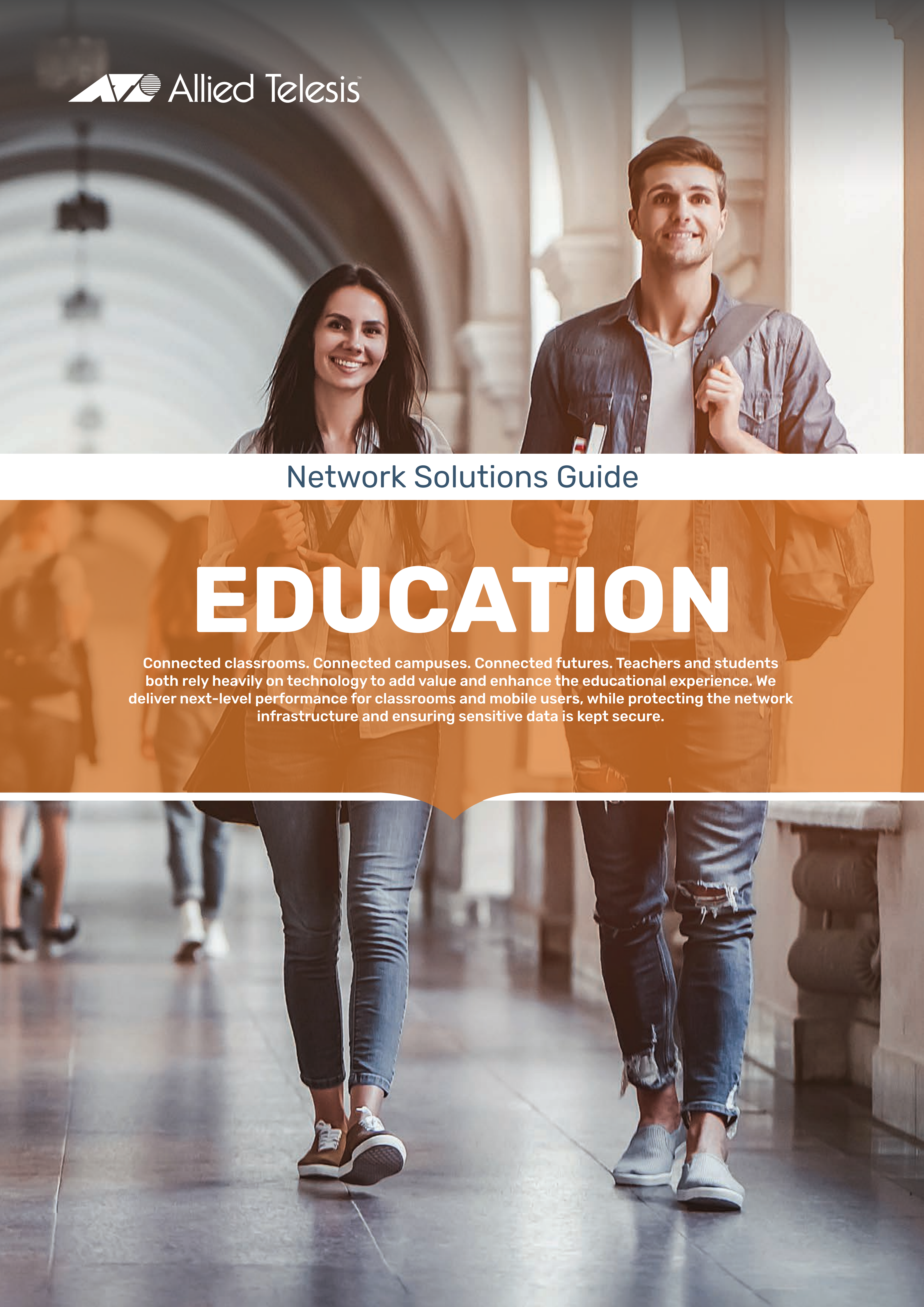


Allied Telesis

Network Solutions Guide

EDUCATION

Connected classrooms. Connected campuses. Connected futures. Teachers and students both rely heavily on technology to add value and enhance the educational experience. We deliver next-level performance for classrooms and mobile users, while protecting the network infrastructure and ensuring sensitive data is kept secure.

Education Network Needs and Objectives

> The education sector is at a very early stage of its digital journey … CIOs are struggling to meet the innovation and transformation challenge.

Source: Gartner Research, 2019

Modern education networks are complex and serve a rapidly developing set of requirements, some of which challenge the technology and its security. Online applications, e-learning and media-rich teaching methods provide immense benefits to the education providers.

Motivated students with access to advanced learning resources, remote schooling and online opportunities are part of the next generation in education and are more likely to achieve better results.

Schools hold the ultimate responsibility for the security of their pupils and networks, and must provide an efficient, safe and effective computing environment which serves the entire school—pupils, teachers, administrators and all the other members of the school community.

When it comes to implementing networks, education providers face a number of challenges. They must provide:

High Speed Wired and Wireless Access

Each classroom must support at least 40 wireless laptop/tablets with high speed access for students and wired connections for blackboards and projectors. Wi-Fi must be available across the campus, indoor and outdoor.

Overall Network Security

Security must cover different concerns, including: sensitive data leakage protection, separate student, teacher and administrative resource availability, and endpoint infection protection and remediation.

Easy Network Management

Network administrators must easily manage wired and wireless devices on-premise and from a remote operations center. Issues can be resolved quickly and failures can be repaired without the need for skilled resources onsite, keeping costs down.

Education Network Priorities

- Facilitate access to information and resources, yet maintain the security of confidential data
- Provide secure network access to offsite staff and students
- Protect your valuable data from network threats both inside and outside of your network
- Support and easily encompass new technologies both now, and as they arrive—without breaking the budget
- Be easy to configure, manage, and troubleshoot, minimizing costly administration and downtime

For further information, please visit www.alliedtelesis.com/solutions/industry/education

Allied Telesis Solution for Education

Allied Telesis is an industry leader in networking solutions.

With our proven history of delivering highly reliable and feature-rich advanced network solutions, more and more education providers are turning to Allied Telesis to achieve their objectives.

At Allied Telesis, we understand the need to supply advanced cutting-edge network services to tomorrow's generation, within limited budgets. Allied Telesis has been implementing leading-edge educational networks for many years. Our advanced high value product portfolio provides the security, mobility and high performance you need for your education network, both now and well into the future.

Let's look at how Allied Telesis meets the challenges faced in education, and provides solutions that facilitate advanced educational opportunities.

Looking to the Future

Allied Telesis products optimize your technology investments by fully integrating with existing systems and applications. As education needs change, your network can easily adapt, because our products provide highly efficient and progressive infrastructure, designed to fulfil your needs.

As new and exciting ideas are implemented in the provision of education, Allied Telesis products remain at the forefront, by providing network infrastructure that encourages creativity, and positively influences the next generation.

Network Access Control

Ensure that your staff and students have constant access to appropriate resources, while still protecting confidential information and maintaining privacy.

The Self-Defending Network

Our smart edge security protects your wired and wireless networks from internal threats by automatically quarantining suspect devices, thus creating a safe environment for students and educators.

Network Management Made Easy

Automate your network management using a single easy-to-use intelligent tool that adds visibility and security, and lowers risks and support costs.

No Compromise Wi-Fi

Ensure reliable, high-performance Wi-Fi connections everywhere they are needed. With high device density support, indoor and outdoor-rated devices provide a single solution for classroom, libraries, gathering and recreational areas.

Digital Video Security

A dedicated product portfolio securely and reliably transports video footage across your IP network.

NETWORK ACCESS CONTROL

Ensure that your staff and students have constant access to appropriate resources by considering access rights at the network architecture level.

Providing individuals with appropriate access to network resources and creating an environment that is ready for digital assessment can seem complex, requiring multiple sets of resource privilege levels to maintain information confidentiality and privacy.

Education providers maintain critical student and curriculum information, which must be kept private and protected from malicious use. An access rights policy must ensure that only the appropriate people and devices can access this confidential information.

Allied Telesis products support Network Access Control (NAC), a leading approach to providing complete control over user access to the network. Users can have different levels of access, allowing for the correct network and resource availability for students, teachers and administration staff. NAC also checks device adherence to network security policies before granting network access, proactively stopping threats before they can enter the network.

NAC has introduced identity-based networking, which is superior to previous methods of controlling online information access. NAC's automated nature is of real benefit for busy IT staff, as it simplifies complex administration tasks.

Many leading network vendors have implemented NAC solutions, and Allied Telesis advanced switching products support a number of these, including solutions from Microsoft, Symantec and Sophos. Allied Telesis products have been extensively tested for compliance with popular NAC products, and we have published convenient step-by-step guides to implementing a comprehensive solution. Allied Telesis products and expertise enable robust NAC solutions with minimum effort.

Integrated Services

Allied Telesis switches simplify administration by integrating several network services:

- Internal RADIUS server checks the identity of users to keep the network safe and free from intruders
- Storm control ensures a robust and resilient network by managing the amount of traffic allowed on the network, and dealing with any unexpected surges
- Internal DHCP server automates the distribution of network addresses to every computer
- A centralized timekeeper ensures your network is always working in full synchronicity
- Loop protection guards against accidental wiring mistakes

For further information, please visit www.alliedtelesis.com/solutions/total-autonomous-networking

Centralizing network administration greatly reduces the need for full time IT experts, while increasing security and robustness.

Source: Gartner Research, 2019

Allied Telesis Approach to Network Access Control

NAC allows for unprecedented control over user access to the network, in order to mitigate threats to network infrastructure. Allied Telesis switches use IEEE 802.1x port-based authentication in partnership with standards-compliant dynamic VLAN assignment, to assess a user's adherence to network security policies and either grant authentication or offer remediation.

Furthermore, if multiple users share a port then multi-authentication can be used. Different users on the same port can be assigned into different VLANs, and so given different levels of network access. Additionally, a Guest VLAN can be configured to provide a catch-all for users who aren't authenticated.

THE SELF-DEFENDING NETWORK

Education organizations are increasingly becoming a target for cyber criminals. Secure connections to online resources and the Internet, protecting both the network and students from inappropriate material and malicious threats, are now mandatory for any education institute.

The traditional security models that focus on preventing attacks from getting inside the network no longer provide enough protection, since attacks can easily come from inside the network via an infected laptop, tablet or any IoT device directly connected on the wired or wireless access network.

In parallel, attackers have increased in sophistication, and threats now come in so many forms that maintaining a secure yet effective network has become a time-consuming and costly challenge.

While the traditional firewall-based approach can detect and block most threats and viruses coming from the Internet, it shows limitations once the attack comes from inside the network. At this stage, the attack will spread east/west on the network (I.e., from one connected device to another), where it can be detected by the firewall only once the threat tries to cross the border to the internet. Once the threat is detected an administrator can be alerted and remediation can begin.

Unfortunately, the remediation process often depends on human resources, with reaction times ranging from minutes, hours or even days, depending on resource availability and skills.

Cybersecurity continues to be a top priority for education CIOs.

Source: Gartner 2020 CIO Agenda on Education

119

schools at least in the USA experienced 122 cyberattacks in 2018, including data breaches, phishing scams and ransomware attacks.

Source: K-12 Cybersecurity Resource Center

For further information, please visit www.alliedtelesis.com/solutions/self-defending-networks

AMF-Sec

The Allied Telesis AMF-Sec Controller enables our state-of-the-art network management and security solution. It provides exactly what education organizations need: reduced management costs, increased security and an improved end-user experience.

Key Features:

- OpenFlow v1.3 compatible
- Suitable for both wired and wireless networks
- Integrates with business apps to save time and money
- Integrates with security products to provide instant threat response
- Intelligently and automatically isolates suspect devices
- Scalable—add more business apps for greater value
- Integrates with our network management tools for greater ease of use

The Self-Defending Network

The Self-Defending Network solution provides an integrated approach to network security, automating manual IT operations and protecting from threats coming both from wired and wireless access devices.

By utilizing the AMF-Sec security engine, which does not require endpoint agents or software, our solution automatically responds to identified threats.

Firewall and security appliances identify threats, then the intelligent engine implementing the Isolation Adapter technology built into AMF-Sec responds immediately to isolate the affected part of the network and quarantine the suspect device. Remediation can be applied so the device can rejoin the network with minimal disruption. Automated responses are configurable, and comprehensive logging provides a clear audit trail.

The AMF-Sec Controller is key to our innovative and award-winning AMF Security solution, enabling Self-Defending Networks that help organizations avoid lost time and unnecessary disruption to network services.

NETWORK MANAGEMENT MADE EASY

Increasing education network complexity significantly increases demands on network management and specialized resources. Implementing automation solutions makes life simpler and more affordable.

Vista Manager EX is a plugin-based single pane-of-glass approach to network management. It has a dashboard showing network details, status and events on a topology map, and it highlights critical issues to minimize reaction time and help resolve problems in a timely manner.

A series of plugins to control the wired network, wireless devices, the WAN link and automation tools make networking easy and the solution modular.

Allied Telesis Autonomous Management Framework™ Plus (AMF Plus)

Reduce network operating costs with the added intelligence and automation of centralized management. Automated services including firmware upgrades, backup, recovery and zero-touch provisioning are only some of the AMF Plus features to minimize the resources required to manage a complex education network.

Autonomous Wave Control (AWC) - plugin

Analyze and optimize the performance of complex wireless networks. Install and forget your wireless network with an autonomous tool that analyzes traffic patterns and automatically configures APs to meet demand.

> "Funding shortfalls and operational costs are top concerns for education organizations."
>
> *Source: K-12 Cybersecurity Resource Center*

For further information, please visit www.alliedtelesis.com/solutions/total-autonomous-networking

AMF PLUS

Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) is a scalable network management platform.

It supports Allied Telesis switching, firewall, and wireless products, as well as a wide range of third-party devices—including video surveillance cameras and IP phones—for truly inclusive network automation.

VISTA MANAGER™

Vista Manager EX delivers state-of-the-art monitoring and automatically creates a complete topology map of switches, firewalls and wireless APs.

VLAN mapping and creation between devices, plus traffic monitoring and WAN mapping, provide effortless management of many, or all, network devices at once.

Vista Manager Mini is embedded in our core Allied Telesis switches and router to enable fast and easy network management for small and medium installations. It provides immediate access to the power of AMF Plus and AWC for wired and wireless management.

Software Defined WAN (SD-WAN)

Centrally manage and automatically optimize inter-branch traffic. Having multiple connections with different performances and cost requires continuous attention. Our SD-WAN orchestrator centrally manages branch office connections for reliable and secure application delivery. Set acceptable performance metrics, automatically optimize and load-balance application delivery, and easily monitor WAN performance.

Simple Network Management Protocol (SNMP) - plugin

Auto-discover and manage a wide range of devices in a multi-vendor environment within Vista Manager EX with the SNMP plugin. Different network views enable visibility the way you prefer. Extend network monitoring with automated notifications and alerts for proactive management.

NO COMPROMISE WI-FI

Wireless today is the first access technology in the educational market. It allows students, teachers and staff members to access the network from any place at any time as the main access choice for class and campus.

A stable wireless connection supporting video and educational content without interruption is mandatory. Unstable wireless connections create lack of focus and affect class progress.

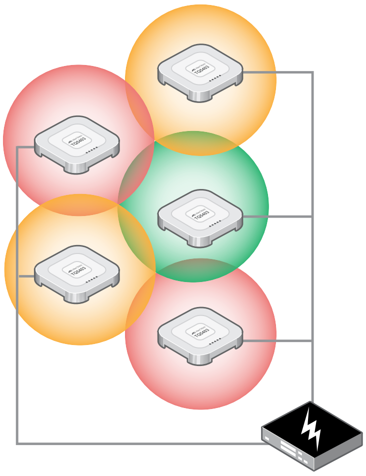
As wireless in class is mandatory, wireless availability in libraries, recreational areas and outdoor spaces is an integral part of the whole education network.

Despite the wireless standard evolution that improves overall performance, there are still technical limitations that mean a skilled technician is required to implement a stable wireless network.

In a wireless network, client disconnection and/or slow communication are typical signs of technical problems. The main reasons for wireless problems are interference between radio channels, external wireless sources not under IT control, and a lack of Access Point (AP) signal strength.

In a dynamic environment like a school building or campus, there is the need for continuous network monitoring and skilled IT resources to maintain the installation under control and provide a valuable wireless service.

AWC



Allied Telesis Autonomous Wave Control (AWC) is an advanced network technology that utilizes Artificial Intelligence (AI) to deliver significant improvements in wireless network connectivity and performance while reducing deployment and operating costs.

For further information, please visit www.alliedtelesis.com/solutions/wifi

No Compromise Wi-Fi

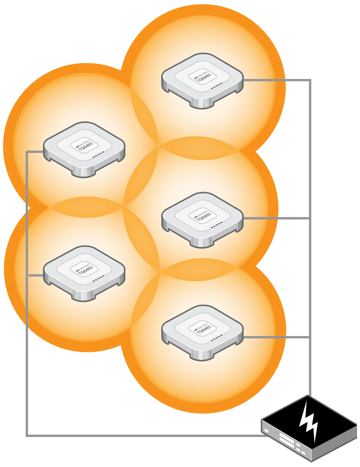
The Allied Telesis No Compromise Wi-Fi solution ensures reliable, high-performance Wi-Fi connections everywhere they are needed, minimizing the need for human intervention.

By analyzing signal coverage gaps and Wi-Fi access point interference, Autonomous Wave Control (AWC) automatically delivers a high-quality wireless experience. Reduce your dependency on skilled network engineers and enjoy lower operating costs.

For critical environments, like great halls, AWC Channel Blanket (AWC-CB) enables control of hybrid APs that simultaneously provide single and multi-channel Wi-Fi connectivity.

Every time a network expansion is required and no wires are available, AWC Smart Connect (AWC-SC) provides a zero-time expansion solution. Just register the APs in the management system, plug in the power and the new AP is ready for use.

AWC-CB

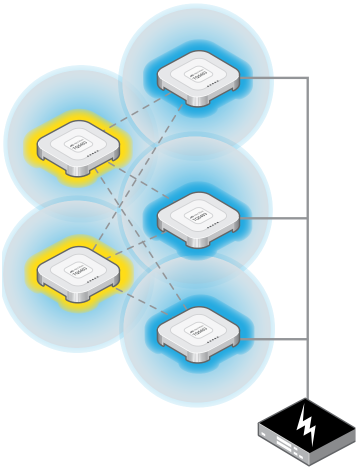


Allied Telesis AWC Channel Blanket (AWC-CB) is the Single Channel solution for Allied Telesis Wireless APs.

All APs that are members of the same blanket operate on the same channel. AWC-CB is an intelligent controller that manages interference and client access.

Together with a traditional Multi Channel approach, it provides a complete wireless access solution for any environment.

AWC-SC



Allied Telesis AWC Smart Connect (AWC-SC) is an effortless wireless network expansion with no added wires. Just register the new AP, plug in the power and it’s ready.

Reduce installation time by 90% by providing autonomous provisioning for event connectivity or fast office expansion without the need for new wires.

DIGITAL VIDEO SECURITY

In any modern network, a large part of the used bandwidth is composed of video streams. Within a school, a campus or a university, there are mainly two different types of streams, each with different impacts on network performance.

IP Video for Security

Student security and protection in the school is part of the whole education offering. Surveillance capability is one of the ways to increase family and student trust in a specific school and to attract new students.

In any video surveillance implementation, all the cameras and video management systems rely on the network infrastructure to transport video. The traffic generated by the surveillance cameras is almost constant during the day. Although this traffic must be planned for, once the network and the link are dimensioned, it usually does not cause any management concerns.

The key part of the installation is powered by Power over Ethernet (PoE) with power consumption that depends on multiple factors such as camera type and accessories. In the network design phase, the access switches connected with the IP cameras must be able to provide enough power to drive all the attached cameras.

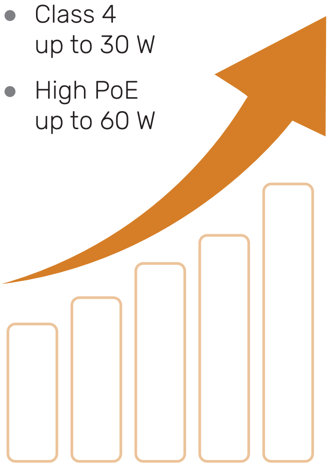
Online Learning

Video is also widely used for lessons, remote learning and as a resource for the students outside of school hours.

The traffic generated by this kind of video is less predictable, and if a whole class is streaming at the same time, traffic spikes can occur. To be effective, the video service must be available without delay or image degradation. Any problems can cause distraction and consequently a loss of student attention. The network design needs to be capable of absorbing traffic spikes without affecting other users or resources.

PoE Classes

- Class 0 up to 15 W
- Class 1 up to 4 W
- Class 2 up to 7 W
- Class 3 up to 15 W
- Class 4
  up to 30 W
- High PoE
  up to 60 W



For further information, please visit www.alliedtelesis.com/solutions/surveillance

Other Video Sources

Another source of traffic is video streaming from other sources such as YouTube, which often are not part of the educational offering, but are still accessed using the school network.

This traffic is largely unpredictable and is often not part of the school services, so it must be controlled to prevent disruption to high-priority services. Typically, this is achieved by allocating the video streams a low priority so they can be discarded if congestion occurs and there is higher priority traffic to be transmitted.

Large bandwidth, correct link dimensioning and priority management are the key elements for reliable and smooth video delivery, for the best user experience and the best learning outcomes.

ABOUT ALLIED TELESIS

For nearly 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and “things”—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis.com.**

Allied Telesis™