atnis

AUTOMATION & TRANSFORMATIONS

IPv6 Ready Enterprise Networks

Our Journey and Achievements

The Critical Shift from IPV4 to IPV6 and "The Call to Action"
for Government and large Enterprises

Background

Governments around the world continue to enable IPv6 adoption. As the pool of IPv4 addresses runs out, a major challenge for governments is planning for a future Internet that can connect billions of people and devices.The goal for governments as well as for organizations that must work with the public sector is to deploy IPv6 securely and cost effectively, with minimal riskacross the network and services infrastructure, to optimize the user experience at each point of the journey.

IPv6 Adoption: Key Business Drivers

Address Exhaustion

The primary driver for IPv6 adoption is the depletion of IPv4 addresses. IPv4, with its 32-bit address space, has a limited number of addresses (approximately 4.3 billion). As more devices connect to the internet, the available IPv4 addresses are quickly running out.

Address Exhaustion

The primary driver for IPv6 adoption is the depletion of IPv4 addresses. IPv4, with its 32-bit address space, has a limited number of addresses (approximately 4.3 billion). As more devices connect to the internet, the available IPv4 addresses are quickly running out.

IPv6 Address Space

IPv6, with its 128-bit address space, provides an astronomically large number of addresses (approximately 340 undecillion). This virtually limitless address space ensures enough IP addresses for all conceivable devices, facilitating the continued growth of the internet.

Content Providers

Major content providers like Google, Facebook, and Netflix have enabled IPv6 on their platforms to help ensure that users accessing these services over IPv6 networks can do so seamlessly. Content providers play a significant role in driving IPv6 adoption by making their services accessible over IPv6.

IPV6 Deployment for a Ministry of Industry, Tourism & Trade Customer in APAC

The Plan aims to streamline the integration of Internet Protocol IPv6, responding to the tremendous growth of Internet and promoting technological innovation and deployment of new services in the field of Information Society (strengthening infomation security and connectivity and facilitating network management). As a Part of National IPv6 deployment plan across all sectors of Governemnt Services.ATNIS was engaged to be part of a very successful program of strategic traNnition to IPv6, by employing the 464XLAT technology for a Ministry of Industry,Tourism and Trade customer in APAC

KEY CHALLENGES

1 Technical Limitations

The reliance on NAT64 and DNS64 technologies initially posed limitations. The main issue was that certain applications, including Skype and WhatsApp, could not operate effectively through NAT64 alone.

2 Operational integration

Integrating 464XLAT within existing infrastructure required careful planning to guarantee seamless service continuity and user experience.

3 Security Challanges

IPv6 technology still faces challenges in terms of IPv4 literals communications and establishing connections from the IPv4 host side.

4 Migration & Go Live

The transition had to be transparent to users while maintaining the quality of service. These, plus supporting a wide range of devices presented significant challenges.

Planning and Early Deployment Phases

First, we started creating a comprehensive addressing plan for the different sized offices, campus buildings, and data centers. Our initial IPv6 addressing scheme followed the guidelines specified in RFC5375 (IPv6 Unicast address assignment:

Assign /64 for each VLAN
Assign /56 for each building
Assign /48 for each campus or office

ATNIS also aggressively started testing and certifying code for the various hardware vendors' platforms and working on building or deploying IPv6 support into our in-house built network management tools

Description of Phases

Phase I

The next steps during this initial implementation phase were to create several fully dual-stacked labs ***(Figure 1)*** and connect them to the dual-stacked router using the same GRE tunnels,but instead of at certain hosts, these GRE tunnels were now terminated at the lab routers

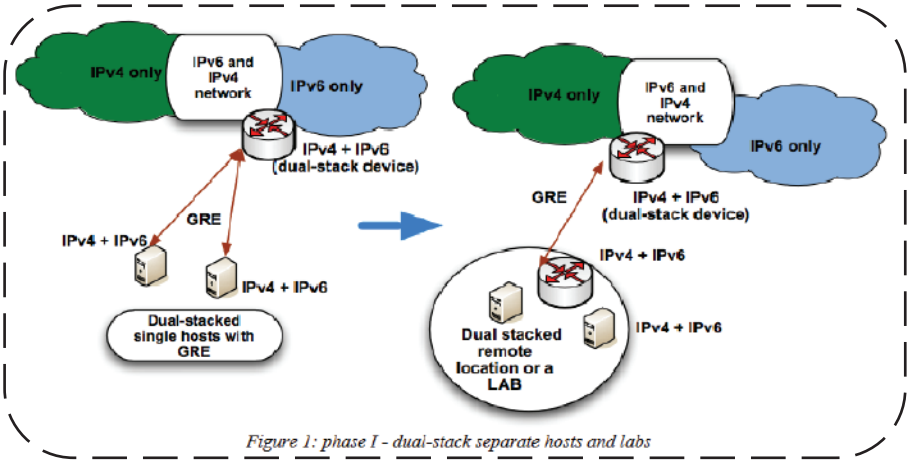

Figure 1: phase I - dual-stack separate hosts and labs

Phase II

In the next phase we started dual-stacking entire offices and campus buildings ***(Figure 2)*** and then building a GRE tunnel from the WAN Border router at each location to the egress iPv6 peering router.

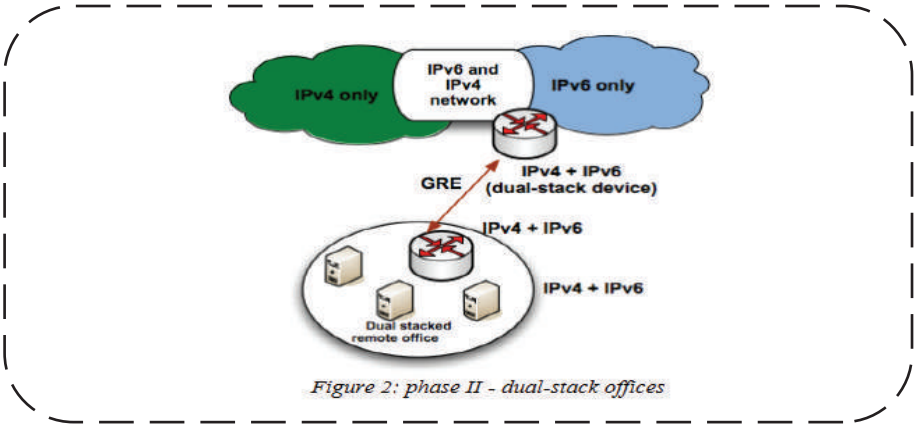

Figure 2: phase II - dual-stack offices

Phase III

In the third phase we started dual-stacking entire offices, while trying to prioritize deployment in offices with immediate need for IPv6 ***(Figure 3)***, e.g. engineers working on developing or supporting applications for IPv6

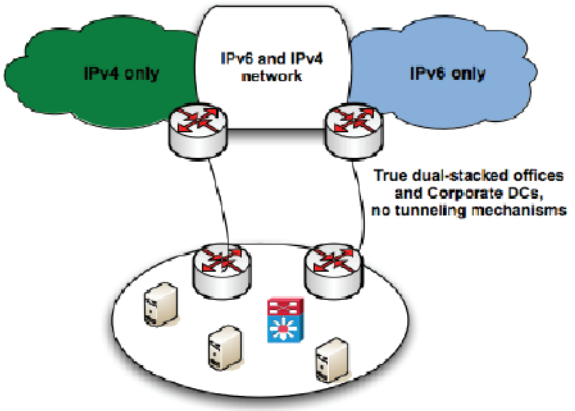

Figure 3: phase III - dual-stack the upstream WAN connections to the transit and MPLS VPN providers

Developing a Plan to Simplify and Future Proof Network

The challenge of this IPv6 deployment was having to first correct this existing (IPv4) architecture to ensure that it would align with the IPv6 deployment and, more importantly, allow for future ISP changes.Typically, the use of NAT and private addresses in IPv4 is considered advantageous when changing providers, as it avoids the need to renumber all users in the network.

In the case of IPv6, there is no need for NAT, therefore, the use of BGP is not only good practice, but essential if you want to employ Provider Independent (PI) addressing to avoid renumbering when changing ISPs. It also allows you to connect to several ISPs (multihoming), which provides complete failover.

Provider-Independent (PI) address space is a block of IP addresses assigned by a Regional Internet Registry (RIR) directly to an end-user organisation. The user must contract with an ISP to obtain routing of the address block within the Internet.

PI addresses offer end-users the opportunity to change ISPs without renumbering of their networks and to use multiple access providers in a multihomed configuration. With PI, the client could still use IPv4 private addresses, together with global IPv6 ones, but can retain most of the network infrastructure with stable addressing for both IPv4 and IPv6 and avoid any kind of disconnections.

ATNIS alternative solutions to BGP for enterprise multihoming in the past, such as the one described in RFC 8475 as well as NPT and Unique Local Address (ULAs). However, these have yet to capture the attention of vendors and are designed for very simple networks, typically with only clients. In the case of the latter two, they also don't exist as standards, so they aren't something to recommend

Address Planning for IPV6 for the Depolyment

The primary attraction to using provider independent (PI) space for this deployment was to ensure that customer is not tied to a specific provider. Provider independent (PI) space also allows the customer to connect to multiple service providers with a single IPv6 address block. These multiple connections provide resiliency and redundancy in case a particular service provider network has issues.

SUBNET PLANNING

1

The Rules

The actual size of the allocation will be based on the expected number of end sites or users, but there are minimum allocation sizes to ease administrative overhead and prevent too much fragmentation. Under these rules, any branch will receive a minimum allocation of a /32, while users will get a minimum assignment of a /48 of address space.

2

Administrative Ease

When designing IPv6 address structures , we stick to 4-bit boundaries. This is because these 4 bits nicely align with the hexadecimal digits that are used in IPv6 addresses, and so greatly reduces the risk for mistakes.

3

Room for Growth

The minimum allocation of a /32 would add another 3 bits –in human terms, that means you could grow eight times as big before you would need to request additional IPv6 addresses!

4

Hierarchy

In the first step we need to define what prefix length (how many networks) we want to use for every network level. In the second step we assign the organization's Locations to the different network levels and create the addressing plan.

LEARNING AND CHALLENGES FOR THE IPV6 DEPLOYMENT

For the successful case on IPv6 transition technologies, we share our reflections that can be helpful for the future development.

SMOOTH ADOPTION &TRANSITION

During the transitional phase toward IPv6, it is crucial to guarantee the IPv4-IPv6 interoperability for the smooth IPv6 adoption. Among various proposals,the once criticized Network Address Translation (NAT) is gaining a positive role in such transition to bridge the gap between two incompatible IP versions. In our project, we investigated the domain of IPv6 transition technologies by focusing on the mechanisms for the NAT discovery and learning of the IPv6 prefix used for protocol translation in an access network.

HURDLE OF COMPLEXITY

Converting from IPv4 to IPv6 also introduces the hurdle of complexity, as IPv6 is significantly more complex and requires tools and strategies to properly manage the network. Therefore companies would have to invest in tools, strategies, and expert personnel to get the best out of IPv6.

SCALABILITY AND DIRECT ADDRESSING CAPABILITIES

IPv6 also has commendable scalability and direct addressing capabilities. This makes it suitable for technologies like IoT and cloud computing. IPv6, With its seemingly unlimited address space, can accommodate billions of devices that can be potentially connected to IoT deployments. Its direct addressing capabilities come in clutch for cloud computing as it enables dynamic comms between devices, applications, and cloud platforms.

SECURITY IMPROVEMENTS

the strengths of IPv6 go beyond just sheer quantity and availability. IPv6 offers significant security improvements over IPv4, as it is more than capable of holding its own against cyber attacks and maintaining integrity in data transmissions.

Conclusion

Networks have fundamentally shifted with intentbased networking to become more flexible, intuitive and interoperable—supported through automation and machine learning to become predictive and self-healing.

Companies can focus on repeatable changes that have a high success rate historically and apply end-to-end automation to implementation and governance processes. Companies should be moving quickly to automate critical network activities because the value proposition is strong. Costs can be reduced significantly, and people can be deployed to work on higher-value activities. Quality improves because less human intervention is required. Speed to value increases dramatically because, with automation, the management and provisioning of millions of devices can happen instantly. Enterprise solutions can be delivered seamlessly as capabilities in a platform. Today's highly virtualized, cloud-enabled networks also require a new security approach to address the high rate of business change and ever-evolving security threats. Automation can provide constantly updated, secure access from device to cloud. Finally, automation is essential to meet the scope and scale of IoT and other new technologies. Companies today may have 10,000 or more network devices. That sounds like a lot, but tomorrow's sensors and devices will dwarf that number by orders of magnitude. The old way of manually updating network equipment doesn't work for upgrading tomorrow's virtual networks of sensors. Future technologies like artificial intelligence and blockchain will require flexible new network capabilities. In other words, the future really does depend on network automation

ATNIS India

15 A 4th floor Building A City Vista Fountain Road Kharadi Pune Maharashtra 411014

enquiry_in@atnis.net

Direct Line: +91-99869 99094

ATNIS Australia

Gateway 1 Level 36 Macquarie Street Sydney NSW 2000

enquiry_au@atnis.net

Direct Line : +61 2 8610 6784

ATNIS Singapore

810 Geylang Road #15-05 City plaza Singapore 409286

enquiry_sg@atnis.net

Direct Line : +65 600024172

ATNIS UAE

HDS Business Centre Tower Cluster M1 Cluster M1 33rd Floor Jumeirah Lake Towers
PO box 340505 Dubai UAE

enquiry_uae@atnis.net

Direct Line : +971 55 635 2075