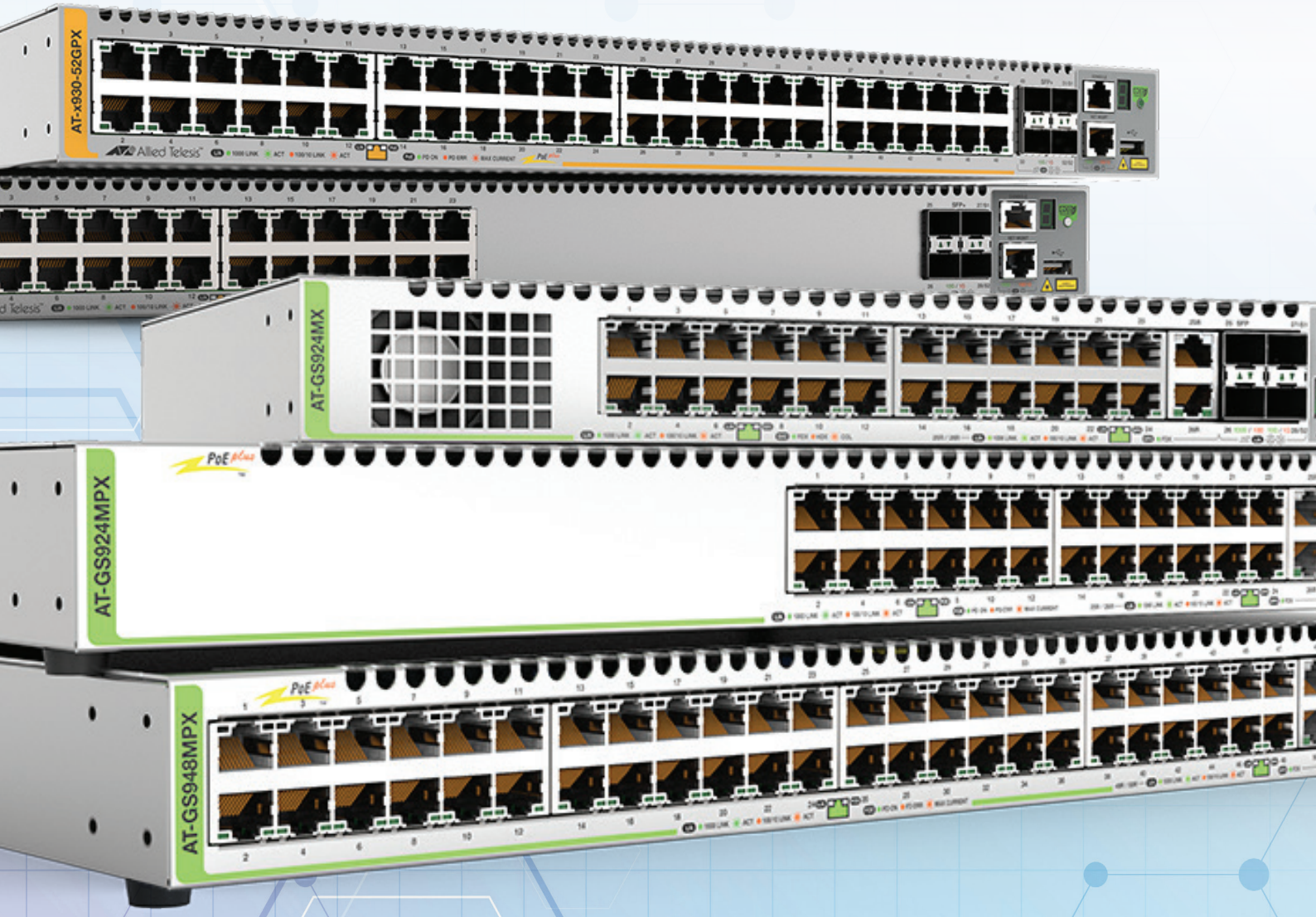
Solution Guide

Allied Telesis

Enterprise Networking Solutions



AlliedTelesis.com

NETWORK SMARTER

Introduction

Today's offices make ever-increasing use of online resources and applications. When the network is down, productivity falls. Network managers need to provide reliable, secure, fast networks that keep businesses running smoothly today and into the future. This dependence on network availability is moving IT managers to review their current facilities, to decide whether there are sufficient capabilities to meet their needs, and when to upgrade.

Choosing the right solution can be difficult when there are so many different requirements that must be satisfied:

- Bandwidth
- Resilience
- Application support
- Management system
- Security
- Future proofing

Allied Telesis has been delivering innovation in this area for some time. This document describes our Enterprise Network Solution, using Allied Telesis products to provide a modular, scalable, and flexible solution suitable for small to large enterprise businesses.

The technologies featured in this solution include:

- Switch stacking with link aggregation for resilience.
- Layer 3 core switching.
- Network Access Control (NAC) for security.
- Quality of Service (QoS) for Voice over IP (VoIP) and video streaming.

This document aims to help you build different bandwidth solutions with similar resilience, QoS, and security features, ensuring that all your current network needs are met with future expansion and new applications catered for.

Building an optimum network

Determining the best design and implementation of your network ensures optimal reliability, availability, scalability, security, and performance for your enterprise.

A number of factors must be considered when deciding upon a network design:

Bandwidth - the network must provide enough throughput now and for a number of years to come. The speed of edge ports and uplinks should match the requirements of current and foreseeable future applications.

Allied Telesis solutions have options that cover 10/100 Mbps or 10/100/1000 Mbps at the edge, with uplinks speeds of 1, 10, 40 and 100 Gbps to support any size network. Multi-Gigabit (2.5 and 5Gbps) ports on some products enable a faster backbone without upgrading existing building cabling. The core switch needs sufficient capacity to aggregate all of these connections, and also to provide resilient server and storage connectivity.

Resilience - downtime immediately impacts on productivity, so resilience is also vital.

- The Allied Telesis solution uses split link aggregation technology in which links from core stacked switches to the edge switches are connected to separate units but grouped together to act as a single link achieving both resilience and improved bandwidth availability.
- Other resilience options are available if the design topology and scale demand it. Ethernet Protected Switched Ring (EPSR), and the standards-based G.8032 Ethernet Ring Protection, ensure that distributed network segments have high-speed, resilient access to online resources and applications. RSTP or MSTP can be used as a fall-back technology or for integration with existing legacy equipment. For further resilience, the use of stacked switches means that uplinks can be connected to different units in the stack enabling both device and path redundancy.
- Recovery times are another important factor. The failure of a stacked unit can be quickly resolved by simply exchanging the failed unit with a new one of the same stack ID.

Application Support - networks are now becoming more than just a means for moving data from server to PC. Converged networks are now becoming the norm with VoIP becoming the telephony system of choice. Multimedia services are also being added and applications are shifting larger files with more graphical content. Network managers want to install equipment that can support PC applications and IP telephony. Power over Ethernet (PoE) options at the edge are available for all solutions. Some may want to have dedicated PoE ports, some will want to be able to plug any device anywhere. In order to support all the necessary applications QoS is essential to ensure that voice and multimedia pass through the network without loss or delay. QoS also allows critical applications to

be prioritized above Internet access and other background functions. Many standards-based VoIP systems now require LLDP-MED protocol for auto-configuration of IP handsets. Support for this is available on all PoE edge switches.

Management - a resilient network is only as good as the management system that informs you that a failure has occurred and the network has healed itself. The network manager is then able to action the repair before the failure can affect the network availability. The network management system performs the following tasks:

- Mapping and monitoring of network devices.
- Monitoring of all resilient functions—PSU, links, stacks etc.
- Alerting of important failures by email, paging etc.
- Collection of statistics to allow reporting on key devices and links.

Security - as the dependence on the network and PCs grow, so do the risks of attack, either malicious or from viruses being unknowingly brought in.

- The Allied Telesis solution offers security for both the network itself, via 802.1x or Network Access Control (NAC), and also for the management of the network devices themselves which can also be protected with centralized authentication.
- Autonomous Management Framework Security (AMF-Sec) enables a self-defending network that protects the inside of the LAN against malicious attack from hackers, and inadvertent threats like staff plugging in USB flash drives that may contain viruses or malware. AMF-Sec instantly respond to alerts, and block the movement of malware within a wired or wireless network. As shown in the diagram, AMF-Sec partners with best-of-breed firewall and security appliances to identify threats, then automatically quarantines the suspect device helping organizations avoid lost time and unnecessary disruption to network services.

Future Proofing - maximize the longevity of your IT investments in a world of ever-changing protocols and constantly evolving security dangers.

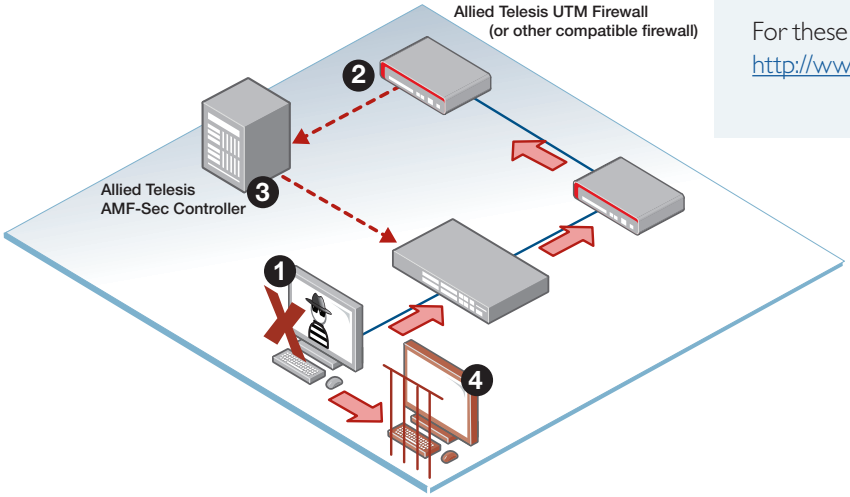
- The Allied Telesis solution allows for future network growth, both in total ports supported and in the uplink speeds that can be used. For example, allowing your current 1 or 10Gbps uplink system to be increased to 40 or 100Gbps in the future. The features within the key switches also allow for flexible configuration to accommodate the bandwidth and QoS requirements of future applications. Core L3 switches are also already capable of IPv6 in hardware.

Training - Allied Telesis can provide scheduled or bespoke group-based training on the equipment and configuration required within the solution.

Other documents you may be interested in:

Solutions:
Find out how our products and industry-leading features create solutions to meet your business needs.
How To Notes:
Find out how to set up and configure key features on Allied Telesis advanced switches and routers.
Success Stories:
Read customer success stories featuring Allied Telesis superior products and features.

For these documents and many more, visit:
http://www.alliedtelesis.com/library



1. Targeted attack inside the network! Threat information sent upline
2. Firewall sends threat notification
3. AMF-Sec instructs switch to shut down threat source
4. Infected device sent to quarantine

Technologies

A set of advanced technologies enable Allied Telesis switches to deliver high value solutions to your network. An overview of each of these technologies is provided - explaining what it does and how it adds value to your business.

Switch stacking with VCStack™

Switch stacking, known as VCStack™ on the AlliedWare Plus products, performs the following functions::

- Combines a number of switches to form a single managed 'virtual' chassis, reducing complexity on the management platform, as seen in Figure 1.
- A number of switches series support flexi-stacking, where any port/speed can be chosen as the stacking ports, enabling flexible deployment to suit the size and bandwidth needs of the network.
- Provides backup of management and configurations. If one unit fails, another will take over management. Configuration files are saved on at least two units.
- Simplifies configuration and increases resilience—all functionality is available across the stack, such as link aggregation, VLANs, etc.
- Reduces failure recovery time by simply setting the stack ID of the replacement and hot-swapping in place of the failed unit. As the configurations are held on another unit, no further reconfiguration is required.

VCStack simple concept

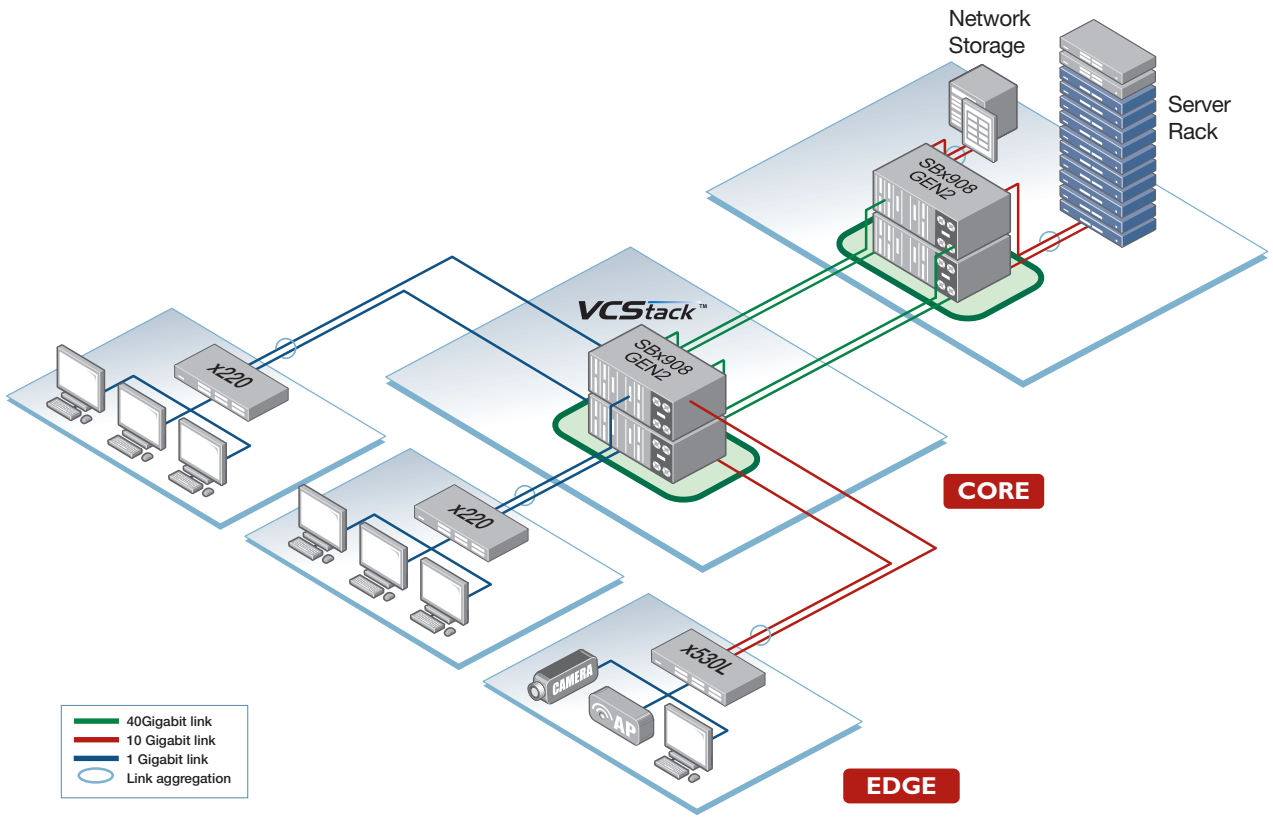


Figure 1

Split link aggregation resilience

One of the perennial problems of Spanning Tree Protocol for resilience is the fact that some links in the system remain blocked when the system is in normal operation, only becoming active when there is a failure. With bandwidth demands increasing on the network, split link aggregation lets the network make use of the full bandwidth of all the links in the network but still offer failover capabilities quicker than STP/RSTP. Switch stacking with functionality common across the stack is the key to deploying this technology.

As shown in Figure 2, links from ports on different switches in the core stack are connected to ports on different switches in the edge stacks. This is a simple deployment to understand and configure. If either a unit or link fails then the remaining link is used to continue network operations and both core and edge stacks can still be managed so the fault can be diagnosed and quickly corrected.

Another benefit of this approach is that if the core switch has L3 configurations then there is no need for further resilience protocols such as VRRP, since there is always a L2 link back to the core which will be acting as the gateway for the subnets attached.

VCStack core stack

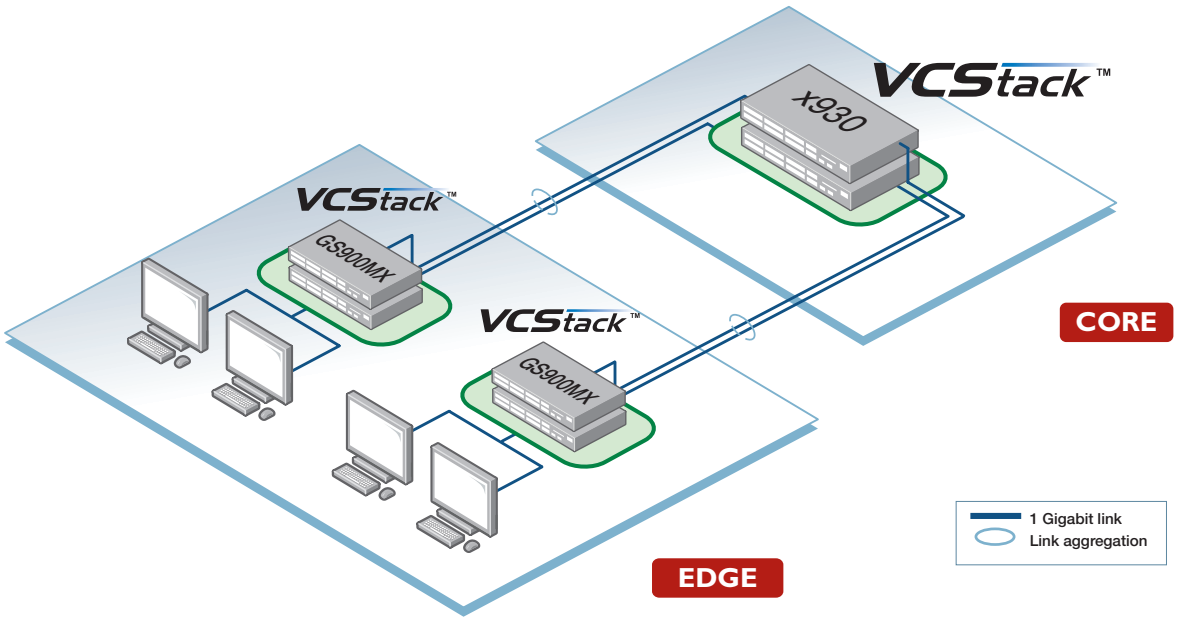


Figure 2

Storm control

The most common reason for outages in an Enterprise LAN is a packet storm caused by an inadvertent loop. Although resiliency protocols like STP are very effective in protecting networks from loops, they are still vulnerable to misconfigurations, and implementation problems.

Therefore, Allied Telesis switches implement a range of loop detection and storm protection mechanisms to contain and suppress storms if loops do occur.

- Rate limiting of flooded packets - broadcast, multicast, and destination-lookup failures - ensure that the switch does not spread the effects of a local storm to other parts of the network.
- Loop detection uses probe packets to detect packets returned to the originator by loops, and takes evasive action when loops are detected. (Available on x-series switches only)
- MAC thrash protection detects cases where one or more MAC addresses are being learnt on different ports in quick succession (indicating that packets from those sources are being looped) and takes evasive action. (Available on x-series switches only)

Tri-authentication, identity-based networking and NAC

A key to a secure LAN is to ensure that devices connecting to the network undergo an authentication process. The level of access that a device is given to the network can then be determined from its response to the authentication challenge. Allied Telesis switches implement a number of options for authenticating devices attaching to the network.

For guest users who have no 802.1x client in their PC, or who have an 802.1x client, but whose credentials are not known to the RADIUS server, there are two options:

- The first option is to place these users into a Guest VLAN for Internet access or basic server functionality.
- The second option, (available on x-series switches only), is to use web-based authentication whereby the LAN switch presents users with a web page into which they can enter a username/password. Based on the credentials entered into that web page, the RADIUS server will be able to inform the switch whether or not to give the user access to the network.

For non-interactive peripheral devices, like printers and scanners, which do not contain 802.1x clients, there is a third authentication method. The switch will fall back to MAC-based authentication. The MAC address of the peripheral device will have to be registered with the RADIUS server, so only peripherals that have been so registered will be allowed to access the network.

Authentication opens the door to identity-based networking. The switch can place authenticated users into a VLAN handed out by the RADIUS server, based on the user's identity. Doing this protects the network, not only from rogue users but also ensures that users can be placed into the correct VLAN with access rights relevant to their job. This removes management overheads associated with moves and changes or hot-desking so users can just plug in and start working. Moreover, web-authenticated users are able to roam within the network without needing to re-authenticate.

Network Access Control (NAC) takes the 802.1x with dynamic VLAN concept another level up the scale. Allied Telesis implementation supports Symantec (SNAC) and Sophos Advanced NAC network access control solutions.

In these solutions a NAC server (as shown in Figure 3) will handle the authentication process and will additionally check the PC client has the appropriate firewall, anti-virus, and software patches running to adhere to an enterprise-wide policy, before it grants access in the appropriate VLAN for that user.

Users not meeting the policy requirements can be placed into a 'remediation' VLAN so that the appropriate services can be installed and enabled. In this way the network can protect itself from attack.

Network Access Control

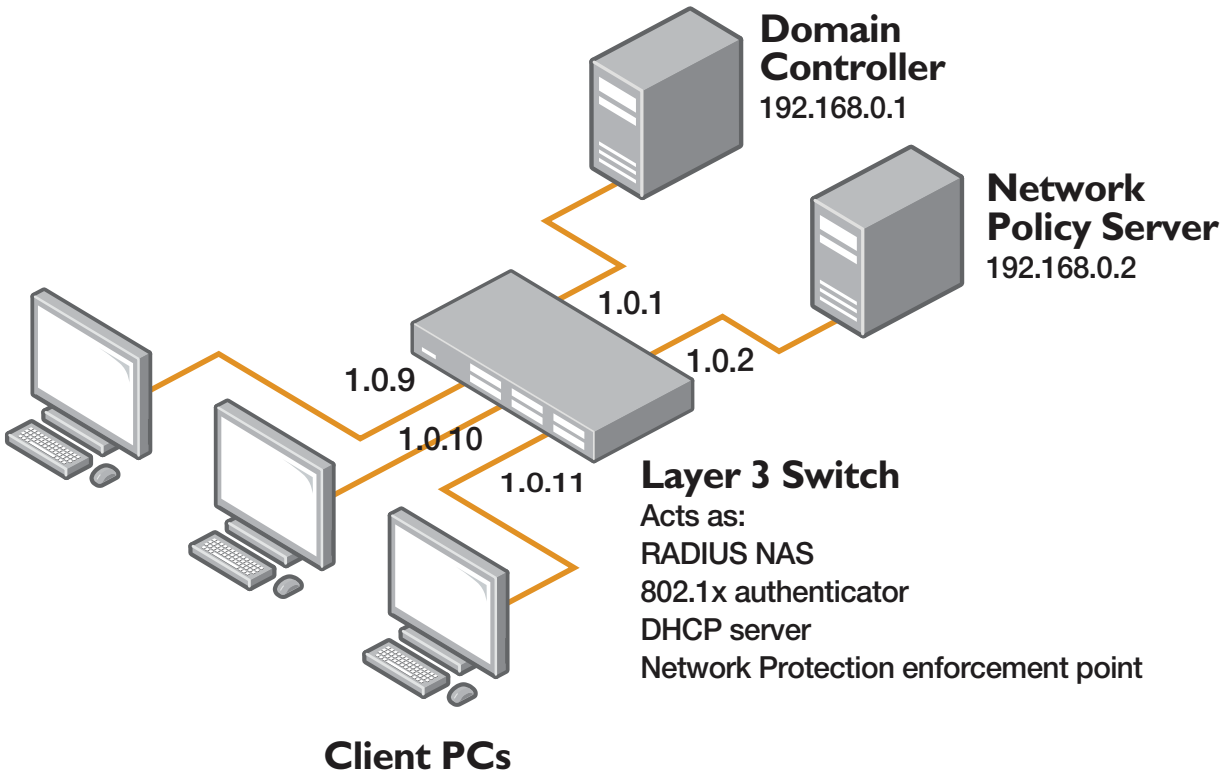


Figure 3

Quality of Service (QoS)

Whilst LAN networks are typically not limited by bandwidth these days, it is still sensible to ensure that even temporary network bottlenecks do not adversely affect those network services that are very loss and delay sensitive.

VoIP and video transmission within LANs are proving very effective in increasing the capability, and lowering the cost of business communications. These services, however, do require very good packet-delivery performance. The key to ensuring they receive the performance they require lies in QoS. If all switches throughout the network are configured to prioritize VoIP and video above all other traffic, then they will be unaffected by all but the most serious network congestion events.

Allied Telesis switches provide a very feature-rich QoS implementation. All switches are able to prioritize traffic based on 802.1p and DSCP marking. Multiple egress queues on all ports provide the ability to give multiple different levels of service to different traffic types. In addition, x-series switches can perform fine-grained classification of traffic types, and marking of packets with QoS values that designate their level of prioritization.

All this QoS activity is performed at wirespeed, with no CPU impact.

Layer 3 core switching

As networks become larger the need for segmentation increases. Allied Telesis core L3 switches have state of the art performance and features for L3 networking. All forwarding is at full wirespeed in hardware, including IPv6. Key features required for enterprise networking to meet today's needs are:

- Standards-based protocols such as RIP, OSPF, and BGP4 for interoperability with other key network devices.
- Equal cost multi-path routing support in hardware to guarantee the most efficient use of all network links.
- Flexible wirespeed hardware filtering via ACLs and QoS for traffic control and security.
- Future proofing with IPv6 routing already supported in hardware.

Using L3 for larger network designs protects these networks from the effects of broadcast storms and aids in rapid location and resolution of problems. L2 resilience is also aided by reducing the size of broadcast domains and the risk of CPU overload causing problems with L2 resilience.

Multicasting

Reliable and effective video transmission on a LAN requires the LAN switches to provide a good set of IP multicasting features.

Allied Telesis switches offer an excellent implementation of L2 and L3 multicasting.

The IGMP querier and snooping feature-sets on the switches are right at the forefront of industry best-practice (which has moved well ahead of the published standards). Per-VLAN snooping, query solicitation, fast-leave, and group filtering all combine to provide a multicast handling capability that matches any requirements.

The PIM implementation supports both Sparse-Mode and Dense-Mode, and has been well field-hardened to provide extremely reliable, high-performance L3 multicasting.

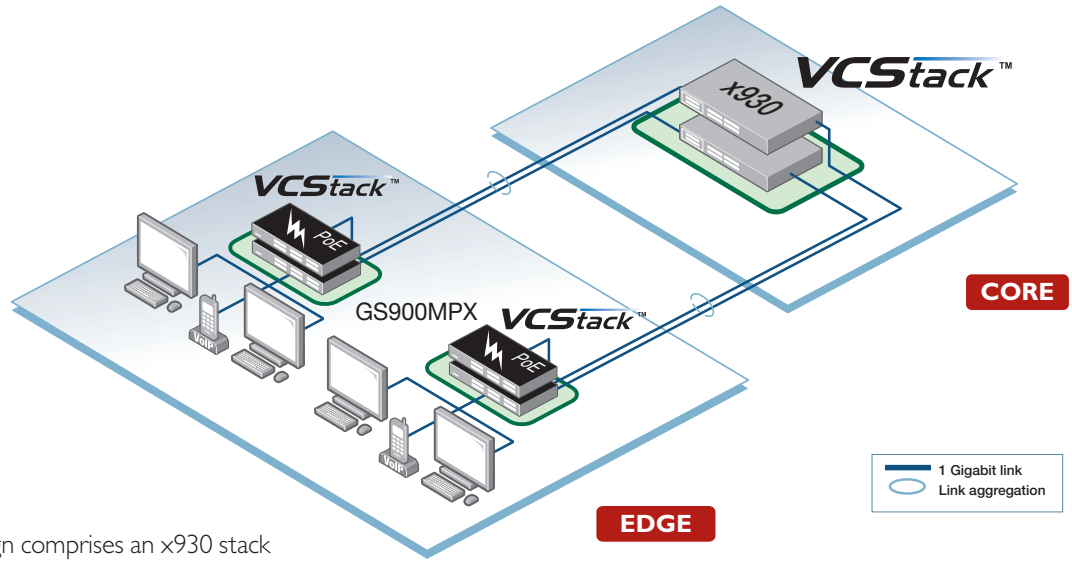
Network Designs and Scaling

The feature-set available on the Allied Telesis LAN switch range supports the requirements of a broad range of business networks. Different networks, of course, are going to need networks at different price and performance points. In addition, networks have a variety of physical connectivity requirements—Copper vs Fiber, PoE vs non-PoE.

Allied Telesis are well aware of these varying requirements, and so offer a range of products and solutions that can satisfy these different needs.

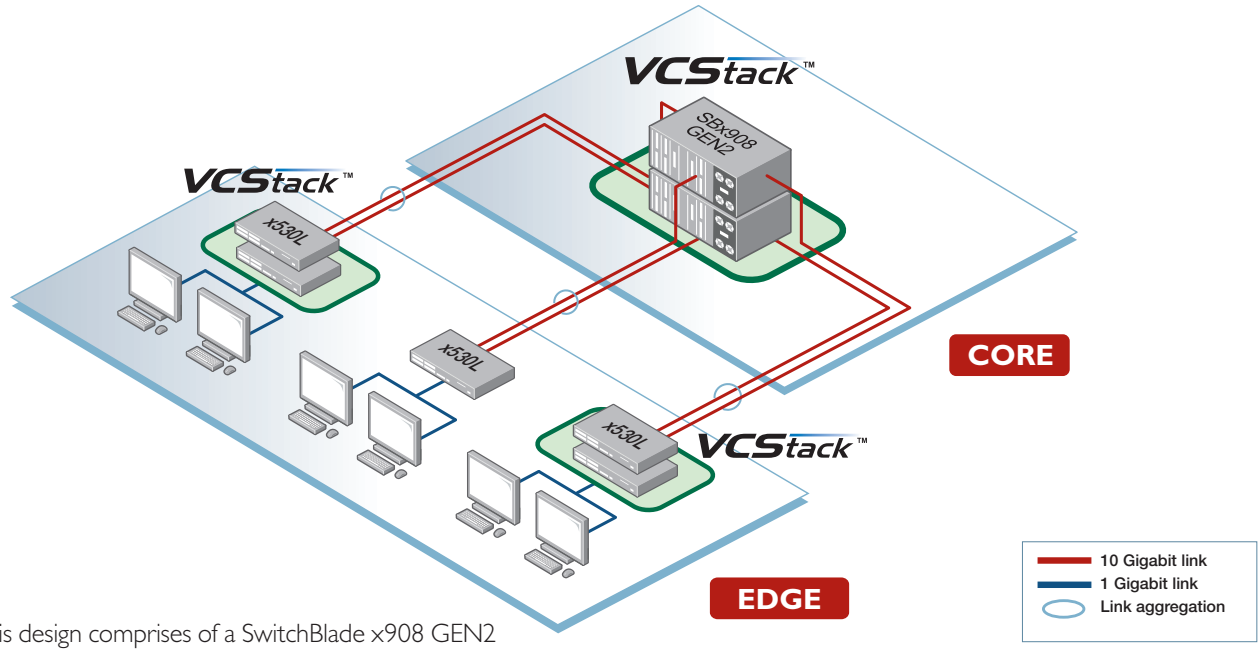
In this section, a set of product and design combinations are presented, which provide an illustration of the range of requirement combinations that can be satisfied by the Allied Telesis LAN switches.

1. Medium speed core and with Gigabit uplinks, Gigabit to the desk



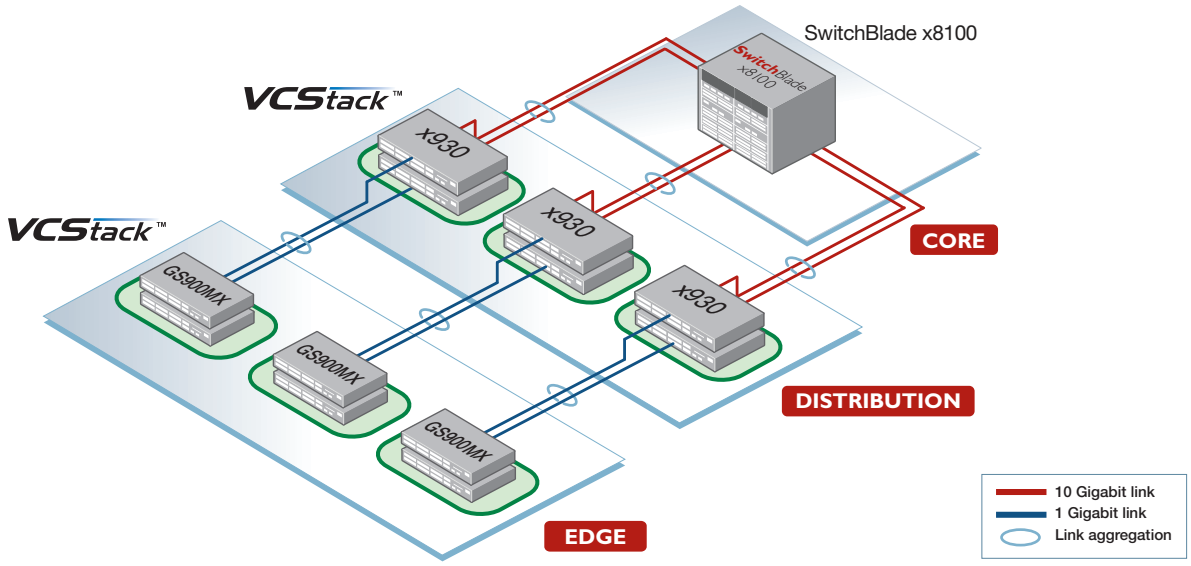
This design comprises an x930 stack at the core with GS900MPX stacks at the access layer with multiple Gigabit links to each stack. PoE provides power for IP Phones.

2. High speed core with 10 Gigabit backbone and Gigabit to the desk



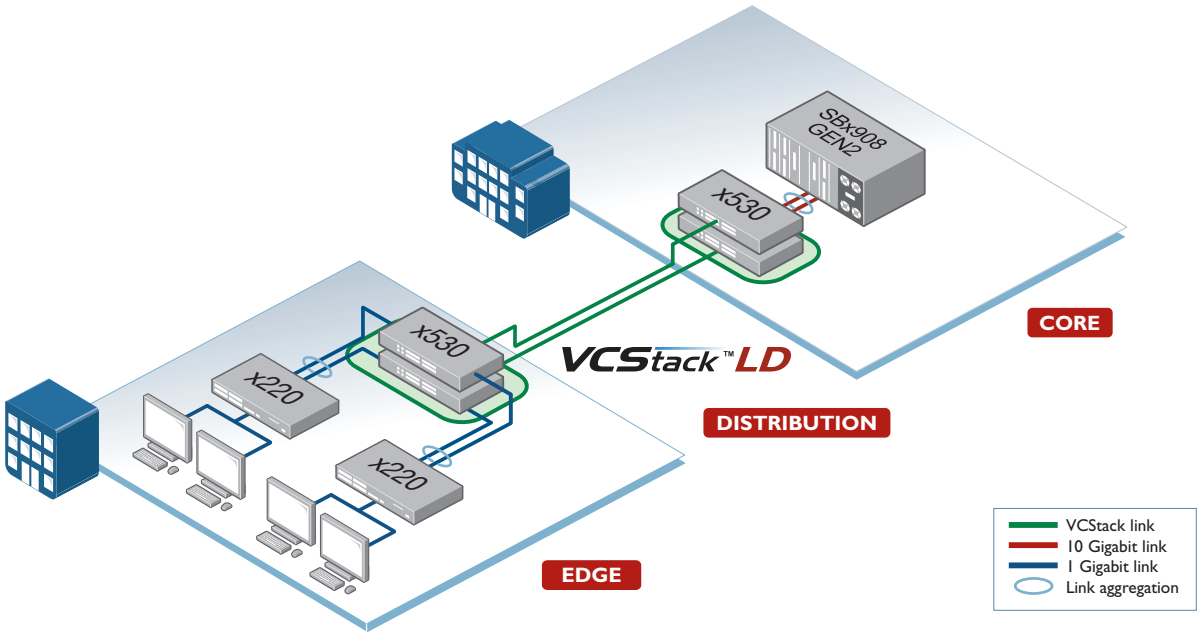
This design comprises of a SwitchBlade x908 GEN2 VCStack at the core with x530L stacks at the access layer using 10 Gigabit uplinks.

3. Three tier model–high speed L3 distributed core, L2/3 distribution layer and Gigabit to the desk



This design comprises of a SwitchBlade x8100 at the core, x930 stacks at the aggregation level and GS900MX stacks at the access edge - showing how L3 resilience combines with basic split link aggregation.

4. Distributed network with long distance VCstack



This design has a SwitchBlade x908 Gen2 at the core, and uses long-distance stacking (VCStack-LD) to connect a remote location, with distribution x530 switches acting as a single virtual unit.

Network Management Software

Allied Telesis devices can be managed individually with a direct connection to the units for configuration via console, Telnet, SSH, and the web-based Device GUI.

For centralized network automation and management, Allied Telesis Autonomous Management Framework, and Vista Manager EX enable a powerful and easy-to-use solution.

AMF™

Autonomous Management Framework™ (AMF)

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 organizations 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.

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.

About Allied Telesis

For more than 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™ (AMF) 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™

C618-31015-00 RevF