White Paper

Allied Telesis

The top 3 network management challenges

BALANCING ACTS IN THE ENTERPRISE NETWORK

Introduction

Organizations rely heavily on their data networks, yet the network goes unnoticed most of the time. Networking infrastructure is an essential component of any business operation, but it is generally not really appreciated or understood by the majority of an organization's staff or management. While users are very aware of any network failures that occur, nobody wants to invest too much money into preventing these failures before they happen.

In this way, network infrastructure can be likened to plumbing: everybody notices when water stops flowing or a leak occurs, but almost nobody thinks about it at any other time. Certainly, very few would see value in investing large amounts of time and money into maintenance and upgrades.

This lack of investment puts pressure on a network. And network failures—in particular security failures—can be very damaging, expensive, and difficult to fix.

Allied Telesis Autonomous Management Framework™ (AMF)
Allied Telesis has developed a network management framework designed specifically to solve the biggest problems that enterprise networks are facing today. AMF takes the unique approach of embedding the management framework into the network itself. By making the network more intelligent, AMF can simplify, and even automate, some of the most challenging and time-consuming tasks in network management.

AMF™

Today's top 3 network challenges

An organization expects its network to be reliable, secure, flexible, expandable and cost-effective. This means that IT teams must perform a series of balancing acts.

The three main challenges are:

- Flexibility vs. Security
- Cost vs. Capability
- Reliability vs. Growth

Flexibility vs. Security

Network security has had to adapt increasingly quickly, in order to keep up with the new ways that users and back-end systems work.

Mobility and variety are currently on the increase at both sides of the enterprise network. At the outer edge, users are operating a growing range of hand-held computing devices. At the inner edge, virtualized servers, new storage devices (NAS and SAN), and data backup mechanisms are replacing what used to be a simple cluster of static servers. Both user needs and business needs are adding new requirements to the list of features that a network must support.

New personal computing devices, with modern operating systems and brand new capabilities, are materializing at an exponential rate. Almost as quickly as a new technology is invented–even one that previously seemed like fantasy, for example making a video call wirelessly while walking around a building–it becomes a necessity. The era of static desk-bound PCs, running a prescribed OS image and a prescribed set of applications, has passed. The enterprise network must now be a more open platform.

This flexibility in end-point devices and applications brings security risks. Contemporary operating systems and data traffic allow the possibility of unique forms of viruses and cyber-attacks. In the highly competitive mobile device market, software is rushed into production as quickly as possible, further increasing the risk of security flaws being introduced.

The act of lifting restrictions on which devices can attach to the network also greatly increases the opportunities for rogue users to gain access. In the era of static desk-bound PCs, it was relatively straight-forward to create lists of allowed devices, and thereby deny connection to anything else. But, now that network users, and even network guests, can connect the devices of their choice, the process of authentication is a lot more challenging.

Flexibility at the inner edge is not quite as security-threatening as that at the outer edge. However, the mobility of virtual servers and storage necessitates more advanced traffic filtering methods.

Additionally, virtual servers and/or their data are increasingly being mirrored to offsite locations for disaster recovery. This introduces yet another piece to the network security puzzle.

Cost vs. Capability

New applications drive requirements for new capabilities within the network infrastructure:

- Multimedia applications require enhancements to network QoS, and the introduction of multicasting protocols.
- High-performance applications, for example high-definition video, high-end CAD and graphics applications, require enhancements to network bandwidth.
- New end-point devices such as wireless APs, VoIP phones, and surveillance cameras require the introduction of PoE and autoconfiguration protocols–for example LLDP-MED.
- Migration to IPv6 requires the introduction of new protocols into the network.
- The amalgamation of new services onto shared network infrastructure requires IP virtualization features such as VRF-lite.
- The introduction of e-commerce and other uptime-critical functions requires improved resiliency within the network infrastructure.

The more functions that converge onto the network, the more capable the network must be. However, enhancing network capability does not come cheap:

- New hardware needs to be introduced to increase bandwidth and PoE.
- New software releases need to be rolled out onto existing hardware, to provide the required new features.
- Configurations on the existing infrastructure need to be updated, to turn on new protocols.
- Cabling needs to be altered, to provide aggregated links or to upgrade to higher-spec cable types.
- Experts need to be hired to manage the more complex feature sets operating in the network.

Within most industries there is a drive to reduce the total cost of ownership of network infrastructure. So, IT staff must find ways to provide and maintain an increasingly capable network on a static or reducing budget.

Reliability vs. Growth

Networks are growing not just in complexity, but also in size. As more and more functions converge onto data networks, the number of devices attached to the network grows, and therefore the number of switching and routing nodes in the network must also grow.

Organizations need to attach more and more of their operations onto the data network–remote locations need connections into central sites; even locations with no staff need network links for surveillance cameras and/or environmental monitoring, and/or control of automated devices.

With growth comes more points of failure. More nodes to fail = more links to fail.

As a rule, the more remote the location of a failure, the longer it takes to resolve. This is particularly problematic for remote sites that have a number of affected staff, but no IT specialist onsite.

For global organizations, remote locations can be in other countries or continents. Maintaining reliable operation of a globally distributed network, that is supporting multiple important functions, is a challenging feat.

AMF can help

As an international network equipment vendor, Allied Telesis has direct knowledge of the challenges faced in a broad range of network environments. With almost 3 decades of experience in the industry, we have built up a wealth of insight into these main network challenges.

This knowledge and insight have fed into a network management framework designed specifically to solve the biggest problems that enterprise networks are facing today. AMF takes the unique approach of embedding the management framework into the network itself.

By making the network more intelligent, AMF can simplify and even automate some of the most challenging and time-consuming tasks in network management.

About AMF

AMF is a set of management functions that are encoded within the software of the network nodes themselves. Common tasks are automated, or made so simple that the everyday running of a network is achieved with considerably reduced overheads, and less opportunity for error.

AMF lets the network be managed as a single unit, by creating a cooperative management plane that unifies the operation of individual network switches.

Enabling plug-and-play networking and zero-touch management, AMF provides:

- centralized management
- auto-backup
- auto-upgrade
- auto-provisioning
- auto-recovery

How AMF solves the top 3 challenges

AMF takes on the top 3 challenges in operating enterprise networks in the following ways:

1. Efficient configuration change management
2. Automated recovery of failed units
3. Automatic provisioning of new units
4. Automated software upgrade

1. Efficient configuration change management

These challenges all feature a need to implement configuration changes across the network. Responding to new security requirements or adding new capabilities invariably requires reconfiguring multiple network nodes. Most often, the changes are required at the edge of the network–the largest set of nodes.

Configuration changes need to be performed quickly, accurately and consistently:

- Working quickly reduces outage windows, and avoids operating in a compromised mode where some of the network has been reconfigured and some has not.
- Working accurately avoids making errors that result in ongoing problems that can take hours, days or even weeks to track down and resolve.
- Applying the configuration consistently means that no ‘holes’ are left in the network. Adding new security configuration to 95% of edge switches is not good enough when you need the security to be upgraded around the entire network edge.

AMF provides the following tools to ease network configuration management:

A unified CLI
The network administrator can be logged into all, or a designated subset, of the nodes in the network simultaneously. Commands entered into this unified session are sent to all the logged-in units at the same time. This means that all the edge switches in the network can be included in a designated subset, and configuration commands can be sent to all those switches at the same time.

This has multiple advantages:
- the process of altering multiple unit configuration is sped up
- the possibility of forgetting to configure some units is eliminated
- the possibility of entering the configuration inconsistently on different units is eliminated

Automated configuration backup
All network nodes back up their configuration automatically to a central device at a configurable time interval. No external servers need to be added to the network, and no special commands need to be set up, to make this automated backup happen. The knowledge of how to perform the backup is embedded into the network switches by default and they will simply just do it.

2. Automated recovery of failed units

If a switch in the network fails, AMF makes replacement very simple. A replacement unit simply needs to be attached to the network, and AMF will take care of loading the right software version and configuration onto it. This is truly a 'plug and play' swap-out. The replacement switch does not need any preparation prior to being connected to the network.

This level of unit replacement automation shifts the balance between growth and reliability. Downtime in remote locations is reduced without the need to deploy more skilled IT staff. The task of plugging in the replacement unit can be carried out by people available at the remote site, who do not need to be IT specialists.

3. Automatic provisioning of new units

Just as the replacement of failed units is simplified by AMF, so also is the addition of new units to the network. When a new switch is connected to an AMF network, the management VLAN is automatically extended to this new unit. It is then immediately accessible for remote management from anywhere in the network.

If the network is being expanded at a remote location, the new switches can simply be shipped directly to that location, taken out of the boxes and attached to the network by whoever is available there.

Distant locations can expand their network without need for visits by skilled operators. The cost of network growth is reduced, without adding risk.

4. Automated software upgrade

Deploying new software across the network in order to provide new functionality has typically been a time-consuming task, and one that involves significant downtime and potential error.

AMF automates the process of upgrading software across a network. The new software images for the network nodes simply need to be collected together in a location, for example on a server drive or on a flash drive, that is accessible to the network. Then a single command is entered on the unified CLI and the software upgrade rolls out across the network.

AMF manages the upgrade in a controlled fashion. Switches are upgraded one at a time. Each switch is rebooted after upgrade, and the success of the upgrade is tested. If problems occur, AMF will recover the network back to a stable state.

This automation of software upgrade reduces the cost and risk of increasing network capability.

Summary

From years of close involvement with our customers, Allied Telesis is well aware of the challenges in enterprise network management. We have created AMF as a framework that provides solutions for those problems, and embeds these tools into the network itself.

AMF provides practical solutions to the challenges that enterprise networks are facing right now. Moreover, AMF will continue to grow and evolve, to change and improve the way that networks operate in the future.

Visit www.alliedtelesis.com/amf for more information about how AMF delivers convenience, simplicity and reliability in enterprise network management, today.

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

C613-08017-00 RevB