

Tecnología inalámbrica

Sergio Fukushima

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



Detallamos en entregas anteriores las tecnologías de red y las distintas variantes de configuración, autenticación y seguridad. En este caso nos ocupamos de las redes inalámbricas, especialmente utilizadas para cubrir grandes áreas como los sistemas de vigilancia para Monitoreo Urbano. Detallamos a continuación recomendaciones, estándares y seguridad de las mismas.



El material técnico que se publica en este informe fue proporcionado por Axis Communications a Revista Negocios de Seguridad®. Prohibida su reproducción (parcial o total) sin el expreso consentimiento del autor o este medio.

■ Índice

Capítulo 1.

Video en red (RNDS N° 45)

Capítulo 2.

Cámaras de red /Cámaras IP (RNDS N° 46)

Capítulo 3.

Elementos de la cámara (RNDS N° 47)

Capítulo 4.

Protección de la cámara y carcacas (RNDS N° 48)

Capítulo 5.

Codificadores de video (RNDS N° 49)

Capítulo 6.

Resoluciones (RNDS N° 51)

Capítulo 7

Compresión de video (RNDS N° 52)

Capítulo 8.

Audio (RNDS N° 53)

Capítulo 9.

Tecnologías de red

1ra. Parte (RNDS N° 54)

2da. Parte (RNDS N° 54)

Capítulo 10.

Tecnología inalámbrica

10.1. Estándares WLAN 802.11

10.2. Seguridad WLAN

10.2.1. WEP (Wired Equivalent Privacy)

10.2.2. WPA/WPA2 (WiFi Protected Access)

10.2.3. Recomendaciones

10.3. Puentes inalámbricos

Capítulo 11.

Sistemas de gestión de video

Capítulo 12.

Consideraciones sobre ancho de banda y almacenamiento

En aplicaciones de videovigilancia, la tecnología inalámbrica es una manera flexible, rentable y rápida de implantar cámaras, especialmente en sistemas que cubren grandes áreas como sistemas de vigilancia estacionamientos, aeropuertos y monitoreo urbano público, ya que elimina la necesidad de utilizar cables terrestres. Además, en edificios antiguos protegidos en los que no se permite la instalación de cables Ethernet, la tecnología inalámbrica pasa a ser la única alternativa.

En general, el mercado ofrece cámaras con soporte inalámbrico integrado. Asimismo, las cámaras de red sin tecnología inalámbrica integrada también se pueden incorporar a una red inalámbrica mediante el uso de un puente.



Mediante el uso de un puente inalámbrico, cualquier cámara de red se puede utilizar en una red inalámbrica.

10.1. Estándares WLAN 802.11

El estándar más habitual para redes inalámbricas de área local (WLAN) es la norma IEEE 802.11. Si bien existen otros estándares y otras tecnologías patentadas, la ventaja de utilizar los estándares inalámbricos 802.11 es que funcionan en un ámbito sin licencia, de manera que no implican ningún coste asociado a la configuración y al funcionamiento de la red. Las extensiones más relevantes del estándar son 802.11b, 802.11g, 802.11a y 802.11n.

La extensión 802.11b, aprobada en 1999, funciona a 2,4 GHz y proporciona velocidades de hasta 11 Mbit/s. Hasta el año 2004, la mayoría de productos WLAN que se vendían se basaban en esta extensión.

La extensión 802.11g, aprobada en 2003, es la variedad más común de 802.11 del mercado. Funciona a 2,4 GHz y proporciona velocidades de hasta 54 Mbit/s. En general, los productos WLAN son compatibles con 802.11b/g.

La extensión 802.11a, aprobada en 1999, funciona en la frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbit/s. En algunas partes de Europa, la banda de frecuencia de 5 GHz no está disponible, ya que se utiliza para sistemas de radares militares. En estas áreas, los com-

Continúa en página 160

Viene de página 156

ponentes WLAN a 5 GHz deben cumplir el estándar 802.11a/h. Otra desventaja de la extensión 802.11a es que la cobertura de la señal es inferior a la de 802.11g, ya que funciona en una frecuencia superior. Así, se requieren muchos más puntos de acceso para la transmisión en 5 GHz que en la de 2.4 GHz.

La extensión 802.11n, que aún no está completada ni ratificada, ejemplifica la siguiente generación de estándares y ofrecerá velocidades de hasta 600 Mbit/s. Los productos compatibles con 802.11n se basan en una versión preliminar.

Al configurar una red inalámbrica es importante tener en cuenta la capacidad de ancho de banda del punto de acceso y los requisitos de ancho de banda de los dispositivos de red. Normalmente, el caudal de datos útil admitido por un estándar WLAN específico es aproximadamente la mitad de la tasa de bits estipulada por el mismo debido a la sobrecarga de la señal y del protocolo. En el caso de las cámaras compatibles con 802.11g, no deben conectarse más de cuatro o cinco cámaras a un punto de acceso inalámbrico.

10.2 Seguridad WLAN

Debido a la naturaleza de las comunicaciones inalámbricas, cualquier dispositivo inalámbrico presente en un área cubierta por una red inalámbrica podrá utilizarla e interceptar datos transferidos en la misma a menos que esté protegida.

Para evitar el acceso no autorizado a los datos transferidos y a la red se han desarrollado tecnologías de seguridad, como WEP y WPA/WPA2, que impiden el acceso no autorizado y cifran los datos que se envían a través de la red.

10.2.1. WEP (Wired Equivalent Privacy)

La WEP evita que los usuarios accedan a la red sin la clave correcta. No obstante, tiene puntos débiles, como claves rela-

tivamente cortas y otros defectos que permiten que las claves se reconstruyan a partir de una cantidad relativamente pequeña de tráfico interceptado. Actualmente, ya no se considera que la WEP proporcione la seguridad necesaria, ya que en Internet se pueden encontrar utilidades que descifran lo que debería ser una clave WEP secreta.

10.2.2 WPA/WPA2 (WiFi Protected Access)

El WPA aumenta significativamente la seguridad, ya que trata las deficiencias del estándar WEP. Asimismo, el WPA incorpora un método estándar de distribución de claves cifradas.

10.2.3 Recomendaciones

A continuación, se enumeran algunas directrices de seguridad para el uso de cámaras inalámbricas de vigilancia:

- Habilitar el inicio de sesión mediante usuario y contraseña en las cámaras.
- Habilitar el cifrado (HTTPS) en las cámaras y en el enrutador inalámbricos. Esto debe realizarse antes de establecer las claves o credenciales de WLAN para evitar el acceso no autorizado a la red con credenciales robadas.
- Garantizar que las cámaras inalámbricas sean compatibles con protocolos de seguridad como IEEE 802.11X y WPA/WPA2.

10.3. Puentes inalámbricos

Algunas soluciones pueden utilizar estándares distintos a la norma 802.11 predominante para mejorar el rendimiento y cubrir distancias mucho mayores, además de aumentar la seguridad. Dos tecnologías utilizadas habitualmente son la de microondas y el láser, que pueden utilizarse para conectar edificios o lugares con enlaces de datos punto a punto de alta velocidad. ■