LIVRE BLANC

Guide explicatif des fiches techniques Axis

Agréments, certifications et protocoles

Mai 2022

AXIS COMMUNICATIONS

Table des matières

1 Introduction

Axis Communications respecte les normes applicables dans son secteur d'activité et les normes de conformité pour tous les produits qu'il commercialise. Ce guide explicatif complète les fiches techniques d'Axis par des définitions et de courtes descriptions des acronymes, agréments, certifications et autres protocoles qu'elles mentionnent.

Ce document fournit des informations sur les parties des fiches techniques illustrées et agrandies ci-dessous.

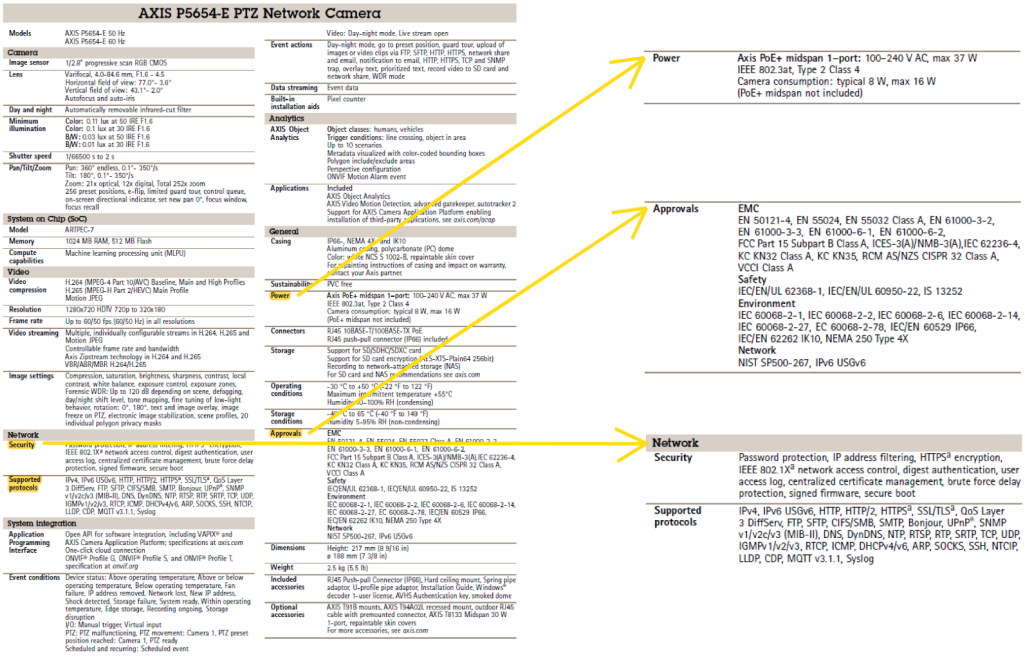

Figure 1. Parties des fiches techniques Axis concernées par ce guide.

2 Agréments

La partie Agréments des fiches techniques Axis se rapporte à la conformité des produits par rapport à une variété de normes. Cette partie est généralement divisée en sous-parties relatives à la compatibilité électromagnétique (CEM), la sécurité, l'environnement, les réseaux et d'autres thèmes qui peuvent concerner la protection contre les explosions ou la sécurité du contrôle d'accès. Une sous-partie peut faire référence aux agréments relatifs aux injecteurs midspan s'ils sont commercialisés avec le produit.

2.1 CEM (compatibilité électromagnétique)

Tous les fabricants doivent déclarer la CEM de leurs produits de vidéo sur IP. Dans certaines circonstances, les fabricants peuvent s'autocertifier, mais la plupart recourent à des laboratoires d'essai accrédités qui délivrent un rapport de conformité. Les approbations CEM portent sur deux aspects : émissivité et immunité.

Émissivité se rapporte à la capacité du matériel à fonctionner correctement sans émission excessive d'énergie électromagnétique susceptible de perturber les autres matériels de son environnement.

Immunité quantifie la capacité des produits électroniques à tolérer l'influence des phénomènes électromagnétiques et de l'énergie électrique (rayonnée ou transmise par conduction) produits par d'autres produits électroniques. En Europe, la CEM est incluse dans le marquage CE, lui-même inclus dans la législation d'harmonisation de l'UE.

Les normes répertoriées ci-dessous définissent les limites et les méthodes d'essai relatives à l'émissivité et à l'immunité électromagnétiques. Comme il n'existe pas d'essai unifié de conformité au niveau mondial, il peut y avoir plusieurs codes en fonction des régions ou des applications.

2.1.1 Normes des matériels informatiques

Ces normes s'appliquent aux appareils multimédias dont la tension d'alimentation CA ou CC ne dépasse pas 600 V. Les appareils multimédias englobent les matériels informatiques, les appareils audio, les systèmes vidéo, les récepteurs hertziens et les équipements de commande d'éclairage scénique.

- EN 55032 Classe A : norme d'émissivité (commerciale, industrielle, professionnelle) harmonisée avec les normes internationales
- EN 55032 Classe B : norme d'émissivité (résidentielle) harmonisée avec les normes internationales
- EN 55035 : Norme d'immunité harmonisée avec les normes internationales

2.1.2 Normes harmonisées par pays/région

- EN 61000-6-1 et EN 61000-6-2 : normes génériques de conformité (Europe)
- FCC Partie 15, sous-chapitre B, Classe A et B : la FCC stipule des prescriptions et des réglementations pour les appareils de télécommunications, qui se rapportent à l'émissivité et non à l'immunité (États-Unis)
- ICES-3(A et B)/NMB-3(A et B) (Canada)
- VCCI Classe A et B (Japon)
- KS C 9832 Classe A et B, KS C 9835, KS C 9547, KS C 9815 (Corée du Sud)
- RCM AS/NZS CISPR 32 Classe A et B (Australie/Nouvelle-Zélande)

2.1.3 Normes complémentaires par application/produit

- EN 50121-4, IEC 62236-4 : stipule des critères de performance pour les appareils de signalisation et de télécommunication susceptibles d'interférer avec d'autres appareillages des environnements ferroviaires.
- EN 50130-4 : s'applique aux composants des systèmes d'alarme, notamment systèmes de détection d'incendie, contre l'intrusion, contre les hold-up, CCTV, de contrôle d'accès et d'alarme sociale.

2.2 Sécurité

- Directive sur les basses tensions (2014/35/EU) : contient les objectifs généraux de sécurité des matériels électriques. Elle veille à la sécurité d'emploi des produits sans risque de blessure ou de préjudice aux biens.
- IEC/EN/UL 62368-1 : conformité des caméras réseau, encodeurs et sources d'alimentation aux exigences visant à réduire les risques d'incendie, de choc électrique ou de blessure aux personnes en contact avec ces équipements.

- IEC/EN/UL 60950-22 : exigences de sécurité spécifiques aux produits et boîtiers destinés à être installés à l'extérieur
- IEC/EN 62471-1 : Sécurité photobiologique des lampes et des appareils utilisant des lampes, limites d'exposition, contrôle des risques pour les yeux et la peau.
- EN/UL/CSA 60065 : s'applique aux appareils alimentés par la tension secteur, par une source d'alimentation, par des batteries ou par un dispositif d'alimentation à distance et destinés à la réception, la production, l'enregistrement ou la reproduction de signaux audio, vidéo et connexes.
- IS 13252 : (norme spécifique à l'Inde) conformité des caméras réseau, encodeurs et sources d'alimentation aux exigences visant à réduire les risques d'incendie, de choc électrique ou de blessure aux personnes en contact avec ces équipements.

2.3 Environnement

2.3.1 Indice de protection IP

La norme IEC (International Electrotechnical Commission) 60529 définit les indices de protection IP sous forme de code à deux chiffres. Le code définit le degré de protection des dispositifs électriques contre un contact accidentel ou la pénétration de corps étrangers, de poussière ou d'eau.

Table 2.1 Indices de protection IP - Premier chiffre après IP : corps étrangers solides

Degré	Protection contre	Efficace contre
0	Non protégé	Aucune protection
1	Objets de taille supérieure à 50 mm	Grande surface du corps, comme le dos d'une main, mais aucune protection contre un contact délibéré avec une partie du corps.
2	Objets de taille supérieure à 12,5 mm	Les doigts et les objets peuvent pénétrer jusqu'à 80 mm, en supposant l'absence de pièces à risque. Les objets d'un diamètre de 12,5 mm ne peuvent pas entrer complètement.
3	Objets de taille supérieure à 2,5 mm	Les objets (par exemple outillage ou câbles) ne peuvent pas entrer.
4	Objets de taille supérieure à 1 mm	Les objets (par exemple fils ou vis) ne peuvent pas entrer.
5	Protection contre la poussière	La poussière peut pénétrer quelque peu dans le caisson, mais pas en quantité suffisante pour empêcher le bon fonctionnement de l'équipement.
6	Étanche à la poussière	Aucune pénétration de poussière.

Table 2.2 Indices de protection IP - Deuxième chiffre après IP : liquides

Degré	Protection contre	Efficace contre
0	Non protégé	Aucune protection particulière
1	Écoulement d'eau	Les gouttes d'eau tombant à la verticale n'ont pas d'effet préjudiciable.

Table 2.2. Indices de protection IP - Deuxième chiffre après IP : liquides (Suite)

2	Écoulements d'eau jusqu'à un angle de 15°	Les écoulements d'eau à la verticale n'ont aucun effet préjudiciable lorsque le boîtier est incliné à un angle de 15° par rapport à sa position normale.
3	Pulvérisation d'eau	Les brouillards d'eau à un angle allant jusqu'à 60° par rapport à la verticale n'ont aucun effet préjudiciable.
4	Projections d'eau	Les éclaboussures d'eau sur le boîtier provenant de n'importe quelle direction n'ont aucun effet préjudiciable.
5	Jets d'eau	La projection d'eau sur le boîtier depuis n'importe quelle direction à partir d'une buse n'a aucun effet préjudiciable.
6	Jets d'eau puissants	L'eau d'une mer déchaînée ou projetée en jets puissants ne peut pas pénétrer dans le boîtier en quantité préjudiciable.
7	Brève immersion dans l'eau	L'eau ne peut pas pénétrer en quantité préjudiciable lorsque le boîtier est immergé dans l'eau, dans des conditions de pression et de temps définies.
8	Immersion permanente dans l'eau	L'équipement est adapté à la submersion continue dans l'eau, dans les conditions spécifiées par le fabricant. Les conditions doivent être plus défavorables que pour l'indice IPX7 (voir cas précédent).
9	Eau projetée par un nettoyeur haute pression ou à jet de vapeur	L'eau dirigée vers le boîtier depuis n'importe quel angle sous très haute pression n'a pas d'effet préjudiciable.

2.3.2 Autres normes IEC

- IEC 60068-2 : norme d'essai environnemental des équipements et produits électroniques pour évaluer leur tenue fonctionnelle dans des conditions ambiantes incluant le froid extrême et la chaleur sèche. Les procédures ci-dessous figurant dans cette norme sont typiquement prévues pour les objets qui parviennent à leur stabilité thermique pendant la procédure d'essai.
  - IEC 60068-2-1 : basse température
  - IEC 60068-2-2 : chaleur sèche
  - IEC 60068-2-6 : vibration (permanente)
  - IEC 60068-2-14 : variation de température
  - IEC 60068-2-27 : choc
  - IEC 60068-2-30 : chaleur humide (cyclique)
  - IEC 60068-2-64 : vibration (aléatoire à large bande)
  - IEC 60068-2-78 : chaleur humide (continue)
- IEC 60825 Classe I : norme qui vérifie que le type de laser employé dans le module de focalisation laser est sans danger dans toutes les conditions d'usage normal.

2.3.3 Classification NEMA

NEMA (National Electrical Manufacturers Association) est une association des États-Unis qui élabore des normes pour les enceintes d'appareillage électrique. NEMA a publié sa propre norme NEMA 250 à l'échelle mondiale. NEMA a également adopté et publié une norme harmonisée des indices IP, ANSI/IEC 60529, par l'intermédiaire de l'ANSI (American National Standards Institute).

La norme NEMA 250 concerne la protection contre la pénétration de matières étrangères, mais elle tient également compte d'autres facteurs tels que la résistance à la corrosion, la tenue et les détails de construction. De ce fait, la classification NEMA est comparable à la classification IP, mais pas l'inverse.

Les normes UL 50 et UL 50E sont basées sur les normes NEMA 250. NEMA autorise l'autocertification, tandis que UL attribue la conformité en exigeant que les produits réussissent des essais et des contrôles d'organismes indépendants.

Table 2.3 Classification NEMA pour les coffrets dans des lieux dépourvus de risques

NEMA	Indice IP équivalent	Intérieur	Extérieur	Protection contre
Type 1	IP10	X		Accès à des pièces à risque et pénétration de corps étrangers (chute de débris). Aucune protection contre les liquides.
Type 3	IP54	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris et poussière soufflée). Pénétration d'eau (pluie, neige fondue, neige). La formation de glace à l'extérieur du coffret ne cause pas de dommages.
Type 3R	IP14	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris). Pénétration d'eau (pluie, neige fondue, neige). La formation de glace à l'extérieur du coffret ne cause pas de dommages.
Type 3S	IP54	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris et poussière soufflée). Pénétration d'eau (pluie, neige fondue, neige). Les mécanismes extérieurs restent manœuvrables lorsqu'ils sont couverts de glace.
Type 4	IP56	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris et poussière soufflée). Pénétration d'eau (pluie, neige fondue, neige, projections et jets d'eau). La formation de glace à l'extérieur du coffret ne cause pas de dommages.
NEMA 4X	IP56	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris et poussière soufflée). Pénétration d'eau (pluie, neige fondue, neige, projections et jets d'eau). Traduit un degré de protection supplémentaire contre la corrosion. La formation de glace à l'extérieur du coffret ne cause pas de dommages.
Type 6	IP67	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris). Pénétration d'eau (par jet d'eau et immersion temporaire occasionnelle à une profondeur limitée). La formation de glace à l'extérieur du coffret ne cause pas de dommages.

Table 2.3. Classification NEMA pour les coffrets dans des lieux dépourvus de risques (Suite)

Type 6P	IP67	X	X	Accès à des pièces à risque et pénétration de corps étrangers (chute de débris). Pénétration d'eau (par jet d'eau et immersion prolongée à une profondeur limitée). Traduit un degré de protection supplémentaire contre la corrosion. La formation de glace à l'extérieur du coffret ne cause pas de dommages.
Type 12	IP52	X		Sans opercule de passage. Accès à des pièces à risque et pénétration de corps étrangers (chute de débris, poussière volante, peluches, fibres et projections solides). Pénétration d'eau (gouttelettes et projections légères).
Type 12K	IP52	X		Avec opercules de passage. Accès à des pièces à risque et pénétration de corps étrangers (chute de débris, poussière volante, peluches, fibres et projections solides). Pénétration d'eau (gouttelettes et projections légères).
Type 13	IP54	X		Accès à des pièces à risque et pénétration de corps étrangers (chute de débris, poussière volante, peluches, fibres et projections solides). Pénétration d'eau (gouttelettes et projections légères). Brouillard, projection et suintement d'huile et de liquides de refroidissement non corrosifs.

NEMA TS 2 est un guide de conception qui s'applique aux équipements de signalisation du trafic.

2.3.4 Certification IK

Les codes IK sont précisés dans IEC/EN 62262, une norme internationale qui spécifie les degrés de protection contre les impacts mécaniques externes. Approuvée initialement en 1994 comme norme européenne EN 50102, elle a été adoptée en tant que norme internationale en 2002.

De nombreux fabricants choisissent de soumettre à l'essai la zone la plus faible d'un produit pour vérifier sa robustesse tout au long de sa durée de vie.

Degré	**IK01**	**IK02**	**IK03**	**IK04**	**IK05**	**IK06**	**IK07**	**IK08**	**IK09**	**IK10**	**IK10+***
Énergie de l'impact (joules)	0,14	0,2	0,35	0,5	0,7	1	2	5	10	20	50*
Masse (kg)	<0,2	<0,2	0,2	0,2	0,2	0,5	0,5	1,7	5	5	
Hauteur de chute (mm)	56	80	140	200	280	400	400	300	200	400	

*Impact jusqu'à 50 J. Le fabricant doit préciser l'énergie, la masse et la hauteur de chute de l'élément percutant.

2.4 Autres agréments

2.4.1 Protection contre les explosions

- IEC/EN/UL/SANS/CSA 60079-0 : exigences générales pour la construction, l'essai et le marquage des matériels et composants Ex prévus pour un usage en atmosphère explosive.
- IEC/EN/UL/SANS/CSA 60079-1 : exigences spécifiques pour la construction et les essais de matériels électriques protégés par le type d'enveloppe antidéflagrante « d » destiné à un usage en atmosphère explosive.

2.4.2 Agréments pour les injecteurs midspan

Lorsqu'un injecteur midspan est livré avec le produit, les agréments concernant spécifiquement l'injecteur sont recensés dans cette partie de la fiche technique. Les explications se trouvent dans les parties précédentes de ce document.

2.4.3 Sécurité du contrôle d'accès

- UL 294 : définit les exigences concernant la construction, la tenue et le fonctionnement des systèmes de contrôle d'accès.

3 Certifications

Lorsqu'une caméra est installée dans un environnement potentiellement explosif, le boîtier doit satisfaire des normes de sécurité très spécifiques. Il doit protéger l'environnement des sources d'inflammation potentielles provenant de la caméra et des autres matériels.

Les produits européens doivent respecter la directive ATEX, dont la norme internationale correspondante est IECEx. L'Amérique du Nord utilise principalement des notations de Classe/Division, du Code national d'électricité NFPA70 aux États-Unis et du code d'électricité canadien CSA C22.1, au lieu du système de Zones décrit dans ATEX et IECEx.

Table 3.1 Classement de protection contre les explosions

Classe / Division	Atmo-sphère	Définition	Zone (IECEx et ATEX)
Classe I / Division 1	Gaz	Zone dans laquelle un mélange explosif est présent en continu ou pendant de longues périodes.	Zone 0
Classe I / Division 1	Gaz	Zone dans laquelle un mélange explosif peut se former dans les conditions normales.	Zone 1
Classe I / Division 2	Gaz	Zone dans laquelle la formation d'un mélange explosif est peu probable dans les conditions normales d'exploitation, et s'il se forme, il n'existe que pendant une courte période.	Zone 2
Classe II / Division 1	Poussière	Zone dans laquelle un mélange explosif est présent en continu ou pendant de longues périodes.	Zone 20

Table 3.1. Classement de protection contre les explosions (Suite)

Classe II / Division 1	Poussière	Zone dans laquelle un mélange explosif peut se former dans les conditions normales.	Zone 21
Classe II / Division 2	Poussière	Zone dans laquelle la formation d'un mélange explosif est peu probable dans les conditions normales d'exploitation, et s'il se forme, il n'existe que pendant une courte période.	Zone 22

4 Alimentation

4.1 Classes d'alimentation par Ethernet (PoE)

Les classes de PoE assurent une distribution efficace de l'énergie par la spécification de la quantité d'électricité que nécessitera un dispositif alimenté.

Table 4.1 Classes de PoE

Classe	Type	Niveau d'alimentation garanti au niveau de la source d'alimentation	Puissance maximale consommée par le dispositif alimenté
0	Type 1, 802.3af	15,4 W	0,44 W - 12,95 W
1	Type 1, 802.3af	40,0 W	0,44 W - 3,84 W
2	Type 1, 802.3af	7,0 W	3,84 W - 6,49 W
3	Type 1, 802.3af	15,4 W	6,49 W - 12,95 W
4	Type 2, 802.3at*	30 W	12,95 W - 25,5 W
6	Type 3, 802.3bt	60 W	51 W
8	Type 3, 802.3bt	100 W	71,3 W

*Ce type est également désigné sous la dénomination PoE+.

5 Réseau

5.1 Protection et gestion de la sécurité

Il existe plusieurs moyens de lutter contre les menaces aux ressources informatiques des systèmes. Certaines menaces présentent des risques pour les dispositifs, tandis que d'autres visent les réseaux ou les données en circulation ou stockées. Voici quelques contrôles de sécurité applicables aux dispositifs et au réseau :

- Les identifiants (nom d'utilisateur/mot de passe) empêchent l'accès non autorisé à la vidéo et à la configuration des dispositifs. Une variété de niveaux de privilèges pour les comptes permet de gérer le type de ressource auquel peut accéder un type d'utilisateur.

- Le filtrage d'adresses IP (pare-feu) limite l'exposition des appareils sur le réseau local, les protégeant ainsi des accès par les clients non autorisés. Cette ligne de défense limite les risques en cas de compromission d'un mot de passe ou de détection d'une nouvelle vulnérabilité critique.
- IEEE 802.1x : protège le réseau des clients non autorisés. 802.1x constitue une protection de l'infrastructure réseau, qui utilise des switches gérés et un serveur RADIUS. Le client 802.1x intégré au dispositif réseau assure l'authentification du dispositif sur le réseau.
- HTTPS (Hypertext Transfer Protocol Secure) : protège les données (vidéo) des interceptions sur le réseau. L'utilisation de certificats signés dans HTTPS constitue un moyen pour un client vidéo de détecter s'il accède à une caméra légitime ou à un ordinateur malveillant usurpant une caméra.
- Signature de firmware : mise en œuvre par l'éditeur de logiciels, qui signe l'image du firmware avec une clé privée tenue secrète. Lorsque cette signature est associée à un firmware, le dispositif valide le firmware avant de l'accepter et de l'installer. Si l'appareil détecte que l'intégrité du firmware est compromise, il rejettera la mise à niveau du firmware. La signature de firmware Axis repose sur la méthode reconnue de chiffrement à clé publique RSA.
- Amorçage sécurisé : processus d'amorçage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM d'amorçage). Basé sur la signature de firmware, l'amorçage sécurisé garantit qu'un dispositif ne peut démarrer qu'avec un firmware autorisé. L'amorçage sécurisé garantit que le dispositif Axis est complètement exempt d'éventuels logiciels malveillants après une remise en paramètres d'usine.
- TPM (Trusted Platform Module) : composant qui procure un ensemble de fonctions cryptographiques adaptées à la protection des informations contre les accès non autorisés. La clé privée est stockée dans le TPM et ne le quitte jamais. Toutes les opérations cryptographiques nécessitant l'utilisation de la clé privée sont envoyées au TPM pour traitement. Cette méthode garantit que la partie secrète du certificat reste sécurisée même en cas de faille de sécurité.
- Axis Edge Vault : module de calcul cryptographique sécurisé (module sécurisé ou élément sécurisé) dans lequel l'ID de dispositif Axis est installé et stocké de manière sûre et permanente.

Pour accéder à des ressources supplémentaires en cybersécurité, visitez *axis.com/cybersecurity*

5.2 Protocoles pris en charge

De nombreux protocoles interviennent pour le transfert sécurisé de données d'un dispositif en réseau vers un autre.

5.2.1 Modèles de référence des protocoles

Le meilleur moyen de cerner la façon dont les différents protocoles interagissent consiste à examiner le modèle de communication OSI (Open Systems Interconnection). Il existe également le modèle de référence TCP/IP.

5.2.1.1 Modèle de référence OSI

Modèle décrivant la communication des données entre des systèmes ouverts. Pour fournir un service, chaque couche utilise les services de la couche immédiatement inférieure. Chaque couche doit respecter certaines règles, ou protocoles, pour exécuter des services.

Couche 7 : application

Met à la disposition des applications certaines fonctions telles que le transfert web, de fichiers et d'e-mail.

Les applications proprement dites, telles que les navigateurs Web ou les programmes de messagerie, existent au-dessus de cette couche et ne relèvent pas du modèle OSI.

Couche 6 : présentation des données

Vérifie que les données envoyées par la couche application d'un système sont lisibles par la couche application d'un autre système. Convertit les formats de données dépendant des systèmes, par exemple ASCII, en un format indépendant qui permet l'échange de données entre plusieurs systèmes dans la syntaxe correcte.

Couche 5 : session (connexion persistante entre hôtes homologues)

Fournit un service orienté application et gère la communication de processus entre deux systèmes. La communication de processus débute avec l'établissement d'une session, qui forme la base d'une connexion virtuelle entre deux systèmes.

Couche 4 : transport (de bout en bout [protocole orienté connexion])

Fournit un service fiable de transfert de données (par contrôle du débit et des erreurs) vers la couche 5 et au-dessus.

Couche 3 : réseau (adressage/fragmentation de paquets)

Effectue le transfert de données proprement dit, par le routage et le transfert des paquets de données entre les systèmes. Crée et administre les tables de routage et propose des options de communication au-delà des limites du réseau. Les données de cette couche sont associées à des adresses de destination et sources, qui servent de base à un routage ciblé.

Couche 2 : liaison de données (trames)

Fournit à la transmission et aux contrôles des données un accès au support de transmission, en combinant les données en unités dénommées trames. La couche 2 est divisée en deux sous-couches, la partie supérieure correspondant au contrôle de liaison logique (LLC, Logical Link Control) et la partie inférieure au contrôle d'accès au support (MAC, Media Access Control). LLC simplifie l'échange des données, tandis que MAC gère l'accès au support de transmission.

Couche 1 : physique (bits)

Fournit des services en appui de la transmission des données sous forme de flux binaire sur un support, par exemple une liaison de transmission filaire ou sans fil.

5.2.1.2 Modèle de référence Transmission Control Protocol/Internet Protocol

Le modèle de référence TCP/IP est un autre modèle permettant de comprendre les protocoles et les modalités de communication. Le modèle de référence TCP/IP comporte quatre couches, qui correspondent au modèle de référence OSI comme ci-dessous.

Table 5.1 Comparaison des modèles de référence

Modèle OSI	Modèle TCP/IP
Couche 7 : application	Couche 4 : application
Couche 6 : présentation	
Couche 5 : session	

Table 5.1. Comparaison des modèles de référence (Suite)

Couche 4 : transport	Couche 3 : transport
Couche 3 : réseau	Couche 2 : réseau Internet
Couche 2 : liaison de données	Couche 1 : interface réseau
Couche 1 : physique	

5.2.2 Protocoles de la couche application

- **CIFS/SMB** (Common Internet File System/Server Message Block) : principalement utilisé pour fournir un accès partagé aux fichiers, imprimantes et ports série, ainsi que pour les communications diverses entre les nœuds d'un réseau.
- **DDNS** (Dynamic Domain Name System) : sert à garder la trace du lien d'un nom de domaine face à un changement d'adresse IPv4.
- **DHCPv4/v6** (Dynamic Host Configuration Protocol) : attribution et gestion automatiques des adresses IP.
- **DNS/DNSv6** (Domain Name System) : convertit les noms de domaine en leur adresse IP associée.
- **FTP** (File Transfer Protocol) : principalement utilisé pour transférer des fichiers d'un serveur vers un client (téléchargement) ou d'un client vers un serveur (chargement). Peut également servir à créer et sélectionner des répertoires et à renommer ou supprimer des répertoires et des fichiers.
- **HTTP** (Hypertext Transfer Protocol) : principalement utilisé pour charger le texte et les images d'un site Web vers un navigateur Web. Les systèmes de vidéo sur IP fournissent un service de serveur HTTP qui permet d'accéder au système par le biais d'un navigateur Web pour télécharger des configurations ou des images en direct.
- **HTTP/2** : révision majeure du protocole HTTP, définie dans la RFC 7540 et publiée en février 2015.
- **HTTPS** (HTTP Secure) : adaptation du protocole HTTP pour sécuriser la communication sur un réseau informatique, largement employée sur Internet. Dans HTTPS, le protocole de communication est crypté par Transport Layer Security (TLS).
- **MQTT** (Message Queuing Telemetry Transport) : protocole de messagerie standard pour l'Internet des objets (IoT). Conçu pour simplifier l'intégration IoT, il est utilisé dans de nombreux secteurs pour connecter des dispositifs distants avec une empreinte de code réduite et une bande passante réseau minimale.
- **NTP** (Network Time Protocol) : sert à synchroniser l'heure d'un ordinateur client ou serveur avec celle d'un autre serveur.
- **RTP** (Real-Time Transport Protocol) : permet le transfert de données en temps réel entre les terminaux d'un système.
- **RTCP** (Real-Time Control Protocol) : fournit des statistiques hors bande et des informations de contrôle à une session RTP. Il se conjugue à RTP pour la livraison et le packaging des données multimédia, mais ne transfère pas les données multimédia en elles-mêmes.
- **RTSP** (Real-Time Streaming Protocol) : contrôle étendu sur la transmission de données multimédia en temps réel.
- **SFTP** (Secure File Transfer Protocol) : assure l'accès aux fichiers, le transfert de fichiers et la gestion de fichiers sur un flux de données fiable.

- **SIP** (Session Initiation Protocol) : protocole de communication pour la signalisation et le contrôle des sessions de communication multimédia.
- **SIPS** (Session Initiation Protocol Secure) : version chiffrée du protocole SIP.
- **SMTP** (Simple Mail Transfer Protocol) : norme de transfert de messages électroniques sur Internet. Les caméras réseau prennent en charge SMTP pour l'envoi d'alertes par e-mail.
- **SNMPv1/v2/v3** (Simple Network Management Protocol) : utilisé pour la surveillance et la gestion à distance d'équipements réseaux tels que switches, routeurs et caméras réseau. La prise en charge de SNMP permet la gestion des caméras réseau par des outils open source.
- **SOCKS** : permet le transfert des paquets réseau entre clients et serveurs à travers un proxy réseau distant.
- **SRTP** (Secure Real-Time Transport Protocol) : permet le transfert chiffré de données en temps réel entre les terminaux du système. Il s'agit d'une variante sécurisée de RTP.
- **SSH** (Secure Shell) : permet la gestion et l'accès au débogage des dispositifs réseau de manière sécurisée sur un réseau non sécurisé.
- **TLSv1.2/v1.3** (Transport Layer Security) : négocie une connexion privée fiable entre le client et le serveur.

5.2.3 Protocoles de la couche transport

- **TCP** (Transmission Control Protocol) : transmission séquentielle fiable et orientée connexion des flux de données. Protocole le plus courant pour la transmission des données.
- **UDP** (User Datagram Protocol) : service de transmission sans connexion, qui privilégie une livraison rapide des données plutôt que fiable.
- **ICMP** (Internet Control Message Protocol) : envoie des messages d'erreur et des informations opérationnelles indiquant qu'un service demandé, un hôte ou un routeur n'est pas disponible.

5.2.4 Protocoles de la couche réseau

- **IGMPv1/v2/v3** (Internet Group Management Protocol) : utilisé par les hôtes et les routeurs adjacents sur les réseaux IPv4 pour créer des groupes multicast, en permettant une exploitation plus efficace des ressources lors de la prise en charge de ces types d'applications.
- **IPv4/IPv6** (Internet Protocol) : adresse publique individuelle nécessaire pour que les dispositifs connectés à Internet puissent communiquer. IPv4, la version d'origine, utilise des adresses sur 32 bits. La version la plus récente, IPv6, utilise des adresses sur 128 bits, divisées en huit groupes de quatre caractères hexadécimaux.
- **USGv6** : profil de normes techniques pour IPv6, défini par le gouvernement des États-Unis pour garantir la compatibilité lors du déploiement de dispositifs réseau IPv6.

5.2.5 Protocoles de la couche liaison de données

- **ARP** (Address Resolution Protocol) : sert à détecter l'adresse MAC de l'hôte de destination.
- **CDP** (Cisco Discovery Protocol) : protocole propriétaire de Cisco servant d'alternative à LLDP pour détecter les informations sur les dispositifs matériels connectés.
- **IEEE 802.3 (i, u, ab)** : norme Ethernet qui définit la communication de données à 10 Mbits/s (10Base-T), 100 Mbits/s (100Base-TX) et 1 Gbit/s (1000Base-T) sur câblage à paires torsadées.

- **LLDP** (Link Layer Discovery Protocol) : sert à annoncer l'identité et les capacités d'un dispositif, ainsi que des autres dispositifs connectés au sein du même réseau.

5.2.6 Protocoles de détection

- **mDNS (Bonjour)** : peut servir à détecter les produits de vidéo sur IP avec un ordinateur Mac, ou en tant que protocole de détection de nouveaux dispositifs sur un réseau quelconque.
- **UPnP** (Universal Plug and Play) : les systèmes d'exploitation de Microsoft peuvent détecter automatiquement les ressources (dispositifs Axis) sur un réseau.
- **Zeroconf** : attribue automatiquement un dispositif réseau à une adresse IP non utilisée sur la plage 169.254.1.0 à 169.254.254.255.

5.2.7 Qualité de service

Dans un réseau IP, le contrôle du partage des ressources réseau est indispensable pour satisfaire les conditions de chaque service.

- **QoS** (Quality of Service) : capacité de hiérarchisation du trafic réseau pour que les flux critiques soient servis avant les flux de moindre priorité. Gain de fiabilité d'un réseau par la gestion de la bande passante utilisable par une application et la possibilité de gérer la bande passante entre applications concurrentes.
- **DiffServ** : le réseau tente de livrer un service particulier en fonction du paramètre QoS spécifié par chaque paquet.

5.2.8 Méthodes de transmission des données

Il existe trois modes de transmission des données sur un réseau informatique.

- **Unicast** : le plus courant, où l'expéditeur et le destinataire communiquent point à point. Les paquets de données sont envoyés à un seul destinataire et aucun autre client ne reçoit ces informations.
- **Multicast** : communication entre un seul émetteur et plusieurs récepteurs sur un réseau. Réduit le trafic réseau en fournissant un seul flux d'informations à plusieurs destinataires.
- **Broadcast** : l'expéditeur envoie les mêmes informations à tous les autres serveurs d'un réseau, tous les hôtes du réseau reçoivent le message et le traitent d'une manière ou d'une autre.

T10169734/FR/M2.2/2205

À propos d'Axis Communications

En concevant des solutions réseau qui améliorent la sécurité et permettent le développement de nouvelles façons de travailler, Axis contribue à un monde plus sûr et plus clairvoyant. Leader technologique de la vidéo sur IP, Axis propose des produits et services axés sur la vidéosurveillance, l'analyse vidéo, le contrôle d'accès, l'interphonie et les systèmes audio. Axis emploie plus de 3 800 personnes dans plus de 50 pays et collabore avec des partenaires du monde entier pour fournir des solutions clients adaptées. Axis a été créée en 1984 et son siège social se situe à Lund, en Suède.

Pour plus d'informations sur Axis, rendez-vous sur notre site Web *axis.com*.