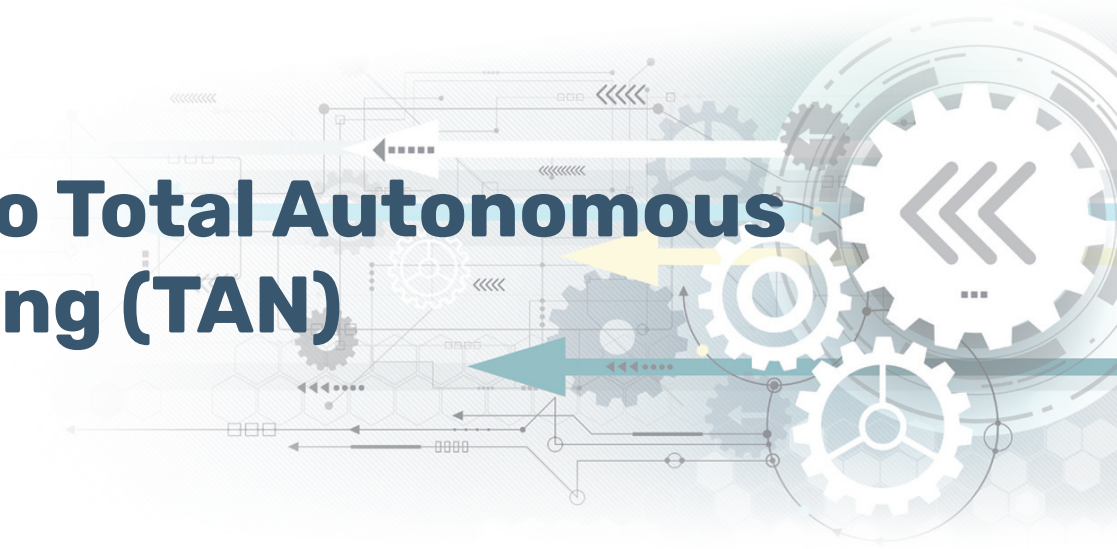
Allied Telesis



5 Steps to Total Autonomous Networking (TAN)

Introduction

As organizations strive to grasp the benefits of an ever-expanding array of technology solutions, the demands on their infrastructure become more and more challenging to manage. Business stakeholders want agility, security, reliability, scalability and a host of other capabilities, with an expectation that costs will stay the same or even lessen. It is the network that bridges the gap between the ideals of the business world and the harsh realities of cost, risk, and physics.

Conventional network management requires skilled resources, particularly at the network edge, doing repetitive or time-consuming tasks. As networks increase in size and complexity, so do the demands on network administrators, to maintain a secure, reliable and agile business tool that keeps pace with an ever-changing commercial landscape.

Stakeholders expect a rapid response to change requests, so network administrators have less time to make more changes, which increases the risk of mistakes.

More recent studies[2] report that up to 70% of data center outages can be attributed to blunders. Growth in network size and the variety of services they deliver have increased the risk of misconfiguration and the impact of such mistakes. Gartner[3] estimates the average cost of an outage at $5,600 per minute, depending on business type and criticality of the service.

The problem is that networking has its origins in the early days of computing when bandwidth was scarce, and security wasn't even a consideration. Although technology has advanced since then, networking has fallen behind, leaving administrators to craft solutions with inadequate tools, creating complex ad-hoc systems that aren't always as reliable or secure as we want.

In this white paper we look at the most time-consuming and error-prone network management activities and suggest five steps an organization can take to adopt network automation and build a reliable, secure and agile network capable of delivering the services that stakeholders demand.

In 2014, Gartner commented that "the undisputed #1 cause of network outages is human error"[1].

Step 1 – Automate configuration management

Most enterprise networks consist primarily of switches that efficiently direct traffic according to rules defined by the network administrator. Configuration files loaded onto each switch contain these rules, in the same way as a program 'configures' a computer how to behave. Complexity arises because each individual switch must be correctly configured - one mistake can introduce issues or vulnerabilities that can degrade performance or security. These mistakes can be difficult to find and may not be noticed until subsequent upgrades or audits are performed. In addition, each switch interacts with its neighbors and adapts its behavior based on traffic conditions. In other words, they are real-time devices responding to external events. This also complicates troubleshooting and can multiply the effects of an error across an entire network.

Managing configuration changes to ensure the correct configuration versions are stored and restored reliably is a significant portion of a network administrator's duties. The process is arduous and error-prone and requires significant skills and discipline to master. This is also true when upgrading firmware, or adding and replacing devices in the network, which has the potential to limit the agility and flexibility of a business to make changes to their networks since they are relying on a few skilled individuals to design and implement the necessary reconfiguration.

Configuration management becomes even more of an issue when dealing with sites that are distant from an organization's head office because those same skilled resources are usually required on site to replace or install equipment to avoid costly mistakes and downtime. Sending a skilled resource to a remote location is time-consuming and costly, but preferable to the risk of an unskilled person attempting to make the changes instead.

In summary, common configuration management pain points for network administrators include:

- Device configuration across multiple devices because mistakes can lead to outages and lost productivity
- Managing configuration changes and maintaining up-to-date firmware versions and security patches on all network devices is time-consuming and can lead to downtime
- Installing or replacing devices requires skilled resources, which can be expensive and time-consuming if devices are in remote locations

Fortunately, tools are available that work with network devices to resolve these issues by automating many common and repetitive tasks. Typically, the administrator configures the automation tool to backup network device configurations at regular intervals, which saves time and reduces the risk of using an incorrect version. Some tools allow for comparisons of configurations to quickly audit changes. Oftentimes configuration change management is a requirement for large networks.

A particularly useful feature is the ability to install or replace devices in the network and configure them automatically. Referred to as zero-touch provisioning, this feature removes the need to have skilled resources on site, which saves time and money.

Network automation tools offer a solution for common configuration management issues. By automating the everyday tasks of configuration management and simplifying deployment of new or replacement devices, the opportunity for mistakes is reduced, and skilled resources can be better utilized.

Recommendation: A significant amount of administration time is consumed managing configurations and firmware updates, which could be better spent on proactive tasks. In addition, the risk of introducing errors means many changes are deferred because the perceived risk is too high. Organizations looking to become more cost-efficient and agile should consider an automated network management tool that integrates configuration management with zero-touch provisioning to reduce the risk of human errors and enable easier implementation of network-wide changes.

Step 2 – Automate Wi-Fi optimization

Wi-Fi is undeniably a critical business tool for convenient mobile connectivity for users and smart devices. In fact, the convenience it offers means we tend to overlook its occasional, but potentially damaging flaws - dropouts, pauses, and reconnections. For personal use, we accept that convenience outweighs reliability, but business systems demand a more robust solution.

The problem with Wi-Fi is that it operates in a dynamic environment, where many factors can influence the users' experience. Since it's a radio-based technology, a good signal is essential. Radio coverage and interference both have major effects on throughput and reliability, and the placement of Wi-Fi access points is critical to achieving the best experience for all users.

Wi-Fi is also a shared medium, meaning that, unlike a wired network, users must share the air with others. This can affect performance, as other users can hog bandwidth or slow connection speeds to a crawl. Legacy devices can unwittingly reduce performance because network speeds reduce to accommodate them, lowering performance for all other users as well.

Network administrators must mitigate these potential risks to good performance by careful planning and continual monitoring of users' experiences. This takes time and requires skills to get it right and keep it working. Wi-Fi is susceptible to external interference too, so if your neighbor deploys a wireless LAN then it may undo all of your careful tuning!

Fortunately, wireless manufacturers are aware of the difficulties of operating a successful Wi-Fi network, and often provide planning tools to help create the best access point layout for optimum radio coverage and monitoring tools to adjust radio channels and signal strength to compensate for external interference. The most useful tools provide a graphical view of the wireless network and its current performance, so the administrator can see at a glance if there are any issues.

Troubleshooting Wi-Fi problems can be time-consuming, so having an integrated suite of tools and dashboards is essential to help keep the wireless network running smoothly. Alternative radio technologies exist that can dramatically ease the problem of interference and can accommodate legacy devices without performance degradation. When integrated into a single management tool, this can simplify administration even more.

Recommendation: There are many Wi-Fi solutions available and organizations need to carefully consider their choices. If organizations are experiencing performance or connectivity issues with their current system, then they should consider a solution that provides automated optimization and the option of using a different radio technology to avoid interference.

Step 3 – Automate WAN traffic management

Managing a modern Wide Area Network (WAN) infrastructure can be costly and time-consuming. Modern applications like Voice over IP (VoIP) calling, video conferencing, streaming media and virtual desktops need low latency while other applications demand ever-increasing bandwidth. Expanding WAN capabilities can be expensive and dealing with multiple management tools and network issues is both frustrating and difficult.

Traditionally, organizations wanting a reliable WAN infrastructure would purchase leased lines or dark fiber to ensure that their traffic is delivered within guaranteed Service Level Agreements (SLAs). Although this approach works, it is expensive and inflexible. Adding or removing capacity takes time for new services to be provisioned and relies on third parties to be responsive.

Today's organizations need agility and cost-effectiveness to remain competitive. Legacy WAN infrastructures struggle to deliver the levels of flexibility and value required. This issue resulted in the development of a new approach to WAN traffic management that aims to provide agility and flexibility with cost controls demanded by modern businesses.

Software-Defined WAN (SD-WAN) is a technology that enables organizations to use their existing customer-premises equipment, with low-cost WAN and Virtual Private Network (VPN) connections, to create managed multi-site networks with minimal administrative effort.

SD-WAN provides the potential to build higher-performance and lower-cost WANs by removing the need for expensive dedicated links and automatically distributing and load balancing traffic over many low-cost commodity link types, such as wireless and broadband. Operating costs are lower, and infrastructure is more resilient, with more independent traffic paths to choose from.

SD-WAN also enables rapid branch office deployment. By embracing automation, new sites can be set up in minutes with a single, centralized management tool, and consistent WAN security policies can be created and managed easily across all branch offices/remote locations.

More sophisticated implementations of SD-WAN offer application optimization, which ensures that critical applications like voice and video always have the traffic bandwidth and link quality they require. This ensures critical applications can deliver the best possible user experience for efficient and reliable business operations.

For additional convenience, SD-WAN and security can be combined into one integrated solution for easier management with just one dashboard to monitor all WAN activity. Traffic can be load-balanced across multiple secure VPN tunnels to make optimal use of available bandwidth to ensure the secure and reliable delivery of sensitive business data.

For a long time, organizations have had little choice about how to create a low-cost and reliable WAN infrastructure. SD-WAN has changed that and offers many benefits to enterprises seeking agility and cost control. When combined with industry-proven firewalls, it becomes more secure and is even easier to deploy, leading to increased agility and cost-savings.

Recommendation: SD-WAN should be considered by any distributed organization looking to reduce WAN operating costs and increase agility. A solution that has security built in will simplify management and reduce costs further.

Step 4 – Automate edge security

Everyone is well aware of the risks of cyber crime from illegal infiltration of corporate networks, yet breaches continue to happen.

In the first half of 2018, more than 4.5 billion records containing sensitive personal or business information were exfiltrated via security breaches[4].

It is clear that current methods of securing sensitive data are insufficient and better protection is required.

The conventional way to protect an organization from attackers and threats is to use a firewall to inspect all traffic to and from the Internet. This is a very common design. However, its focus on external protection leaves the organization vulnerable to attacks from within which could be from mobile devices or files copied from external media. It should be noted that almost 50% of people who find an unknown USB stick will plug it into a computer[5], which bypasses firewall security completely.

To make matters worse, firewalls are only able to block suspicious traffic that is passing through the firewall itself, they cannot act upon the network device that is causing the problem; either requesting the unacceptable content or accessing the infected/sensitive files. All the firewall can do is alert the administrator to manually investigate and resolve. That takes time and resources – time for the threat to spread or time for the attacker to copy sensitive business information. When the network is under attack, time is of the essence. Millions of records can be extracted in seconds, so a five-minute delay waiting for an administrator to shut down the attack can lead to disastrous results.

What is required is an automatic shutdown mechanism that detects attacks and takes immediate action to prevent further damage. Ideally, the network would defend itself automatically upon detecting a security breach. Responses would be immediate, and the suspect device would be isolated from the network, preventing further damage and leaving other users to continue working unaffected.

The “Self-Defending Network” approach is most successful when the solution is integrated with existing networking equipment and tools, and does not introduce excessive overheads for management or operation. A vendor-agnostic solution is best suited for Enterprises, since most will have outlaid considerable capital on their firewall solutions and will be unwilling to replace them. The solution becomes even more attractive if it can operate on both wired network switches and wireless access points—the true edges of the network that are most vulnerable to attack.

Recommendation: Organizations concerned about network security should review their security practices at the edge of their network. If these are weak, then consider investing in an automated security system that can detect and block exfiltration attacks immediately but is also integrated with existing networking equipment to protect their investment and simplify management.

Step 5 – Program the network

Over the years, network devices have gained features, and management systems are smarter and offer more automation features and time-saving widgets. However, the network is still treated as an interconnected mesh of discrete devices that each have their own configurations and need to be managed individually for the most part. This costs time and resources and is extremely error-prone. As networks expand the cost to maintain them grows too.

Software-Defined Networking (SDN) is the industry term for network programmability, but it tends to be heavily associated with a specific protocol called OpenFlow. Although successful in the data center, OpenFlow applications for the enterprise are few and far between, because it is difficult to integrate with real-world applications. However, there are other ways to achieve a software-defined network.

Scripting has been used since networking began as a way of automating repetitive tasks. Today it is the Application Programmable Interface (API) that is the most appealing for enterprises because it uses familiar tools, requires little training, and jobs performed by existing scripts can be reworked and extended easily. Network administrators find that the API features align closely with those available from the CLI they are familiar with. So, they can achieve complex tasks easily with minimum programming effort.

Making the network programmable enables it to be integrated with other business systems. In a smart building for example, the API can provide access to information such as PoE device power consumption and sensor data (e.g. when a door opens, how long a light has been on). This enables a wide range of analysis and monitoring possibilities and enables intelligent control systems to use this data to optimize power consumption and reduce building running costs.

The other advantage of a programmable network is that it can be made to respond to network events and reconfigure automatically (also known as event-driven network programming). For example, if a real-time event occurs such as link-down, a range of actions based on the current state of the network can be taken to provide the best response to the problem.

Programmable networks provide a range of benefits for organizations seeking to squeeze extra performance from their network or looking to integrate it with their business systems for more efficiency or better visibility.

Recommendation: Organizations wishing to build future-proof infrastructure or looking at ways to optimize the management of a multi-vendor network should explore options for programmability. Investing in equipment that has a well-supported API will enable them to gain benefits today by developing bespoke solutions for improved efficiency or business integration and be well-placed in the future to adopt promising technologies such as intent-based networking.

Total Autonomous Networking (TAN)

Allied Telesis has been helping enterprises build secure, reliable networks for over 30 years. In that time, we have learned a lot about the issues administrators face. For many, their daily workload consists of routine tasks that soak up their valuable time, and inadequate tools that don't adequately protect them from the risks of mistakes.

To overcome these challenges, we have developed a powerful solution called Total Autonomous Networking (TAN) that incorporates a suite of automation functions to perform many of these tasks automatically or simplify them to save time and risk. Integrated with a single pane-of-glass dashboard, this tool reduces training time, reduces the chance of outages, increases agility and saves money.

The core of TAN is a management dashboard called Vista Manager EX, which provides complete control and visibility of all devices on the network. Integrated with an automation engine (Autonomous Management Framework™), it gives administrators the power and visibility to control their network with more speed and less risk. Feature-rich plugins provide extensions to automate additional aspects of the network such as Wi-Fi, SD-WAN and edge security.

TAN delivers an integrated and intuitive solution to support your automation requirements at each step towards the agile, secure and reliable network your organization needs.

Step 1 – Automated configuration management

TAN delivers real and immediate value to the enterprise by freeing up the time of network administrators, allowing time for proactive projects rather than reactive maintenance. Management control is centralized, and powerful automation enables firmware upgrades and network-wide configuration changes to be made quickly, easily and risk-free. Repetitive tasks are automated or simplified and zero-touch provisioning allows skilled resources to stay in the network operating center instead of wasting time traveling to remote locations to install or repair units.

Step 2 – Automated Wi-Fi optimization

Allied Telesis automated Wi-Fi solution combines innovative, easy-to-use management tool with an automated tuning engine, and a choice of radio technologies to give customers the optimal wireless experience. Delivering a No Compromise Wi-Fi solution is an effective alternative to the conventional one-size-fits-all approach.

Step 3 – Automated WAN traffic management

Combine the benefits of SD-WAN's application optimization with Allied Telesis industry-certified secure firewalls, for an easy-to-use security solution that optimizes and protects all WAN traffic. TAN enables organizations to manage and secure their WAN infrastructure from a single point, using the same single pane-of-glass management tool used by the rest of their network.

Step 4 – Automated edge security

Build a self-defending network with TAN that works with existing firewalls to take instant action if a threat is identified. Responses are fast and accurate, no manual intervention is required, and the actions taken are logged then presented visually to the administrator. Suspect devices can be automatically isolated whether they are on the wired or wireless network, ensuring there are no weaknesses anywhere across the entire network. Most common firewall products are supported, centralizing security policies from just one device, and saving the organization from additional expense.

Step 5 – Programmable networks

For ultimate control of the network, programmability is key. The AlliedWare Plus™ network operating system from Allied Telesis gives you the choice of an industry-certified OpenFlow implementation, and support for a RESTful API that is easy to use and freely available. This enables an organization to develop their own automated event-driven actions to provide an agile and flexible network infrastructure or integrate with business systems for increased efficiency and visibility to support business objectives.

Conclusion

Network administrators need help to make network changes rapidly without risk, and to have time to be proactive and innovative to deliver the benefits their stakeholders demand. TAN is a solution from Allied Telesis that aims to give administrators the help they need, without raising costs through the need for more resources or specialized skills.

To find out more about how you can start taking steps towards the many benefits of TAN, contact Allied Telesis.

[1] https://blogs.gartner.com/andrew-lerner/2014/07/11/network-downtime/

[2] https://www.cw.com.hk/it-hk/uptime-institute-70-dc-outages-due-to-human-error

[3] https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

[4] https://www.cbronline.com/news/global-data-breaches-2018

[5] https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots/

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

C613-08042-00 RevC