whitepaper

Best Practices for Managing IP Resources

By: Brien M. Posey

solarwinds

whitepaper

A number of recent trends within the IT industry are causing automated IP address management to become an essential part of the management layer for networks of nearly every size. Although most prudent network administrators probably recognize the need for automated IP address management, figuring out how to best manage IP addresses can be challenging. This whitepaper provides a number of best practices for ongoing IP address management.

Considerations for Best Practices

Although there are a number of different software solutions available for automated IP address management, the features and capabilities differ widely from one product to the next. The best practices discussed in this whitepaper are based on ideal circumstances. Not every IP address management product includes all the functionality around which the various best practices are based.

Determine the Most Effective Method of Transitioning to an Automated IP Address Management System

Automated IP address management software has existed for quite some time, it's only now starting to become popular. Even today, most organizations still manage IP addresses by using spreadsheets. It's the inefficiency and potential for human error involved in using spreadsheets that's starting to drive IT administrators to adopt automated solutions.

Even though automated IP address management software helps to greatly reduce the chances of IP address related problems. You still have to account for the possibility of human error, the software is only as good as its configuration.

When an organization decides to adopt IP address management software, it's important to acquire software that offers the option to import IP address data from spreadsheets. The alternative is to manually enter the data. This process can be time consuming & error-prone, resulting in configuration errors, and lead to a variety of network problems.

One reason why importing spreadsheet data isn't more widely supported is because there's no such thing as a standard spreadsheet for IP address management. The only way to reliably import spreadsheet data directly into an IP address management system is if the software allows the administrator to custom map spreadsheet columns to data fields within the application.

Unfortunately, even the best spreadsheet importing mechanism can't eliminate problems related to inaccuracies within a spreadsheet. If a spreadsheet contains inaccurate data then an IPAM system that uses this data will also be inaccurate. The only way to guarantee the accuracy of data within the IPAM system is to perform live network scans, rather than merely importing legacy data.

whitepaper

Use Spreadsheets for Planning Purposes Only

It's worth noting that having the ability to import spreadsheet data is useful for more than just the initial transition to automated IP address management. Imagine a situation in which an organization needs to create a new subnet. An administrator could potentially create the subnet directly through the IP address management system, and then add the necessary IP addresses. However, this might not always be the best approach. After all, unchecked administrative actions carry the potential for human error.

As a general best practice, an administrator might consider defining the new subnet and the corresponding IP address blocks through a spreadsheet. The advantage to doing this is that spreadsheets can easily be shared with others. The proposed subnet configuration spreadsheet could be shared with other administrators throughout the organization, so that each has the opportunity to review the proposed configuration and check for anything that might be problematic. Once the spreadsheet data has been thoroughly reviewed, it can then safely be imported into the IP address management system.

The same process is also useful for organizations that are beginning to make the transition to IPv6. An administrator can use a spreadsheet to define IPv6 address ranges, and then import the spreadsheet once they're confident the data is correct.

Keep in mind however, that while spreadsheets are useful for planning new address scopes, spreadsheets shouldn't be used for ongoing management of those scopes. The use of spreadsheets for IP address management negates the benefits derived from the use of an automated IP address management system.

Configuring IP Address Lease Durations based on How the Scope Will Be Used and on the Number of Available Addresses

The transition that occurs as you implement a new automated IP address management system is also a great time to reevaluate your DHCP server lease configuration. When a DHCP server grants an IP address to a client, the client doesn't have permanent possession of the IP address. Instead, the DHCP server leases the IP address to the client for a predetermined length of time (although the client can automatically renew the lease).

Although there's usually a lot of planning that goes into DHCP scope configuration, the lease duration is an often overlooked configuration parameter. However, it's important to carefully consider the terms of DHCP leases, because the lease duration can have a direct impact on IP address consumption on your network.

When a client leases an IP address, the client effectively retains ownership of the IP address for the duration of the lease. As such, a client that only needs an IP address for a few minutes could conceivably tie up an IP address for several days.

One of the things that you can do to ensure that IP addresses are used efficiently on your network is to set the DHCP server lease terms based on the type of clients that the DHCP server services. For example, if you have a DHCP server that assigns IP addresses to desktop PCs, then you can probably get away with using a long lease period. After all, desktop PCs are usually semi-permanent assets that are used consistently over an extended period of time.

On the other hand, if you have a DHCP server that services wireless BYOD clients, then it's a good idea to set the lease duration for that DHCP server to a relatively short period of time (such as a few hours). End-user's wireless devices tend to be used in a very inconsistent manner. For instance, some users may only occasionally bring a personal device into the office. Other users might only use a device until the next model comes out, while others may use multiple devices. These factors lend themselves to the excessive consumption of IP addresses. The only practical way to limit IP address consumption for these types of devices is to keep the DHCP lease duration short.

If a DHCP server is configured to provide short term IP address leases, then it's important for the DNS server to be able to keep pace with all other leases, lease renewals, and lease expirations. Otherwise, the DNS server could contain outdated host records that don't match the IP addresses that have actually been issued.

As a best practice, administrators should use an IP management system that tightly couples DNS and DHCP so that IP addresses and DNS records are updated simultaneously. Doing so not only avoids problems stemming from outdated host records, but it also helps to improve overall work efficiency for the administrative staff.

At first, the idea of achieving DNS/DHCP interoperability may seem impractical, especially when DHCP and DNS servers are from different vendors. However, software based solutions exist that can act as a management layer that provides reliable interoperability between heterogeneous DNS and DHCP solutions. This approach is usually preferable to purchasing an appliance based solution because it allows the organization to leverage their existing investment, rather than performing a "rip and replace" method. An overlay solution is also less likely to require a long and disruptive transition process than switching from existing DNS and DHCP servers to an appliance based solution.

Use Automated Scanning to Discover Subnets and Open IPs, and to Maintain an Accurate Inventory

Another best practice is to periodically compile an IP address inventory so you can see what resources are present on your network and how they're being used.

Although most of the IP address management products that are available today offer some sort of inventory reporting mechanism, these applications use a variety of techniques to compile the inventory data.

At first, the method from which an IP address management system acquires inventory data would seem to be irrelevant. However, the method which inventory data is acquired can have a direct correlation to the accuracy of the data.

Most, if not all IP address management systems use a database to maintain a record of the IP addresses that have been issued. Some IP address management systems build IP address inventory reports by performing database queries. The problem with this approach is that the database content may or may not accurately reflect the resources that are in use on the network. For instance, what happens when someone configures a machine to use a static IP address, but doesn't enter the address into the IP address management system?

The only way to protect against these types of inaccuracies is to periodically scan the network to make sure that IP address information logged in the database matches the IP addresses that are actually in use on the network. Active network scanning can help to detect inconsistencies related to manually configured devices and rogue DHCP servers (including wireless access points).

Because active scanning produces more reliable data than a simple database query, the next logical question to ask would be, how should the network be scanned? The best IP management systems use a variety of scanning techniques. For example, some use a combination of neighbor scans (which is based around ARP tables), ICMP scans, and SNMP scans.

The reason why the best products use multiple scanning techniques is because each scanning method has its strengths and weaknesses. For example, ICMP scans are sometimes referred to as ping sweeps. A ping sweep pings individual IP addresses in an effort to determine whether or not a particular IP address is being used.

This method generally works really well for providing a real-time picture of the IP addresses that are active on your network at a given moment. Of course this is assuming that device firewalls aren't configured to block ICMP traffic. It's also worth noting that ping sweeps can only report IP address usage information for devices that are powered on. Furthermore, a ping sweep will only confirm that an IP address is actively being used. It doesn't provide information about IP addresses that have been issued to a device that are currently powered off or disconnected, nor does it gather any diagnostic data from a device.

Keep in mind that there's nothing wrong with performing a ping sweep. Ping sweeps are an important part of scanning the network. It's just that a ping sweep shouldn't be the only method used for determining the network status.

Conversely, SNMP scans are useful for gathering data around the health of a managed device. Devices such as routers, switches, and servers typically support SNMP monitoring. This is useful in that it becomes possible to detect conditions that might require an administrator's attention. However, SNMP can't be used as the sole mechanism for IP address monitoring because it's unlikely that every device on the network will include the required SNMP agent.

This isn't to say that an IP address database is useless, only that the database shouldn't be used as an authoritative source for determining current IP address assignments. That process is best handled by active scans. The role of the database should ideally be to act as a historical log of IP address assignment data. This data can serve some useful purposes.

Historical IP address assignment data is useful for security purposes because it allows an administrator to determine who had an IP address at a specific point in time. Historical data is also very useful for tracking IP address consumption over time and performing long term capacity planning.

Use Monitoring to Proactively Identify IP Conflicts or Low Scope Address Pools

Active IP network scanning could be construed as IP address monitoring, however monitoring involves more than that. A network scan compiles an inventory of the IP addresses that are being actively used at that particular point in time. Monitoring on the other hand, involves actively making use of inventory data. The purpose of monitoring is to raise administrative awareness of situations that could potentially be problematic—either from a network configuration standpoint, or from a security standpoint.

It might seem strange to bring up security in a discussion of IP address management best practices, but it does have its place. Consider for example an IP subnet that's used solely for desktop PCs. Now imagine that the DHCP server on that subnet leases an IP address to a PC that has an unrecognized MAC address. As an administrator, that's probably the sort of thing that you would want to know about. Unless you have recently purchased a new PC or replaced a network adapter, the presence of an unrecognized MAC address could mean that someone has connected a rogue device to the subnet.

As previously mentioned, IP address usage logging is useful from a capacity planning standpoint. As an administrator, it's your job to make sure that users are able to connect to the network. In order to do so however, you must ensure that the available pool of IP addresses is never depleted. This is where historical logging comes into play. By examining your historical logs, it's possible to track IP address consumption over time, thereby allowing you to make projections regarding eventual IP address depletion.

Of course using past IP address usage statistics to make future projections would be a very tedious process if you had to work solely with raw data. Therefore, it's important to make sure that your IP address management software is capable of tracking and projecting IP address consumption so that you don't have to do it manually.

Any good IP address monitoring solution should also have an alerting mechanism. On a large network there can be thousands of IP addresses in use at any given time. It's unrealistic to expect an administrator to be able to spot a problem with a single address.

If the IP address management software detects a condition that warrants an administrator's attention, the software needs to be able to alert the administrator so he or she can take appropriate action. For example, if an IP address block started running low on addresses, the administrator would probably need to know that.

It would be naïve to assume that an administrator is constantly watching an IP address management console screen. As such, alerts need to be configurable in a way that allows the administrator to receive the alert in a way that is sure to be noticed. For example, an administrator might want to receive alerts through email or through a text message.

Although monitoring and alerting capabilities are important, it's equally important for an IP address management system to be able to facilitate the rapid detection, diagnosis, and remediation of problems. Suppose for instance that an IP address conflict existed on the network. A comprehensive IP address management solution shouldn't only detect the conflict, but should also be able to analyze where the improperly configured device is located by analyzing switch port data. Once the device has been located on the network, the software should be able to temporarily disable the switch port that's being used by the device in question, assign a new IP address to the device, and then update any related DNS entries.

Manage IP Addressing in a Way that Ensures Consistency and Operational Efficiency

There are several best practices around the actual management of your IP address space once an IP address management system is in place. The first best practice involves the way administrative tasks are performed. Normally, IP address related management tasks are performed on a per server basis. For example, if an administrator needed to create a DHCP server scope, they would typically logon to an individual DHCP server in order to create the scope.

IP address management software forces you to rethink the way that such activities are performed. A good IP address management system should serve as a management layer that spans the entire organization. In other words, if you need to perform a management task, such as creating a DHCP server scope, you would perform it through the IP address management software rather than interacting directly with an individual DHCP server.

Of course this raises the issue of compatibility. Before investing in an IP address management system, it's important to make sure that the system is compatible with your DHCP and DNS servers. Ideally, the IP address management software should support DHCP and DNS solutions from multiple vendors.

Keep in mind that one of the most important reasons for deploying an IP address management system is that the software should improve the efficiency of managing IP addresses. These gains in efficiency come in a number of forms, but one of the ways in which efficiency is improved is through the standardization of management tasks.

If an administrator performs tasks such as creating DHCP scopes or DNS records directly through the IP address management software, as opposed to performing the tasks directly on a DHCP or DNS server, then it means that the administrator is using the IP address management software in place of the native DHCP and DNS management tools. This allows for standardization in multivendor environments. If for example an administrator needs to create a DNS record, they could create the record using a standardized interface regardless of the vendors. DNS server is ultimately going to be hosting the record.

The concept of a standardized management interface that spans the entire organization and that's vendor agnostic is extremely important. Having such an interface greatly reduces the administrative learning curve, while also eliminating the inconsistencies that inevitably exist in multivendor environments.

The fact that it's possible to use a single tool to manage all DNS and DHCP servers across the entire organization has other implications as well. In larger organizations, there may be formalized management boundaries that exist. Any tool that provides an organization level management structure absolutely must respect departmental boundaries within the organization.

For instance, an organization may be structured in a way that places a different administrator in charge of the various subnets. This is especially common in larger organizations that have campus area networks. This type of management model is sometimes also used by organizations that have chosen to allow, Bring Your Own Device. In such organizations, there may be an administrator dedicated to maintaining wireless subnets, and the supporting infrastructure that allows end-users to connect personal devices to the corporate network.

In any case, an IP address management system must be able to adhere to established administrative boundaries. Otherwise, the solution will be disruptive to the organizations established management framework.

Ideally, an IP management system should allow administrative access to be delegated by subnet. Furthermore, the software should allow for the use of role based access control. For example, an organization may wish to differentiate between an administrator who can update DHCP and DNS records and an administrator who can perform DHCP and DNS updates, but also initiate manual scans of the network.

A permissions model should ideally also include a permission that can be assigned in order to achieve read only administrative access. Read only administrative access is useful for a couple of different reasons. This type of permission is most commonly used for administrative training. Imagine for a moment that an organization hires a new administrator. If the new administrator isn't already familiar with the IP address management software that the organization is using, then allowing the administrator to interact with the software without the proper training could potentially be dangerous. Providing such an administrator with read only administrative access gives them the opportunity to explore the system, and learn how the IP address management software works without having to worry about accidentally making any changes.

View only administrative permissions can sometimes be useful outside of training situations. Consider an organization in which multiple administrators are each responsible for overseeing individual subnets. In such an organization, each administrator should only have administrative access to the subnet that they monitor. However, some organizations also extend view only permissions to other subnets as a courtesy to the administrators. The reasoning behind this is that if an administrator encounters a problem, and they suspect that the problem might be related to the way that another subnet is configured, they can at least look at the configuration data for the remote subnet to see if their suspicions are correct. If the administrator does in fact discover a problem, they can contact the administrator for the remote subnet and discuss the problem with them.

Conclusion

As you can see, there are a number of best practices surrounding the use of IP address management software. Ultimately however, many of these best practices boil down to making sure that you adopt an IP address management system that allows for efficient and practical management of IP and related resources. Furthermore, IP address management software must be flexible enough to allow various best practices to be followed, otherwise the organization may not be much better off, compared to when they were using a manual approach.

All that being said, your IP address management system should encompass the following: deliver reduced operational costs by reducing labor and inefficiencies related to assigning, inventorying, and deprovisioning IP addresses. Similarly, the system should decrease costs by automatically diagnosing IP related issues on the organization's network. These cost saving benefits can only be achieved if the IP address management system provides certain key capabilities, such as:

- Automated network (subnet and device) scanning to build accurate address space maps and available IP's within an address block. It should also take the guess work out of finding open addresses and virtually eliminate accidental duplicate IP address usage.
- Integrated DHCP and DNS administration to reduce effort and improve accuracy provisioning and decommissioning IP's. It should offer Multi-vendor DHCP and DNS support. Further, it should use existing investments in DHCP and DNS services, while providing a single and consistent management interface.
- Monitoring, alerting, and troubleshooting. Make sure critical resources and operations are working as intended and if problems occur, then know before they become big problems and have the tools to fix issues fast.
- Role-based administration allows distributed and specialized admin teams to use the same tools and work together to manage DHCP, DNS, and IP resources.
- Integration with other IT management tools.

To learn more about how SolarWinds IPAM can help you implement these best practices for managing your DHCP, DNS and IP Addresses, please visit:

solarwinds.com/ip-address-manager.aspx

whitepaper

About the Author

Brien Posey is a freelance technology author with over two decades of IT experience, and has received Microsoft's MVP award 13 times for his work with Windows Server, IIS, Exchange Server, and File Systems / Storage. Posey has authored dozens of books and many thousands of articles, and routinely speaks at various international IT events. Prior to going freelance, Brien served as CIO for a national chain of hospitals and healthcare facilities. Previously he served as a network engineer for the United States Department of Defense at Fort Knox. He has also worked as a network administrator for some of the nation's largest insurance companies.