Informe técnico

Guía rápida de las fichas técnicas de Axis

Homologaciones, certificaciones y protocolos

Febrero de 2019

Índice

1. Introducción

Axis Communications cumple las normas aplicables del sector y las normativa de cumplimiento obligado en todos los productos que lanza al mercado. Este documento complementa las fichas técnicas de Axis con definiciones y descripciones simplificadas de las siglas, homologaciones, certificaciones y protocolos que figuran en las mismas.

En la versión actual, este documento proporciona información sobre los apartados de las fichas técnicas que están resaltados y ampliados en la imagen que se muestra a continuación.

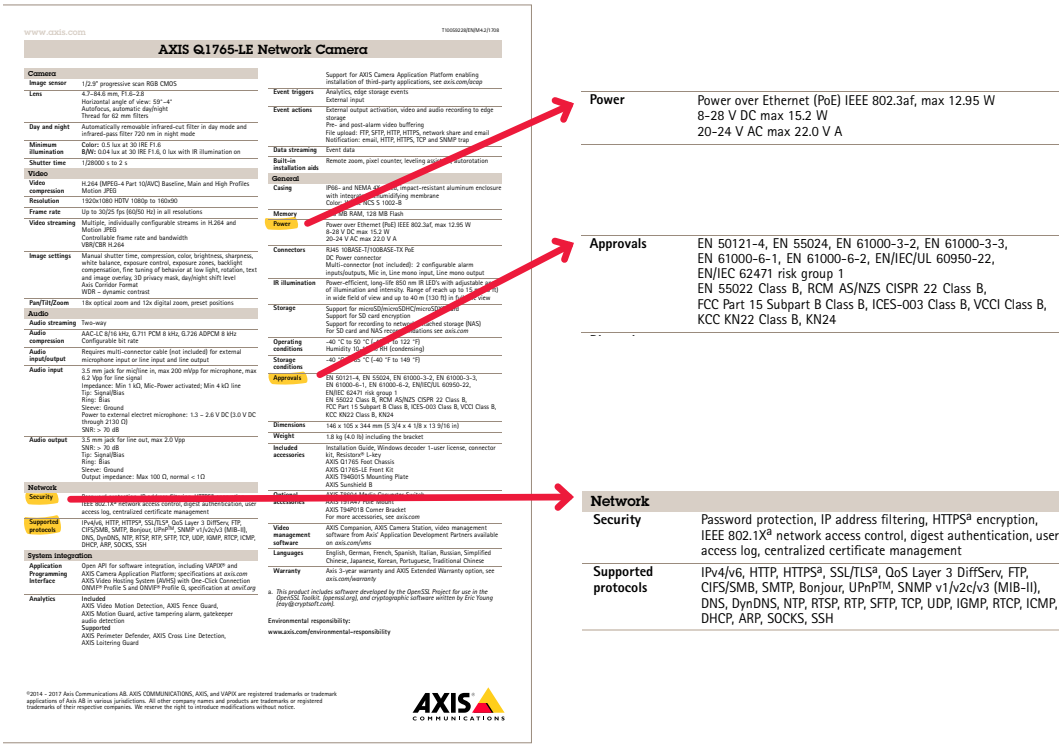

Figura 1. Apartados de la ficha técnica de Axis resaltados en los que se centra el documento actual.

2. Homologaciones

El apartado de homologaciones de las fichas técnicas de Axis se refiere al cumplimiento de diversas normas. El apartado se subdivide a menudo en otras secciones dedicadas a CEM, Seguridad, Medio Ambiente y Otros, donde "Otros" puede referirse a la protección contra explosiones o a la seguridad en el control de acceso. También puede haber una subdivisión para las homologaciones que afecten al midspan, en aquellos casos en los que se venda un midspan con el producto.

2.1 CEM (compatibilidad electromagnética)

Todos los fabricantes de vídeo en red deben declarar la CEM de sus productos de vídeo en red. En algunas circunstancias, los fabricantes pueden autocertificarse, pero la mayoría de ellos recurren a laboratorios de pruebas acreditados que proporcionan un informe para verificar el cumplimiento de las normas. Las homologaciones de CEM tienen dos partes, emisión e inmunidad, como se indica a continuación.

La emisión se refiere a la capacidad del equipo para funcionar satisfactoriamente sin emitir demasiada energía electromagnética que pueda perturbar a otros equipos ubicados en ese entorno.

La inmunidad es un indicador de la capacidad de los productos electrónicos para tolerar la influencia de fenómenos electromagnéticos y la energía eléctrica (radiada o conducida) de otros productos electrónicos. En Europa, la CEM está incluida en la marca CE, que a su vez está recogida en la legislación sobre armonización de la UE.
Las normas que se enumeran a continuación definen los límites y métodos de prueba de emisiones electromagnéticas, así como las pruebas de inmunidad. Puesto que no existe una única prueba que abarque el cumplimiento de forma global, cada región o aplicación puede tener un código diferente.

2.1.1 Normas aplicables a los equipos de tecnología de la información (ETI)

> EN 55022 Clase A: norma sobre emisiones (comercial, industrial, empresarial), armonizada con las normas internacionales

> EN 55022 Clase B: norma sobre emisiones (residencial), armonizada con las normas internacionales

> EN 55024 Clase A: norma sobre inmunidad (comercial, industrial), armonizada con las normas internacionales

> EN 55024 Clase B: norma sobre inmunidad (residencial), armonizada con las normas internacionales

2.1.2 Normas armonizadas por país o región

> EN 61000-6: normas de cumplimiento genéricas (Europa)

> FCC Parte 15 Subparte B Clase A y B: FCC dicta reglas y normativas para dispositivos de telecomunicaciones; consulte las disposiciones sobre emisiones, no sobre inmunidad (Estados Unidos)

> ICES-003 Clase A y B (Canadá)

> VCCI (Japón)

> KN22, KN24, KN32, KN35 (Corea)

> CISPR 22 Clase A y B (Australia/Nueva Zelanda)

2.1.3 Normas adicionales por aplicación o producto

> EN 50121-4, IEC 62236-4: ofrece criterios de rendimiento para equipos de señalización y telecomunicaciones que podrían interferir con otros equipos en entornos ferroviarios.

> EN 50130-4: se aplica a los componentes de sistemas de alarma, como sistemas de control de acceso, sistemas CCTV, sistemas de detección y alarmas contra incendios, sistemas de alarma contra intrusos, sistemas de alarma sociales.

> EN 55032 (emisiones) – EN 55035 (inmunidad): se aplica a los equipos multimedia (EMM) con una fuente de CA o CC que no sobrepasa los 600 V. Por equipo multimedia se entiende un equipo de tecnología de la información (ETI), equipo de audio, equipo de vídeo, equipo receptor de difusiones, equipo de control de iluminación para eventos de entretenimiento.

2.2 Seguridad

> Directiva sobre baja tensión (2014/35/UE): proporciona objetivos generales para la seguridad de los equipos eléctricos. Garantiza que los productos se puedan usar de forma segura sin riesgo de que se produzcan lesiones físicas o daños materiales.

> IEC/EN/UL 60950-1: cumplimiento por parte de cámaras de red, codificadores y fuentes de alimentación de los requisitos dispuestos para reducir los riesgos de incendio, descarga eléctrica o lesión en cualquier persona que pudiera entrar en contacto con el equipo.

> IEC/EN/UL 60950-22: requisitos de seguridad específicos para productos de exterior y carcasas de exterior.

> IEC/EN 62471: requisitos para límites de exposición, evita los peligros para los ojos y la piel.

> EN 62368-1: sustituye a la norma EN 60950, pero ambas coexistirán hasta 2019. La IEC y UL desarrollan normas gemelas con la misma referencia.

> EN/UL/CSA 60065: se aplica a los aparatos electrónicos diseñados para recibir corriente de la red eléctrica de un equipo de abastecimiento, de baterías o de una fuente de alimentación remota, y que tienen por finalidad recibir, generar, grabar o reproducir audio, vídeo o señales asociadas.

2.3 Entorno

2.3.1 Clasificación IP

La IEC (International Electrotechnical Commission; Comisión Electrotécnica Internacional), en su norma IEC 60529, define las clasificaciones IP (protección contra entrada o protección internacional) con un código de dos dígitos. Dicho código define el nivel de protección de los aparatos eléctricos contra la entrada de objetos sólidos o polvo, el contacto accidental y el agua.

Tabla 1. Clasificación IP, primer dígito (IP**x**x): objetos sólidos extraños

Nivel	Protección contra	Eficaz contra
0	Sin protección	Sin protección
1	Objetos de más de 50 mm	Superficie extensa del cuerpo, como el dorso de la mano, pero sin protección contra el contacto deliberado con una parte del cuerpo.
2	Objetos de más de 12,5 mm	Los dedos u otros objetos pueden penetrar hasta 80 mm, siempre y cuando estén a salvo de piezas peligrosas. Los objetos con un diámetro de 12,5 mm no pueden penetrar en su totalidad.
3	Objetos de más de 2,5 mm	Objetos como herramientas y alambres gruesos no pueden penetrar de ninguna forma.
4	Objetos de más de 1 mm	Objetos como alambres y tornillos no pueden penetrar de ninguna forma.
5	Protección contra el polvo	No se evita por completo la penetración del polvo, aunque esta no se produce en un volumen suficiente como para impedir que el equipo funcione correctamente.
6	Estanco al polvo	Sin penetración de polvo

Tabla 2. Clasificación IP, segundo dígito (IPx**x**): líquidos

Nivel	Protección contra	Eficaz contra
0	Sin protección	Sin protección especial
1	Goteo de agua	El goteo de agua (gotas que caen verticalmente) no tiene efectos perjudiciales.
2	Goteo de agua con una inclinación de hasta 15º	El goteo de agua en vertical no tiene efectos perjudiciales si la carcasa se inclina en un ángulo de hasta 15° con respecto a su posición normal.
3	Pulverización de agua	La pulverización de agua a un ángulo de hasta 60° con respecto a la línea vertical no tiene efectos perjudiciales.
4	Salpicadura de agua	El agua proyectada contra la carcasa desde cualquier dirección no tiene efectos perjudiciales.
5	Agua a presión	Los chorros de agua proyectados desde una boquilla contra la carcasa desde cualquier dirección no tienen efectos perjudiciales.
6	Agua a alta presión	Los oleajes intensos o el agua proyectada en chorros potentes no pueden penetrar en la carcasa en un volumen perjudicial.
7	Inmersión breve en agua	No resulta posible la penetración de un volumen perjudicial de agua cuando se sumerge la carcasa en agua en unas determinadas condiciones de presión y tiempo.
8	Inmersión continua en agua	El equipo es apto para una inmersión continua en agua en determinadas condiciones, especificadas por el fabricante. Las condiciones deben ser más rigurosas que para IPX7 (véanse las entradas anteriores).
9	Agua de limpieza a alta presión y con chorro de vapor	El agua dirigida hacia la carcasa desde cualquier ángulo a muy alta presión no tiene efectos perjudiciales.

2.3.2 Otras normas IEC relevantes

> IEC 60068-2 es una norma para la realización de pruebas ambientales de equipos y productos electrónicos que tiene por finalidad evaluar su capacidad de ofrecer resultados en condiciones ambientales tales como el frío y el calor seco extremos. Los procedimientos que se indican a continuación con respecto a esta norma suelen estar dirigidos a objetos que alcanzan una temperatura estable durante el procedimiento de prueba.

- IEC 60068-2-1: frío
- IEC 60068-2-2: calor seco
- IEC 60068-2-6: vibración (continua)
- IEC 60068-2-14: cambio de temperatura
- IEC 60068-2-27: impactos
- IEC 60068-2-30: calor húmedo (cíclico)
- IEC 60068-2-64: vibración (ancho de banda aleatorio)
- IEC 60068-2-78: calor húmedo (estable)

> IEC 60825 Clase I es una norma dirigida a asegurar que el tipo de láser empleado en el módulo de enfoque de láser resulte seguro en todo tipo de condiciones de uso normal.

2.3.3 Clasificación NEMA

NEMA (National Electrical Manufacturers Association) es una asociación estadounidense que ofrece normas para carcasas de equipos eléctricos. NEMA ha presentado su propia norma, NEMA 250, a nivel mundial. NEMA también ha adoptado y publicado una norma IP de armonización, ANSI/IEC 60529, por medio del American National Standards Institute (ANSI).

NEMA 250 comprende la protección contra la entrada de materias, pero también otros factores como la resistencia a la corrosión, el rendimiento y los detalles de construcción. Por ello, el tipo NEMA es comparable a IP, si bien IP no es comparable a NEMA.

Las normas de UL, UL 50 y UL 50E, se basan en la norma NEMA 250. NEMA permite la autocertificación, mientras que UL exige que los productos superen unas pruebas e inspecciones de terceros para obtener el nivel de cumplimiento.

Tabla 3. Clasificaciones NEMA para carcasas en lugares no peligrosos

NEMA	Clasificación IP equivalente	Interiores	Exteriores	Protección contra
Tipo 1	IP10	X		Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Sin protección contra líquidos.
Tipo 3	IP54	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve). No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 3R	IP14	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Entrada de agua (lluvia, aguanieve, nieve). No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 3S	IP54	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve). Los mecanismos externos permanecen operativos cuando se cargan de hielo.
Tipo 4	IP56	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve, salpicaduras de agua y chorro de agua con manguera). No resultará dañado por la formación de hielo en el exterior de la carcasa.
NEMA 4X	IP56	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo arrastrado por el viento). Entrada de agua (lluvia, aguanieve, nieve, salpicaduras de agua y chorro de agua con manguera). Proporciona un nivel de protección adicional contra la corrosión. No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 6	IP67	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Entrada de agua (agua dirigida con una manguera y entrada de agua durante una inmersión temporal puntual a poca profundidad). No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 6P	IP67	X	X	Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión). Entrada de agua (agua dirigida con una manguera y entrada de agua durante una inmersión prolongada a poca profundidad). Proporciona un nivel de protección adicional contra la corrosión. No resultará dañado por la formación de hielo en el exterior de la carcasa.
Tipo 12	IP52	X		Sin paneles de desmontaje rápido. Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo en circulación, pelusa, fibras y residuos proyectados). Entrada de agua (goteo y salpicaduras ligeras).
Tipo 12K	IP52	X		Con paneles de desmontaje rápido. Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo en circulación, pelusa, fibras y residuos proyectados). Entrada de agua (goteo y salpicaduras ligeras).
Tipo 13	IP54	X		Acceso a componentes peligrosos y entrada de objetos sólidos extraños (suciedad en suspensión y polvo en circulación, pelusa, fibras y residuos proyectados). Entrada de agua (goteo y salpicaduras ligeras). Pulverizaciones, salpicaduras y escapes de aceite y refrigerantes no corrosivos.

2.3.4 Clasificación IK

La clasificación IK se puede encontrar en IEC/EN 62262, una norma internacional que especifica grados de protección frente a impactos mecánicos externos. Se aprobó inicialmente en 1994 como norma europea EN 50102 y se homologó como norma internacional en 2002.

Muchos fabricantes optan por someter a pruebas la parte más débil de un producto para garantizar su robustez a lo largo de toda su vida útil.

Tabla 4. Clasificación IK

Nivel	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
Energía del impacto (julios)	0,14	0,2	0,35	0,5	0,7	1	2	5	10	20	50*
Masa (kg)	<0,2	<0,2	0,2	0,2	0,2	0,5	0,5	1,7	5	5	
Altura de caída (mm)	56	80	140	200	280	400	400	300	200	400	

*Impacto hasta 50 J. El fabricante debe indicar la energía, la masa y la altura de caída del elemento causante del impacto.

2.4 Otras homologaciones

2.4.1 Protección contra explosiones

> EC/EN/UL/SANS/CSA 60079-0: requisitos generales para construcción, pruebas y marcado de equipos y componentes antideflagrantes diseñados para emplearse en atmósferas explosivas.

> IEC/EN/UL/SANS/CSA 60079-1: requisitos específicos para la construcción y pruebas de equipos eléctricos con el tipo de carcasas ignífugas de protección "d", diseñados para utilizarse en atmósferas con gases explosivos.

2.4.2 Homologaciones para midspan

En aquellos casos en los que se incluye un midspan con el producto, las homologaciones relacionadas de manera específica con el midspan se indican en este apartado de la ficha técnica. Se pueden obtener explicaciones en los apartados anteriores de este documento.

2.4.3 Seguridad en el control de acceso

> UL 294: define los requisitos relativos a la construcción, el rendimiento y el funcionamiento de sistemas de control de acceso.

3. Certificaciones

Cuando se instala una cámara en un entorno potencialmente explosivo, la carcasa debe cumplir unas normas de seguridad muy concretas. Debe proteger el entorno de posibles fuentes de deflagración presentes en la cámara y en otros equipos.

Los productos europeos deben cumplir con la directiva ATEX, y la norma internacional correspondiente es IECEx. En Norteamérica se utilizan principalmente las clasificaciones de clase/división de NEMA en detrimento del sistema de zonas descrito en ATEX e IECEx.

Tabla 5. Clasificaciones de protección contra explosiones

Clase / División	Atmósfera	Definición	Zona (IECEx y ATEX)
Clase I / División 1	Gas	Área donde la mezcla explosiva está presente de forma continua o presente durante largos periodos de tiempo.	Zona 0
Clase 1 / División 1	Gas	Área donde podría formarse una mezcla explosiva durante el funcionamiento normal.	Zona 1
Clase 1 / División 2	Gas	Área en la que es poco probable que se forme una mezcla explosiva durante el funcionamiento normal y, en caso de producirse, solo existirá durante un breve periodo de tiempo.	Zona 2
Clase II / División 1	Polvo	Área donde la mezcla explosiva está presente de forma continua o presente durante largos periodos de tiempo.	Zona 20
Clase II / División 1	Polvo	Área donde podría formarse una mezcla explosiva durante el funcionamiento normal.	Zona 21
Clase II / División 2	Polvo	Área en la que es poco probable que se forme una mezcla explosiva durante el funcionamiento normal y, en caso de producirse, solo existirá durante un breve periodo de tiempo.	Zona 22

4. Alimentación

4.1 Clases de Power over Ethernet (PoE)

Las clases de PoE garantizan una distribución eficiente de la energía al especificar la cantidad de energía que necesitará un dispositivo alimentado (DA).

Tabla 6. Clases de PoE

Clase	Tipo	Nivel de potencia garantizado en el equipo de fuente de alimentación (EFA)	Nivel de alimentación máximo empleado por el dispositivo alimentado (DA)
0	Tipo 1, 802.3af	15,4 W	0,44 W - 12,95 W
1	Tipo 1, 802.3af	40,0 W	0,44 W - 3,84 W
2	Tipo 1, 802.3af	7,0 W	3,84 W - 6,49 W
3	Tipo 1, 802.3af	15,4 W	6,49 W - 12,95 W
4	Tipo 2, 802.3at*	30 W	12,95 W - 25,5 W
6	Tipo 3, 802.3bt	60 W	51 W
8	Tipo 4, 802.3bt	100 W	71,3 W

*Este tipo también recibe el nombre de PoE+.

5. Red

5.1 Protección y control de seguridad

Hay varias formas de contrarrestar las amenazas dirigidas hacia los activos del sistema. Algunas amenazas suponen un riesgo para los dispositivos, mientras que otras constituyen un riesgo para las redes o los datos en tránsito o en almacenamiento. Los siguientes son algunos controles de seguridad seleccionados que se pueden aplicar a dispositivos y redes:

> Las credenciales (usuario y contraseña) protegen contra el acceso sin autorización a las imágenes de vídeo y evitan el acceso sin autorización a la configuración del dispositivo. Disponer de diferentes niveles de privilegios de cuentas permite controlar quién puede acceder a cada contenido.

> La filtración de IP (cortafuegos) reduce la exposición a la red local de un dispositivo y lo protege frente a clientes que intenten acceder a él sin autorización. Esto reduce los riesgos en caso de que se descubra la contraseña de un dispositivo y también mitiga los riesgos en caso de que se localice una nueva vulnerabilidad crítica.

> 802.1X: protege la red de clientes sin autorización. 802.1X es un sistema de protección de infraestructura de red que utiliza switches y un servidor RADIUS gestionados. El cliente de 802.1X instalado en el dispositivo ofrece autenticación al dispositivo que se encuentra en la red.

> HTTPS (Hypertext Transfer Protocol Secure; protocolo protegido para transferencia de hipertexto) protege los datos (vídeo) frente a interceptaciones en la red. El uso de certificados firmados en HTTPS proporciona un medio para que un cliente de vídeo detecte si está accediendo a una cámara auténtica o a un ordenador malintencionado que se hace pasar por una cámara.

Para acceder a más recursos sobre ciberseguridad, visite www.axis.com/cybersecurity

5.2 Protocolos compatibles

Son muchos los protocolos que intervienen cuando se transfieren datos de forma segura de un dispositivo en red a otro.

5.2.1 Modelos de referencia de protocolos

La mejor manera de entender cómo interactúan los diferentes protocolos es examinar el modelo de comunicación OSI (Open Systems Interconnection; interconexión de sistemas abiertos). También está el modelo de referencia TCP/IP.

5.2.1.1 Modelo de referencia OSI

Modelo que describe la comunicación de datos entre sistemas abiertos.
Para prestar un servicio, cada capa utiliza los servicios de la capa inmediatamente inferior.
Cada capa debe seguir determinadas reglas, o protocolos, para realizar servicios.

Capa 7: aplicación
Realiza funciones como transferencia web, de archivos y correos electrónicos para las aplicaciones.

Ejemplos
> Protocolo de transferencia de archivos (FTP)
> Protocolo sencillo de transferencia de correo (SMTP)
> Protocolo de transferencia de hipertexto (HTTP)

Las aplicaciones como tales, como es el caso de los navegadores web o los programas de correo electrónico, existen por encima de esta capa y no están cubiertas por el modelo OSI.

Capa 6: presentación (datos)
Garantiza que los datos enviados por la capa de aplicación de un sistema los pueda leer la aplicación de otro sistema. Convierte formatos de datos dependientes del sistema, como ASCII, en un formato independiente, permitiendo el intercambio de datos sintácticamente correctos entre diferentes sistemas.

Ejemplos
> Telnet
> Apple Filing Protocol

Capa 5: sesión (conexión persistente entre hosts pares)
Proporciona un servicio orientado a aplicaciones y se encarga de la comunicación de procesos entre dos sistemas. La comunicación de procesos comienza con el establecimiento de una sesión, que constituye la base para una conexión virtual entre dos sistemas.

Ejemplos
> Llamada de procedimiento remota
> Sistema de archivos de red

Capa 4: transporte (transporte de extremo a extremo [protocolo orientado a la conexión])
Proporciona un servicio fiable de transferencia de datos (a través del control de flujo y control de errores) a la capa 5 y superiores.

Ejemplos:
> Protocolo de control de transmisión (TCP)
> Protocolo de datagramas de usuarios (UDP)

Capa 3: red (paquete [direccionamiento/fragmentación])
Realiza la transferencia de datos propiamente dicha, enrutando y reenviando paquetes de datos entre sistemas. Crea y administra tablas de enrutamiento y proporciona opciones para comunicarse más allá de los límites de la red. Los datos de esta capa se asignan a direcciones de destino y de origen, que se utilizan como base para el enrutamiento previsto.

Ejemplos
> IP (Internet Protocol; protocolo de Internet): dirección pública individual necesaria para que los dispositivos que operan a través de Internet puedan comunicarse.
> IPv4: versión original de IP, utiliza direcciones de 32 bits
> IPv6: la versión más reciente de IP, utiliza direcciones de 128 bits que se dividen en ocho grupos de cuatro dígitos hexadecimales
> Protocolo de información de enrutamiento
> Seguridad de protocolo de Internet (IPSec)

Capa 2: enlace de datos (marcos)
Proporciona transmisión de datos y controla el acceso al medio de transmisión, combinando los datos en unidades denominadas "marcos". La capa 2 se divide en dos subcapas, la superior corresponde al control de enlace lógico (LLC, Logical Link Control) y la inferior corresponde al control de acceso a medios (Media Access Control, MAC). LLC simplifica el intercambio de datos, mientras que MAC controla el acceso al medio de transmisión.

Ejemplos
> IEEE 802.2 (LLC)
> IEEE 802.3 (MAC de Ethernet)
> 802.11 (WLAN MAC)

Capa 1: física (bits)
Proporciona servicios que admiten la transmisión de datos como un flujo de bits a través de un medio, por ejemplo, un enlace de transmisión a través de cable o inalámbrico.

5.2.1.2 Modelo de referencia de protocolo de control de transmisión/protocolo de Internet (TCP/IP)

El modelo de referencia TCP/IP es otro modelo que se emplea para entender los protocolos y cómo se produce la comunicación. El modelo de referencia TCP/IP se divide en cuatro capas diferentes que corresponden al modelo de referencia OSI, descrito anteriormente.

Tabla 7. Comparación de los modelos de referencia

Modelo OSI	Modelo TCP/IP
Capa 7: aplicación	Capa 4: aplicación
Capa 6: presentación	
Capa 5: sesión	
Capa 4: transporte	Capa 3: transporte
Capa 3: red	Capa 2: Internet
Capa 2: enlace de datos	Capa 1: interfaz de red
Capa 1: física	

5.2.2 Protocolos para la gestión de direcciones IP

DHCP (Dynamic Host Configuration Protocol; protocolo de configuración dinámica de hosts): asignación y gestión automática de direcciones IP.

DNS (Domain Name System; sistema de nombres de dominio): convierte los nombres de dominios en su dirección IP asociada, interviene en la capa de transporte.

DynDNS (Dynamic Domain Name System; sistema dinámico de nombres de dominio): se utiliza para hacer un seguimiento del enlace de un nombre de dominio con el fin de cambiar las direcciones IPv4.

UPnP (Universal Plug and Play; plug and play universal): los sistemas operativos de Microsoft pueden detectar de forma automática recursos (un dispositivo Axis) en una red.

Zeroconf: asigna de manera automática un dispositivo de red a una dirección IP sin utilizar entre 169.254.1.0 y 169.254.254.255

Bonjour: se puede usar para descubrir productos de vídeo en red con ordenadores Mac o como protocolo de descubrimiento para dispositivos nuevos en cualquier red.

ARP (Address Resolution Protocol; protocolo de resolución de direcciones): se emplea para descubrir la dirección MAC del host de destino.

5.2.3 Protocolos de nivel de aplicación

HTTP (Hypertext Transfer Protocol; protocolo de transferencia de hipertexto): se utiliza principalmente para cargar texto e imágenes desde un sitio web hasta el navegador web. Los sistemas de vídeo en red proporcionan un servicio de servidor HTTP que permite acceder a los sistemas a través de navegadores web para descargar configuraciones o imágenes en directo.

HTTPS (HTTP Secure): adaptación del protocolo de transferencia de hipertexto (HTTP) para realizar una comunicación segura en una red de ordenadores; de uso generalizado en Internet. En HTTPS, el protocolo de comunicación está cifrado por medio de Transport Layer Security (TLS, capa de transporte seguro).

FTP (File Transfer Protocol; protocolo de transferencia de archivos); se utiliza principalmente para transmitir archivos desde un servidor a un cliente (descarga) o desde un cliente a un servidor (subida). También se puede utilizar para crear y seleccionar directorios y renombrar o eliminar directorios y archivos.

RTP (Real-Time Transport Protocol; protocolo de transporte en tiempo real): permite la transferencia de datos en tiempo real entre extremos del sistema.

RTCP (Real-Time Control Protocol; protocolo de control en tiempo real): ofrece estadísticas fuera de banda e información de control de una sesión de RTP. Se asocia con RTP en la entrega y empaquetado de datos multimedia, pero no transporta ningún dato multimedia por sí solo.

RTSP (Real-Time Streaming Protocol; protocolo de transmisión en tiempo real): control ampliado durante la transmisión de medios en tiempo real.

SMTP (Simple Mail Transfer Protocol; protocolo sencillo de transferencia de correo): el estándar para la transferencia de correo electrónico a través de Internet. Las cámaras de red admiten SMTP para poder enviar alertas por correo electrónico.

SNMP (Simple Network Management Protocol; protocolo sencillo de administración de red): se emplea para supervisar y gestionar de forma remota equipos conectados en red, como switches, routers y cámaras de red. La compatibilidad con SNMP permite gestionar las cámaras de red mediante herramientas de código abierto.
SIP (Session Initiation Protocol; protocolo de inicio de sesión); protocolo de comunicación para señalar y controlar sesiones de comunicación multimedia.

SSL/TLS (Secure Sockets Layer/Transport Layer Security; capa de zócalos seguros/capa de transporte seguro): negocia una conexión privada y fiable entre el cliente y el servidor. SSL precedió a TLS, que era el estándar habitual.

LLDP (Link Layer Discovery Protocol; protocolo de descubrimiento de capa de enlace): se utiliza para dar a conocer la identidad y las capacidades de un dispositivo, así como de otros dispositivos conectados dentro de la misma red.

CIFS/SMB (Common Internet File System/Server Message Block; sistema de archivos comunes de Internet/bloque de mensajes de servidor): se utiliza principalmente para proporcionar un acceso compartido a archivos, impresoras y puertos serie, así como diversas comunicaciones entre los nodos de una red.

NTP (Network Time Protocol; protocolo de hora de red): se utiliza para sincronizar la hora del cliente o el servidor de un ordenador con la de otro servidor.

SFTP (Secure File Transfer Protocol; protocolo de transferencia segura de archivos): ofrece acceso a archivos, transferencia de archivos y gestión de archivos a través de cualquier flujo de datos fiable.

IGMP (Internet Group Management Protocol; protocolo de gestión de grupos de Internet): utilizado por hosts y routers adyacentes en redes IPv4 para crear afiliaciones a grupos de multidifusión, permite utilizar los recursos de una forma más eficiente al dar soporte a estos tipos de aplicaciones.

5.2.4 Protocolos de transporte de datos

TCP (Transmission control protocol; protocolo de control de transmisión): entrega de flujos de datos orientada a la conexión, fiable y en orden. Es el protocolo más habitual para el transporte de datos.

UDP (User Datagram Protocol; protocolo de datagramas de usuarios): servicio de transmisión sin conexión, da prioridad a la entrega a tiempo de los datos por encima de la fiabilidad.

ICMP (Internet Control Message Protocol; protocolo de mensajes de control de Internet): envío de mensajes de error e información sobre funcionamiento donde se indica que un servicio solicitado no está disponible o que no se ha podido acceder a un host o router.

5.2.5 Unidifusión, difusión y multidifusión

Existen tres métodos diferentes para transmitir datos en una red informática.

Unidifusión: es el más habitual, el remitente y el destinatario se comunican según un patrón de punto a punto. Los paquetes de datos se envían a un solo destinatario y ningún otro cliente recibirá esa información.

Multidifusión: comunicación entre un solo remitente y varios destinatarios de una red. Reduce el tráfico de red al entregar un solo flujo de información a muchos destinatarios.

Difusión: el remitente envía la misma información a todos los demás servidores de la red; todos los hosts de la red reciben el mensaje y lo procesarán de una u otra forma.

5.2.6 Calidad de servicio

En una red IP es necesario controlar cómo se comparten los recursos de la red para cumplir con los requisitos de cada servicio.

QoS (Quality of Service; calidad del servicio): capacidad para priorizar el tráfico de red de tal modo que se puedan atender los flujos críticos antes que los flujos con menos prioridad. Mayor fiabilidad de una red al controlar la cantidad de ancho de banda que puede usar una aplicación y proporcionar la capacidad de controlar la competencia entre aplicaciones por el ancho de banda disponible.

DiffServ: la red trata de prestar un servicio específico según la QoS especificada por cada paquete.

73136/ES/R1/1905

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones en red que mejoran la seguridad y suponen una nueva manera de hacer negocios. Como líder de la industria del vídeo en red, Axis pone a su disposición productos y servicios de videovigilancia y analítica, control de accesos y sistemas de audio. Axis cuenta con más de 3.000 empleados especializados en más de 50 países, y proporciona soluciones a sus clientes en colaboración con empresas asociadas de todo el mundo. Fue fundada en 1984 y su sede central se encuentra en Lund, Suecia.

Para más información sobre Axis, visite nuestro sitio web www.axis.com

AXIS COMMUNICATIONS