Realtime
publishers

Migrating to IPv6

The Essentials Series

Managing IPv6: Challenges and Solutions

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Managing IPv6: Challenges and Solutions

The migration from IPv4 to IPv6 will take time and resources. Network devices will be upgraded and reconfigured, applications will be changed to support the new protocol, and client devices will be upgraded. While all this is going on, business operations will have to continue without disruption. Executives and managers will rightly ask, Is this all necessary? If so, how do we minimize the cost and the risk of the migration? This article highlights management challenges faced during the migration to IPv6 and their solutions:

- Making the business case for migrating to IPv6
- Planning the migration to IPv6
- Establishing the importance of network monitoring
- Determining security considerations of migrating from IPv4 to IPv6

Let's begin with the justification for migrating to IPv6.

Making the Business Case for Migrating to IPv6

For many businesses, IPv4 has worked well. Servers, workstations, and even mobile devices are functioning together over the corporate and public networks. Service is generally reliable and for most speeds is sufficient to meet business requirements. Why change? The answer is that the decision is not one that is isolated to a single business; it a collective decision.

The Internet is changing. The first article of this series described how the demand for IP addresses exhausted the available supply. IPv6 implements a much larger address space with more than enough addresses for the foreseeable future. The problem from a network management point of view is that IPv4 and IPv6 implement different logical networks. There are ways to make IPv4 and IPv6 work together, such as the dual-stack and tunneling approaches described in the second article of this series, but even these approaches require an implementation of IPv6. It is difficult to formulate a reasonable scenario where a business could maintain for the long term an IPv4-only implementation.

The migration to IPv6 is not an isolated business decision. The Internet is changing and we must adapt to these changes. Just as we all have to agree about which side of the road we will all drive on, we have to collectively decide how we will structure network traffic. Of course, you do not *have* to drive on the same side of the road as everyone else; it is just that the consequences of choosing to operate differently will tend to eliminate those drivers. The same could be said for failing to use common networking protocols, although the consequences of failing to use common network protocols will emerge over the long term. IPv4 will continue to work, but your ability to continue to access external services will degrade over time.

Even if a business decides to operate an IPv4 network internally, it will still have to work with business partners, collaborators, and ISPs who are transitioning to IPv6. IPv4 will continue to work as a networking protocol, but without support for IPv6, you will be limited in the resources and services you will have access to.

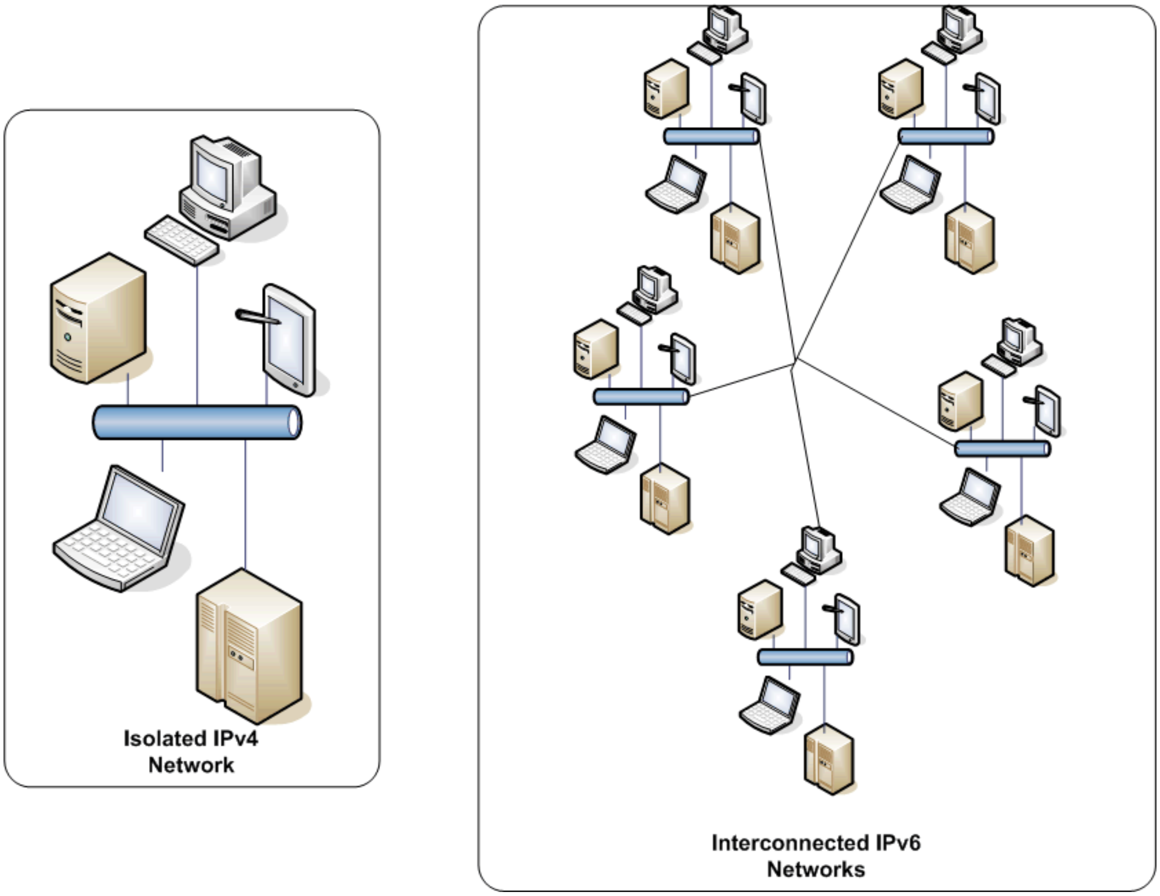

Figure 1: IPv4 networks will continue to function even if there is no migration to IPv6; however, over time, more resources will become inaccessible as they become available only to other IPv6 devices.

Planning the Migration to IPv6

Planning to migrate to IPv6 is a four-step process:

1. Assessing current network architecture
2. Assessing current application requirements
3. Prioritizing the need for IPv6 support
4. Determining which transition strategy to use

Assessing Current Network Architecture

During the network architecture assessment stage, you review an inventory of network devices, such as routers, switches, access points, and so on:

- Do these devices support IPv6?
- If not currently supporting IPv6, are upgrades available to support IPv6?
- What are the configurations of servers and client devices?

This information will be needed to determine whether a dual-stack approach is a viable strategy for supporting both IPv4 and IPv6.

In addition to understanding individual device characteristics, it is important to have a comprehensive inventory of devices and connectivity at the port level. Such an inventory could be undertaken manually, but that option is only practical for very small networks; network discovery tools should be used to collect information on layer 2 and layer 3 network levels. The details collected can then be used to generate maps, documentation, and in some cases, support query support tools.

Assessing Current Application Requirements

In addition to a hardware inventory and assessment, you need to ascertain the same type of information about applications. Do applications make assumptions about running on an IPv4 network—for example, does the application collect and store IP addresses for any reason? In many cases, applications do not have to know the implementation details of the network protocol. One of the advantages of the four levels of the Internet protocols (link, Internet, transport, and application) is that, for the most part, the details of lower levels are hidden by upper levels.

Prioritizing the Need for IPv6 Support

The third step of planning is to prioritize the need for IPv6 support. If a business partner is delivering services over IPv6, only then applications that make use of that partner's services is a clear candidate for early migration. Services that use SSL/TSL-encrypted communication can leverage the built-in encryption of IPv6. At the other end of the priority spectrum, legacy applications that are schedule to be retired may not warrant any substantial effort to migrate them to IPv6.

Determining Which Transition Strategy to Use

With assessments of network infrastructure and application requirements, you can make decisions about which transition strategy to use: dual stack, tunneling, translation, or some combination of the three. The dual-stack approach offers flexibility and minimizes the overhead of tunneling or translating but at the expense of additional resource demands. Translation and tunneling avoid the need for running two network stacks, but each of these has their limitations.

Planning a migration to IPv6 can be streamlined if device and application information is readily available. Asset management systems might contain sufficient details to allow one to quickly assess the configurations of devices. Of course, networks are dynamic and you should consider the dynamic as well as the static aspects of the network.

Importance of Network Monitoring

Networks are dynamic in two ways: the patterns of data movement across the network are constantly changing, and the infrastructure itself changes over time.

Monitoring Network Traffic

Network traffic is constantly in flux. At one point, a data warehouse process is copying large files from a transaction processing server to a staging area, while another time, customers are generating a steady stream of transactions on the company Web site. Although traffic patterns will change from one minute to the next, there are likely to be discernable patterns in traffic. There may be, for example, periods of peak demand in the middle of the night when bulk data copies and backups are performed. There may be spikes in network traffic early in the day as users check their email, run reports, and perform other routine tasks. There may also be longer-term patterns that vary with the time of month or year.

Understanding the variation in network traffic patterns is important to understanding how well service levels are maintained. Simple aggregate statistics such as average latency and average bandwidth utilization are sometime useful but they mask the potentially problematic peak utilization times. It may not help to have a reasonable average application response time when response time during peak demand periods is well below requirements. It is in situations such as these that you need to be aware of the state of the network.

Network awareness is the process of tracking the operations, configurations, and performance of network devices and traffic on the network. Monitoring network traffic helps to verify assumptions about application behavior and network traffic. This is especially important for enterprise applications. The way you use these applications changes over time, and assumptions about application demands on network resources can change over time. When you add to this complex scenario a transition from IPv4 to IPv6, the monitoring becomes even more complex and challenging. You now, in effect, have two networks to monitor. Network monitoring tools are available to help systems administrators, application managers, and network managers collect information about the status of the network and its impact on application performance.

Monitoring Network Configuration

In addition to monitoring network traffic, you should have tools that support monitoring changes in network configuration and devices. Again, this type of management tool is valuable under normal circumstances, but during the transition from IPv4 to IPv6, this tool type can be even more useful because of the additional management overhead that exists during the transition. A special aspect of network monitoring is maintaining an awareness of the security of the network.

Security Considerations

Monitoring traffic should also take into account security considerations. Routine monitoring can provide a baseline of reasonable and expected network traffic patterns. These patterns can be used with statistical techniques to detect significant variations from normal patterns, which can be indicative of a security issue. For example, a download of large files from one server to another may not be all that unusual unless the target server is outside the corporate network and in a country in which the company has no routine business.

Logging, reporting, and analyzing both IPv4 and IPv6 traffic should be done throughout the transition. Attackers do not limit themselves to one protocol. Security monitoring is especially important during periods where configurations are changing and new software is being introduced. There is always a chance of introducing an error or misconfiguring a device, but when many devices are changing at once, there are more opportunities for mistakes.

Summary

The Internet is moving from IPv4 to IPv6. This is a collective decision driven in large part by the exhaustion of IPv4 addresses. To continue to function, grow, and adopt new services, businesses should plan to migrate to IPv6. Fortunately, there are ways to deploy both IPv4 and IPv6 at the same time. Maintaining two logical networks over the same infrastructure creates additional management overhead, but tools are available to address these needs.