White Paper

Allied Telesis

Easing the Enterprise transition to IPv6

Introduction

The world is moving inexorably from IPv4 to IPv6. However, many organizations feel that they currently have no need for IPv6. If a business has plenty of IPv4 addresses, a reliable Network Address Translation (NAT) infrastructure, and no IPv6-specific applications, it can experience little compulsion to take on the perceived expense and disruption of integrating IPv6 into its network.

However, there are many compelling reasons for making the move to IPv6:

- **The Internet is a global entity**
  Organizations with online services are connected to the whole world, including those parts of the world where IPv4 addresses have already run out. Not being IPv6-ready can make a business inaccessible—if an organization wants to be accessed by those people who only have an IPv6 address, then they need their services to be accessible by IPv6.

- **Mobile Internet services are moving quickly to IPv6**
  The native backbone protocol of 4G and 5G mobile networks is IPv6.

- **The 'Internet of Things'**
  While the day when fridges, stoves, light sockets, and more will all have their own IP addresses is not yet here, the installation of large arrays of Internet-connected objects is already happening: 'smart grids' are well established; video surveillance cameras are installed by the millions worldwide; environmental sensor arrays are being built; and "smart city" (IPv6-connected street lights, parking meters, traffic signals, bus stops, etc.) solutions are in use. The business opportunities these afford, and the potential benefits for all organizations—using smart supply chains, smart manufacturing systems, and more—are enormous. The communication technologies inherent in these innovations all utilize IPv6.

- **In-vehicle Internet.**
  The network mobility technology that underlies the so-called 'Car-to-x' communication (car-to-car, car-to-business, car-to-signals, etc.) is inherently more effective over IPv6 than IPv4. Moreover, the new communication systems operating between components within a vehicle are using IPv6 transport.

Full global accessibility already requires IPv6, and the business opportunities of the near future will be based around IPv6 communications.

Making the transition

The good news is that the transition from IPv4 to IPv6 can occur gradually. Because switches, servers, workstations, routers and more invariably provide dual-stack capability, it is completely feasible to continue operating with the original IPv4 infrastructure while an IPv6 infrastructure is gradually built up in parallel. Services can cut over from IPv4 to IPv6 one at a time. Very often the cutover can be quite transparent to users—it is a simple matter of changing Domain Name System (DNS) server entries, so that their network connections resolve to new IPv6 addresses.

However, IT teams still face a number of challenges along the way. Transitioning a network from IPv4 to IPv6 is not an entirely simple process.

Some of these challenges are:

- **Obtaining an IPv6 address range**
  An organization has to decide whether to obtain this from their Internet Service Provider (ISP), or to apply directly to their Regional Internet Registry (APNIC, ARIN, RIPE NCC, Lacnic, or AFRINIC).

- **Provisioning IPv6 Internet access**
  The organization must be certain that it is connecting through ISP(s) that provide reliable native IPv6 Internet access, and they must agree on the method by which their IPv6 subnet will be advertised to the world.

- **Planning the addressing scheme**
  The IPv6 address range allocated to the organization must be split into subnets, and distributed to different parts of the network.

- **Learning the differences between IPv4 and IPv6**
  IPv6 introduces a number of new concepts, for example neighbor discovery, router discovery, link-local addresses, and address auto-configuration. IT teams must master these concepts, and be completely aware of the operational differences between IPv4 and IPv6.

- **Deciding on an address allocation process**
  Should all the allocation be done by Dynamic Host Configuration Protocol for IPv6 (DHCPv6), or should auto-configuration be used for the majority of workstations? Or is it more appropriate to use a mixture of the two?

- **Upgrading applications to IPv6-capable versions**
  Management tools, server applications, security backend and more, all need to be upgraded or reconfigured to operate on IPv6 as well as IPv4. This new capability then needs to be tested.

- **Configuring network nodes**
  IPv6 addresses, services, security features, Quality of Service (QoS), routing protocols, and so on all need to be correctly configured on the network's switches and routers, whilst not adversely affecting their existing handling of IPv4 traffic.

- **Learning how to troubleshoot IPv6 issues**
  The logic of stepping through typical IPv6 network problems is different to the logic of working through similar problems in an IPv4 network. The thought processes that network administrators have developed from their IPv4 troubleshooting experience must be rewired to deal with the way IPv6 operates.

A transition-friendly network infrastructure

It is highly desirable that existing network infrastructure has been implemented in a manner that helps, rather than hinders, the move to IPv6.

In practical terms, this means that the equipment which makes up the network should fulfill the following requirements:

- **The IPv6 packet forwarding performance must be as good as the IPv4 performance**
  It is not acceptable to step down from hardware wire-speed IPv4 routing to a substandard level of IPv6 routing in software. Any decline in forwarding performance would lead to users perceiving the introduction of IPv6 as a profound failure.

- **The network must provide the same level of resiliency for IPv6 as it does for IPv4**
  Rapid failover of IPv4 traffic on link or unit failure must be matched by equally as rapid failover of IPv6 traffic. Users who have come to rely on a very high level of uptime for IPv4-based services will not be forgiving of new IPv6 services that do not achieve the same level of uptime.

- **Solid, reliable IPv6 security must be available**
  By default, firewalls and filters set up for blocking IPv4-based attacks will typically let IPv6 traffic straight through unchecked. It is vital that the network can be easily configured to be as secure against IPv6-based attacks as it is against IPv4-based attacks.

- **IPv6 services must be provided the same QoS as their IPv4 counterparts**
  The key to QoS is accurate, careful classification of different traffic types. Network equipment must provide an IPv6 traffic classification facility that is just as sophisticated as its IPv4 traffic classification.

- **The routing protocol structure for IPv6 needs to mirror that of IPv4**
  If there is not a simple one-to-one correspondence between the implementation of the IPv4 and IPv6 routing protocols in the network, then network maintenance will be onerous and error-prone.

- **The network equipment must be securely manageable by IPv6**
  Introducing an IPv6 infrastructure means bringing in IPv6-based management tools that enable monitoring and troubleshooting of IPv6 traffic, and allow IPv6 capability testing. The equipment in the network must be capable of interacting with these IPv6-based management tools, by having IPv6 implementations of services like Simple Network Management Protocol v3 (SNMPv3), Secure Shell (SSH), Ping, Traceroute, and more.

Allied Telesis Enterprise/Metro Networking Solution

Allied Telesis provides high-performance, resilient Enterprise networks, based around converged and distributed cores. With options for Chassis-based resiliency, Virtual Chassis Stacking (VCStack™) and rapid-convergence Ethernet rings, Allied Telesis provide near-hitless failover core and distribution-layer solutions that fit a wide variety of Enterprise, Campus and Metro applications.

The design of the network solutions, and the design of the Allied Telesis x-Series switches from which these solutions are built, make them ideal for pain-free introduction of IPv6 into existing IPv4 networks. These solutions meet all of the challenges of transitioning a network from IPv4 to IPv6:

- The Layer 3 switches are built around Application-Specific Integrated Circuits (ASICs) that support IPv6 right on a par with IPv4. Their Layer 2 and Layer 3 forwarding performance for IPv6 is wirespeed, just as for IPv4.

- Master controllers in the core Chassis and Virtual Chassis Stacks use Graceful Restart (GR), also known as Non Stop Forwarding (NSF) during failover to achieve true Layer 3 router resiliency. This ensures data continues to flow, even as the core chassis drops out of the routing protocol briefly when the master controller fails over. This technique is equally as effective for IPv6 routing as for IPv4. As a result, when services are moved over from IPv4 to IPv6, they suffer no reduction in uptime.

- Security within the switching infrastructure relies on wirespeed traffic filtering, using hardware-based Access Control Lists (ACLs). Allied Telesis x-Series switches provide filtering granularity on L2/L3/L4 fields, within IPv6 packets that match their filtering granularity for IPv4. Also, the number of IPv6 ACLs that can be created is on a par with the number of IPv4 ACLs.

- The application of QoS to IPv6 traffic is equally as precise as it is for IPv4.

- Allied Telesis x-Series switches implement the same three routing protocols—RIP, OSPF and BGP—in both IPv4 and IPv6. The IPv6 implementations of routing protocols are mature and feature-rich, so almost any existing IPv4 routing protocol configuration can be mirrored in IPv6. No changes need to be made to the existing IPv4 routing protocol configuration to accommodate IPv6 requirements. The IPv4 routing simply continues to run, and the IPv6 configuration easily slots in beside it.

- Management services and utilities on the Allied Telesis x-Series switches are provided in IPv4 and IPv6 versions. This includes not just SSH, SNMPv3, Web management, Ping, and Traceroute, but also NTP, DNS, DHCP, sFlow. So, a full IPv6 network management system can be built up, and verified, around the switch infrastructure.

Allied Telesis Autonomous Management Framework™

Taking the pain out of network reconfiguration

Allied Telesis x-Series switches provide one other significant advantage to any organization that is making the transition to IPv6.

Configuring IPv6 features on all the switches in a network involves a lot of repetitive command line entry, as each switch across the network needs to be configured with IPv6 addresses, IPv6 filters, IPv6 services, IPv6 routing protocols, and more. Not only is this work repetitive and time consuming, it is also error prone. Entering a command correctly on 49 switches, but failing to add it on the 50th switch can result in odd problems or security holes in the network, which can take a long time to track down and resolve.

Inconsistent application of security features, in particular, can be very costly. A security infrastructure is only as strong as its weakest link. If the necessary filtering/authentication/encryption configuration has been incorrectly applied to just one edge switch, then this creates a vulnerable hole in the security framework. Malicious exploitation of such a hole can be very costly for an organization, in terms of virus-induced downtime, lost data, exposure to breach-of-privacy litigation, loss of reputation, and more.

Allied Telesis x-Series switches support the Allied Telesis Autonomous Management Framework™ (AMF). AMF delivers immediate value to businesses of all sizes, with centralized network management able to treat a network of any size as a single, converged entity. AMF minimzes the effort and risk of large-scale configuration or software upgrades in a network.

The key aspects of AMF that simplify the IPv6 transition are:

- **Unified command line**
  AMF enables the network administrator to be logged into multiple switches at the same time. Any command entered during this unified login session is sent to all the switches in the group.

  This is ideal for a situation like an IPv6 transition, when the same new configuration needs to be applied to numerous switches. AMF enables these pieces of configuration to be typed in just once—which saves time, avoids errors, and provides configuration consistency across the network.

- **Automated software upgrade**
  With a single command, AMF can be set rolling on the task of installing a new software version on some or all of the switches in the network. When an organization's network software needs to be upgraded to enable new IPv6 features, AMF makes this upgrade process simple and reliable.

- **Automated backup**
  The network nodes will automatically upload their configuration, and software image, to a central repository at regular intervals. So, as the network is being configured for IPv6, the new configurations are automatically backed up.

Summary

The requirement for global accessibility, and the need to be part of new business opportunities, are the drivers for bringing IPv6 into the world's networks.

The integration of IPv6 into an enterprise network need not be difficult, expensive or disruptive. If the network infrastructure is truly IPv6 ready, then the process of putting new IPv6 configuration in beside existing IPv4 configuration is reasonably straightforward.

Allied Telesis enterprise network solutions provide networks that are truly IPv6 ready. Allied Telesis also provide AMF, a scalable network management platform that reduces the work, and risk, involved in upgrading a network to IPv6. It supports Allied Telesis switching, firewall, and wireless products, as well as a wide range of third-party devices—including video surveillance cameras and IP phones—for truly inclusive network automation.

About Allied Telesis

For over 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

© 2020 Allied Telesis, Inc. All rights reserved.

C613-08018-00 RevB