

Guide des solutions réseau

EDUCATION

Salles de classe connectées, campus connectés. Aujourd'hui, pour ajouter de la valeur et améliorer l'expérience éducative, les enseignants et les étudiants dépendent de la technologie. Nous proposons des solutions réseau de hautes performances, pour les salles de classe et les utilisateurs mobiles, tout en protégeant l'infrastructure et en garantissant la sécurité des données sensibles.

Besoins et objectifs



Le secteur de l'éducation est en pleine évolution 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 formation.

Les élèves qui auront accès à des ressources d'apprentissage avancées, à l'enseignement à distance et aux applications en ligne, seront plus susceptibles d'obtenir de meilleurs résultats.

Les écoles ont la responsabilité ultime de la sécurité de leurs élèves et de leurs réseaux, et doivent fournir une solution efficace, sûre et un environnement informatique efficace au service de toute l'école - élèves, enseignants, administrateurs et tous les autres membres de la communauté scolaire.





Lorsqu'il s'agit de mettre en place une infrastructure réseau, les prestataires de services sont confrontés à plusieurs défis. Ils doivent permettre :



Un accès filaire et sans fil haut débit

Chaque salle de classe doit prendre en charge au moins 40 ordinateurs portables / tablettes sans fil avec accès haut débit pour les étudiants et connexions filaires pour les tableaux noirs et les projecteurs. Le Wi-Fi doit être disponible sur le campus, à l'intérieur et à l'extérieur.



La sécurité globale du réseau

La sécurité doit répondre à différentes préoccupations, notamment: la protection contre les fuites de données sensibles, la disponibilité des ressources distinctes pour les étudiants, les enseignants et les administrateurs et la protection et la désinfection des équipements informatiques.



Une gestion simplifiée du réseau

Les administrateurs réseau doivent pouvoir gérer facilement les appareils câblés et sans fil sur site et à partir d'un centre d'opérations distant. Les problèmes peuvent être résolus rapidement et les défaillances peuvent être réparées sans avoir besoin de ressources qualifiées sur place, ce qui réduit les coûts de fonctionnement.

Priorités du réseau Education

Faciliter l'accès aux informations et aux ressources tout en préservant la sécurité des données confidentielles

Fournir un accès réseau sécurisé au personnel et aux étudiants hors site

Protéger vos précieuses données contre les menaces réseau, à la fois de l'intérieur et de l'extérieur de votre réseau

Acquérir et intégrer facilement les nouvelles technologies à la fois maintenant et dès leur arrivée - sans exploser le budget

Etre simple à configurer, à gérer et à dépanner, en minimisant 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'Education

Allied Telesis est un fournisseur majeur de solutions réseau.

Allied Telesis est un acteur historique dans la fourniture de solutions de réseau avancées, fiables, sécurisées et riches en fonctionnalités. de plus en plus de prestataires se tournent vers Allied Telesis pour atteindre ses objectifs.

Allied Telesis met en œuvre des réseaux éducatifs de pointe depuis de nombreuses années. Notre catalogue étendu de produits à haute valeur ajoutée offre la sécurité, la mobilité et les hautes performances dont vous avez besoin pour votre réseau éducatif, à la fois maintenant et pour l'avenir avec un très bon retour sur investissement (RSI ou ROI).

Voyons comment Allied Telesis relève les défis auxquels l'éducation est confrontée et propose des solutions qui facilitent les possibilités de formation avancées.

Regarder vers l'avenir

Les produits Allied Telesis optimisent vos investissements technologiques en s'intégrant pleinement aux systèmes et applications existants. Comme l'éducation a besoin d'évoluer, votre réseau peut facilement s'adapter, car nos produits permettent une infrastructure parfaitement efficace et évolutive, conçue pour répondre à vos besoins.

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



Contrôle d'accès réseau

Assurez-vous que votre personnel et vos étudiants ont un accès constant aux ressources appropriées, tout en protégeant les informations confidentielles et en préservant la confidentialité.



Le Self-Defending Network

Notre sécurité Smart Edge 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 de réseau simplifiée

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



No Compromise Wi-Fi

Assurez des connexions Wi-Fi fiables et de hautes performances partout où elles sont nécessaires. Grâce à la prise en charge de l'ensemble des appareils connectés. Nos bornes Wi-Fi professionnelles homologuées pour l'intérieur et l'extérieur offrent une solution unique pour les salles de classe, les bibliothèques, les lieux de rassemblement et de loisirs.



Sécurité vidéo numérique

Un portefeuille de produits dédié transporte de manière sécurisée et fiable des séquences vidéo sur votre réseau IP.

CONTRÔLE D'ACCÈS AU RÉSEAU

Assurez-vous que votre personnel et vos étudiants ont un accès constant 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 une évaluation numérique peut sembler complexe, nécessitant plusieurs ensembles de niveaux de privilège de ressources pour maintenir la vie privée et la confidentialité des informations.

Les prestataires de services du monde de l'éducation, conservent des informations essentielles sur les étudiants et les programmes d'études, qui doivent rester confidentielles et 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 Network Access Control (NAC, contrôle d'accès au réseau), une approche de pointe pour fournir un contrôle complet sur l'accès des utilisateurs au réseau. Les utilisateurs peuvent avoir différents niveaux d'accès, ce qui permet une disponibilité du réseau concerné 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, arrêtant proactivement les menaces avant qu'elles ne puissent pénétrer dans le réseau.

Le NAC permet de mettre en place un réseau basé sur l'identité, qui est supérieur aux méthodes précédentes de contrôle de l'accès aux informations en ligne. La nature automatisée du NAC présente un réel avantage pour le personnel informatique, car elle simplifie les tâches d'administration complexes.

De nombreux fournisseurs de premier plan ont mis en œuvre des solutions NAC, mais les produits de commutation avancés Allied Telesis prennent en charge un certain nombre d'entre eux, comme les solutions de Microsoft, Symantec et Sophos. La conformité des produits Allied Telesis aux produits NAC populaires a été largement testée et nous avons publié des guides pratiques étape par étape pour mettre en œuvre une solution complète. Les produits et l'expertise d'Allied Telesis permettent de mettre en place des solutions NAC robustes avec un minimum d'effort.

Services intégrés

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

- Le serveur RADIUS interne vérifie l'identité des utilisateurs pour protéger le réseau et le protéger des intrus
- Le Storm control garantit un réseau robuste et résilient en gérant la quantité de trafic autorisée sur le réseau et en traitant toute surtension inattendue
- Le serveur DHCP interne automatise la distribution des adresses réseau sur chaque ordinateur
- Un chronomètre centralisé garantit que votre réseau fonctionne toujours en parfaite synchronisation
- La protection contre les boucles protège contre les erreurs de câblage accidentelles

Pour plus d'informations, merci de visiter la page www.alliedtelesis.com/solutions/total-autonomous-networking

L'administration centralisée
du réseau, réduit
considérablement le temps
d'intervention des experts,
tout en augmentant la
sécurité et la robustesse.

Approche Allied Telesis pour le contrôle d'accès au réseau

Le NAC permet un contrôle sans précédent de l'accès des utilisateurs au réseau ce qui abaisse les menaces pesant sur l'infrastructure du réseau. Les commutateurs Allied Telesis utilisent une authentification basée sur le port IEEE 802.1x conjugué à une attribution de VLAN dynamique conforme aux normes, pour évaluer l'adhésion d'un utilisateur aux politiques de sécurité du réseau et accorder une authentification ou proposer une correction.

Si plusieurs utilisateurs partagent le même réseau, la multi-authentification peut être utilisée. On peut affecter différents utilisateurs sur le même réseau qui peuvent être affectés à différents VLAN, et donc à différents niveaux d'accès au réseau. De plus, un VLAN invité peut être configuré pour fournir un accès aux utilisateurs qui ne sont pas authentifiés.





LE SELF-DEFENDING NETWORK

Les organisations éducatives deviennent de plus en plus une cible pour les cybercriminels. Des connexions sécurisées aux ressources en ligne et à Internet, protégeant à la fois le réseau et les étudiants contre le matériel inapproprié et les menaces malveillantes, sont désormais obligatoires pour tout établissement d'enseignement.

Les modèles de sécurité traditionnels qui visent à empêcher les attaques de pénétrer 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 infecté, une tablette ou tout appareil IoT directement connecté sur le réseau d'accès filaire ou sans fil.

Parallèlement, les attaquants ont gagné en sophistication et les menaces se présentent désormais sous tellement de formes que le maintien d'un réseau sécurisé mais efficace est devenu un défi long et coûteux.

Bien que l'approche traditionnelle basée sur un pare-feu puisse détecter et bloquer la plupart des menaces et virus provenant d'Internet, elle présente des limites une fois que l'attaque provient de l'intérieur du réseau. À ce stade, l'attaque se propagera est/ouest sur le réseau (c'est-à-dire d'un appareil connecté à un autre), où elle ne pourra être détectée par le pare-feu qu'une fois que la menace tentera de franchir la frontière vers Internet. Une fois la menace détectée, un administrateur peut être alerté et la correction peut commencer.

Malheureusement, le processus de correction dépend souvent des ressources humaines, avec des temps de réaction allant de quelques minutes à quelques jours, selon la disponibilité des ressources et les compétences.

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

Source: Gartner 2020 CIO Agenda on Education

119
écoles au moins aux États-Unis ont connu 122 cyberattaques en 2018, y compris des violations de données, des escroqueries par phishing et des attaques de ransomwares.

Source: K-12 Cybersecurity Resource Center

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

Pour plus d'informations, rendez-vous sur **alliedtelesis.com**

Guide des solutions pour l'Éducation | 7

Le contrôleur Allied Telesis AMF-Sec est une solution de gestion de réseau et de sécurité de pointe. Il fournit exactement ce dont les organisations éducatives ont besoin: des coûts de gestion réduits, une sécurité accrue et une expérience utilisateur améliorée.

Principales caractéristiques:

- Compatible avec OpenFlow v1.3
- Convient aux réseaux câblés et sans fil
- S'intègre aux applications professionnelles pour gagner du temps et de l'argent
- S'intègre aux produits de sécurité pour fournir une réponse instantanée aux menaces
- Isole intelligemment et automatiquement les appareils suspects
- Évolutif: ajoutez plus d'applications professionnelles pour plus de valeur
- S'intègre à nos outils de gestion de réseau pour une plus grande facilité d'utilisation

Le Self-Defending Network

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

En utilisant le moteur de sécurité AMF-Sec, qui ne nécessite ni agents ni logiciels d'extrémité, notre solution répond automatiquement aux menaces identifiées.

Le pare-feu et les dispositifs de sécurité identifient les menaces, puis le moteur intelligent implémentant l'Isolation Adapter technology intégré à AMF-Sec répond immédiatement pour isoler la partie affectée du réseau et mettre en quarantaine le périphérique suspect. La correction peut être appliquée afin que l'appareil puisse rejoindre le réseau avec un minimum de perturbations. Les réponses automatisées sont configurables et une journalisation complète fournit une piste d'audit claire.

Le contrôleur AMF-Sec est la clé de notre solution innovante et primée, la solution Self-Defending Networks, elle, aide les organisations à éviter les pertes de temps et les interruptions inutiles des services réseau.





LA GESTION DE RÉSEAU SIMPLIFIÉE



L'augmentation de la complexité du réseau éducatif augmente considérablement les demandes de gestion de réseau et de ressources spécialisées. La mise en œuvre de solutions d'automatisation simplifie le quotidien et réduit les coûts de fonctionnement.

Vista Manager EX est une solution graphique modulaire qui, grâce à plusieurs plugins, qui peuvent être ajoutés, permet de gérer graphiquement et contrôler les réseaux cablés, sans fil et Wan. En affichant l'état du réseau et les événements sur une carte topologique, elle vous permet de réagir plus rapidement face aux problèmes critiques.

Une série de plugins permettent de contrôler le réseau câblé, les appareils sans fil, la liaison WAN et les outils d'automatisation facilitent la mise en réseau et la solution modulaire.

Autonomous Management Framework (AMF) - plugin

Réduisez les coûts d'exploitation du réseau avec l'intelligence et l'automatisation supplémentaires de la gestion centralisée. Services automatisés, les mises à niveau de l'OS, la sauvegarde, la récupération et le provisionnement sans contact ne sont que quelques-unes des fonctionnalités d'AMF pour minimiser les ressources nécessaires à la gestion d'un réseau éducatif complexe.

Autonomous Wave Control (AWC) - plugin

Analysez et optimisez les performances des réseaux sans fil complexes. Installez et oubliez votre réseau sans fil avec 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 d'exploitation sont les préoccupations majeures pour les organisations éducatives”.

*Source: K-12 Cybersecurity
Centre de ressources*

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



Autonomous Management Framework™ (AMF) d'Allied Telesis est une plateforme de gestion de réseau évolutive.

Il prend en charge la commutation Allied Telesis, le pare-feu et les produits sans fil, ainsi qu'une large gamme d'appareils tiers, notamment des caméras de vidéosurveillance et des téléphones IP, pour une automatisation de réseau véritablement inclusive.

Software Defined WAN (SD-WAN) - plugin

Gérez de manière centralisée et optimisez automatiquement entre vos sites. Avoir plusieurs connexions avec des performances et des coûts différents nécessite une attention continue. Notre orchestrateur SD-WAN gère de manière centralisée les connexions des succursales pour une livraison d'applications fiable et sécurisée. Définissez des mesures de performances acceptables, optimisez et équilibrez automatiquement la livraison des applications et surveillez facilement les performances du WAN.

Simple Network Management Protocol (SNMP) - plugin

Étendez la surveillance de votre réseau à des périphériques tiers dans Vista Manager EX. Ses alertes et modifications automatiques, vous permettent une gestion proactive.

AT-VISTA MANAGER™ EX

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 une gestion sans effort de nombreux ou de tous les appareils réseau à la fois.

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





NO COMPROMISE WI-FI



Le WI-FI est aujourd’hui une technologie essentielle sur le marché de l’éducation. Il permet aux étudiants, aux enseignants et aux membres du personnel d’accéder au réseau à tout moment et en tout lieu en tant que principal choix d’accès pour la classe et le campus.

Une connexion sans fil stable prenant en charge le contenu vidéo et éducatif sans interruption est obligatoire. Les connexions sans fil instables créent un manque de concentration et affectent la progression de la classe.

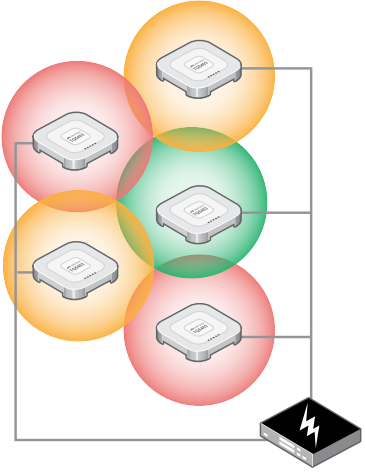
Le sans fil en classe est obligatoire, la disponibilité d’un réseau sans fil dans les bibliothèques, les zones de loisirs et les espaces extérieurs fait partie intégrante de l’ensemble du réseau éducatif.

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

Dans un réseau sans fil, la déconnexion du client et/ou une communication lente sont des signes typiques de problèmes techniques. Les principales raisons des problèmes sans fil sont les interférences entre les canaux radio, les sources sans fil externes non contrôlées par les informaticiens, le manque de puissance du signal du point d’accès (AP).

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





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

Pour plus d’informations, merci de visiter la page www.alliedtelesis.com/solutions/wifi

No Compromise Wi-Fi

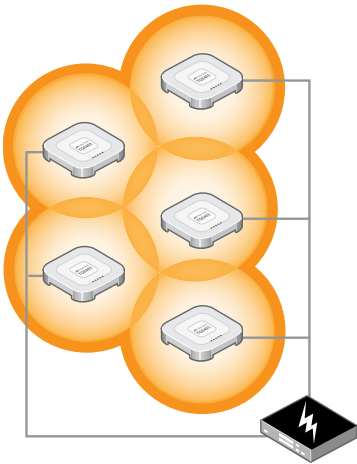
La solution No Compromise Wi-Fi d'Allied Telesis garantit des connexions Wi-Fi fiables et de hautes performances partout où elles sont nécessaires, minimisant le besoin d'intervention humaine.

En analysant les écarts de couverture du signal et les interférences des points d'accès Wi-Fi, Autonomous Wave Control (AWC) offre automatiquement une expérience sans fil de haute qualité. Vous gagnez du temps et profitez de coûts d'exploitation réduits.

Pour les environnements critiques, comme les grandes salles, AWC Channel Blanket (AWC-CB) permet de contrôler les points d'accès hybrides qui fournissent simultanément une connectivité Wi-Fi monocanal et multicanal.

Chaque fois qu'une extension de réseau est requise et qu'aucune connexion n'est disponible, AWC Smart Connect (AWC-SC) fournit une solution d'extension instantanée. Enregistrez simplement les points d'accès dans le système de gestion, branchez l'alimentation et le nouveau point d'accès est prêt à l'emploi.

AWC-CB

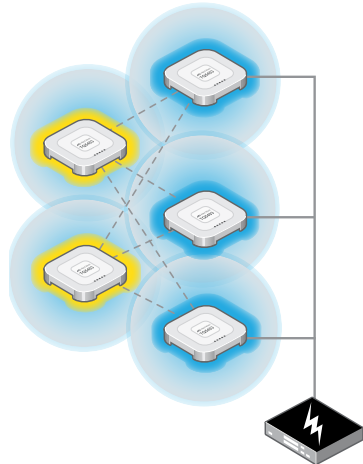


Allied Telesis AWC Channel Blanket (AWC-CB) est la solution monocanal pour les points d'accès sans fil Allied Telesis.

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

Associé à une approche multicanal traditionnelle, il fournit une solution d'accès sans fil complète pour tout environnement.

AWC-SC



Allied Telesis AWC Smart Connect (AWC-SC) est une extension de réseau sans fil sans effort, sans câbles supplémentaires. Enregistrez simplement le nouveau point d'accès, branchez le courant et il est prêt.

Réduisez le temps d'installation de 90% en fournissant un approvisionnement autonome pour la connectivité des événements ou l'expansion rapide du bureau 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 différents, chacun ayant des impacts différents 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 spécifique et d'attirer de nouveaux élèves.

Dans toute installation de vidéosurveillance, toutes les caméras et tous les systèmes de gestion vidéo reposent sur l'infrastructure réseau pour transporter la vidéo. Le trafic généré par les caméras de surveillance est quasi constant pendant la journée. Bien que ce trafic doive être planifié, une fois le réseau et la liaison dimensionnés, il ne pose généralement aucun problème de gestion.

L'installation est alimentée en POE (Power over Ethernet) avec une consommation électrique qui dépend de plusieurs facteurs tels que le type de caméra et les accessoires (chauffage, moteurs, etc.). Dans la phase de conception du réseau, les commutateurs d'accès connectés aux caméras IP doivent être en mesure de fournir suffisamment de puissance pour piloter toutes les caméras connectées.

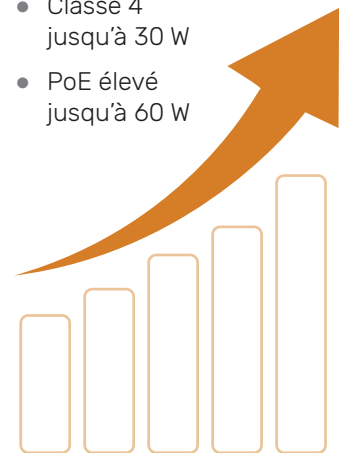
Apprentissage en ligne

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

Le trafic généré par ce type de vidéo est moins prévisible et si une classe entière est diffusée en même temps, des pics de trafic peuvent se produire. Pour être efficace, le service vidéo doit être disponible sans délai ni dégradation d'image. Tout problème peut provoquer une distraction et, par conséquent, une perte d'attention 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



Autres sources vidéo

Une autre source de trafic est le streaming vidéo à partir d'autres sources telles que YouTube, qui ne font souvent pas partie de l'offre éducative, mais qui sont toujours accessibles via le réseau scolaire.

Ce trafic est largement imprévisible et ne fait souvent pas partie des services scolaires, il doit donc être contrôlé pour éviter toute interruption des services hautement prioritaires. En règle générale, cela est obtenu en attribuant aux flux vidéo une faible priorité afin qu'ils puissent être rejetés en cas d'encombrement et qu'il y ait un trafic de priorité plus élevée à transmettre.

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



PROGRAMME EDUCATION/RECHERCHE ALLIED TELESIS



Progressions Ensemble

Informations

- Newsletters
- Webinars
- Livres Blancs et guides d'installations
- Catalogue dédié

Formations

- Atelier workshop une journée gratuite
- Formations certifiantes deux jours

Services

- Diagnostic réseau Gratuit
- Audit WIFI Gratuite
- Accompagnement projet, équipe technique spécialisée

Tests

- Prêt de matériel (POC)
- Try and Buy et solutions de Financement

Contact

Dominique Lidurin

Key Account Manager
Education France

Tel : 07 60 37 42 33

dominique_lidurin@alliedtelesis.com

N'attendez-pas, Inscrivez-vous dès maintenant <https://www.alliedtelesis.com/fr/contact>

A PROPOS D'ALLIED TELESIS

Depuis près de 30 ans, Allied Telesis offre une connectivité fiable et intelligente pour tout type d'environnement, des organisations d'entreprise aux projets d'infrastructure complexes et stratégiques 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 Allied Telesis, telles que Allied Telesis Autonomous Management Framework™ (AMF) et Enterprise SDN, garantissent une évolution du réseau, capable de suivre le rythme et fournir des solutions efficaces et sécurisées pour les personnes, les organisations et les «objets», à la fois aujourd'hui et dans le futur.

Allied Telesis est reconnu pour innover dans la manière dont les services et les applications sont fournis et gérés, ce qui se traduit par une valeur accrue et des coûts d'exploitation réduits.

Rendez-nous visite en ligne sur **alliedtelesis.com**.

