White Paper

Allied Telesis

SDN and the changing face of Enterprise networks

Introduction

Enterprise data networks have evolved rapidly over the last few decades, and are continuing to evolve at a steady pace.

The office data networks of the 1990s were unsophisticated. PCs and servers shared lengths of coaxial cable, or chains of hubs and repeaters. The goal was simply to get packets back and forth in a relatively reliable fashion. Bandwidth management, access control, high availability and loop protection were beyond the capability of the equipment in use at that time.

As with any technology going through a maturing phase, LAN networking had a period of competing options. At the transport layer, Token Ring and FDDI were serious alternatives to Ethernet until Gigabit Ethernet arrived. At the networking layer, enterprise networks ran multiple protocols. For a long time, IPv4 was a minor player in comparison to Appletalk, IPX and NetBEUI.

However, with the standardization onto IP over Ethernet, the industry has moved forward rapidly. Since 2000, with the transport layer and network layer battles out of the way, the business of adding capability, reliability and performance to enterprise networks has progressed in earnest:

- Performance went ahead in leaps:
  - Layer 3 switching extended wirespeed forwarding right across the LAN.
  - Ethernet jumped from 100Mbps to 1Gbps to 10Gbps, while price per port continued to fall.
  - Forwarding tables expanded by factors of 10.
- Security extended from the Internet gateway into the whole network.
- Multiple generations of link and device resiliency solutions were developed.
- Bandwidth management and Quality of Service (QoS) grew in scope and precision.
- Network management, monitoring and diagnostic features advanced in breadth and depth.
- Routing protocols and IP service utilities matured, through the work of the Internet Engineering Task Force (IETF).

Today, enterprise networks are rich with complexity and capability. Voice and video have converged with data onto a single IP-over-Ethernet infrastructure. Wireless Ethernet connectivity has become ubiquitous. High levels of security, reliability and manageability are now a basic expectation.

However, it is important not to fall into the trap of thinking that the time of innovation is at an end. Despite the huge amount of progress made so far, there is still no room for complacency. Technical advances are driven by the need to meet challenges, and there are still plenty of problems arising in the realm of enterprise networking. More innovation is needed, and so enterprise networking continues to innovate.

Today's challenges

Bring Your Own Device (BYOD)

The rapid proliferation of mobile computing devices has irrevocably changed the landscape. The days of enterprise networks being accessed just from a fixed set of user equipment sanctioned by the IT team are gone forever.

Not only are these mobile devices diverse, the applications they provide to users are advancing in every direction at once. Dealing with the mobility, diversity, and rapid advancement of these devices, while maintaining the security, reliability and performance of the network, is a unique challenge.

Disaster recovery

Backing up servers to tape on a daily or weekly basis is no longer sufficient. In the case of a severe event that takes premises out of action, the time taken to re-establish all services and content from tape is not acceptable. Organizations need real-time mirroring of servers to an offsite location, and a process to cut over to running services live from that offsite location.

Managing a mirrored infrastructure, and the data flows to keep the mirror site in sync, are not simple matters.

Mixed data usage

The convergence of real-time services like VoIP, video conferencing, surveillance video and machine control onto the data network still provides problems to be solved.

Particularly problematic are:

- The increasing size of files that need to be transferred across the network. Items like Computer Aided Design (CAD), movie production or medical imaging files are large pieces of data that need to be transferred speedily, because a user is waiting to view the file. These bursts of rapid file transfer provide serious bandwidth competition for real-time services.
- The amount of ad-hoc video conferencing, using applications like Skype, that occurs now. Even though these video calls are not scheduled events using the organizing video conferencing suite, users expect reasonable quality in the call, and are typically unaware of the effects their calls may be having on other data flows in the network.

Private Data centers

Server rooms no longer hold just a set of file servers, with inbuilt disk storage. Now, even moderate-sized organizations host a number of virtualized servers, accessing data from a Storage Area Network (SAN) or a set of Network Attached Storage (NAS) devices.

Low-latency, high bandwidth data transfer is expected within these in-house data centers. Also, as services move between physical hosts, and data migrates between storage locations, the switching equipment must be reactive to these changes. This level of network performance and reactivity has not been typical in enterprise networks in the past.

Cloud-based applications

The most high-profile development in data networking in recent years has been the emergence of 'the cloud' as a repository of data and applications.

Cloud-hosted services put unprecedented pressure on Internet connections, creating another growing bandwidth management headache.

Increased data exchange with clients

In a number of commercial and government sectors, the exchange of high volumes of data with clients is an essential component of the organization's operation. Moreover, much of this data transfer needs to be performed securely.

Reliably providing controlled secure access to private servers, whilst ensuring acceptable data transfer rates, is an area ripe for innovation.

High bandwidth connectivity with external mobile users

The flip-side of BYOD is that the mobile devices that users bring into the office are also with them when they are out of the office. The ability to check email, update records and examine data—anywhere, anytime—is something users greatly appreciate, and the uptake of this opportunity has been enormous.

Altogether, this trend to remote access from mobile devices is distinctly beneficial for productivity and data security, but it is yet another trend that is putting pressure on WAN bandwidth. So much activity—downloading email attachments, loading data files and viewing multimedia content—that was previously carried out over the LAN is now occurring across the Internet. What's more, the bandwidth of mobile data connections is now in the multiple megabits per second, and users expect their mobile devices to receive data at a decent rate.

Maintaining a good service to mobile users requires taking a fresh approach to how data services are provided. It makes sense for organizations to take advantage of cloud-based services, which have high bandwidth Internet access, to serve mobile users. But at the same time, LAN-based users experience better performance from servers located in-house. How to achieve a balance between on-site and off-site location of services, or even migrate users' points of access as they move around, are new technical puzzles for IT teams to solve.

Energy efficiency

Reducing energy consumption in order to manage costs, achieve sustainability goals, and adhere to legislative requirements, is a key performance objective within organizations world-wide. The focus on resource conservation is now far more than just lip service—many organizations are instituting a role of Chief Sustainability Officer, who has a seat at the board table.

IT staff know that not all their servers and network equipment need to run 24/7, and that services can tick along on less equipment at certain times of the day, and certain days of the week. But, automating the shut-down of the right equipment at the right times, without impacting users, is by no means simple.

Extending network reach

As IP-over-Ethernet becomes the universal communication medium, the range of locations and equipment that connect to data networks is expanding apace. Electronic signage, alarm monitors, surveillance cameras, pumping stations, environmental data collectors, radars, solar panels, vehicles and more, are all joining onto the enterprise network. Each has its own characteristics and requirements, and special challenges for IT.

Monitoring, troubleshooting and controlling connections to such a variety of devices, in such a variety of locations, many of them physically remote with no staff onsite, is going to be very different to in-house network operation.

Managing complexity

The most immediate challenge that enterprise network managers are facing today is the fact that managing complex networks is difficult.

As network equipment grows in complexity, and the applications running over the network diversify, network managers are caught in a bind. On one hand, enterprises are increasingly dependent on the reliable operation of their data network. On the other hand, ensuring reliable interoperation of all these applications, and troubleshooting the issues that arise, is increasingly difficult.

Meeting the challenges

The industry has not simply put these new challenges into the too-hard basket, but is developing new ways of working that will meet the current challenges, and further evolve the operation of enterprise networking.

Frequently, these initiatives are collectively described as Software Defined Networking (SDN). However, as with any umbrella term, SDN means different things to different people. It is important not to assume that SDN is a paradigm change that will uniformly re-engineer the world's networks into new mode of operation.

Rather, SDN should be treated as a way of thinking about network control. The SDN way of thinking recognizes two key points:

1. Individual network nodes do not have a broad view of what is happening in the network. Therefore the control of forwarding decisions in the network (commonly referred to as 'the control plane') cannot be entirely left in the hands of individual network nodes. Instead some, or all, of the network control plane must be put into the hands of centralized software applications which can take input from multiple network elements and exert influence on the forwarding decisions of multiple network nodes at once.
2. Configuring and monitoring network nodes as a set of discrete individuals is unnecessarily inefficient. If the network nodes can be managed more as a distributed forwarding fabric, then significant efficiencies can be gained, and range of network management activities can be automated.

it is very important to consider how the SDN approach to network control and network management can be applied to the current challenges in enterprise networking.

Controlling the control plane

The self-organizing protocols that have provided the characteristic distributed control plane in data networks for the past few decades are very well suited to tasks like removing network loops, distributing routes, controlling resilient links and authenticating connected devices. But they are not well suited to activities that need a wider overview of the network, or end-to-end management of data flows.

For example, the distributed control plane is not well suited to:

- Measuring the aggregate data transmission rate between two sectors of a network, and determining that the traffic can all be re-routing to a new path, so that under-utilized ports and switches can be taken down to save power.
- Receiving notification that an important video conference is about to begin, and will pass through the same bottleneck point as a series of large file transfers, and therefore re-routing the file transfers away from the bottleneck.
- Moving VPN connections off to a cloud-based service, or back again, when the volume of email transactions from remote mobile users rises above or falls below a given threshold.
- Applying network-wide throttling to a particular traffic type, due to detection of a virus infection on a newly attached mobile device.

The SDN approach can be applied to enterprise networking by developing applications that:

- Receive feeds of traffic sampling data, and analyze the data to identify traffic patterns that represent threats or overuse of policy-controlled online sites like Facebook or YouTube. Then, automatically update network node operating parameters, so they block or throttle that traffic.
- Recognize when an authenticated user, connected wirelessly to the network, roams to different sectors of the network. Upon recognizing this user's change of location, any policies applied to their connection point, or dynamic configuration required to provide them access to certain services, can be automatically updated in the relevant network nodes.
- Monitor the load on Network Function Virtualization (NFV) instances, such as Intrusion Detection System (IDS) services, Virtual Private Network (VPN) controllers and Transmission Control Protocol (TCP) accelerators; add or remove instances as appropriate; and update network nodes to route the right traffic to the right NFV instances.

Automating management

The model of manually managing network nodes as discrete units cannot remain viable in the current operating environment. Network management must evolve, so that changes can be rolled out more rapidly, and problems can be solved efficiently.

Applying SDN to network management involves three main strands of development:

1. Embedding more management intelligence into the network nodes themselves, so they can actively participate in a unified network management framework, rather than being passively managed.
2. Enhancing the analytic information that network nodes can provide, so that a deep picture of the network's state can be accessed at any given time.
3. Creating applications that can work with the network nodes' embedded management intelligence to simplify and automate network management tasks. The scope of operation of these applications will grow as the level of analytics they gather from the network increases.

Reworking network management by implementing these lines of development will create networks in which:

- New nodes are automatically configured as soon as they are attached to the network.
- The configuration changes required to support new services are rolled out across the network from a single console.
- Troubleshooting is aided by the ability to drill down into detailed network state information, and to step through a replay of the way the network's state changed over a specified time period.

Allied Telesis initiatives in enterprise SDN

Allied Telesis is a leader in the evolution of enterprise networking. For three decades, as enterprise networking has developed, Allied Telesis equipment and solutions have been at the leading edge of progress. The company is presently working on several fronts to implement the solutions that will meet the current and future challenges in this sector.

Allied Telesis Autonomous Management Framework™ (AMF)

The Allied Telesis initiatives have been spearheaded by advances in the field of network management automation. Allied Telesis recognize that the growing operating cost of network management is an almost universal issue for organizations around the world, and have focused significant innovative energy on creating a framework for automation of network management.

The result of this work is AMF, a combination of embedded management intelligence and a central controller which automates such tasks as:

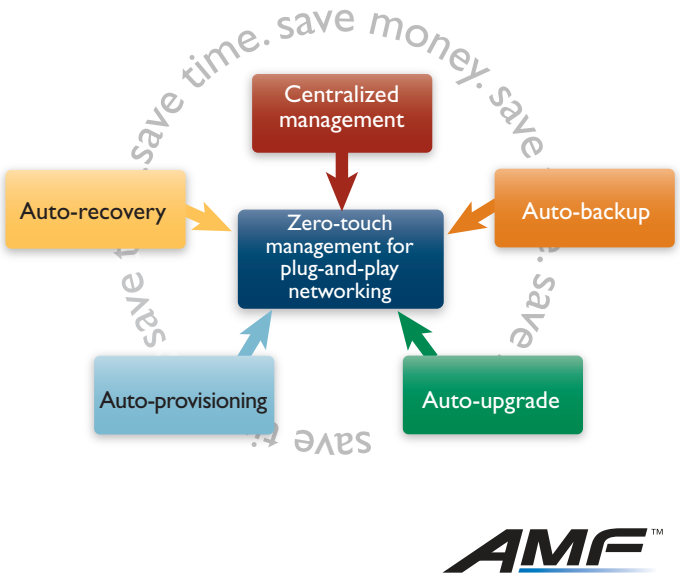
- Adding a new switch to a network
- Replacing a failed switch
- Installing a software upgrade across the network
- Backing up configuration and software images from network nodes
- Updating configuration on multiple network nodes at once

This framework unifies the network nodes into a single management plane that overlays the network to provide the automated functionality. As new nodes are added to the network, the management plane is immediately expanded to include them. The plane extends seamlessly across WAN links or VPNs to include remote sites, and unstaffed locations.

Openflow

Allied Telesis have integrated Openflow into the AlliedWare Plus Operating System, to provide an Openflow API on the x-series Ethernet switches.

This standards-based SDN API enables the switches to be controlled by any SDN controller that uses Openflow as its southbound communication method.



Future directions

Building on the foundation provided by AMF and the Openflow implementation, Allied Telesis will continue to evolve their enterprise SDN solutions.

The unique integration of an embedded management framework and a standards-based SDN API, along with planned Network Function Virtualization (NFV) offerings, will provide a strong platform on which to move enterprise networks forward.

The directions in which the Allied Telesis solutions will be looking to take enterprise networks are:

- Complete unified network management of wired, wireless, LAN and WAN components, using AMF.
- Cloud-based network management control.
- Integration of network management, SDN apps and user identity servers.
- Inclusion of NFV components into the unified management and control-plane solution.
- Extension of integrated management out to new classes of Ethernet-connected devices, to provide a coherent interface onto the 'Intranet of Things".

Conclusion

In the early days of networking the focus was on delivering reliable connectivity with consistent performance to ensure that users were able to access services when they needed to. Today, networks—particularly wired networks—are extremely reliable, deliver performance in the order of Gigabits or tens of Gigabits per second to the user and are packed with features to improve reliability and security.

The challenges of today are no longer around how to deliver access and performance, but rather are focused on how to keep up with the dynamic nature of technology environments, how to simplify infrastructure, and how to do more with the limited resources within an organization.

SDN, AMF and Openflow are important technologies that will enable organizations to overcome these challenges today and will continue to evolve to overcome the challenges of tomorrow.

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

C613-08024-00 RevB