IPv6 Shadow Networks are Here Today
Executive Summary

Many enterprises are planning to transition their working environments to IPv6 over the next two to ten years. But long transition horizons should not fool IT organizations into thinking that all IPv6 issues can be deferred to the future. End points – PCs and Macs as well as smartphones and tablets – are enabled with IPv6 today. Carriers provide IPv6 services, and moderately modern routers and switches are IPv6-ready.

These facts raise a key issue: you may very well have IPv6 connectivity and traffic in your enterprise today. If it’s not in your network policy to allow that, you’re out of compliance. If you haven’t confirmed that your security infrastructure is properly enabled and configured, you have unanticipated vulnerabilities. Best practices suggest:

1. Get visibility into IPv6 traffic today
2. Audit for compliance against IPv6 plans
3. Remediate to regain compliance with IPv6 plans

You need to get visibility into IPv6 traffic – how much, what applications, who’s doing it – to take full control of your IPv6 transitions. Blue Coat PacketShaper provides real-time application and content-level visibility and QoS control of IPv6 and all application traffic on the network. It’s part of a full IPv6 portfolio from the leader in WAN optimization and web security. It lets you understand your IPv6 exposure so you can audit against your plans and remediate as necessary.

IPv6 Shadow Networks are Here Today

Transitions to IPv6 networks, for many enterprises, seem years away. With just 0.51 percent of end users accessing the Internet via IPv6, the traffic is currently low. France has the greatest adoption (4.5 percent), followed by Japan (1.54 percent). And even though IPv4 addresses have been exhausted, network address translation (NAT) technologies, for most organizations, mask a compelling need to migrate the entire network infrastructure to IPv6.

Forget the fact that you maintain overlapping subnet assignments on a spreadsheet. Forget that you can’t get your video conferencing system to talk to a business partner on the outside. Forget that you find your access control lists (ACLs) nearly impossible to manage. Who wants to upgrade the infrastructure to an addressing scheme where you can’t remember all the digits of your favorite FTP server, where ACLs are even more complex and – more importantly – where user PCs and smartphones have public IP addresses that can be reached directly? Sounds scary. Let’s add a year to the migration plan.

The problem is, builders of IT infrastructure have been anticipating IPv6 for some time – at least builders of some parts of the infrastructure. Truth be told, vendors in the user OS space and the web have been further ahead in enabling their software content to be fluent in IPv6. A number of IT equipment infrastructure vendors, however, have been slow to deliver full IPv6 capabilities. (Note: one way to spot technology laggards is to ask vendors if they’re fully IPv6-compatible).

---

Core Infrastructure: IPv6 Enabled. Key Components: Playing Catch-Up

Smart sensor networks, a key driver of IPv6, are increasingly used by utilities, medical device makers, transportation networks, and logistics and inventory management systems. That dangers that may lurk for pacemakers, utility meters, or highway bridge sensors connected to the internet is a subject for another discussion. The sheer eventual volume – billions and billions – of these devices is helping to drive IPv6 adoption. Setting aside those emerging IPv6 use cases, which are highly specialized, are there use cases relevant to the enterprise?

Smartphones and tablets bring the issue directly into the enterprise space [we’re not forgetting PC OS, which will be covered next]. Employees are bringing their iPhones, iPads and Android-powered devices to connect onto corporate networks today. This Bring Your Own Device (BYOD) trend adds to network traffic [content downloads, OS updates, etc.], and the devices have native IPv6 capability. The number of these devices will only grow in coming years. With Apple, IPv6 became enabled with v4 of iOS in June of 2010; Android followed with v2.3.4 in 2011. With those releases, smartphones and tablets can automatically configure IPv6 networking.

PCs – yes, and Macs too – now have native IPv6. Microsoft PC/Server OS history with IPv6 has been a long and deliberate march to mainstream code, beginning with Windows 2001 SP1 and XP in 2001. Vista has a dual stack of IPv4 and IPv6. Microsoft Windows 7 has full-on IPv6, which it uses when speaking with Windows Server 2008. If IPv6 NDP is turned on, these operating systems will all connect IPv6. Users can configure IPv6 connectivity.

Much of the base networking infrastructure has been enabled with IPv6. Cisco, the largest provider of enterprise network infrastructure, moved to full IPv6 support with IOS version 10.xxxxx. Carriers have been offering IPv6 services for a number of years. Here is a summary of IPv6 adoption by vendors:

<table>
<thead>
<tr>
<th>Element</th>
<th>IPv6 Aware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Smartphones and Tablets</strong></td>
<td>Apple iOS (Apple iPhone, iPad) – IPv6 native support with version 4, released June 2010.</td>
</tr>
<tr>
<td></td>
<td>Android (Samsung, HTC, Motorola, LG, etc.) – IPv6 support began with version 2.3.4, released in 2011.</td>
</tr>
<tr>
<td></td>
<td>Apple MAC OS X – Mac OS X has shipped support for IPv6 since Mac OS X v10.1, and enabled it by default since Mac OS X v10.3. Latest version is 10.7.3 released Feb 2012.</td>
</tr>
<tr>
<td><strong>Network and Security Infrastructure</strong></td>
<td>Network Switches and Routers – Cisco, Juniper, HP, and Huawei have also supported IPv6 in their operating systems. Features supported by vendors have changed from year to year.</td>
</tr>
<tr>
<td></td>
<td>Firewalls – Similarly, CheckPoint, Juniper Netscreen, and Cisco Pix have supported IPv6 for years. The key question here is feature parity.</td>
</tr>
<tr>
<td></td>
<td>WAN Optimization – Again, feature parity with IPv6 is key. Many vendors claim IPv6 capability, but that claim only applies to a subset of their available features. Blue Coat is the only WAN optimization vendor that provides all acceleration services over IPv6; Riverbed and Cisco do not.</td>
</tr>
</tbody>
</table>
We can see, then, that even though some of the infrastructure is enabled, the biggest concerns around IPv6 technology are the lack of feature parity (Source: Arbor Networks):

IPv6 Security Concerns - Source: Arbor Networks

-> Firewalls – Can they be configured for IPv6 policies? Is VoIP (or other specific or advanced features) IPv6-capable?

-> Web security – Can you see IPv6? Can you write IPv6 policy and enforce it? Can you terminate IPv6 traffic, and rewrite it in IPv6 or translate it to IPv4?

-> WAN optimization – Can you optimize IPv6 traffic? Does your CIFS protocol acceleration work over IPv6? How about MAPI? Too often, optimizers can apply basic data-reduction technologies, but have not advanced all their capabilities to IPv6.

The second biggest issue according to that same Arbor survey was visibility into IPv6. If you’ve set up a transition plan over the next two to five years, you may not even be looking for IPv6 traffic – because you don’t think you need to, or because your tools are incapable of doing it.

An IPv6 Planning Scenario and its Implications

Now, does IPv6 just drop into the network? No. It doesn’t spontaneously spawn and set up connectivity. Let’s look at a possible scenario. Say you have a plan that specifies supporting IPv6 at some point in 2014 – today, a distant inevitability. In the meantime, you’re rolling through some major infrastructure upgrades. You’ve just got a new load of Cisco 7300’s. You’re looking ahead to CCIE certification, looking for some bragging rights, perhaps adding some good copy to your résumé, and saving the work of reconfiguring until later – so you implement dual-stack IPv4/v6 configurations of your new products. You’re ahead of the curve, dropping some OSPFv3 or multi-topology IS-IS with a side of DHCPv6 and DNS for IPv6. If your desktop infrastructure is locked down and unable to set up IPv6 connectivity that’s fine; no IPv6 here. You’re compliant.

But what happens if your PC group hasn’t locked down the PCs and desktops? What about people who are bringing in their own iPhones or Androids or Macs with OSX? Some curious user – an engineer or a gearhead in the desktop PC group – configures units for IPv6. Suddenly, you have IPv6 in your network.
Compliance and Covert Channels

There are two main concerns with unauthorized IPv6 traffic on your network: compliance and covert channels. The compliance issue arises when IPv6 traffic appears before it’s explicitly supported in your IPv6 transition plans. Covert channels refers to the risk that the security infrastructure can’t protect IPv6 communications, which most commonly move through web gateways.

Remember that IPv6 transition plan that we talked about earlier? Well, laying down a policy that you won’t support IPv6 until 2014, then rolling out infrastructure that actually enables IPv6 support before that date, opens up significant compliance issues. In fact, stating policy and a plan and not enforcing it is worse than not having stated policy at all (apparently, being clueless is more defensible legally than articulating a policy that is not enforced). The transition timeline is aligned with other parts of the infrastructure – the PC group, firewalls, web security, and access and content policies. Your infrastructure may be ahead of the curve, but the IPv6 truck may be coming around that curve at high speed.

Even worse, if you haven’t set up (or configured) traffic that’s bypassing your web security and firewall controls, it may be that covert channels are being set up with the outside world. Modern versions of firewalls are IPv6 capable, but if the installations haven’t been updated to versions that support IPv6, or if they haven’t been configured, you may have a problem. Some specific features may not be fully IPv6 enabled. An IPv6 VoIP exploitation may be possible, but the probabilities are in your favor. But what about web access?

The Web is the scariest part of the world today. Malnets lurk in IPv4 and are developing rapidly in the IPv6 space. IPv6 has distinct advantages, but it introduces a number of security issues. Some of those issues are explored more deeply in the upcoming paper, *IPv6 - a Catalyst and an Evasion Tool for Botnets and Malware Distribution Networks*, by Qing Li, Chris Larsen and Tim van der Horst. The issues include:

- The change from a tightly controlled IPv4 addressing scheme protected by NAT
- Publicly addressable IPv6 endpoints inside your network
- Vulnerability to more rapidly changing malware networks that leverage IPv6
- Specific targeting of IPv6 devices, including mobile devices

Outbound port 80 access is probably enabled by your firewall policy – which moves the problem to your web gateway infrastructure. Blue Coat’s Secure Web Gateway technology not only has full IPv6 support, but even has IPv4-IPv6 network gateway services to help with transitions. This raises key questions:

- Are you full security-services IPv6 compliant? Can you see IPv6? Terminate it? Translate?
- What security policies should you put into place for IPv6?
- How should you set up security policy migration from IPv4 to IPv6?
**Best Practices for Eliminating IPv6 Shadow Networks**

To take control of your IPv6 network traffic, and to ensure that you get back into a state of compliance and remain compliant, you need to take these key steps:

1. **Get visibility into IPv6 traffic today.** This is the most critical step, but it’s the simplest step when you have the right set of tools. You need to ask these questions: Do I have IPv6 traffic? How much? What impact is it having? What applications are driving it? What users? We detail this in the following section, Getting Visibility.

2. **Audit for compliance against IPv6 plans.** Once you’ve identified IPv6 traffic, you need to evaluate that usage against your IPv6 transition plans. Here are some key questions to ask:
   a. **IPv6 use today:** Does it comply with transition policies and plans? Do you have to add exceptions to accommodate experimental or other acceptable use?
   b. **Security policy plans for migration from IPv4 to IPv6:** What are they? Do you need to expedite basic configurations to accommodate use cases?
   c. **Firewall policies:** Are firewalls properly configured? For basic and application-specific functionality?
   d. **Web access policies:** Are they IPv6 aware? Are they configured to fit use cases?
   e. **PCs:** Have you locked down the enterprise-owned PC configurations to avoid unanticipated traffic?
   f. **IP address management (IPAM):** Have you configured addresses properly to avoid unanticipated use cases?

3. **Remediate and monitor to regain compliance with IPv6 transition plans.**
   a. **Alter IPv6 transition plans to fit acceptable use.** You may have found legitimate uses of IPv6 in your enterprise that weren’t anticipated when you did the original planning. At this point, recognize that you can add support for experimental and other acceptable uses of IPv6 that have been identified. Re-specify acceptable IPv6 config/traffic today and at upcoming milestones. But make sure the acceptable uses are secure. If you have implemented dual-stack architecture, take the next step to assure that you’re eliminating covert channels to the outside world:
      i. Check access and general security infrastructure and policies.
      ii. Check firewall configuration, as well as router/switch infrastructure.
      iii. Configure Secure Web Gateway policies to include IPv6.
   b. **Shut down IPv6 access that is out of compliance.** Whether it’s locking down the endpoints, eliminating the dual-stack implementations, or more tightly controlling the IPAM and routing policies, eliminate the parts of the infrastructure that enable unauthorized uses that take you out of compliance.
   c. **Control via change management.** Make IPv6 access part of your change management processes. This helps prevent unauthorized, untested usages and can help you reduce future troubleshooting and assessments. The idea is to get your network compliant, then manage changes to ensure that you remain compliant, a common ITIL practice.
   d. **Monitor traffic for ongoing assurance of compliance.** Compliance is an ongoing process, not a one-time check of traffic. Change management will provide a process by which new uses can be implemented in a controlled way. But you should remain vigilant to uses that may bypass these formalized channels. By properly configuring your monitoring tools, you can ensure that you become aware of new influences in the network, whether it’s IPv6 or potentially disruptive applications. Adaptive Response, described in the next section, simplifies the monitoring of IPv6 traffic.
Getting Visibility into IPv6 Today

We’ve spent some time outlining the problem and steps you can take to manage through the issue. Here we get into more detail about that first step – Getting Visibility – as well as how to set up ongoing monitoring of your network to assure continued compliance.

At this point, we’re focusing on Blue Coat’s PacketShaper as a means of getting visibility into IPv6 traffic. We’ll start with the steps into discovering and monitoring IPv6 traffic, then talk a bit about the functionality of PacketShaper that enables this process. You may discover that PacketShaper is not only effective in spotting IPv6 traffic, but that it gives you a unique application and content-level view of all your traffic – not just IPv6. With that information, you can drive powerful QoS control policies and report usage by application. But let’s get to the specific process to get visibility:

- **Deploy a PacketShaper on the WAN or Internet link.** The appliance acts as a transparent bridge, evaluating all traffic in real time. It can be deployed inline or out of line. Inline mode is preferred, because it enables you to configure shaping policies that actually control traffic. Out-of-line deployments are also available, via taps, span or mirror ports; while they’re simpler to insert in light of network change control, their use disables the ability to apply shaping policies.

- **Enable Auto-Discovery and Scan for IPv6 Traffic.** Once Auto-Discovery is enabled, PacketShaper classifies all the traffic on the network, at the application and content level. PacketShaper provides a granular view of network traffic, grouping more than 700 applications and tens of millions of web sites into high-level categories. As part of that discovery process, PacketShaper will automatically discover IPv6 traffic on the network, populating a separate portion of the “class tree” and providing insight into the types of IPv6 traffic you have on the network. It’s not typical to have massive amounts of IPv6, but this will provide insight into how much resource it consumes.
IPv6 Shadow Networks are Here Today

- **Identify the Who.** PacketShaper top-talkers analysis provides IP information about the hosts using IPv6 applications. The above screen shot shows the internal host, the external host, and the specific applications being used.

- **Report on bandwidth consumption by application and content type.** The implementation of Auto Discovery has the benefit of not only identifying IPv6 traffic, but also classifying all applications on the network. How much multimedia video traffic consumes your WAN? What about social networking? Wall posts, video and gaming can all be broken out separately. In the example Top Ten view shown here, we see that YouTube is dominating this T1 (1.54Mbps) link. The classification traffic goes far beyond port 80.

- **Shape traffic to contain disruptive traffic and unauthorized IPv6 traffic.** IPv6 traffic typically isn’t driven by an application that is taking massive amounts of bandwidth – though it may be. We usually see multimedia downloads or even anti-virus updates driving performance issues.

- **Configure an automated alert for the emergence of new IPv6 traffic flows.** To maintain a continuous view of IPv6, you can set up an ongoing monitoring configuration that provides an alert if IPv6 traffic pops up in the network. This is known as adaptive response, and it lets you configure PacketShaper to send an SNMP trap or an email when IPv6 traffic is detected. If you want to use a more advanced action file, you can create a policy for dynamic containment of potential impacts.
Visibility: Understand What’s Going On
PacketShaper provides the most intelligent real-time view of application traffic available on the market today. Whether it’s seeing IPv6, tracking your core enterprise applications, or categorizing all your web-bound SSL, PacketShaper classifies, measures and reports network traffic at the application and business level. Here are some key capabilities:

- **Real time auto-discovery and classification of applications on the WAN and internet.** As we stated earlier, the PacketShaper bridges traffic and automatically classifies it and sorts it into classes. Classification is very granular and specific, but we simplify it by grouping applications into seven high-level categories.

- **Application and content view of your traffic.** PacketShaper uses a number of different approaches – Layer 7 technologies, behavioral patterns, protocol validation and content categorization – to identify more than 700 applications and tens of millions of web sites. PacketShaper even gives you flexibility to create your own classifications using IP information, Layer 7 information, SOA directories and other parameters to identify applications of which you may not be aware.

- **A real-time web classification engine powered by WebPulse.** When web traffic appears that PacketShaper hasn’t seen before – whether HTTP or SSL – it leverages Blue Coat WebPulse™ cloud infrastructure to provide real-time categorization.

- **Detailed usage and troubleshooting.** PacketShaper tracks over 100 statistics for every traffic class that is identified. Not only peak and average bandwidth usage, but also end user response times (separated by network and server response times), TCP health, host information and more.

- **WAN budget consumption.** The application and content level measurements of bandwidth allow you to report how much budget is being consumed by specific applications. How much is taken up by recreational traffic like YouTube, social networking, gaming and general web browsing? How much is actually allocated to core applications?

Control: Reclaim Bandwidth, Contain Disruptive Applications, and Assure Core Performance
Once you have identified traffic at an application and content level, you can proceed to make intelligent shaping decisions. Certainly routers, WAN optimization equipment and other network elements have QoS capabilities. The problem is that the level of intelligence at which they operate is based on network port numbers and other IP information. In a world where the vast majority of applications work on web interfaces over ports 80, 8080 and 443, you need a higher level of intelligence to make shaping decisions. That’s where PacketShaper’s QoS controls come in. Here are some key capabilities:
IPv6 Shadow Networks are Here Today

- **Reclaim 20 to 60 percent of WAN bandwidth (and WAN budget).** Do this by containing recreational applications. Recreation often consumes 40 to 60 percent of bandwidth. A simple partition in which you allocate 20 percent of traffic to recreation allows you to cap YouTube, ESPN, and other video and recreational sites.

- **Assure the performance of mission-critical applications.** Reclaiming bandwidth from recreation often relieves the network of peak capacity issues, fixes performance related to bandwidth constraints, and realigns your network with enterprise focus. In addition, you can put explicit guarantees at the application level – per application, even per flow – to make sure your most critical applications perform to expectation.

- **Manage internet traffic asymmetrically.** A single internet link can often service an enterprise’s cloud and SaaS-connected applications, VPN traffic, and web presence, along with all the general internet access from employees. Blue Coat allows you to segment bandwidth and protect key internet use cases from employees’ overuse of entertainment and recreation, including Facebook gaming and video. Patented TCP rate control throttles lower-priority traffic to assure bandwidth for important use cases.

- **Allocate bandwidth fairly among like users for VDI and other.** Multiple users at a remote site often contend for bandwidth, especially in virtual desktop infrastructure deployments. One user with a bandwidth intensive YouTube session can overwhelm other users who are using interactive applications. Dynamic sub-partitions fairly allocate bandwidth partitions for VDI or other applications on a fair per-user basis.

- **Deploy voice and video conferencing across internet links.** Modern MPLS networks often provide bandwidth priority for voice and video conferencing. Operating those technologies over internet access, however, often requires PacketShaper to preserve bandwidth for each video session or voice call.

- **Contain disruptive enterprise applications.** Even useful enterprise applications can be disruptive. For example: when large anti-virus files are distributed, or remote backup processes are triggered, or users start up a desktop video conference using MS Lync, they can suddenly consume significant amounts of bandwidth, causing performance and capacity issues for the rest of the applications. Application-level controls assure that even these enterprise applications don’t completely overwhelm more sensitive and mission-critical applications.
Get control of IPv6 now. And plan to be successful.
Applying Blue Coat technology to the growing presence of IPv6 can put you back into compliance – and keep you there. The clear visibility delivered by Blue Coat PacketShaper makes it possible for you to set policy for all internet traffic, including IPv6. You set limits on recreation traffic, protect performance of mission-critical applications, and dramatically reduce bandwidth and budget. Let us show you how.

A Complete IPv6 Transition Tool Set
Blue Coat provides the ability to visualize, secure and accelerate IPv6 (with IPv4) applications and traffic that helps businesses drive growth and productivity while ensuring compliance and security at the same time.

-> Network/Internet Visibility and Control: Packetshaper (release 9.1) provides full visibility of IPv6-based applications and Internet-based services traffic and enables full bandwidth control for mixed IPv4 and IPv6 traffic. Visibility and control for proactive management and prioritization of WAN and Internet application and network traffic.

-> Web Security: ProxySG Proxy Edition removes many of the barriers to migration. Security risks are present in both transition and in the native IPv6 environments. ProxySG’s complete IPv6 support enables policy-aided migration without compromising on security. ProxySG also allows complete and intelligent policy-based management of traffic, applications, and content.

-> WAN and Internet Optimization: MACH5 can fully optimize and accelerate IPv6-based application or Internet traffic along with IPv4-based applications and traffic to provide reduced bandwidth costs and greater performance for applications and users.