

# THE BENEFITS OF COMPREHENSIVE IP MANAGEMENT (IPV6, IPV4, DHCP AND DNS)



# THE BENEFITS OF COMPREHENSIVE IP MANAGEMENT (IPV6, IPV4, DHCP AND DNS)

## INTRODUCTION

For the past several years we've been hearing stories about the shortcomings associated with IPv4 including how the Internet is running out of addresses, how IPv4 is not "future-proof", and how the new IPv6 is going to make managing networking services a lot easier. For the most part the stories are true. So why has there been such tepid adoption of IPv6? Since the launch of IPv6 in 2012, less than 4% of today's Internet traffic is IPv6. The reason is there are a lot of switching costs associated with adopting IPv6. Make no mistake, IPv6 is here to stay. And even though the transition to IPv6 will likely occur slowly, you should be actively managing IPv6 now! In fact, it's likely that IPv6 is already enabled and operational on your network right now. So the question is not when should you begin managing IPv6, but rather what are you doing today to manage IPv6? This paper will examine the risks of an IPv6 "shadow network" and provide recommendations on how to proactively detect and manage IPv6 devices and services.

## THE PROBLEM

You may be unknowingly operating a shadow IPv6 network right now. Many of the new hosts you've added to your network, due to expansion or system lifecycle replacement, are IPv6 capable and IPv6 enabled by default. While IPv6 certainly does not make your network inherently less secure, neglecting to actively manage IPv6 can introduce security risks. Having operational IPv6 hosts on your network may represent a security risk if your processes and controls are unaware of IPv6-enabled hosts and traffic. In addition, the existence of IPv6 in the network introduces the need for new processes and controls for comprehensive IP address management that have likely not been implemented. Without these processes and controls, there could be a covert route operating in and out of the network. What follows is just a sampling of potential security risks inherent to unmanaged IPv6 usage.

### Multicast

IPv6 does not support IPv4 "broadcast" addresses. Rather, it expands the use of multicast addresses and can be used to deliver additional capabilities like service solicitation and address resolution. As a result, well-known multicast addresses may be exploited to reveal unpublished resources like critical core devices or application servers. Once identified, these resources then become the target of more malicious actions. Multicast configurations and associated protocols and services need to be carefully managed and explicitly enabled as needed.

### Stateless Address Autoconfiguration (SLAAC)

IPv6 provides by default an automated method for an IPv6 host to obtain an IP address without any manual configuration or interaction with a DHCP server. This means it's possible for a device to operate stealthily on a network. One possible way to manage this risk is to disable SLAAC and use DHCPv6. This will allow you one way to maintain visibility and control access to your network.

### Security Controls

It's entirely possible that some of your security controls (e.g., firewalls, filters, NIDS, etc.) either don't work with IPv6 or have not been configured to work with IPv6. This has the effect of letting IPv6 hosts onto your network undetected and letting IPv6 traffic go unmonitored. There have been



many reports and studies that document how malicious tools can be used to detect IPv6-capable hosts, take control of IPv6 autoconfiguration, and begin tunneling IPv6 traffic in and out of IPv4 networks undetected. One way to address this risk is to either verify appropriate IPv6 security controls are in place or to aggressively filter or block IPv6 traffic as needed.

## Vulnerabilities

Many vendors have supported IPv6 for a number of years. However, the process of hardening these implementations is ongoing. New vulnerabilities will inevitably be discovered and exploited, which can lead to a loss of system confidentiality, integrity, and availability. To address this risk, it's important to identify at-risk hosts and actively manage security updates.

## THE SOLUTION

To actively manage these risks, and many more not covered in this paper, organizations are encouraged to adopt a comprehensive IP management strategy. The National Institute of Standards and Technology has provided a number of specific recommendations for addressing interim IPv6 security and the transition from IPv4 to IPv6. Here are some of their recommendations.

### Subnet Management

The design considerations for an IPv6 subnet are different from those of an IPv4 subnet. With IPv4 the focus was on accommodating future growth; an IPv6 subnet should address operational and security requirements. Accordingly the master subnet allocation plan should be highly hierarchical and designed to support meaningful network segmentation. This will make it easier to design, implement, and efficiently manage effective access controls on firewalls, routers, and VLANs.

### Address Management

IPv6 offers multiple methods for assigning addresses to a host. These include autoconfiguration, DHCP, and manual. Unfortunately, one size does not fit all and no single method is likely to be used exclusively. As a result, each approach must be carefully evaluated and used according to operational need. Regardless of how addresses are assigned to an IPv6 host, there will be a continuing need to formally manage address blocks and to use automation tools to manage address inventories and DHCP configurations.

### Transition Tactics

IPv6 and IPv4 will almost certainly coexist on networks for some time to come. Therefore, organizations must adopt a strategy right now to best facilitate this coexistence. Possible approaches include running dual protocol stacks, protocol tunneling, and address translation. Each has advantages and each carries unique management responsibilities and administrative burdens. Furthermore, it should also be noted that each approach need not be used exclusively. For example one approach may be used for a period of time and then deprecated in favor of another approach.

## RECOMMENDATIONS

Because IPv4 and IPv6 will coexist for some time, the need for holistic DDI management will be even greater. Comprehensive Management of IPv6, IPv4, DHCP, and DNS is almost a necessity because of:

- The particular need to identify and track IPv6 devices
- The need to concurrently manage IPv4 and IPv6 address blocks, DHCP, and DNS services
- The need to monitor IPv4 and IPv6 resources and tasks
- The need to reduce administrative burdens as IP-connected devices continue to proliferate

## HOW A DDI SOLUTION CAN HELP

We've seen that IPv6 addresses are more complex, longer, and harder to remember. The address boundaries and dynamic assignment of addresses are much more difficult compared to IPv4. Therefore, spreadsheets visibly fall short of providing the necessary approach for efficient management. An integrated DHCP, DNS, and IPAM (DDI) tool simplifies the whole process of IP address management for both IPv4 and IPv6 by helping network administrators eliminate network conflicts and outages, track critical assets, and ensure network security. An integrated tool also provides reports based on a wide range of parameters, including IP address status (dynamic, static, available, reserved, etc.), hostnames, MAC address, and more.

### Subnet Creation, Mapping and Management

Planning, designing, and maintaining an operationally efficient and secure IPv6 network needs clear understanding of business requirements both current and future, existing devices that are already on IPv6, and devices that need updating. A few important tasks include:

- Identifying and documenting devices that currently support IPv6
- Mapping existing IPv4 space to proposed IPv6 space
- Documenting devices that need to be added/replaced for IPv6 support

Creating subnets and grouping them into segments according to location, department, function, etc., facilitates better management and control of your organization's IP space. The spreadsheet import functionality in some management systems can be problematic as administrators have to first ensure that the spreadsheet data is accurate and up-to date. Instead of this manual effort, automated discovery of IPv4 subnets and of IPv6 devices directly from your routers is both fast and accurate. This type of automated discovery saves time, reduces errors, and provides a more accurate IP Address Management solution.

### Management of IP Address Blocks

Essentially every networked application and device depends on IP addressing and requires accurate address assignment. Managing these IP addresses is becoming increasingly difficult as new services such as VoIP, BYOD, Virtualization, and IoT increase IP address assignment needs. This rapid increase in the number of IP addresses is in addition to the ongoing transition to IPv6. All this means that having a robust IP address management solution that allocates, classifies, and tracks your ever-changing IP addresses is essential to managing a mission critical network.

Efficient management of IP addresses provides visibility to the real-time status of your IP addresses and increases the speed with which you can troubleshoot issues and meet IP requirements. Having up-to-date and accurate information supports administrators in making optimum use of their IP address space. Networks that have both IPv4 and IPv6 must have a system that helps manage both address blocks together. In short, even a basic IPAM solution should allow for all stages of IP management—address planning, automated discovery, configuration and management of the address space, accurate reporting of IP address usage along with work flow and role-based delegation of management tasks—for both IPv4 and IPv6 addresses.

### Management of DHCP and DNS

DHCP allows network administrators to centrally manage and automate the assignment of IP addresses while DNS does the necessary translation between machine names and IP addresses. Managing both DHCP and DNS are integral to managing IP addresses. Having an integrated tool that automates DHCP, DNS, and IPAM (DDI) is crucial in helping network administrators more easily manage the ever growing number of IPv4 and IPv6 addresses in use on your network.

DHCP automatically assigns and leases out IP addresses for a fixed time frame enabling unused addresses to be reclaimed and used again. A complete IP address management solution should



be able not only to read the current status of DHCP scopes from your current multi-vendor DHCP servers, but also able to push out changes to your multi-vendor DHCP servers, including changes to DHCP scopes and split scopes. Manual changing of DHCP settings on each DHCP server can be time consuming and error-prone. Administrators need to be able to keep close track of all subnets and scopes approaching capacity and provision accordingly.

Similarly, manual update of DNS records can lead to records becoming corrupt, contain incorrect information or sometimes even disappear. These types of errors increase security and compliance risks as well as outages of IT services. Being able to read data from multi-vendor DNS servers and to push out changes to your multi-vendor DNS servers is a critical component of a comprehensive DDI solution.

A major challenge associated with IPv6 is that a device connected via IPv4 cannot communicate directly with a device connected via IPv6. This poses a compatibility challenge and until all networks and devices are IPv6 capable, we need to run both protocols simultaneously. So network administrators need DHCP and DNS that support both address spaces along with a comprehensive IPAM strategy that allows full view and management of your IP addresses.

### Monitoring IP Resources

Network Administrators are constantly under pressure to provide uninterrupted IT operations. Gaining visibility into the allocation of IP resources and reducing potential management blind spots presented by IPv6 devices in the network requires an integrated DDI tool. And, with IPv6 being already available on most devices nowadays, your DDI tools need to be clearly aware of your network's IPv6 configuration as well.

To avoid network issues like DHCP servers running out of IP addresses, IP address conflicts leading to connectivity problems, issues due to DNS and DHCP misconfigurations, and so on, continued monitoring and management of IP resources is imperative. Proactive monitoring and alerting helps eliminate network downtime due to IP-related issues. Monitoring also helps in accurate planning for IP resources and informed decision making.

### CONCLUSION

To sustain future growth without relying exclusively on IPv4, the most effective way to manage the shortage of IPv4 addresses is to allow networks to support both IPv4 and IPv6 simultaneously. SolarWinds IP Address Manager (IPAM) is a DDI solution that supports both IPv4 and IPv6 addresses. It also offers functionalities like:

- Centralized management of IP addresses with multi-vendor DHCP and DNS server support
- Automated discovery and scanning for IPv6 devices
- Monitoring and alerting of IP resources and other IP-related information like IP conflicts, DNS record mismatches, DHCP scope utilization, and more
- IP address usage history tracking and event logs for troubleshooting
- Integration with SolarWinds User Device Tracker (UDT), which provides device and switch port details with remote port shutdown capability

As we move further away from IPv4 and into IPv6, organizations large and small need to consider IPAM as a requirement for a modern network, especially with the increasing demand of IP addresses. A robust IPAM solution with integrated DNS, DHCP, and IPAM allows real-time and efficient management of your IP address space. It takes a huge load off the network administrator by providing centralized visibility and management, while having a positive effect on network uptime and security.



## REFERENCES

- <http://en.wikipedia.org/wiki/IPv6>
- <http://www.worldipv6launch.org/infographic/>

## ADDITIONAL RESOURCES

**Recorded Webinar:** The Benefits of Comprehensive IP Management (IPv6, IPv4, DHCP, and DNS), presented by Digital Government Institute

**Free Trial:** SolarWinds IP Address Manager – [Download Now](#)

## ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide, from Fortune 500 enterprises to nearly every civilian agency, DoD branch, and intelligence agency. In all market areas, the SolarWinds approach is consistent—focusing exclusively on IT pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors.

SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Each solution is rooted in the company's deep connection to its user base, which interacts in an online community, thwack®, to solve problems, share technology and best practices, and directly participate in the product development process. SolarWinds provides IT management and monitoring solutions to numerous common public-sector IT challenges, including continuous monitoring, cybersecurity, network operations, compliance, data center consolidation, cloud computing, mobile workforce and devices, and scaling to the enterprise. SolarWinds software is available on the U.S. General Services Administration (GSA) Schedule, Department of Defense ESI, and numerous other contract vehicles. For more information and fully-functional free trials, visit <http://www.solarwinds.com/federal>.

