February 2010 \$199

# InformationWeek :: analytics

Analytics.InformationWeek.com

# Strategy Session

Presented in conjunction with



# IPv6: Time to Move

Version 6 of the Internet Protocol is the Rodney Dangerfield technology of our time. But if you don't give the coming switchover some respect, it may end up costing you. IPv6 brings new security and performance challenges, and it's coming to a network near you—maybe a lot sooner than you think. In this *InformationWeek Analytics* Strategy Session report, we'll look at what IPv6 means for you and outline three steps to take now.

**By Ray Soucy** 



#### Strategy Session

	U
	-
	Ζ
ш	
0	
	_
ш	
Ш	
$\triangleleft$	C
⊢	

- 3 Author's Bio
- 4 Tech Basics
- 6 Tick Tock, Tick Tock
- 6 Figure 1: 2010 IT Maintenance Investments
- 8 It Doesn't Have to Be Ugly
- 9 Getting It Done
- 9 Procrastination Pays
- 10 3 Steps to IPv6

**ABOUT US** | *InformationWeek Analytics'* experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption best practices gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com*, executive editor **Lorna Garey** at *lgarey@techweb.com* and research managing editor **Heather Vallis** at *hvallis@techweb.com*. Find all of our reports at *www.analytics.informationweek.com*.





# Strategy Session



Ray Soucy Networkmaine **Ray Soucy** is a communications specialist with Networkmaine, a unit within the University of Maine System tasked with providing Maine's research and education community with high-capacity connectivity using some of the newest technologies on the market. Ray has driven Networkmaine's IPv6 deployment efforts for

the past two years. Contact him at www.soucy.org.



# Strategy Session

Tech Basics

**IPv4 allows for approximately** 4.2 billion addresses, which seemed like a lot when it was implemented. But in the early 1990s, concern started to grow that we'd run out. With the proliferation of mobile devices and the desire to connect everything—let's not forget the Internet refrigerator—some predicted that by 2010, we no longer would be able to issue new IP addresses. Now that 2010 is here, and with a world population projected to be double that of available address space before this decade is out, the once laughed-at IPv6 is suddenly finding itself the center of attention among network engineers.

Some background: Today public- and private-sector organizations use Network Address Translation (NAT), a specification that enables IT to assign multiple local private addresses while sharing one IPv4 address for external communications. While NAT has kept IPv4 alive for the past decade, it's just a stopgap—and one that is approaching the end of its usefulness. To tackle the issue long term, the IETF developed the IPv6 protocol, which supports a mind-bogglingly greater number of addresses by moving from a 32-bit to a 128-bit address space that allows for 340 undecillion (3.4 X 10^38) addresses.

Besides allowing unique IP addresses to be assigned to every device on the Internet, IPv6 tackles shortcomings of IPv4 via greater address assignment and gateway selection flexibility, an emphasis on multicast for sharing traffic intelligently, address mobility, the introduction of scoped addressing, and the incorporation of IP security (IPSec). IPv6 clearly has a lot to offer, and yet, it has gone largely ignored. At the Ripe 57 Conference in October 2009, for example, a Google engineer presented research showing that no country had over 1% of addresses using IPv6.

It's not like the government hasn't tried to spur adoption. In August 2005, the OMB issued Memorandum M-05-22, which established the goal of enabling all federal government agency network backbones to transmit IPv4 and IPv6 traffic, and support IPv4 and IPv6 addresses, by June 30, 2008. In June 2009, OMB reported that all major agencies met that dead-

# Strategy Session

Tech Basics

line. However, OMB asked only that agencies demonstrate the ability to transmit IPv6 traffic from the Internet and external peers, through the core network backbone to the LAN; transmit IPv6 traffic from the LAN, through the core network backbone, and back out to the Internet and external peers; and transmit IPv6 traffic from the LAN, through the core network backbone to another LAN. With no requirement to enable IPv6 for services and applications, many felt that the OMB fell short of its goal of promoting adoption. Perhaps not surprisingly then, in a recent *InformationWeek Analytics* poll on government IT priorities, IPv6 was at the very bottom of the heap in terms of perceived success. And if even the government is ignoring IPv6, there's little likelihood enterprises will move to fully implement it—until we actually do begin to run out of addresses, that is.

And that may happen sooner than you think. In fact, we see a two-year window before a lack of IPv6 support causes real pain.

For enterprises, IPv6 adoption is fairly complex and may require outside help. The primary issue is around coexistence and interoperability with the existing IPv4-based infrastructure that will be with us for some time, but there are also security and management issues that make adoption challenging. Fortunately, the OMB mandate did have one positive impact: Native IPv6 connectivity is increasingly becoming available from ISPs, often for little or no additional cost. It's time to get moving on a plan.



# Tick Tock, Tick Tock

Chances are, you're thinking about how many times you've heard that this will *finally* be the year of IPv6. Well, this is not yet another article trying to convince you that IPv6 will revolutionize the Internet—the fact is, IPv6 won't revolutionize much of anything. It might, however, end up costing you money just to stay on par with competitors.

That's because what we call the Internet is becoming a legacy service.

In 2007, the American Registry for Internet Numbers (ARIN) predicted that IP address space would be exhausted in 2010. While we're not there just yet, the clock is definitely ticking loudly enough that Tier-1 service providers have been scrambling to deploy IPv6 on their networks.

Figure 1

# **2010 IT Maintenance Investments**

Please rate how the following technology maintenance projects and investments will be treated in 2010.

1 Investment will get cut significantly	Investment will increase significantly 5
	3.2
	Data center software infrastructure (virtualization, management software, SOA, Web services or other infrastructure upgrades)
	3.1
	Scheduled security/compliance upgrades (e.g. data leak prevention, encryption, e-mail archiving, etc.)
	3.1
	Data center hardware infrastructure (servers, storage, switches, etc.)
	3.0
	Scheduled infrastructure upgrades (e.g. networking, wireless infrastructure, remote office infrastructure)
	3.0
	Upgrades to back office software (financials, ERP, etc.)
2.9	
Upgrades to end user software (productivity apps)	
2.9	
Scheduled upgrades to end user hardware (laptops, desktops, smartphones, etc.)	

Note: Mean average ratings based on a 5-point scale, where 1 is "investment will get cut significantly" and 5 is "investment will increase significantly" Data: *InformationWeek Analytics* Outlook 2010 Survey of 360 business technology professionals



Over the past year, we've seen major players like Google begin to offer services over IPv6, and more recently, popular online content providers like Netflix and YouTube have joined in.

So what's the big deal? You're already connected to the Internet, right?

Yes, but as ISPs need to get more users online, they'll be forced to find new and creative ways to provide access. This means moving to IPv6. However, IPv6 in itself doesn't address the challenge of preserving access to the legacy Internet. As address space becomes increasingly sparse, users will be forced to employ a series of proxies and translators to reach the legacy Internet. The ability of hosts to communicate directly could be crippled, limiting communication and collaboration applications that depend on peer-to-peer connectivity.

If your organization maintains a customer-facing Web site, the upshot is that those proxies and translators will be standing between you and your clients—likely degrading connectivity and the customer experience. The way to avoid this? Get IPv6 in place on customer-facing services today, and start preparing for IPv6 on the LAN tomorrow. You may think you have time, but late last year Comcast announced plans to deploy IPv6 to customers, and today it's in public trials—the first of many such moves.

Thankfully, pieces have been falling into place for the past few years in terms of making IPv6 a reality. With the release of Windows 7, we see a serious attempt from Microsoft to bring enterprise-ready IPv6 to the PC. Building on the IPv6 base that was developed for Windows Server 2003 and Vista, Windows 7 provides a mature and stable implementation of IPv6 for enterprise environments—and it works out of the box.

Don't get complacent, though; IPv6 isn't simple to roll out. It has implications for performance, security and service availability. Your IT staff will need time to get familiar with the technology and plan a proper deployment strategy. This will involve answering a few questions: Can your current network equipment handle IPv6? Do your service providers offer native IPv6 connectivity? What about your servers, do they support IPv6? The answer for most shops is "yes," but these are all issues you need to start addressing now. Waiting until the CEO is upset because his IPv6-only connection to your Web site is slow is not a situation you want to be in.

You have two choices for the changeover: Provide your staff the time it needs to get up to speed on IPv6, or dish out big bucks to get a consultant to opine that all your hardware is



junk. After which, you'll likely be told that the service provider you just signed a two-year contract with doesn't route IPv6 for customers yet, and your network engineers will be falling over themselves trying to make it all work anyway.

Starting to get the picture?

# It Doesn't Have to Be Ugly

Thankfully, the changeover needn't be painful. IPv6 and IPv4 can run side by side on your existing network. Heck, chances are IPv6 traffic is traversing your network now, without you even knowing it—as more OSes and devices enable IPv6 by default, we've seen an uptick in the amount of IPv6 traffic between hosts on the LAN, regardless of whether IPv6 has been officially deployed.

If you need a business justification, security is one of the main motivations: Better to be aware of and manage this traffic than to get blindsided. The security community has already started to issue warnings that, because IPv6 is ignored by most networks, it will become a significant component for malware writers developing techniques for new attacks. If your IT staff doesn't understand IPv6, it can't secure it.

While IPv6 may introduce concerns, it also brings to the table new technology to help build more secure networks. Key to IPv6 is a full end-to-end implementation of IPSec for moving security out of the application layer and end-to-site encryption, replacing the traditional role of the VPN. In fact, Microsoft's new DirectAccess technology uses IPv6 IPSec exclusively to achieve end-to-end and end-to-site security for remote connections.

But don't just operate from a defensive posture. IPv6 provides the flexibility to carry the Internet though the 21st century. As we enter a period of the "two Internets" (customers, partners and suppliers with native IPv6 and those without) businesses will need to adapt to ensure they're able to service everyone.



## **Getting It Done**

IPv6 won't be a hard cut-over. Most legacy devices will never support IPv6, and moving to an IPv6-only network isn't feasible quite yet. While there are technologies being developed to provide IPv6-only networks with access to the IPv4 Internet, our current recommendation for the transition is to run a dual-stack network in which IPv4 and IPv6 coexist. The great thing is about this approach is that IPv6 doesn't become an upgrade, but instead, an addition to your network. IPv6-capable PCs and devices can make use of both IPv4 and IPv6, giving IPv6 preference when available as indicated by DNS, assuming the host is set to prefer IPv6 addresses. Devices without IPv6 support continue as if nothing has changed.

Larger networks will want to pay attention to their address allocation mechanisms. IPv6 offers the ability for devices to autonomously determine their IPv6 addresses; this is known as "stateless" address configuration. Stateless address configuration is a great tool for IPv6, especially on smaller and ad-hoc networks where IP address management concerns are minimal, and is the default for most IPv6 routing platforms. Networks requiring a bit more control will find that DHCPv6 is quickly maturing and works out of the box for most OSes. By disabling stateless configuration on a network and using only DHCPv6, you can control which hosts get assigned IPv6 addresses, much as with IPv4. This functionality may come at the cost of excluding some hosts, such as those running Mac OS X, from using IPv6 unless manually configured, but for some shops the ability to enable IPv6 on a per-host basis can make a rollout on the LAN much less painful.

Finding support in infrastructure gear won't be difficult, either. Windows Server 2008 supports all services in IPv6-only operation. This includes Active Directory for both DNS and DHCPv6. For Unix shops, IPv6 services have been available for much of the past decade.

## **Procrastination Pays**

If you've done nothing, you can pat yourself on the back for your procrastination. It's paid off. Large deployments of IPv6 to date have taken years to complete, usually resulting in lessons learned the hard way. But finally, support has improved, and information has never been more accessible.

Start now getting your IT staff up to speed so your organization can make intelligent decisions about IPv6. Within two years, chances are you will be forced to use IPv6 on some level. Some

say the day will come sooner. And two years is just about the time it takes for a full IPv6 deployment in a midsize to large organization.

Here are three steps you should take now to save money and grief.

#### 3 Steps to IPv6

## 1: Enable IPv6 on outward-facing online services.

These are the services that allow your customers to interact with you over the Internet. They might even be the only way you generate revenue. If these are managed though a hosting or co-location provider, ask your rep what it will take to get your sites talking IPv6. If your provider stares blankly or says it doesn't offer IPv6, start looking for a new partner.

The best rates usually come tied to service commitments; if you're in a contract right now and your provider doesn't offer native IPv6, at least you have time to identify it as a requirement for your next renewal. Most ISPs that support IPv6 offer it at little or no additional cost.

Moving to support IPv6 on these services is often the lowest barrier to entry, and can be a good opportunity to build working experience with IPv6 for your IT staff.

# 2: Identify IPv6 support in hardware.

Start checking to see what gear supports IPv6 so you'll have time to work on getting replacements if needed. You'll probably find that the majority of your infrastructure equipment already supports IPv6, and by including this consideration in purchasing decisions from here on out, you can avoid costly upgrades for the sake of IPv6 in the future.

## **3: Engage your IT staff.**

Finally, make IPv6 a priority with your staff. Have employees focus on getting a test network up and running on the IPv6 Internet. They'll need to start learning about IPv6 addressing, routing and security early on. Don't be afraid to set target dates. It will show them you're committed to IPv6. Taking these steps now could help you avoid the costs of a rushed deployment.