Solutions Guide

Allied Telesis

LAN and WAN Protection

Allied Telesis security features safeguard networks and mitigate attacks

Contents

About Allied Telesis

Allied Telesis has been serving the needs of the network communications industry for over 30 years. Although the technology we design and build has evolved significantly over time, our reputation for standards-based performance, product reliability and value has remained constant for all our customers and partners around the globe.

With a wide-ranging portfolio of products and technologies providing end-to-end networking solutions for enterprise, government, education and critical infrastructure customers, Allied Telesis is the smarter choice.

We are committed to providing our customers with quality solutions, designed and built to the highest standards. Our manufacturing conforms to ISO 9001 standards, and all our facilities adhere to the strict ISO 14001 standard to ensure a healthier planet.

Networks for today and tomorrow

Right now, we are engaged in some of the most advanced and innovative next-generation network research. We are focussed on developing and producing the intelligent, autonomously controlled and managed systems needed, in a world where the Internet of Things (IoT) is the norm.

Our R&D investments are putting us on the main stage in the exploding era of IoT. Cloud computing uses servers, applications and other resources linked via networks, so the infrastructure of those networks and the ability to autonomously discover, manage and resolve network issues are fundamental to network operations.

We're here for you

We also take advantage of our position as a network specialist to provide network administration software solutions. These range from administration and equipment monitoring, to authentication and status analysis.

We also offer market and solution-specific courses and certifications, audit packages and designs for healthcare and physical security/IP video surveillance applications. Our comprehensive support ensures that customers recover from a system fault with little to no downtime.

Network smarter with Allied Telesis

Our world is increasing in complexity. Organizations are changing at an ever-increasing rate. Businesses face an uphill battle to adapt to change, and to stay ahead of the competition. At the same time, our cities are increasingly becoming more populated—and with this growth, issues such as demand on resources and public safety become a key focus for government and civic leaders.

Introduction

The increasing number of connected devices in today's networks has created an insatiable demand for access to information, when and where we need it. This increasing reliance on IT resources and applications has changed the way we do business. Digital security is now a principal concern for network administrators, who must ensure maximum availability of the corporate network and Internet access.

There are several ways to increase the robustness of your modern network. Allied Telesis uses industry-leading switching technology to provide a comprehensive security suite, which provides a multi-layered solution to safeguard the network and combat common threats.

This document discusses three ways in which Allied Telesis switches ensure a reliable and secure network infrastructure. It also looks at some common network attacks, and how these can be mitigated using Allied Telesis equipment.

1. Secure Device Management

AMF restricted-login

Allied Telesis Autonomous Management Framework™ (AMF) is integrated into Allied Telesis devices running the AlliedWare Plus operating system. It automates and simplifies many tasks, with powerful features like centralized management, auto-backup, auto-upgrade, auto-recovery and more, providing plug-and-play networking with zero-touch recovery.

An AMF area has a master and member nodes. By default, users logged into any node on an AMF network can manage any other node by using either working-sets (a group of nodes able to be managed together) or AMF remote login to access another device. If the access provided by this feature is too broad, or contravenes network security restrictions, it can be limited by using atmf restricted-login, which changes the access so that:

1. Users who are logged into non-master nodes cannot execute any commands that involve working-sets, and
2. From non-master nodes, users can use remote-login, but only to login to a user account that is valid on the remote device (via a statically configured account or RADIUS/ TACACS+). Users must also enter the password for that user account.

Once you have enabled atmf restricted-login, certain other commands that utilize the AMF working-set command will operate only on the AMF master, such as the atmf reboot-rolling and show atmf group members commands.

Boot Loader Security

The boot loader is effectively the BIOS of the switch. Boot loader security should be implemented to prevent unauthorized access to the boot loader, which will then require a password to access boot up options. This also prevents the possibility of circumventing passwords on the switch without the boot loader password.

NOTE: This renders the switch unconfigurable if passwords are lost.

SSH/Telnet

When remotely logging in to monitor or manage a switch, Secure Shell (SSH) access provides confidentiality and integrity of data by encrypting management sessions and is the recommended way to communicate with switches. Telnet and HTTP are other ways to communicate with the management interface of switches, however these are not secure methods and it is recommended that they are disabled.

Syslog

To provide a detailed audit trail in the event of a suspected security breach or other problem, a Syslog server should be configured so switch log messages are stored in a central repository and available for later auditing or fault-finding.

Simple Network Management Protocol (SNMP)

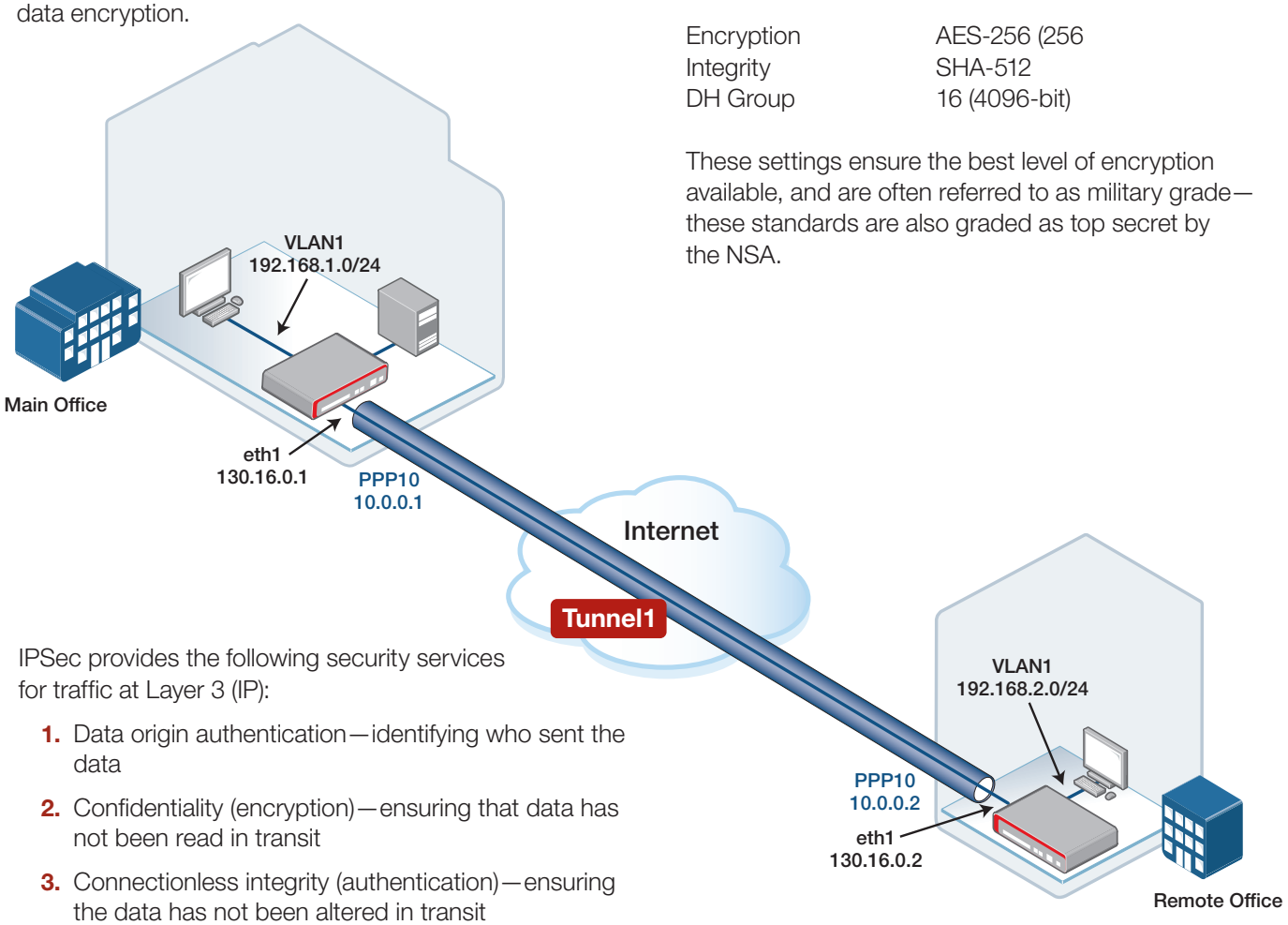
Network management systems often use SNMP to communicate with network switches and other devices. Using SNMPv3 provides secure access with authentication and encryption of SNMP management data. This data can then be used to check the status of any device on the network. For example, link down, edge device (camera, PC, door access controller) offline, link utilization, and uptime. Any anomalies can be shown on a network map to aid in fault-finding.

2. Securing the WAN

Site-to-Site Virtual Private Networks (VPNs)

A firewall at business branch locations manages connection to the Internet. The firewalls grant or restrict access to any type of online service or application. A site-to-site VPN established across the Internet will connect two branch offices together, and create a safe and encrypted connection to securely transport business data.

A site-to-site VPN uses the firewall to connect the entire branch office network in one location to the network in another—often connecting branch-office users to the head-office network. End-node devices in the branch office do not need VPN clients. because the firewall handles the connection. Most site-to-site VPNs connecting over the internet use IPSec for data encryption.



IPSec provides the following security services for traffic at Layer 3 (IP):

1. Data origin authentication—identifying who sent the data
2. Confidentiality (encryption)—ensuring that data has not been read in transit
3. Connectionless integrity (authentication)—ensuring the data has not been altered in transit
4. Replay protection—detecting packets received more than once, to help protect against Denial of Service (DoS) attacks

IPsec operation uses negotiated connections between peer devices (firewalls at each location). These connections are called Security Associations.

It is recommended that you no longer use DES, 3DES, MD5 (including HMAC variant), and Diffie-Hellman (DH) groups 1, 2 and 5. Instead, you should use AES, SHA and DH Groups 14 or higher—this is referred to as Next Generation Encryption (NGE), and is a lot more secure.

The minimum recommended IPsec and IKE settings for Next-Generation Encryption (NGE) are:

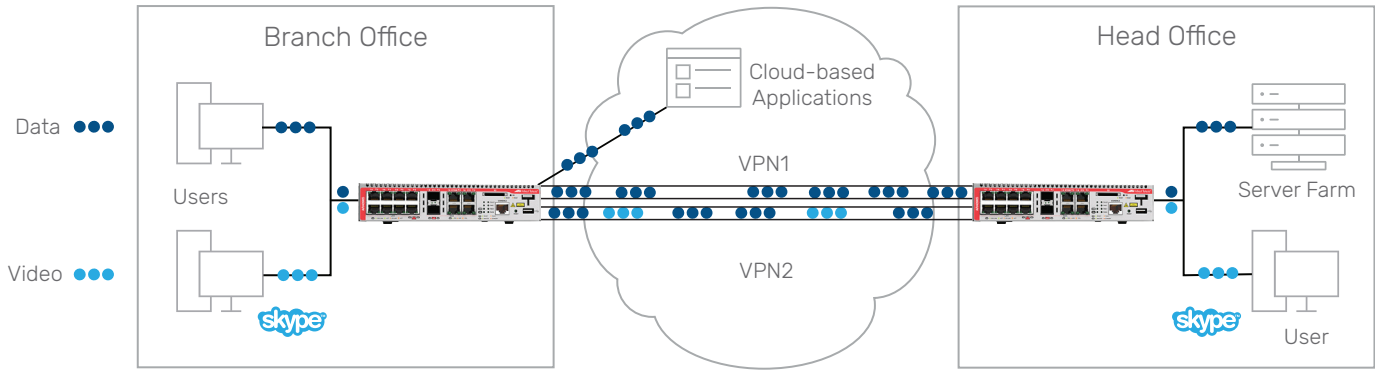
Encryption	AES-128 (128-bit)
Integrity	SHA-265 (128-bit)
DH group	15 (3072-bit)

However, the recommended IPsec and IKE settings are:

Encryption	AES-256 (256
Integrity	SHA-512
DH Group	16 (4096-bit)

These settings ensure the best level of encryption available, and are often referred to as military grade—these standards are also graded as top secret by the NSA.

SD-WAN



Expanding Wide Area Network (WAN) connections between offices can be expensive, and network management and troubleshooting is complex and time-consuming. Software Defined WAN (SD-WAN) lets business customers use existing physical branch office firewalls, and connect via low-cost Internet connections and VPNs. Vista Manager EX incorporates an SD-WAN orchestrator to let you create fully managed multi-site networks, integrating links and optimizing application flows to the Internet and right across the enterprise VPN infrastructure.

SD-WAN offers several advantages over traditional WAN solutions:

1. You can build higher-performance WANs using lower-cost and commercially-available Internet access. This lets you partially or entirely replace more expensive private WAN connection technologies, such as MPLS.
2. To reduce costs and mitigate risks, you can select any type of WAN connectivity to lower costs without compromising security. Traffic can then be load-balanced across these VPN tunnels to make optimal use of available bandwidth.
3. Dynamic path selection allows administrators to set performance thresholds for different applications. You can ensure that critical applications and data transfers always use the best path based on the quality (loss, latency and jitter) of the available VPN tunnels. For example, different quality settings can be configured for real-time applications such as voice and video conferencing, as opposed to data-transfer applications such as FTP.
4. SD-WAN automatically uses the best VPN tunnel to send traffic based on performance metrics, meaning that the internet provider with the best/most reliable connection will be used in a resilient architecture.

3. Securing the LAN

Inter-switch connections

Allied Telesis Ethernet Protection Switched Ring (EPSRing™)

In distributed networks, switches often use fiber connections for inter-switch connectivity in a ring topology, so a method of protecting the network from loops is required. EPSRing enables high-speed ring-based networks with failover in as little as 50ms.

ESPRing sends out control packets on a control VLAN configured on the switch, and these packets are expected to make a complete loop of the ring to maintain its integrity. If the packets do not make a complete loop then the ring is deemed to be down, and a fault will be reported to the management platform. EPSRing will automatically send packets around the ring the other way, with near instant failover, providing a powerful solution for service providers meeting stringent service level agreements.

AMF Secure Mode

AMF Secure Mode improves the security of the AMF network by reducing the risk of unauthorized access. It achieves this by:

1. Adding an authorization mechanism before allowing a member to join an AMF network.

2. Encrypting all AMF packets sent between AMF nodes.
3. Additional logging, which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

When running in Secure Mode, the controllers and masters in the AMF network form a group of certification authorities. A node may only join a secure AMF network once authorized by a master or controller. When enabled, all devices in the AMF network must be running in Secure Mode, and unsecured devices cannot join. NOTE: In AMF Secure Mode, the atmf restricted-login feature is automatically enabled. This restricts the atmf working-set command to users that are logged in to an AMF master. This feature can't be disabled independently of Secure Mode.

Active Fiber Monitoring (AFM)

AFM is built into many Allied Telesis switches, and constantly monitors the amount of light being received by the switch on fiber ports. If the light level changes, the system sends an alert that the fiber may have been tampered with, and can automatically shut down the link. AFM protects against fiber eavesdropping and prevents data theft.

VLAN Tagging Ingress Filtering

VLAN Tagging (802.1Q) is a method of forwarding logically separate VLAN data across network inter-connects. It does this by adding "tags" to the data. If the port is tagged for a set of VLANs, then a tagged packet will be accepted into the port only if it is tagged with the VLAN ID of one of the tagged VLANs configured on the port—otherwise the data will be dropped. So, if a switch is removed or a rouge switch inserted, unless the inserted switch is configured with the same parameters, all data will be dropped, and alerts will be sent to the management system that the link is offline—thus protecting the network.

Link Aggregation Control Protocol (LACP)

LACP is a method of aggregating multiple physical links into one higher bandwidth virtual connection. It can be configured on all switch uplink ports, and once configured will send out control packets to check the status of all links. If the switch does not receive the correct LACP information for a given link, it will prevent any data from using that link, and use the other link aggregation members instead. An alert is sent to the management system so the faulty link can be rectified.

Edge port security

Network Access Control (NAC)

NAC allows for unprecedented control over user/device access to the network, in order to mitigate threats to network infrastructure. Using 802.1x port-based authentication in partnership with standards-compliant dynamic VLAN assignment, it is highly regarded as the most secure way to restrict access to the network at port level.

NAC uses a RADIUS server to authenticate any user or device connected to a port with 802.1x configured. Edge ports are locked down and require the user device to ask for access, then the switch will negotiate between the device and the RADIUS server to check authentication credentials. If the device is granted access, the VLAN association for that device is issued to the switch from the RADIUS server, ensuring the device has the correct level of network access. This prevents unwanted access, as the device must provide the server with unique certificate information as well as username and password. Ports that are waiting to authenticate a client device using 802.1x are placed in an isolated VLAN.

Port Security

The ability to limit the number of workstations that can connect to specific ports on the switch is managed with Port Security. If these limits are breached, or access from unknown workstations is attempted, the port can do any or all of the following: drop the untrusted data, notify the network administrator, or disable the port. This means that a device cannot move from one port to another; if a device is changed it will not gain access to the network. Port security is not currently supported when used alongside 802.1x, as 802.1x locks a single MAC address (single client/workstation) to a port.

Dynamic Host Configuration Protocol (DHCP) Snooping

DHCP servers allocate IP addresses to clients, and the switch keeps a record of addresses issued on each port. IP Source Guard checks against the DHCP snooping database to ensure only clients with specific IP and MAC address can access the network.

DHCP snooping can be combined with other features, like Dynamic ARP Inspection, to increase security in Layer 2 switched environments. Additionally, you can add static entries to this database and configure a port to

only accept access from a single device on a port, which will enable the edge ports to have the same functionality as port security with the added benefit of checking the IP address and VLAN settings. This prevents devices being moved around within the network and protects against rogue DHCP servers. It also provides a traceable user history, which meets the growing legal requirements placed on Service Providers.

VLAN Tagging Ingress Filtering

As well as managing data on inter-switch links as discussed earlier, ingress filtering protects edge ports by not allowing any VLAN tagged packets.

Secure configuration of Spanning Tree Protocol (STP)

STP is the most commonly used means of preventing loops in Layer 2 networks. There are two protection mechanisms that must be enabled to maximize robustness, as STP has no inbuilt security:

1. **STP Root Guard** – prevents a malicious user from accessing inappropriate data on the network, by allowing the network administrator to securely enforce the topology of the spanning tree.
2. **BPDU guard** – similarly increases the security of STP by allowing the network administrator to enforce the borders of the spanning tree, keeping the active topology predictable. BPDU Guard prevents any edge device (I.e. a camera, door access controller or PC) from being replaced with a switch by a malicious user trying to gain network access. If the edge switch sees STP packets on a link with this feature enabled, the link will be shut down to prevent unwanted access.

Storm Protection

Storm Protection reduces the adverse effects of any network loop that would potentially swamp the network. There are three facets that work together to protect the network from storms:

1. **Loop detection** – monitors traffic for the return of a loop detection probe packet. In the event of a problem, it can take a variety of actions including logging a fault, alerting the network administrator or disabling a link.
2. **Thrash limiting** – detects a loop if certain device hardware MAC addresses are being rapidly relearned on different ports. In the event of a problem, similar actions to those of loop detection can be taken.
3. **Storm control** – limits the rate at which a port will forward broadcast, multicast or unknown unicast packets. This controls the level of traffic that a loop may cause to be flooded in the network.

Control Plane Prioritization (CPP)

CPP prevents the switch Control Plane (which looks after network management traffic) from becoming flooded in the event of a network storm or Denial of Service (DoS) attack, ensuring critical network control traffic always reaches its destination.

Denial of Service (DoS) attack prevention

A DoS attack is an attempt to make online resources unavailable to users. There are numerous known DoS attacks that can be monitored. When detected, the options are to notify network administration, and/or shut down the affected switch port.

Access Control Lists (ACLs) and Filters

Managing traffic volume and the types of traffic allowed on the network is essential to ensure high performance, guard against unwanted traffic and provide continuous access to important data. Powerful ACLs and filtering capability provide a mechanism for network traffic control, all handled in the switch hardware, so wire-speed performance is maintained.

Shutdown

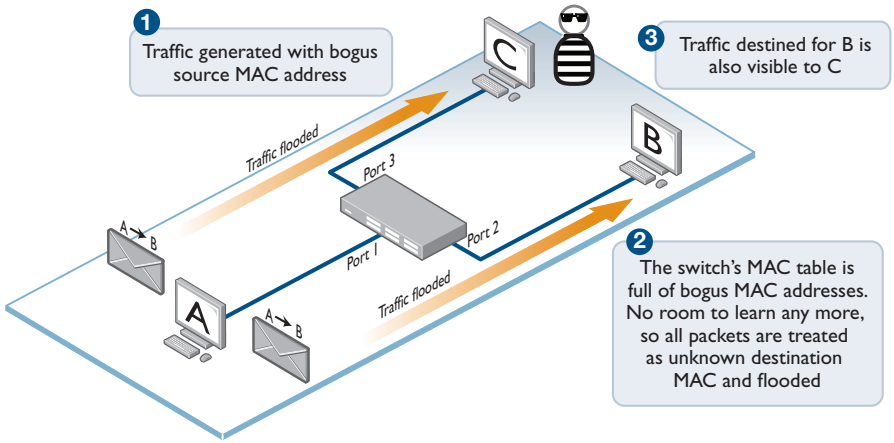
All unused edge ports should be shut down to prevent unwanted network access. Additionally, shut down ports should be placed into an isolated VLAN so if any were unintentionally left online, they would still be isolated from any network data.

4. Common network attacks

1. MAC flooding attack

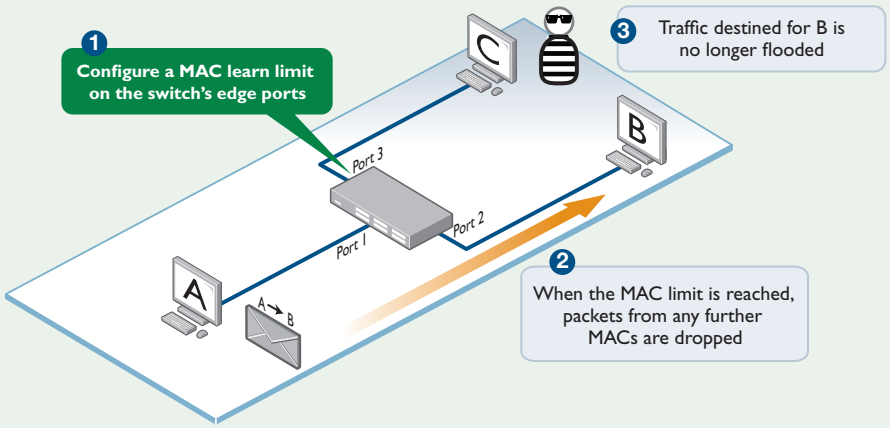
What are MAC flooding attacks?

MAC flooding attacks facilitate information stealing by providing a source of accessible data. In a MAC flooding attack, a malicious host sends packets from thousands of different bogus source MAC addresses, which then fill the forwarding database. Once full, legitimate traffic is flooded and becomes widely accessible, as the switch does not have room to learn any more specific destination addresses in the forwarding database. The malicious user has essentially turned the switch into a low-intelligence pseudo-hub, allowing them to sniff all flooded traffic, thereby stealing data and passwords.



How do Allied Telesis switches protect you?

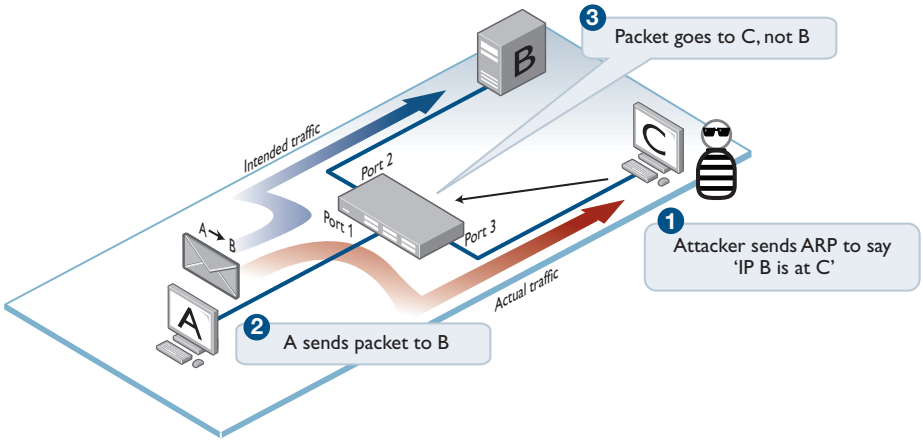
Allied Telesis switches provide two security measures to protect your LAN from MAC flooding attacks. The first is host authentication, whereby authenticating ports only accept traffic from the MAC addresses of authenticated hosts. The second is port security, which controls how many MAC addresses can be learnt on a specific port. When a limit is breached, the switch will take one of three user-configurable actions—drop the untrusted data, notify the network administrator, or disable the port while the intrusion is investigated.



2. Address Resolution Protocol (ARP) spoofing attacks

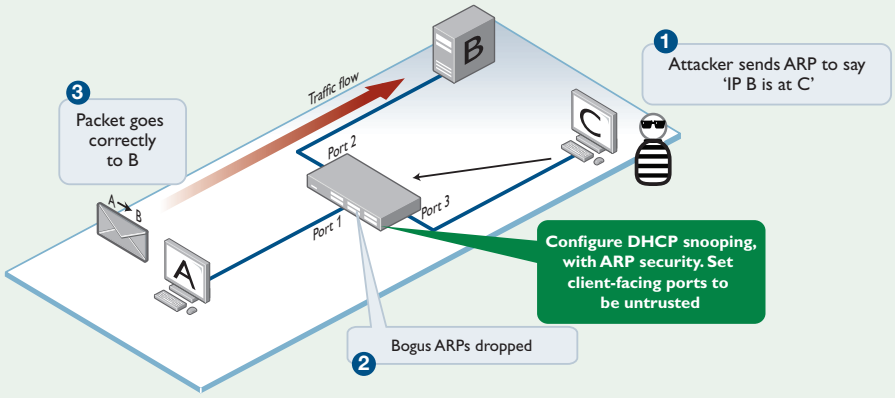
What are ARP spoofing attacks?

An ARP spoofing attack is another form of information-stealing attack. A malicious host sends an ARP reply to a host's ARP request for a server. The hacker falsely claims to be that server by tying their own MAC address to the IP address owned by the server. The bogus ARP message then also adds an entry into the switch ARP table. When workstation A sends a message destined for server B, the bogus ARP entry diverts that message to hacker C. This enables the hacker to steal data and passwords.



How do Allied Telesis switches protect you?

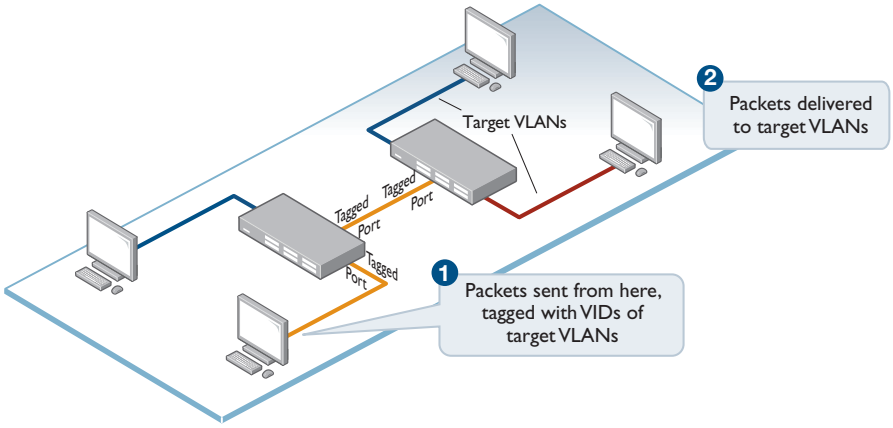
Allied Telesis switches use DHCP Snooping with ARP Security to protect your network from ARP spoofing attacks. All ARP replies from untrusted ports are checked to ensure they contain legitimate network addressing information, safeguarding the network and the business.



3. VLAN hopping attacks

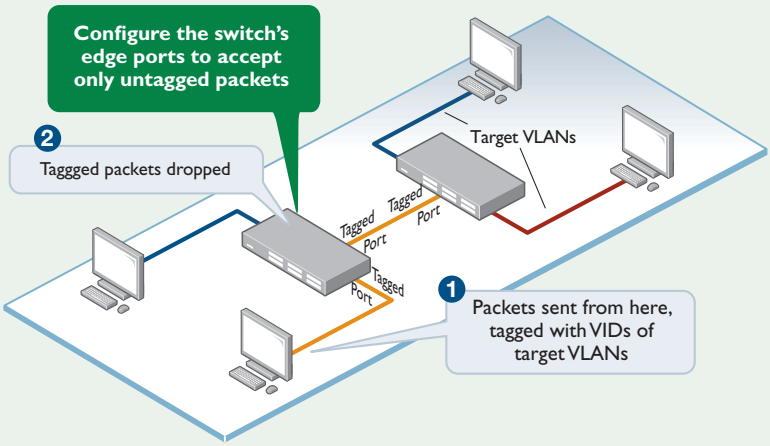
What is a basic VLAN hopping attack?

A malicious user in one VLAN gains unauthorized access to another VLAN by sending tagged packets into the network with the VID of the target VLAN. By default, many switches will simply look at the tag on the packet, and pass the packet to the corresponding VLAN, even if the ingress port is not a member of that VLAN.



How do Allied Telesis switches protect you?

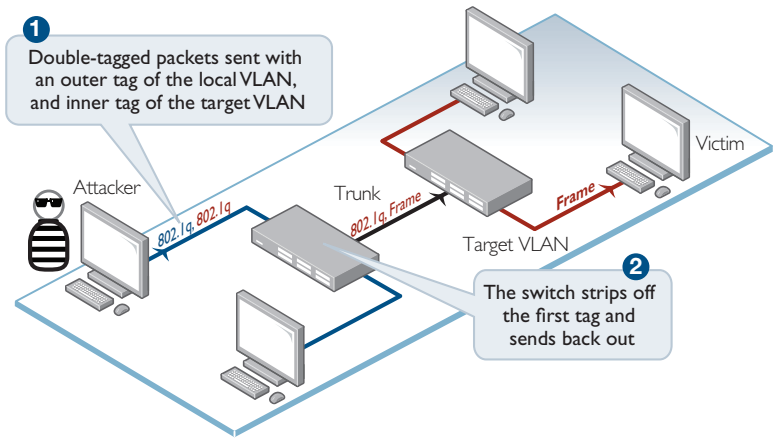
To eliminate basic VLAN hopping attacks, Allied Telesis switches use Ingress Filtering to drop packets tagged with VIDs that do not correspond to the VLAN of the ingress port, as workstations attached to edge ports should not send tagged packets into the network.



4. Double-tag VLAN hopping attacks

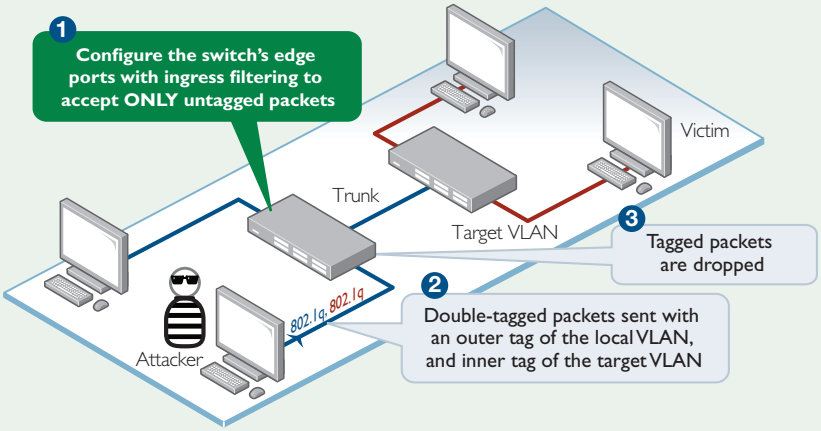
What is a double-tag VLAN hopping attack?

A malicious user sends a packet that is tagged twice. In the outer tag is their own VID, and in the inner tag is the VID of an unauthorized VLAN to which the attacker is trying to gain access. The switch removes the outer tag and passes the packet to the next switch. The packet's inner VLAN tag—the unauthorized VLAN's VID—then becomes the sole VLAN identifier, and the packet makes its way to the target VLAN.



How do Allied Telesis switches protect you?

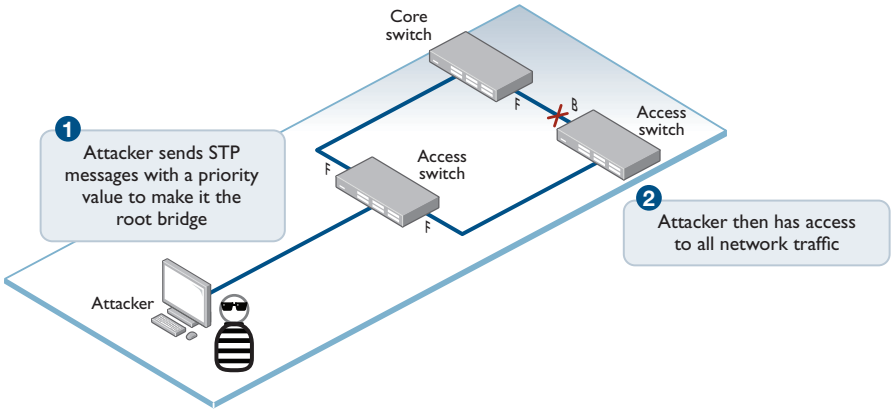
To eliminate double-tag VLAN hopping attacks, Allied Telesis switches employ the same solution as for basic VLAN hopping attacks. Ingress Filtering drops all tagged packets, since workstations attached to edge ports should not send tagged packets into your network.



5. Spanning Tree Protocol (STP) Attack

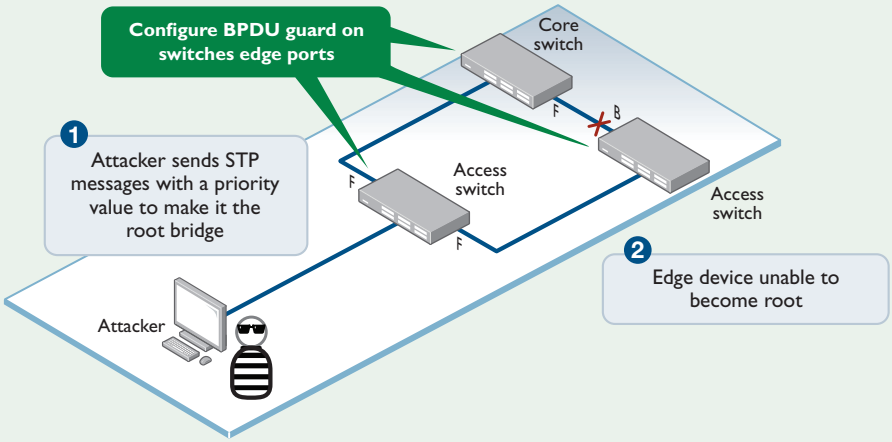
What is STP attack?

STP prevents loops in Layer 2 networks, while allowing path redundancy. Switch ports are designated as being either in a forwarding state or a blocked state. If a path becomes unavailable, the network responds by unblocking a previously blocked path to allow traffic to flow. STP is reliant on the establishment of a 'root bridge', which is the unique root of the network tree. In an STP attack, a malicious user sends an STP message—a Bridge Protocol Data Unit (BPDU)—with a priority value that makes it the root bridge, and thus compromises the network topology by forcing it to reconfigure.



How do Allied Telesis switches protect you?

Allied Telesis switches prevent STP attacks by using BPDU guard on edge ports, preventing bogus STP messages originating from a workstation. Additionally, the root guard feature can be used to narrow down the region of the network within which the root bridge must reside.

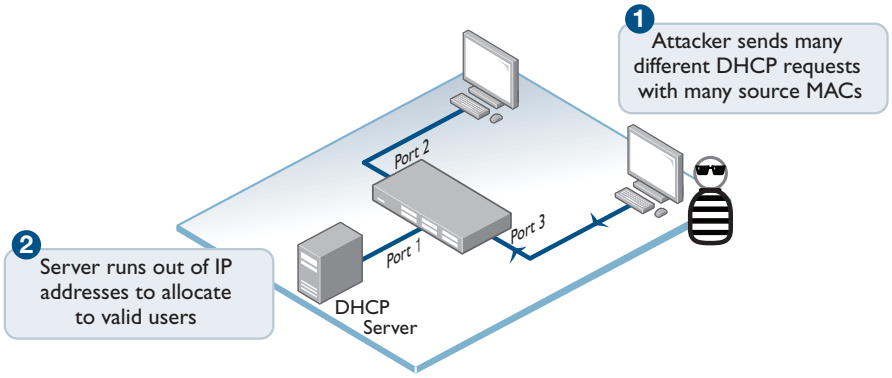


6. Dynamic Host Configuration Protocol (DHCP) attacks

DHCP servers allocate IP network addresses to hosts, allowing them to access resources on the network. There are two forms of DHCP attack which can compromise your network access:
DHCP starvation attacks, and DHCP rogue server attacks.

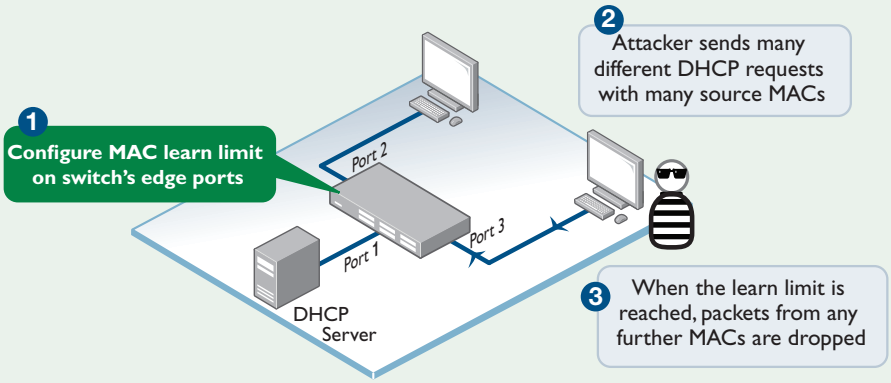
What is a DHCP starvation attack?

In a DHCP Starvation attack, a malicious user inundates the DHCP server with countless DHCP requests from different bogus MAC addresses. The DHCP server eventually runs out of IP addresses. As a result, valid users are unable to obtain an IP address, effectively blocking their network access.



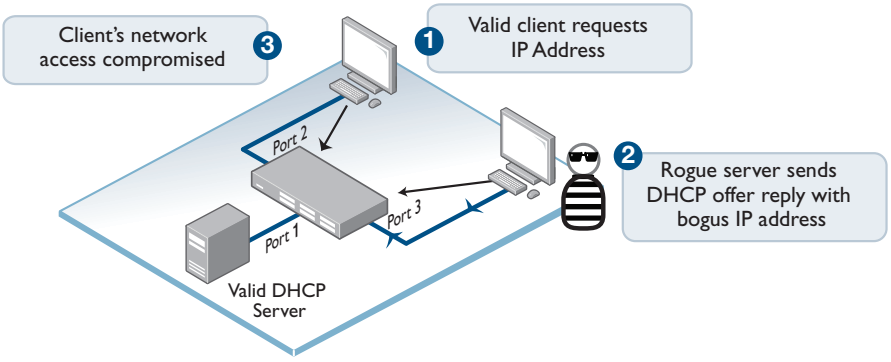
How do Allied Telesis switches protect you?

Allied Telesis switches prevent this specialized Denial of Service (DoS) attack with port security. Edge ports are configured with a MAC learn limit. Once the learn limit is reached, no further different MAC addresses are allowed on the port. Notifications can be sent to a network management station when the limit is reached to alert the network manager of excessive MAC activity on a port. Additionally, the port can be automatically disabled, to lock down that connection while the intrusion is investigated.



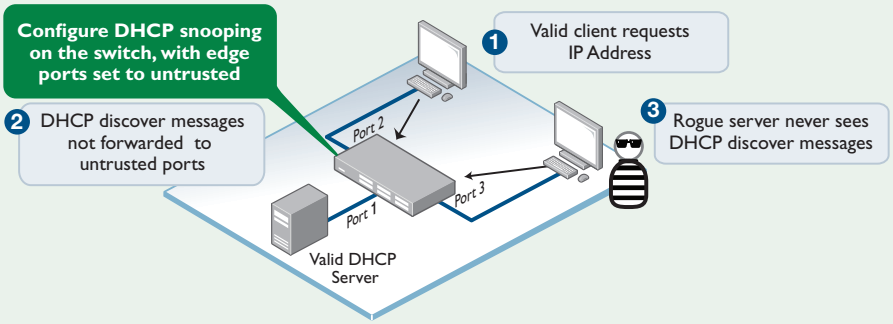
What is a DHCP rogue server attack?

A malicious user's computer disguises itself as a DHCP server and responds to DHCP requests with bogus information. At the very least, this results in compromised network access. In more sophisticated attacks, it can be used to direct users to websites masquerading as secure sites, for example a bank, and thereby steal passwords and personal information.



How do Allied Telesis switches protect you?

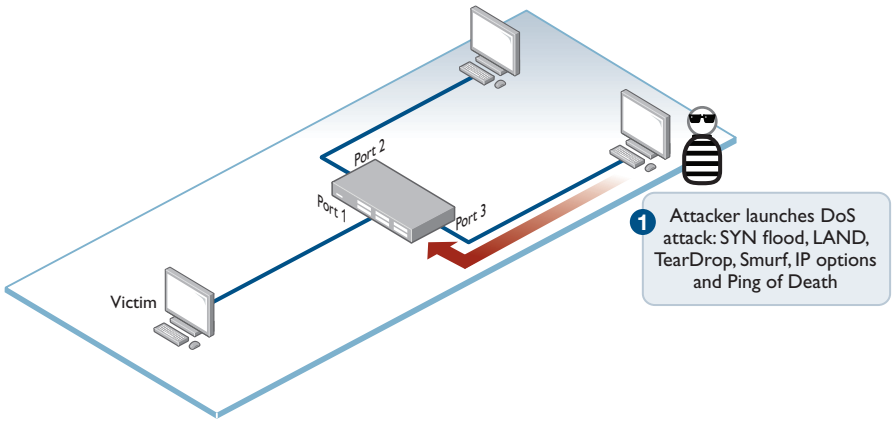
Allied Telesis switches avoid DHCP rogue server attacks by using DHCP Snooping. Edge ports are designated as 'untrusted' ports. The switch will not accept any DHCP server traffic on untrusted ports, so the rogue server is blocked from interacting with DHCP clients.



7. Denial of Service (DoS) attacks

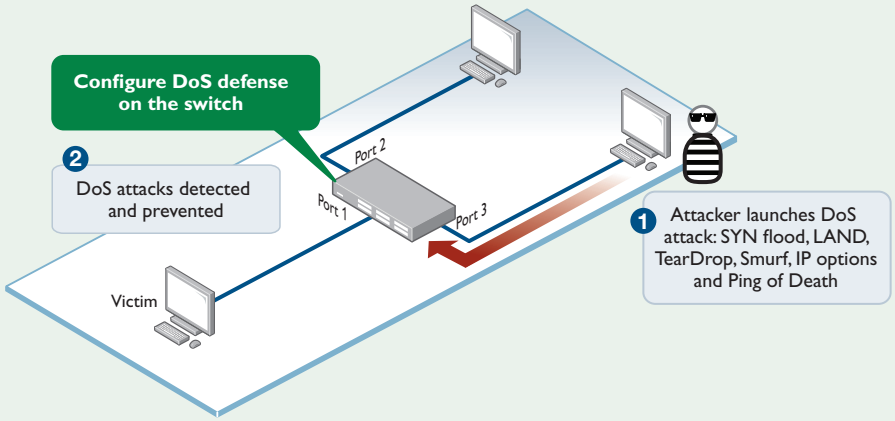
What is a DoS attack?

There are many different types of DoS attacks that can threaten your network. Some attacks exploit invalid packet formats, causing target devices to 'hang'—for example Tear Drop, IP Options or Ping of Death attacks. Other attacks initiate a packet storm targeted at a specific 'victim', such as Smurf attacks. Still others initiate numerous TCP connections with a victim, to consume resources on the victim device—like SYN flood attacks.



How do Allied Telesis switches protect you?

Allied Telesis switches can mitigate all these attacks using DoS defence. Furthermore, the DoS defence for most of these attacks is implemented in the switch silicon, so it does not affect network performance.



5. Some key Allied Telesis technologies

The following innovative Allied Telesis technologies enable safe and secure networking, and automated management to ease the burden of administration.

Alliedware Plus™ Operating System

AlliedWare Plus is an advanced, feature-rich, next-generation Operating System (OS) that delivers the functionality, scalability, performance and reliability your network demands. Built on industry standards and with a user interface that is easy to understand, AlliedWare Plus is the perfect solution for IoT and SDN-enabled networks where greater intelligence, advanced security and automated services are required.

AlliedWare Plus combines superior networking functionality and strong management capabilities with the exceptional performance that today's networks demand. Many of the commands can be used in scripts, allowing the automation of configuration tasks. Users can also utilize Triggers, which provide a powerful mechanism for automatic and timed management by automating the execution of commands in response to specific events. Because it is standards-based, it also assures full interoperability with other major network equipment and emphasizes improved usability and high reliability for a superior customer experience.

Ease of Management

The AlliedWare Plus OS incorporates an industry-standard Command Line Interface (CLI), facilitating intuitive manageability. Each command is associated with a specific function or task. Many commands can be used in scripts, allowing automation of configuration tasks. Users can also utilize Triggers, which provide a powerful mechanism for automatic and timed management, by automating the execution of commands in response to specific events.

With three distinct modes, the CLI is very secure. In User exec mode, the user can view settings and troubleshoot problems, but cannot make changes to the system. In Privileged exec mode, the user can change system settings and restart the device. Configuration changes may only be made in Global configuration mode, reducing the risk of accidental changes.

The Allied Telesis Device GUI can be used on our AlliedWare Plus switches and routers/firewalls and provides an easy-to-use and powerful way to monitor and manage the device. Models that support integrated wireless management also have an inbuilt network map, to enable easy wireless deployment with floor and heatmaps to monitor performance.

Autonomous Management Framework™ (AMF)

Managing network infrastructure is time intensive, costly and has traditionally required expensive, third-party applications to effectively manage larger networks. Cloud computing and converged infrastructures deliver a great deal of business value to the enterprise, but they also add complexity. In turn, networks must be more fluid and evolve at increasingly greater speeds in order to keep pace with the modern applications and service delivery models that are driving that complexity. For everything from virtualization to mobility and BYOD, networks must be able to keep pace with business. AMF helps IT do just that by greatly reducing the time and cost of managing network infrastructure.

AMF delivers real and immediate value to businesses by solving one of IT's most pressing needs. It provides a converged infrastructure that can be managed as a single entity, reducing complexity and TCO, and allowing more to be done with less.

AMF is an embedded technology native to Allied Telesis switches and routers that delivers real and immediate value to businesses. The most pressing needs of many organisations demand a single, converged infrastructure that can be managed as a single entity, reducing complexity and TCO and allowing more to be done with less.

AMF achieves this and more by delivering:

- Unified network management from any device across the network.
- Graphical management of the network with Vista Manager EX.
- Private or public cloud deployment options with AMF Cloud.
- Network automation that simplifies and automates tasks across the network.
- Network intelligence that reacts to changes within the network and automatically changes the topology of the network.
- Automatic backup, restore, and recovery of devices as they are added to the network.

Through this combination of robust features, AMF drives lower network operating expenses by reducing the complexity and level of effort required to maintain the network. One Allied Telesis customer has reported a 60% reduction in operational costs by deploying AMF.

AMF-Sec

Autonomous Management Framework Security (AMF Security)

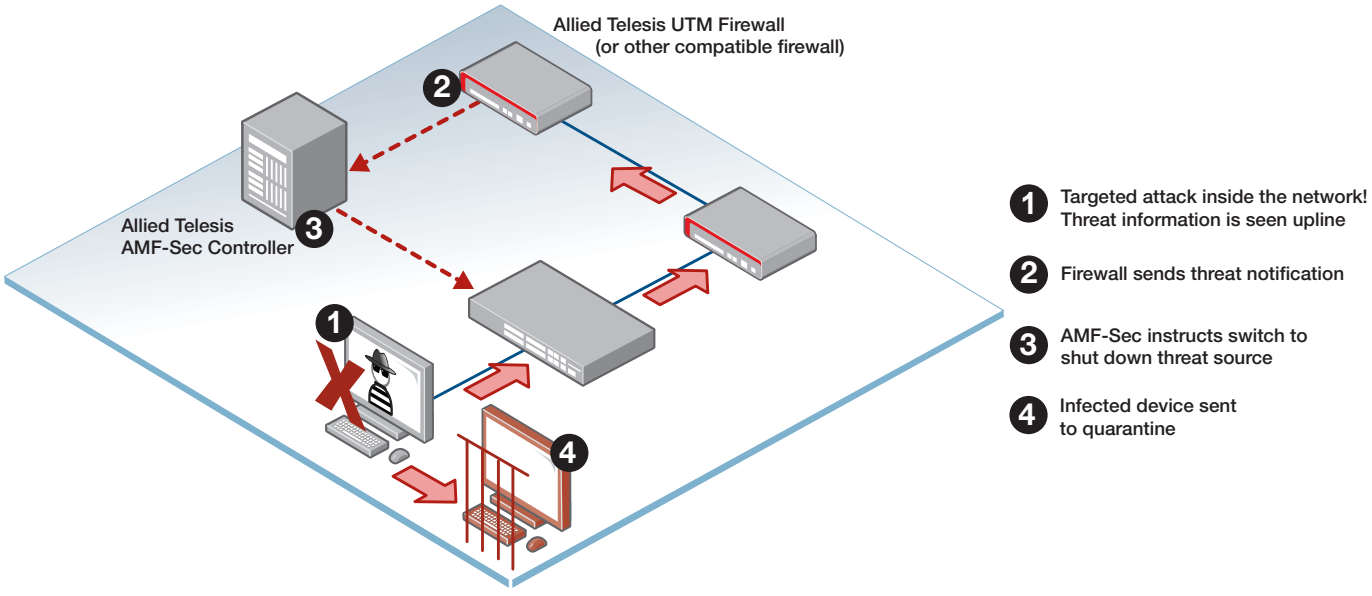
Today's network threat landscape has changed, and the internal LAN is now susceptible to malicious attack from hackers who continually evolve ways to exploit security weaknesses. Even inadvertent threats like staff plugging in USB flash drives that may contain viruses or malware need to be managed and contained.

AMF (described previously) simplifies and automates network management. AMF-Sec adds a powerful security component with an intelligent, fully featured SDN controller. It reduces manual effort and cost by working with security applications to instantly respond to alerts, and block the movement of malware within a wired or wireless network – protecting the LAN from internal threats.

AMF-Sec partners with best-of-breed firewall and security appliances to identify threats, then the intelligent Isolation Adapter engine built into our AMF–Sec controller responds immediately to isolate the affected part of the network, and quarantine the suspect device. Remediation can be applied so the device can re-join the network with minimal disruption. 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, to enable a self-defending network that helps organizations avoid lost time and unnecessary disruption to network services.

Any security issues are highlighted in Vista Manager EX, our monitoring and management tool, and an email can be sent to alert network administrators that AMF-Sec has automatically protected the network, and allow remediation to be managed locally or remotely.



AWC™

Autonomous Wave Control (AWC)
AWC automates wireless networking so IT staff to concentrate on other value-added tasks and services. A secure and easy way to manage Wi-Fi network is a must with the growth in mobile and BYOD wireless devices accessing online resources and applications. Wireless client on an AWC network can be part of a self-defending network solution using AMF Security as described previously.

Three key components make up our No Compromise Wireless solution, and enable:

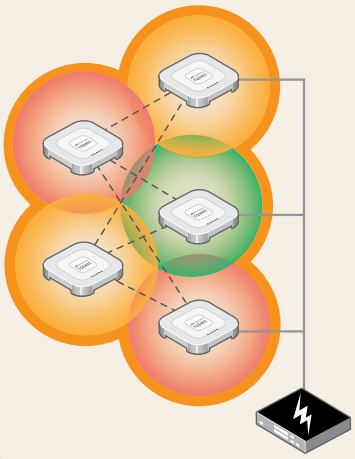
- Automatic optimization of the wireless network (AWC)
- Seamless roaming for Wi-Fi clients (AWC-CB)
- Plug-and-play wireless network growth (AWC-SC (available in 2020))

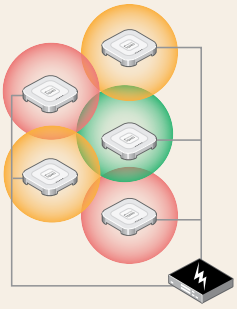
No Compromise Wi-Fi

Mixed-channel architecture for mission-critical networks

Don't sacrifice your networks performance for reliability

- World's-first hybrid access points
- Simultaneous single and multi-channel connectivity
- Maximizes wireless performance
- Provides seamless roaming
- Self-forming, self-optimizing Wi-Fi network

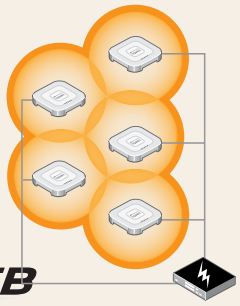




AWC™

AWC Network Optimization
Maximum wireless performance

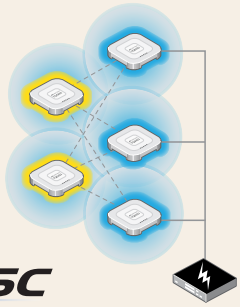
- Automatically analyzes multi-channel Wi-Fi networks
- Autonomously optimizes wireless performance
- Responds to user bandwidth demands
- Provides a superior Wi-Fi user experience
- Reduces deployment time and cost



AWC™-CB

AWC Channel Blanket
Uninterrupted Wi-Fi with seamless roaming

- APs operate on a single channel
- Provides seamless-roaming with reliable coverage
- Designed for dynamic physical environments
- Simplified management lowers operation cost
- Easy deployment without channel design



AWC™-SC

AWC Smart Connect
Effortless wireless network growth

- Innovative wireless AP uplink connectivity
- Plug-and-play wireless network growth
- Auto-optimization of wireless throughput
- Zero-touch access point deployment
- Supports all AWC and AWC-CB benefits

VISTA MANAGER™ EX

Vista Manager EX – Powerful network management and monitoring

Vista Manager EX is the intelligent way to monitor and manage your entire network, including AMF controlled switches and routers, AWC controlled wireless access points, and third party devices.

Single-pane-of-glass visibility improves network management. Enjoy complete network monitoring from the dashboard—including network details, status, event information and a topology map, where critical issues are highlighted for timely resolution. Intuitive access to powerful features like service and performance monitoring, control of wired and wireless devices, and automation tools, makes networking easy.

Further intuitive tools include wireless floor and heat maps to easily check on access point performance, a network traffic map to view utilization and protocol use across all links, and a central orchestrator for inter-branch WAN links.

This broad management feature-set supports network administrators in enabling a secure online LAN and WAN environment for all users.

VCStack™

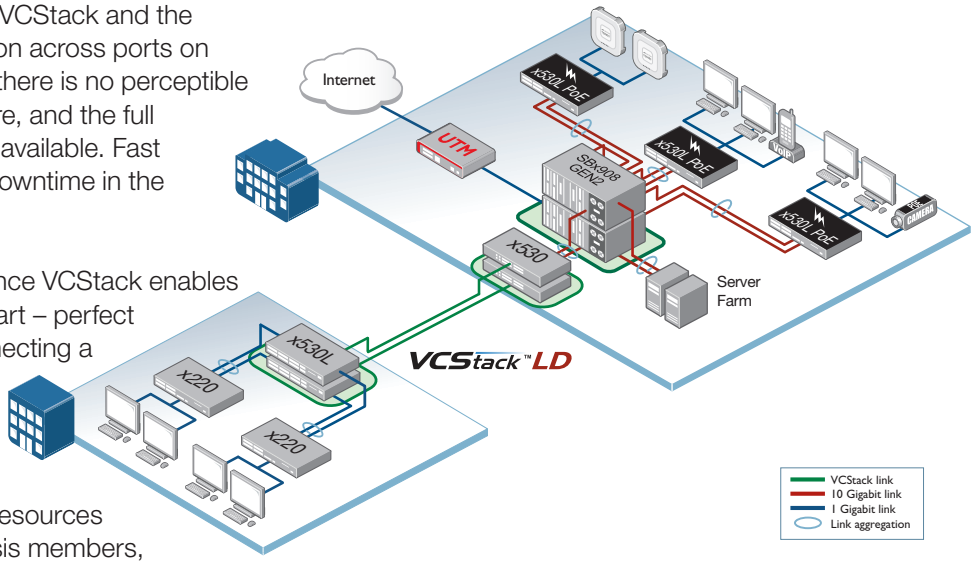
Virtual Chassis Stacking (VCStack™)

Using Allied Telesis VCStack in your network allows multiple switches to appear as a single virtual chassis.

In normal operation, this virtual chassis acts as a single switch, simplifying management. The diagram shows link aggregation between the core VCStack and the edge switches. With link aggregation across ports on different virtual chassis members, there is no perceptible disruption in the case of a link failure, and the full bandwidth of the network remains available. Fast failover ensures minimal network downtime in the event of a problem.

Using fiber connectivity, long distance VCStack enables stack member to be kilometers apart – perfect for a distributed environment, connecting a single virtual chassis across the campus or even the city.

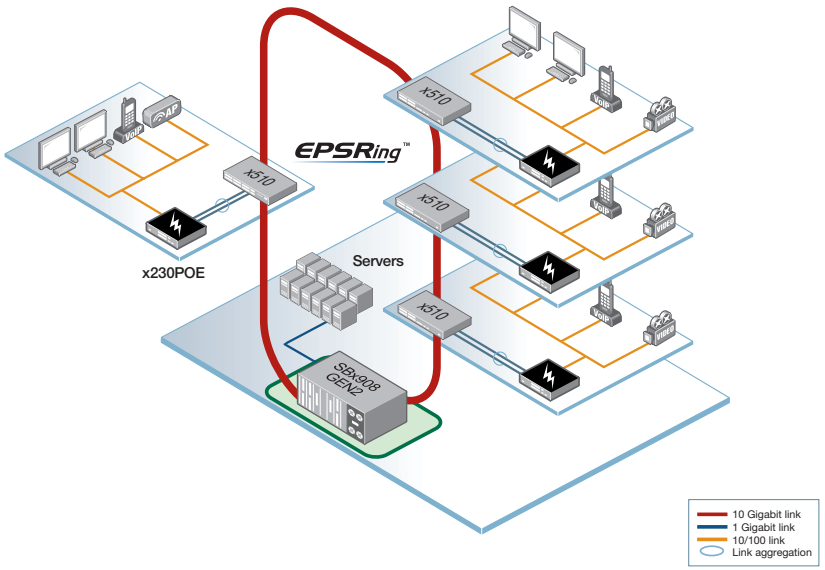
VCStack and link aggregation provide a solution where network resources are spread across the virtual chassis members, ensuring device and path resiliency. Virtualization of the network core ensures uninterrupted access to information when needed.



Ethernet Protection Switched Ring (EPSRing™)

EPSRing allows switches to form a high-speed protected ring running at today's fastest Ethernet speeds and capable of recovery within as little as 50ms.

EPSR is perfect for high performance and high availability in distributed environments. SuperLoop Prevention (SLP) enables a link between two EPSR nodes to be in separate EPSR domains, improving redundancy and network fault resiliency.



Active Fiber Monitoring (AFM)

AFM is a technology pioneered by Allied Telesis which provides specialized data protection on optical links. You can enjoy non-stop, automated monitoring of all your optical fiber with no need for expensive third-party equipment.

A unique solution, AFM works by detecting very small changes in the amount of light received on a fiber link. When an intrusion is attempted, the light level changes because some of the light is redirected by the eavesdropper onto another fiber. AFM detects this intrusion and raises the alarm. The link can then either be shut down automatically, or an operator can be alerted to manually intervene. Configuration is simple—just "set and forget".

Power over Ethernet Plus (PoE+)

With PoE, a separate power connection to media end points such as IP phones and wireless access points is not necessary. PoE+ provides even greater flexibility, providing the capability to connect devices requiring more power (up to 30 Watts)—for example, tilt and zoom security cameras. Some of our switches also support PoE++ and can provide up to 60 Watts per port.

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

C618-31047-00 REV C