Tecnologías de red


Sergio Fukushima
Technical Manager South America
de Axis Communications
sergio.fukushima@axis.com

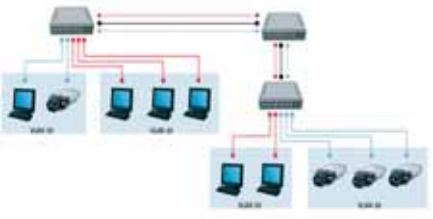
Se utilizan diversas tecnologías de red para proporcionar las numerosas ventajas de un sistema de video en red. Este capítulo comienza con unos apartados dedicados a la red de área local, concretamente a las redes Ethernet y sus componentes compatibles. También se tratan el uso de la alimentación a través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

Indice

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

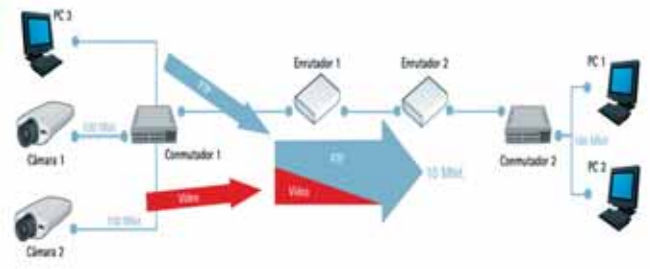
Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y videovigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores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

Continúa en página 108

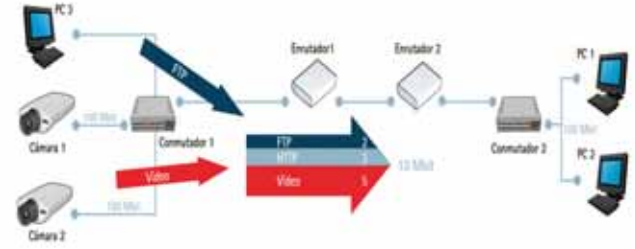
Viene de página 104

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

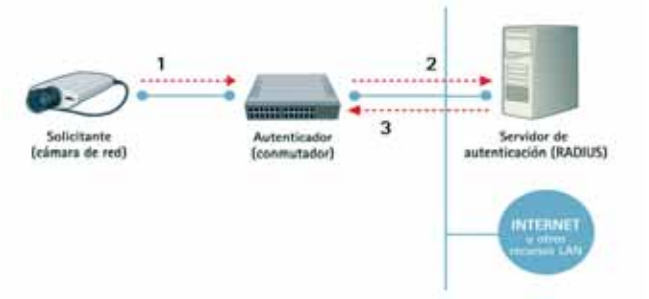
2) El conmutador o punto de acceso reenvía la consulta a un servidor de autenticación, por ejemplo, un servidor RADIUS (Remote Authentication Dial-In User Service) como Microsoft Internet Authentication Service

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 112

Viene de página 108

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



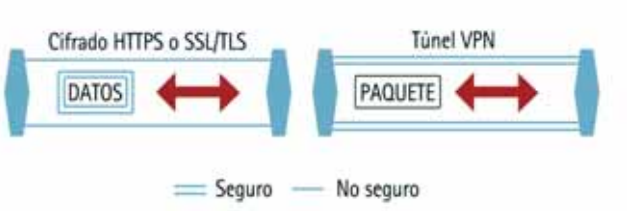
IEEE 802.1X habilita la seguridad basada en puertos, en la que participan un solicitante (una cámara de red), un autenticador (un conmutador) y un servidor de autenticación. Paso 1: se solicita el acceso a la red; Paso 2: la solicitud se reenvía al servidor de autenticación; Paso 3: la autenticación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