efficient iP™

White Paper

10 Key Best Practices for Efficient IP Address Management (IPAM)

In an ever-evolving business environment, IT agility and efficiency have become of strategic interest to companies, in order to stay competitive and execute sustainable long-term growth. IP address plans, DNS and DHCP services are network foundations playing a key role in meeting these challenges. Over time, IP addressing environments have become both mission-critical and very complex to manage. The bottom line is that organizations are now as agile as their IP infrastructure foundation.

In order to make your network's IP addressing environment as flexible, secure, reliable and responsive as possible, the following simple best practices should be followed :

- Maintain centralized, unified and automated IP Address Management services for holistic visibility, overall consistency control and lightning-fast services.
- Determine IP plan structure and naming strategy based on business needs for operational efficiency and scalability
- Define corporate standards and enforce assignment policies to streamline and simplify deployment processes
- Optimize IP space fragmentation for network scalability, agility and routing performance
- Delegate DNS, DHCP and IP address management wisely and enable "On-demand self services" to decrease operating costs while improving SLAs
- Maintain a change history for easier and faster troubleshooting
- Leverage periodic audits and manage reconciliation for proactive management, mobility tracking and quality control
- Regularly Monitor IP space, DNS and DHCP usage for accurate network capacity planning
- Ensure DDI services availability for business continuity
- Start planning IPv6 transition now

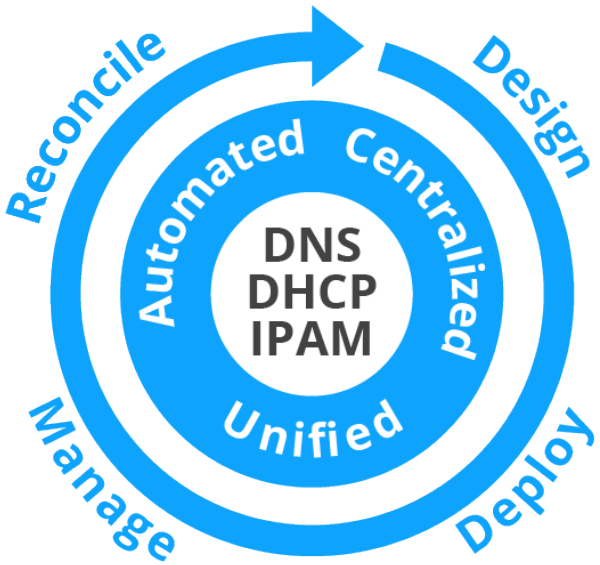
For a variety of reasons, including mergers, acquisitions and rapid growth, many networks have become a hodge-podge of different naming and addressing schemes. The explosion of IP-based devices, mobility, virtualization and cloud computing have only added to the problem. The resulting complexity can quickly lead to critical issues when underestimated or incorrectly addressed. IP addressing plans with DNS and DHCP services are critical network foundations upon which infrastructure scalability, routing performance and application accessibility directly rely.

Therefore, IP address management (IPAM) services are vital for providing efficient change management in order to ensure the quality and continuity of IT operations. The guidelines below are fundamental best practices for successful implementation of an IPAM service which maintains IT operation reliability and automation, thus enhancing business efficiency.

1» Maintain centralized, unified and automated IP Address Management services for holistic visibility, overall consistency control and lightning-fast services.

A central inventory is a foundation for the overall network consistency control. It offers a holistic view and immediate access to any IP space information. It also prevents many common manual errors such as conflicting assignment of IP addresses, undesired subnet overlapping, conflicting DHCP configurations, incompatible VLAN(s) deployment, and naming convention errors. Additionally, it provides efficient capacity planning tools to anticipate address pool exhaustion as well as global reporting capabilities that engineers need to ensure the infrastructure's optimal operation level.

Since IP addresses, VLANs, DNS records and DHCP leases are mutually dependent resources, they should not be managed independently but with a global approach. Consider implementing a unified management framework that will handle these elements and their dependencies, ensuring the ongoing consistency of the related repositories while significantly reducing administration costs. For instance, the allocation of an IP address should automatically update the DNS service's configuration by creating type A, PTR and CNAME records on the appropriate DNS servers associated with the prefix belonging to this address.



2» Determine IP plan structure and naming strategy based on business needs for operational efficiency and scalability

It is very important to design an IP addressing schema according to a model that supports a business. Organizations sometimes fall into the trap of pushing for the opposite. Regardless of how a business changes, matures or grows, IT departments sometimes only see through the eyes of the network, thinking the business should fit into the context of an existing infrastructure instead of how infrastructure should fit the business. This can very quickly lead to variety of issues such as limited change capacity, complex security policy definition or reduced network performance.

Enabling quick and smooth evolution of business operation is key, meaning that IP plan schemas must be flexible enough to ensure ease of change management for optimal company operating capabilities- from deployment of new services (VoIP, CCTV, private cloud) to mergers and acquisitions or opening of subsidiaries.

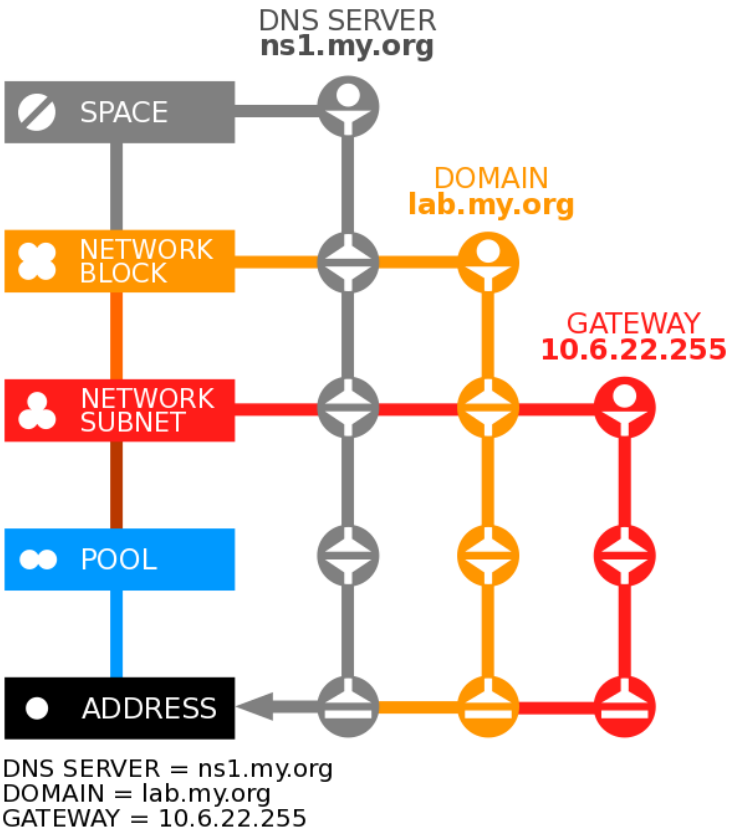
However, despite the need for designing an address schema that supports the business, it should not be forgotten that technical constraints must be taken into consideration to ensure the performance, scalability and security of any network. A numbering plan should permit the efficient routing of traffic, while properly applying the correct security policy and quality of service on a per application basis.

For both a technical and business approach, designing a multi-level hierarchy should be considered. For example, an initial level is designed regarding routing considerations typically done per region, and then sub-levels for subsidiaries and points of presence.

3» Define corporate standards and enforce assignment policies to streamline and simplify deployment processes

As we have seen previously, an IP address plan defines the intrinsic structure of any network and its related routing policy. In addition, it is also the skeleton upon which company's policy management should be defined in order to streamline and simplify deployment processes of IP, DNS & DHCP services. For each level of the IP plan hierarchy, specific options, attributes (tags) and properties should be pre-defined. For instance, IP addresses provisioned into a DMZ subnet could be registered in a specific DNS zone and VoIP subnets could be automatically created with specific IP-phone vendor options. Inheritances from a level to a sub-level of the hierarchy should also be integrated in this policy enforcement strategy for an end-to-end approach.

At the same time, an IPAM can store a lot of information about provisioned IP resources. Guiding users on easily and properly documenting assignments is therefore key to consider for network management efficiency and capacity planning purposes. The use of templates of forms per object type, such as for servers or printers, reduces the deployment complexity as it limits the amount of information to be qualified while constraining at the most granular level specific policies. For instance, naming conventions could be easily enforced alongside the IP plan structure through built-in rules & wizard-driven deployments according to the object type, location and finally, the qualified name.



Inheritance of various properties across IP objects

This top-down approach extended at the company level maximizes resource capacity, enhances the overall network consistency and provides the required flexibility for ever-evolving environments. The delegation of network management is dramatically simplified, as policies and conventions are automatically applied.

4» Optimize IP space fragmentation for network scalability, agility and routing performance

Uncontrolled IP space fragmentation can quickly impact a business by reducing the ability to deploy new subnets and scale a network according to its needs, thus degrading a network's performances and complexifying its administration.

For instance, when dealing with a business reorganization rife with unstructured assignments, network administrators may have no other choice than to split some blocks, in which subnets may have been assigned haphazardly. Typically there are a few at the beginning of a block's range, and some at the end. As a result, the block reorganization complexifies the routing and filtering policy leading to potential network performance and/or security issues.

Consequently, optimizing subnet aggregation to avoid IP prefixes' fragmentation is important. When designing an IP address plan, one should consider allocating subsequent prefixes per region, saving some of them for future use. Then, the resulting region prefixes can be split into smaller units that will match local business presence. Only then should the assignment of the service and application subnets intended to be deployed locally (so that the related policies apply) be planned.

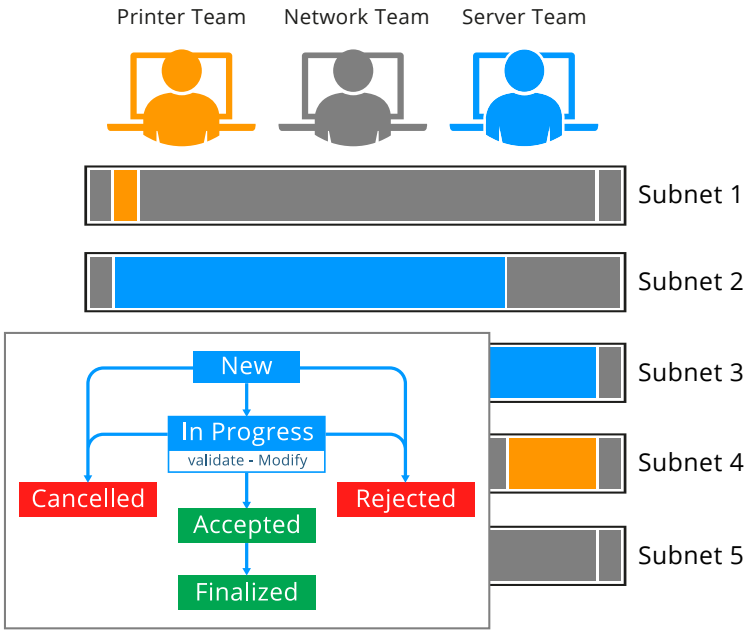
Doing so mitigates the risk of maintaining unnecessary routes due to a fragmented routing topology, and simplifies network administration. Additionally, subnet summarization in complex environments will improve network performance by minimizing the number of routes in the forwarding tables - saving router memory and decreasing latency.

5» Delegate network management wisely and enable "On-demand self services" to decrease operating costs while improving SLA

Delegation is a win-win in an industrialization process, allowing a team to focus on its own valuable tasks while its "customers" become empowered for quicker services delivery. This follows the current trend regarding IT automation that progressively allows the delegation of technical actions to non-experts.

This applies to network management, as handling resources can be time consuming. Organizations should implement a proper rights management system that allows for delegation authorization according not only to a rigid resources hierarchy, but also to business operational needs.

It can also be useful to delegate authorization on other basisl. For example, it might be wise to delegate IP address management to a team in charge of a service to which dedicated subnets are allocated. A help desk may be given visibility on connected computers, laptops or printers for which they are responsible. Similarly, a VoIP team could manage the IP resources within the subnets dedicated to this service. Leveraging end users themselves is also possible, by providing them with a proper portal allowing them to register their own personal devices connected to the enterprise network.



6» Maintain a change history for easier and faster troubleshooting

IP Addresses and DNS records are critical resources that are used to access any device or service through a network. Any change to an IP address assignment or DNS configuration can significantly impact the availability and quality of any service. Even if straightforward and rigorous management procedures have been defined, there may be misconfigurations. Tracking every change affecting the IPAM, DNS or DHCP is highly recommended for both security and troubleshooting purposes. This should enable quick identification of each change, with full details (Who-What-When) to ensure fruitful analysis.

7» Leverage periodic audits and manage reconciliation for proactive management, mobility tracking and quality control

The best IP schemas and smartest assignment policies can quickly become worthless if there is no control over their precise and continuous application. An accurate and on-going audit of IP resources is a crucial process to ensure the consistency of an IPAM reference database over time. It allows for the identification of assignment issues, unused resources and to maintain adequately-sized networks, as well as switching equipment and address pools across a network. Furthermore, combining such audits with DNS/DHCP service configuration compliance should be considered, as it will ensure the consistency of your network service delivery.

An efficient audit system must offer the reporting capabilities of:

- Identifying connected network devices
- Tracking MAC-IP address associations
- Tracking per device IP address assignments
- Tracking conflictual VLAN deployment
- Identifying conflictual IP address and port assignments
- Identifying unused IP addresses and networks
- Identifying unused DHCP ranges and static leases
- Comparing DNS database with IPAM database
- Comparing DNS/DHCP services options configured across servers

Any IPAM deployment should be associated with the implementation of an automatic inventory process, designed to confront and reconcile the results of the network discovery with the database used as a reference in the infrastructure management process.

8» Regularly Monitor IP space, DNS and DHCP usage for precise capacity planning

IP addresses and DNS records are limited resources, which makes it important to plan and supervise their usage. Leveraging periodic audits and real-time monitoring tools for building address utilization statistics across IP spaces (especially within DHCP ranges) helps to implement a realistic capacity plan. This allows for the proactive request of new public IP address ranges, or taking proper action within a private IP address space to prevent loss of ability to deliver network connectivity to new services or clients due to an IP address shortage.

DNS Resource Records must not be ignored. It is important to take advantage of periodic audits to identify and clean up DNS server configurations. Orphan DNS entries that are no longer related to any assigned IP address should be removed as often as possible. These prevent the reuse of the related FQDN (Fully Qualified Domain Name) in the deployment of new services. Worse, they may allow some users to access deprecated applications which can lead to a security breach.

9» Ensure DDI services availability for business continuity

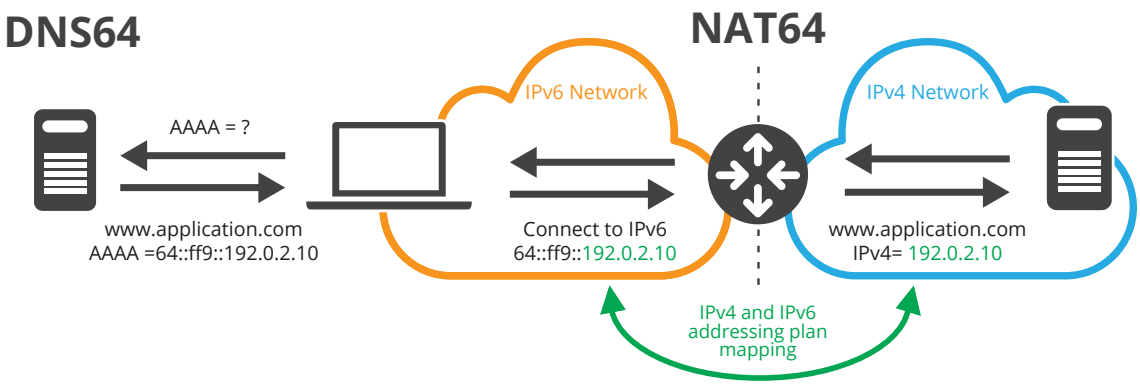
DNS, DHCP and IPAM (DDI) services are critical IP network services. Their availability is crucial to ensure access to any other network service such as web browsing, email or even VoIP. It is recommended to deploy IPAM, DNS and DHCP services using highly available platform patterns. If an IPAM service's redundancy relies on active/passive clustering to ensure database consistency, one should consider active/active deployments across several data centers geographically distributed for DNS and DHCP platforms. This ensures the maximum availability of these mission-critical services while complying with disaster recovery best practices.

At the same time, it is wise to implement an active monitoring solution to monitor DDI services using active polling, in order to measure service performance and detect potential failures. For even better visibility, measuring the real latency and availability of DDI services from the users' point of view is also beneficial. This allows for better troubleshooting and a heightened user experience.

10» Start planning IPv6 transition now

IPv4 address exhaustion is already pressuring – even mandating – IPv6 usage in regions like Europe and Asia. Many organizations have already deployed dual-stack IPv6 on their public network links to ensure their communication with anyone on the Internet. Yet, most of their private IT infrastructures still rely on IPv4, while hyperscale datacenters, BYOD and IoT are pushing the need for activating IPv6.

As a network foundation, one of the most important steps of any IPv6 deployment project is the IP addressing plan definition alongside DNS and DHCP services. IPv4 and IPv6 coexistence management requires a structured IP addressing schemes mapping strategy. Whether it's parity-based or a different approach, the mapping design must scale easily, simplify dual-stack deployments, ensure service access consistency, and maximize resource capacity.



Even trickier when deploying IPv6 is the protocol's inner capability to auto-address the connected devices using their interfaces' MAC addresses, combined with any prefix broadcasted by the local routers. This extra feature called "IPv6 Stateless Address AutoConfiguration" (SLAAC) should be disabled, and instead it is recommended to use DHCPv6 to always assign IP addresses and forego the seeming convenience of SLAAC. This allows an organization to retain control over IP address assignment on a network.

Leveraging years of working with customers and analysts, this white paper suggests the top best practices for effectively managing the IP address space within an enterprise. Exercising some or all of these practices can drastically improve the business efficiency of organizations, resulting in cost and time savings, as well as increased customer satisfaction. Utilizing our experience and these recommendations, EfficientIP has developed solutions and products to simplify the way that businesses manage their IP addresses, including IPAM for Linux as well as Microsoft.

efficient iP™

REV: C-1708

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
3 HarbourFront Place, Level 11
HarbourFront Tower 2, Singapore 099254
+65 6678 7752