Allied Telesis

Five Steps to Network Virtualization and Transformation

Introduction

Today's businesses are operating in an increasingly competitive environment. Globalization means competitors are no longer just local - they can be anywhere around the world. New market entrants use technology to drive disruption and capture the market share from established players. Technologies such as cloud computing, Artificial Intelligence (AI) and the Internet of Things (IoT) are transforming the way organizations operate and compete. Further, not only does technology enable innovation and disruption, it also improves efficiency and gives organizations a competitive edge.

This white paper examines how the network underpins the ongoing global business transformation. Importantly, it looks at five key steps every organization must take to position their network, to take full advantage of technology now and transform their business for tomorrow.

The Continuing Importance of Network Planning

Cloud Computing, along with the increasing deployment of AI and IoT systems, network administrators must focus on the underlying network infrastructure. Industry watchers predict that IoT spending will grow 15% each year, reaching a staggering $1 trillion by 2020. By 2025 there will be over 80 billion connected devices, which will collectively generate over 180 trillion gigabytes of new data annually.

Just a few years ago, network planning was still predominantly focused on delivering reliable connectivity within the LAN and across the WAN. Today's conversation has moved well beyond connection reliability, turning instead to broader discussions on optimizing application delivery and performance from agile, self-managing, programmable networks.

Understanding the nuances of each application, along with who (or what) will be using them, is crucial when choosing the best medium or path with which to deliver the optimal experience. And with the rapid growth in connected devices, flexibility and agility are key to coping with the increasing network demands and ensuring the most appropriate path between device and application.

While basic connectivity may be taken for granted today, many organizations still operate a

plethora of different networks with limited or no interconnectivity.

The reasons for this are many and varied, but generally sit in one or more of the following categories:

- Applications and services are the responsibility of different business units, or outsourced to different providers
- The value that can be unlocked by converging networks and applications is not appreciated or understood
- A (misguided) belief exists that systems are more secure if they are not interconnected

Steps Every Organization Should Take to Position Their Network for the Future

One: Adopt IP Everywhere

Before embarking on an exploration of future technologies, it is important to look at the past and the changes that have occurred over the last 10 to 15 years with respect to applications, systems and connectivity.

Historically, each different system or application within an organization was delivered using separate communications cabling, separate technology hardware, and more importantly, a unique set of skills to deploy and manage - with little to no commonality across systems.

For example, a CCTV system used to require its own coaxial or fiber cabling for signal transmission, along with cable to deliver power to cameras, along with matrix switches and a bank of recording equipment for recording and storage of video. A telephone system used to require its own twisted pair cabling for signal transmission, along with a PBX for switching calls and interfacing with the PSTN.

Because there was no commonality in how systems were connected, deployed or managed, there was no efficiency or economies of scale that could be leveraged. This resulted in relatively high installation costs for labor and equipment, and high ongoing operational costs due to the uniqueness of skills required.

Although the Internet Protocol (IP) was developed in the mid 1970s, it wasn't until the 1990s and the development of the Internet and graphical web browsers such as Mosaic, Netscape Navigator and Internet Explorer that IP saw widespread adoption throughout government, academic and enterprise organizations.

Initially used for connecting desktop computers for file and print services and Internet access, it wasn't long before IP found its way into the telecommunications world as a means of transforming circuit-based carriage networks into packet-based networks, which resulted in some of the earliest examples of network convergence.

From there, IP PBXs soon made their way onto the market, along with other systems or applications that were IP-enabled such as video-conferencing, CCTV and Building Management Systems (BMS).

While IP is almost ubiquitous today, it is important to understand that for true convergence and virtualization, every application and system within an organization must be IP-enabled.

Two: Push for Network Convergence

Within the technology world, the word convergence has many meanings and over time has been interpreted to mean different things. In the late 1990s and early 2000s, convergence was a term that typically referred to using IP for voice, video and data services – generally over a common network infrastructure.

Today, convergence is more likely to refer to the convergence between Information Technology (IT) systems which are used for data and information-centric computing, and Operational Technology

(OT) systems which are used to control and monitor activity and devices throughout an organization.

Technologies such as network, storage and computing are generally recognized as IT systems or technologies. Systems such as Supervisory Control and Data Acquisition (SCADA) used within a manufacturing facility or utility, or a Building Management System (BMS) used within a commercial building are considered to be OT systems. Other examples of OT systems include CCTV, access control, energy management and fire systems.

The benefits of operating a single, converged network infrastructure are many, and include:

- **Less unnecessary duplication** – deploying multiple networks results in duplication of cabling infrastructure along with the associated switching equipment, which increases cost and decreases efficiency.
- **Lower space and power requirements (direct and indirect)** – operating multiple networks requires more space within communications locations, and needs more power for both operation and environmental conditioning.
- **Reduced administration (deployment and operational)** – deploying and operating multiple networks requires greater resources because of the number of devices that need to be managed, and may result in a need for additional skill-sets required if numerous vendors are involved.
- **Increased flexibility, scalability and agility** – operating a single, converged infrastructure delivers greater flexibility, scalability and agility to the organization. Adding a new device is more simple as there is only one network, and deploying a new application is faster as it doesn't necessitate deploying a new network.
- **Greater security** – the increasing adoption of IoT and the rapidly-growing number of connected endpoints means security is more important than ever. IT research and advisory company Gartner reports that nearly 90% of organizations with connected OT infrastructures have experienced a security breach with their SCADA/ICS architectures, with more than half of those breaches occurring in the last 12 months. Security is of paramount importance and can be implemented more consistently across a single converged infrastructure than multiple disparate networks.

It is important to recognize that network convergence is not just a technological challenge, but an organizational challenge. In order to deliver convergence there must be a strong alignment between different business units – particularly IT and OT – and ultimately only one owner of the converged infrastructure.

In addition to internal organizational alignment, it is important to consider convergence when engaging external organizations and agencies. Organizations routinely approach the market to procure systems and services by tender, and it is commonplace for new OT systems such as BMS or CCTV to be tendered in order to ensure consistent, competitive responses. To take advantage of convergence, to reduce the cost of acquisition and ongoing management, and to take advantage of the value that can be delivered, it is important that new systems operate over the organization's converged infrastructure rather than delivering yet another set of equipment to be managed.

By leveraging a single, converged infrastructure under the control of a single business unit, organizations can achieve significant IT/OT network performance improvements and efficiencies.

Three: Consider Network Orchestration

With the evolution of networking and the transition to tomorrow's network, there are still plenty of challenges to overcome in the networking realm. We have witnessed the convergence of IT and OT systems and improved alignment between different business units. Changes in the way business units behave and interact has also seen the role of the Chief Information Officer (CIO) evolve - from leading the delivery of IT, to a role that focuses more on getting the most from processes, information and

relationships across all technologies throughout the organization - including both IT and OT.

Operating a converged infrastructure delivers many benefits to the organization, and one of those benefits is a reduction in the number of devices that need to be managed. This can be taken one step further, using software to reduce the operational workload of configuration, troubleshooting and asset management - capabilities commonly referred to today as network orchestration. Orchestration allows the network to be managed as a single entity, which delivers benefits not only in terms of reducing workload, but also around improving consistency and security.

There is nothing worse than when things don't quite work right, knowing there is a definite cause but not quite being able to find it. Making changes to network elements discretely, one at a time, is fraught with danger as a single misplaced keystroke can result in changes to network behavior that can be time-consuming to eradicate. Orchestration technology does away with this challenge because the network is managed as a single, autonomous entity, and changes are made consistently and simultaneously to every device. This not only assists with eliminating pesky issues, but also in improving security by ensuring that security policy is consistently deployed across the entire network.

Industry research indicates that major security threats include viruses (77%), internal (73%) or external (70%) hackers, the leakage of sensitive or confidential information (72%), and the lack of device authentication (67%). And over a third are now concerned with the exploitation of backdoors built into connected IoT devices.

While orchestration technology won't eliminate these security breaches, the consistency it delivers ensures security policy is deployed consistently. Should a virus or attack be identified, updates to security policy can be rapidly deployed to mitigate the damage caused.

Managing the network as a single, autonomous entity is not the only benefit of orchestration technologies. Some vendors have extended this technology to deliver other benefits as well:

- **Automated provisioning** – allows untouched, unconfigured devices to be added directly to the network and automatically provisioned to reduce the time and skills required to deploy new services
- **Automated upgrade** – allows the automated upgrading of a group of devices or all devices across the network, and then performs a rolling reboot to maximize network connectivity during the process
- **Automated backup** – automates the backup and management of configurations for devices across the network
- **Automated recovery** – allows true 'zero touch' replacement of a failed device by simply connecting the device and powering it up - the network automatically recovers the device to the state prior to failure

Four: Plan for Network Virtualization

Network orchestration is primarily targeted at the network management plane. The emphasis is on overcoming challenges around device management, such as time and effort required to manage and improve consistency and security.

However network virtualization, otherwise known as Software Defined Networking (SDN), is the decoupling of the network control plane from the forwarding plane of network devices. It allows network control to become directly programmable, and the underlying infrastructure to be abstracted for applications and network services.

While the above paragraph is quite abstract in its own right, in essence SDN is about removing the decision-making process of how to forward network traffic from the underlying network hardware to a centralized programmable controller.

The increasing use of virtualized servers and storage and cloud-based applications, along with a need for scalability and agility, means today's applications must be better. And with the rapid growth in connected IoT devices and the sheer volume of predicted traffic, paving the way for the applications of tomorrow requires a fundamental shift in the underlying network technology. This is where network virtualization and SDN comes in.

Some of the benefits of SDN (and SD-WAN) include:

- **Greater security** – With growing concerns about security, particularly with the convergence of IT and OT, SDN can deliver greater security. Instead of relying on endpoint security or inspection at the network perimeter, SDN controllers make decisions about how and where to forward traffic on a packet-by-packet or flow-by-flow basis, which means they are far more responsive to changes in traffic patterns throughout an organization.
- **Better application experience** – along with security, one of the primary advantages of SDN is the ability to shape and control traffic on an application-by-application and flow-by-flow basis, improving networking responsiveness and delivering a better user experience.
- **Centralized provisioning** – decoupling the decision-making process from the underlying hardware and moving it to a controller makes having a centralized view of the network easier. By abstracting the control and data planes, SDN can also accelerate and simplify the delivery of new services - not just across the network, but across all virtual infrastructure from a single location.
- **Greater Flexibility and agility** – having the network controlled by a centralized controller makes it more agile, and facilitates more rapid change. The fact that the controller is programmable also provides an unimaginable degree of flexibility, allowing organizations to create networks that meet their exact application and business requirements.

While network virtualization and SDN are relatively new technologies, IDC predicts the SDN market will continue to grow at 25% year-on-year to 2021, and now considers that SDN is emerging out of the early adopter and into the early mainstream stage of its development.

Network administrators should prepare for the deployment and adoption of network virtualization technology by ensuring it is a requirement of any network or virtualization technology acquisition.

Five: Research and Monitor Intent-Based Networking

Intent-Based Networking (IBN) is an automated tool that helps network engineers plan, design and operate networks to improve agility and availability. Along with network virtualization, IBN is set to deliver a paradigm shift to the benefits delivered by networks. This technology, which Gartner Analyst Andrew Lerner has identified as the 'next big thing' in networking, promises to deliver more agile networks with fewer issues across heterogeneous devices. This in turn offers benefits such as reduced operational expenditure, continuously optimized performance, better compliance and an improved user experience. Where network virtualization delivers programmatic control of the network, IBN drives the network configuration algorithmically, so it can respond faster and scale larger than anything that relies on human intervention.

IBN allows the administrator to move away from configuring desired outcomes in esoteric device-specific command lines, and instead use a natural language or graphical interface to express intent. For example, they may want to prevent members of the engineering group from accessing sales data, or they may want to ensure there are always two separate paths between servers. Recent advances in formal verification techniques and modeling languages such as YANG have enabled IBN to become a practical solution to answer the question, "Is my network configured correctly?"

The key to IBN is the continuous cycle of verification and remediation, which constantly checks that network configuration meets business intent and makes corrections in real-time.

IBN consists of a number of components, each of which delivers benefits

- Management Dashboard configures the system (expresses intent) and monitors operation. Although IBN's purpose is to run the network autonomously, human intervention is required (and desirable) for some time yet.
- Intent Translation takes the "what" and translates it into the "how". Typical interfaces are either menu-driven graphical, or a more sophisticated natural language option.
- Network Verification proves that that translated configuration will deliver the desired intent with no security or reliability issues. This component uses formal verification tools to mathematically test and exhaustively prove that the configuration is correct.
- Remediation reacts to changes in real time, for example if a link fails, or a device goes offline. Capable of learning from past incidents and incorporating network best practices thanks to Machine Learning (ML), it can apply corrective actions to a wide variety of network issues. This is the newest area for IBN development and although great progress has been made, experts agree that for some time, humans will still be required to approve the corrective actions suggested by a remediation engine.

Arguably, the greatest benefit of the IBN solution is formal verification of the network configuration by the Network Verification component. This verifies that network configuration meets the intent, and ensures there are no security breaches or policy violations.

Take Full Advantage of New Technology and Transform Your Business

With increasing competition, there has never been a greater need for businesses to adapt and become more efficient. Fortunately, technologies such as cloud computing, Artificial Intelligence and the Internet of Things are enabling organizations to transform the way they operate and compete to achieve these goals.

Within the realm of technology, the network plays a pivotal role - it underpins the transformation that is taking place within businesses as they seek to become more agile and efficient, and 'do more with less'.

Of particular importance, network convergence, orchestration and virtualization deliver a multitude of benefits to organizations which include:

- Reduced capital and operational expenditure
- Greater flexibility, scalability and agility
- Better application experience
- Greater security

In addition to these benefits, following the five steps outlined in this document will allow organizations to remain at the forefront of technology adoption and stay ahead of their competitors.

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

C613-08041-00 RevB