White Paper

A Migration Path to Software-Defined Networking (SDN) in an Enterprise Network

Introduction

Bringing software control into an Enterprise network does not have to be an abrupt overnight change. In fact, transitioning from a traditional network to one that is based on Software-Defined Networking (SDN), can, and should, occur in a gradual manner.

There are a number of reasons why an abrupt transition to a completely software-defined network is extremely difficult to execute. For a start, the amount of planning that is required to ensure the continued operation of all current network services makes it prohibitively difficult—there are innumerable details to consider and analyze, and too many unexpected behaviors to foresee.

Testing the new solution is also problematic. It is not possible to pre-test the whole system, as that would mean setting up an entire parallel data network. It is only feasible to test limited subsets of the network.

Furthermore, the logistics of completing a network cutover to SDN in an acceptable outage window are extremely challenging.

The reality is that migrating to a software-defined network is necessarily a progressive process, which should occur in a series of steps, each of which addresses a particular need.

Contents

Introduction 1
Why change to SDN? 2
Cost reduction 2
Increased flexibility 2
Greater security 3
Improved user experience 3
A three-phase process 3
- Phase 1: unified management 3
- Phase 2: OpenFlow hybrid 4
- Phase 3: optimum SDN deployment 4

Secure Enterprise SDN–a real SDN solution for the Enterprise 5
- Delivering the goals of Enterprise SDN 5
- Conclusion 5
- About Allied Telesis, Inc. 6

Why change to SDN?

The data network is a tool of the Enterprise, and the only reason for altering the operation of the network is to make it a tool that better serves the Enterprise. Putting time and money into reworking the network, simply to make it a different-looking network without any added value, is pointless.

The starting point of this transition is to identify the ways in which the business expects to get more value from its new, software-defined data network. The major benefits of introducing software control into the network are:

- **Cost reduction**
- **Increased flexibility**
- **Greater security**
- **Improved user experience**

These benefits are explained in more detail in the following sections.

Cost reduction

Network operating costs can be reduced in two main ways: simplifying complex tasks, and automating routine tasks. Clever software is the key to achieving both.

Software assistance simplifies complex tasks such as:

- Troubleshooting problems
- Bulk reconfiguration
- Predicting resource contention

Unifying the network under software control enables the reliable automation of routine activities, such as:

- Configuration backups
- Software upgrades
- Replacing faulty units

Reducing the amount of time that needs to be spent on these activities enables IT engineers to use their valuable hours performing more skilled tasks.

Increased flexibility

Mobility, convergence, and the proliferation of applications have all rapidly increased the number of capabilities that are now expected of an Enterprise network. These new capabilities must be delivered, and in a manner that conforms to organizational policies. As a result, today's networks must operate in an increasingly agile manner which takes into account a large number of factors—including user identity, application content, device context and usage policies.

Gaining consistent levels of content awareness and dynamic behavior across the entire network would require capabilities that network nodes typically do not possess.

Centralizing content awareness, context awareness and decision making, and then pushing instructions out to the network nodes, is the most practicable means of achieving the required dynamic behavior throughout a network.A centralized application that orchestrates data transfer can have this knowledge of file sizes and priorities. If the orchestrating application can tell the switching nodes which sessions to put onto which links, then files can be transferred with maximum efficiency.

Greater security

A strong trend in advanced persistent threats is the installing of a “Trojan horse” application into the network. This Trojan will perform actions within the network, and may only very infrequently communicate with hosts outside the network.

Hence, threat protection systems that only monitor data exchanged with the Internet, will often miss the signs of a Trojan having been installed within the network, or will pick up the signs too late.

Again, the data analysis and decision making capabilities required for accurate threat protection are beyond the means of most network nodes, and so must be centrally provided. Centralized protection software can instruct network nodes to block the sources of suspicious traffic as it is detected.

Improved user experience

Increased flexibility, responsiveness and threat protection, together with reduced downtime, all add up to an improved user experience.

The majority of users give very little thought to the network infrastructure except when it malfunctions. What users want is high-performance access to their services and applications, when and where they need it. The best way to provide this experience is to optimize the network behavior, by means of responsive intelligent control.

A three-phase process

Gaining software control is a three-phase process:

- Phase 1: unified management
- Phase 2: OpenFlow hybrid
- Phase 3: optimum SDN deployment

Each phase is described in more detail in the following sections.

Phase 1: unified management

The first step towards bringing software control into a network is to unify the management of the network, so that it can be managed as a single entity.

Allied Telesis unifies network management with Allied Telesis Autonomous Management Framework™ (AMF), which embeds an intelligent management framework into a network.

AMF provides:

- Automatic creation of a management communication path throughout the network
- Automation of routine tasks such as backups, software upgrades and device health-checking
- Zero-touch replacement of failed units, and provisioning of new network nodes
- Collection of troubleshooting information from multiple nodes concurrently

These facilities achieve the bulk of the cost-reduction needs when transitioning to a software-controlled network. Furthermore, AMF facilitates the introduction of control applications. The ability to configure multiple nodes simultaneously is a key enabler of event-based network control applications. Such programs can easily alter filters, QoS settings, VLAN parameters or routing policies across the whole network, based on such factors as time of day, server load, sustained WAN congestion, and many more.

Introducing AMF into an existing network is straightforward—it simply requires a few configuration commands on each device. Importantly, AMF can operate in a mixed-vendor network. AMF connections can be tunneled across non-AMF-capable networks, thereby enabling it to be extended across the Internet or other WAN service.

This is a low-impact first step, which yields a high return in cost savings and centralized network control.

Phase 2: OpenFlow hybrid

Whilst AMF provides unified network management, the key to direct programmatic control of network data flows is OpenFlow.

OpenFlow is an open-standards interface that allows fine-grained control over how a network device forwards or drops data streams. Once OpenFlow is enabled on network nodes, detailed programmatic control becomes possible.

Fortunately, OpenFlow can be brought into a network in a staged fashion. A network can operate quite successfully for an extended period in a hybrid OpenFlow mode. The hybrid mode can apply to the network as a whole, in a situation where some nodes in the network support OpenFlow while others don't. Furthermore, nodes themselves can operate in hybrid mode, whereby some ports or VLANs are controlled by OpenFlow and some are not.

So, for example, OpenFlow can be introduced on a set of edge switches—maybe those in a particular department—and perhaps even on just some ports of those switches. In this way, software for network control can be trialed on a subset of users. These users' data can then be controlled by centralized software applications. For instance, the policy routing and bandwidth limits applied to their data streams can be controlled by instructions from the centralized software, rather than by static configuration on the switches. The performance of this new mode of operation, and its ability to apply finer control based on network conditions, can then be evaluated and optimized.

The hybrid mode of operation provides a suitable environment in which to determine which SDN applications truly add value to the organization, and which are of limited, or no benefit.

Phase 3: optimum SDN deployment

The transition from a hybrid network to a completely software-defined network may be very gradual, or may in fact never be complete. The deployment of SDN may only provide distinct benefit in certain sections of the network, and not be extended to other sectors.

On the other hand, in some networks, the benefits of SDN are so clear that it is quickly deployed to the whole network.

Whatever the case, the peaceful coexistence of traditional and software-defined networking means that the optimum level of SDN in the network can be discovered over time, and regularly reviewed as the technology develops.

Secure Enterprise SDN—a real SDN solution for the Enterprise

Allied Telesis have created a true, practical, Enterprise SDN solution, called Secure Enterprise SDN.

The elements of this solution are:

- AMF, to provide unified network management
- OpenFlow, to provide an open-standards control interface to the networking nodes
- Secure Enterprise SDN Controller (SESC)—Allied Telesis' Openflow controller
- Security, mobility and user/device management applications

This solution can be implemented in the multi-phase manner described above, pausing at any step along the way, or can be taken quickly through to a completely SDN-controlled network.

Irrespective of the extent to which the network is transferred to SDN control, the solution is an effective framework within which to bring SDN into the network.

The policies applied to groups of users can be defined in an HR-facing application, and back-end software converts these policies into instructions which are delivered, via the SDN controller, to individual network nodes. The network recognizes the identities of connected users and dynamically applies access restrictions, service levels, and device usage permissions, based on user profiles defined in the HR application.

Device security postures defined as high-level policies are applied in a granular fashion to each connected device, and non-conformant devices are automatically quarantined.

Rules for the use of mobile devices are applied as filters that block certain traffic to/from mobile devices, and as disconnection of devices being operated outside of allowed locations.

Traffic security is applied at the heart of the network, immediately recognizing threat-related traffic, and rapidly disconnecting the source device from the network.

Delivering the goals of Enterprise SDN

The SES solution delivers the expected benefits of SDN in the Enterprise, by:

- Using software to translate business rules into network control, rather than requiring IT staff to perform that translation, and manually implement it as network node configuration commands.
- Ensuring unfailing security scanning of connected devices, and rapid, automated response to security threats detected in the network.
- Reducing the time spent on network control and configuration—thereby reducing network operating costs.
- Providing users with a consistent, reliable network experience.

Conclusion

Transitioning from a traditional network to one that is based on SDN can, and should, occur in a gradual manner. The migration to a software-defined network should ideally be a three-phase process, in which each step towards gaining software control addresses a need, and thus provides a benefit.

Managing the migration in this way avoids potential problems, issues and outages, and allows the network to meet the major benefits of introducing software control—cost reduction, increased flexibility, greater security, and an improved user experience.

About Allied Telesis, Inc.

For nearly 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

C613-08035-00 RevB