Tecnologías de red

Se utilizan diversas tecnologías de red para proporcionar las numerosas ventajas de un sistema de video en red. Este capítulo comienza con unos apartados dedicados a la red de área local, concretamente a las redes Ethernet y sus componentes compatibles. También se tratan el uso de la alimentación a través de Ethernet, las direcciones IP y el transporte de datos, entre otros temas.

\\ Cap. IX
Primera Parte

Indice

Capítulo 1.
Video en red (Pág. 18)
Capítulo 2.
Cámaras de red /Cámaras IP (Pág. 32)
Capítulo 3.
Elementos de la cámara (Pág. 48)
Capítulo 4.
Protección de la cámara y carcasas (Pág. 68)
Capítulo 5.
Codificadores de video (Pág. 80)
Capítulo 6.
Resoluciones (Pág. 92)
Capítulo 7
Compresión de video (Pág. 110)
Capítulo 8.
Audio (Pág. 120)

Capítulo 9.
Tecnologías de red
1ra. Parte
9.1. *Red de área local y Ethernet*
9.1.1. *Tipos de redes Ethernet*
9.1.2. *Conmutador*
9.1.3. *Alimentación a través de Ethernet*
9.2. *Internet*
9.2.1. *Direcciones IP*
9.2.2. *Protocolos de transporte de datos para video en red*

Capítulo 10.
Tecnología inalámbrica
Capítulo 11.
Sistemas de gestión de video
Capítulo 12.
Consideraciones sobre ancho de banda y almacenamiento

9.1. Red de área local y Ethernet

Una red de área local (LAN) es un grupo de ordenadores conectados a un área localizada para comunicarse entre sí y compartir recursos como, por ejemplo, impresoras. Los datos se envían en forma de paquetes, para cuya transmisión se pueden utilizar diversas tecnologías. La tecnología LAN más utilizada es la Ethernet y está especificada en una norma llamada IEEE 802.3. (otros tipos de tecnologías de redes LAN son Token Ring y FDDI).

Ethernet utiliza una topología en estrella en la que los nodos individuales (dispositivos) están conectados unos con otros a través de un equipo de red activo como un conmutador. El número de dispositivos conectados a una LAN puede oscilar entre dos y varios miles.

El medio de transmisión físico para una LAN por cable implica cables, principalmente, de par trenzado o bien fibra óptica. Un cable de par trenzado consiste en ocho cables que forman cuatro pares de cables de cobre trenzados y se utiliza con conectores RJ-45 y sockets. La longitud máxima de un cable de par trenzado es de 100 metros mientras que para la fibra, el máximo varía entre 10 y 70 kilómetros, dependiendo del tipo. En función del tipo de cables de par trenzado o de fibra óptica que se utilicen, actualmente las velocidades de datos pueden oscilar entre 100 Mbit/s y 10.000 Mbit/s.

El cable de par trenzado está formado por cuatro pares de cables trenzados que normalmente se conectan por el extremo a un conector RJ-45.

Por regla general, las redes siempre deben tener más capacidad de la que se necesita. Para preparar una red para el futuro es una buena idea diseñar una red que solamente utilice el 30% de su capacidad. Actualmente una red necesita cada vez más y más rendimiento, ya que hay cada vez más aplicaciones que funcionan a través de redes. Mientras que los conmutadores de red (de los que se habla a continuación) son fáciles de actualizar con el paso del tiempo, el cable suele ser mucho más difícil de sustituir.

9.1.1. Tipos de redes Ethernet

- Fast Ethernet: Hace referencia a una red Ethernet que puede transferir datos a una velocidad de 100Mbit/s. Se puede basar en cable de par trenzado o de fibra óptica (la antigua Ethernet de 10 Mbit/s todavía se instala y se usa, pero este tipo de redes no proporcionan el ancho de ban-

Continúa en página 136

Viene de página 132

da necesario para algunas aplicaciones de video en red).

La mayoría de dispositivos que se conectan a una red, como un portátil o cámara de red, están equipados con una interfaz Ethernet 100BASE-TX/10BASE-T -comúnmente llamada interfaz 10/100-, que admite tanto Ethernet a 10 Mbit/s como Fast Ethernet. El tipo de cable de par trenzado compatible con Fast Ethernet se denomina Cat-5.

- Gigabit Ethernet: También puede basarse en cable de par trenzado o de fibra óptica, proporciona una velocidad de transferencia de datos de 1.000 Mbit/s (11 Gbit/s) y es cada vez más frecuente. Se espera que pronto sustituya a la Fast Ethernet como norma de hecho.

El tipo de cable de par trenzado compatible con Gigabit Ethernet es el Cat-5e, en el que los cuatro pares de cables trenzados se utilizan para alcanzar la alta velocidad de transferencia de datos. Para los sistemas de video en red se recomienda Cat-5e u otras categorías de cable superiores. La mayoría de las interfaces son compatibles con las versiones anteriores de Ethernet 10 Mbit/s y 100 Mbit/s y se conocen como interfaces 10/100/1000.

Para la transmisión a larga distancia se puede utilizar cable de fibra como el 1000BASE-SX (hasta 550 metros) y el 1000BASE-LX (hasta 550 metros con fibras ópticas multimodo y hasta 5.000 metros con fibras de modo único).

Las grandes distancias se pueden cubrir con los cables de fibra óptica. La fibra suele usarse en la red troncal de una red y no en nodos como una cámara de red.

- 10 Gigabit Ethernet: Es la última generación, proporciona una velocidad de transferencia de datos de 10 Gbit/s (110.000 Mbit/s) y se puede utilizar con fibra óptica o cable de par trenzado. 10GBASE-LX4, 10GBASE-ER y 10GBASE-SR por cable de fibra óptica se pueden utilizar para cubrir distancias de hasta 10.000 metros. Con una solución de par trenzado se requiere un cable de altísima calidad (Cat-6a o Cat-7). La Ethernet de 10 Gbit/s se utiliza principalmente como red troncal en aplicaciones de gama alta que requieren una velocidad de transferencia de datos muy alta.

9.1.2. Conmutador

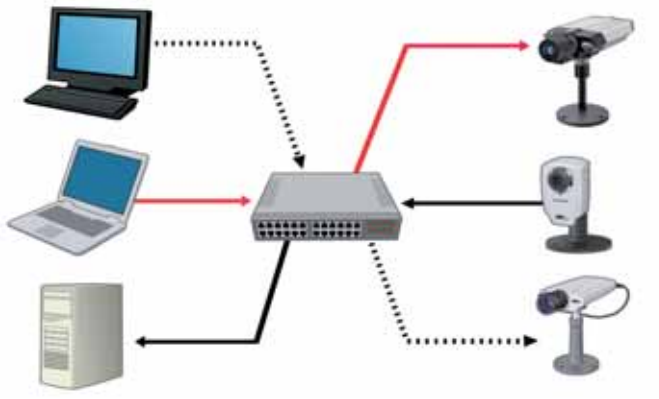
Cuando sólo dos dispositivos necesitan estar comunicados directamente el uno con el otro por medio de un cable de par trenzado, se puede utilizar el llamado cable cruzado. El cable cruzado simplemente cruza el par de transmisión de un extremo del cable con el par de recepción del otro extremo y viceversa.

Sin embargo, para conectar diversos dispositivos a una LAN se requiere un equipo de red, como un conmutador de red, que utiliza un cable de red convencional en lugar de un cable cruzado.

La función principal de un conmutador de red es remitir los datos de un dispositivo a otro en la misma red. Es un método eficaz, puesto que los datos se pueden dirigir de un dispositivo al otro sin que ello afecte a otros dispositivos que utilicen la misma red.

Un conmutador registra las direcciones MAC (Media Access Control/ Control de acceso al medio) de todos los dispositivos conectados (cada dispositivo de red tiene una dirección MAC única, que está formada por una serie de números y letras establecida por el fabricante y suele encontrarse en la etiqueta del producto). Cuando un conmutador recibe datos, los remite sólo al puerto que está conectado a un dispositivo con la dirección MAC de destino adecuada.

Los conmutadores suelen indicar su rendimiento en velocidades por puerto y en plano posterior o velocidades internas (ambas en velocidad de bits y paquetes por segundo). La velocidad por puerto indica la velocidad máxima en un puerto concreto. Esto significa que la velocidad de un conmutador, por ejemplo, 100 bit/s, suele ser el rendimiento de cada puerto.



Con un conmutador de red, la transferencia de datos se gestiona de manera muy eficaz, ya que el tráfico de datos se puede dirigir de un dispositivo a otro sin afectar a cualquier otro puerto del conmutador.

Un conmutador de red normalmente admite distintas velocidades de transferencia de datos de forma simultánea. La velocidad más común solía ser 10/100, que admite tanto Ethernet 10 Mbit/s como Fast Ethernet. Pero 10/100/1000 se está posicionando rápidamente como el conmutador estándar y, por lo tanto, admite simultáneamente Ethernet de 10 Mbit/s, Fast Ethernet y Gigabit Ethernet. La velocidad y el modo de transferencia entre un puerto de un conmutador y un dispositivo conectado normalmente se determinan mediante la negociación automática, en la que se utiliza la velocidad de transferencia de datos más alta y el mejor modo de transmisión. Un conmutador también permite que un dispositivo conectado funcione en modo dúplex completo: por ejemplo, enviar y recibir datos al mismo tiempo, dando como resultado un mejor rendimiento.

Los conmutadores pueden tener diferentes características y funciones. Algunas incluyen la función de enrutador. Un conmutador también puede admitir Alimentación a través de Ethernet o Calidad de servicio, que controla la cantidad de ancho de anda que utilizan las distintas aplicaciones.

9.1.3. Alimentación a través de Ethernet

La Alimentación a través de Ethernet (PoE) permite proveer de energía a los dispositivos conectados a una red Ethernet usando el mismo cable que para la comunicación de datos. Su uso es muy frecuente en teléfonos IP, puntos de acceso inalámbricos, cámaras de red conectadas a una LAN.

La principal ventaja de PoE es el ahorro de costos que conlleva. No es necesario contratar a un electricista ni instalar una línea de alimentación separada. Esto supone una ventaja, sobre todo en zonas de difícil acceso. El hecho de que no sea necesario instalar otro cable de alimentación puede suponer un ahorro de varios centenares de dólares, dependiendo de la ubicación de la cámara. PoE también facilita el hecho de cambiar la ubicación de la cámara o añadir otras cámaras al sistema de videovigilancia.

Además, aumenta la seguridad del sistema de video. Un sistema de videovigilancia con PoE se puede alimentar desde una sala de servidores, que a menudo está protegida con un SAI (Sistema de alimentación ininterrumpida). Esto significa que el sistema puede funcionar incluso durante un apagón.

Por las ventajas que tiene PoE, se recomienda usarla en tantos dispositivos como sea posible. La energía de un conmutador o midspan con PoE debería ser suficiente para los dispositivos co-

Continúa en página 140

Viene de página 136

nectados y éstos deberían admitir la clasificación de potencia. Todo ello se explica a en este capítulo con más detalle.

- Norma 802.3af y High PoE: Actualmente la mayoría de dispositivos PoE cumplen con la norma IEEE 802.3af, publicada en 2003. Esta norma utiliza cables estándares Cat-5 o superiores y asegura que la transferencia de datos no se vea afectada. En dicha norma, al dispositivo que proporciona la energía se le llama equipo de suministro eléctrico (PSE). Éste puede ser un conmutador o midspan habilitado para PoE. El dispositivo que recibe la energía se conoce como dispositivo alimentado (PD). Esta función normalmente está integrada en un dispositivo de red, como una cámara o en un splitter independiente.

La compatibilidad con versiones anteriores de dispositivos de red que admiten PoE está garantizada. La norma incluye un método para identificar automáticamente si un dispositivo es compatible con PoE y sólo se le proporciona energía una vez que se ha confirmado dicha compatibilidad. Esto también implica que el cable Ethernet conectado a un conmutador PoE no proporcionará energía alguna si no está conectado a un dispositivo habilitado para PoE, lo cual elimina el riesgo de una descarga eléctrica al instalar una red o renovar la instalación.

En un cable de par trenzado hay cuatro pares de cables trenzados. PoE puede utilizar dos pares de cables "de recambio" o bien superponer el actual a los pares de cables usados para la transmisión de datos. Los conmutadores con PoE integrada a menudo proporcionan la electricidad por medio de los dos pares de cables utilizados para la transmisión de datos, mientras que los midspans normalmente usan los dos pares de recambio. Un PD admite las dos opciones. Según la IEEE 802.3af, un PSE proporciona un voltaje de 48 VCC con una potencia máxima de 15,44 W por puerto. Pero, teniendo en cuenta que en un cable de par trenzado hay pérdida de potencia, un PD sólo garantiza 12,95 W. La norma IEEE 802.33 especifica varias categorías de rendimiento para los PD.

Los PSE como los conmutadores o midspans normalmente proporcionan una potencia de entre 300W y 500W. En un conmutador de 48 puertos significaría una potencia de 6 a 10W por puerto, en caso de que todos los puertos estuvieran conectados a dispositivos con PoE. Salvo que los PD admitan clasificación de potencia, los 15,44W deben reservarse en su totalidad para los puertos que utilicen PoE, lo que implica que un conmutador con 300W sólo puede alimentar 20 de los 48 puertos. Sin embargo, si todos los dispositivos comunicaran al conmutador su condición de dispositivos de clase 1, los 300W bastarían para alimentar a los 48 puertos.

Clasificaciones de potencia según IEEE 802.3af

Clase	Nivel de potencia mín. en PSE	Nivel de potencia máx. en PD	Uso
0	15.4 W	0.44 – 12.95 W	Predeterminado
1	4.0 W	0.44 – 3.84 W	Opcional
2	7.0 W	3.84 – 6.49 W	Opcional
3	15.4 W	6.49 – 12.95 W	Opcional
4	Tratado como Clase 0	-	Reservado para usos futuros

La mayoría de cámaras de red fijas pueden recibir energía por medio de PoE con la norma IEEE 802.3af y normalmente se identifican como dispositivos de clase 1 o 2.

Con la norma en desarrollo IEEE 802.3at o PoE+, el límite de potencia aumenta hasta al menos 30 W por medio de dos pares de cables de un PSE. Las especificaciones finales todavía están por determinar y se espera que la norma se ratifique.

Mientras tanto, los midspans y splitters con la norma en desarrollo IEEE 802.3at (High PoE) pueden utilizarse para dispositivos como cámaras y domos PTZ con control motor, así como para cámaras con calefactores y ventiladores, que requieren más potencia de la que proporciona la norma IEEE 802.3af.

- Midspans y splitters: Los midspans y splitters (también conocidos como splitters activos) son equipos que permiten que una red existente sea compatible con la Alimentación a través de Ethernet.

Un sistema existente se puede actualizar con la función PoE mediante un midspan y un splitter.

El midspan, que proporciona más energía al cable Ethernet, se coloca entre el conmutador de red y los dispositivos alimentados. Para asegurarse de que la transferencia de datos no se vea afectada, es importante recordar que la distancia máxima entre la fuente de datos (el conmutador, por ejemplo) y los productos de video en red no debe ser superior a 100 metros. Esto significa que el midspan y el splitter o splitters activos deben colocarse a una distancia no superior a 100 metros.

Un splitter sirve para separar la energía y los datos de un cable Ethernet en dos cables separados, de modo que se puedan conectar a un dispositivo sin PoE integrada. Puesto que la PoE o High PoE proporciona 48 VCC, la otra función del splitter consiste en bajar el voltaje a un nivel adecuado para el dispositivo, por ejemplo, 2 o 5 V.

9.2. Internet

Para enviar datos entre un dispositivo conectado a una red de área local a otro conectado a otra LAN se requiere una vía de comunicación estándar, ya que es posible que las redes de área local utilicen distintos tipos de tecnologías. Esta necesidad lleva al desarrollo de un sistema de direcciones IP y protocolos basados en IP para comunicarse a través de Internet, que conforma un sistema global de redes informáticas interconectadas (las LAN también pueden utilizar direcciones y protocolos IP para comunicarse dentro de una red de área local, aunque el uso de las direcciones MAC es suficiente para la comunicación interna).

Antes de abordar el tema de las direcciones IP, a continuación se tratan algunos de los conceptos básicos de la comunicación a través de Internet, tales como los enrutadores, cortafuegos y proveedores de servicios de Internet.

- Enrutadores: Para enviar paquetes de datos de una LAN a otra a través de Internet debe utilizarse un equipo de red llamado enrutador de red. Un enrutador guía la información de una red a otra basándose en las direcciones IP. Sólo remite los paquetes de datos que deben enviarse a otra red. Normalmente se utiliza para conectar una red local a Internet. Tradicionalmente se denominaba a los enrutadores "puertas de Enlace".

- Cortafuegos: Sirven para evitar los accesos no autorizados hacia o desde una red privada. Se pueden implementar tanto en el hardware como en el software o en una combinación de ambos. Normalmente se utilizan los cortafuegos para evitar que usuarios no autorizados accedan a redes privadas conectadas a Internet. Los mensajes que entran y salen de Internet pasan por

Continúa en página 144

Viene de página 140

el cortafuegos, que los examina y bloquea aquellos que no cumplen con los criterios de seguridad especificados.

- Conexiones a Internet: Para conectar una LAN a Internet debe establecerse una conexión de red a través de un proveedor de servicios de Internet (ISP). En una conexión a Internet se utilizan términos como velocidad de subida y velocidad de bajada. La velocidad de subida describe la velocidad de transferencia con la que se pueden subir datos del dispositivo a Internet: por ejemplo, cuando se envía un video desde una cámara de red. La velocidad de bajada es la velocidad de transferencia con la que se bajan archivos: por ejemplo, cuando un monitor de ordenador recibe un video. En la mayoría de los casos -como un portátil conectado a Internet, por ejemplo-, la descarga de información desde Internet es la velocidad más importante a tener en cuenta. En una aplicación de video en red con una cámara de red situada en una ubicación remota, la velocidad de subida es más relevante, puesto que los datos (el video) de la cámara de red se subirán a Internet.

9.2.1. Direcciones IP

Cualquier dispositivo que quiera comunicarse con otros dispositivos a través de Internet debe tener una dirección IP única y adecuada. Las direcciones IP sirven para identificar a los dispositivos emisores y receptores. Actualmente existen dos versiones IP: IP versión 4 (IPv4) e IP versión 6 (IPv6). La principal diferencia entre ellas es que una dirección IPv6 tiene una longitud mayor (128 bits, en comparación con los 32 bits de una dirección IPv4). Actualmente las direcciones IPv4 son las más difundidas.

9.2.1.1. Direcciones IPv4

Las direcciones IPv4 se agrupan en cuatro bloques, cada uno de los cuales se separa con un

punto. Cada bloque representa un número entre 0 y 255, por ejemplo: 192.168.12.23.

Algunos bloques de direcciones IPv4 se han reservado exclusivamente para uso privado. Estas direcciones IP privadas son desde 10.0.0.0 hasta 10.255.255.255, desde 172.16.0.0 hasta 172.31.255.255 y desde 192.168.0.0 hasta 192.168.255.255. Este tipo de direcciones sólo se pueden utilizar en redes privadas y no está permitido reenviarlas a Internet a través de un enrutador. Todos los dispositivos que quieran comunicarse a través de Internet deben tener su propia dirección IP pública. Una dirección IP pública es una dirección asignada por un proveedor de servicios de Internet. Un ISP puede asignar direcciones IP dinámicas, que pueden cambiar durante una sesión, o direcciones estáticas, que normalmente implican una cuota mensual.

- Puertos: Un número de puerto define un servicio o aplicación en concreto para que el servidor receptor (por ejemplo una cámara de red) sepa cómo procesar los datos entrantes. Cuando un ordenador envía datos vinculados a una aplicación concreta, normalmente añade el número de puerto a una dirección IP sin que el usuario lo sepa. Los números de puerto pueden ir del 0 al 65535. Algunas aplicaciones utilizan los números de puerto que les ha preasignado la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, un servicio web vía http se suele asignar al puerto 80 de una cámara de red.

- Configuración de las direcciones IPv4: Para que una cámara de red o codificador de video funcione en una red IP, se le debe asignar una dirección IP. Hay básicamente dos formas de configurar una dirección IPv4 para un producto de video en red

1) de forma automática con el DHCP (Protocolo de configuración dinámica de host)

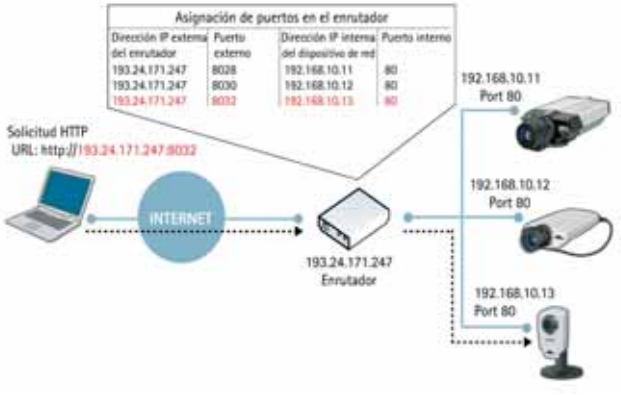
2) introduciendo manualmente una dirección IP estática en la interfaz del producto de video en red, una máscara de subred y la dirección IP del enrutador predeterminado o bien utilizando un software de gestión.

El DHCP gestiona un conjunto de direcciones IP que puede asignar dinámicamente a una cámara de red/codificador de video. A menudo la función DHCP la realiza un enrutador de banda ancha, que sucesivamente recibe sus direcciones IP de un proveedor de servicios de Internet. Una dirección IP dinámica significa que la dirección IP para un dispositivo de red puede cambiar de un día para otro. Para usar direcciones IP dinámicas se recomienda que los usuarios registren un nombre de dominio (por ejemplo, www.mycamera.com) para el producto de video en red en un servidor de DNS (Sistema de nombres de dominio) dinámico, el cual siempre puede vincular el nombre de dominio del producto a cualquier dirección IP que tenga asignada. (Un nombre de dominio se puede registrar a través de algunos de los sitios web de DNS dinámico más conocidos, como www.dyndns.org).

A continuación se explica cómo configurar una dirección IPv4 con el DHCP. Cuando una cámara de red/codificador de video se conecta, envía una solicitud de configuración a un servidor DHCP. Este servidor responde con una dirección IP y una máscara de subred. Entonces, el producto de video en red puede actualizar un servidor NDS dinámico con su dirección IP actual, de modo que los usuarios puedan acceder al producto usando un nombre de dominio.

- NAT (Network address translation, Traducción de dirección de red): Para que un dispositivo de red con una dirección IP privada pueda enviar información a través de Internet, debe utilizar un enrutador compatible con NAT. Con esta técnica, el enrutador puede traducir una dirección IP privada en una pública sin el conocimiento del host que realiza el envío.

- Reenvío de puertos: Para acceder a cámaras ubicadas en una LAN privada a través de Internet, la dirección IP pública del enrutador debería usarse junto con el número de puerto correspondiente del codificador de video o la cámara de red en la red privada. Dado que un servicio web a través de HTTP normalmente se asigna al puerto 80, en un escenario con varios codificadores de video o cámaras de red que utilizan el puerto 80 para HTTP en una red privada ocurre lo siguiente: en lugar de cambiar el número de puerto HTTP predeterminado en cada producto de video en red, puede configurarse un enrutador para asociar un único número de puerto HTTP al puerto HTTP predeterminado y a la dirección IP de un producto de video en red concreto. Este proceso se denomina reenvío de puertos y funciona como se indica a continuación.



Gracias al reenvío de puertos del enrutador, es posible acceder a cámaras de red de una red local con direcciones IP privadas a través de Internet. En la ilustración, el enrutador reenvía los datos (solicitud) que recibe el puerto 8032 a una cámara de red con la dirección IP privada 192.168.10.13 a través del puerto 80. A continuación, la cámara empieza a enviar video.

Los paquetes de datos entrantes llegan al enrutador a través de su dirección IP pública (externa) y un número de puerto específico. El enrutador está configurado para reenviar los datos que

Continúa en página 146

Viene de página 144

entran por un número de puerto predefinido a un dispositivo específico de la parte del enrutador correspondiente a la red privada. A continuación, el enrutador sustituye la dirección del emisor por su propia dirección IP privada (interna). Para el cliente receptor, el enrutador es el origen de los paquetes. Con los paquetes de datos salientes ocurre lo contrario. El enrutador sustituye la dirección IP privada del dispositivo origen por la IP pública del propio enrutador antes de enviar los datos a través de Internet.

El reenvío de puertos normalmente se realiza al configurar por primera vez el enrutador. Cada enrutador tiene su propio método de reenvío de puertos y existen sitios web como www.portfoward.com que ofrecen instrucciones paso a paso para distintos enrutadores. Normalmente, el reenvío de puertos implica el uso de la interfaz del enrutador con un navegador de Internet. Asimismo, también requiere el acceso a la dirección IP pública (externa) del enrutador y a un número de puerto único que se asigna a la dirección IP interna del producto de video en red específico y a su número de puerto para la aplicación.

9.2.1.2. Direcciones IPv6

Las direcciones IPv6 se escriben en notación hexadecimal y constan de ocho bloques de 16 bits cada uno, divididos por los puntos. Por ejemplo, 2001:0da8:65b4:05d3:1315:0461:7847

Entre las principales ventajas de IPv6, además de disponer de una gran cantidad de direcciones IP, se incluye la posibilidad de habilitar un dispositivo para que configure automáticamente su dirección IP mediante la dirección MAC. En la comunicación a través de Internet, el host solicita y recibe del enrutador el prefijo necesario del bloque de la dirección pública, así como información adicional. Se utilizan el prefijo y el sufijo del host, de modo que con IPv6 ya no es necesario el protocolo DHCP para la asignación de direcciones IP ni la definición manual de las mismas. También deja de ser necesario el reenvío de puertos.

Otras ventajas de IPv6 son la renumeración para simplificar el cambio de redes corporativas entre proveedores, un enrutamiento más rápido, el cifrado punto a punto según IPSec y la conectividad mediante la misma dirección al cambiar de red (Mobile IPv6).

Las direcciones IPv6 se escriben entre corchetes en las URL. Un puerto específico se puede indicar de a siguiente manera: http://[[2001:0da8:65b4:05d3:1315:7c1f:0461:7847]:8081/

9.2.2. Protocolos de transporte de datos para video en red

El Protocolo de control de transmisión (TCP, Transmission Control Protocol) y el Protocolo de

datagramas de usuario (UDP, User Datagram Protocol) son los protocolos basados en IP que se utilizan para enviar datos. Estos protocolos de transporte actúan como portadores para muchos otros protocolos. Por ejemplo, HTTP (Hyper Text Transfer Protocol), que se utiliza para visualizar páginas web en servidores de todo el mundo a través de Internet, se realiza en TCP.

TCP proporciona un canal de transmisión fiable basado en la conexión. Gestiona el proceso de división de grandes bloques de datos en paquetes más pequeños y garantiza que los datos enviados desde un extremo se reciban en el otro. La fiabilidad de TCP en la retransmisión puede producir retrasos significativos, por lo que en general se utiliza cuando la fiabilidad de la comunicación prevalece sobre la latencia del transporte.

UDP es un protocolo sin conexión que no garantiza la entrega de los datos enviados, dejando así todo el mecanismo de control y comprobación de errores a cargo de la propia aplicación. No proporciona transmisiones de pérdida de datos, por lo que no provoca retrasos adicionales. ■

Protocolos y puertos TCP/IP utilizados para video en red

Protocolo	Transporte	Puerto	Uso habitual	Uso en video en red
FTP (Protocolo de transferencia de ficheros)	TCP	21	Transferencia de archivos a través de Internet/intranets.	Transferencia de imágenes o video desde un codificador de vídeo/cámara de red a un servidor FTP o a una aplicación.
SMTP (Protocolo simple de transferencia de correo)	TCP	25	Envío de mensajes de correo electrónico.	Un codificador de video/cámara de red puede enviar imágenes o notificaciones de alarma utilizando su cliente de correo electrónico integrado.
HTTP (Protocolo de transferencia de hipertexto)	TCP	80	Se utiliza para navegar por la red, por ejemplo, para recuperar páginas web de servidores.	Es el modo más habitual para transferir video de un codificador de vídeo/cámara de red, en el que el dispositivo de video en red funciona básicamente como servidor web que pone el video a disposición del usuario o del servidor de aplicaciones que lo solicita.
HTTPS (Protocolo de transferencia de hipertexto sobre capa de sockets)	TCP	443	Acceso seguro a páginas web con tecnología de cifrado.	Transmisión segura de video procedente de codificadores de video/cámaras de red.
RTP (Real Time Protocol)	UDP/TCP	No definido	Formato de paquete RTP estandarizado para la entrega de audio y de video a través de Internet (a menudo utilizado en sistemas de transmisión multimedia o videoconferencia).	Un modo habitual de transmitir video en red basado en H.264/MPEG y de sincronizar video y audio, ya que RTP proporciona la numeración y la datación secuencial de paquetes de datos, lo que permite volver a unirlos en el orden correcto. La transmisión se puede realizar mediante unidifusión o multidifusión.
RTSP (Protocolo de transmisión en tiempo real)	TCP	554	Utilizado para configurar y controlar sesiones multimedia a través de RTP	Utilizado para configurar y controlar sesiones multimedia a través de RTP

Tecnologías de red

Se utilizan diversas tecnologías de red para proporcionar las numerosas ventajas de un sistema de video en red. Este capítulo comienza con unos apartados dedicados a la red de área local, concretamente a las redes Ethernet y sus componentes compatibles. También se tratan el uso de la alimentación a través de Ethernet, las direcciones IP y el transporte de datos, entre otros temas.

\\ Cap. IX
Segunda Parte

Indice

Capítulo 1.
Video en red (Pág. 18)
Capítulo 2.
Cámaras de red /Cámaras IP (Pág. 32)
Capítulo 3.
Elementos de la cámara (Pág. 48)
Capítulo 4.
Protección de la cámara y carcasas (Pág. 68)
Capítulo 5.
Codificadores de video (Pág. 80)
Capítulo 6.
Resoluciones (Pág. 92)
Capítulo 7
Compresión de video (Pág. 110)
Capítulo 8.
Audio (Pág. 120)
Capítulo 9.
Tecnologías de red
1ra. Parte (Pág. 132)
2da. Parte
9.3. *VLAN*
9.4. *Calidad de servicio*
9.5. *Seguridad en red*
9.5.1. *Autenticación mediante nombre de usuario y contraseña*
9.5.2. *Filtro de direcciones IP*
9.5.3. *IEEE 802.1X*
9.5.4. *HTTPS o SSL/TLS*
9.5.5. *VPN (Red privada virtual)*
Capítulo 10.
Tecnología inalámbrica
Capítulo 11.
Sistemas de gestión de video
Capítulo 12.
Consideraciones sobre ancho de banda y almacenamiento

9.3 VLAN

Al diseñar un sistema de video en red, a menudo existe la intención de mantener la red sin contacto con otras redes por motivos tanto de seguridad como de rendimiento. A primera vista, la elección obvia sería construir una red independiente. Aunque esto simplificaría el diseño, los costos de adquisición, instalación y mantenimiento probablemente serían más elevados que si se utilizara una tecnología de red virtual de área local (VLAN).

VLAN es una tecnología que segmenta las redes de forma virtual, una funcionalidad que admiten la mayoría de conmutadores de red. Esto se consigue dividiendo los usuarios de la red en grupos lógicos. Sólo los usuarios de un grupo específico pueden intercambiar datos o acceder a determinados recursos en la red. Si un sistema de video en red se segmenta en una *VLAN*, sólo los servidores ubicados en dicha *LAN* podrán acceder a las cámaras de red. Normalmente, las LAN conforman una solución mejor y más rentable que una red independiente. El protocolo que se utiliza principalmente al configurar *VLAN* es IEEE 802.1Q, que etiqueta cada marco o paquete con bytes adicionales para indicar a qué red virtual pertenece.

En este gráfico, las VLAN se configuran en varios conmutadores. Primero cada LAN se segmenta en VLAN 20 y VLAN 30. Los vínculos entre los conmutadores transportan los datos de las distintas VLAN. Sólo los miembros de la misma VLAN pueden intercambiar datos, ya sea dentro de la misma red o a través de redes distintas. Las VLAN se pueden utilizar para separar una red de video de una red de oficina.

9.4. Calidad de servicio

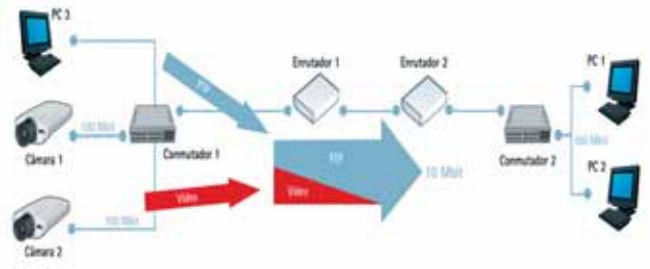
Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y videovigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de maneras distintas para cada tipo de servicio (voz, datos y video) del tráfico de la red.

Continúa en página 152

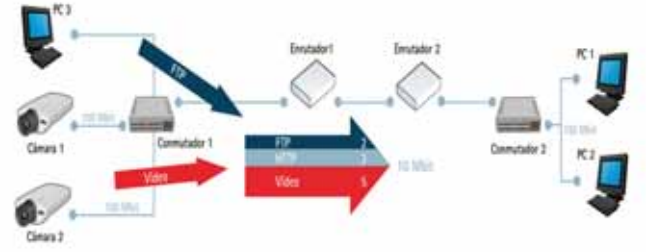
Viene de página 148

Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

El término Calidad de servicio hace referencia a una cantidad de tecnologías, como DSCP (Differentiated Service Codepoint), que pueden identificar el tipo de datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío. Las ventajas principales de una red sensible a la QoS son la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso del ancho de banda. El tráfico PTZ, que a menudo se considera crítico y requiere una latencia baja, es un caso típico en el que la QoS puede garantizar respuestas rápidas a solicitudes de movimiento. El requisito previo para utilizar QoS en una red de video es que todos los conmutadores, enrutadores y productos de video en red admitan QoS.



Red ordinaria (sin QoS). En este ejemplo, PC1 está reproduciendo dos secuencias de video de las cámaras 1 y 2. Cada cámara transmite a 2,5 Mbit/s. De repente, PC2 inicia una transferencia de archivos desde PC3. En este escenario, la transferencia de archivos intentará utilizar la capacidad total de 10 Mbit/s entre los enrutadores 1 y 2, mientras que las secuencias de video intentarán mantener su total de 5 Mbit/s. Así, ya no se puede garantizar la cantidad de ancho de banda destinada al sistema de vigilancia y probablemente se reducirá la frecuencia de imagen de video. En el peor de los casos, el tráfico del FTP consumirá todo el ancho de banda disponible.



Red con QoS. En este escenario, se ha configurado el enrutador 1 para dedicar hasta 5 Mbit/s de los 10 disponibles a la transmisión de video. El tráfico del FTP puede utilizar un máximo de 2 Mbit/s, y HTTP, junto con el resto del tráfico, pueden utilizar un máximo de 3Mbit/s. Con esta división, las transmisiones de video siempre tendrán disponible el ancho de banda que necesitan. Las transferencias de archivos se consideran menos importantes y, por lo tanto, obtienen menor ancho de banda; sin embargo, aún quedará ancho de banda disponible para la navegación web y el resto del tráfico. Hay que tener en cuenta que estos valores máximos sólo se aplican en caso de congestión en la red. El ancho de banda disponible que no se use se podrá utilizar por cualquier tipo de tráfico.

9.5. Seguridad de red

Existen varios niveles de seguridad para proteger la información que se envía a través de las redes IP. El primer nivel es la autenticación y la autorización. El usuario o dispositivo se identifica en la red y en el extremo remoto con un nombre de usuario y una contraseña, que se verifican antes de permitir que el dispositivo entre en el sistema. Se puede conseguir seguridad adicional cifrando los datos para evitar que otros usuarios los utilicen o los lean. Los métodos más habituales son HTTPS (también conocido como SSL/TLS), VPN y WEP o WPA en redes inalámbricas. El uso del cifrado puede ralentizar las comunicaciones en función del tipo de implementación y cifrado utilizados.

9.5.1. Autenticación mediante nombre de usuario y contraseña

La autenticación mediante nombre de usuario y contraseña es el método más básico para proteger los datos en una red IP. Este método debería ser suficiente en escenarios que no requieran niveles de seguridad elevados o en los que la red de video esté separada de la red principal y los usuarios no autorizados no puedan acceder físicamente a ella. Las contraseñas se pueden cifrar o descifrar cuando se envían. La primera opción es la más segura.

9.5.2. Filtro de direcciones IP

Los productos de video en red proporcionan un filtro de direcciones IP, que concede o deniega los derechos de acceso a las direcciones definidas. Una de las configuraciones habituales de las cámaras de red es la de permitir que únicamente la dirección IP del servidor que hospeda el software de gestión de video pueda acceder a los productos de video en red.

9.5.3. IEEE 802.1X

Muchos productos de video en red son compatibles con IEEE 802.1X, que proporciona autenticación a los dispositivos vinculados a un puerto LAN. El estándar IEEE 802.1X establece una conexión punto a punto o impide el acceso desde el puerto de la LAN si la autenticación es errónea. También evita el denominado "porthi-jacking", es decir, el acceso de un equipo no autorizado a una red mediante una toma de red del interior o del exterior de un edificio. IEEE 802.1X resulta útil en aplicaciones de video en red, ya que a menudo las cámaras de red están colocadas en espacios públicos en los que una toma de red accesible puede suponer un riesgo para la seguridad. En las redes de las empresas en la actualidad, el estándar IEEE 802.1X se está convirtiendo en un requisito básico para establecer cualquier conexión a una red.

En un sistema de video en red, IEEE 802.1X funciona como se indica a continuación:

1) Una cámara de red envía una solicitud de acceso a la red a un conmutador o punto de acceso

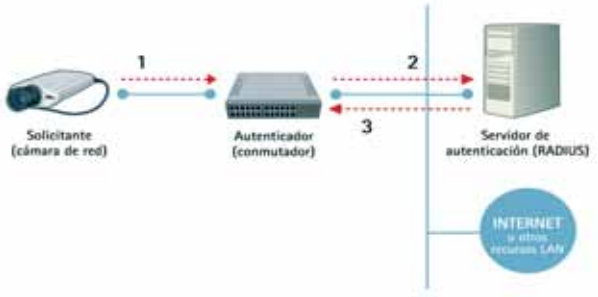
2) El conmutador o punto de acceso reenvía la consulta a un servidor de autenticación, por ejemplo, un servidor RADIUS (Remote Authentication Dial-In User Service) como Microsoft Internet Authentication Service

3) Si la autenticación se realiza correctamente, el servidor indica al conmutador o punto de acceso que abra el puerto para permitir el paso de los datos procedentes de la

Continúa en página 156

Viene de página 152

cámara por el conmutador y así enviarlos a través de la red.



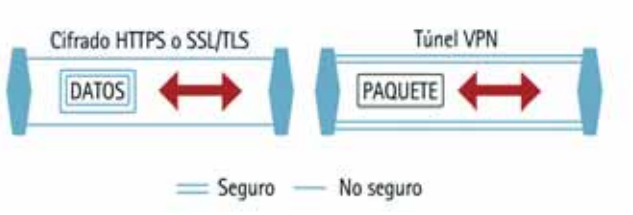
IEEE 802.1X habilita la seguridad basada en puertos, en la que participan un solicitante (una cámara de red), un autenticador (un conmutador) y un servidor de autenticación. Paso 1: se solicita el acceso a la red; Paso 2: la solicitud se reenvía al servidor de autenticación; Paso 3: la autenticación se realiza correctamente y se indica el conmutador que permita que la cámara de red envíe los datos a través de la red.

9.5.4. HTTPS o SSL/TLS

El protocolo HTTPS (Hyper Text Transfer Protocol Secure) es idéntico a HTTP excepto en una diferencia clave: los datos transferidos se cifran con Capa de sockets seguros (SSL) o Seguridad de la capa de transporte (TLS). Este método de seguridad aplica el cifrado a los propios datos. Muchos productos de video en red son compatibles con HTTPS, lo que permite la visualización segura de video en un navegador web. Sin embargo, el uso de HTTPS puede ralentizar el enlace de comunicación, en consecuencia, la frecuencia de imagen del video.

9.5.5. VPN (Red privada virtual)

Con una VPN se puede crear un "túnel" de comunicación seguro entre dos dispositivos y, por lo tanto, una comunicación segura a través de Internet. En esta configuración, se cifra el paquete original, incluidos los datos y su cabecera, que puede contener información como las direcciones de origen y destino, el tipo de información que se envía, el número de paquete en la secuencia y la longitud del paquete. A continuación, el paquete cifrado se encapsula en otro paquete que solo muestra las direcciones IP de los dos dispositivos de comunicación, es decir, los enrutadores. Esta configuración protege el tráfico y su contenido del acceso no autorizado, y sólo permite que trabajen dentro de la VPN los dispositivos con la clave correcta. Los dispositivos de red entre el cliente y el servidor no podrán acceder a los datos ni visualizarlos.



La diferencia entre HTTPS (SSL/TLS) y VPN es que en HTTPS sólo se cifran los datos reales de un paquete. Con VPN se puede cifrar y encapsular todo el paquete para crear un "túnel" seguro. Ambas tecnologías se pueden utilizar en paralelo, aunque no se recomienda, ya que cada tecnología añadirá una carga adicional que puede disminuir el rendimiento del sistema. ■

MAXIMPORT
EQUIPOS DE COMUNICACIONES - GPS TRACKING
REPARACIONES - ACCESORIOS - BATERIAS - MEGAFONOS
GPS TRACKER PERSONAL
* Boton de Panico.
* Quad Band GSM
* Motion Switch
* Parlante Microfono
* SMS/GPRS
* UDP/TCP
* Bateria de 2760/5750/11500mAh.
* Fastest Tracking Interval 12 Seg.
* Modo Sleep hasta 3 Años
BFDX
BF-8700
$ 548.00 IVA Inc.
*16 Canales
*136-174 / 430-470/ 470-512MHz.
*4/5 Wts.
*CTCSS/DCS
* Bateria Li-Ion
* Cargador Mesa
GARANTIA 1 AÑO
Vertex Standard
VX-231
Consultar
*16 Canales
*136-174 / 430-470/ 470-512MHz.
*4/5 Wts.
*CTCSS/DCS
* Bateria Ni-MH
* Cargador Mesa
GARANTIA 1 AÑO
MOTOROLA
EP450
Consultar
*16 Canales
*136-174 / 430-470/ 470-512MHz.
*4/5 Wts.
*CTCSS/DCS
* Bateria Li-Ion
* Cargador Mesa
GARANTIA 1 AÑO
ACCESORIOS ORIGINALES / GENERICOS
MEGAFONOS MANO Y CINTURA
AV. GAONA 3510 - C1416DSX CIUDAD DE BUENOS AIRES info@maximport.com.ar
TEL: (011)4637-3003 FAX: (011)4637-3111 www.maximport.com.ar