

Preparing your organisation for the coming of IPv6

Shirleen Heah, Managing Consultant – National Business Consulting,
Dimension Data Australia



Contents

Abstract	01
Analysis	01
Background	01
Understanding IPv4	02
Introduction of IPv6	03
Reasons for building IPv6 capability	03
When to consider moving to IPv6	04
Factors to consider when moving to IPv6	05
Risks of not having IPv6 capability	05
Level of IPv6 adoption in Australia	06
Preparing for the coming of IPv6	07
Recommendations	07
Conclusion	07
Additional details	10
IPv4 address allocation	10
Last of IPv4 address allocation	10
Who is building IPv6 capability?	11
Appendix A: Sample list of automated inventory software vendors	12

Abstract

There has been concern in the industry about IPv4 address space running out. Although the central registrar of the Internet – the Internet Assigned Numbers Authority (IANA) – exhausted its free public IPv4 address pool in February 2011, **this has no immediate impact on most service providers and enterprises**. Most of these organisations have more than enough public IPv4 addresses for their needs. The Internet will also not suddenly “cease to exist” because the IPv4 address pool has run out. Enterprises on IPv4 can still communicate with other enterprises and customers who are still using IPv4 protocol.

However, **the day will come** when every enterprise would need to either migrate to IPv6 or build a capability to communicate externally with IPv6 endpoints. The growth potential of enterprises without IPv6 capability will be limited if they are not able to communicate with new and existing customers and business partners who are on the new protocol.

To mitigate this concern, the enterprise should prepare itself for the day when it would need to be IPv6-capable. It should start educating itself and take stock of its inventory to understand the current state of its environment. Then, it should develop a strategy to communicate with IPv6.

The moment to embark on this journey is to start preparing for this capability now.

Analysis

Background

There has been a lot of hype over the past few years about the coming of Internet Protocol version 6 (IPv6) to replace Internet Protocol version 4 (IPv4) to ensure that the Internet can continue to support **the predicted growth**, especially with the introduction of emerging markets and the increased use of mobile devices.

IPv4 is the current most popular Internet Protocol [IP] for enterprise networks and has been for the past decade. It is the standard that most Internet and Internet-derived networks (intranets and extranets) use today.

It is well understood that the IPv4 address pool will be exhausted, as there is a finite number of IPv4 addresses. The exhaustion may not occur today or even in the next year because it is believed that most enterprises have more than **sufficient** public IPv4 addresses for their needs – but it will occur sometime in the next few years.

The question then is: what are enterprises doing to prepare themselves for the ultimate end date when there are truly no more IPv4 addresses to be allocated for use?

“There has been a **lot of hype** over the past few years about the coming of Internet Protocol version 6 ...”

Understanding IPv4

Traditionally, IPv4 address allocation was handed out in a “class” system. Each class was allocated a standard number of IP addresses, with:

- Class A having 16 million contiguous IPv4 addresses;
- Class B having 64,000 contiguous IPv4 addresses; and
- Class C having 256 contiguous IPv4 addresses.

This method of allocation was **inefficient**. For example, an organisation that could demonstrate a need for more addresses than, say, a “standard industry” allocation (e.g. Class B) could only be provided with the next higher class (i.e. Class A). This meant that the organisation would be

allocated a far greater number of IP addresses than necessary (i.e. 16 million addresses versus 64,000 addresses), and there may be some unused IPv4 addresses remaining within the organisation.

What is the problem regarding IPv4?

There are issues associated with the pending exhaustion of IPv4 addresses even though there is **no apparent immediate impact** on most enterprises – most enterprises will still have more than enough public IPv4 addresses for their needs in the near future even after the IANA has exhausted its free public IPv4 address pool.

Firstly, the day will come when there are truly no more IPv4 addresses to

be allocated for use. When this day arrives, the Internet will not be able to continue to grow because an IP address is required to participate in the Internet.

Secondly, the value of the Internet grows as the number of connected hosts and servers grows. If no more hosts can be added because there are no more IPv4 addresses, or if the hosts can be added but cannot communicate due to the use of different protocols, the Internet as a communication medium will no longer increase in value or increase in value at the same rate. Connections that can only communicate partially with the rest of the existing Internet will not have the same benefits as those that can communicate fully.

“...the value of the Internet grows as the number of **connected hosts** and servers grows.”

Introduction of IPv6

IPv6 is the next version of IPv4 – there is no IPv5 – and has been in existence since the mid-1990s. It was developed as the long-term solution when the Internet first experienced the possibility of IPv4 address exhaustion.

IPv6 has not gained much traction since its inception because the short term solutions, the Classless Inter-Domain Routing (CIDR) system and Network-Address Translation (NAT), have been efficiently extending the lifespan of IPv4.

- The CIDR solution did away with the class (A, B and C) boundaries. Instead, it allowed both address allocation and routing to have a floating boundary between the network and host portion of the IPv4 address, thus avoiding wasting IP addresses.
- The NAT solution is the practice of multiplexing addresses and is most commonly used to share

one or more globally-routed IP addresses among a larger number of computers using private or unrouted IP address space. It has been very successful as a method of reducing IPv4 address consumption.

IPv6 has been designed to provide a large increase in address space compared to IPv4. It supports 340 trillion, trillion, trillion (2^{128}) addresses compared to IPv4, which only supports 4.3 billion (2^{32}) addresses, thus ensuring that the Internet will effectively not “run out” of IP addresses.

Well, at least not in this lifetime.

Proponents of IPv6 believe that IPv6 will provide increased integrated security¹, increased quality of service mechanisms and better routing stability. Functionally, IPv6 also supports auto-configuration and mobility.

Reasons for building IPv6 capability

IPv6 deployment has been building slowly but is expected to gain momentum over the next few years due to the imminent shortage of IPv4 addresses.

Currently, enterprises are integrating IPv6 into their networks for the following reasons:

- Need for massive address space due to the nature of their business (e.g. public network operators such as mobile operators, cable TV providers and public utilities);
- No longer able to obtain IPv4 addresses to support organisational growth;
- Growth in the countries’ Internet usage (Asia and developing countries); or
- Mandated (by governments), including as a requirement to win (government) contracts.

1. To organisations that see NAT as security and because IPv6 does not require NAT, this appears to signify a reduction in the security of IPv6. To address all user concerns related to networks without NAT, the Internet Engineering Task Force (IETF) developed RFC 4846, *Local Network Protection for IPv6*, which provides guidelines and explanations of IPv6 features and configurations that match the perceived benefits of NAT.

When to consider moving to IPv6

From an enterprise perspective, the case to transition to IPv6 is driven by the interaction between the enterprise and its systems, partners, suppliers and customers. For example, enterprises will need to be able to communicate with external IPv6 endpoints if:

- Their customers are using Microsoft DirectAccess (an option for secure remote access over the Internet) on Windows Server 2008 and Windows 7;
- They interact with network systems that connect the physical world such as sensor networks (e.g. smart meters) and industrial automation; or

- Their Internet customer base is natively IPv6; i.e. if their Internet customers are predominantly in Asia – Japan, China and Korea – and other developing countries, and/or mobile users.

The following four questions will help an enterprise determine if and when it needs to build IPv6 capability:

- Is there a mandate for the enterprise to transition to IPv6?
- What is the enterprise type?
- With which organisations does the enterprise (want to) work?
- Who are the enterprise’s customers?

Category	Possibility of transitioning to or building IPv6 capability
IPv6 mandate	If there is a mandate for the enterprise to be IPv6 compliant, the enterprise will have no choice but to either start planning its transition or build its capability and be one of the first adopters of IPv6. This category of IPv6 adopters include suppliers working with organisations that are or will be using IPv6.
Enterprise type	If the enterprise is a large organisation/public utility company (e.g. serving the utility smart grids or smart cars) or public network operator (e.g. ISP infrastructure networks, telecommunication companies and carriers such as cable TV providers and mobile operators with a large client base of smart phone and voice over IP users), it would be a likely candidate to migrate to IPv6 in the coming years as it would need to deliver IP connectivity to millions of end-points that have not been previously addressed (e.g. mobile phones, set-top boxes and utility meters) to enable identifiable new services).
Type of partners	An enterprise would need to have IPv6 capability if it is connected to IPv6-enabled business partners. This does not mean that the enterprise must migrate its entire infrastructure to IPv6; it is only required to create the ability to communicate with the external IPv6 endpoints at its partner sites.
Customer base	Emerging markets and mobile users will be the most significant IPv6 users. An enterprise would lose its existing customers or not be able to obtain new customers if it is not able to communicate with the emerging markets and this broad set of mobile users.

The findings from this research showed that even if the enterprise has not decided to migrate its entire network to IPv6, it should start preparing for the capability to support its remote IPv6 partners and customers, and provide gateway services to its IPv4 applications.

Factors to consider when moving to IPv6

The migration from IPv4 to IPv6 has been likened to resolving the Y2K issue, but without a looming deadline. It is, however, not a networking-only issue. It affects the whole enterprise and requires cross-functional group participation, with a high level of synchronised activities. Minimally, the enterprise needs to address the following areas when planning to migrate its environment to IPv6:

Networking equipment and services:

WAN routers will need to be upgraded, and hardware may need to be upgraded if performance is affected. The following may also need to be upgraded to ensure performance is not affected: LAN switches, hardware and software; WAN optimisers; Domain Name System (DNS) and directory services. The investment required to upgrade the entire network to IPv6 to an acceptable performance could be substantial.

Network bandwidth: Using IPv6 can reduce bandwidth efficiency. Enterprises will need to determine the additional overhead introduced by IPv6 and ensure sufficient bandwidth is purchased and allocated.

Operating systems: Enterprises need to consider client PC and server requirements, as processing the larger IPv6 header usually reduces

performance. Although the reduction in performance may not be noticeable at the desktop, the server infrastructure may require significant upgrade just to support the same workload as was supported under IPv4. The latest operating systems typically have IPv6 built in or installed as a separate feature. Others may require upgrade or third party IPv6 software added.

Software networking applications:

Enterprises that opted to run software-based networking servers such as proxies and load-balancers may need to update their old version applications. If other backward compatible changes have made their way into the codes, the configuration settings and tweaks will need to be thoroughly tested to ensure that they still work the way they should before going live with the upgrades.

Other networked devices and tools:

This is one of the most challenging areas of IPv6 transition as some of these devices and tools may not be within the responsibility of the IT department. This group of devices are the non-PC devices connected to the IP network such as: IP phones, printers, PDA and cameras. Additionally, enterprises need to understand their security devices such as firewalls and intrusion detection systems as many security devices do not offer equivalent capabilities in IPv6 as compared to the functionality for IPv4.

Middleware and application software:

A significant number of software in environments where performance is critical, such as most middleware, accesses the network directly rather than via the protocol stack in the operating system. Finding out which software does this and then configuring or rewriting the application is the most challenging part of IPv6 migration. Although they are addressing this issue, many vendors of packaged applications and off-the-shelf software are unable to confirm their software in this regard.

Risks of not having IPv6 capability

When IPv4 address allocation finally and truly ceases to be available and most Internet participants and users are mainly using IPv6, the enterprises that are not IPv6-capable (either no IPv6 or NAT capability, or have not yet transitioned to IPv6) may be constrained in their ability to participate in the Internet.

IPv4 address structure and protocol formats are not compatible with IPv6, and the two protocols will not be able to communicate with each other.

An enterprise's growth potential will be limited if it is unable to communicate with new and existing customers and business partners who have moved to the new protocol.

Level of IPv6 adoption in Australia

At the time this paper was written, there has not been a single known enterprise, government or private organisation in Australia that has transitioned to IPv6. Australia is still in the very early stages in the IPv6 lifecycle, with only a few organisations starting to develop IPv6 strategies and plans, and conducting limited discovery of their networks to understand the status of the devices.

The limited understanding and knowledge of the product, combined with the lack of technical skills, have been major contributors in the slow adoption of IPv6. Organisations are planning to “wait and see”, as lessons learnt from overseas (mainly from the United States and Europe) have been discouraging due to the number of issues that have become apparent during the transition, including:

- **Operational readiness:** Having IPv6-compliant products does not necessarily mean that the devices are ready for operations. It is not merely an act of directly replacing a product currently running on IPv4 with an IPv6-compliant product (e.g. replacing existing router with IPv6-compliant router) or a roll forward of IPv4 features onto IPv6. The transition process is more complex and requires understanding of the new product functionality and requirements, and conducting thorough testing of the business applications (for example, SAP) to ensure that they can be fully operational in IPv6.
- **Sufficient capacity:** The IPv6 header is larger than IPv4, and requires more bandwidth for the network to achieve the current level of performance at the very least. Otherwise, the network and server performance will be adversely affected, and this will be detrimental to the support for the transition.
- **Service management processes:** The service management processes will need to be reconfigured to manage the new environment in terms of hardware performance and configuration items’ dependencies. This additional ongoing activity needs to be costed and included in the transition budget and plan.
- **Lack of skills:** There is a lack of understanding of IPv6 features. As a result, the first generation roll-outs outside Australia did not include all the IPv4 functionalities in use. Australian IT organisations should establish training programs to ensure that all IPv6 desired functionalities are rolled out during the transition process.
- **Phased approach:** A detailed, step-by-step approach is recommended for IPv6 transition so that the current infrastructure is not disrupted. There is just too much risk to migrate the infrastructure in a “big bang”. The transition strategy should ensure that IT organisations can successfully deploy IPv6, that it performs to business expectations and can be managed in accordance with industry standard service levels.

“Australia is still in the **very early stages** in the IPv6 lifecycle, with only a few organisations starting to develop IPv6 strategies and plans ...”

Preparing for the coming of IPv6

IPv6 is coming and will affect everyone on the Internet sooner or later. When IPv4 addresses truly and finally run out in the next few years, enterprises may be forced to enable IPv6 capabilities externally or use NAT to communicate if they want to connect to new Internet consumers and business partners, or existing customers and organisations who have been IPv6-enabled.

So, how does an enterprise facing this onslaught go about preparing for the day when it has to either transition to, or communicate with, IPv6?

The enterprise should embark on a journey that will lead it to IPv6 capability, whether it be from transitioning its entire infrastructure or just creating an ability to communicate with external IPv6 endpoints, by:

1. Assessing the enterprise
 - a. Conduct an inventory of the enterprise's existing IPv4 addresses and utilisation.
 - b. Take a comprehensive inventory of IPv6 readiness of all network devices within the enterprise.
2. Requesting funding and support
 - a. Develop the business case to create the ability to communicate with external IPv6 endpoints or transition the infrastructure to IPv6.
 - b. Obtain commitment from project sponsor and support from senior management. This is an expensive exercise and is a multi-year project.
3. Shaping the journey
 - a. Develop IPv6 strategy.
 - b. Develop IPv6 capability plan.
4. Designing the IPv6 solution
5. Implementing the IPv6 solution
6. Managing the IPv6 solution
7. Optimising the IPv6 solution.

The remainder of this paper will discuss *Step 1: Assessing the enterprise*, focusing on how to conduct an inventory of the enterprise's existing IPv4 addresses and utilisation, taking a comprehensive inventory of all the network devices and assessing their IPv6 readiness.

Assessing the enterprise: Inventory IPv4 addresses and utilisation

Taking an inventory of the enterprise's IPv4 addresses enables the enterprise to understand where and how its IP addresses are being used. This is the most urgent step, as the ability to see this current status will enable the enterprise to analyse how soon it will run out of IPv4 addresses (if it does) and in which specific location, so that it can plan its mitigation strategy.

Many large enterprises have a number of IP address assignments spread across divisions and departments. Often, enterprises acquire address space as the result of mergers or acquisitions. Multinationals typically have IP addresses in each of the regions in which they do business. Centralising IP address management and having a complete list of all IP address space that has been assigned to the enterprise will provide the enterprise with a complete picture and enable it to efficiently use this increasingly scarce resource in the future.

Additionally, it has been anticipated that the public IPv4 address space will become a financial asset, and enterprises will be obliged to account for these assets and their utilisation.

If the enterprise has more than sufficient IPv4 addresses for its own needs and growth, it may want to consider the opportunity to participate in the commercial trading of IPv4 addresses with other organisations, subject to the approval of the Regional Internet Registry (RIR). This is only recommended if the enterprise understands and has a full picture of its usage and the current status of all its IP addresses.

**Assessing the enterprise:
Comprehensive inventory of IPv6
readiness of all network devices**

The next step is for the enterprise to create a comprehensive inventory of all network devices to understand their IPv6 readiness. This will enable the enterprise to determine where and how its applications deal with IP addresses, and especially how they touch business partners and consumers externally. The enterprise could then conduct an impact analysis on any changes it makes to the infrastructure, and ensure that all changes are thoroughly tested before any changes are put into production.

This asset inventory would assess IPv6 status of each type of hardware and software, indicating:

- If the asset is IPv6 capable, and at what performance.
- If the asset is not IPv6 capable, the upgrade required to make it IPv6 capable.
- If the asset is independent of the IP address.
- If the asset's IPv6 status is unknown, and testing is required for in-house developed applications or a third-party/vendor is providing information.
- The expected life of the asset, as testing is not required if the asset is no longer required before it needs to be IPv6 capable.

Network devices that need to be identified include:

- Servers, including web and network;
- Network equipment, including routers and switches;
- Firewalls;
- Desktops;
- Peripherals, including printers and hand-held devices;
- Applications residing on the network equipment;
- Operating systems;
- Host components – any device with an IP, layer-3 interface; and
- Network providers.

There are automated inventory software tools in the marketplace today to assist the enterprise in the discovery of all network-connected devices on the network, including external facing services such as email and web.

The enterprise may also need to perform some of the discovery tasks manually when there are non-PC devices connected to the IP network that are outside the responsibility of, and are not known to, the IT department.

It is a major challenge for most enterprises to keep their master databases up to date, and to maintain a full and complete list of all their configuration items. However, without a comprehensive inventory of all the enterprise's configuration items, the enterprise will not be able to make a full and complete assessment of the impact of moving to IPv6. Without this information, it is a huge risk for the enterprise as the negative impact of any change to its systems will have a direct effect on its ability to communicate with its external facing customers and business partners.

“... without a **comprehensive inventory** of all the enterprise's configuration items, the enterprise will not be able to make a full and complete assessment of the impact of moving to IPv6.”

Recommendations

The enterprise needs to prepare itself for the day when it would need to take action towards having IPv6 capability.

- As a first step, the enterprise needs to educate itself. It needs to take stock of its inventory and understand the current state of its environment.
- Then, it needs to develop a strategy to mitigate all its known risks and decide how it needs to communicate with IPv6 – either by transitioning its entire infrastructure or by creating the ability to connect and communicate with external IPv6 endpoints.

Conclusion

Organisations need to bear in mind the following when transitioning to IPv6:

- An IPv6-compliant product does not necessarily mean that the device is operationally ready without thorough testing and understanding of the product features and requirements.
- The business applications (for example, SAP) might be dependent on IPv6 operations. As a result, thorough application testing is needed prior to IPv6 release to production.
- Sufficient bandwidth needs to be purchased and allocated for the additional overhead introduced by IPv6 to ensure no reduction in network and server performance.
- The service management processes will need to be reconfigured to monitor the new environment.
- A phased approach is recommended as it is less risky and less disruptive to the current infrastructure of the production environment.

In conclusion, there is no immediate threat of IPv4 address space being exhausted in the near future. The Internet will not suddenly “cease to exist” when you wake up one day. However, the day will come when every enterprise would need to be IPv6 capable, by either migrating to IPv6 or building a capability to communicate externally with IPv6 endpoints.

The enterprise is advised to start preparing for this capability now.

“The enterprise **needs to prepare itself** for the day when it would need to take action towards having IPv6 capability.”

Additional details

IPv4 address allocation

On the Internet, the allocation of Internet Protocol (IP) addresses is hierarchical; i.e. all Internet addresses are held by a world-wide authority, the IANA, who will allocate large blocks of free IPv4 addresses to regional groups of authorities, the RIRs who, in turn, will allocate smaller blocks of IPv4 addresses to local level authorities (national registrars) and finally to ISPs to allocate individual blocks of IP addresses to consumers and enterprises (see Figure 1).

Traditionally, IPv4 addresses were also handed out hierarchically in class A, B or C system. Each class was allocated a standard number of IP addresses, with Class A having the largest share at 16 million contiguous IP addresses. A Class B allocation has 64,000 contiguous IP addresses and a Class C allocation has 254 contiguous IP addresses.

IANA would only allocate Class A space to RIRs.

However, if further down the hierarchy, a large enterprise could demonstrate that it needed more addresses than a typical Class B allocation, it may be granted a Class A allocation that it may not have fully utilised. This original method of allocation of IPv4 addresses was inefficient and, as a consequence, there may potentially be quite a few unused IPv4 addresses within enterprises. Small enterprises were generally allocated Class C networks.

This “wasteful” method of IP address allocation was replaced by the CIDR system as a short-term solution when the Internet community faced imminent address exhaustion. CIDR allowed both address allocation and routing to have a floating boundary between the network and host portion of IPv4 address. Together with the NAT solution, CIDR extended the protocol lifespan by another ten-plus years.

Last of IPv4 address allocation

In February 2011, the IANA had exhausted its public IPv4 address pool. However, this has no immediate impact on the RIRs or on parties further down the hierarchy (i.e. most service providers and enterprises):

- It is understood that there are sufficient IPv4 addresses to allocate to service providers and enterprises until about 2015 – the RIRs and national registrars still have their own pools of unallocated IPv4 addresses.
- Enterprises have more than enough public IPv4 addresses for their needs due to the original method of IPv4 address allocation, as they used relatively few public IP addresses. In addition, enterprises can also use private IPv4 to address internal needs, leaving their public IPv4 addresses unused.

Gartner predicts² that by 2013, unallocated IPv4 addresses will cease to be obtainable from 90 percent of national registrars. By 2015, 17 percent of global Internet users will use IPv6, with 28 percent of new Internet connections running on the protocol. This means that over 80 percent of users will still be using only IPv4 in 2015, with an estimated 50 percent still using only IPv4 in 2020. Most IPv6 adoption will be from emerging markets (cloud computing, the next YouTube or the next Google), Asia and developing countries, and mobile users.

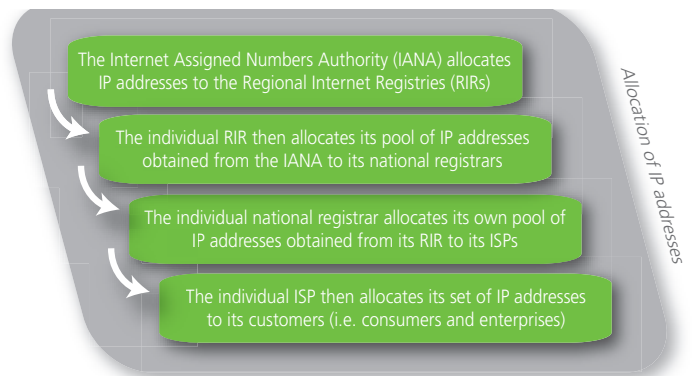


Figure 1: The process of disseminating IP addresses

To buy time, there are ways to postpone the depletion of IPv4 or the move to IPv6:

- Reclaim unused address space. These address spaces have been allocated but are unused. They can be traded commercially between enterprises, subject to RIR approval. A major problem with reclaiming network space is that the parties from whom the addresses would be reclaimed would be forced to renumber networks in different space.
- Releasing reserved address ranges. A significant fraction of IPv4 address space is reserved for purposes that may no longer be a priority such as X.25 integration and can be released for use.
- Increase use of NAT. The NAT can continue to be used to translate from internal IPv4 to external and public IPv6. NAT is the practice of multiplexing addresses and is most commonly used to share one or more globally-routed IP addresses among a much larger number of computers using private or unrouted IP address space. It has been very successful as a method of reducing IPv4 address consumption.

Who is building IPv6 capability?

Currently, the US Government (Department of Defence, Office of Management and Budget), Asia (Japan, China, Korea) and Europe are making the move to IPv6.

From Asia's perspective, it is imperative that they have access to more address space due to the growth in their Internet usage. They are unable to obtain more IPv4 addresses as blocks of IPv4 addresses have been previously allocated to US companies, educational institutions and government agencies – the US was amongst the first countries to request IP addresses due to its leadership role in development in the IP network space. The Chinese, Korean and Japanese governments have mandated that ISPs also support IPv6 in their countries.

In the military environment, the combination of expanded addressing with mobility will lend itself to transform access to information on the battlefield from tanks to soldiers, down to any number of smaller equipment. The US Office of Management and Budget has also mandated that all government IP networks be “capable” of supporting, although not necessarily use, IPv6. IPv6 support may also be required to win government contracts.

Réseaux IP Européens (RIPE), the agency that oversees IP addressing in Europe has announced that it will no longer be able to distribute IPv4 address space to new Internet networks.

“Currently, the **US Government** (Department of Defence, Office of Management and Budget), **Asia** (Japan, China, Korea) and **Europe** are making the move to IPv6.”

Appendix A: Sample list of automated inventory software vendors

The following table provides a desktop market scan summary of a sample list of automated inventory software tools – IP address tracker and network device tools:

Organisation	Tool name	Description	Features and functions
Alcatel-Lucent	VitalQIP	<p>Alcatel-Lucent VitalQIP™ DNS/DHCP IP Address Management Software is a solution for automating IP address management services across networks. It streamlines management and cuts administrative costs. Based on a recent IDC study, VitalQIP customers on average see an ROI of over 900 percent and a payback period of 106 days.</p> <p>The VitalQIP Appliance addresses the shift in the IP Address Management (IPAM) market towards appliances for increased reliability, manageability, scalability and security, and seamlessly integrates with VitalQIP DNS/DHCP and IP Address Management Software.</p> <p>Though organisations of any size can benefit from automating and centralising IP address management, it is more suitable for organisations with 1000 or more IP addresses.</p>	<p>Innovative Profiling Capabilities</p> <ul style="list-style-type: none"> Enterprise can create a base of network and customer information that allows it to define and manage subnets and network services. <p>Flexible Subnet Management</p> <ul style="list-style-type: none"> Today's networks must be updated constantly to keep up with frequent moves, mergers, and reorganisations that cause address space to become fragmented. <p>Customisable User Interface</p> <ul style="list-style-type: none"> Delivers a user interface that streamlines operations and allows the enterprise to plan, model, and build an IP network that reflects the enterprise's structure and goals. <p>Ability to Change DNS Options on Multiple Domains Simultaneously</p> <ul style="list-style-type: none"> The ability to modify multiple domains simultaneously can reduce operational expenses of configuring the network. <p>Windows Support</p> <ul style="list-style-type: none"> Supports Microsoft Windows DNS/DHCP servers with support of sites, subnets, and secure zones in Active Directory. <p>DNS & DHCP Server Compatibility</p> <ul style="list-style-type: none"> Supports BIND-compliant DNS servers. The Alcatel-Lucent DHCP Server can update both primary and secondary DNS servers with resource record information as DHCP leases are granted and deleted. <p>End-to-end Feature Appliance Solution</p> <ul style="list-style-type: none"> Centralised appliance management data store to keep track of services and status of remote appliances. Automated software upgrade capability with rollback options. Secure communication between AMS and appliances with unique appliance key generation. Logical grouping of appliances for ease of upgrades. Remote start/stop/initialise of services. High availability using heartbeat and virtual address mechanism.
BMC Software	IT Asset Management	<p>Part of the BMC Remedy IT Service Management Suite, the product:</p> <ul style="list-style-type: none"> Automates IT asset configuration Manages the entire lifecycle of IT assets — from procurement through retirement. 	<ul style="list-style-type: none"> Discovers all IT assets — mainframe, distributed and virtual. Provides data reconciliation, software title normalisation, and a rules-based software licence compliance engine. Enables licence harvesting. Includes BMC Atrium CMDB. Integrates IT asset and service support repositories. Architecture extends and adapts out-of-the-box workflows and data model without programming.

Organisation	Tool name	Description	Features and functions
BT Diamond IP	IPControl	IPControl is a comprehensive IP address management (IPAM) solution. It is available as a software application or pre-installed on Sapphire™ appliances. Newly integrated with NetControl, the block management solution, IPControl provides centralised, full lifecycle of IPAM functions, including IPv4 and IPv6 address space assignment, allocation/re-allocation, pool monitoring, and utilisation tracking, creation and deployment of multi-vendor DNS and DHCP configurations. It also has flexible deployment options for integration with multi-vendor DNS/DHCP infrastructure, intuitive graphical user interface and customisability via ExtenSimple™ architecture.	<p>Address Planning</p> <ul style="list-style-type: none"> • IPv4 and IPv6 networks can be allocated to any CIDR size or prefix length with the ability to configure individual IP addresses, ranges or address pools within networks.. • Ability to choose automated address allocation to maximise utilisation efficiency or use the manual override option for more control over address allocation • User-defined policies determine which block and device types are permitted within the hierarchy and who can administer them. • Address utilisation trending and forecasting enables proactive address capacity management. • Provides “planned vs. actual” views of IP address space. <p>DNS/DHCP Server Configuration</p> <ul style="list-style-type: none"> • Server templates streamline the server configuration process. • Supports DHCP failover, multi-tiered addressing, multi-homed hosts, processing, client IP and dynamic DNS. • DNS configuration verification tool is included in the software. <p>Address Management</p> <ul style="list-style-type: none"> • IPControl's container structure enables address management according to enterprise topology, geography or other user-defined hierarchy. • Layer 2 switch, Layer 3 router and IP discovery features enable IP inventory assurance and identify potential access control violations. • Advanced IPv6 address management enables automated block allocation, ip6.arpa domain creation, AAAA/PTR resource record automation and tracks both IPv4 and IPv6 address space in a single database repository. • Automates reporting to RIRs. • User-defined thresholds and alerts provide notification of impending address depletion. • Multiple graphical reports are available for any level in the container or address block hierarchy. • Audit Reporting can be used to track administrators, subnets, devices, IP addresses, DNS resource records and containers. • Granular administrator policies control access by function, geography, domains, subnets and blocks.

Organisation	Tool name	Description	Features and functions
Computer Associates	NIMsoft monitoring solution	<p>Automatic Discovery and Deployment Finds, identifies and displays network elements. Data is immediately available as part of the CMDB to provide visibility of an organisation's infrastructure. The CMDB Visualizer shows the relationships between various configuration items that make up IT business services.</p> <p>RCA and Topology Manager Shows a complete network topology. Automatically discovers IP device, and maps out the relationships and dependencies in the network environment. Provides a user interface for viewing the hierarchical and dependent structure of large, complex networks. Administrators can filter their view by network component, and generate network topology maps.</p>	<p>Discovery Features</p> <ul style="list-style-type: none"> • Delivers scalability, featuring multiple discovery agents that can work in parallel to scan different network areas. • Allows duplicate addresses in different network areas e.g., in NAT environments. • Discovers both router and switch-based connections across LAN, WAN, and meshed architectures. • Features cluster awareness – correctly mapping clustered systems using a common MAC address. • Offers VM awareness, distinguishing between physical and virtual machines to present an accurate topology. <p>Intuitive and Flexible Topology Views</p> <ul style="list-style-type: none"> • Offers a visual topology and relationship viewer that enables user to select from different layout formats, including orthogonal, hierarchal, circuit, circular, and natural or organic. • To support large scale networks, an automatic micromap is provided to view the entire layout. Ability to traverse the micromap and zoom in on different network segments as required. Plus, ability to mouse over individual IP devices and see specific details of that device. • View is automatically overlaid with availability status data of all monitored IP devices. Connection properties are displayed when user clicks on a line or connection between two devices. The connection properties show the connection status (SNMP operational and administrative status), connection speed, each device, and each interface on either end of the connection. <p>Intelligent Root Cause Analysis</p> <ul style="list-style-type: none"> • Features an engine that analyses alarms for likely root causes, based on the layer 2 relationships identified. • Automatic discovery is used to gather layer 2 relationships automatically and is a requirement for layer 2 root cause analysis. The relationship service will support multiple relationship types. These may include some custom relationships like customer, location and service. <p>Multi-tenant Support</p> <ul style="list-style-type: none"> • For service providers with many clients, the multi-tenant capabilities allow segregate and view subsets of large, distributed networks and service provider infrastructures.

Organisation	Tool name	Description	Features and functions
Crypton Computers	Easy-IP	<p>Easy-IP monitors network changes by using an auto-discovery tool with SNMP to maintain an accurate, up-to-date inventory for all the subnets, IP addresses and network devices.</p> <p>It has an intuitive web-based GUI and can be accessed by multiple administrators in diverse geographical locations – from any web browser.</p> <p>Easy-IP enables the enterprise to plan the IP addressing scheme, discover the network devices, keep track of all changes, and provide detailed custom management reports.</p> <p>By automating complex IP addressing tasks like VLSM and subnet partitioning, Easy-IP reduces the administrative overhead associated with IP address management.</p>	<ul style="list-style-type: none"> • Easy-to-use interface, including visual drag and drop feature. • Automated subnet allocation. • Network auto-discovery. • Advanced grouping and filtering, including sorting. • Builds up-to-date inventory of all network equipment, servers and printers using SNMP. • Built-in MIB browser enables customised reports and provides ability to create comprehensive inventory of the network. • Provides import facility to incorporate existing IP information from spreadsheets, or text files. • Provides exports to industry-standard file formats. • Provides multi-user access control. • Provides granular access rights; user access can be granted based on countries, regions, departments, or specific subnets or IP address ranges. • Enables Service Providers to manage multiple overlapping IP address space for their customers. • Provides user-defined custom fields. • Built-in report templates, and all reports can be exported to HTML, CSV or text format and can be modified, viewed, or printed. • Ability to generate reports based on user-defined custom fields. • Includes Template Wizard for Service Providers to submit reports to RIRs in the required format, including IPv4 address space utilisation reports. • Built-in Task Scheduler to automate tasks such as Database Backup, Network Discovery or Reporting to run daily, weekly or monthly, at a suitable time.
FrontRange Solutions	FrontRange Discovery	<p>FrontRange Discovery employs a hybrid audit technology to provide visibility of all IT assets on the corporate network, including hardware and software that is physical or virtual, and any platforms they are running on.</p> <p>FrontRange Discovery gives IT and business managers immediate access to a full network inventory for the entire organisation.</p> <p>FrontRange Discovery keeps an eye on the network assets by automatically identifying new hardware and software and adding them to the comprehensive IT asset repository – with no manual intervention.</p> <p>Whether the aim is to take control of software licensing, drive down IT costs or ensure that projects are brought in on time and under budget, FrontRange Discovery provides a dynamically-updated baseline of IT asset information across the entire network.</p>	<ul style="list-style-type: none"> • 100 percent asset visibility – discovers all IP-addressable hardware on the network, including PCs, servers, switches, network printers and other devices. • Virtual Audit – discovers and tracks virtual hardware and software, supporting VMware and Microsoft virtualisation technologies. • Thin Client Audit – identifies software published on XenApp 4.5 and 5.0 servers. • Multi-platform – tracks hardware and software across all major enterprise platforms, including Windows (now with Windows 7 and 2008), Linux, Unix, Mac OS X (including 10.5 and 10.6) and AIX. • Remote auditing – keeps tabs on all IT assets anywhere in the organisation, whether in the head office, branch location or remotely-connected to the network. • Multi-user web reports – shares audit information with multiple colleagues and creates personalised web-based views of key reports.

Organisation	Tool name	Description	Features and functions
GestióIP	GestióIP	GestióIP is automated, Web based IPAM software. It features network discovery functions and offers search and filter functions for both networks and host, permitting Internet Search Engine equivalent expressions. This lets the enterprise find the information that administrators frequently need easily and quickly. GestióIP also incorporates an automated VLAN management system.	<ul style="list-style-type: none"> • Easy usage and clear presentation of data. • Powerful quick-search for both network and host directly accessible from every page, permitting Internet Search Engine equivalent expressions like "exact match" or "-string_to_ignore". • Possibility to independently manage the address ranges for different clients. • Incorporated VLAN management system. • Network and VLAN discovery via SNMP. • Host discovery via SNMP and DNS. • Shows host status. • Split/join/scaling up/scaling down networks (host entries can be maintained). • Shows free network ranges. • Integrated subnet calculator. • Customisable columns for networks and hosts. • Reservation of IP ranges for special usage (e.g. DHCP). • Web form to migrate easily from spreadsheet-based (.xls - MS Excel) IP address management to GestióIP IPAM. • Web form to import networks from SNMP-enabled devices. • Web form to export networks or host to CSV files. • Automatic update of the networks via SNMP. • Automatic update of the networks against DNS. • Automatic update of the networks against OCS Inventory NG. • Statistics. • Fully auditable. • Easy, script-based installation. • Well-documented. • Multilingual (Brazilian-Portuguese, English, Spanish, Italian, Catalan, German). • Full IPv4 support (IPv6 will come with GestióIP v3.0).
Hewlett Packard (multiple products)	HP Networking Intelligent Management Center	HP Intelligent Management Center (IMC) is a single-point network management solution that provides visibility across networks, enabling the management of resources, services and users.	<p>Manageability</p> <ul style="list-style-type: none"> • End-point awareness and VoIP device tracking – a device map view that displays which endpoints are directly connected to the device, including phones, cameras, PCs, and authenticated users; provides real-time location and inventory reporting for VoIP phones, including network details such as VLAN assignment, QoS setting, and PoE status. <p>Integration</p> <ul style="list-style-type: none"> • HP NNMi integration – <ul style="list-style-type: none"> o HP networking device management – can be integrated with HP NNMi to provide advanced HP networking device support. • HP Network Node Manager integration – optional integration with HP Network Node Manager (NNM) v7.5; when integrated with NNM, HP PCM Plus shares NNM's discovery data and provides additional functionality for HP networking devices.

Organisation	Tool name	Description	Features and functions
Hewlett Packard (multiple products) (cont.)	Discovery and Dependency Mapping Advanced Edition (DDMA)	HP Intelligent Management Center (IMC) is a single-point network management solution that provides visibility across networks, enabling the management of resources, services and users.	<ul style="list-style-type: none"> Automates the discovery of infrastructure and software. Enables understanding of service decomposition. Enables visibility into existing legacy IT infrastructure.
	Network Node Manager	<p>Automates the process of developing and continually updating topology of the physical and virtual network services, and the complex relationships between them.</p> <p>Products include:</p> <ul style="list-style-type: none"> HP NNMi HP NNMi Advanced NNMi Smart Plug-ins 	<ul style="list-style-type: none"> Geo-diverse architecture (Global Network Management) that supports multi-tenancy. Discovery and monitoring of VMware ESX virtual machines and the physical network connections that support them. IPv6 discovery and monitoring in the context of the greater IPv4 environment. Reduces the cost of delivering improved network availability. Consolidates network management infrastructure. Wizards and spiral discovery process. Intelligent automation.
IBM	Tivoli Provisioning Manager Inventory	<p>Tivoli® Provisioning Manager Inventory discovery enables the discovery of hardware and software resources installed.</p> <p>The Tivoli Provisioning Manager network discovery allows discovery of IT infrastructure over SSH, SMB, and SNMP to find network devices. Organisations can create a discovery configuration specifying what they want to discover and specify the scope. This is identified using IP addresses, IP address ranges, and subnets.</p> <p>Remote Execution and Access (RXA) discovery</p> <ul style="list-style-type: none"> Discovers Windows®, Linux®, AIX, Solaris and HP-UX resources using RXA that identifies if your resources are working over SMB or SSH protocols. <p>SNMP discovery</p> <ul style="list-style-type: none"> Discovers resources, switches, and routers. 	<p>Discovery and inventory management</p> <ul style="list-style-type: none"> Discovers IT resources and their relationships. Helps with the manual maintenance of assets. Enables tracking of IT assets through an automated hardware and software inventory of computer devices. Discovers computers, network devices like routers, firewalls, middleware software, and business applications. Helps to accurately answer the following questions: <ul style="list-style-type: none"> What hardware? What software? What are the relationships and dependencies? <p>Microsoft® Active Directory discovery</p> <ul style="list-style-type: none"> For discovering resources by organisational unit. For discovering Microsoft Active Directory groups. For discovering resource attributes defined in Microsoft Active Directory. <p>Tivoli Provisioning Manager network discovery</p> <ul style="list-style-type: none"> For detecting network devices (such as computers and switches) and a minimal set of configuration information needed to manage these devices (such as hostname, IP address, operating system). Tivoli Provisioning Manager Inventory discovery. For discovering and keeping up-to-date the hardware and software configuration of the computers in your environment.

Organisation	Tool name	Description	Features and functions
Infoblox, Inc.	NetMRI Discovery Module	<p>The NetMRI Discovery Module automates normal manual tasks. Instead of guessing what is on the network, the NetMRI Discovery Module auto-discovers multi-vendor routers, switches and other layer 2 and 3 network devices. In addition, the discovery includes end-points so the enterprise has a complete view of the network components. This information can also be integrated with the Infoblox IPAM solution for more comprehensive views. The NetMRI Discovery Module eliminates the risk of out-of-date or incorrect information so IT teams have an accurate inventory, visualisation of topology and complete understanding of the network and its components.</p>	<ul style="list-style-type: none"> • Auto-discovery of multiple vendors for routers, switches and other layer 2 and 3 network devices. • Detailed inventory including device and chassis components, interfaces, operating system and model types. • Layer 2 and 3 network summaries including routes, subnets, VLANs, HSPR/VRP groups, and ports. • Topology views highlight complex components with easy-to-understand visualisation. • Standard and custom report options for asset inventory and management. • Easy sync with Infoblox IPAM solution. • Automatic update of IPAM fields with detailed layer 2 and 3 network components. • Deployed as an appliance for easy installation and set-up. • Easily add custom device support.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • GHANA • KENYA
MOROCCO • NAMIBIA • NIGERIA
SAUDI ARABIA • SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY • HUNGARY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES