

Guide des solutions réseau

ÉDUCATION

- Des salles de classe connectées. Des campus connectés. Les enseignants et les étudiants s'appuient fortement sur la technologie pour ajouter de la valeur et améliorer l'expérience d'apprentissage. Nous offrons des performances et une accessibilité de haut niveau pour les salles de classe et les utilisateurs mobiles, tout en garantissant la sécurité des données sensibles.

Besoins et objectifs du réseau d'éducation



Le secteur de l'éducation n'en est qu'à ses débuts en matière de numérique... Les DSI ont du mal à relever le défi de l'innovation et de la transformation.

Source: Gartner Research, 2019

Les réseaux éducatifs modernes sont complexes et répondent à un ensemble d'exigences en évolution rapide, dont certaines remettent en cause la technologie et sa sécurité. Les applications en ligne, l'apprentissage en ligne et les méthodes d'enseignement riches en médias offrent d'immenses avantages aux prestataires de services éducatifs.

Les élèves motivés ayant accès à des ressources d'apprentissage avancées, à l'enseignement à distance et à des possibilités en ligne font partie de la prochaine génération de l'éducation et sont plus susceptibles d'obtenir de meilleurs résultats.

Les écoles sont responsables en dernier ressort de la sécurité de leurs élèves et de leurs réseaux, et doivent fournir un environnement informatique efficace et sûr au service de l'ensemble de l'établissement - élèves, enseignants, administrateurs et tous les autres membres de la communauté scolaire.





Lorsqu'il s'agit de mettre en œuvre des réseaux, les prestataires de services éducatifs sont confrontés à un certain nombre de défis. Ils doivent fournir :



Accès filaire et sans fil à haut débit

Chaque salle de classe doit pouvoir accueillir au moins 40 ordinateurs portables/tablettes sans fil avec un accès à haut débit pour les étudiants et des connexions filaires pour les tableaux et les projecteurs. Le Wi-Fi doit être disponible sur l'ensemble du campus, à l'intérieur comme à l'extérieur.



Sécurité globale du réseau

La sécurité doit couvrir différents aspects, notamment : la protection contre les fuites de données sensibles, la disponibilité séparée des élèves, des enseignants et des ressources administratives, ainsi que la protection contre les infections des points d'accès et les mesures correctives.



Gestion aisée du réseau

Les administrateurs de réseau doivent gérer facilement les dispositifs câblés et sans fil sur site et à partir d'un centre d'opérations à distance. Les problèmes peuvent être résolus rapidement et les pannes peuvent être réparées sans qu'il soit nécessaire de faire appel à des ressources qualifiées sur place, ce qui permet de réduire les coûts.

Priorités du réseau d'éducation

- Faciliter l'accès à l'information et aux ressources, tout en maintenant la sécurité des données confidentielles
- Fournir un accès sécurisé au réseau au personnel et aux étudiants hors site
- Protégez vos données précieuses contre les menaces à l'intérieur et à l'extérieur de votre réseau
- Prendre en charge et intégrer facilement les nouvelles technologies, aujourd'hui et à mesure qu'elles arrivent, sans grever le budget
- Être facile à configurer, à gérer et à dépanner, ce qui minimise les coûts d'administration et les temps d'arrêt

Pour plus d'informations, veuillez visiter www.alliedtelesis.com/solutions/industry/education

Solution Allied Telesis pour l'éducation

Allied Telesis est un leader dans le domaine des solutions de réseau.

Grâce à notre expérience éprouvée dans la fourniture de solutions réseau avancées hautement fiables et riches en fonctionnalités, de plus en plus d'établissements d'enseignement se tournent vers Allied Telesis pour atteindre leurs objectifs.

Chez Allied Telesis, nous comprenons la nécessité de fournir des services de réseau de pointe à la génération de demain, dans le cadre de budgets limités. Allied Telesis met en œuvre des réseaux éducatifs de pointe depuis de nombreuses années. Notre portefeuille de produits avancés à haute valeur ajoutée fournit la sécurité, la mobilité et la haute performance dont vous avez besoin pour votre réseau éducatif, aujourd'hui et à l'avenir.

Voyons comment Allied Telesis relève les défis de l'éducation et fournit des solutions qui facilitent les possibilités d'éducation avancées.

Regarder vers l'avenir

Les produits Allied Telesis optimisent vos investissements technologiques en s'intégrant parfaitement aux systèmes et applications existants. Au fur et à mesure que les besoins éducatifs évoluent, votre réseau peut facilement s'adapter, car nos produits fournissent une infrastructure hautement efficace et évolutive, conçue pour répondre à vos besoins.

Alors que des idées nouvelles et passionnantes sont mises en œuvre dans le domaine de l'éducation, les produits d'Allied Telesis restent à l'avant-garde, en fournissant une infrastructure réseau qui encourage la créativité et influence positivement la prochaine génération.



Contrôle d'accès au réseau

Veillez à ce que votre personnel et vos étudiants aient constamment accès aux ressources appropriées, tout en protégeant les informations confidentielles et en préservant la vie privée.



Le réseau d'autodéfense

Notre sécurité intelligente protège vos réseaux câblés et sans fil des menaces internes en mettant automatiquement en quarantaine les appareils suspects, créant ainsi un environnement sûr pour les étudiants et les enseignants.



La gestion des réseaux en toute simplicité

Automatisez la gestion de votre réseau à l'aide d'un outil intelligent unique et facile à utiliser, qui renforce la visibilité et la sécurité et réduit les risques et les coûts d'assistance.



Wi-Fi sans compromis

Garantissez des connexions Wi-Fi fiables et performantes partout où elles sont nécessaires. Grâce à la prise en charge d'une densité élevée d'appareils, les appareils d'intérieur et d'extérieur constituent une solution unique pour les salles de classe, les bibliothèques, les lieux de rassemblement et les espaces de loisirs.



Sécurité vidéo numérique

Une gamme de produits dédiés permet de transporter de manière sûre et fiable des séquences vidéo sur votre réseau IP.

CONTRÔLE D'ACCÈS AU RÉSEAU

Veillez à ce que votre personnel et vos étudiants aient constamment accès aux ressources appropriées en tenant compte des droits d'accès au niveau de l'architecture du réseau.

Fournir aux individus un accès approprié aux ressources du réseau et créer un environnement prêt pour l'évaluation numérique peut sembler complexe et nécessiter de multiples niveaux de privilèges pour préserver la confidentialité des informations et le respect de la vie privée.

Les prestataires de services éducatifs conservent des informations essentielles sur les élèves et les programmes scolaires, qui doivent rester confidentielles et être protégées contre toute utilisation malveillante. Une politique de droits d'accès doit garantir que seules les personnes et les appareils appropriés peuvent accéder à ces informations confidentielles.

Les produits Allied Telesis prennent en charge le contrôle d'accès au réseau (NAC), une approche de pointe qui permet de contrôler complètement l'accès des utilisateurs au réseau. Les utilisateurs peuvent avoir différents niveaux d'accès, ce qui permet une disponibilité correcte du réseau et des ressources pour les étudiants, les enseignants et le personnel administratif. Le NAC vérifie également l'adhésion des appareils aux politiques de sécurité du réseau avant d'accorder l'accès au réseau, ce qui permet d'arrêter les menaces de manière proactive avant qu'elles ne pénètrent dans le réseau.

NAC a introduit la mise en réseau basée sur l'identité, qui est supérieure aux méthodes précédentes de contrôle de l'accès à l'information en ligne. La nature automatisée de NAC est un réel avantage pour le personnel informatique occupé, car elle simplifie les tâches d'administration complexes.

Services intégrés

Les commutateurs Allied Telesis simplifient l'administration en intégrant plusieurs services réseau :

- Le serveur RADIUS interne vérifie l'identité des utilisateurs afin de préserver la sécurité du réseau et d'éviter les intrusions
- Le contrôle des tempêtes garantit un réseau robuste et résilient en gérant la quantité de trafic autorisée sur le réseau et en faisant face à toute augmentation inattendue
- Le serveur DHCP interne automatise la distribution des adresses réseau à chaque ordinateur
- Un chronomètreur centralisé garantit que votre réseau fonctionne toujours en parfaite synchronisation
- La protection contre les boucles permet d'éviter les erreurs de câblage accidentelles

Pour plus d'informations, veuillez visiter www.alliedtelesis.com/solutions/total-autonomous-networking

La centralisation de l'administration du réseau réduit considérablement le besoin d'experts informatiques à plein temps, tout en augmentant la sécurité et la robustesse.

Source: Gartner Research, 2019

De nombreux fournisseurs de réseaux de premier plan ont mis en œuvre des solutions NAC, et les produits de commutation avancés d'Allied Telesis prennent en charge un certain nombre d'entre elles, y compris les solutions de Microsoft, Symantec et Sophos. Les produits Allied Telesis ont fait l'objet de nombreux tests de conformité avec les produits NAC les plus répandus, et nous avons publié des guides pratiques étape par étape pour la mise en œuvre d'une solution complète. Les produits et l'expertise d'Allied Telesis permettent de mettre en place des solutions NAC robustes avec un minimum d'efforts.

Approche d'Allied Telesis en matière de contrôle d'accès au réseau

Le NAC permet un contrôle sans précédent de l'accès des utilisateurs au réseau, afin d'atténuer les menaces qui pèsent sur l'infrastructure du réseau. Les commutateurs Allied Telesis utilisent l'authentification IEEE 802.1x basée sur le port en partenariat avec l'affectation dynamique de VLAN conforme aux normes, pour évaluer l'adhésion d'un utilisateur aux politiques de sécurité du réseau et soit accorder l'authentification, soit proposer une remédiation.

En outre, si plusieurs utilisateurs partagent un port, il est possible d'utiliser l'authentification multiple. Les différents utilisateurs d'un même port peuvent être affectés à différents VLAN, et donc bénéficier de différents niveaux d'accès au réseau. En outre, un VLAN invité peut être configuré pour servir de fourre-tout aux utilisateurs qui ne sont pas authentifiés.





LE RÉSEAU D'AUTODÉFENSE

Les établissements d'enseignement deviennent de plus en plus la cible des cybercriminels. Les connexions sécurisées aux ressources en ligne et à l'internet, protégeant à la fois le réseau et les étudiants contre les contenus inappropriés et les menaces malveillantes, sont désormais obligatoires pour tout établissement d'enseignement.

Les modèles de sécurité traditionnels qui se concentrent sur la prévention des attaques à l'intérieur du réseau n'offrent plus une protection suffisante, car les attaques peuvent facilement provenir de l'intérieur du réseau via un ordinateur portable, une tablette ou tout appareil IoT infecté directement connecté sur le réseau d'accès câblé ou sans fil.

Parallèlement, les attaquants ont gagné en sophistication et les menaces se présentent aujourd'hui sous des formes si diverses que le maintien d'un réseau sécurisé mais efficace est devenu un défi coûteux en temps et en argent.

Si l'approche traditionnelle basée sur le pare-feu peut détecter et bloquer la plupart des menaces et des virus provenant de l'internet, elle montre ses limites dès que l'attaque provient de l'intérieur du réseau. À ce stade, l'attaque se propage d'est en ouest sur le réseau (c'est-à-dire d'un appareil connecté à un autre), où elle ne peut être détectée par le pare-feu qu'une fois que la menace tente de franchir la frontière vers l'internet. Une fois la menace détectée, un administrateur peut être alerté et les mesures correctives peuvent commencer.

La cybersécurité continue d'être une priorité absolue pour les DSI du secteur de l'éducation.

Source: Gartner 2020 CIO Agenda on Education

119

aux États-Unis au moins, les écoles ont subi 122 cyberattaques en 2018, notamment des violations de données, des escroqueries par phishing et des attaques de ransomware.

*Source : Cybersécurité K-12
Centre de ressources*

Pour plus d'informations, veuillez visiter www.alliedtelesis.com/solutions/self-defending-networks

AMF-SEC

Le contrôleur AMF-Sec d'Allied Telesis permet de mettre en œuvre notre solution de pointe en matière de gestion et de sécurité du réseau. Il répond exactement aux besoins des établissements d'enseignement : réduction des coûts de gestion, renforcement de la sécurité et amélioration de l'expérience de l'utilisateur final.

Caractéristiques principales :

- Compatible avec OpenFlow v1.3
- Convient aux réseaux câblés et sans fil
- Intégration avec les applications professionnelles pour gagner du temps et de l'argent
- S'intègre aux produits de sécurité pour fournir une réponse instantanée aux menaces
- Isolation intelligente et automatique des dispositifs suspects
- Évolutif - ajoutez plus d'applications d'entreprise pour une plus grande valeur ajoutée

S'intègre à nos outils de gestion de réseau pour une plus grande facilité d'utilisation

Malheureusement, le processus de remédiation dépend souvent des ressources humaines, avec des temps de réaction allant de quelques minutes à quelques heures, voire quelques jours, en fonction de la disponibilité et des compétences des ressources.

Le réseau d'autodéfense

La solution Self-Defending Network offre une approche intégrée de la sécurité du réseau, en automatisant les opérations informatiques manuelles et en protégeant contre les menaces provenant des dispositifs d'accès câblés et sans fil.

En utilisant le moteur de sécurité AMF-Sec, qui ne nécessite pas d'agents ou de logiciels pour les points finaux, notre solution répond automatiquement aux menaces identifiées.

Les pare-feu et les dispositifs de sécurité identifient les menaces, puis le moteur intelligent mettant en œuvre la technologie Isolation Adapter intégrée à AMF-Sec réagit immédiatement pour isoler la partie du réseau affectée et mettre en quarantaine l'appareil suspect. Des mesures correctives peuvent être appliquées pour que l'appareil puisse rejoindre le réseau avec un minimum de perturbations. Les réponses automatisées sont configurables et la journalisation complète fournit une piste d'audit claire.

Le contrôleur AMF-Sec est la clé de notre solution de sécurité AMF innovante et primée, qui permet de créer des réseaux d'autodéfense aidant les organisations à éviter les pertes de temps et les interruptions inutiles des services de réseau.





LA GESTION DES RÉSEAUX EN TOUTE SIMPLICITÉ



La complexité croissante des réseaux éducatifs augmente considérablement les exigences en matière de gestion de réseau et de ressources spécialisées. La mise en œuvre de solutions d'automatisation simplifie la vie et la rend plus abordable.

Vista Manager EX est une approche de la gestion de réseau basée sur des plug-ins. Il dispose d'un tableau de bord affichant les détails, l'état et les événements du réseau sur une carte topologique, et il met en évidence les problèmes critiques afin de minimiser le temps de réaction et d'aider à résoudre les problèmes en temps opportun.

Une série de plug-ins pour contrôler le réseau câblé, les appareils sans fil, la liaison WAN et les outils d'automatisation facilitent la mise en réseau et rendent la solution modulaire.

Allied Telesis Autonomous Management Framework™ Plus (AMF Plus)

Réduisez les coûts d'exploitation du réseau grâce à l'intelligence et à l'automatisation de la gestion centralisée. Les services automatisés, y compris les mises à jour de micrologiciels, la sauvegarde, la récupération et le provisionnement sans contact ne sont que quelques-unes des caractéristiques de l'AMF Plus qui permettent de minimiser les ressources nécessaires à la gestion d'un réseau éducatif complexe.

Autonomous Wave Control (AWC) - plugin

Analysez et optimisez les performances de réseaux sans fil complexes. Installez et oubliez votre réseau sans fil grâce à un outil autonome qui analyse les modèles de trafic et configure automatiquement les points d'accès pour répondre à la demande.

“Les déficits de financement et les coûts opérationnels sont les principales préoccupations des organisations éducatives.”

*Source : Cybersécurité K-12
Centre de ressources*

Pour plus d'informations, veuillez visiter www.alliedtelesis.com/solutions/total-autonomous-networking

AMF PLUS

Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) est une plate-forme de gestion de réseau évolutive.

Il prend en charge les produits de commutation, de pare-feu et sans fil d'Allied Telesis, ainsi qu'une large gamme de périphériques tiers, y compris les caméras de vidéosurveillance et les téléphones IP, pour une automatisation du réseau vraiment complète.

VISTA MANAGER™

Vista Manager EX offre une surveillance de pointe et crée automatiquement une carte topologique complète des commutateurs, des pare-feu et des points d'accès sans fil.

Le mappage et la création de VLAN entre les appareils, ainsi que la surveillance du trafic et le mappage WAN, permettent de gérer sans effort un grand nombre d'appareils réseau, voire tous, à la fois.

Vista Manager Mini est intégré dans nos principaux commutateurs et routeurs Allied Telesis pour permettre une gestion rapide et facile du réseau pour les petites et moyennes installations. Il offre un accès immédiat à la puissance de l'AMF Plus et de l'AWC pour la gestion des réseaux câblés et sans fil.

Software Defined WAN (SD-WAN)

Gestion centralisée et optimisation automatique du trafic interprofessionnel. Disposer de plusieurs connexions avec des performances et des coûts différents nécessite une attention permanente. Notre orchestrateur SD-WAN gère de manière centralisée les connexions des succursales pour une livraison fiable et sécurisée des applications. Définissez des mesures de performance acceptables, optimisez et équilibrez automatiquement la livraison des applications et surveillez facilement les performances du réseau étendu.

Simple Network Management Protocol (SNMP) - plugin

Auto-découvrez et gérez une large gamme d'appareils dans un environnement multi-fournisseurs dans Vista Manager EX avec le plugin SNMP. Différentes vues du réseau permettent d'obtenir la visibilité que vous souhaitez. Étendez la surveillance du réseau avec des notifications et des alertes automatisées pour une gestion proactive.





WI-FI SANS COMPROMIS



Le sans fil est aujourd'hui la première technologie d'accès sur le marché de l'éducation. Elle permet aux étudiants, aux enseignants et aux membres du personnel d'accéder au réseau depuis n'importe quel endroit et à n'importe quel moment, en tant que principal choix d'accès pour la classe et le campus.

Une connexion sans fil stable supportant la vidéo et le contenu éducatif sans interruption est obligatoire. Les connexions sans fil instables entraînent un manque de concentration et affectent les progrès de la classe.

Le sans-fil étant obligatoire dans les classes, la disponibilité du sans-fil dans les bibliothèques, les espaces de loisirs et les espaces extérieurs fait partie intégrante de l'ensemble du réseau d'éducation.

Malgré l'évolution de la norme sans fil qui améliore les performances globales, il existe encore des limitations techniques qui font qu'un technicien qualifié est nécessaire pour mettre en place un réseau sans fil stable.

Dans un réseau sans fil, la déconnexion des clients et/ou la lenteur des communications sont des signes typiques de problèmes techniques. Les principales raisons de ces problèmes sont les interférences entre les canaux radio, les sources externes sans fil qui ne sont pas sous le contrôle de l'IT, un manque de puissance du signal du point d'accès (AP).

Dans un environnement dynamique tel qu'un bâtiment scolaire ou un campus, il est nécessaire de surveiller en permanence le réseau et de disposer de ressources informatiques qualifiées pour maintenir l'installation sous contrôle et fournir un service sans fil de qualité.

AWC

Allied Telesis Autonomous Wave Control (AWC) est une technologie réseau avancée qui utilise l'intelligence artificielle (IA) pour apporter des améliorations significatives à la connectivité et aux performances des réseaux sans fil tout en réduisant les coûts de déploiement et d'exploitation.

Pour plus d'informations, veuillez visiter www.alliedtelesis.com/solutions/wifi

Wi-Fi sans compromis

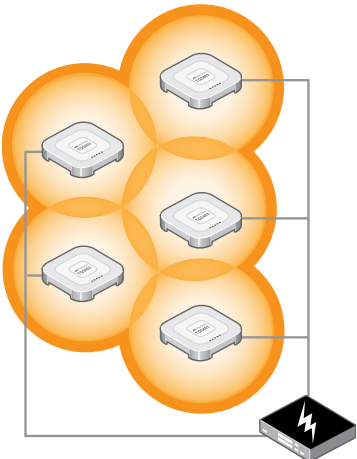
La solution No Compromise Wi-Fi d'Allied Telesis garantit des connexions Wi-Fi fiables et performantes partout où elles sont nécessaires, en minimisant le besoin d'intervention humaine.

En analysant les lacunes de la couverture du signal et les interférences des points d'accès Wi-Fi, le contrôle autonome des ondes (AWC) offre automatiquement une expérience sans fil de haute qualité. Réduisez votre dépendance à l'égard d'ingénieurs réseau qualifiés et bénéficiez de coûts d'exploitation réduits.

Pour les environnements critiques, comme les grandes salles, la couverture de canal AWC (AWC-CB) permet de contrôler les points d'accès hybrides qui fournissent simultanément une connectivité Wi-Fi à canal unique et à canaux multiples.

Chaque fois qu'une extension du réseau est nécessaire et qu'aucun câble n'est disponible, AWC Smart Connect (AWC-SC) fournit une solution d'extension en temps zéro. Il suffit d'enregistrer les points d'accès dans le système de gestion, de brancher l'alimentation et le nouveau point d'accès est prêt à être utilisé.

AWC-CB

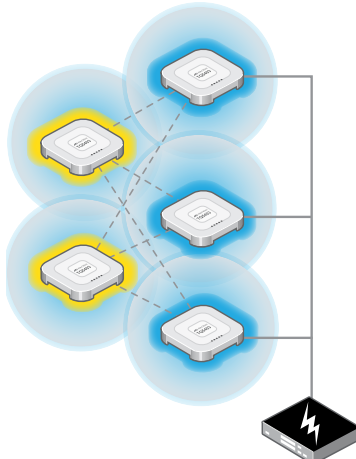


Allied Telesis AWC Channel Blanket (AWC-CB) est la solution de canal unique pour les AP sans fil d'Allied Telesis.

Tous les points d'accès membres de la même couverture fonctionnent sur le même canal. L'AWC-CB est un contrôleur intelligent qui gère les interférences et l'accès des clients.

Associé à une approche multicanal traditionnelle, il constitue une solution d'accès sans fil complète pour tous les environnements.

AWC-SC



Allied Telesis AWC Smart Connect (AWC-SC) est une extension de réseau sans fil sans effort et sans fils supplémentaires. Il suffit d'enregistrer le nouveau point d'accès, de brancher l'alimentation et c'est prêt.

Réduisez le temps d'installation de 90 % en fournissant un provisionnement autonome pour la connectivité événementielle ou l'expansion rapide des bureaux sans avoir besoin de nouveaux câbles.



SÉCURITÉ VIDÉO NUMÉRIQUE



Dans tout réseau moderne, une grande partie de la bande passante utilisée est composée de flux vidéo. Au sein d'une école, d'un campus ou d'une université, il existe principalement deux types de flux, chacun ayant un impact différent sur les performances du réseau.

Vidéo IP pour la sécurité

La sécurité et la protection des élèves à l'école font partie de l'ensemble de l'offre éducative. La capacité de surveillance est l'un des moyens d'accroître la confiance des familles et des élèves dans une école donnée et d'attirer de nouveaux élèves.

Dans toute mise en œuvre de vidéosurveillance, toutes les caméras et tous les systèmes de gestion vidéo s'appuient sur l'infrastructure réseau pour transporter la vidéo. Le trafic généré par les caméras de surveillance est presque constant au cours de la journée. Bien que ce trafic doive être planifié, une fois que le réseau et la liaison sont dimensionnés, il ne pose généralement pas de problème de gestion.

La partie principale de l'installation est alimentée par Power over Ethernet (PoE) avec une consommation électrique qui dépend de plusieurs facteurs tels que le type de caméra et les accessoires (chauffage, moteurs, etc.). Lors de la phase de conception du réseau, les commutateurs d'accès connectés aux caméras IP doivent être en mesure de fournir suffisamment d'énergie pour alimenter toutes les caméras connectées.

Apprentissage en ligne

La vidéo est également largement utilisée pour les cours, l'apprentissage à distance et comme ressource pour les étudiants en dehors des heures de cours.

Le trafic généré par ce type de vidéo est moins prévisible, et si toute une classe diffuse en même temps, des pics de trafic peuvent se produire. Pour être efficace, le service vidéo doit être disponible sans retard ni dégradation de l'image. Tout problème peut entraîner une distraction et, par conséquent, une perte d'attention de la part des élèves. La conception du réseau doit être capable d'absorber les pics de trafic sans affecter les autres utilisateurs ou ressources.

Classes PoE

- Classe 0 jusqu'à 15 W
- Classe 1 jusqu'à 4 W
- Classe 2 jusqu'à 7 W
- Classe 3 jusqu'à 15 W
- Classe 4 jusqu'à 30 W
- PoE élevé jusqu'à 60 W



Pour plus d'informations, veuillez visiter www.alliedtelesis.com/solutions/surveillance

Autres sources vidéo

Une autre source de trafic est la diffusion de vidéos à partir d'autres sources telles que YouTube, qui ne font souvent pas partie de l'offre éducative, mais qui sont tout de même accessibles via le réseau de l'école.

Ce trafic est largement imprévisible et ne fait souvent pas partie des services de l'école. Il doit donc être contrôlé pour éviter de perturber les services prioritaires. Généralement, on y parvient en attribuant aux flux vidéo une faible priorité afin qu'ils puissent être rejetés en cas d'encombrement et si un trafic plus prioritaire doit être transmis.

Une large bande passante, un dimensionnement correct de la liaison et une gestion des priorités sont les éléments clés d'une diffusion vidéo fiable et fluide, pour une expérience utilisateur et des résultats d'apprentissage optimaux.

À PROPOS ALLIED TELESIS

Depuis près de 30 ans, Allied Telesis fournit une connectivité fiable et intelligente aux entreprises et aux projets d'infrastructure complexes et essentiels dans le monde entier.

Dans un monde qui évolue vers les villes intelligentes et l'Internet des objets, les réseaux doivent évoluer rapidement pour relever de nouveaux défis. Les technologies intelligentes d'Allied Telesis, telles qu'Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) et Enterprise SDN, garantissent que l'évolution du réseau peut suivre le rythme et fournir des solutions efficaces et sécurisées pour les personnes, les organisations et les "choses", aujourd'hui et à l'avenir.

Allied Telesis est reconnu pour avoir innové dans la manière dont les services et les applications sont fournis et gérés, ce qui se traduit par une augmentation de la valeur et une réduction des coûts d'exploitation.

Visitez-nous en ligne sur alliedtelesis.com.

