de mi PC -> Propiedades -> Nombre de equipo -> Cambiar

Ahí daremos el nombre del grupo de trabajo del equipo el cual queremos que sea miembro.

Por ultimo si ya tenemos todo bien armado solo nos aseguramos si ya estamos en red, entramos en el Panel de control -> Conexiones de red -> Mis sitios de Red -> Ver equipos del grupo de trabajo y ahí deberán aparecer las demás computadoras o bien dando un ping a la dirección IP de otro equipo para ver si nos responde.

4.3 CONFIGURAR ENRUTAMIENTO Y ACCESO REMOTO PARA UNA INTRANET EN WINDOWS SERVER 2003 ENTERPRISE EDITION Y WINDOWS SERVER 2003 STANDARD EDITION

A continuación se describe cómo configurar en Windows Server 2003 Standard Edition o Windows Server 2003 Enterprise Edition un Servicio de enrutamiento y acceso remoto que permita a los usuarios autenticados conectarse de forma remota a otra red a través de Internet. Esta conexión segura proporciona acceso a todos los recursos de red internos, como mensajería, uso compartido de impresoras y archivos, y acceso al servidor Web. El carácter remoto de esta conexión es transparente para el usuario, de modo que la experiencia general de la utilización del acceso remoto es similar a la de trabajar en una estación de trabajo en una red local.

Instalar el Servicio de enrutamiento y acceso remoto. De forma predeterminada, el Servicio de enrutamiento y acceso remoto se instala automáticamente durante la instalación de Windows Server 2003, pero está deshabilitado.

4.3.1 Para habilitar el Servicio de Enrutamiento y Acceso Remoto

1. Haga clic en **Inicio**, seleccione **Herramientas administrativas** y, a continuación, haga clic en **Enrutamiento y acceso remoto.**

2. En el panel de la izquierda de la consola, haga clic en el servidor correspondiente al nombre del servidor local.
   Si el icono tiene un círculo de color rojo en la esquina inferior izquierda, el Servicio de enrutamiento y acceso remoto no está habilitado. Vaya al paso 3.
   Si el icono tiene una flecha de color verde que señala hacia arriba en la

esquina inferior izquierda, el servicio está habilitado. En este caso, quizá desee volver a configurar el servidor. Para volver a configurar el servidor, en primer lugar debe deshabilitar Enrutamiento y acceso remoto. Para ello, haga clic con el botón secundario del Mouse (ratón) en el servidor y, después, haga clic en **Deshabilitar Enrutamiento y acceso remoto**. Haga clic en **Sí** cuando aparezca un mensaje informativo.

3. Haga clic con el botón secundario del Mouse (ratón) en el servidor y, después, haga clic en Configurar y habilitar Enrutamiento y acceso remoto para iniciar el Asistente para instalación del servidor de enrutamiento y acceso remoto. Haga clic en Siguiente.

4. Haga clic en Acceso remoto (acceso telefónico o red privada virtual) para que los equipos remotos puedan marcar o conectarse a esta red a través de Internet. Haga clic en Siguiente.

5. Haga clic en VPN para el acceso a una red privada virtual o en Acceso telefónico, dependiendo de la función que vaya a asignar al servidor, si sera un servidor de acceso remoto o sera un servidor de acceso para la red virtual.

6. En la página Conexión VPN, haga clic en la interfaz de red conectada a Internet y, después, haga clic en Siguiente.

7. En la página Asignación de direcciones IP, realice una de las siguientes acciones:

Si se va a utilizar un servidor DHCP[16] para asignar direcciones a clientes remotos, haga clic en Automáticamente y, después, en Siguiente. Vaya al paso 7.

- Para proporcionar a los clientes remotos direcciones sólo de un conjunto predefinido, haga clic en De un intervalo de direcciones especificado.

[16] en la mayoría de los casos, la opción DHCP es más fácil de administrar. Sin embargo, si DHCP no está disponible, debe especificar un intervalo de direcciones estáticas.

El asistente abre la página Asignación de intervalo de direcciones.

1. Haga clic en Nuevo.
2. En el cuadro Dirección IP inicial, escriba la primera dirección IP del intervalo de direcciones que desea utilizar.
3. En el cuadro Dirección IP final, escriba la última dirección IP del intervalo. Windows calcula automáticamente el número de direcciones.
4. Haga clic en Aceptar para volver a la página Asignación de intervalo de direcciones.
5. Haga clic en Siguiente.
6. Acepte la opción predeterminada de No, usar Enrutamiento y acceso remoto para autenticar las solicitudes de conexión y, después, haga clic en Siguiente.
7. Haga clic en Finalizar para habilitar el Servicio de enrutamiento y acceso remoto, y para configurar el servidor de acceso remoto.
8. Después de configurar el servidor para que reciba conexiones de acceso telefónico, configure una conexión de cliente de acceso remoto en la estación de trabajo cliente.

4.3.2 Para Configurar un Cliente para Acceso Telefónico

Nota: Como hay varias versiones de Microsoft Windows, los pasos siguientes pueden ser diferentes en su equipo. Si es así, consulte la documentación del producto para realizar estos pasos.

1. Haga clic en Inicio, en Panel de control y, después, haga doble clic en Conexiones de red.
2. En Tareas de red, haga clic en Crear una conexión nueva y, a continuación, haga clic en Siguiente.

3. Haga clic en Conectarse a la red de mi lugar de trabajo para crear la conexión de acceso telefónico y, después, haga clic en Siguiente.

4. Haga clic en Conexión de acceso telefónico y, a continuación, en Siguiente.

5. En la página Nombre de conexión, escriba un nombre descriptivo para la conexión y, después, haga clic en Siguiente.

6. En la página Número de teléfono que desea marcar, escriba el número de teléfono del servidor de acceso remoto en el cuadro de diálogo Número de teléfono.

7. Siga uno de estos procedimientos y, a continuación, haga clic en Siguiente:

Si desea permitir que cualquier usuario que inicie sesión en la estación de trabajo tenga acceso a esta conexión de acceso telefónico, haga clic en El uso de cualquier persona.

- Si desea que esta conexión sólo esté disponible para el usuario que ha iniciado sesión actualmente, haga clic en Sólo para mi uso.

8. Haga clic en Finalizar para guardar la conexión.

4.3.3 Para configurar un cliente para acceso a VPN

Para configurar un cliente para el acceso a una red privada virtual (VPN, Virtual Private Network), siga estos pasos en la estación de trabajo cliente. **Nota***:* Como hay varias versiones de Microsoft Windows, los pasos siguientes pueden ser diferentes en su equipo. Si es así, consulte la documentación del producto para realizar estos pasos*.*

1. Haga clic en Inicio, en Panel de control y, después, haga doble clic en Conexiones de red.

2. En Tareas de red, haga clic en Crear una conexión nueva y, a continuación, haga clic en Siguiente.

3. Haga clic en Conectarse a la red de mi lugar de trabajo para crear la conexión de acceso telefónico y, después, haga clic en Siguiente.

4. Haga clic en Conexión de red privada virtual y, después, haga clic en Siguiente.

5. En la página Nombre de conexión, escriba un nombre descriptivo para la conexión y, después, haga clic en Siguiente.

6. Siga uno de estos procedimientos y, a continuación, haga clic en Siguiente.

Si el equipo está conectado a Internet de forma permanente, haga clic en No usar la conexión inicial.

Si el equipo se conecta a Internet por medio de un proveedor de servicios Internet (ISP), haga clic en Usar automáticamente esta conexión inicial y, después, haga clic en el nombre de la conexión con el ISP.

7. Escriba la dirección IP o el nombre de host del equipo servidor VPN (por ejemplo, ServidorVPN.DominioDeEjemplo.com).

8. Siga uno de estos procedimientos y, a continuación, haga clic en Siguiente:

Si desea permitir que cualquier usuario que inicie sesión en la estación de trabajo tenga acceso a esta conexión de acceso telefónico, haga clic en El uso de cualquier persona.

Si desea que esta conexión sólo esté disponible para el usuario que ha iniciado sesión actualmente, haga clic en Sólo para mi uso.

9. Haga clic en Finalizar para guardar la conexión.
10.

4.4 CONCEDER A LOS USUARIOS ACCESO A SERVIDORES DE ACCESO REMOTO

Puede utilizar directivas de acceso remoto para conceder o denegar la autorización según criterios como la hora del día, el día de la semana, la pertenencia del usuario a grupos de seguridad de Windows Server 2003 o el tipo de conexión solicitado. Si un servidor de acceso remoto es miembro de un dominio, puede configurar estos valores mediante la cuenta de dominio del usuario.

Nota: Para mas información sobre directivas vea el capítulo quinto
Si el servidor es independiente o es miembro de un grupo de trabajo, el usuario debe tener una cuenta local en el servidor de acceso remoto.

4.4.1 Conceder derechos de acceso remoto a cuentas de usuario individuales

Si administra el acceso remoto basándose en una cuenta de usuario, siga estos pasos para conceder derechos de acceso remoto:

1. Haga clic en Inicio, seleccione Todos los programas, Herramientas administrativas y, a continuación, haga clic en Usuarios y equipos de Active Directory.

2. Haga clic con el botón secundario del Mouse (ratón) en la cuenta de usuario a la que desea conceder derechos de acceso remoto, haga clic en Propiedades y, a continuación, haga clic en la ficha Marcado.

3. Haga clic en Permitir acceso para conceder al usuario permiso de marcado y, a continuación, haga clic en Aceptar.

4.4.2 Configurar derechos de acceso remoto basados en la pertenencia a grupos

Si administra el acceso remoto basándose en grupos, siga estos pasos para conceder derechos de acceso remoto:

1. Cree un grupo que contenga miembros a los que se les permita crear conexiones VPN.
2. Haga clic en Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Enrutamiento y acceso remoto.
3. En el árbol de consola, expanda Enrutamiento y acceso remoto, expanda el nombre del servidor y, a continuación, haga clic en Directivas de acceso remoto.
4. Haga clic con el botón secundario del Mouse (ratón) en el panel de la derecha, seleccione Nuevo y, a continuación, haga clic en Directiva de acceso remoto.
5. Haga clic en Siguiente, escriba el nombre de la directiva y, a continuación, haga clic en Siguiente.
6. Haga clic en VPN para el acceso a una red privada virtual o en Acceso telefónico para el acceso telefónico y, después, haga clic en Siguiente.
7. Haga clic en Agregar, escriba el nombre del grupo que creó en el paso 1 y, después, haga clic en Siguiente.
8. Siga las instrucciones que aparecerán en pantalla para finalizar el asistente.
9. Si el servidor VPN ya permite servicios de acceso telefónico a redes remoto, no elimine la directiva predeterminada; en su lugar, muévala para que quede como la última directiva que se evalúa.

4.5 PARA ESTABLECER UNA CONEXIÓN REMOTA

Nota: Como hay varias versiones de Microsoft Windows, los pasos siguientes pueden ser diferentes en su equipo. Si es así, consulte la documentación del producto para realizar estos pasos.

1. En la estación de trabajo cliente, haga clic en Inicio, en Conexiones de red y, después, en la nueva conexión que ha creado.

2. En el cuadro Nombre de usuario, escriba su nombre de usuario.

   Si la red a la que desea conectarse tiene varios dominios, quizás tenga que especificar un nombre de dominio. En tal caso, utilice el formato nombreDominio \ nombreUsuario en el cuadro Nombre de usuario.

3. En el cuadro Contraseña, escriba su contraseña.

4. Si utiliza una conexión de acceso telefónico, compruebe el número de teléfono que se indica en el cuadro Marcar para asegurarse de que es el correcto. Asegúrese de que ha especificado los números adicionales que debe marcar para obtener una línea externa o una llamada de larga distancia.

5. Haga clic en Marcar o en Conectar (en el caso de conexiones VPN). El equipo establece una conexión con el servidor de acceso remoto. El servidor autentica al usuario y registra el equipo en la red.

SOLUCIONAR PROBLEMAS

En esta sección se describe cómo solucionar algunos problemas que pueden surgir al intentar configurar el acceso remoto.

No están disponibles todos los valores de configuración para marcar del usuario. Si el dominio basado en Windows Server 2003 utiliza el modo mixto, no estarán disponibles todas las opciones de configuración. Los administradores sólo pueden conceder o denegar acceso al usuario y especificar las opciones de

devolución de llamada (éstas son las opciones de permiso de acceso disponibles en Microsoft Windows NT 4.0). Las restantes opciones están disponibles después de cambiar el dominio al modo nativo.

CAPÍTULO QUINTO

SEGURIDAD EN SERVIDORES DE ACCESO REMOTO

5.1 ESTABLECER LA SEGURIDAD

En Windows 2000 y los sistemas operativos de la familia Windows Server 2003, puede elegir uno de dos modos de seguridad:

Seguridad media. Es el modo de compatibilidad con los permisos de Windows NT 4.0 Terminal Server Edition

Seguridad completa. Es el modo para los permisos de Windows 2000 y los sistemas operativos de la familia Windows Server 2003

En ambos modos, el descriptor de seguridad TERMINAL SERVER USER se aplica en numerosas claves del Registro y en directorios del sistema de archivos. La diferencia entre los dos modos se basa en la forma en que se aplica el descriptor de seguridad.

En el modo Seguridad media, el descriptor de seguridad se agrega a cada miembro del grupo Usuarios. En Windows NT 4.0, cuando los permisos de un usuario se evalúan para determinar el acceso a un archivo o una entrada del Registro, la presencia del descriptor de seguridad autoriza el acceso.

Esta aplicación del descriptor de seguridad permite a los miembros del grupo Usuarios ejecutar programas que de otro modo podrían no funcionar en el modo de permisos más riguroso, Seguridad completa, utilizado en Windows 2000 y en los sistemas operativos de la familia Windows Server 2003. Sin embargo, cuando elige el modo Seguridad media, cualquier usuario del sistema puede cambiar los archivos y opciones del Registro en muchos lugares de todo el sistema, aunque los archivos de datos de otros usuarios puedan no ser visibles. Un usuario con

malas intenciones podría aprovecharse de esta situación y reemplazar un programa conocido y fiable por otro con el mismo nombre pero con fines dañinos.

Por el contrario, el modo Seguridad completa no aplica el descriptor a cada usuario. En cambio, las aplicaciones deben escribirse para ejecutarse en el contexto de un usuario normal. Cuando dude, debería elegir el modo Seguridad completa y probar sus aplicaciones en dicho modo.

5.2 COMO CAMBIAR PERMISOS PARA LA COMPATIBILIDAD DE CARACTERES

1. Abra Configuración de Servicios del Terminal Server.

2. En el árbol de la consola, haga clic en Configuración de servidor.

3. En el panel de detalles, haga clic con el botón secundario en Compatibilidad de permisos y después en Propiedades.

4. Seleccione Seguridad completa para proporcionar el entorno más seguro o Seguridad media para proporcionar un entorno compatible con la mayor parte de las aplicaciones antiguas y, después, haga clic en Aceptar. Como se muestra en la sguiente pagina, Fig. Num. 5.1.

Para llevar a cabo este procedimiento, debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente. Si el equipo está conectado a un dominio, los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento. Como práctica recomendada de seguridad, considere la posibilidad de utilizar la opción Ejecutar como para realizar este procedimiento.

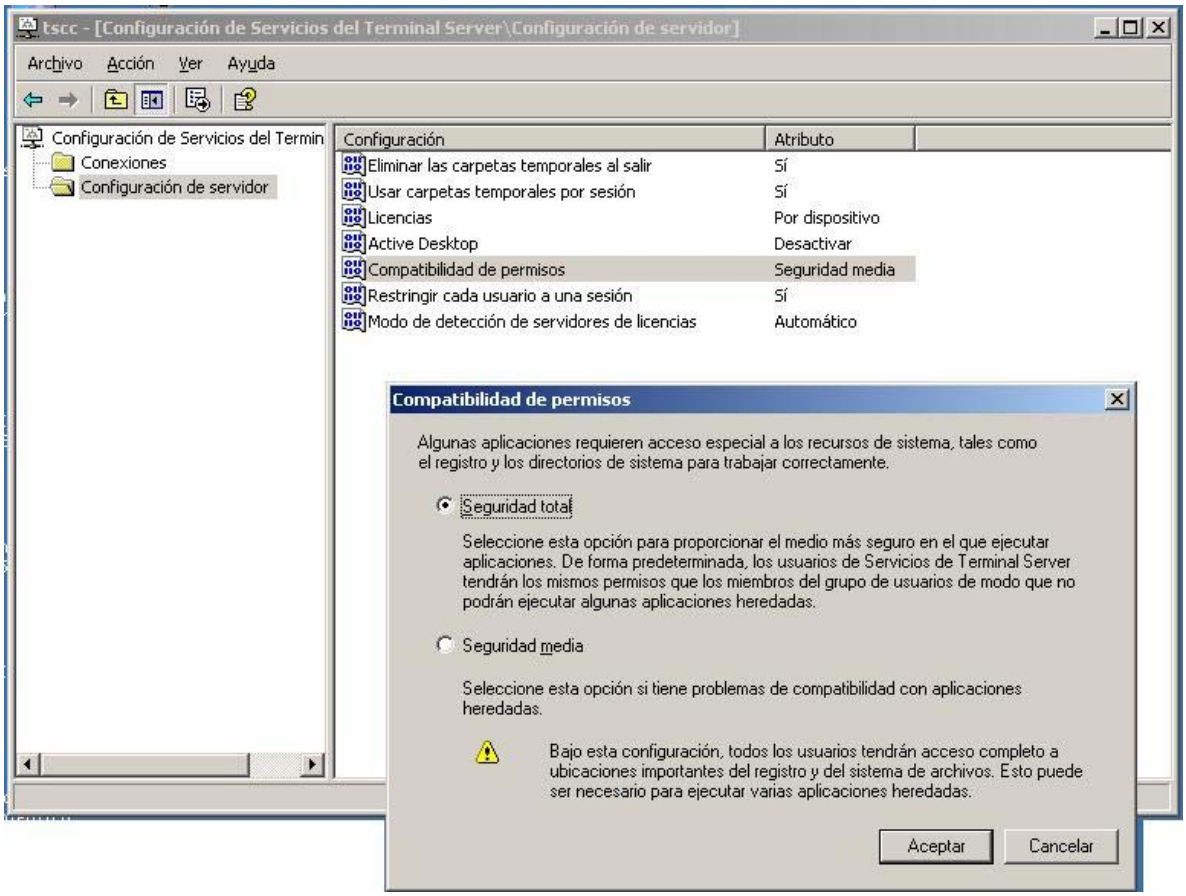


Fig. Num. 5.1

5.3 GRUPOS LOCALES PREDETERMINADOS

En la carpeta Grupos, situada en Usuarios y grupos locales de MMC (Microsoft Management Console), se muestran los grupos locales predeterminados, así como los creados por el usuario. Los grupos locales predeterminados se crean automáticamente al instalar un servidor independiente o un servidor miembro donde se use Windows Server 2003. Al pertenecer a un grupo local, se le proporcionan al usuario los derechos y capacidades necesarios para realizar diversas tareas en el equipo local.

5.3.1 Para agregar un miembro a un grupo local

1. Abra Administración de equipos.[17]

2. En el árbol de la consola, haga clic en Grupos.

3. Haga clic con el botón secundario del Mouse en el grupo al que desee agregar un miembro, haga clic en Agregar al grupo y, a continuación, en Agregar.

4. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, realice las acciones siguientes:

Para agregar al grupo una cuenta de usuario o de grupo, escriba el nombre de ésta. En Escriba los nombres de objeto que desea seleccionar y después, haga clic en Aceptar.

Para agregar una cuenta de equipo a este grupo, haga clic en Tipos de objetos, active la casilla de verificación Equipos y a continuación, haga clic en Aceptar. En Escriba los nombres de objeto que desea seleccionar, escriba el nombre de la cuenta de equipo que desee agregar al grupo y, después, haga clic en Aceptar.

Para quitar un miembro de un grupo local, seleccione la cuenta de usuario, cuenta de equipo o cuenta de grupo en Miembros y, a continuación, haga clic en Quitar.

Los derechos y permisos asignados a un grupo se asignan a todos sus miembros.

Reduzca al mínimo necesario el número de usuarios del grupo Administradores, ya que en un equipo local los miembros de dicho grupo tienen permisos de Control total.

[17] Para abrir Administración de equipos, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Administración de equipos.

Si el equipo se ha unido a un dominio, también puede agregar a un grupo local las cuentas de usuario, de equipo y de grupo de ese dominio y de los dominios de confianza.

5.4 GRUPOS PREDETERMINADOS

Los grupos predeterminados, como el grupo Administradores de dominio, son grupos de seguridad que se crean automáticamente al crear un dominio de Active Directory. Estos grupos predefinidos permiten controlar el acceso a los recursos compartidos y delegar funciones administrativas específicas en todo el dominio.

A muchos grupos predeterminados se les asigna automáticamente un conjunto de derechos de usuario que autoriza a los miembros del grupo a realizar acciones específicas en un dominio, como iniciar una sesión en un sistema local o efectuar copias de seguridad de archivos y carpetas. Por ejemplo, un miembro del grupo Operadores de copia de seguridad tiene derecho a realizar operaciones de copia de seguridad en todos los controladores del dominio.

Cuando agrega un usuario a un grupo, el primero recibe todos los derechos de usuario y permisos asignados a ese grupo en todos los recursos compartidos.

5.4.1 Tipos de grupos. Los grupos se utilizan para reunir las cuentas de usuario, las cuentas de equipo y otras cuentas de grupo en unidades administrables. Al trabajar con grupos en lugar de usuarios individuales se simplifica el mantenimiento y la administración de la red.

Hay dos tipos de grupos en Active Directory: grupos de distribución y grupos de seguridad. Puede utilizar los grupos de distribución para crear listas de distribución de correo electrónico y los grupos de seguridad para asignar permisos a los recursos compartidos.

A) Grupos de distribución. Los grupos de distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como Exchange) para enviar correo electrónico a grupos de usuarios. Los grupos de distribución no tienen habilitada la seguridad,

lo que significa que no se pueden incluir en las listas de control de acceso discrecional (DACL). Si necesita un grupo para controlar el acceso a los recursos compartidos, cree un grupo de seguridad.

B) Grupos de seguridad. Si se utilizan adecuadamente, los grupos de seguridad suponen un modo eficaz de asignar el acceso a los recursos de su red. Los grupos de seguridad permiten:

Asignar derechos de usuario a grupos de seguridad en Active Directory Los derechos de usuario se asignan a los grupos de seguridad para determinar qué acciones pueden llevar a cabo los miembros del grupo en el ámbito de un dominio (o bosque). Los derechos de usuario se asignan automáticamente a varios grupos de seguridad durante la instalación de Active Directory para facilitar a los administradores la definición de la función administrativa de un usuario dentro del dominio. Por ejemplo, un usuario que se agrega al grupo Operadores de copia en Active Directory puede restaurar y hacer copias de seguridad de los archivos y directorios ubicados en cada controlador del dominio.

Esto es posible porque, de manera predeterminada, los derechos de usuario para hacer copias de seguridad de archivos y directorios y Restaurar archivos y directorios se asignan automáticamente al grupo Operadores de copia de seguridad. Por tanto, los miembros de este grupo heredan los derechos de usuario asignados al grupo.

Con Directiva de grupo, puede asignar derechos de usuario a los grupos de seguridad, lo que le ayudará a delegar tareas específicas. Siempre debe asignar las tareas delegadas con discreción, ya que un usuario poco experto al que se le asignen demasiados derechos en un grupo de seguridad podría perjudicar seriamente su red.

5.5 DIRECTIVAS DE TERMINAL SERVER

5.5.1 Configurar servicios de Terminal Server con directiva de grupo. Puede usar Directiva de grupo para configurar conexiones de Servicios de Terminal Server, establecer directivas de usuario, configurar clústeres de servidores Terminal Server y administrar sesiones de Servicios de Terminal Server. Puede habilitar Directiva de grupo para los usuarios de un equipo, para equipos en concreto o para grupos de equipos que pertenezcan a una unidad organizativa de un dominio. Si desea configurar directivas para los usuarios de un equipo determinado, debe ser el administrador del mismo. Si desea configurar directivas para una unidad organizativa en un dominio, debe ser administrador de dicho dominio.

5.5.2 Habilitar directivas de grupo en un equipo en concreto. Si desea configurar directivas de Servicios de Terminal Server para un equipo en particular o para los usuarios de ese equipo, abra el complemento Editor de objetos de directiva de grupo con el fin de modificar la directiva de grupo local.

Cuando abra el complemento Editor de objetos de directiva de grupo, haga clic en Plantillas administrativas para expandirlo y, después, haga clic en la carpeta Servicios de Terminal Server que contenga las directivas que desee establecer. La configuración de esas directivas aparece en el panel de detalles.

Nombre De Directiva Directiva ->Configuración del equipo (o Configuración de usuario) -> Plantillas administrativas/Componentes de Windows -> Servicios de Terminal Server

Para determinar si la directiva está habilitada, deshabilitada o sin configurar, consulte el texto explicativo correspondiente a esa directiva en el complemento Editor de objetos de directiva de grupo.

5.5.3 Habilitar directivas de grupo en una unidad organizativa de un dominio

Si desea establecer directivas de Servicios de Terminal Server para un dominio, debe utilizar un equipo configurado como controlador de dominio y ser administrador de dicho dominio.

Después de configurar el equipo como controlador de dominio, la consola Usuarios y equipos de Active Directory aparece en la carpeta Herramientas administrativas en el menú Programas. Puede utilizar esta herramienta con el fin de establecer directivas para unidades organizativas en el dominio. Antes de comenzar, debe comprobar que la opción Directiva de grupo está seleccionada (en la ficha Extensiones del cuadro de diálogo Agregar o quitar complemento). A continuación, debe confirmar que la extensión Plantillas administrativas (Usuarios) está seleccionada para Directiva de grupo.

Nota: Las directivas de grupo de Servicios de Terminal Server se pueden usar para administrar los equipos donde se use alguno de los sistemas operativos de la familia Windows Server 2003 únicamente.

5.5.4 Introducción a directiva de grupo

Puede abrir el Editor de objetos de directiva de grupo de varias maneras, dependiendo de la acción que desee llevar a cabo y del objeto al que desee (una de las formas es escribir en el menú inicio ejecutar mmc y se abre la siguiente venta ver Fig. Num. 5.2) aplicar la Directiva de grupo.

En este caso agregaremos el editor de objetos de directiva de grupo siga estos pasos:

A) En el menú inicio en damos un clic en ejecutar

B) Escribimos mmc y damos clic en aceptar

C) Al abrir la ventana como se muestra en la Fig. Num. 5.2 entramos en archivo

D) Seleccionamos agregar o quitar complemento damos clic en agregar

E) Seleccionamos editor de objeto de directiva de grupo y agregamos.

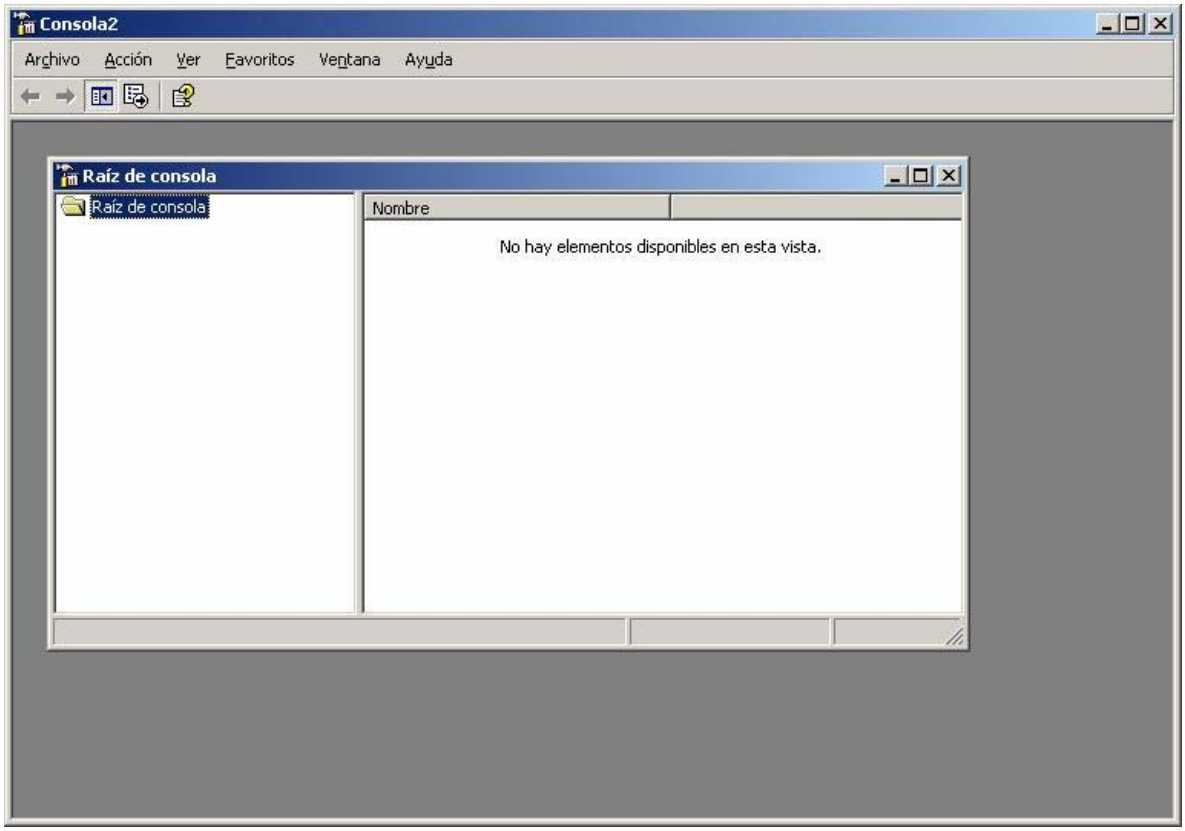


Fig. Num. 5.2

Como se muestra en la Fig. Num.5.3. La configuración de Directiva de grupo define los distintos componentes del entorno de escritorio del usuario que tiene que un administrador del sistema necesita gestionar; por ejemplo, los programas que están disponibles para los usuarios, los programas que aparecen en el escritorio del usuario y las opciones del menú Inicio. Para crear una configuración de escritorio específica para un determinado grupo de usuarios, utilice el Editor de objetos de directiva de grupo.

La configuración de Directiva de grupo que especifique se incluye en un objeto de directiva de grupo, que a su vez está asociado con objetos de Active Directory seleccionados (sitios, dominios o unidades organizativas). La Directiva de grupo

no se aplica sólo a los usuarios y a los equipos clientes, también se aplica a los servidores miembros, los controladores de dominio y otros equipos con Microsoft Windows 2000 que estén en el ámbito de administración. De modo predeterminado, la Directiva de grupo que se aplica a un dominio (es decir, que se aplica en el nivel de dominio, directamente sobre la raíz de Usuarios y equipos de Active Directory) afecta a todos los equipos y usuarios del dominio. Usuarios y equipos de Active Directory también proporciona una unidad organizativa Controladores de dominio integrada. Si guarda ahí sus cuentas de controlador de dominio, puede utilizar el objeto de directiva de grupo Directiva predeterminada de controladores de dominio para administrar los controladores de dominio independientemente de otros equipos.

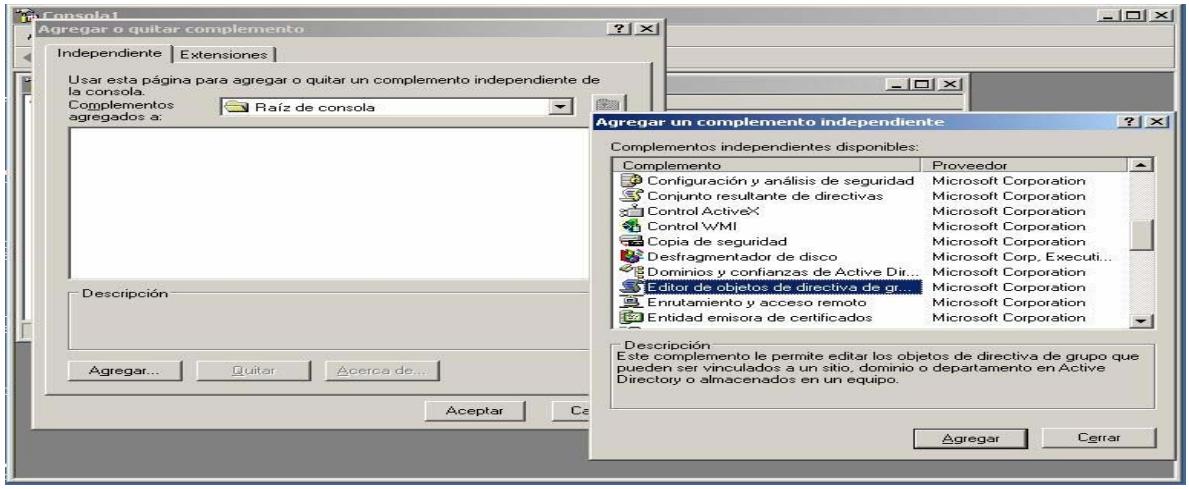


Fig. Num. 5.3

La Directiva de grupo incluye parámetros de directiva para Configuración de usuario, que afecta a los usuarios y para Configuración de equipo, que afecta a los equipos.

5.5.5 Formas de abrir el editor de objetos de directiva de grupo

Equipo local. Para editar un objeto de directiva de grupo local

En el Editor de objetos de directiva de grupo, modifique el objeto de directiva de grupo local;

1. Abra el Editor de objetos de directiva de grupo.

2. En el árbol de la consola, haga doble clic en las carpetas para ver las directivas en el panel de detalles.

3. En el panel de detalles, haga doble clic en una directiva para abrir el cuadro de diálogo Propiedades y, a continuación, cambie la configuración de la directiva.

Nota: Otra forma de abrir el editor de objetos de directiva de grupo es: clic en Inicio, luego en Ejecutar, escriba gpedit.msc y, a continuación, haga clic en Aceptar. Los cambios efectuados en el objeto de directiva de grupo local se guardan automáticamente

Otro Equipo en la red. Abra el objeto de directiva de grupo local que está almacenado en el equipo de red

Para abrir el Editor de objetos de directiva de grupo como complemento MMC

1. Abra Microsoft Management Console.

2. En el menú Archivo, haga clic en Agregar o quitar complemento.

3. En la ficha Independiente, haga clic en Agregar.

4. En la lista Complementos independientes disponibles, haga clic en Editor de objetos de directiva de grupo y, a continuación, haga clic en Agregar.

5. En el cuadro de diálogo Seleccionar un objeto de directiva de grupo, haga clic en Equipo local para modificar el objeto de directiva de grupo local o haga clic en Examinar para buscar el objeto de directiva de grupo que desee modificar.

6. Haga clic en Finalizar, en Cerrar y, a continuación, en Aceptar. El Editor de objetos de directiva de grupo abre el objeto de directiva de grupo para modificarlo.

Notas: Para abrir Microsoft Management Console, haga clic en Inicio, Ejecutar, escriba mmc y, a continuación, haga clic en Aceptar. Si desea guardar una

consola del Editor de objetos de directiva de grupo y elegir el objeto de directiva de grupo que se abre en ella desde la línea de comandos, active la casilla de verificación Permitir que cambie el enfoque del complemento de directivas de grupo cuando se inicie desde la línea de comandos, en el cuadro de diálogo Seleccionar un objeto de directiva de grupo.

A continuación, busque el equipo de red. Debe tener derechos administrativos en el equipo de red.

Sitio. Para abrir el Editor de objetos de directiva de grupo desde Sitios y servicios de Active Directory. Abra el Editor de objetos de directiva de grupo;

1. Abra Sitios y servicios de Active Directory[18]

2. En el árbol de la consola, haga clic con el botón secundario del Mouse (ratón) en el sitio para el que desee establecer la Directiva de grupo.

Nota: 1. Haga clic en Propiedades y, a continuación, en la ficha Directiva de grupo ver Fig. Num. 5.4 en la siguiente pagina.

2. Realice una de estas acciones:

A) Para modificar un objeto de directiva de grupo, haga clic en él y, después, haga clic en Edición.

B) Para crear un objeto de directiva de grupo, haga clic en Nuevo, escriba un nombre para él y, a continuación, haga clic en Edición.

Dominio. Para abrir el Editor de objetos de directiva de grupo desde Usuarios y equipos de Active Directory

[18] • Para abrir Sitios y servicios de Active Directory, haga clic en Inicio, Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Sitios y servicios de Active Directory.

• Puede abrir el Editor de objetos de directiva de grupo de varias maneras, dependiendo de la acción que desee llevar a cabo y del objeto al que desee aplicar la Directiva de grupo. A continuación, vincule un objeto de directiva de grupo al sitio deseado.

1. Abra el Editor de objetos de directiva de grupo, como se muestra en la Sig. Fig.

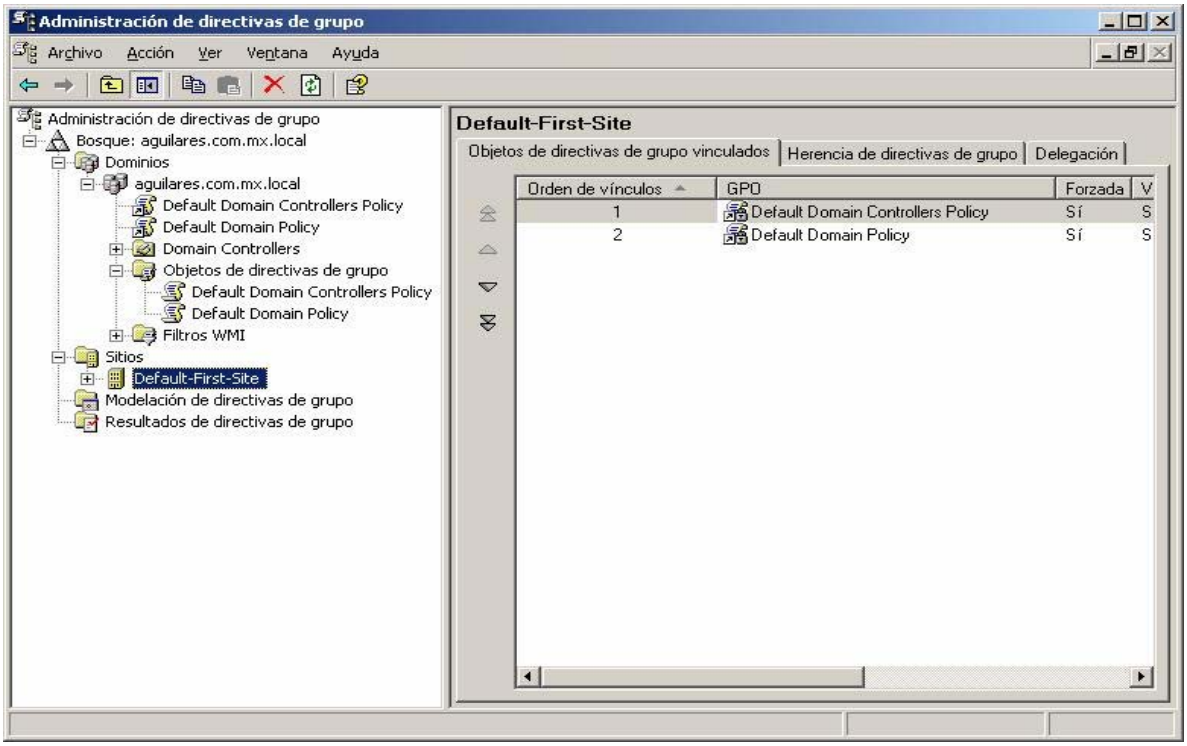


Fig. Num. 5.4

2. Abra Usuarios y equipos de Active Directory.

3. En el árbol de la consola, haga clic con el botón secundario del Mouse en el dominio o unidad organizativa para los que desee establecer la Directiva de grupo.

Nota: Usuarios y equipos de Active Directory ->dominio -> unidad organizativa -> unidad organizativa secundaria

4. Haga clic en Propiedades y, a continuación, en la ficha Directiva de grupo.

5. Realice una de estas acciones:

Para modificar un objeto de Directiva de grupo, haga clic en el objeto y, después, haga clic en Editar.

Para crear un objeto de directiva de grupo, haga clic en Nuevo, escriba un nombre para el nuevo objeto y, a continuación, haga clic en Editar.

Notas: Para abrir Usuarios y equipos de Active Directory, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Usuarios y equipos de Active Directory.

Puede abrir el Editor de objetos de directiva de grupo de varias maneras, dependiendo de la acción que desee llevar a cabo y del objeto al que desee aplicar la Directiva de grupo.

5. A continuación, vincule un objeto de directiva de grupo al dominio deseado.

5.5.6 Unidades organizativas. Para abrir el Editor de objetos de directiva de grupo desde Usuarios y equipos de Active Directory

1. Abra el Editor de objetos de directiva de grupo,

2. Abra Usuarios y equipos de Active Directory.

3. En el árbol de la consola, haga clic con el botón secundario del Mouse en el dominio o unidad organizativa para los que desee establecer la Directiva de grupo.

Nota: Usuarios y equipos de Active Directory ->dominio -> unidad organizativa -> unidad organizativa secundaria

4. Haga clic en Propiedades y, a continuación, en la ficha Directiva de grupo.

5. Realice una de estas acciones:

- Para modificar un objeto de Directiva de grupo, haga clic en el objeto y, después, haga clic en Editar.

- Para crear un objeto de directiva de grupo, haga clic en Nuevo, escriba un nombre para el nuevo objeto y, a continuación, haga clic en Editar.

- Para abrir Usuarios y equipos de Active Directory, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Usuarios y equipos de Active Directory.

- Puede abrir el Editor de objetos de directiva de grupo de varias maneras, dependiendo de la acción que desee llevar a cabo y del objeto al que desee aplicar la Directiva de grupo.

6. A continuación, vincule un objeto de directiva de grupo a la unidad organizativa deseada. También puede vincular un objeto de directiva de grupo a una unidad organizativa que se encuentre en un nivel superior de la jerarquía de Active Directory. De esta forma, la unidad organizativa podrá heredar la configuración de la Directiva de grupo.Si desea establecer directivas de Servicios de Terminal Server para un dominio, debe utilizar un equipo configurado como controlador de dominio y ser administrador de dicho dominio.

Después de configurar el equipo como controlador de dominio, la consola Usuarios y equipos de Active Directory aparece en la carpeta Herramientas administrativas en el menú Programas. Puede utilizar esta herramienta con el fin de establecer directivas para unidades organizativas en el dominio. Antes de comenzar, debe comprobar que la opción Directiva de grupo está seleccionada (en la ficha Extensiones del cuadro de diálogo Agregar o quitar complemento). A continuación, debe confirmar que la extensión Plantillas administrativas (Usuarios) está seleccionada para Directiva de grupo.

Nota: Las directivas de grupo de Servicios de Terminal Server se pueden usar para administrar los equipos donde se use alguno de los sistemas operativos de la familia Windows Server 2003 únicamente.

CAPÍTULO SEXTO

TERMINAL SERVER Y ESCRITORIO REMOTO PARA LA ADMINISTRACION

6.1 SERVICIOS DE TERMINAL SERVER

6.1.1 Introducción a Servicios de Terminal Server. Servicios de Terminal Server proporciona acceso remoto a un escritorio de Microsoft Windows a través de software de cliente ligero, con lo que se permite al equipo cliente actuar como emulador de terminal. Servicios de Terminal Server sólo transmite al cliente la interfaz de usuario del programa. El cliente devuelve las pulsaciones de teclado y los clics de Mouse para ser procesados en el servidor. Los usuarios que inician una sesión sólo ven su sesión, administrada de manera transparente por el sistema operativo del servidor e independiente de cualquier otra sesión de cliente. El software de cliente puede ejecutarse en varios dispositivos hardware de cliente, incluidos equipos y terminales basados en Windows. Otros dispositivos, como los equipos Macintosh o las estaciones de trabajo que usan UNIX, también pueden usar software de otros proveedores para conectar con un servidor Terminal Server.

Servicios de Terminal Server es la tecnología subyacente en varias de las características y componentes de los sistemas operativos de la familia Microsoft Windows Server™ 2003. Por ejemplo, Terminal Server y Escritorio remoto para administración.

Terminal Server permite distribuir de una manera eficaz y confiable programas basados en Windows con un servidor de red. Con esta herramienta, desde un único lugar de instalación varios usuarios pueden tener acceso al escritorio de un servidor que ejecute alguno de los sistemas operativos de la familia Windows Server 2003. Los usuarios pueden ejecutar programas, guardar archivos y usar recursos de red como si estuvieran sentados ante el equipo. Los Servicios de

Terminal Server en modo de administración remota, proporciona acceso remoto al escritorio de un equipo donde se use alguno de los sistemas operativos de la familia Windows Server 2003, con lo que se permite al usuario administrar su servidor, incluso un servidor Microsoft Windows 2000, desde prácticamente cualquier equipo de la red.

6.1.2 Servicios de Terminal Server.

Ventajas de los servicios de Terminal Server

- Lleva al escritorio los sistemas operativos de la familia Windows Server 2003 con mucha más rapidez.

- Servicios de Terminal Server sirve como comodín en la migración de los escritorios antiguos a Microsoft Windows XP Professional, al ofrecer en los equipos donde se usan versiones anteriores de Windows una apariencia de escritorio similar a la de los sistemas operativos de la familia Windows Server 2003.

- Hay disponibles clientes de Servicios de Terminal Server para numerosas plataformas de escritorio diferentes incluidas Microsoft MS-DOS, terminales que usan Windows, Macintosh y UNIX. Además, una versión basada en el Web del cliente de Servicios de Terminal Server (Conexión a Escritorio remoto) ofrece la capacidad de conexión de Servicios de Terminal Server a los equipos que disponen de acceso al Web y un explorador Internet Explorer.

- Aprovecha al máximo el hardware existente. Servicios de Terminal Server amplía el modelo de computación distribuida al permitir a los equipos operar simultáneamente como clientes ligeros y como equipos personales con toda clase de características.

- Los equipos pueden seguir siendo usados para la función que venían desempeñando en las redes existentes y, a la vez, como clientes ligeros capaces de emular el escritorio de Windows XP Professional.

- Implementación centralizada de programas. Con Terminal Server, todas las tareas de ejecución de programas y procesamiento y almacenamiento de datos se llevan a cabo en el servidor, lo que permite centralizar la implementación de los programas. Terminal Server garantiza que todos los clientes puedan tener acceso a la misma versión de un programa. El software se instala sólo una vez en el servidor, en lugar de en todos los escritorios de la organización, lo que reduce los costos que implica la actualización de equipos individuales.

Características de los servicios de Terminal Server.

- Terminal Server proporciona a equipos remotos acceso a programas para Windows que se ejecutan en Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition o Windows Server 2003, Datacenter Edition.

- Con Terminal Server puede proporcionar un lugar de instalación único que permita el acceso de más de un usuario a cualquier equipo donde se use alguno de estos productos.

- Los usuarios pueden ejecutar programas, guardar archivos y utilizar recursos de red desde una ubicación remota como si dichos recursos estuvieran instalados en su propio equipo.

- **Acceso remoto a las aplicaciones**. Terminal Server envía del servidor al cliente la pantalla de la aplicación, en lugar de sus datos. Esto significa que es posible proporcionar a los usuarios acceso a aplicaciones que usan una gran cantidad de datos a través de conexiones con poco ancho de banda (por ejemplo, una conexión de acceso telefónico a 28800 bps) y proporcionar un rendimiento superior al que se obtendría sin Terminal Server.

- **Acceso a una única aplicación**. Terminal Server puede proporcionar a los usuarios acceso a una única aplicación publicada si no se requiere acceso a un escritorio completo de Windows XP.

- **Administrador de Servicios de Terminal Server**. Con el Administrador de Servicios de Terminal Server puede ver información de los servidores Terminal Server en los dominios de confianza. Esta información incluye todas las sesiones, los usuarios y los procesos de cada servidor Terminal Server. También puede utilizar esta utilidad para realizar diversas acciones de administración del servidor.

- **Control remoto**. Servicios de Terminal Server proporciona control remoto integrado a la familia Windows Server 2003.

- **Redirección de audio**. La redirección de audio permite la reproducción de sonido en un equipo cliente con cualquier aplicación que intente reproducir sonido de onda en una sesión de Terminal Server. Esta característica proporciona capacidades básicas de audio, por ejemplo, para los archivos .wav adjuntos en mensajes de correo electrónico, documentos o multimedia simple de transmisión por secuencias.

- **Integración de directivas de grupo**. Terminal Server está integrado con Directiva de grupo, lo que permite utilizar funciones de redirección, acceso mediante contraseñas y configuración de papeles tapiz para administrar el modo en que se utiliza un servidor con Terminal Server habilitado.

- **Mejoras en la resolución y en el color**. A partir de ahora, Servicios de Terminal Server, la tecnología subyacente de Terminal Server, admite un mayor número de colores y una mayor resolución de pantalla. Mediante Conexión a escritorio remoto se puede configurar el número de colores desde 256 hasta Color verdadero, y la resolución desde 640 × 480 píxeles hasta el máximo admitido por los dispositivos de vídeo del cliente. Deben habilitarse límites de resolución y de color tanto en el servidor como en el cliente.

6.2 Licencias de Terminal Server.

Se requiere una licencia válida emitida por un servidor de licencias de Terminal Server para que un cliente pueda iniciar una sesión en un servidor Terminal Server.

El método de Licencias de Terminal Server es independiente del método de concesión de licencias utilizado por los clientes de sistemas operativos Microsoft® Windows Server 2003.

Un servidor de licencias almacena las licencias de todos los clientes. Un servidor Terminal Server debe ser capaz de conectarse con un servidor de licencias activado para poder emitir licencias definitivas a los clientes. Al activar un servidor de licencias, Microsoft proporciona al servidor un certificado digital que valida su propiedad e identidad. Mediante este certificado, el servidor de licencias puede realizar transacciones con Microsoft y recibir licencias de cliente para los servidores Terminal Server. Si instala un servidor de licencias pero no lo activa, ese servidor sólo emite licencias temporales.

En implementaciones pequeñas, es aceptable instalar en el mismo equipo físico tanto el servidor Terminal Server como Licencias de Terminal Server. Sin embargo, en implementaciones mayores, considere instalar Licencias de Terminal Server en un servidor independiente. Observe que un servidor de licencias puede atender simultáneamente a varios servidores.

Debe configurar Licencias de Terminal Server correctamente para que el servidor Terminal Server siga aceptando conexiones de los clientes. Para que tenga tiempo de sobra para implementar un servidor de licencias, Terminal Server proporciona un período de gracia para la licencia durante el que no se requiere un servidor de licencias. Durante este período de gracia, un servidor Terminal Server puede aceptar conexiones de clientes sin licencia sin tener que ponerse en contacto con un servidor de licencias. El período de gracia comienza la primera vez que el servidor Terminal Server acepta una conexión de un cliente. Finaliza cuando se implementa un servidor de licencias y éste emite su primera licencia de acceso de

cliente (CAL)[19] definitiva o una vez transcurridos 120 días, depende de lo que se produzca antes.

Antes de instalar el servidor de licencias, debe determinar cuál de las dos funciones necesita: un servidor de licencias de dominio o un servidor de licencias empresarial. De forma predeterminada, un servidor de licencias se instala como servidor de licencias empresarial.

Después de instalar el servidor de licencias, debe activarlo e instalar licencias CAL mediante el Asistente para activación de servidor de licencias de Terminal Server.

6.2.1 Activar un servidor de licencias de Terminal Server. Debe activar un servidor de licencias de Termina Server, y luego adquirir e instalar el número adecuado de licencias de acceso de cliente (CAL) antes de que el servidor de licencias pueda emitir CAL permanentes a los clientes del servidor Terminal Server. Un servidor de licencias instalado pero no activado sólo emite licencias temporales. Estas licencias temporales permiten a los clientes conectarse al servidor de Terminal Server durante 90 días.

De otra forma tenemos que adquirir las licencias[20] Para activar un servidor de licencias, utilice Licencias de Terminal Server. Al activar un servidor de licencias, el Centro de activación de Microsoft (Clearinghouse) proporciona al servidor un certificado digital X.509 que valida la propiedad e identidad del servidor. Mediante este certificado, el servidor de licencias puede posteriormente realizar transacciones con el Centro de activación de Microsoft y recibir CAL permanentes para sus servidores Terminal Server. Para activar el servidor de licencias valla a el menú inicio -> Herramientas Administrativas -> Licencias de Terminal Server -> seleccionamos el servidor que queremos activar -> Clic en el menú acción ->

[19] Client Access License
[20] (comprarlas) en Microsoft (http://go.microsoft.com/fwlink/?LinkID=26223)

Activar el servidor de licencias. En la siguiente pagina Fig. Num. 6.1 muestra donde se activa el servidor de licencias.

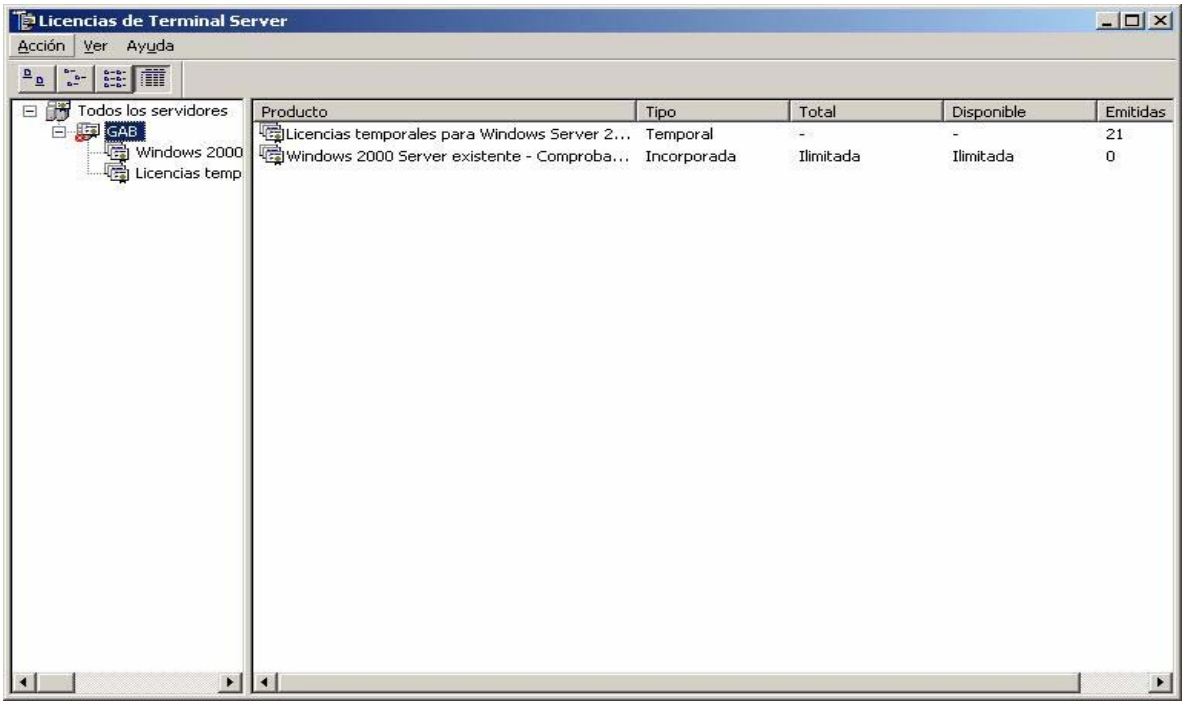


Fig. Num. 6.1

La información que se suministra al Centro de activación de Microsoft (Clearinghouse) a través de Internet o World Wide Web se cifra como medida de seguridad y se almacena de forma segura en una base de datos dedicada del Centro de activación de Microsoft. Esta información no se mezcla con ninguna otra información que pueda haber facilitado a Microsoft en otros contextos y no se muestra a terceros.

6.2.2 Equilibrio de carga y servidores Terminal Server. Equilibrio de carga sondea los recursos de procesamiento de diversos servidores mediante el protocolo de red TCP/IP. Puede utilizar este servicio con un clúster de servidores Terminal Server para distribuir las sesiones en varios servidores y con ello escalar el rendimiento de un único servidor Terminal Server. Directorio de sesión, incluido en Windows Server 2003, Enterprise Edition y Windows Server 2003, Datacenter Edition, permite controlar las sesiones desconectadas del clúster y garantiza que los usuarios se vuelvan a conectar a dichas sesiones.

6.3 ADMINISTRACIÓN DE CONEXIONES DE SERVICIOS DE TERMINAL SERVER

Administración de conexiones de Servicios de Terminal Server trabaja con el servicio de equilibrio de carga que se utilice para asegurar que los usuarios se vuelven a conectar al servidor original que aloja sus sesiones de Terminal Server desconectadas sin que se aperciban de ello. Los componentes de Administración de conexiones de Servicios de Terminal Server son:

- Una solución de equilibrio de carga de red (Equilibrio de carga de red, operación por turnos Sistema de nombres de dominio (DNS) u otra solución de terceros).

- Dos o más servidores Terminal Server, agrupados lógicamente en un clúster de Terminal Server.

- Un servidor de directorio de sesión. Este equipo puede ser cualquiera que ejecute Windows Server 2003, Enterprise Edition o Windows Server 2003, Datacenter Edition, que sea visible en la red y ejecute el servicio Directorio de sesión de Servicios de Terminal Server. Se recomienda que el servidor de directorio de sesión tenga una gran disponibilidad en la red y no ejecute Terminal Server.

El proceso de Administración de conexiones de Terminal Server es el siguiente:

- Cuando un usuario inicia sesión en el clúster de servidores Terminal Server, el servidor que recibe la solicitud del cliente envía una consulta al servidor de directorio de sesión.

- El servidor de directorio de sesión comprueba el nombre de usuario en su base de datos y envía el resultado al servidor que realiza la solicitud.

- Si el usuario no tiene sesiones desconectadas, el inicio de sesión continúa en el servidor que contiene la conexión inicial.

- Si el usuario tiene una sesión desconectada en otro servidor, la sesión del cliente se pasa a ese servidor y el proceso de inicio de sesión continúa.

- Cuando el usuario inicia sesión en la sesión desconectada, se actualiza el directorio de sesión.

6.3.1 Directorio de sesión de servicios de Terminal Server. El servicio Directorio de sesión de Servicios de Terminal Server es una base de datos que contiene las sesiones en servidores Terminal Server de un clúster y proporciona la información utilizada en el momento de la conexión para conectar a los usuarios con las sesiones existentes.

Cuando se inicia el servicio Directorio de sesión, crea el grupo local "Equipos de directorio de sesión". De manera predeterminada, este grupo no está rellenado. Debe elegir los equipos o grupos que desea que participen en el servicio Directorio de sesión y Cambiar la pertenencia a grupos manualmente al grupo Equipos de Directorio de sesión.

6.4 APLICACIONES DE GRUPOS ACTIVE DIRECTORY

A) Para agregar o quitar un miembro de un grupo de Active Directory

1. Abra Usuarios y equipos de Active Directory.

2. En el árbol de la consola, haga doble clic en el nodo de dominio.

3. Haga clic en la carpeta que contenga el grupo al que desea agregar o quitar un miembro.

4. En el panel de detalles, haga clic con el botón secundario del Mouse en el grupo y después en Propiedades.

5. Haga clic en la ficha Miembros y, a continuación, realice una de las acciones siguientes:

Para agregar un miembro a un grupo, haga clic en Agregar. En Escriba los nombres de objeto que desea seleccionar, escriba el nombre del usuario, grupo o equipo que desee agregar al grupo y, después, haga clic en Aceptar.

Para quitar un miembro de un grupo, haga clic en el miembro que desee quitar y, después, en Quitar.

Nota: Para llevar a cabo este procedimiento, debe ser miembro del grupo Operadores de cuentas, del grupo Administradores de dominio o del grupo Administradores de organización de Active Directory, o bien debe tener delegada la autoridad correspondiente. Como práctica recomendada de seguridad, considere la posibilidad de utilizar la opción Ejecutar como para realizar este procedimiento. La figura 6.2 muestra como podemos quitar los miembros de un grupo de Active Directory .

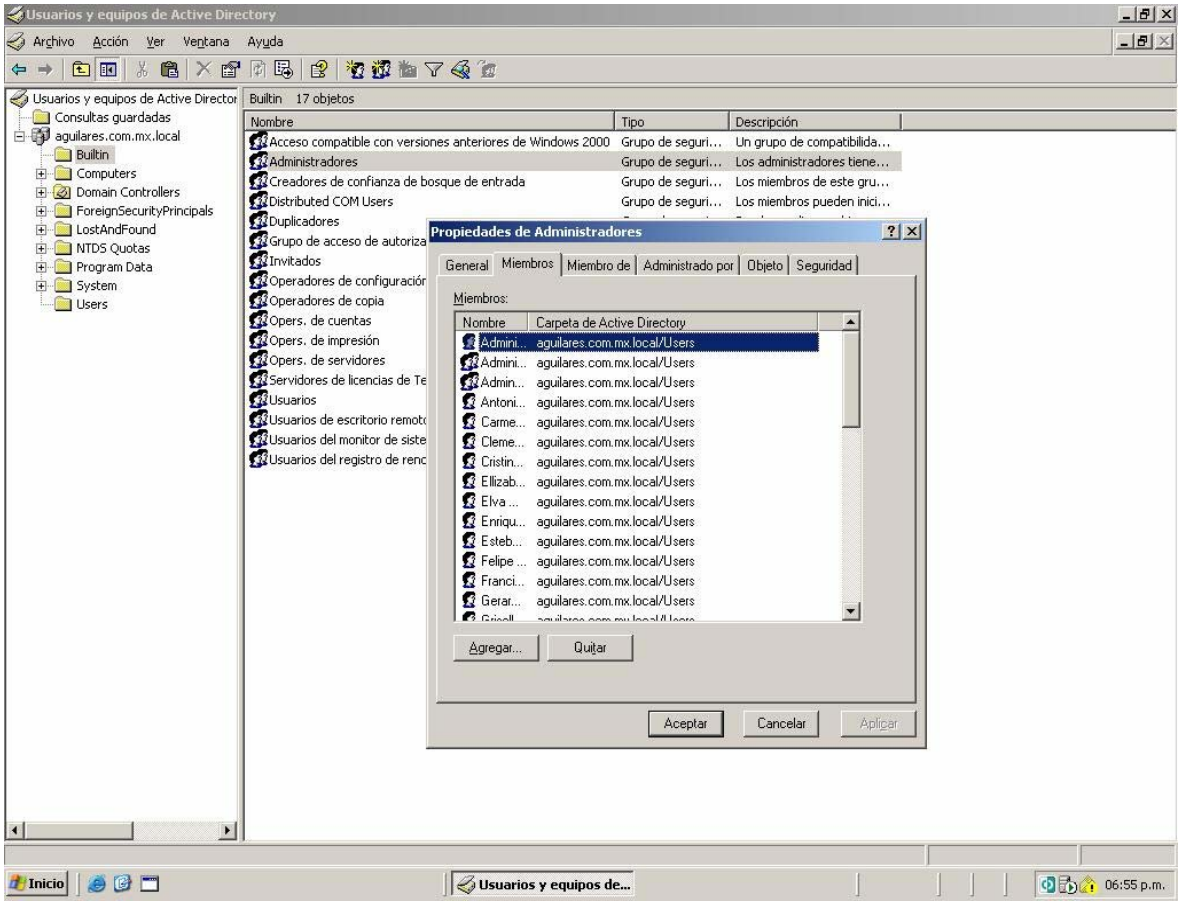


Fig. Num. 6.2

B) Para agregar o quitar un miembro de un grupo en un equipo local

1. Abra Administración de equipos[21].

2. En el árbol de la consola, haga clic en **Grupos**.

Notas: Administración de equipos -> Herramientas del sistema -> Usuarios y grupos locales -> Grupos

Haga clic con el botón secundario del Mouse en el grupo al que desea agregar o del que desea quitar un miembro y haga clic en Propiedades.

Realice una de las acciones siguientes:

Para agregar un miembro a un grupo, haga clic en Agregar. En Escriba los nombres de objeto que desea seleccionar, escriba el nombre del usuario, grupo o equipo que desee agregar al grupo y, después, haga clic en Aceptar.

Para quitar un miembro de un grupo, haga clic en el miembro que desee quitar y, después, en Quitar.

C) Para iniciar el servicio Directorio de sesión

1. Abra Servicios.[22] Como se muestra en la Fig. Num. 6.3

2. Haga doble clic en Propiedades de directorio de sesión de Servicios de Terminal Server.

[21] Para abrir Administración de equipos, haga clic en **Inicio**, en **Panel de control**, haga doble clic en **Herramientas administrativas** y, a continuación, haga doble clic en **Administración de equipos**.
[22] Para abrir el complemento Servicios manualmente, haga clic en **Inicio**, elija **Herramientas administrativas** y, a continuación, haga clic en **Servicios**.

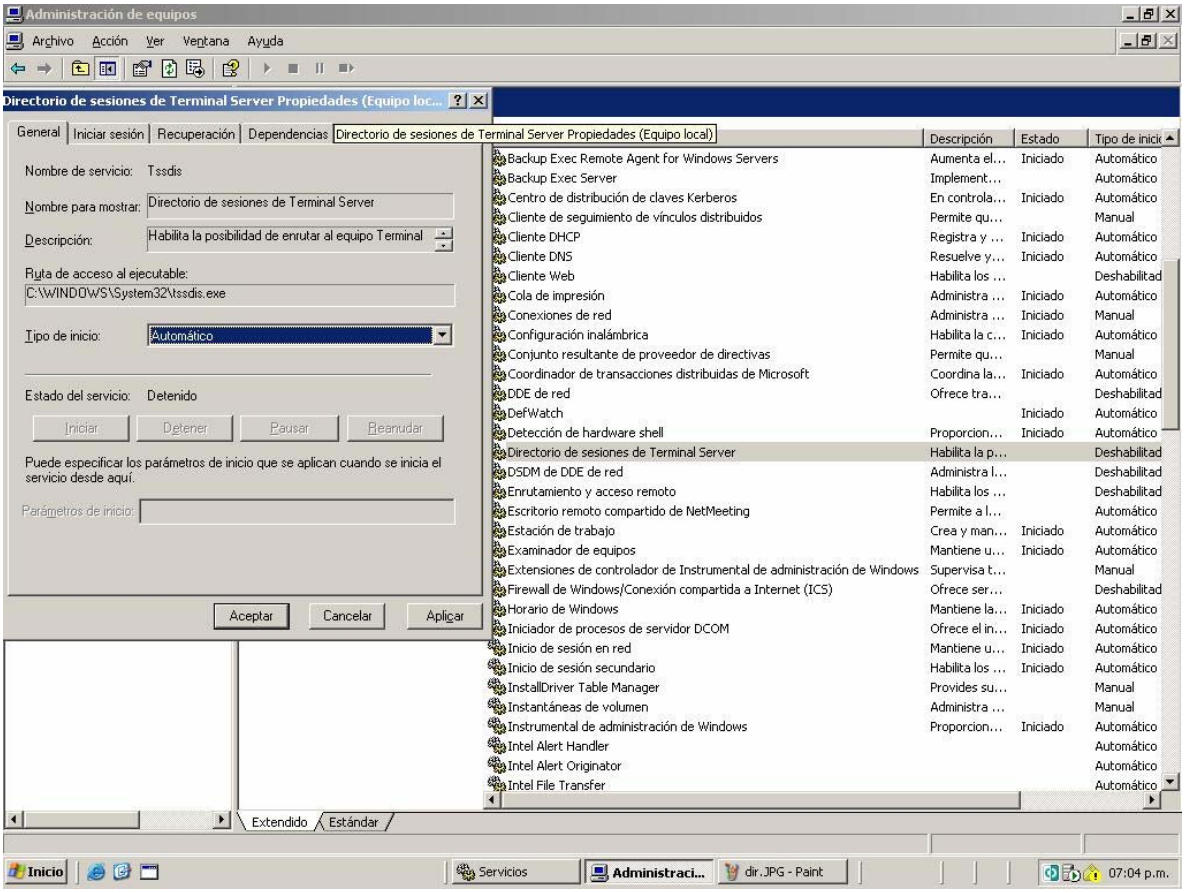


Fig. Num. 6.3

3. Para iniciar el servicio, haga clic en Iniciar. Para asegurarse de que el servicio se ejecute siempre que el servidor se inicie, en Tipo de inicio, haga clic en Automático.

D) Para crear un clúster de Terminal Server

1. Abra el objeto de directiva de grupo correspondiente a la unidad organizativa que contenga los servidores Terminal Server que vayan a participar en el clúster.

2. En Plantillas administrativas, en la carpeta Componentes de Windows/Servicios de Terminal Server/Directorio de sesión, habilite la opción Directorio de sesión activo.

3. En la opción Servidor de directorio de sesión, haga clic en Habilitar, escriba el nombre del servidor donde se ejecute el servicio Directorio de sesión y haga clic en aceptar.

4. En la opción Nombre del clúster de directorio de sesión, haga clic en Habilitar, especifique un nombre para este clúster de Terminal Server y haga clic en aceptar.

6.5 APLICACIONES PARA CONFIGURAR TERMINAL SERVER

A) Para instalar **Terminal Server**

1. Abra el Asistente para configurar su servidor.

2. Haga clic en Siguiente y siga las instrucciones que aparecerán en la pantalla Pasos preliminares.

3. Haga clic en Siguiente y, en la pantalla Función del servidor, seleccione Terminal Server.

4. Haga clic en Siguiente y siga las instrucciones del asistente.

5. Algunos programas podrían no funcionar correctamente cuando se instala Terminal Server. Si es así, una vez instalado Terminal Server, debe reinstalar todos estos programas mediante Agregar o quitar programas para el acceso en múltiples sesiones.

En la siguiente pagina Fig. Num. 6.4. Muestra donde se configura un servidor de Terminal Server.

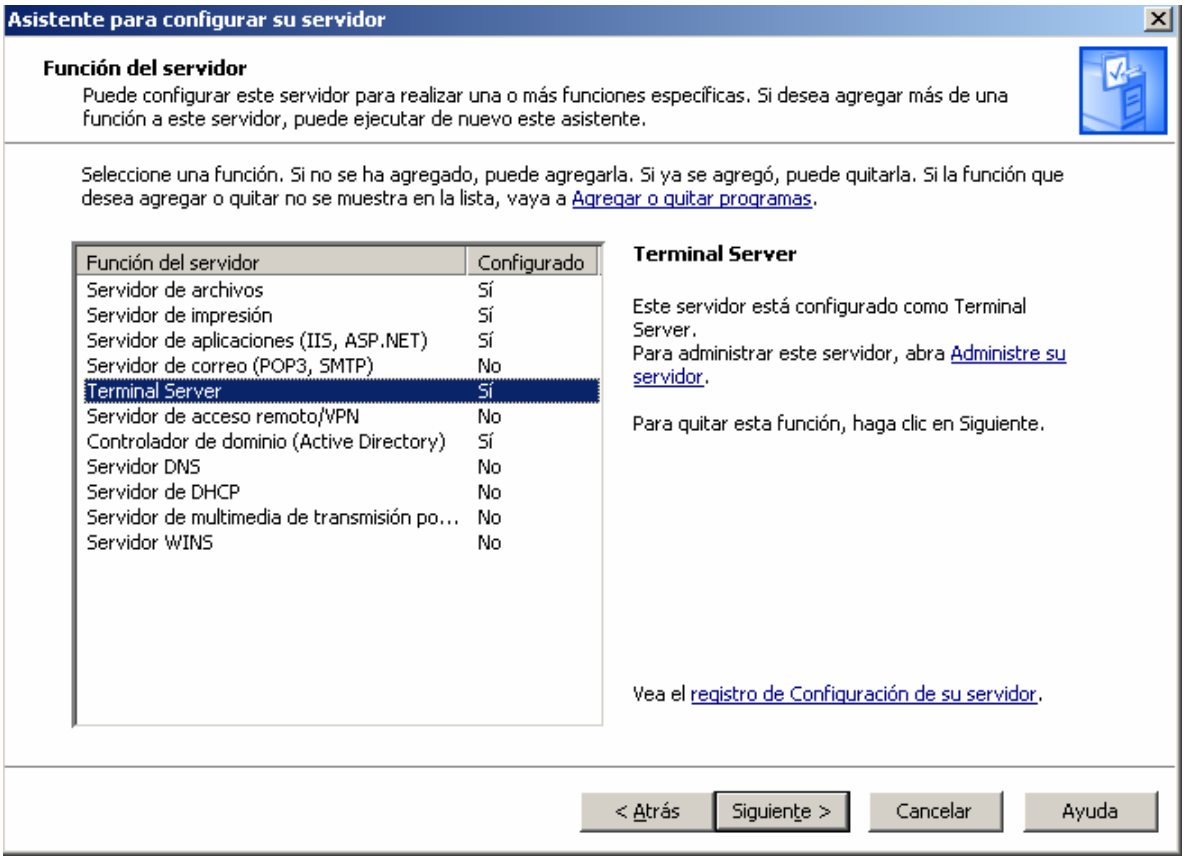


Fig. Num. 6.4

B) Para Instalar los servicios de **Terminal Server**

1. En el panel de control -> Agregar y quitar programas
2. En el botón agregar y quitar componentes
3. Seleccionar Terminal Server

C) Como Instalar el servidor de licencias

1. En el panel de control/Agregar y quitar programas
2. En el botón agregar y quitar componentes
3. Seleccionar Servidor de Licencias de Terminal Sever

6.6 APLICACIONES PARA TRABAJAR CON SERVIDORES TERMINAL SERVER

A) Para conectar con servidores **Terminal Server**

1. Abra Administrador de Servicios de Terminal Server.[23]

2. Expanda el dominio que contenga los servidores a los que desee conectarse, come se muestra en la Fig. Num. 6.5

3. Realice una de las acciones siguientes:

Para conectarse a un servidor Terminal Server específico, haga clic con el botón secundario del Mouse en él y, a continuación, haga clic en Conectar.

Para conectarse a un equipo que no aparezca en el panel de exploración del complemento Escritorios remotos, haga clic con el botón secundario del Mouse en Todos los servidores enumerados, haga clic en Conectarse al equipo, especifique el nombre de un equipo y, después, haga clic en Aceptar.

[23] Para abrir el Administrador de Servicios de Terminal Server, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Administrador de Servicios de Terminal Server.
Sólo debería conectarse a un servidor Terminal Server cada vez. Cuando un servidor se conecta, el Administrador de Servicios de Terminal Server consulta información acerca de sus sesiones y procesos. La conexión de más de un servidor cada vez podría sobrecargar los recursos del sistema.

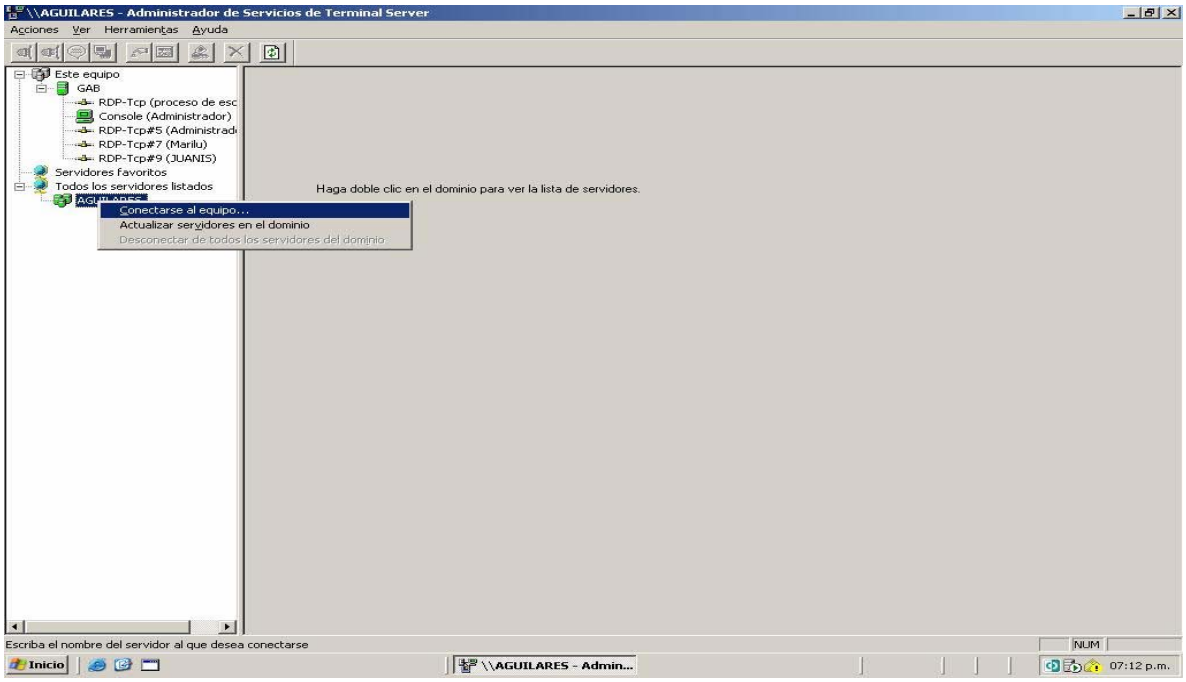


Fig. Num. 6.5

B) Para desconectarse de servidores **Terminal Server**

1. Abra Administrador de Servicios de Terminal Server.[24]

2. Expanda el dominio que contenga los servidores de los que desee desconectarse.

3. Realice una de las acciones siguientes:

Para desconectarse de un servidor de Terminal Server específico, haga clic con el botón secundario del Mouse en él y, a continuación, haga clic en Desconectar.

[24] Para abrir el Administrador de Servicios de Terminal Server, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Administrador de Servicios de Terminal Server.
Para desconectarse de todos los servidores de todos los dominios de la red, haga clic con el botón secundario del Mouse en Todos los servidores listados y, a continuación, haga clic en Desconectar de todos los servidores.

Para desconectarse de todos los servidores de Terminal Server del dominio, haga clic con el botón secundario del Mouse en el dominio y, a continuación, haga clic en Desconectar de todos los servidores del dominio.

C) Para buscar todos los servidores **Terminal Server** de un dominio

1. Abra Administrador de Servicios de Terminal Server.[25]

2. Haga clic con el botón secundario Mouse en los servidores Terminal Server que desee buscar y, a continuación, haga clic en Buscar servidores en el dominio.

D) Para agregar un servidor **Terminal Server** a la lista Favoritos

1. Abra Administrador de Servicios de Terminal Server.

2. Expanda el dominio que contenga el servidor que desee agregar a la lista Favoritos.

3. Haga clic con el botón secundario del Mouse (ratón) en el servidor y, después, haga clic en Agregar a Favoritos.

E) Para quitar un servidor **Terminal Server** de la lista Favoritos

1. Abra Administrador de Servicios de Terminal Server.

2. Expanda el nodo Servidores favoritos.

3. Haga clic con el botón secundario del Mouse (ratón) en el servidor y, después, haga clic en Quitar de Favoritos.

---

[25] Para abrir el Administrador de Servicios de Terminal Server, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Administrador de Servicios de Terminal Server.
En función del número de servidores de la red, esto puede suponer un lapso prolongado de tiempo.

6.7 APLICACIÓN PARA ADMINISTRAR CLIENTES

A) Como desconectar una sesión de un cliente

1. En el servidor de Terminal Server Inicio/Herramientas Administrativas/Administrador de servicios de Terminal Server
2. En el menú despegable en la cadena Todos los servidores listados
3. Escoger el servidor de Terminal Server
4. En la ventana derecha en la ficha usuarios seleccionar el usuario con un click derecho y seleccionar desconectar

B) Como Cerrar y Terminar una sesion de un cliente

1. En el servidor de Terminal Server Inicio/Herramientas Administrativas/Administrador de servicios de Terminal Server
2. En el menú despegable en la cadena Todos los servidores listados
3. Escoger el servidor de Terminal Server
4. En la ventana derecha en la ficha usuarios seleccionar el usuario con un click derecho y seleccionar Cerrar Sesion

D) Como Cerrar un Proceso Especifico de un Cliente

1. En el servidor de Terminal Server Inicio/Herramientas Administrativas/Administrador de servicios de Terminal Server
2. En el menú despegable en la cadena Todos los servidores listados
3. Escoger el servidor de Terminal Server
4. En la ventana derecha en la ficha procesos seleccionar el proceso con un click derecho y seleccionar Terminar Proceso.

6.8 APLICACIÓN PARA ADMINISTRAR USUARIOS, SESIONES Y PROCESOS

A) Para conectar con otra sesión

A) Abra Administrador de Servicios de Terminal Server.

2. Haga clic con el botón secundario en la sesión con la que desee conectar y,

3. A continuación, haga clic en Conectar.

4. Se conectará a una nueva sesión y se desconectará de la anterior.

Notas: Siempre podrá conectarse a una sesión que haya iniciado con la misma cuenta de usuario. Para conectarse a la sesión de otro usuario, debe tener los permisos Control total o Acceso de usuario.

Sólo es posible conectarse a una sesión desde otra. Para poder conectarse a otra sesión debe abrir el Administrador de Servicios de Terminal Server o utilizar el comando tscon desde una sesión.

Sólo es posible conectarse a una sesión que esté en modo activo o desconectado.

No es posible conectarse a otra sesión desde la sesión de consola.

B) Para desconectarse de una sesión

1. Abra Administrador de Servicios de Terminal Server.
2. Haga clic con el botón secundario del Mouse en la sesión de la que desee desconectarse y, después, haga clic en Desconectar.

Notas: Siempre puede desconectarse de sus propias sesiones; sin embargo, para desconectar una sesión perteneciente a otro usuario necesita el permiso Control total.

Para abrir el Administrador de Servicios de Terminal Server, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Administrador de Servicios de Terminal Server.

Una vez desconectada, la sesión permanece abierta en el servidor Terminal Server en estado desconectado y las aplicaciones que se estuvieran ejecutando siguen haciéndolo. Las aplicaciones continuarán ejecutándose hasta que la sesión vuelva a conectarse, sin perderse datos.

También puede utilizar el comando tsdiscon para desconectarse de una sesión.

Puede restablecer una sesión que se encuentra en estado de desconexión, con lo que la elimina del servidor. Debe tener permiso Control total para ello.

C) Para cerrar la sesión de un usuario

1. Abra Administrador de Servicios de Terminal Server.

   En la ficha Usuarios, haga clic con el botón secundario del Mouse (ratón) en el usuario cuya sesión desee cerrar y, a continuación, haga clic en Cerrar sesión.

Precaución:

Si se cierra la sesión de un usuario sin advertir primero, se puede causar la pérdida de los datos en dicha sesión. Para advertir al usuario antes de tomar esta medida, debe enviarle un mensaje mediante Enviar mensaje en el menú Acciones.

Notas: Siempre puede cerrar sus propias sesiones, pero para cerrar sesiones de otros usuarios debe tener el permiso Control total.

Para abrir el Administrador de Servicios de Terminal Server, haga clic en Inicio, en Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en Administrador de Servicios de Terminal Server. Cuando se cierra la sesión de un usuario, terminan todos los procesos y la sesión se elimina del servidor.

D) Para enviar un mensaje a un usuario[26]

1. Abra Administrador de Servicios de Terminal Server.

2. Haga clic con el botón secundario del Mouse en la sesión o usuario a los que desee enviar el mensaje y, a continuación, haga clic en Enviar mensaje Aparecerá el cuadro de diálogo Enviar mensaje.
3. En Título del mensaje, escriba el título del mensaje.
4. En Mensaje, escriba la información que desee enviar al usuario. Para iniciar un párrafo, presione CTRL+ENTRAR.
5. Para enviar el mensaje, haga clic en Aceptar.

E) Para restablecer una sesión[27]

1. Abra Administrador de Servicios de Terminal Server.

2. Haga clic con el botón secundario del Mouse en la sesión que desee restablecer y, después, haga clic en Restablecer. Las sesión se elimina inmediatamente del servidor.

F) Para ver la información de estado de una sesión

1. Abra Administrador de Servicios de Terminal Server.

---

[26] Utilice esta característica para notificar a los usuarios la desconexión inminente, el estado de los servidores u otra información del sistema.
Sólo puede enviar mensajes a usuarios cuyas sesiones estén activas o conectadas, incluida la sesión de la consola.
También puede utilizar el comando msg para enviar mensajes a usuarios.

[27] Siempre puede restablecer sus propias sesiones, pero para restablecer una sesión perteneciente a otro usuario necesita el permiso Control total.
Tenga en cuenta que, si se restablece la sesión de un usuario sin advertir primero, se puede causar la pérdida de datos en la sesión.
Sólo debe restablecer una sesión en caso de funcionamiento anómalo o cuando parezca que se ha bloqueado.
Si restablece una sesión de escucha, se restablecerán todas las sesiones que utilizan la conexión.
También puede utilizar el comando reset session para restablecer una sesión.
No es posible ver información de estado de las sesiones de consola o de escucha.

2. Haga clic con el botón secundario del Mouse en la sesión cuya información de estado desee consultar y, a continuación, haga clic en Estado. Se presenta la información de Estado correspondiente a la sesión.
3. Para actualizar esta información, haga clic en Actualizar ahora.
4. Para restablecer los contadores, haga clic en Restablecer contadores.

Notas: Siempre puede ver la información de estado de sus propias sesiones. Para ver información de estado de una sesión que pertenezca a otro usuario, debe tener los permisos Control total o Acceso de usuario, o asignársele específicamente el permiso avanzado Consulta de información.

G) Para controlar de forma remota una sesión

1. Abra Administrador de Servicios de Terminal Server.

2. Haga clic con el botón secundario del Mouse (ratón) en la sesión que desee supervisar y, después, haga clic en Control remoto. Aparecerá el cuadro de diálogo Control remoto.
3. En Tecla de acceso rápido, seleccione las teclas que desee utilizar para terminar una sesión de control remoto y, después, haga clic en Aceptar. La tecla de acceso rápido predeterminada es CTRL+* (utilice la tecla * del teclado numérico).

Notas: Cuando desee terminar el control remoto, presione CTRL+* (u otra tecla de acceso rápido que haya definido).

Debe disponer del permiso Control total para controlar de forma remota otras sesiones.

Para configurar el control remoto para una conexión, utilice Configuración de Servicios de Terminal Server. El control remoto también se puede configurar en función de cada usuario con la extensión de Servicios de Terminal Server a Usuarios y grupos locales, y Usuarios y equipos de Active Directory.

Antes de comenzar la supervisión, el servidor informa al usuario de que la sesión se va a controlar de forma remota, a menos que se deshabilite esta advertencia. Es posible que la sesión parezca detenida durante algunos segundos mientras espera la respuesta del usuario.

Al entrar en la sesión de control remoto, la sesión actual comparte todas las entradas y salidas con la sesión que está supervisando.

Su sesión debe ser capaz de admitir la resolución de vídeo utilizada en la sesión que se controle de forma remota o, de lo contrario, se producirá un error en la operación.

La sesión de consola no puede controlar de forma remota otra sesión ni puede ser controlada de forma remota por otra sesión.

También puede utilizar el comando shadow para controlar de forma remota otra sesión.

H) Para terminar un proceso[28]

1. Abra Administrador de Servicios de Terminal Server.
2. En la ficha Procesos, en la columna Usuario, haga clic con el botón secundario del Mouse (ratón) en el proceso que desee terminar y, a continuación, haga clic en Terminar el proceso .

Notas: Debe tener permiso Control total para terminar un proceso.

Tenga en cuenta que terminar un proceso sin advertir primero puede causar la pérdida de datos en la sesión del usuario.

Puede que necesite terminar un proceso debido a que la aplicación no responde.

[28] También puede utilizar el comando tskill para terminar un proceso.

6.9 VENTAJAS DE ESCRITORIO REMOTO PARA ADMINISTRACIÓN

A) Administración remota. Escritorio remoto para administración de Servicios de Terminal Server permite la administración remota de Windows Server 2003, lo que ofrece a los administradores del sistema un método para administrar de forma remota su servidor desde cualquier cliente mediante una conexión LAN, WAN o de acceso telefónico. Se puede tener acceso simultáneamente hasta a dos sesiones remotas, más la de consola. Para usar esta característica no se requiere una licencia de Terminal Server.

B) Conexión a Escritorio remoto. Con Conexión a Escritorio remoto puede conectarse fácilmente a un servidor Terminal Server o a cualquier equipo que ejecute Escritorio remoto. Sólo necesita acceso y permisos de red para conectarse al otro equipo. De forma opcional, puede especificar una configuración especial para la conexión y, a continuación, guardarla para la próxima vez que se conecte.

CAPÍTULO SÉPTIMO

APLICACIÓN PARA ESTABLECER UNA CONEXIÓN REMOTA A UNA PC, LAN Y WAN Y SU GESTION REMOTA

En este capítulo veremos los procedimientos para establecer una conexión remota a una PC, LAN, WAN.

7.1 CONECTARSE A UNA PC REMOTAMENTE

Debemos de habilitar los servicios de acceso remoto

1. Click derecho sobre el icono de PC.
2. Propiedades.
3. En la pestaña de acceso remoto/ Habilitar la asistencia remota.
4. En Configuración avanzada establecer los parámetros si queremos que al equipo se controle remotamente y cuantos días necesitamos que estén abiertas las conexiones.
5. Usando escritorio remoto o Terminal Services tecleamos el nombre del equipo o en su defecto dando una direccion ip.

7.2 CONECTARSE A UN SERVIDOR DE TERMINAL SERVER CON SISTEMA OPERATIVO WINDOWS 2003 MEDIANTE EL CLIENTE DE TERMINAL SERVICES O ESCRITORIO REMOTO PARA SU ADMINISTRACIÓN USANDO UNA LAN

1. Debemos instalar los servicios de Terminal Server al igual que un servidor de licencias. Usando el escritorio remoto para la administración podemos compartir nuestros discos duros asi como nuestros recursos como unidades extraíbles e impresoras con el fin de crear una red virtual que nos simule aun mas que estamos dentro de nuestra oficina, para hacer esto seguiremos los siguientes pasos

2. abra el escritorio remoto

Nota: Inicio -> Programas -> Accesorios -> Comunicaciones -> Conexión a escritorio remoto

3. Usando escritorio remoto o **Terminal Services** tecleamos el nombre del equipo o en su defecto dando una direccion ip

4. En el Botón opciones en la pestaña recursos locales seleccionar unidades de disco e impresoras

5. por ultimo conectar y para que se nos muestren nuestros discos duros y unidades abrimos el icono de mi PC y ahí encontraremos nuestras unidades

7.3 CONECTARSE A UN SERVIDOR DE TERMINAL SERVER CON SISTEMA OPERATIVO WINDOWS 2003 MEDIANTE EL CLIENTE DE TERMINAL SERVICES O ESCRITORIO REMOTO PARA SU ADMINISTRACIÓN USANDO UNA WAN

1. Debemos instalar los servicios de **Terminal Server** al igual que un servidor de licencias.

Nota: Para instalar un servidor de licencias y los servicios de **Terminal Server** es necesario abrir Inicio -> Panel de Control -> Agregar y Quitar Programas -> Agregar o Quitar Componentes de Windows. Aquí seleccionamos Licencias de Terminal Server y Terminal Server.

2. Debemos Contar con un cortafuegos, para proteger nuestra LAN de cualquier ataque. Este firewall es necesario porque como tendremos una IP publica y a su vez acceso o salida a Internet podemos estar expuestos a cualquier virus informático además de que el firewall lo usaremos como DHCP.

3. Debemos deshabilitar el DHCP del servidor ya que solo lo queremos como servidor de servicios remotos.

4. Habilitar el DHCP del firewall que es el que otorgara las direcciones ip de los equipos de nuestra LAN al igual que a los clientes remotos.

5. Debemos de contar con una IP estática otorgada por nuestro proveedor de servicios de Internet que es la dirección pública que se usara para conectarnos desde cualquier parte.

6. Una vez teniendo en cuenta lo antes mencionado pasamos a darle un dirección IP estática a nuestro servidor en este caso se usara para ligarla al firewall y hacer el enlace.

7. La dirección pública en este caso la que nos dio nuestro proveedor la pondremos en el firewall en la configuración de la LAN

Notas: El modem debe de estar configurado como bridge o modo puente ya que solo lo queremos para que nos de la señal DSL para hacerlo debemos de seguir los siguientes pasos:

A) Resetear el modem es decir regresarlo a la configuración de fábrica.

B) Conectar el modem con un cable de red paralelo a la PC para configurarlo

C) Abrir un explorador de Internet y en la dirección URL escribimos; **http://**192.168.1.254/mdc (es la dirección de fabrica).

D) En configuración avanzada -> Configuración de Servicios. Seleccionamos no habilitar Enrutamiento.

La Salida de red la conectaremos al firewall que es el encargado de rutear y asignar las direcciones IP

En la configuración de la Lan donde va conectado el moden que trae como contrato en la línea la dirección IP publica la se introducirá ese valor ejem: 215.68.97.100

En la administración del firewall pondremos la dirección de nuestro servidor en este caso la 172.16.10.200 si no conoce podemos obtenerlo entrando en el símbolo del sistema y ejecutar el comando ipconfig, para que nos regrese el valor de la dirección IP.

8.- Por último usando cualquiera de nuestros clientes ya sea por medio de **Terminal Services** o Escritorio Remoto nos podemos conectar siguiendo los siguientes pasos:

1. Ejecutar el cliente de acceso remoto (ver figuras 7.1 y 7.2 sig. pag.).

2. Teclear la dirección IP pública.

3. Clic en conectar.

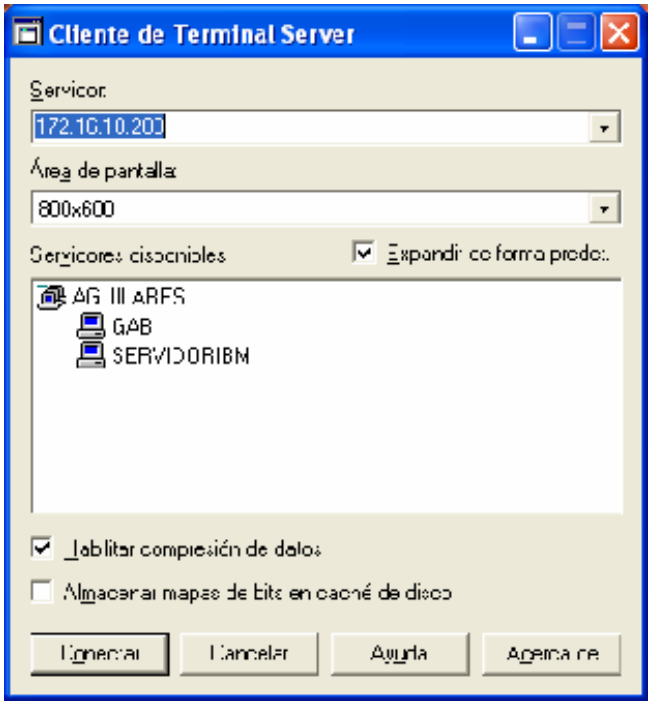


Fig. Num. 7.1

Fig. Num. 7.2

7.4 COMANDOS DE LOS SERVICIOS DE TERMINAL SERVER

Change logon. Habilita o deshabilita los inicios de sesión desde las sesiones de cliente o muestra el estado de inicio de sesión actual. Esta característica es útil para el mantenimiento del sistema.

Sintaxis: *change logon* {*/enable* | */disable* | */query*}

Parámetros;

I*enable***.** Habilita los inicios de sesión desde las sesiones del cliente, pero no desde la consola.

/disable. Deshabilita los inicios de sesión posteriores desde las sesiones del cliente, pero no desde la consola. Los usuarios conectados actualmente no se ven afectados.

*/query***.** Muestra el estado del inicio de sesión actual, ya esté habilitado o deshabilitado.

Cprofile[29]. Limpia el espacio desperdiciado de los perfiles especificados y, si las asociaciones de archivo específicas del usuario están deshabilitadas, las quita del Registro. Los perfiles que se están usando actualmente no se modifican.

Sintaxis: *cprofile* [*/l] [/i] [/v*] [listaDeArchivos]

Parámetros;

/l. Limpia todos los perfiles locales. También puede especificar una lista de perfiles adicionales en el parámetro listaDeArchivos.

/i. En cada perfil, pide la intervención del usuario de forma interactiva.

/v. Muestra información acerca de las acciones que se realizan.

Observaciones: Sólo los administradores pueden ejecutar cprofile.

Los servidores Terminal Server utilizan las asociaciones de archivo para determinar qué aplicación se utilizará para tener acceso a archivos de varios tipos. Los tipos de archivo se registran mediante el Explorador de Windows.

Las asociaciones de archivo por usuario permiten que cada usuario asocie una aplicación diferente a un tipo de archivo específico. Por ejemplo, un usuario podría asociar los archivos .doc a Microsoft Word y otro podría asociarlos a WordPad de Windows.

En caso de que se habiliten, *cprofile* sólo quita el espacio sin usar del perfil del usuario. Si se deshabilitan, *cprofile* también quita las entradas del Registro correspondientes.

Ejemplos;

---

[29] La modificación incorrecta del Registro puede dañar gravemente el sistema. Antes de realizar cambios en el Registro, debe hacer una copia de seguridad de los datos de valor que contenga el equipo.

Para limpiar todos los perfiles locales sin que el sistema pida confirmación para cada uno, escriba:

cprofile /l. Para limpiar los perfiles locales y que el sistema solicite confirmación para cada uno, escriba: *cprofile /l /i*

Logoff. Cierra la sesión de un usuario y elimina la sesión del servidor.

Sintaxis: *logoff*[{*IdSesión* | *nombresesión*}] [*/server*:nombreServidor] [*/v*]

Parámetros;

IdSesión. Especifica el identificador numérico con el que el servidor puede identificar la sesión.

nombresesión. Especifica el nombre de la sesión.

/server:nombreServidor. Especifica el servidor Terminal Server que contiene la sesión de usuario que desea cerrar. Si no se especifica este parámetro, se utiliza el servidor donde el usuario está activo actualmente.

/v. Muestra información acerca de las acciones que se realizan.

/?. Muestra la Ayuda en el símbolo del sistema.

Observaciones: Siempre puede cerrar la sesión a la que está conectado actualmente. No obstante, debe disponer del permiso de Control total para cerrar las sesiones de otros usuarios.

Si se cierra la sesión de un usuario sin advertir primero, se puede causar la pérdida de los datos en dicha sesión. Para advertir al usuario antes de emprender esta acción, debe enviarle un mensaje mediante el comando msg.

En caso de que no se especifique ningún identificador o nombre para la sesión, el uso del comando logoff cerrará la sesión actual del usuario. El nombre de sesión que especifique debe estar activo.

Cuando se cierra la sesión de un usuario, finalizan todos los procesos y la sesión se elimina del servidor.

No es posible cerrar la sesión de un usuario desde la sesión de consola.

Ejemplos;

1. Para cerrar la sesión actual de un usuario, escriba:

Logoff. Para cerrar la sesión actual de un usuario con el identificador de sesión, por ejemplo, la sesión 12, escriba:

logoff 12. Para cerrar la sesión de un usuario con el nombre de la sesión y servidor, por ejemplo, la sesión TERM04 en el servidor WF12, escriba:

logoff TERM04 /server:WF12

Msg. Envía un mensaje a un usuario.

Sintaxis: *Msg* {nombreDeUsuario | nombreDeSesión | IdDeSesión |time: segundos [mensaje]}

Parámetros;

nombreUsuario. El nombre del usuario que debe recibir el mensaje.

nombreSesión. El nombre de la sesión en la que se debe recibir el mensaje.

IdSesión. El identificador numérico de la sesión cuyo usuario debe recibir el mensaje.

/time:segundos. Especifica el intervalo de tiempo durante el que se mostrará el mensaje enviado en la pantalla del usuario. Cuando se alcanza el límite de tiempo, el mensaje desaparece. Si no se establece el límite de tiempo, el mensaje permanece en la pantalla hasta que el usuario lo ve y hace clic en Aceptar.

Nota: El texto del mensaje que desea enviar. En caso de que no se escriba ningún mensaje, se le pedirá que lo haga o se leerá la entrada estándar (es decir, stdin) para el mensaje. Para enviar un mensaje incluido en un archivo, escriba el símbolo menor que (<) seguido del nombre de archivo.

/*?*. Muestra la Ayuda en el símbolo del sistema.

Observaciones: Si no especifica un nombre de usuario o de sesión, msg mostrará un mensaje de error. El nombre de sesión que especifique debe estar activo.

El usuario debe tener permiso de acceso para enviar mensajes.

Ejemplos;

1. Para enviar un mensaje titulado "Quedemos hoy a la 1 p.m." a todas las sesiones del usuario JUAN, escriba:

msg JUAN Quedemos hoy a la 1 p.m.

2. Para enviar el mismo mensaje a la sesión 02, escriba:

msg modem02 Quedemos hoy a la 1 p.m.

3. Para enviar el mensaje a la sesión 12, escriba

msg 12 Quedemos hoy a la 1 p.m.

4. Para enviar un mensaje a todos los usuarios que han iniciado la sesión, escriba:

msg * Quedemos hoy a la 1 p.m.

5. Para enviar un mensaje a todos los usuarios, con un tiempo de espera de confirmación (por ejemplo, 10 segundos), escriba:

msg * /TIME:10 Quedemos hoy a la 1 p.m.

Reset session. Permite restablecer (eliminar) una sesión del servidor Terminal Server.

Sintaxis: *reset session* {nombreDeServidor | I*dDeSesión*} [/server:nombreDeServidor] [/*v*]

Parámetros;

nombreSesión. El nombre de la sesión que desea restablecer. Para determinar el nombre de la sesión, utilice el comando query session.

IdSesión. El identificador de la sesión que restablecer

/server: nombreDeServidor. Especifica el servidor Terminal Server que contiene la sesión que se va a restablecer. En caso de que no se especifique ningún servidor, se utilizará el servidor actual.

/v. Muestra información acerca de las acciones que se realizan.

/?. Muestra la Ayuda en el símbolo del sistema.

Observaciones: Siempre es posible restablecer sesiones propias, sin embargo, para restablecer una sesión de otro usuario es necesario el permiso de acceso de Control total.

Tenga en cuenta que, si se restablece la sesión de un usuario sin advertírselo primero, tal acción puede causar la pérdida de datos en la sesión.

Sólo debe restablecerse una sesión cuando no funcione correctamente o parezca que ha dejado de responder.

El parámetro /server sólo es necesario si utiliza reset session desde un servidor remoto.

Tsdiscon. Desconecta una sesión de un servidor Terminal Server.

Sintaxis: *Tsdiscon* [{*IdDeSesión* | *nombreDeSesión*}] [/server:nombreDeServidor] [/*v*]

Parámetros;

IdSesión. El identificador de la sesión que se va a desconectar.

nombreSesión. El nombre de la sesión que se va a desconectar.

/server:nombreDeServidor. Especifica el servidor Terminal Server que contiene la sesión que se va a desconectar. En caso de que no se especifique ningún servidor, se utilizará el servidor actual.

/v. Muestra información acerca de las acciones que se realizan.

/?. Muestra la Ayuda en el símbolo del sistema.

Observaciones: Debe disponer del permiso de Control total para desconectar la sesión de otro usuario.

En caso de que no se especifique ningún nombre o identificador de sesión, *tsdiscon* desconecta la sesión actual.

Las aplicaciones que se estaban ejecutando al desconectar la sesión se ejecutarán automáticamente cuando vuelva a conectarse, sin perder los datos. Si utiliza reset session para terminar la ejecución de las aplicaciones de la sesión desconectada, tenga en cuenta que los datos de la sesión podrían perderse.

El parámetro /server sólo es necesario si utiliza *tsdiscon* desde un servidor remoto.

La sesión de consola no se puede desconectar.

Ejemplos;

1. Para desconectar la sesión actual, escriba:

tsdiscon

2. Para desconectar la sesión 10, escriba:

tsdiscon 10

3. Para desconectar la sesión TERM04, escriba:

tsdiscon TERM04

Tskill. Termina un proceso

Sintaxis: *Tskill* {IdProceso | NombreProceso} [/server:NombreServidor] [{/id:IdSesión | /a}] [/v]

Parámetros;

IdProceso. El identificador del proceso que desea terminar

nombreProceso. El nombre del proceso que desea terminar. Puede utilizar caracteres comodín para especificar este parámetro. Especifica el servidor Terminal Server que contiene el proceso que desea terminar. En caso de que no se especifique ningún servidor, se utilizará el servidor actual.

tsshutdn /*server*:TerminalServer1 /*reboot*

7.5 CÓMO CONFIGURAR UN ESCRITORIO REMOTO Y GESTIONAR LAS CONEXIONES REMOTAS

Para configurar una conexión de escritorio remoto entre un equipo remoto con Windows XP Professional y un equipo local siga estos pasos.

A) Configurar el equipo remoto[30]

[30] A los administradores se les conceden privilegios de acceso remoto automáticamente.
Para que su equipo acepte conexiones remotas, debe utilizar Windows NT4 Terminal Server Edition, Windows 2000 Server, Windows XP Professional, o un sistema operativo Windows Server 2003. Para obtener más información, vea la Ayuda correspondiente a la plataforma de su sistema operativo.

En el equipo remoto con Windows XP Professional, siga estos pasos:

1. Haga clic en Inicio y, a continuación, haga clic con el botón secundario del mouse en el icono Mi PC.

2. En el menú contextual que aparece, haga clic en Propiedades.

3. Haga clic en la ficha Remoto y, a continuación, active la casilla de verificación Permitir a los usuarios conectarse remotamente a este equipo. Ver fig. Num. 7.3 en la siguiente pagina.

4. Cuando se le pregunte si desea confirmar este cambio, haga clic en Aceptar.

5. Haga clic en Seleccionar usuarios remotos y, a continuación, haga clic en Agregar para especificar cuentas de usuario adicionales para que se les conceda acceso remoto.

6. Cuando termine de agregar cuentas de usuario, haga clic en Aceptar. Asegúrese de que la cuenta que está agregando existe realmente en el equipo remoto. Si la cuenta no existe en el equipo remoto, créela.

7. Haga clic en Aceptar y de nuevo en Aceptar.

B) Para crear una conexión nueva

1. Abra Conexión a Escritorio remoto.

2. En Equipo, escriba el nombre o la dirección IP de un equipo. El equipo puede ser un servidor Terminal Server o un equipo que ejecute Windows XP Professional o un sistema operativo Windows Server 2003 en el que esté habilitado Escritorio remoto y para el que tenga permisos de Escritorio remoto.

Para abrir **Conexión a Escritorio remoto**, haga clic en **Inicio**, seleccione **Programas** o **Todos los programas**, **Accesorios**, **COMUNICACIÓNes** y, a continuación, haga clic en **Conexión a Escritorio remoto**. Para ver una lista de los equipos disponibles en el dominio, haga clic en la flecha **Equipo** y seleccione **<Examinar más**

3 .Haga clic en Conectar .Aparecerá el cuadro de diálogo Iniciar sesión en Windows.

4. En el cuadro de diálogo Iniciar sesión en Windows, escriba su nombre de usuario, su contraseña y el dominio (si es necesario) y, a continuación, haga clic en Aceptar.

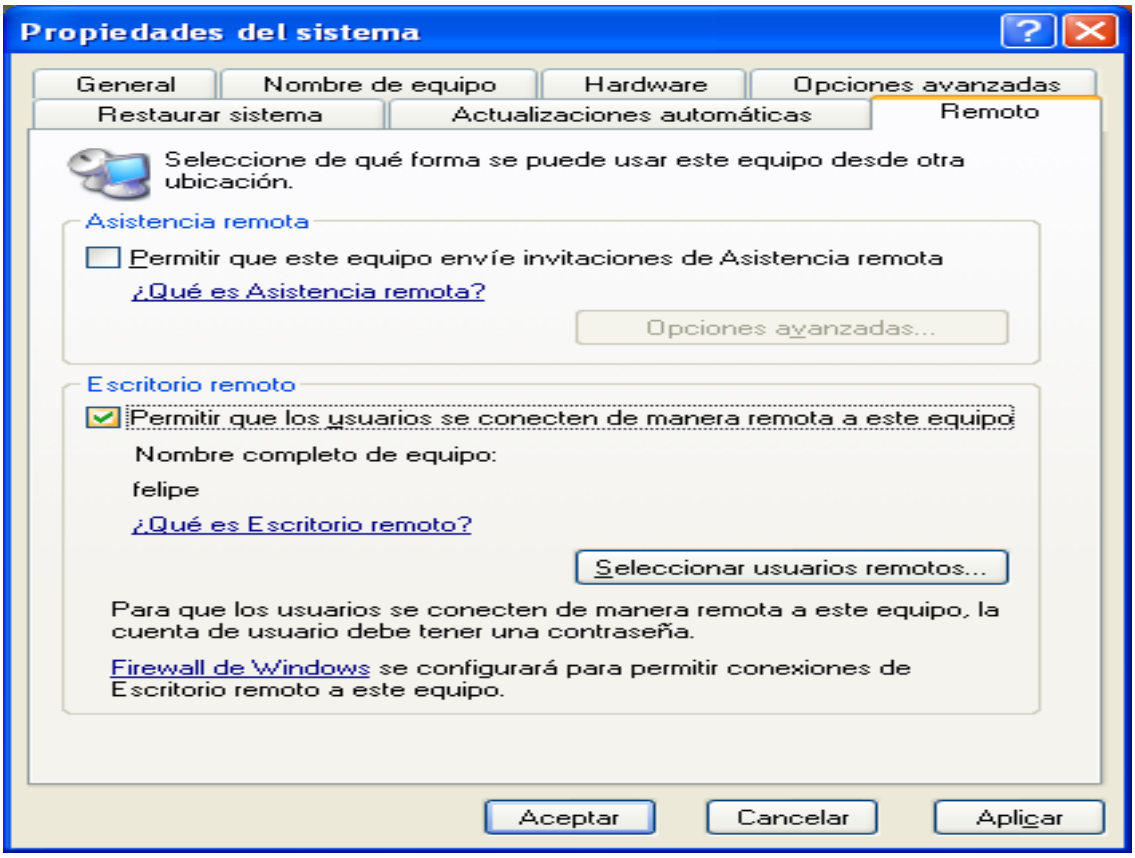


Fig. Num. 7.3

B) Para volver a establecer una conexión anterior

1. En la ventana Conexión a Escritorio remoto, haga clic en la flecha Equipo y seleccione el nombre del equipo al que desea conectarse ver fig. Num 7.4.

2. Haga clic en Conectar. Aparecerá el cuadro de diálogo Iniciar sesión en Windows.

3. En el cuadro de diálogo Iniciar sesión en Windows, escriba su nombre de usuario, su contraseña y el dominio (si es necesario) y, a continuación, haga clic en Aceptar.

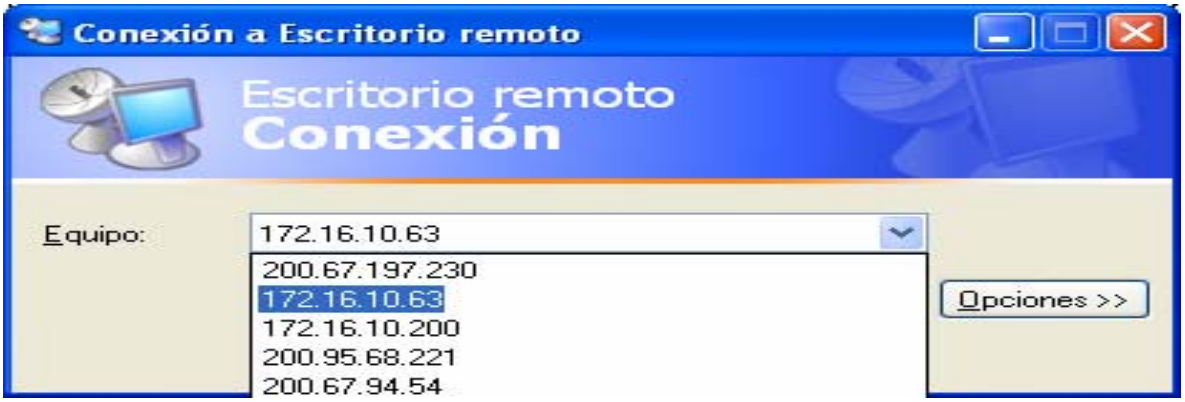


Fig. Num. 7.4

C) Para guardar la configuración de su conexión en un archivo

1. Abra Conexión a Escritorio remoto.

2. Haga clic en Opciones.

3. Especifique la configuración que desee para esta conexión (como el tamaño de la pantalla, la información de inicio de sesión automático y las opciones de rendimiento).

4. En la ficha General, haga clic en Guardar como.

5. Escriba un nombre para el archivo de conexión guardado y, después, haga clic en Guardar.

Notas: Las conexiones se guardan como archivos de protocolo de escritorio remoto (.rdp). Cada archivo .rdp contiene toda la información correspondiente a una conexión con un servidor Terminal Server, incluidos los valores de Opciones configurados cuando se guardó el archivo. Puede personalizar cualquier número de archivos .rdp, incluidos archivos para conectarse a un mismo servidor con diferentes configuraciones. Por ejemplo, puede guardar un archivo que establezca

una conexión con MiServidor en modo de pantalla completa y otro que le conecte al mismo equipo con un tamaño de pantalla de 800×600. El archivo de conexión predeterminada, Default.rdp, se almacena oculto en Mis documentos. Los archivos de conexión que cree también se almacenarán en Mis documentos, pero no estarán ocultos. Para modificar un archivo .rdp y cambiar la configuración de conexión que contiene, haga clic con el botón secundario del Mouse (ratón) en el archivo y, a continuación, haga clic en Modificar.

D) Para abrir una conexión guardada

1. En el Explorador de Windows, abra la carpeta Mis documentos.

2. Haga doble clic en el archivo .rdp correspondiente a la conexión que desea abrir.

E) Para desconectar sin finalizar una sesión

1. En la ventana Conexión a Escritorio remoto, haga clic en Inicio y, después, en Apagar. Aparecerá el cuadro de diálogo Salir de Windows.

2. Haga clic en Desconectar y, después, en Aceptar.

F) Para cerrar y finalizar la sesión

1. En la ventana Conexión a Escritorio remoto, haga clic en Inicio y, después, en Apagar. Aparecerá el cuadro de diálogo Salir de Windows.

2.Haga clic en Cerrar sesión de nombreUsuario y, después, haga clic en Aceptar.

G) Para copiar y pegar un archivo de un equipo local a un equipo remoto

1. Utilice Conexión a Escritorio remoto para establecer una conexión con un equipo remoto.

2. En la barra de tareas del equipo remoto, haga clic en Inicio y, a continuación, haga clic en Mi PC, o bien haga doble clic en el icono Mi PC del escritorio del equipo remoto. Cuando se abre el Explorador de Windows en el equipo

remoto, muestra las unidades del equipo remoto. Si eligió que sus unidades locales estén disponibles en una sesión, el Explorador de Windows del equipo remoto también mostrará las unidades del equipo local. En el siguiente ejemplo puede ver cómo se asigna nombre a las unidades del equipo local cuando aparecen en el Explorador de Windows del equipo remoto. Cliente TS es el nombre que Conexión a Escritorio remoto asigna a su equipo local.

3. Haga clic con el botón secundario del Mouse (ratón) en el archivo del equipo local que desea transferir al equipo remoto y, después, haga clic en Copiar.

4. En la misma ventana del Explorador de Windows, busque la ubicación del equipo remoto en la que desea pegar el archivo.

5. Haga clic con el botón secundario del mouse en el icono de la carpeta y, a continuación, haga clic en Pegar.

H) Para copiar y pegar un archivo de un equipo remoto a un equipo local

1. Utilice Conexión a Escritorio remoto para establecer una conexión con un equipo remoto.

2. En la barra de tareas del equipo remoto, haga clic en Inicio y, a continuación, haga clic en Mi PC, o bien haga doble clic en el icono Mi PC del escritorio del equipo remoto. Cuando se abre el Explorador de Windows en el equipo remoto, muestra las unidades del equipo remoto. Si eligió que sus unidades locales estén disponibles en una sesión, el Explorador de Windows del equipo remoto también mostrará las unidades del equipo local. En el siguiente ejemplo puede ver cómo se asigna nombre a las unidades del equipo local cuando aparecen en el Explorador de Windows del equipo remoto. Cliente TS es el nombre que Conexión a Escritorio remoto asigna a su equipo local.

3. Haga clic con el botón secundario del Mouse (ratón) en el archivo del equipo remoto que desea transferir al equipo local y, después, haga clic en Copiar.

4. En la misma ventana del Explorador de Windows, busque la ubicación del equipo local en la que desea pegar el archivo.

5. Haga clic con el botón secundario del Mouse en el icono de la carpeta y, a continuación, haga clic en Pegar.

I) Para volver a conectar si se corta la conexión

1. Abra Conexión a Escritorio remoto.

2. Haga clic en Opciones.

3. En la ficha Experiencia, active la casilla de verificación Volver a conectar si se pierde la conexión.

J) Para cambiar el tamaño de la pantalla para las conexiones

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Pantalla, bajo Tamaño del escritorio remoto, arrastre el control deslizante para elegir el tamaño del escritorio remoto. Arrastre el control deslizante por completo hacia la derecha para ver la pantalla completa.

3. Haga clic en Conectar.

K) Para cambiar la configuración de color para las conexiones

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Pantalla, en la lista Colores, haga clic en la resolución de colores que desee.

3. Haga clic en Conectar.

L) Para mejorar el rendimiento de las conexiones

1. En el cuadro de diálogo Conexión a Escritorio remoto, haga clic en Opciones y, a continuación, haga clic en la ficha Experiencia.

2. En el cuadro Rendimiento, elija la velocidad de la conexión. Para mejorar el rendimiento de la conexión, puede permitir que aparezcan ciertas características de la sesión remota de Windows si están habilitadas en el equipo remoto. Las características que pueden cambiarse dependen de la velocidad de la conexión.Si elige Personalizar, podrá activar cualquier combinación de casillas de verificación. Las opciones elegidas se guardarán en un archivo de conexión (.rdp).

M) Para mostrar la barra de conexión en modo de pantalla completa

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2 .En la ficha Pantalla, active la casilla Mostrar barra de conexión cuando haya pantalla completa.

3. Haga clic en Conectar.

N) Para especificar un programa para que se inicie al establecer la conexión

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Programas, bajo Iniciar un programa, haga clic en Iniciar el siguiente programa al conectarse.

3. En el cuadro Nombre de archivo y ruta de acceso del programa, escriba la ruta de acceso y el nombre de archivo del programa que desea que se ejecute una vez creada la conexión.

4. De forma opcional, en el cuadro Iniciar en la carpeta siguiente, escriba la ruta de acceso al directorio de trabajo del programa.

5. Haga clic en Conectar.

Ñ) Para configurar las conexiones para reproducir audio

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Recursos locales, en la lista Sonido de equipo remoto, haga clic en la opción que desee.

- Para ejecutar archivos de sonido durante la sesión de Escritorio remoto y oírlos en el equipo local, elija Traer a este equipo.
- Para ejecutar archivos de sonido durante la sesión de Escritorio remoto y reproducirlos sólo en el equipo remoto, elija Dejar en el equipo remoto.
- Para deshabilitar todos los sonidos durante las sesiones de Escritorio remoto, elija No reproducir.
- Haga clic en Conectar.

O) Para hacer que las unidades de disco locales estén disponibles en una sesión

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Recursos locales, bajo Dispositivos locales, haga clic en Unidades de disco.

3. Haga clic en Conectar.

P) Para hacer que la impresora local esté disponible en una sesión

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Recursos locales, bajo Dispositivos locales, haga clic en Impresoras.

3. Haga clic en Conectar.

Q) Para hacer que el puerto serie local esté disponible en una sesión

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Recursos locales, en Dispositivos locales, haga clic en Puertos serie.

3. Haga clic en Conectar.

R) Para hacer que una tarjeta inteligente esté disponible en una sesión[31]

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Recursos locales, bajo Dispositivos locales, haga clic en Tarjeta inteligente.

S) Para configurar las teclas de método abreviado de Windows en una sesión

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Recursos locales, bajo Teclado, haga clic en la lista Aplicar combinaciones de teclas de Windows y, a continuación, haga clic en la opción que desee. Esta opción afecta al comportamiento de las combinaciones de teclas de método abreviado de Windows (como ALT+TAB) cuando está conectado a un equipo remoto.

Notas: Para configurar la conexión de forma que las teclas de método abreviado de Windows siempre se apliquen al escritorio local, elija En el equipo local.

Para configurar la conexión de forma que todas las teclas de método abreviado de Windows se apliquen al escritorio del equipo remoto, elija En el equipo remoto.

Para configurar la conexión de forma que las teclas de método abreviado de Windows se apliquen al equipo remoto únicamente cuando la conexión esté en modo de pantalla completa, elija Sólo en modo de pantalla completa.

---

[31] La opción de habilitar la redirección de una tarjeta inteligente no se mostrará a menos que haya una tarjeta inteligente y el servicio esté habilitado.

3. Haga clic en Conectar.

T) Para configurar el almacenamiento de mapas de bits en caché

1. En la ventana Conexión a Escritorio remoto, haga clic en Opciones.

2. En la ficha Experiencia, compruebe que está activada la casilla de verificación Almacenar mapas de bits en caché. O bien, para deshabilitar el almacenamiento de mapas de bits en caché, desactive la casilla de verificación Almacenar mapas de bits en caché.

3. Haga clic en Conectar.

CONCLUSIONES

Los servicios de acceso remoto en este tiempo son de gran importancia ya que con ellos podemos trabajar en cualquier parte del mundo con solo conectarnos al Internet. Con esto conseguimos una gran ventaja ya que podemos contar con los recursos, archivos, etc. que nos proporciona nuestro lugar de trabajo, podemos incluso trabajar en el camino con una conexión inalámbrica.

En los capítulos tratados podemos constatar que a medida de que se van actualizando los sistemas operativos, se hace más seguro y casi de forma automática la instalación y configuración del RAS que sus siglas significan (Servicio de Acceso Remoto) o bien un servidor de aplicaciones de Terminal Server en los sistemas de Windows más actuales con la ayuda de asistentes.

Los capítulos que se trataron están basados en la tecnología NT, que además proporcionaron a los usuarios un trabajo mas seguro. Si hay algo en lo que Windows NT es fuerte son los Servicios de Acceso Remoto ya que proporciona varias formas para configurar tanto seguridad como controlar accesos a los usuarios remotos.

Windows 2003 basándose en la tecnología NT proporciona una plataforma más fuerte con opciones de seguridad mas elevadas, como limitar a los usuarios remotos a ciertos recursos de la intranet por medio de las directivas de seguridad, con más opciones de configuración tanto de enrutamiento como en el cliente para tener acceso a una VPN.

En Windows 2003 se puede configurar derechos de acceso remoto basados en la pertenencia a grupos, conceder derechos de acceso remoto a cuentas de usuario individuales, conceder a los usuarios acceso a servidores de acceso remoto. Nos presenta varias formas de configuración de seguridad ya que esta es de suma importancia para nuestra empresa.

La tecnología empleada para acceder remotamente a un servidor fuera de nuestra ubicación fue mejorada con el acceso de Escritorio Remoto, ya que de esta forma podemos compartir recursos locales y visualizarlos en el servidor remoto donde será más fácil mapear las unidades de almacenamiento e impresoras. Esta tecnología evita que nos conectemos a un sitio FTP para usarlo como puente, para transferir archivos a nuestro equipo local.

BIBLIOGRAFIA

Carl Siechert, *Microsoft Windows XP. Running* +, McGraw-Hill, 2002, p.p. 1024

Elena Raya Pérez; José Luis Raya, *Windows 2000 Server: instalación, configuración y administración*., Ra-ma, 2003, p.p. 1200

KENLEY Martín y cols., *Aprendiendo Windows NT, Prentice May Hispanoamericana*, S.A., México, 1998, p.p. 510

RAYA, J.L. y RAYA, L., *Windows Server 2003. Instalación y Configuración Avanzada*, Ra-ma, 2004, p.p. 792

Stanek William R., *Windows Server 2003 Manual del Administrador*, Mc Graw Hill, 2003, p.p. 435

OTRAS FUENTES

http://www.consulintel.es/Html/Tutoriales/Articulos/serv_a_r.html

http://www.microsoft.com/LATAM/OEM/NTW/BRK/RAS.HTM

http://www.ual.es/ServInf/COMUNICACIÓNes/modem_ras/modem_ras.html

http://www.supervia.com/i+.htm

http://www.upsp.edu.pe/manuales/nt4-2.html

http://nevada.ual.es/COMUNICACIÓNes/servicios/ras/modem_vpn.html#_xp

http://soporte.udg.mx/tutoriales/conf_conexion/winnt/index.html