White Paper

Allied Telesis

Reducing the burden of network management

Introduction

Ethernet networking has developed at an immense rate in the last 20 years. Not long ago, an Ethernet network consisted of a length of coaxial cable punctuated by BNC connectors.

Now, Ethernet networks consist of switches with a plethora of features. Even Layer 2 switches have a raft of features for security, resiliency, performance optimization, loop protection, and network management, etc. When it comes to Layer 3 switches, of course, the feature-set becomes even richer.

Managing a large network of feature-rich equipment is not without expense. Many organizations are faced with a dilemma—do they pay big dollars for skilled specialists to optimize and maintain their Ethernet infrastructure; or do they keep the network simple, and ask the server administrators to manage the Ethernet infrastructure as best they can?

Even if the network configuration is kept relatively simple, maintenance tasks on a large network can be difficult and error-prone. It is time consuming and disruptive to carry out maintenance such as software upgrades, address renumbering, and security policy changes, etc. across dozens of switches. It is easy to make an error somewhere along the way. Network configuration errors can manifest themselves as annoying intermittent problems that take days to track down and resolve.

Software Defined Networking (SDN)

Software Defined Networking (SDN) has attracted a great deal of attention for its claims of solving a number of common networking problems, namely: simplified network management; optimized link utilization; and use of cheaper commodity switching hardware. Until now, most of the examples of how SDN actually achieves any of these have applied only to large data center environments.

In data centers, the network, servers and storage are the core of the business. Maximizing the performance and flexibility of that system provides their competitive edge. Hence data centers are adopting emerging SDN technologies.

They are investing considerable capital and time to implement these technologies in their environment, and to maintain, enhance and upgrade them. As the array of competing solutions are coming to market, different cloud computing providers are backing different solutions as the one that will give them a competitive edge for at least the medium term.

But, these solutions are not really aimed at simplifying day-to-day tasks like replacing failed units, rolling out firmware upgrades, etc. Rather, they are aimed at enabling networks to respond to the needs of highly virtualized servers.

SDN for the Enterprise

Currently, outside of the data center, the requirements for extreme network responsiveness and flexibility do not exist. Investment in the tools and expertise required to achieve a data center-like network solution simply is not justified. The risk of choosing an unsatisfactory vendor in a market where the clear long-term players have not yet shaken out is very hard to justify.

The growth of the data center market has not yet greatly changed the nature of the problems that need to be solved outside of the data center. Surveys of Enterprise network administrators repeatedly highlight that they face the same pressing problems:

- security
- reliability
- ease of management
- reduction of power consumption
- integration of real-time services (voice and video)

One of the claimed advantages of SDN is the promise of centralized management that treats the network as a single virtual device. In fact, at present, SDN is not providing the simplified management that Enterprise networks need.

Allied Telesis Management Framework

Simplified network management

In the recent "2013 SDN Survey: Growing Pains" by Information Week*, 53% of network administrators wanted SDN to "automate more provisioning and management" in their networks. Other sources have shown that up to 60% of network administration consists of repetitive and mundane tasks that could be performed by less skilled staff, or automated completely. This clearly shows that day-to-day network management tasks are considered to be a major pain point by most network administrators.

The types of day-to-day tasks that soak up inordinate amounts of network administrator time are:

- configuration management
- deploying new devices (extending the network)
- replacing existing devices
- making configuration changes on multiple devices
- rolling out new firmware

In a modern converged network environment, employees rely on access to online resources and applications. With the complexity of modern networking equipment, changes on one device in the network can have a knock-on effect throughout the rest of the network, resulting in unacceptable network downtime. If a mistake is made, then troubleshooting the root cause of the problem can turn into a lengthy process. Therefore highly skilled personnel are required to perform these every-day tasks to avoid introducing network affecting issues, and ensure the availability of business-critical online services.

In an effort to reduce the risk of errors and to save time, many network administrators write scripts to perform the configuration changes. However scripting requires a high degree of skill too, and since the script is likely to be performing multiple configuration changes, it is necessary to comprehensively test the script before deployment. Testing the script requires a sandbox area of the network where changes can be made without affecting other users. However creating the sandbox requires additional resources and increased administration time.

Allied Telesis recognized these facts some time ago and responded by developing a framework to simplify the management of Enterprise networks. This framework is called Allied Telesis Management Framework (AMF).

What is AMF?

AMF is a sophisticated suite of protocols and management tools that provide a simplified approach to network management. Common tasks are automated or made so simple that the everyday running of a network can be achieved without the need for highly-trained, and expensive, network engineers. AMF enables an entire network to be managed as a single entity from any device within the network. This provides flexibility and resiliency should the management device become unavailable.

AMF can be overlaid on top of an existing network very easily; the physical topology of the network does not need to change. AMF will determine the optimal logical topology for its own control plane and will automatically maintain that. The other network devices only have to know which device is the AMF Master to be able to join the AMF network. The Master is responsible for managing the membership of all the nodes and is responsible for scheduling and storing the automatic configuration and firmware backups.

AMF simplifies these common network management tasks:

1. Backing up the network
2. Adding new units to the network
3. Recovering failed units with new units
4. Making configuration changes to multiple units
5. Rolling out a firmware upgrade

AMF delivers true centralized management of an entire network from any single device through a simple and intuitive Command Line Interface (CLI). Configuration files and firmware files are automatically backed up regularly and are available for regenerating failed devices; and configuration changes can be made on multiple devices at the same time. This combination of features enables AMF to lower network operating expenses by reducing the skill level required to maintain the network. One Allied Telesis customer has reported a 60% reduction in operational costs.

* http://reports.informationweek.com/abstract/6/11255/Data-Center/2013-SDN-Survey:-Growing-Pains.html

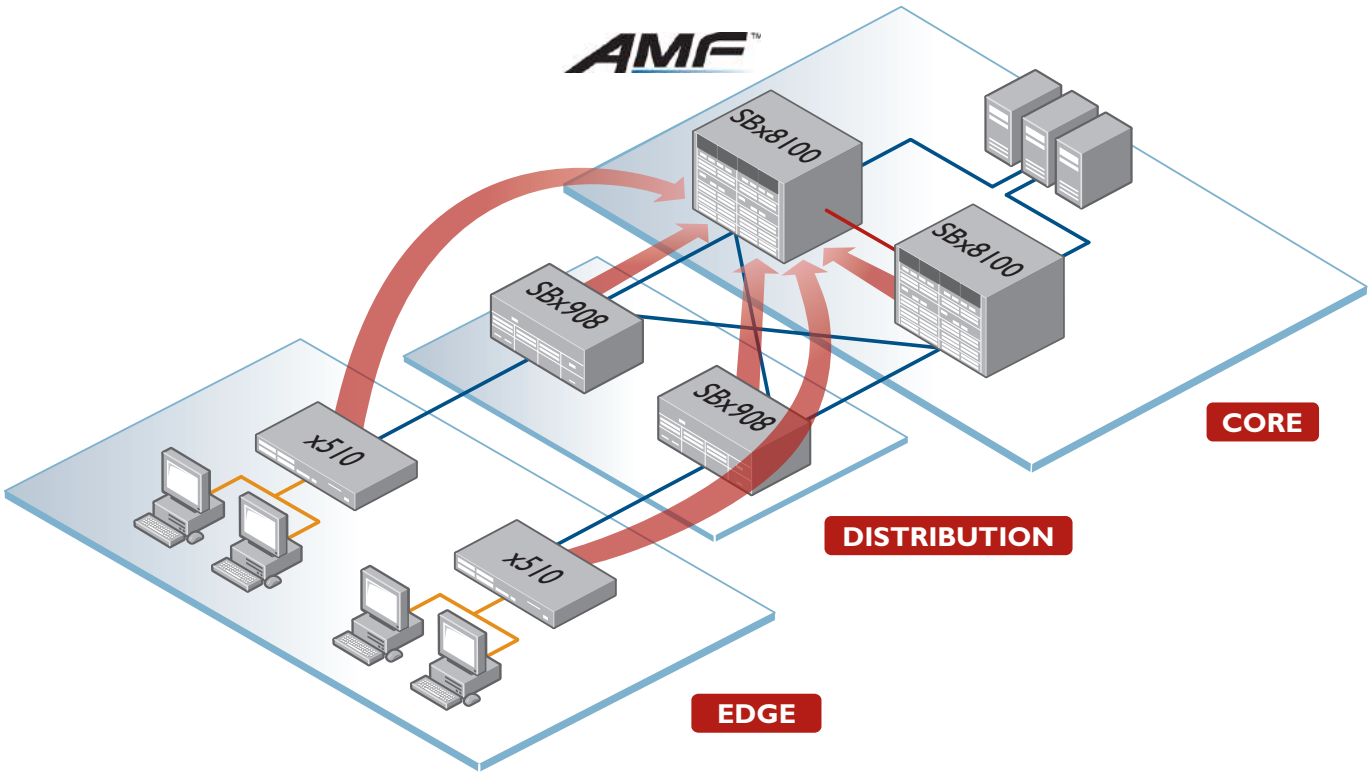
AMF Features

1. Backing up the network

Backing up a large network can be a complex and time-consuming task. The firmware version for each switch needs to be known in case a replacement is necessary. All current firmware versions need to be stored in an easily accessible location so they can be loaded onto new units if required. The configuration of each switch also needs to be backed-up as this may change quite regularly with updates to network topology, or for example, security policy changes. This configuration backup needs to happen regularly to ensure the very latest version is readily available.

With AMF, Auto-backup does a daily backup of the firmware, configuration, and other files important to switch operation such as scripts. These are stored on the AMF master, so are instantly available if required to load onto a new network device, or restore a current device.

Auto-backup removes a large time-consuming task from the network administrators, and provides peace-of-mind networking with the knowledge that there is always a complete and up to date network backup available.



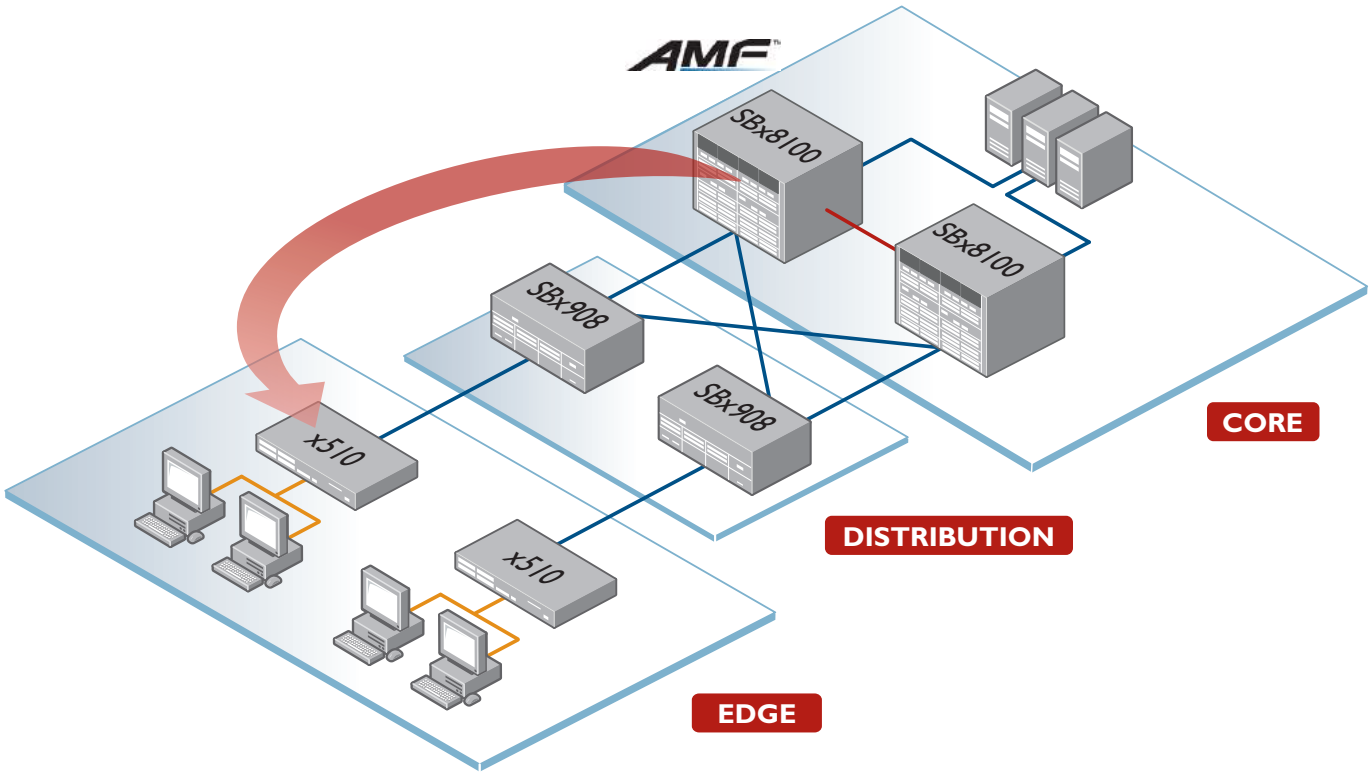
AMF Auto-backup

2. Adding a device to an AMF network

In traditional networks, adding a new device into the network requires that the device is pre-configured and tested before it is able to join. There is an inherent risk with simply adding an unconfigured device then attempting to configure it in-situ. It may cause unpredictable behavior on the network.

With AMF, Auto-provisioning allows devices to be added straight into the network. AMF will isolate the device until it has been successfully configured as an AMF node. When a device attempts to join the AMF, it sends a request to the master, which checks its membership database to either allocate a unique node name or check that the supplied node name is unique. If membership is accepted, then the node is allowed to join and its configuration and firmware files will be automatically backed up on the master each day from then on.

The configuration of the node can be handled automatically by the master or manually by the user. If automatic configuration is selected, another node's configuration will be used as a pre-defined template for the new node. In this way it becomes very easy to rapidly grow the network without increasing the burden of configuration management.



AMF Auto-provisioning

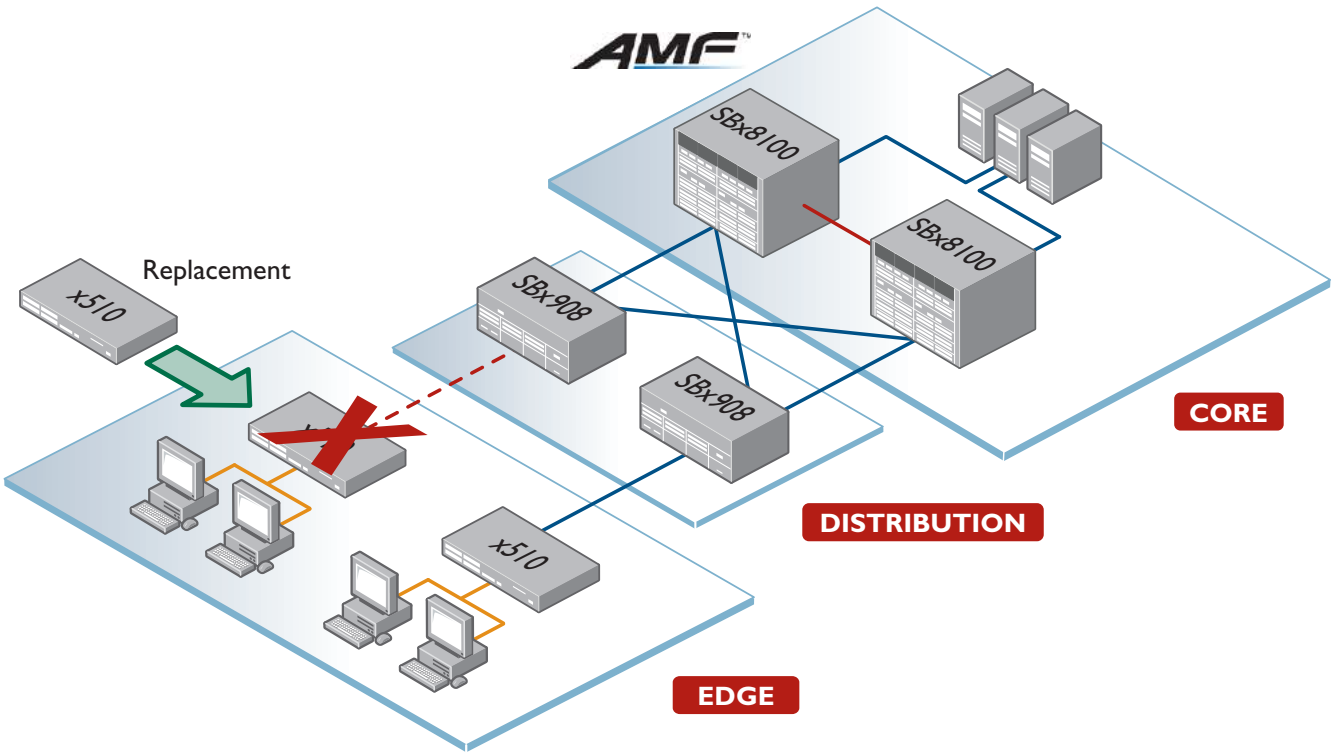
3. Replacing a failed device

The most common form of unplanned disruption to a network, other than traffic storms, is device failure. When this occurs, the network manager has to rapidly find a suitable replacement device and pre-configure it with the same configuration as the failed device (assuming it can be readily found). Then the device can be installed into the network and service can be resumed. This takes time and can lead to mistakes if the work is done hurriedly.

With AMF, if a device fails, Auto-recovery with zero-touch management enables quick and easy recovery. Another device with no configuration is all that is required. The new device is simply cabled into the AMF network using the same cables in the same ports as the failed device. When the new device is turned on, AMF will push the failed device's configuration and release file to the new device.

This will create a replica of the failed device. After the new device reboots, it should look exactly like the original device, with the same AMF node name and configuration.

The entire process can be completed in only a few minutes without any stress, safe in the knowledge that the re-configuration of the new device will be handled automatically by AMF.



AMF Auto-recovery

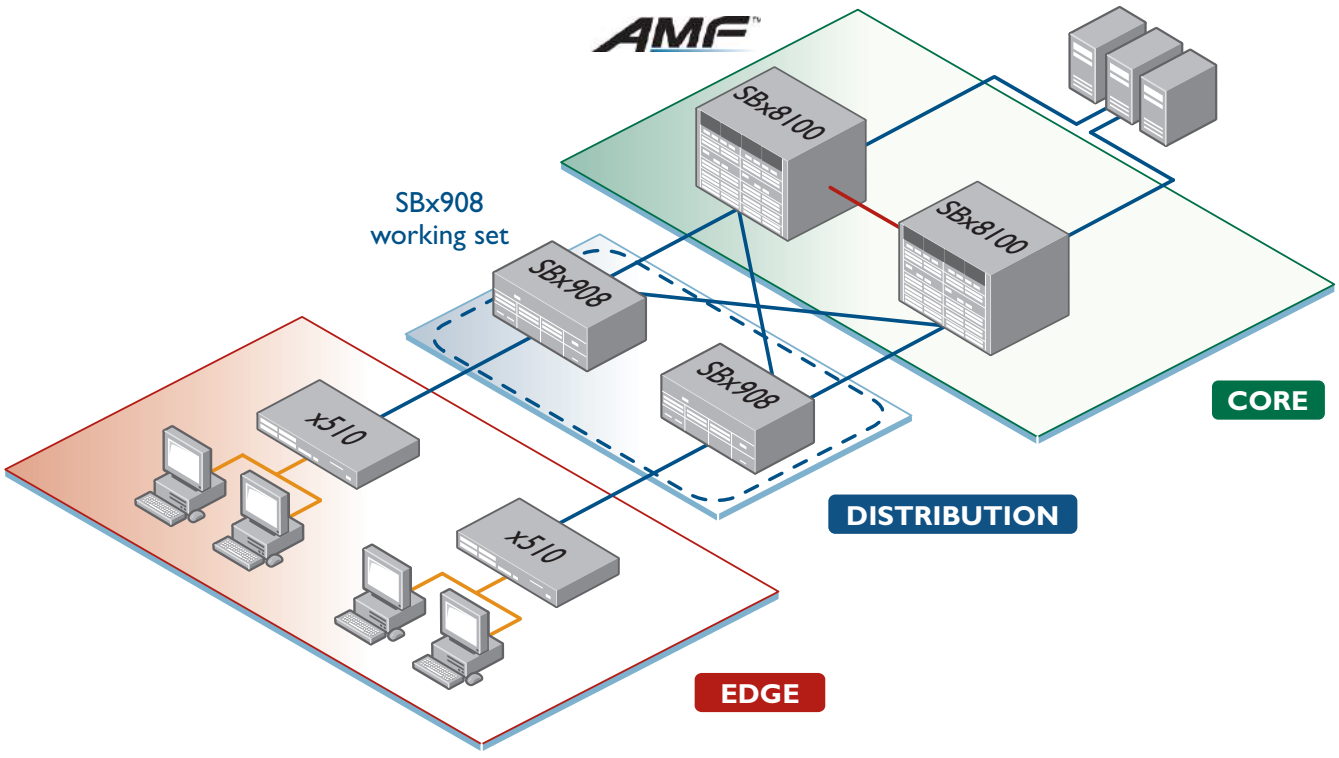
4. Configuring multiple devices

A powerful feature of AMF is the ability to run CLI commands on multiple nodes at once. This centralized management saves time when configuration changes need to be made across several devices. With AMF, the CLI commands are issued only once. AMF ensures each device receives and processes the commands.

AMF uses the concept of "working sets" of nodes that share some common characteristic, for example "edge switches" or "second floor". For convenience, some working sets are pre-defined, for example "x510", "SBx908" or "PoE".

To issue a CLI command to multiple nodes, the user simply selects the working set then starts running CLI commands as normal. Each node in the working set will receive the command and any output will be returned back to the user. Output from multiple devices is combined into a single easy to read entry. Errors are logged and returned separately so the user knows which nodes in the working set have executed the command successfully, and which have not.

Any node can be used to manage the AMF network, so working set commands can be issued from any node in the AMF network to any other group of nodes.



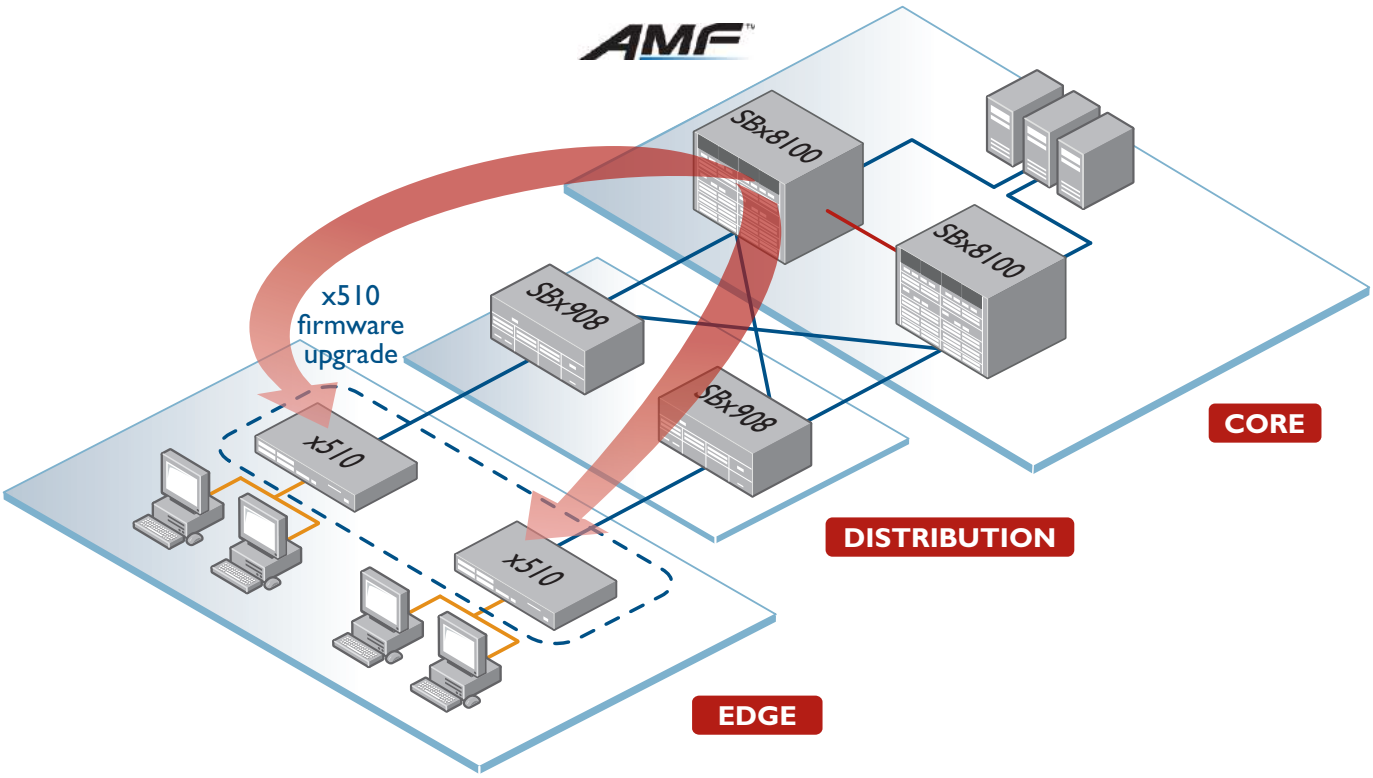
AMF Centralized management

5. Upgrading device firmware

In a similar way to the CLI working sets, Auto-upgrade allows firmware upgrades to be rolled out to groups of nodes or the entire AMF network quickly and easily.

The user selects or creates a working set of the group of nodes to be upgraded, then issues the CLI commands to load the new firmware release onto each device in preparation for a reboot.

Rolling reboot can be used instead of rebooting all nodes at the same time. Rolling reboot ensures that only one node is rebooting at any one time, so maximum network connectivity is retained throughout the firmware upgrade process. Of course, the rolling reboot can be scheduled to run overnight if required to avoid disruption during the day.



AMF Auto-upgrade

AMF enhances existing features

AMF integrates with existing features to produce an improved solution offering. Advanced resiliency features such as Ethernet Protection Switched Ring (EPSRingTM) and Virtual Chassis Stacking (VCStackTM) can combine with AMF. These advanced Allied Telesis features produce highly resilient networks that are simple to configure and manage, leading to higher uptime and lower operating costs. AMF also integrates seamlessly with existing features such as SNMP, to ensure that traditional management tools can still be used, avoiding unnecessary replacement costs and expensive re-training. Network troubleshooting is enhanced by AMF's ability to issue commands to multiple nodes and view all their output immediately in one location, leading to faster and easier problem diagnosis.

Packet storms caused by unprotected loops are a prevalent problem in Ethernet networks. AMF relies on the inbuilt loop protection mechanisms in Allied Telesis products to prevent network storms:

- Spanning tree—IEEE standard protocols STP, RSTP, and MSTP
- Loop detection—switches transmit Layer 2 loop detection frames, and take action on receiving back their own frames
- MAC thrash detection—switches monitor the rate at which MAC addresses move from port to port, and take action if MAC addresses make multiple rapid transitions.

These features work in concert with each other to protect your AMF network from the disruption of network storms.

Next Steps

There are a number of features that will be developed in future versions of AMF:

- Data plane management
- AMF High Availability
- AMF across WAN links to enable centralized management of remote branch offices
- SDN integration to manage traffic flows

Data plane management

AMF maintains its own control plane to be resilient and loop free. No matter how the AMF nodes are physically cabled together, AMF will determine a control-plane topology and will maintain that throughout changes in the physical cabling.

A future development will extend this feature to include the data plane. The topology discovery and control of alternative paths will be extended from the management framework (AMF) to the whole data plane of the network. The advantage will be that users no longer need to worry about how to connect their network devices together, because AMF will manage the logical topology itself. If the physical topology changes, then AMF will react and will ensure that user data continues to flow.

AMF High Availability

AMF nodes are aware of their neighbors and the network connections they have. If devices are physically connected with resilience in mind, it is possible for a device to take over from another device should it suddenly fail. This feature will become part of AMF in the future and will offer the fast failover benefits of stackable devices without the restrictions of special cabling or device homogeneity.

AMF across WAN links

The current version of AMF is designed to be used in a LAN environment, however it is envisioned that customers will see the benefits of centralized, simple network management of remote locations too. For this reason, the ability to have an AMF network that spans WAN links will become a reality in a future version of AMF.

SDN integration to manage traffic flows

Ultimately AMF will incorporate the flow-based traffic management aspects of SDN to provide a truly end-to-end flexible and responsive network management platform. This enables the customer's business rules to be built into the network management software rather than being implemented in obscure scripts running on networking devices. This further enables customers to concentrate less on day-to-day reactive network management and more on managing their business, creating services and planning for the future.

Above all, Allied Telesis is committed to making network management easy, so although AMF will be a sophisticated and powerful solution, it will still be intuitive and easy to use.

Summary

Data networking continues to evolve rapidly, as it has for the last two or three decades. As technology continues to improve, so user expectations increase; new solutions are required to meet those higher expectations, thereby driving technology improvements, and so on.

On occasions, significant new concepts, like Software Defined Networking, come into play: offering the potential to solve a range of problems and leap technology forward. At times like this, it can be difficult to discern which benefits the new concept will bring in the short term, and which will emerge as the new technology matures.

As a leading vendor of Ethernet networking products and solutions, Allied Telesis is highly focused on delivering the benefits of new networking technology to our customers. We are doing this through the Allied Telesis Management Framework (AMF) development program.

About Allied Telesis, Inc.

Founded in 1987, and with offices worldwide, Allied Telesis is a leading provider of networking infrastructure and flexible, interoperable network solutions. The Company provides reliable video, voice and data network solutions to clients in multiple markets including government, healthcare, defense, education, retail, hospitality, and network service providers.

Allied Telesis is committed to 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 is delivering the benefits of Software Defined Networking (SDN) through its Allied Telesis Management Framework (AMF) technology.

Allied Telesis has identified simple centralized management as the immediate benefit of SDN for enterprise customers.

Allied Telesis Management Framework (AMF) delivers on the promise of SDN by centralizing and greatly simplifying tasks such as:

- Backing up the network
- Adding new devices to the network
- Recovering failed devices with new devices
- Making configuration changes to multiple devices
- Rolling out a firmware upgrade

Allied Telesis

the **solution** : the **network**

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

C613-08015-00 RevC