

Network Solutions Guide

ISTRUZIONE

Aule connesse. Campus connessi. Futuro connesso. Insegnanti e studenti fanno molto affidamento sulla tecnologia per aggiungere valore e migliorare l'esperienza educativa. Forniamo prestazioni di livello superiore per le aule e gli utenti mobili, proteggendo al contempo l'infrastruttura di rete e garantendo la protezione dei dati sensibili.

Esigenze e obiettivi delle reti per l'istruzione



Il settore dell'istruzione è all'inizio della sua trasformazione digitale ... i CIO stanno lavorando per affrontare la sfida dell'innovazione e della trasformazione.

Fonte: Ricerca Gartner, 2019

Le moderne reti per l'istruzione sono complesse e devono soddisfare una moltitudine di requisiti in rapido mutamento, alcuni di questi requisiti mettono in discussione la tecnologia e la sua sicurezza. Applicazioni Online, e-learning e metodi di insegnamento ricchi di contenuti multimediali forniscono immensi benefici per tutti gli operatori nel settore dell'istruzione.

Gli studenti più motivati con accesso a risorse di apprendimento avanzate, istruzione remota e opportunità online rappresentano la prossima generazione e hanno maggiori probabilità di ottenere risultati migliori.

Le scuole hanno la responsabilità ultima per la sicurezza dei loro alunni e delle loro reti e devono fornire un ambiente di lavoro efficiente, sicuro ed efficace che serva l'intera scuola - alunni, insegnanti, amministratori e tutti gli altri membri della comunità scolastica.





Quando si tratta di implementare le reti, gli operatori del settore dell'istruzione devono affrontare una serie di sfide. Devono fornire:



Accesso alla rete ad alta velocità sia per la rete cablata che wireless

Ogni classe deve supportare almeno 40 laptop/tablet wireless con accesso ad alta velocità per gli studenti e connessioni cablate per lavagne e proiettori. L'accesso Wi-Fi deve essere disponibile in tutto il campus, al chiuso e all'aperto.



Sicurezza Complessiva Della Rete

La sicurezza deve coprire diversi aspetti, tra cui: protezione dalla perdita di dati sensibili, disponibilità di risorse separate per studenti, insegnanti e amministrativi e protezione e correzione delle infezioni dei dispositivi.



Facilità Di Gestione

Gli amministratori di rete devono gestire facilmente i dispositivi cablati e wireless nel sito e da un centro operativo remoto. I problemi devono essere risolti rapidamente e i guasti devono essere riparati senza la necessità di risorse qualificate in loco, mantenendo bassi i costi.

Priorità Delle Reti Per l'Istruzione

Facilitare l'accesso alle informazioni e alle risorse, pur mantenendo la sicurezza dei dati riservati

Fornire un accesso sicuro alla rete al personale e agli studenti anche al di fuori dell'istituto

Proteggere i dati importanti dalle minacce di rete sia all'interno che all'esterno della rete locale

Sostenere e comprendere facilmente le nuove tecnologie sia quelle in uso che quelle che stanno per arrivare, minimizzando l'impatto sul budget

Essere facile da configurare, gestire e veloce nel risolvere i problemi, riducendo al minimo i costi amministrativi e i tempi di inattività

Per ulteriori informazioni, visitare www.alliedtelesis.com/solutions/industry/education

Allied Telesis Soluzioni per l'istruzione

Allied Telesis è un leader del settore nelle soluzioni di networking.

Con la nostra comprovata storia di fornitore di soluzioni di rete avanzate altamente affidabili e ricche di funzionalità, sempre più operatori nel settore dell'istruzione si rivolgono a Allied Telesis per raggiungere i loro obiettivi.

In Allied Telesis, comprendiamo la necessità di fornire servizi di rete avanzati all'avanguardia pronti per le generazioni future, con budget limitati. Allied Telesis ha implementato reti per l'istruzione all'avanguardia per molti anni. Il nostro portafoglio di prodotti ad alto valore aggiunto offre la sicurezza, la mobilità e le prestazioni di cui ogni rete ha bisogno, sia ora che in futuro.

Diamo un'occhiata a come Allied Telesis risponde alle sfide presenti nel settore dell'istruzione e fornisce soluzioni che facilitano opportunità didattiche avanzate.

Guardando al futuro

I prodotti Allied Telesis ottimizzano gli investimenti tecnologici integrandosi completamente con i sistemi e le applicazioni esistenti. Man mano che l'istruzione cambia, la rete può adattarsi facilmente, perché i nostri prodotti forniscono un'infrastruttura altamente efficiente e scalabile, progettata per soddisfare tutte le esigenze.

Mentre nuove idee creative sono implementate nel campo della didattica, i prodotti Allied Telesis rimangono in prima linea, per fornire infrastrutture di rete che incoraggiano la creatività, e influenzano positivamente la prossima generazione.



Controllo Di Accesso Alla Rete

Assicura che il personale e gli studenti abbiano accesso costante alle risorse appropriate, pur proteggendo le informazioni riservate e mantenendo la privacy.



La Rete Self-Defending

La nostra soluzione di smart edge security protegge le reti cablate e wireless dalle minacce interne mettendo automaticamente in quarantena i dispositivi sospetti, creando così un ambiente sicuro per studenti ed insegnanti.



Gestione Della Rete Semplificata

Automatizza la gestione della rete utilizzando un unico strumento intelligente di facile utilizzo che aggiunge visibilità e sicurezza e riduce i rischi e i costi di supporto.



Wi-Fi senza compromessi

Garantisce connessioni Wi-Fi affidabili e ad alte prestazioni ovunque siano necessarie. Con un supporto per installazioni con un'alta densità di dispositivi interni ed esterni offrono un'unica soluzione per aule, biblioteche, palestre, aree di ritrovo e ricreative.



Videosorveglianza Digitale

Un portafoglio di prodotti dedicato trasporta in modo sicuro e affidabile le riprese video attraverso la tua rete IP.





CONTROLLO DI ACCESSO ALLA RETE

Assicurare al personale e gli studenti accesso costante alle risorse appropriate considerando i diritti di accesso a livello di architettura di rete.

Fornire agli individui un accesso appropriato alle risorse di rete e creare un ambiente pronto per la gestione degli esami in maniera digitale può sembrare complesso, richiedendo più gruppi di livelli di accesso delle risorse per mantenere la riservatezza e la privacy delle informazioni.

Gli operatori del settore dell'istruzione gestiscono informazioni critiche su studenti e curriculum, che devono essere private e protette da utilizzi dannosi. Una politica sui diritti di accesso deve garantire che solo le persone e i dispositivi appropriati possano accedere a queste informazioni riservate.

I prodotti Allied Telesis supportano il Network Access Control (NAC), un approccio all'avanguardia per fornire un controllo completo sull'accesso degli utenti alla rete. Gli utenti possono avere diversi livelli di accesso, consentendo la corretta disponibilità di rete e risorse per studenti, insegnanti e personale amministrativo. NAC verifica inoltre l'aderenza dei dispositivi alle politiche di sicurezza della rete prima di concedere l'accesso alla rete, arrestando in modo proattivo le minacce prima che possano entrare nella rete.

NAC ha introdotto il controllo basato sull'identità, che è superiore ai precedenti metodi di controllo dell'accesso alle informazioni online. La natura automatizzata di NAC è di reale beneficio per il personale IT, in quanto semplifica le complesse attività di amministrazione.

Molti fornitori di soluzioni di reti hanno implementato funzionalità NAC e i prodotti Allied Telesis supportano molte di queste implementazioni, tra le altre le soluzioni di Microsoft, Symantec e Sophos. I prodotti Allied Telesis sono stati ampiamente testati per la conformità con i più diffusi prodotti NAC e abbiamo pubblicato comode guide passo-passo per implementare una soluzione completa. I prodotti e le competenze di Allied Telesis consentono soluzioni NAC robuste con il minimo sforzo.

Servizi Integrati

Gli switch Allied Telesis semplificano l'amministrazione integrando diversi servizi di rete quali:

- RADIUS server interno per controllare l'identità degli utenti e per mantenere la rete sicura e libera da intrusi
- Storm control garantisce una rete solida e resiliente gestendo la quantità di traffico consentita sulla rete e affrontando eventuali picchi imprevisti
- Il server DHCP interno automatizza la distribuzione degli indirizzi di rete a ogni computer
- Un timekeeper centralizzato garantisce che la rete funzioni sempre in piena sincronicità
- Loop Protection, contro accidentali errori di cablaggio

Per ulteriori informazioni, visitare www.alliedtelesis.com/solutions/total-autonomous-networking

La centralizzazione dell'amministrazione di rete riduce notevolmente la necessità di esperti IT, aumentando al contempo sicurezza e robustezza.

L'approccio Allied Telesis al controllo dell'accesso alla rete

NAC consente un controllo senza precedenti sull'accesso degli utenti alla rete, al fine di mitigare le minacce all'infrastruttura di rete. Gli switch Allied Telesis utilizzano l'autenticazione basata su porta IEEE 802.1x in collaborazione con l'assegnazione VLAN dinamica, per valutare l'aderenza di un utente alle politiche di sicurezza della rete e concedere l'autenticazione o offrire un piano di soluzione dei problemi.

Inoltre, se più utenti condividono una porta, è possibile utilizzare l'autenticazione multipla. Utenti diversi sulla stessa porta possono essere assegnati a diverse VLAN, e così dare diversi livelli di accesso alla rete. Inoltre, può essere configurata una VLAN guest per fornire un accesso per gli utenti che non sono autenticati.





LA RETE SELF-DEFENDING

Le istituzioni educative stanno diventando sempre più un bersaglio per i criminali informatici. Le connessioni sicure alle risorse online e a Internet che proteggono sia la rete che gli studenti da materiale inappropriato e minacce dannose, sono fondamentali per qualsiasi istituto o scuola.

I tradizionali modelli di sicurezza che si concentrano sulla prevenzione degli attacchi che arrivano dall'esterno della rete locale non forniscono più una protezione sufficiente, poiché gli attacchi possono facilmente provenire dall'interno della rete tramite un laptop, un tablet o qualsiasi dispositivo IoT infetto collegato alla rete di accesso cablata o wireless.

Parallelamente, gli attacchi sono aumentati in termini di sofisticazione e le minacce ora si presentano in così tante forme che mantenere una rete sicura ma efficace è diventata una sfida costosa e dispendiosa in termini di tempo.

L'approccio tradizionale basato su firewall può rilevare e bloccare la maggior parte delle minacce e dei virus provenienti da Internet, ma mostra alcune limitazioni una volta che l'attacco proviene dall'interno della rete. In questa fase, l'attacco si diffonderà est/ovest sulla rete (cioè da un dispositivo connesso a un altro), e può essere rilevato dal firewall solo una volta che la minaccia tenta di attraversare il confine con internet. Una volta rilevata la minaccia, un amministratore di rete viene avvisato e può iniziare la fase di risoluzione del problema.

Sfortunatamente, il processo di bonifica spesso dipende dalle risorse IT disponibili, con tempi di reazione che vanno da alcuni minuti, ad ore o addirittura giorni, a seconda della disponibilità della risorsa con adeguata competenza.

La cybersecurity continua ad essere un priorità assoluta per i CIO nel settore dell'istruzione.

Fonte: Agenda CIO 2020 di Gartner sull'istruzione

119

Almeno 119 scuole negli Stati Uniti hanno subito 122 attacchi informatici nel 2018, tra cui violazioni dei dati, truffe di phishing e attacchi ransomware.

*Fonte: K-12 Cybersecurity
Altre Risorse*

Per ulteriori informazioni, visitare www.alliedtelesis.com/solutions/self-defending-networks

Il Controller AMF-Sec Allied Telesis è il cuore della nostra soluzione di sicurezza e gestione della rete all'avanguardia. Fornisce esattamente ciò di cui gli istituti e le scuole hanno bisogno: costi di gestione ridotti, maggiore sicurezza e una migliore esperienza dell'Utente finale.

Caratteristiche Principali:

- Compatibile con OpenFlow v1. 3
- Adatto sia per reti cablate che wireless
- Si integra con le applicazioni aziendali per risparmiare tempo e denaro
- Si integra con i prodotti di sicurezza per fornire una risposta immediata alle minacce
- Isola in modo intelligente e automatico i dispositivi sospetti
- Scalabile: si possono aggiungere più applicazioni aziendali per un risultato migliore
- Si integra con i nostri strumenti di gestione della rete per una maggiore facilità d'uso

La Rete Self-Defending

La soluzione di rete Self-Defending fornisce un approccio integrato alla sicurezza della rete, automatizzando le Operazioni IT manuali e proteggendo dalle minacce provenienti sia da dispositivi di accesso cablati che wireless.

Utilizzando il motore di sicurezza AMF-Sec, che non richiede l'installazione di software sugli endpoint, la nostra soluzione risponde automaticamente alle minacce identificate.

Firewall e appliance di sicurezza identificano le minacce, quindi il motore intelligente che implementa la tecnologia Isolation Adapter integrata in AMF-Sec risponde immediatamente per isolare la parte interessata della rete e mettere in quarantena il dispositivo sospetto. La correzione può essere applicata in modo che il dispositivo possa riconnettersi alla rete con interruzioni minime. Le risposte automatizzate sono configurabili e la registrazione completa fornisce una traccia chiara.

Il Controller AMF-Sec è la chiave della nostra soluzione di sicurezza AMF innovativa e pluripremiata, consentendo reti Self-Defending che aiutano le aziende a evitare perdite di tempo e interruzioni inutili dei servizi di rete.





GESTIONE DELLA RETE SEMPLIFICATA



L'aumento della complessità della rete aumenta in modo significativo le richieste di gestione della rete e di risorse specializzate. L'implementazione di soluzioni di automazione rende la vita più semplice e la soluzione più conveniente.

Vista Manager EX ha un approccio single pane-of-glass ed è basata su plugin per la gestione della rete. Ha una dashboard che mostra i dettagli della rete, lo stato e gli eventi su una mappa topologica e mette in evidenza i problemi critici per ridurre al minimo i tempi di reazione e aiutare a risolvere i problemi in modo tempestivo.

Una serie di plugin per controllare la rete cablata, i dispositivi wireless, il collegamento WAN e gli strumenti di automazione rendono la gestione facile e la soluzione modulare.

Autonomous Management Framework (AMF) - plugin

Riduci i costi operativi della rete con l'intelligenza e l'automazione aggiuntive date dalla gestione centralizzata. Servizi automatizzati, inclusi aggiornamenti firmware, backup, ripristino e provisioning zero-touch sono solo alcune delle funzionalità AMF per ridurre al minimo le risorse necessarie per gestire una rete complessa.

Autonomous Wave Control (AWC) - plugin

Analizza e ottimizza le prestazioni di reti wireless complesse. Installa e dimentica la tua rete wireless con uno strumento autonomo che analizza i modelli di traffico e configura automaticamente gli AP per soddisfare le richieste.

“Carenze di finanziamento e alti costi operativi sono le principali preoccupazioni per scuole, campus e università.”

*Fonte: K-12 Cybersecurity
Altre Risorse*

Per ulteriori informazioni, visitare www.alliedtelesis.com/solutions/total-autonomous-networking



Allied Telesis Autonomous Management Framework™ (AMF) è una piattaforma di gestione della rete scalabile.

Supporta switch Allied Telesis, firewall, e prodotti wireless, così come una vasta gamma di dispositivi di terze parti - tra cui telecamere di videosorveglianza e telefoni IP - per una automazione di rete veramente inclusiva.

Software Defined WAN (SD-WAN) - plugin

Gestisce centralmente e ottimizza automaticamente il traffico tra le sedi. Gestire connessioni multiple con prestazioni e costi diversi richiede un'attenzione continua. Il nostro orchestratore SD-WAN gestisce centralmente le connessioni delle filiali per una distribuzione affidabile e sicura del traffico. Imposta metriche di prestazioni accettabili, ottimizza e bilancia automaticamente la distribuzione del traffico e monitora le prestazioni della WAN.

Simple Network Management Protocol (SNMP) - plugin

Il plugin SNMP all'interno di Vista Manager EX trova automaticamente e gestisce una vasta gamma di dispositivi in un ambiente multi-vendor. Diverse visualizzazioni della rete consentono la visibilità nel modo desiderato. Estendere il monitoraggio della rete con notifiche e avvisi automatizzati per una gestione proattiva.

AT-VISTA MANAGER™ EX

Vista Manager EX offre un monitoraggio all'avanguardia e crea automaticamente una mappa topologica completa di switch, firewall e AP wireless.

La mappatura e la creazione di VLAN tra dispositivi, oltre al monitoraggio del traffico e alla mappatura WAN, forniscono una gestione semplice di molti o tutti i dispositivi di rete contemporaneamente.

Vista Manager Mini è integrato negli switch e router Allied Telesis per consentire una gestione della rete facile e veloce in installazioni di piccole e medie dimensioni. Fornisce accesso immediato alla potenza di AMF e AWC per la gestione della rete cablata e wireless.





WI-FI SENZA COMPROMESSI

Il wireless oggi è la prima tecnologia di accesso all'interno delle reti per l'istruzione. Consente a studenti, insegnanti e membri del personale di accedere alla rete da qualsiasi luogo in qualsiasi momento ed è il metodo di accesso principale per istituti e scuole.

Una connessione wireless stabile che supporti video e contenuti educativi senza interruzioni è fondamentale. Le connessioni wireless instabili distruggono e influenzano il progresso di apprendimento della classe.

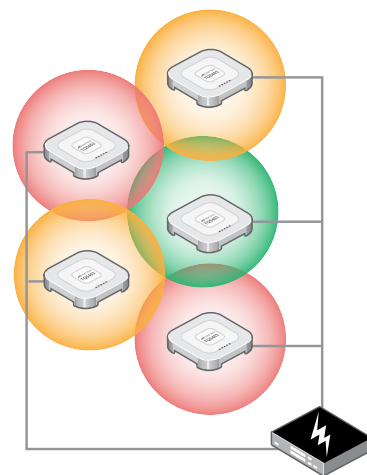
Il wireless nelle classi è necessario, e la disponibilità wireless nelle biblioteche, nelle aree ricreative e negli spazi esterni è diventata parte integrante dell'intera rete.

Nonostante l'evoluzione dello standard wireless che migliora le prestazioni complessive, ci sono ancora limitazioni tecniche che richiedono un tecnico esperto per implementare una rete wireless stabile.

In una rete wireless, la disconnessione del client e/o la comunicazione lenta sono segni tipici di problemi tecnici. Le ragioni principali dei problemi wireless sono le interferenze tra i canali radio, le sorgenti wireless esterne non sotto il controllo IT e la mancanza di potenza del segnale dell'access point.

In un ambiente dinamico come un edificio scolastico o un campus, c'è la necessità di un monitoraggio continuo della rete e di risorse IT qualificate per mantenere l'installazione sotto controllo e fornire un prezioso servizio wireless.

AWC[™]



Allied Telesis Autonomous Wave Control (AWC) è una tecnologia di rete avanzata che utilizza l'intelligenza artificiale (AI) per offrire miglioramenti significativi nella connettività e nelle prestazioni della rete wireless riducendo al contempo i costi di implementazione e operativi.

Per ulteriori informazioni, visitare www.alliedtelesis.com/solutions/wifi

Wi-Fi senza compromessi

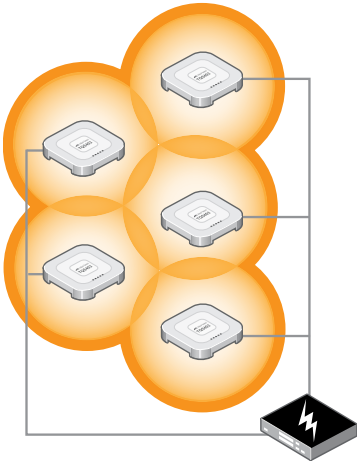
La soluzione Wi-Fi Allied Telesis senza compromessi garantisce connessioni Wi-Fi affidabili e ad alte prestazioni ovunque siano necessarie, riducendo al minimo la necessità di un intervento umano.

Analizzando le lacune di copertura del segnale e le interferenze del punto di accesso Wi-Fi, Autonomous Wave Control (AWC) offre automaticamente un'esperienza wireless di alta qualità. Riduce la dipendenza da tecnici di rete qualificati e garantisce costi operativi inferiori.

Per gli ambienti critici, come le grandi sale, AWC Channel Blanket (AWC-CB) consente il controllo di AP ibridi che forniscono contemporaneamente connettività Wi-Fi a canale singolo e multicanale.

Ogni volta che è richiesta un'espansione di rete e non sono disponibili cavi, AWC Smart Connect (AWC-SC) fornisce una soluzione di espansione a tempo zero. Basta registrare gli AP nel sistema di gestione, collegare l'alimentazione e il nuovo AP è pronto per l'uso.

AWC-CB

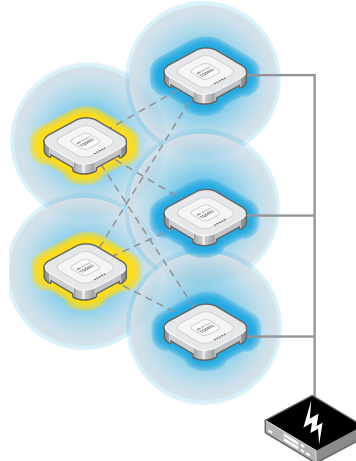


Allied Telesis AWC Channel Blanket (AWC-CB) è la soluzione a canale singolo per AP wireless Allied Telesis.

Tutti gli AP sono membri dello stesso blanket e operano sullo stesso canale. AWC-CB è un controller intelligente che gestisce le interferenze e l'accesso dei client.

Insieme a un approccio multicanale tradizionale, fornisce una soluzione di accesso wireless completa per qualsiasi ambiente.

AWC-SC



Allied Telesis AWC Smart Connect (AWC-SC) fornisce un'espansione di rete wireless senza sforzo e senza fili aggiunti. Basta registrare il nuovo AP, collegare l'alimentazione ed è pronto.

Riduci i tempi di installazione del 90% fornendo un provisioning autonomo per la connettività in occasione di eventi o una rapida espansione dell'ufficio senza la necessità di nuovi cavi.



VIDEOSORVEGLIANZA DIGITALE



In qualsiasi rete moderna, gran parte della larghezza di banda utilizzata è composta da flussi video. All'interno di una scuola, un campus o un'università, ci sono principalmente due diversi tipi di flussi video, con impatti diversi sulle prestazioni della rete.

Video IP per la sicurezza

La sicurezza e la protezione degli studenti nella scuola fanno parte dell'intera offerta educativa. La capacità di sorveglianza è uno dei modi per aumentare la fiducia della famiglia e degli studenti in una scuola e per attirare nuovi studenti.

In qualsiasi implementazione di videosorveglianza, tutte le telecamere e i sistemi di gestione video si basano sull'infrastruttura di rete per il trasporto di video. Il traffico generato dalle telecamere di sorveglianza è quasi costante durante il giorno. Anche se questo traffico deve essere considerato in fase di progetto, una volta che la rete e il collegamento sono dimensionati, di solito non causa problemi di gestione.

La parte fondamentale dell'installazione è alimentata da Power over Ethernet (PoE) con un consumo energetico che dipende da molteplici fattori come il tipo di telecamera e gli accessori (riscaldatore, motori, ecc.). Nella fase di progettazione della rete, gli switch di accesso collegati alle telecamere IP devono essere in grado di fornire energia sufficiente per pilotare tutte le telecamere collegate.

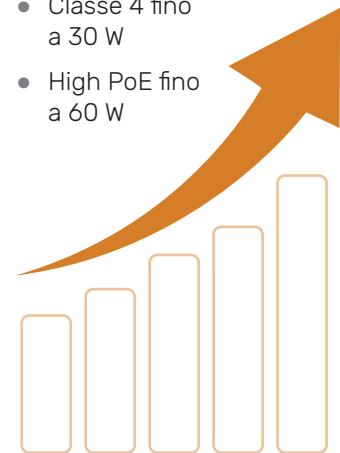
Apprendimento Online

Il Video è anche ampiamente utilizzato per le lezioni, l'apprendimento a distanza e come risorsa per gli studenti al di fuori dell'orario scolastico.

Il traffico generato da questo tipo di video è meno prevedibile, e se un'intera classe è in streaming allo stesso tempo, picchi di traffico possono verificarsi. Per essere efficace, il servizio video deve essere disponibile senza ritardi o degrado dell'immagine. Eventuali problemi possono causare distrazione e di conseguenza una perdita di attenzione degli studenti. La progettazione della rete deve essere in grado di assorbire i picchi di traffico senza influenzare altri utenti o risorse.

Classi PoE

- Classe 0 fino a 15 W
- Classe 1 fino a 4 W
- Classe 2 fino a 7 W
- Classe 3 fino a 15 W
- Classe 4 fino a 30 W
- High PoE fino a 60 W



Per ulteriori informazioni, visitare www.alliedtelesis.com/solutions/surveillance

Altre Sorgenti Video

Un'altra fonte di traffico è lo streaming video da altre fonti come YouTube, che spesso non fanno parte dell'offerta educativa, ma sono accessibili utilizzando la rete scolastica.

Questo traffico è in gran parte imprevedibile e spesso non fa parte dei servizi scolastici, quindi deve essere controllato per evitare interruzioni ai servizi ad alta priorità. In genere, ciò si ottiene assegnando ai flussi video una priorità bassa in modo che possano essere scartati se si verifica una congestione o c'è traffico con priorità più elevata da trasmettere.

Adeguate larghezza di banda, dimensionamento corretto dei collegamenti e gestione delle priorità sono gli elementi chiave per una distribuzione video affidabile e fluida, per la migliore esperienza utente e i migliori risultati di apprendimento.

A PROPOSITO DI ALLIED TELESIS

Per più di 30 anni, Allied Telesis ha fornito connettività affidabile e intelligente per ogni mercato, dalle aziende a progetti di infrastrutture complesse e critiche in tutto il mondo.

In un mondo che si muove verso le smart city e l'internet delle cose, le reti devono evolversi rapidamente per affrontare nuove sfide. Allied Telesis Smart technologies, così come Allied Telesis Autonomous Management Framework™ (AMF) e Enterprise SDN, assicurano che l'evoluzione della rete possa tenere il passo e fornire soluzioni efficienti e sicure per persone, aziende e "cose", sia ora che nel futuro.

Allied Telesis è riconosciuta per aver innovato il modo in cui i servizi e le applicazioni vengono erogati e gestiti, con conseguente aumento del valore e minori costi operativi.

Venite a trovarci online all'indirizzo **alliedtelesis.com**.

