WHITE PAPER

Guia rápido das fichas técnicas da Axis

Aprovações, certificações e protocolos

Maio 2022

Sumário

1 **Introdução** 3

2 **Aprovações** 3

2.1 EMC (Compatibilidade eletromagnética) 3

2.2 Segurança 4

2.3 Ambiente 5

2.4 Outras aprovações 9

3 **Certificações** 9

4 **Fonte de alimentação** 10

4.1 Classes de PoE (Power over Ethernet) 10

5 **Rede** 10

5.1 Controle de proteção e segurança 10

5.2 Protocolos compatíveis 11

1 Introdução

A Axis Communications adere às normas e padrões de conformidade aplicáveis do setor em todos os produtos lançados no mercado. Este documento complementa as fichas técnicas da Axis com definições e breves descrições sobre os acrônimos, aprovações, certificações e protocolos nelas encontrados.

Este documento fornece informações sobre as seções da ficha técnica destacadas e ampliadas abaixo.

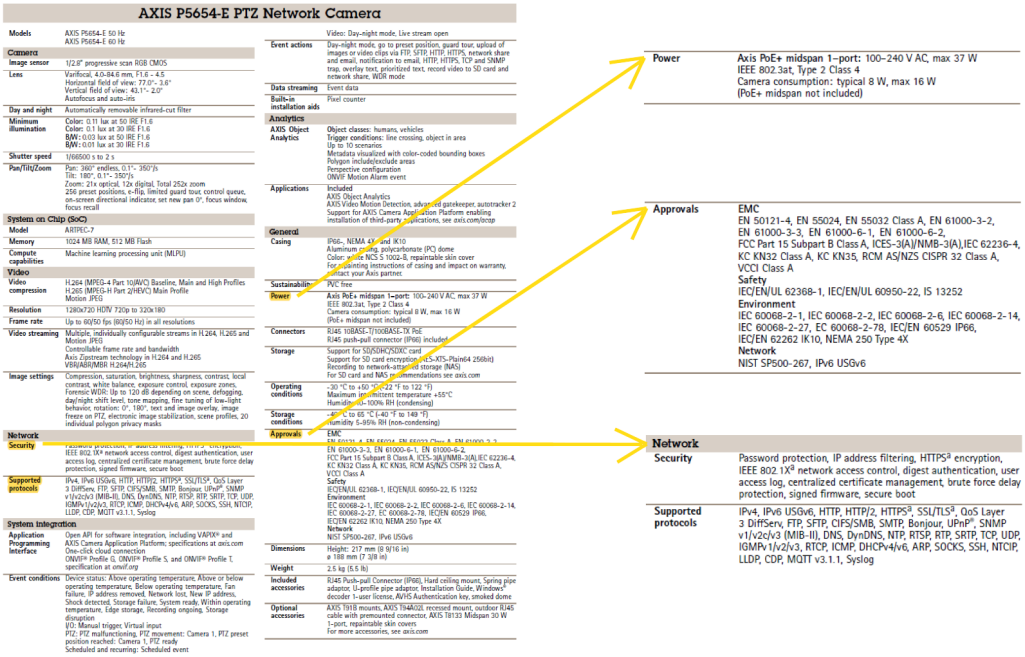

Figure 1. Destaque das seções das fichas técnicas da Axis abordadas neste documento.

2 Aprovações

A seção de aprovações das fichas técnicas da Axis está relacionada à conformidade com vários padrões. A seção geralmente é dividida em subseções sobre EMC, Segurança, Ambiente, Rede e Outros, onde "Outros" pode abordar proteção contra explosão ou segurança no controle de acesso. Além disso, pode haver uma subseção para aprovações relacionadas a midspan, nos casos em que um midspan é vendido juntamente com o produto.

2.1 EMC (Compatibilidade eletromagnética)

Todos os fabricantes de produtos de vídeo em rede devem declarar a EMC de seus produtos. Em algumas circunstâncias, os fabricantes podem se autocertificar, mas a maioria usa laboratórios de teste credenciados que fornecem um relatório para verificar a conformidade. As aprovações de EMC são baseadas em duas partes, emissão e imunidade.

Emissão diz respeito à capacidade do equipamento de funcionar satisfatoriamente sem emitir energia eletromagnética excessiva que possa afetar outros equipamentos no ambiente.

Imunidade é a medida de capacidade dos produtos eletrônicos de tolerar a influência dos fenômenos eletromagnéticos e da energia elétrica (irradiada ou conduzida) de outros produtos eletrônicos. Na Europa, a EMC está incluída na marcação CE (Conformidade europeia), que, por sua vez, está incluída na legislação de harmonização da União Europeia.

As normas listadas a seguir definem limites e métodos de testes de emissões eletromagnéticas e testes de imunidade. Como não há um teste que englobe a conformidade a nível mundial, pode haver códigos distintos para diferentes regiões ou aplicações.

2.1.1 Normas para ITE (Equipamentos de tecnologia da informação)

Esses padrões se aplicam a equipamentos multimídia (MME) que têm uma tensão de alimentação CA ou CC, não superior a 600 V. O equipamento multimídia (MME) é definido como o equipamento de tecnologia da informação (ITE), equipamento de áudio e de vídeo, equipamento receptor de transmissão e de controle de iluminação de entretenimento.

- EN 55032 Classe A: padrão de emissão (comercial, industrial, empresarial) articulado com os padrões internacionais.
- EN 55032 Classe B: norma de emissão (residencial) harmonizada com normas internacionais.
- EN 55035: padrão de imunidade articulado com os padrões internacionais

2.1.2 Normas harmonizadas por país/região

- EN 61000-6-1 e EN 61000-6-2: padrões genéricos de conformidade (Europa).
- FCC Parte 15, Subparte B, Classes A e B: a FCC (Comissão Federal de Comunicações dos EUA) estipula regras e regulamentações para dispositivos de telecomunicação, referentes à emissão, não à imunidade (Estados Unidos).
- ICES-3(A e B)/NMB-3(A e B) (Canadá)
- VCCI Classe A e B (Japão)
- KS C 9832 Classe A e B, KS C 9835, KS C 9547, KS C 9815 (Coreia)
- RCM AS/NZS CISPR 32 Classe A e B (Austrália/Nova Zelândia)

2.1.3 Normas adicionais por aplicação/produto

- EN 50121-4, IEC 62236-4: fornecem critérios de desempenho para aparelhos de sinalização e telecomunicações que possam interferir com outros aparelhos em ambientes ferroviários.
- EN 50130-4: aplicável aos componentes de sistemas de alarme, incluindo sistemas de controle de acesso, sistemas de CFTV, sistemas de detecção de incêndio e alarme de incêndio, botões de pânico, sistemas de alarme de invasão, sistemas de alarme social.

2.2 Segurança

- A Diretriz de baixa tensão (2014/35/UE): fornece objetivos gerais para a segurança de equipamentos elétricos. Garante que o uso dos produtos seja seguro, sem que haja riscos de ferimentos ou danos materiais.

- IEC/EN/UL 62368-1: conformidade de câmeras de rede, codificadores e fontes de alimentação com requisitos destinados a reduzir riscos de incêndios, choques elétricos ou ferimentos para qualquer pessoa que entre em contato com o equipamento.
- IEC/EN/UL 60950-22: requisitos de segurança específicos para produtos para uso em ambientes externos e para compartimentos para ambientes externos
- IEC/EN 62471-1: os requisitos de segurança fotobiológica de lâmpadas e dos sistemas de lâmpadas para limites de exposição evitam riscos para os olhos e a pele.
- EN/UL/CSA 60065: aplicável a aparelhos eletrônicos projetados para serem alimentados pela rede elétrica, dispositivos de alimentação, baterias ou alimentação remota e destinados à recepção, geração, gravação ou reprodução de áudio, vídeo e sinais associados, respectivamente.
- IS 13252: conformidade específica da Índia para câmeras de rede, codificadores e fontes de alimentação com requisitos destinados a reduzir riscos de incêndios, choques elétricos ou ferimentos para qualquer pessoa que entre em contato com o equipamento.

2.3 Ambiente

2.3.1 Grau de proteção IP

O padrão IEC 60529 da IEC (Comissão eletrotécnica internacional) define as classificações IP (proteção contra entrada ou proteção internacional) como um código de dois dígitos. O código define o grau de proteção de aparelhos elétricos contra a entrada de objetos sólidos ou poeira, contato acidental e água.

Tabela 2.1 Classificações de IP - o primeiro dígito após o IP: objetos sólidos estranhos

Grau	Proteção contra	Eficácia contra
0	Sem proteção	Sem proteção.
1	Objetos maiores do que 50 mm	Grandes superfícies do corpo, como o dorso das mãos, porém, sem proteção contra contato proposital com alguma parte do corpo.
2	Objetos maiores do que 12,5 mm	Dedos ou outros objetos podem penetrar até 80 mm, desde que estejam protegidos contra peças perigosas. Objetos com diâmetro de 12,5 mm não são capazes de penetrar totalmente.
3	Objetos maiores do que 2,5 mm	Objetos, como ferramentas e arames grossos, não são capazes de penetrar de forma alguma.
4	Objetos maiores do que 1 mm	Objetos, como fios e parafusos, não são capazes de penetrar de forma alguma.
5	Proteção contra poeira	Não há proteção total contra a entrada de poeira, mas a poeira não entra em quantidade suficiente para interferir na operação satisfatória do equipamento.
6	Vedação contra poeira	Sem entrada de poeira.

Tabela 2.2 Classificações de IP - o segundo dígito após o IP: líquidos

Grau	Proteção contra	Eficácia contra
0	Sem proteção	Sem proteção especial.

Tabela 2.2. Classificações de IP - o segundo dígito após o IP: líquidos (Continuação)

1	Goteira de água	Gotejamento de água (gotas caindo verticalmente) não têm nenhum impacto negativo.
2	Gotejamento de água quando inclinado em até 15°	O gotejamento de água vertical não tem nenhum impacto negativo quando o compartimento é inclinado em ângulos de até 15° a partir de sua posição normal.
3	Água borrifada	Água borrifada em um ângulo de até 60° na vertical não tem nenhum impacto negativo.
4	Respingos de água	Respingos de água lançados contra o compartimento, de qualquer direção, não têm nenhum impacto negativo.
5	Jatos de água	A água projetada de um bocal contra o compartimento, de qualquer direção, não tem nenhum impacto negativo.
6	Jatos fortes de água	A água em um ambiente com mar agitado ou projetada em jatos potentes não é capaz de entrar no compartimento em quantidades prejudiciais.
7	Breve imersão na água	A entrada de água em quantidade prejudicial não é possível quando o compartimento está imerso em água sob condições definidas de pressão e tempo.
8	Submersão contínua na água	O equipamento é compatível com submersão contínua na água sob determinadas condições, que devem ser especificadas pelo fabricante. As condições devem ser mais severas do que aquelas definidas para o grau de proteção IPX7 (consulte o item anterior).
9	Jatos de água sob alta pressão e limpeza com jato de vapor	A água direcionada para a caixa de proteção, de qualquer ângulo e sob pressão muito elevada, não tem nenhum impacto negativo.

2.3.2 Outras normas relevantes da IEC

- IEC 60068-2: um padrão para testes ambientais de equipamentos e produtos eletrônicos para avaliar sua capacidade de desempenho em condições ambientais, incluindo frio extremo e calor seco. Os procedimentos abaixo neste padrão são normalmente destinados a objetos que alcançam estabilidade de temperatura durante o procedimento de teste.
  - IEC 60068-2-1: frio
  - IEC 60068-2-2: calor seco
  - IEC 60068-2-6: vibração (contínua)
  - IEC 60068-2-14: mudança de temperatura
  - IEC 60068-2-27: impacto
  - IEC 60068-2-30: calor úmido (cíclico)
  - IEC 60068-2-64: vibração (aleatória de banda larga)
  - IEC 60068-2-78: calor úmido (estado constante)
- IEC 60825 Classe I: um padrão que garante que o tipo de laser usado no módulo de foco a laser seja seguro sob todas as condições de uso normal.

2.3.3 Grau de proteção NEMA

A NEMA (National Electrical Manufacturers Association) é uma associação localizada nos EUA que fornece padrões para compartimentos de equipamentos elétricos. A NEMA lançou seu próprio padrão NEMA 250 em todo o mundo. Além disso, adotou e publicou um padrão IP de harmonização, o ANSI/IEC 60529, por meio do ANSI (American National Standards Institute).

A norma NEMA 250 aborda a proteção contra entrada, mas também considera outros fatores, como resistência à corrosão, desempenho e detalhes estruturais. Devido a isso, o tipo de classificação NEMA é comparável à classificação IP, porém, a IP não é comparável à NEMA.

Os padrões UL 50 e UL 50E são baseados nos padrões NEMA 250. O NEMA permite a autocertificação, enquanto o UL reforça a conformidade, exigindo que os produtos sejam aprovados em testes e inspeções de terceiros.

Tabela 2.3 Graus de proteção NEMA para compartimentos em locais não perigosos

NEMA	Classificação IP equivalente	Ambientes internos	Ambientes externos	Proteção contra
Tipo 1	IP10	X		Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira). Sem proteção contra líquidos.
Tipo 3	IP54	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira transportada pelo vento). Entrada de água (chuva, granizo, neve). Não sofrerá danos devido à formação de gelo na parte externa do compartimento.
Tipo 3R	IP14	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira). Entrada de água (chuva, granizo, neve). Não sofrerá danos devido à formação de gelo na parte externa do compartimento.
Tipo 3S	IP54	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira transportada pelo vento). Entrada de água (chuva, granizo, neve). Os mecanismos externos permanecem operáveis quando cobertos por gelo.
Tipo 4	IP56	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira transportada pelo vento). Entrada de água (chuva, granizo, neve, respingos de água e jatos de água lançados usando uma mangueira). Não sofrerá danos devido à formação de gelo na parte externa do compartimento.
NEMA 4X	IP56	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira transportada pelo vento). Entrada de água (chuva, granizo, neve, respingos de água e jatos de água lançados usando uma mangueira). Fornece um grau de proteção adicional contra corrosão. Não sofrerá danos devido à formação de gelo na parte externa do compartimento.

Tabela 2.3. Graus de proteção NEMA para compartimentos em locais não perigosos (Continuação)

Tipo 6	IP67	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira). Entrada de água (jatos de água lançados por mangueiras e entrada de água durante submersão temporária ocasional sob profundidade limitada). Não sofrerá danos devido à formação de gelo na parte externa do compartimento.
Tipo 6P	IP67	X	X	Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira). Entrada de água (jatos de água lançados por mangueiras e entrada de água durante submersão prolongada sob profundidade limitada). Fornece um grau de proteção adicional contra corrosão. Não sofrerá danos devido à formação de gelo na parte externa do compartimento.
Tipo 12	IP52	X		Sem orifícios pré-furados. Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira circulante, fiapos, fibras e resíduos). Entrada de água (goteiras e respingos leves).
Tipo 12K	IP52	X		Com orifícios pré-furados. Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira circulante, fiapos, fibras e resíduos). Entrada de água (goteiras e respingos leves).
Tipo 13	IP54	X		Acesso a peças perigosas e entrada de objetos estranhos sólidos (queda de poeira e poeira circulante, fiapos, fibras e resíduos). Entrada de água (goteiras e respingos leves). Borrifos, espirros e infiltração de óleo e líquido de arrefecimento não corrosivos.

O NEMA TS 2 é um guia de design que se aplica a equipamentos de sinalização de tráfego.

2.3.4 Grau de proteção IK

As classificações IK podem ser encontradas no IEC/EN 62262, um padrão internacional que especifica os graus de proteção contra impactos mecânicos externos. Originalmente aprovado em 1994 como padrão europeu, o EN 50102 foi adotado como um padrão internacional em 2002.

Muitos fabricantes optam por testar a parte mais frágil de um produto para garantir a resistência ao longo de sua vida útil.

Grau	IK01	IK02	IK03	IK04	IK05	IK06	IK07	IK08	IK09	IK10	IK10+*
Energia de impacto (joule)	0,14	0,2	0,35	0,5	0,7	1	2	5	10	20	50*
Massa (kg)	<0,2	<0,2	0,2	0,2	0,2	0,5	0,5	1,7	5	5	
Altura da queda (mm)	56	80	140	200	280	400	400	300	200	400	

*Impacto de até 50 J. O fabricante deve indicar a energia, a massa e a altura de queda do elemento em destaque.

2.4 Outras aprovações

2.4.1 Proteção contra explosão

- IEC/EN/UL/SANS/CSA 60079-0: requisitos gerais para fabricação, testes e marcação de equipamentos Ex e componentes Ex destinados ao uso em atmosferas explosivas.
- IEC/EN/UL/SANS/CSA 60079-1: requisitos específicos para fabricação e testes de equipamentos elétricos com compartimento à prova de fogo com proteção do tipo "d", destinados ao uso em atmosferas com gases explosivos.

2.4.2 Aprovações para midspans

Para casos em que um midspan é incluído juntamente com o produto, as aprovações especificamente relacionadas ao midspan são listadas nessa seção da ficha técnica. As explicações podem ser encontradas nas seções anteriores deste documento.

2.4.3 Segurança no controle de acesso

- UL 294: define os requisitos relativos à fabricação, ao desempenho e à operação de sistemas de controle de acesso.

3 Certificações

Quando uma câmera é instalada em um ambiente potencialmente explosivo, a caixa de proteção deve atender a padrões de segurança muito específicos. As caixas devem proteger o ambiente contra ignitores potenciais da câmera e de outros equipamentos.

Os produtos europeus devem estar em conformidade com a diretiva ATEX e o padrão internacional correspondente é IECEx. A América do Norte usa principalmente as classificações de Classe/Divisão do NFPA70 (Código elétrico nacional, NEC) e CSA C22.1 (Código elétrico canadense, CEC) para o sistema de zonas descrito no ATEX e IECEx.

Tabela 3.1 Graus de proteção contra explosões

Classe/Divisão	Atmosfera	Definição	Zona (IECEx e ATEX)
Classe I/Divisão 1	Gás	Área em que a mistura explosiva está continuamente presente ou está presente por longos períodos.	Zona 0
Classe I/Divisão 1	Gás	Área em que é provável que haja a presença de mistura explosiva durante a operação normal.	Zona 1
Classe I/Divisão 2	Gás	Área em que a presença de uma mistura explosiva não é provável durante a operação normal e, caso ocorra, estará presente apenas por um curto período de tempo.	Zona 2

Tabela 3.1. Graus de proteção contra explosões (Continuação)

Classe II/Divisão 1	Poeira	Área em que a mistura explosiva está continuamente presente ou está presente por longos períodos.	Zona 20
Classe II/Divisão 1	Poeira	Área em que é provável que haja a presença de mistura explosiva durante a operação normal.	Zona 21
Classe II/Divisão 2	Poeira	Área em que a presença de uma mistura explosiva não é provável durante a operação normal e, caso ocorra, estará presente apenas por um curto período de tempo.	Zona 22

4 Fonte de alimentação

4.1 Classes de PoE (Power over Ethernet)

As classes de PoE garantem a distribuição eficiente da energia, especificando a quantidade de energia que um dispositivo alimentado exigirá.

Tabela 4.1 Classes de PoE

Classe	Tipo	Nível de potência garantido no PSE (Equipamento de fornecimento de energia)	Nível máximo de potência usado pelo PD (Dispositivo alimentado)
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 3, 802.3bt	100 W	71,3 W

*Esse tipo também é conhecido como PoE+.

5 Rede

5.1 Controle de proteção e segurança

Existem várias maneiras de combater as ameaças aos ativos do sistema. Algumas ameaças representam riscos para os dispositivos, enquanto outras representam riscos para as redes ou os dados em trânsito/armazenamento. Veja alguns controles de segurança selecionados que podem ser aplicados a dispositivos e redes:

- As credenciais (usuário/senha) protegem contra o acesso não autorizado aos vídeos e impedem o acesso não autorizado às configurações do dispositivo. A aplicação de diferentes níveis de privilégios de conta proporciona controle sobre quem tem acesso ao quê.
- A filtragem de endereço IP (firewall) reduz a exposição da rede local de um dispositivo e, assim, protege contra o acesso de clientes não autorizados. Isso reduz os riscos caso a senha de um dispositivo seja comprometida e uma nova vulnerabilidade crítica seja descoberta.
- O IEEE 802.1x: protege a rede de clientes não autorizados. O 802.1x é uma proteção de infraestrutura de rede, que usa switches gerenciados e servidor RADIUS. O cliente 802.1x no dispositivo fornece autenticação para o dispositivo na rede.
- HTTPS (Protocolo de transferência de hipertexto seguro): protege os dados (vídeo) contra interceptação da rede. O uso de certificados assinados em HTTPS fornece um modo de detecção para um cliente de vídeo caso ele esteja acessando uma câmera legítima ou um computador mal intencionado que esteja se passando por uma câmera.
- Firmware assinado: é implementado pelo fornecedor de software que assina a imagem de firmware com uma chave privada, a qual é mantida em segredo. Se um firmware tiver essa assinatura conectada a ele, um dispositivo validará o firmware antes de aceitar sua instalação. Se o dispositivo detectar que a integridade do firmware está comprometida, ele rejeitará a atualização do firmware. O firmware assinado Axis baseia-se no método de criptografia de chave pública RSA amplamente aceito pelo setor.
- Inicialização segura: é um processo de inicialização que consiste em uma cadeia inquebrável de software validado criptograficamente e que começa em uma memória imutável (ROM de inicialização). Baseada em firmware assinado, a inicialização segura garante que um dispositivo possa ser inicializado somente com firmware autorizado. A inicialização segura garante que o dispositivo Axis seja completamente limpo contra possíveis malwares após uma reinicialização para os padrões de fábrica.
- TPM: um Módulo de plataforma confiável é um componente que fornece um conjunto de recursos de criptografia adequados para a proteção de informações contra acesso não autorizado. A chave privada é armazenada no TPM e nunca deixa o TPM. Todas as operações de criptografia que exigem o uso da chave privada são enviadas para o TPM para processamento. Isso garante que a parte secreta do certificado permaneça segura, mesmo em caso de violação de segurança.
- Axis Edge Vault: um módulo de computação criptográfica seguro (módulo seguro ou elemento seguro) no qual a ID do dispositivo Axis é instalada e armazenada de forma segura e permanente.

Para ter acesso a mais recursos de segurança cibernética, consulte *axis.com/cybersecurity*

5.2 Protocolos compatíveis

Muitos protocolos entram em ação quando dados são transferidos com segurança de um dispositivo de rede para outro.

5.2.1 Modelos de referência de protocolos

A melhor maneira de entender como os diversos protocolos interagem é examinar o modelo de comunicação OSI (Interconexão de sistemas abertos). Existe também o modelo de referência TCP/IP.

5.2.1.1 Modelo de referência OSI

Um modelo que descreve a comunicação de dados entre sistemas abertos. Para fornecer um serviço, cada camada utiliza os serviços da camada imediatamente abaixo dela. Cada camada deve seguir determinadas regras, ou protocolos, para executar os serviços.

Camada 7 — Aplicação

Disponibiliza funções, como transferências da Web, de arquivos e de e-mails, para os aplicativos.

Os aplicativos propriamente ditos, como navegadores da Web ou programas de e-mail, existem acima dessa camada e não são abrangidos pelo modelo OSI.

Camada 6 — Apresentação (dados)

Garante que os dados enviados pela camada de aplicação de um sistema possam ser lidos pela camada de aplicação de outro sistema. Converte formatos de dados dependentes do sistema, como o ASCII, em um formato independente, permitindo uma troca de dados sintaticamente correta entre diferentes sistemas.

Camada 5 — Sessão (conexão persistente entre hosts do mesmo nível)

Fornece um serviço voltado para a aplicação e lida com a comunicação de processos entre dois sistemas. A comunicação de processos começa com a criação de uma sessão, o que fornece a base para uma conexão virtual entre os sistemas.

Camada 4 — Transporte (transporte de ponta a ponta, protocolo voltado para a conexão)

Fornece um serviço de transferência de dados confiável (por meio do controle de fluxo e do controle de erros) para a Camada 5 e camadas superiores.

Camada 3 — Rede (pacote, endereçamento/fragmentação)

Executa a transferência de dados propriamente dita, roteando e encaminhando pacotes de dados entre sistemas. Cria e administra tabelas de roteamento e fornece opções de comunicação além dos limites da rede. Aos dados nessa camada são atribuídos endereços de destino e de origem, que são usados como a base para o roteamento direcionado.

Camada 2 — Enlace de dados (quadros)

Fornece transmissão de dados e controla o acesso ao meio de transmissão, combinando dados em unidades conhecidas como quadros. A camada 2 é dividida em duas subcamadas, a faixa superior que corresponde ao LLC (Controle de enlace lógico) e a parte inferior que corresponde ao controle de acesso à mídia (MAC). O LLC simplifica a troca de dados, enquanto o MAC controla o acesso ao meio de transmissão.

Camada 1 — Física (bits)

Fornece serviços compatíveis com a transmissão de dados, como um fluxo de bits por um meio, como por exemplo, um link de transmissão com ou sem fio.

5.2.1.2 Modelo de referência de Protocolo de controle de transmissão/Protocolo de Internet

O modelo de referência TCP/IP é outro modelo usado para entender os protocolos e como a comunicação ocorre. É dividido em quatro camadas, que correspondem ao modelo de referência OSI, conforme descrito a seguir.

Tabela 5.1 Comparação dos modelos de referência

Modelo OSI	Modelo TCP/IP
Camada 7 — Aplicação	Camada 4 — Aplicação
Camada 6 — Apresentação	
Camada 5 — Sessão	
Camada 4 — Transporte	Camada 3 — Transporte
Camada 3 — Rede	Camada 2 — Internetwork (ligação entre redes)
Camada 2 — Enlace de dados	Camada 1 — Interface de rede
Camada 1 — Física	

5.2.2 Protocolos da camada de aplicação

- **CIFS/SMB** (Sistema de arquivo comum de Internet/Bloco de mensagens do servidor): usado principalmente para fornecer acesso compartilhado a arquivos, impressoras e portas seriais, além de comunicações diversas entre os nós de uma rede.
- **DDNS** (Sistema dinâmico de nomes de domínio): é usado para rastrear os links dos nomes de domínio dos endereços IPv4 dinâmicos.
- **DHCPv4/v6** (Protocolo de configuração dinâmica de host): atribuição automática e gerenciamento de endereços IP.
- **DNS/DNSv6** (Sistema de nomes de domínio): converte nomes de domínio em seus endereços IP associados.
- **FTP** (Protocolo de transferência de arquivos): usado principalmente para transmitir arquivos de um servidor para um cliente (download) ou de um cliente para um servidor (upload). Também pode ser usado para criar e selecionar diretórios e renomear ou excluir diretórios e arquivos.
- **HTTP** (Protocolo de transferência de hipertexto): usado principalmente para carregar textos e imagens de um site para um navegador da Web. Os sistemas de vídeo em rede fornecem um serviço de servidor HTTP que permite acessá-los usando navegadores da Web para fazer download de configurações ou exibir imagens ao vivo.
- **HTTP/2**: uma grande revisão do protocolo HTTP definido no RFC 7540 e lançado em fevereiro de 2015.
- **HTTPS** (HTTP seguro): uma adaptação do HTTP (Protocolo de transferência de hipertexto) para comunicação segura por uma rede de computadores, amplamente utilizado na Internet. No HTTPS, a comunicação é criptografada pelo protocolo TLS (Segurança da camada de transporte).
- **MQTT** (Transporte de telemetria de enfileiramento de mensagens): um protocolo de mensagens padrão para a Internet das coisas (IoT). Ele foi desenvolvido para integração simplificada com a IoT e é usado em uma ampla variedade de setores para conectar dispositivos remotos com o mínimo de código e largura de banda de rede.
- **NTP** (Protocolo de tempo para redes): usado para sincronizar a hora de um cliente ou servidor de computador com a de outro servidor.
- **RTP** (Protocolo de transporte em tempo real): permite a transferência de dados em tempo real entre os pontos de extremidade do sistema.

- **RTCP** (Protocolo de controle em tempo real): fornece estatísticas fora da banda e informações de controle para uma sessão de RTP. Ele é associado ao RTP na entrega e no empacotamento de dados multimídia, mas não transporta dados de mídia por si só.
- **RTSP** (Protocolo de streaming em tempo real): controle ampliado da transmissão de mídia em tempo real.
- **SFTP** (Protocolo de transferência segura de arquivos): fornece acesso, transferência e gerenciamento de arquivos em qualquer stream de dados confiável.
- **SIP** (Protocolo de início de sessão): protocolo de comunicação para sinalização e controle de sessões de comunicação multimídia.
- **SIPS** (Protocolo de início de sessão segura): versão criptografada do SIP.
- **SMTP** (Protocolo de transferência de correio simples): o padrão de transferência de e-mails pela Internet. As câmeras de rede são compatíveis com o SMTP para permitir o envio de alertas por e-mail.
- **SNMPv1/v2/v3** (Protocolo de gerenciamento de rede simples): usado para monitorar e gerenciar remotamente equipamentos em rede, como switches, roteadores e câmeras de rede. O suporte SNMP permite que as câmeras de rede sejam gerenciadas por ferramentas de código aberto.
- **SOCKS**: permite a transferência de pacotes de rede entre clientes e servidores por meio de um proxy de rede remoto.
- **SRTP** (Protocolo de transporte seguro em tempo real): permite a transferência criptografada de dados em tempo real entre os pontos de extremidade do sistema e, portanto, é uma variante segura do RTP.
- **SSH** (Secure Shell): permite o gerenciamento e a depuração do acesso a dispositivos de rede com segurança em uma rede não segura.
- **TLSv1.2/v1.3** (Segurança da camada de transporte): negocia uma conexão privada e confiável entre o cliente e o servidor.

5.2.3 Protocolos da camada de transporte

- **TCP** (Protocolo de controle de transmissão): entrega voltada para a conexão confiável e ordenada dos streams de dados. O protocolo mais comum de transporte de dados.
- **UDP** (Protocolo de datagrama do usuário): serviço de transmissão sem conexão, que favorece a entrega oportuna de dados, em oposição à confiabilidade.
- **ICMP** (Protocolo de mensagens de controle da Internet): envia mensagens de erro e informações operacionais indicando a indisponibilidade de um serviço solicitado ou a incapacidade de acessar um host ou roteador.

5.2.4 Protocolos da camada de rede

- **IGMPv1/v2/v3** (Protocolo de gerenciamento de grupos da Internet): usado por hosts e roteadores adjacentes em redes IPv4 para estabelecer associações em grupos de multicast. Permite o uso mais eficiente dos recursos ao oferecer suporte a esses tipos de aplicativos.
- **IPv4/IPv6** (Protocolo de Internet): um endereço público individual necessário para a comunicação dos dispositivos habilitados para Internet. O IPv4 é a versão original e usa endereços de 32 bits. O IPv6 é a versão mais recente e usa endereços de 128 bits divididos em oito grupos de quatro dígitos hexadecimais.
- **USGv6**: um perfil de padrões técnicos para IPv6, definido pelo governo dos EUA para garantir a compatibilidade ao adquirir dispositivos de rede habilitados para IPv6.

5.2.5 Protocolos da camada de enlace de dados

- **ARP** (Protocolo de resolução de endereço): usado para detectar o endereço MAC do host de destino.
- **CDP** (Cisco Discovery Protocol): protocolo proprietário da Cisco usado como alternativa ao LLDP para detectar informações sobre dispositivos de hardware conectados.
- **IEEE 802.3 (i, u, ab)**: padrões para Ethernet que definem a comunicação de dados de 10 Mb/s (10Base-T), 100 Mb/s (100Base-TX) e 1 Gb/s (1000Base-T) em um cabeamento de par trançado.
- **LLDP** (Protocolo de descoberta de camada de link): usado para anunciar a identidade e as capacidades de um dispositivo, bem como outros dispositivos conectados na mesma rede.

5.2.6 Protocolos de descoberta

- **mDNS (Bonjour)**: pode ser usado para detectar produtos de vídeo em rede usando computadores Mac ou como um protocolo de detecção para novos dispositivos em qualquer rede.
- **UPnP** (Plug and play universal): os sistemas operacionais da Microsoft podem detectar automaticamente os recursos (dispositivos Axis) em uma rede.
- **Zeroconf**: aloca automaticamente um dispositivo de rede para um endereço IP não utilizado no intervalo de 169.254.1.0 a 169.254.254.255.

5.2.7 Qualidade de serviço

Em uma rede IP, é necessário controlar como os recursos de rede são compartilhados para atender aos requisitos de cada serviço.

- **QoS** (Qualidade de serviço): capacidade de priorizar o tráfego de rede para que os fluxos críticos possam ser atendidos antes dos fluxos com menos prioridade. Proporciona maior confiabilidade na rede, controlando a quantidade de largura de banda que um aplicativo pode usar e fornecendo a capacidade de controlar a concorrência pela largura de banda entre os aplicativos.
- **DiffServ**: a rede tenta entregar um serviço específico baseado na QoS especificada por cada pacote.

5.2.8 Métodos de transmissão de dados

Existem três métodos para transmitir dados em uma rede de computadores.

- **Unicast**: o mais comum, o remetente e o destinatário estabelecem uma comunicação ponto a ponto. Os empacotadores de dados são enviados apenas a um destinatário, e nenhum outro cliente receberá as informações.
- **Multicast**: comunicação entre um único remetente e vários destinatários em uma rede. Reduz o tráfego de rede fornecendo um único stream de informações a vários destinatários.
- **Broadcast**: o remetente envia as mesmas informações para todos os outros servidores em uma rede; todos os hosts na rede recebem a mensagem e a processam de alguma forma.

T10169734/PT/M2.2/2205

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e mais seguro criando soluções em rede que fornecem percepções que permitem melhorar a segurança e encontrar novas formas de fazer negócios. Como líder do setor de vídeo em rede, a Axis oferece produtos e serviços para sistemas de monitoramento e análise de vídeo, controle de acesso, intercomunicação e áudio. A Axis conta com mais de 3.800 funcionários dedicados em mais de 50 países e colabora com parceiros em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e sua sede está localizada em Lund, na Suécia.

Para obter mais informações sobre a Axis, visite nosso site *axis.com*.