



*The knowledge
behind the network.®*

Best Practices for Next-Generation IP Address Management

By Tim Rooney

Director, Product Management

INS

Best Practices for Next Generation IP Address Management

By Tim Rooney, Director, Product Management

Introduction

IP management can be defined broadly as encompassing three major interrelated functions:

- ▶ **IP address inventory** – Obtaining and defining public and private IP address space, and allocating that address space to locations, subnets, devices, address pools, and users on the network.
- ▶ **Dynamic IP address services management** –Defining the parameters associated with each address pool defined within the IP address space management function, appropriately configuring Dynamic Host Configuration Protocol (DHCP) servers to supply relevant IP addresses and parameters to requesting users, and effectively managing the capacity of address pools to assure that dynamic IP addresses are available for those who need them and are permitted to have them.
- ▶ **IP name services management** – As devices are assigned IP addresses statically or dynamically, configuring appropriate Domain Name System (DNS) servers with address-to-name and name-to-address resource records so that end users may access hosts and/or applications by name (e.g., by URL) is critical. Managing name space and name services also requires proper design of the name space, configuration of other relevant DNS resource records, and many behavioral aspects of DNS as well.

Each of these functions is critical to the proper operation of an IP network. Users need at least one IP address to access the network, whether via a wired or wireless LAN interface, VoIP device, video device, etc., and they need to access resources on the network and the Internet to maintain a high level of productivity. The job of an effective IP address manager is essentially to be invisible. In other words, as users attach to various network points, they are automatically configured to communicate and easily access network resources by URL/name. Effective IP management requires proper allocation of address space so there's adequate address capacity where it's needed when it's needed, accurate configuration of DHCP servers for dynamic address users, including differentiation of employees versus "guests", and accurate configuration of DNS servers so resources can be accessed easily. When these behind-the-scenes tasks are flawlessly executed, network users don't need to contact the help desk with complaints about the network; the IP address manager is invisible.

This white paper provides IT professionals a guide for how to flawlessly execute tasks for IP management, and recommends best practices for simplifying the IP management process. These best practices are derived from the INS software division's leadership team's collective experience in the IP management space obtained through numerous implementations of IP management systems, and interactions with end users and industry analysts. Many members of the team have also been active in the Internet Engineering Task Force (IETF) in evolving IP technology.

IP Address Inventory Management

IP address inventory has several facets in its own right. This function within IP management lays the foundation for the other IP management functions, and impacts other critical IP network functions, not the least of which is routing. Most enterprise organizations will obtain public IP address space from an ISP, though some that have been using the Internet for some time have a legacy relationship with their Regional Internet Registry, e.g., ARIN and RIPE. After a block of public IP address space has been obtained, it can then be allocated to locations across the network. Similarly, private IP address space (RFC 1918) can also be allocated in a similar manner.

Address Planning

When planning to allocate IP address space, whether private or public, administrators must forecast the IP address capacity requirements in each end user accessible subnet on the network. This is typically based on the number of end users located at each site, the number of visitors or mobile users expected at the site, and the number of IP addresses required on average for each end user. While the easy answer is to grossly oversize each subnet, in reality this isn't feasible given IP address space constraints. Even for plentiful private address space for large networks requiring a centralized IP management system, costs associated with managing many large networks can be prohibitive. Given these address space sizing constraints, administrators must ultimately allocate an address block to each site.

Address Allocation

An additional constraint is that the allocated address block be appropriate to the routing infrastructure supporting each site. Block allocations at each site must “roll up” in terms of maximizing address hierarchy in order to facilitate route aggregation for routing protocols such as OSPF (Open Shortest Path First). Maximizing route aggregation helps to reduce routing protocol traffic and keep routing tables manageable. In addition, it helps to reduce the probability of rendering certain networks unreachable. This can occur when an address block from one region is assigned to another region but the block is included in a higher layer route advertisement, rendering the assigned block unreachable outside the advertising region. The address space planning process then needs to carefully consider the macro level requirements for address space as well as the rollup of individual address space requirements. For example, a global corporation may wish to subdivide its space among a core backbone of sites covering three continents (Figure 1). It may make sense to subdivide the “root” address block into three in a manner that meets the current and foreseeable capacity needs of each continent. To size each block properly, planners must define the individual site

requirements, perhaps roll these up to regional levels for a mid tier within the routing topology, and then roll up to the tri-continental core routers. Modeling address space in such a hierarchical, inheritance-based manner, then allocating space optimally at each hierarchy layer, is key to maximizing address utilization in a routing-efficient manner.

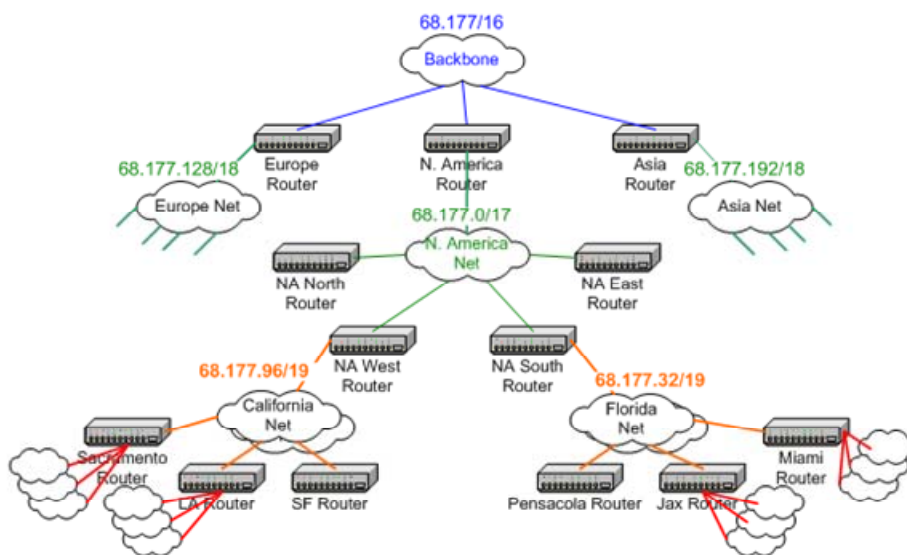


Figure 1: Hierarchical Network Allocation

If IP network allocation is done improperly, duplicate IP addresses can be assigned, networks can be rendered unreachable due to the route summarization example described above, or IP address space itself can be rendered unusable if address allocation is not only performed hierarchically, but in an optimal manner to preserve address space for use elsewhere. Due to the nature of binary arithmetic in subnetting IP networks, errors or suboptimal allocations can occur, resulting in ineffective address capacity utilization. When more address space is needed, such inefficiencies would likely need to be corrected via a painful renumbering process before additional address space would be granted by an Internet Registry or ISP.

Managing Address Dynamics

After the initial sizing and deployment, even when done perfectly, changes inevitably occur. New corporate sites are opened and others are consolidated. Perhaps more mobile users require IP addresses on a subnet than initially expected. Additional IP addresses for redeployed servers are required on a subnet. New services such as VoIP are rolled out. Note that these events, whether initiated by business requirements impacting site openings and closures, by IT in deploying additional IP services such as VoIP and adding more servers or devices for performance or other reasons, or by end user behavior in terms of addressing requirements at particular sites, all impact the IP address space. Staying on top of these and other changes, which reflect the organic nature of IP networks, is absolutely necessary for effective IP address space management.

IPv6

Issues with address space management become even more critical as IPv6 begins to make inroads into service provider and enterprise networks. The sheer size and hexadecimal representation of IPv6 addresses invites operator errors, stifling effective IP address management. And because few if any customers will actually deploy IPv6 in a “greenfield” environment, integration of IPv4 and IPv6 address allocation processes is crucial.

IP Address Inventory Management Best Practices

The following are best practices for IP address inventory management.

Best Practice

<input checked="" type="checkbox"/> Inventory address space in a centralized database	<p>IP address space, both public and private, is a precious asset, one that provides the fundamental entity for network communications. Therefore, it must be tracked in a centralized repository to maintain consistency and accuracy. Of course, accuracy requires updates to the database upon address space allocations, “free-ups”, and ideally utilization per allocated block or subnet.</p>
<input checked="" type="checkbox"/> Rigorously record allocations and periodically reconcile actual IP-related data from the network with the inventory database.	<p>Maintaining inventory database accuracy is crucial. If the IP address inventory only tracks top-down allocations of address space entered by administrators manually, how do you know it’s accurate? Comparing the inventory database with network actuals is crucial to identifying discrepancies and tracking IP management processes. For example, if someone circumvented the conventional update process, whereby the inventory database was not “informed” of the change, the identification of this discrepancy would not only highlight an inventory mismatch, but also bring out this network change control issue. Whether you employ a top-down or bottom-up approach to allocating addresses to router interfaces or address pools to DHCP servers, updating the inventory must be a key step in the process. Periodically reconciling the network actuals with the database plan is an effective way to monitor the process and keep inventory accurate.</p>

<p>☑ Perform and track address space allocations in accordance with routing topology to model and optimize route aggregation.</p>	<p>Network allocations should be made in an optimal manner, maximizing utilization of address space, while mapping to the topology model. Allocating address space along a hierarchical structure that models the routing topology facilitates route aggregation to keep routing overhead to a minimum. If exceptions to the aggregation model are necessary, for whatever reason, they can be made knowingly and routes can be proactively updated to maintain reachability. Since routing topology often maps to an organization's locations, sites, or business unit hierarchy, this hierarchical modeling of address space typically provides the added benefit of tracking address allocations to these entities.</p>
<p>☑ Implement common allocation policies within address blocks to promote consistent subnet addressing.</p>	<p>Many organizations allocate or reserve specific portions of each subnet for ranges of static device addresses and dynamic address ranges. For example, you may reserve addresses .1 and .2 for router addresses on a subnet (or the first and second addresses in general), .3 and .4 for time servers, etc. Provision of a common allocation template promotes consistency in allocation and deployment, and also makes for easier troubleshooting as needed with consistently allocated subnets.</p>
<p>☑ Maintain additional information as appropriate per IP device.</p>	<p>Keeping track of what device is occupying each IP address in a subnet is critical to IP management. However, many such devices have other attributes that should be tracked within an IP management solution. Not the least of these attributes is what other IP addresses the device in question occupies. Many devices have multiple IP addresses, whether for virtual networking, IPv4 and IPv6 addressing, or for multi-homed devices. Multi-homed devices have multiple interface cards, each occupying one or more IP addresses. Beyond this critical IP address information, tracking other attributes, including device type, location, administrative contact, asset information, and associated resource records to name a few, are equally crucial.</p>
<p>☑ Monitor address utilization to capacity manage the IP address space.</p>	<p>Although initial addressing needs may be impeccably forecast, changes happen in IP networks due to business, IT, or other reasons. Despite the best planning efforts, IP networks seem to have an organic nature, where address needs rise and fall at different times at various locations within the network. Address utilization statistics across subnets and DHCP pools should be collected to provide snapshot and historical tracking of address use. This information can also be trended via linear regression models to identify potential future address depletion times. This trending analysis provides another decision criterion in the IP address capacity management process.</p> <p>Additional criteria for even more proactive management of IP address capacity require the use of alerts for notification of pending address depletions before they happen. Alerts should be programmed for address pools or networks approach full capacity. This proactive measure can assuage potential pending address depletions, which can render end users unable to communicate due to the lack of addresses.</p>
<p>☑ Keep IPv6 in mind when considering IP address investments, even if IPv6 is on the outskirts of your planning horizon.</p>	<p>If your organization is considering adoption of some or all of the best practices outlined in the section to centralize IP inventory, automate allocation processes, etc., consider your long-term plans for IPv6 and if appropriate, require IPv6 support in any tools you invest in to protect your investment for years to come.</p>

Dynamic IP Address Services Management

Following the IP inventory best practices described above can help maintain adequately sized networks and address pools across the network. But sizing address pools to supply IP addresses to end users, critical as it is, is just the beginning of the process of address assignment via DHCP. After all, you don't want just anyone to get any IP address on your network to access network resources! So there's more to configuring DHCP servers than address pool allocations. Additional configuration elements include valid options and policies with associated values for each address pool, valid or invalid devices by MAC address, client class, or user authentication, device software validation, and DHCP failover configuration.

Policy Management

As many or all DHCP servers will require similar DHCP policies, we recommend that you centralize the configuration of these servers to create a single or set number of policies, then deploy the policy(ies) across your servers. This practice ensures a consistent and accurate approach to setting these critical policies. Otherwise, you must be concerned with entering basically the same information multiple times into each of your servers. A similar argument can be made for defining DHCP option sets, with defined DHCP options and valid values for use on assignment.

Discriminatory Address Management

In terms of discriminating address assignment, there are several levels of policies or controls most DHCP solutions provide. The first is to simply filter by the MAC address of the client requesting an address. If the DHCP server has a list of acceptable (and/or unacceptable) MAC addresses, it can be configured to provide a certain IP address and associated parameters to those clients with acceptable MAC addresses, and either no IP address or a limited function IP address to those without acceptable MAC addresses. By *limited function IP address*, we mean that the network routing infrastructure is pre-configured to route IP packets with such addresses to only certain networks, such as to the Internet only, or even nowhere.

This type of IP address and configuration assignment is also possible by filtering on the client class of the client requesting an IP address. Certain clients, such as VoIP phones, provide additional information about themselves when requesting an IP address in the vendor class field of the DHCP packet. The user class field may also be used. The DHCP server can be configured to recognize the user classes and/or vendor classes of devices on your network to provide additional information to the DHCP server when assigning the IP address and configuration parameters. Addresses can be assigned from a certain pool and/or additional configuration parameters can be assigned to the client via standard or vendor-specific DHCP options.

A third level of discriminating IP address assignment is possible by authenticating the user of the machine requesting an IP address. This function can be used in conjunction with MAC address and client class discrimination described above. For example, if a client with an unacceptable MAC address attempts to obtain an IP address, one option is to completely deny an address; another option is to require the user of the client to login via a secure access web page. This enables easier capture of new MAC addresses for legitimate users of your network. (Those users sometimes pop in new interface cards!) Solutions ranging from simple perl scripts to sophisticated integrated software solutions are available to direct such users to a login/password requesting webpage. A simple lookup against a database of legitimate users then allows access or denial of the client to a production IP address.

Beyond these device identification measures based on MAC addresses, client classes, and user authentication, DHCP can also provide additional validation on the machine requesting the IP address. The DHCP process can be used to invoke an external security scanning system to scan the requesting client for viruses or to validate use of acceptable virus protection software. This device scanning step can be used alone or in conjunction with the device identification measures to provide a robust access security solution via DHCP.

DHCP Failover

DHCP failover is recommended to provide address services redundancy across your IP network. If a DHCP server crashes, a failover server can take over and begin processing DHCP transactions. This provides a higher availability service for your end user clients requesting IP addresses. If clients cannot get IP addresses, they will be unproductive and will call the help desk!

Dynamic IP Address Assignment Management Best Practices

The following are best practices for IP address assignment management.

Best Practice

<input checked="" type="checkbox"/> Centralize DHCP server configuration to improve configuration accuracy and consistency.	Utilizing a single interface and database to configure a number of DHCP servers provides the ability to enter configuration parameters once, and deploy the “master” configuration to multiple DHCP servers. This promotes consistency of configuration and simpler address pool allocation and reallocation as necessary for ongoing address pool capacity management, while still allowing for per-server configuration.
<input checked="" type="checkbox"/> Implement security measures to provide selective address assignment.	Implement one or more of the following approaches: <ul style="list-style-type: none">• Device identification via MAC address – filter client requests against a list of acceptable and/or unacceptable MAC addresses• Device identification via client class – provide additional configuration information for known client classes configured on your network• User identification via authentication – support user login/password authentication against a database or other authentication scheme• Invoke device security scanning or software validation – scan the requesting device for viruses and/or valid software prior to granting a production IP address
<input checked="" type="checkbox"/> Adopt and use established DHCP option and policy sets across your DHCP servers.	This allows implementation of a consistent set of policies across a variety of DHCP servers, each with its own address pools. This approach allows mobile clients to obtain a consistent IP configuration, no matter where they connect into the network.
<input checked="" type="checkbox"/> Configure DHCP failover for high availability address assignment services.	IP address assignment is the first basic step to communicating on an IP network. Make sure this service is available to your clients in a high availability configuration. This can be accomplished in at least two ways. <ul style="list-style-type: none">• The first mechanism is the traditional failover scheme where a common address pool is shared among two DHCP servers. One DHCP server is the primary server and processes DHCP address requests; the other server is a failover server, or “hot standby”, keeping in synch with the primary’s DHCP lease bindings and heartbeat messages. Should the primary server fail, the failover server can kick in and begin handling DHCP address requests.• The second mechanism that can be employed when address space is not overly constrained, e.g., 10.0.0.0 space for some users, is to deploy two address pools of the same size, but of different addresses. This “double scope” approach uses two address pools that can serve the same set of clients independently and alleviates the need for inter-server heartbeat communications, while providing sufficient address capacity for the end users requiring addresses.

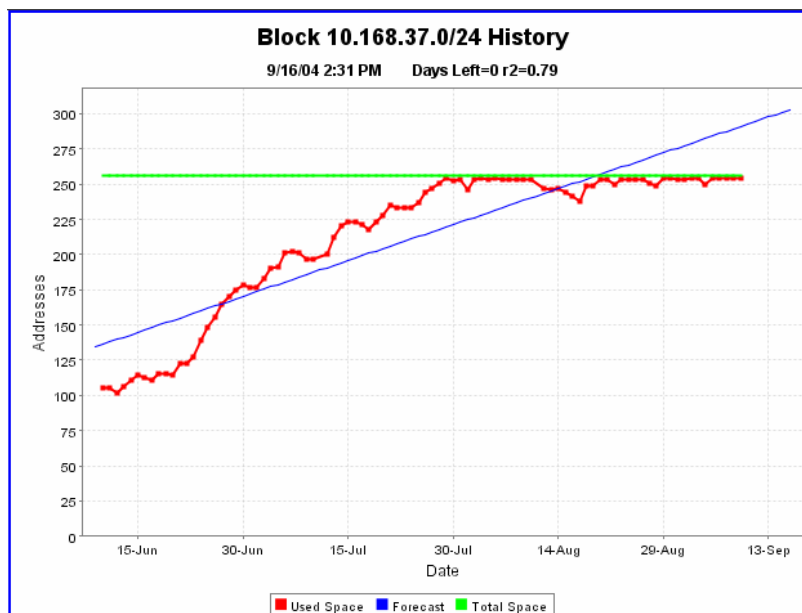
☑ Track dynamic address assignments and monitor utilization of address pools, including shared subnets, to proactively manage address pool utilization.

As with the address inventory capacity management best practices, this “corollary” best practice recommends use of DHCP monitoring of address assignments and address pool utilization, including shared pools or shared subnets, to net out the capacity impacts from a pool and pool user perspective.

☑ Maintain IP address pool history data to monitor address usage trends and proactively align address space to where it’s needed.

While alerting and thresholds provide an effective notification of an impending address depletion based on recent actual utilization data, having the ability to track utilization “snapshots” over time is effective to identify address utilization trends. Accessing address pool historical data in a graphical form (Figure 2) especially helps convey at a glance the general utilization trends and enables proactive management of address pools while facilitating proactive realignment of address pool capacity as necessary to prevent address depletions.

Figure 2: Graphical Address Pool Capacity History and Trending



IP Name Services Management

After a user on your network obtains an IP address and related IP configuration via DHCP, hopefully all of which happens seamlessly behind the scenes, most end users will immediately access their email and/or the web or intranet. The ability to send email to someone’s address at a destination host and browse the web via universal resource locator (URL) makes email and web browsing easy and user-friendly. Your computer communicates with the email server and web server via IP packets using IP addresses, not names or URLs. Fortunately DNS was invented to allow users to type text-based addresses while providing a mechanism to translate these text-based addresses into IP addresses that computers can communicate. It’s not a stretch to say that without DNS, these applications could function but would be totally unusable for 99% of your company’s population. Needless to say, DNS services must be configured accurately, and be highly available to users.

DNS Resource Records

It's up to IP address managers to properly configure the DNS servers in the network with the information needed to resolve host names and URLs into IP addresses. This means that not only statically configured IP devices like routers, web servers, email servers and the like need to have entries in DNS, but also dynamically configured IP devices like printers and even end user machines. In many cases, websites perform a *reverse* DNS lookup for an IP address before continuing a web session to validate that the requesting IP address has some form of legitimacy in DNS. This implies an integration between DHCP and DNS, referred to Dynamic DNS, which is an automated process to update DNS upon address assignment by a DHCP server.

Beyond name-to-address translation and vice versa, DNS provides many other “translation” applications, which we won't go into here. Each translation type maps to one or more resource record types in DNS. For example, an “A” resource record type is used to translate a text-based host name into an IPv4 address. While all resource record types follow the same basic format in terms of fields within the record, the syntax is not intuitive nor is it easy to identify errors until problems arise. While DNS does provide a mechanism for a master DNS server to update its slaves via a zone transfer, in some cases, it is desirable to operate in a multi-master mode of operation, whereby each master must be updated individually. This opens the door to potential errors in not only resource record configuration but also in other DNS options and directives, of which there are many.

DNS Options

Configuring these DNS options is critical to properly defining the behavior of the DNS server, in terms of zone transfers, security measures, and other operational parameters. Various directives exist in varying forms in different DNS server versions. For example, logging configuration varies between BIND versions 8 and 9. Other vendors' DNS implementations may have other nuances in configuration. Keeping track of the proper syntax for the particular vendor/version you're running may be tedious, but it's absolutely critical to keeping DNS up and running.

DNS Security and Availability

In terms of security measures for DNS, the following are recommended approaches:

- ▶ Configure ACLs – configure which IP addresses or networks can query, notify, update, and transfer to or from each name server.
- ▶ Configure transaction signature keys – sign each update and zone transfer with the use of transaction signature keys (TSIG keys).

DNS is architected with high availability in mind, with the ability to configure a master or multiple master DNS server(s) and a set of slave DNS servers that receive resource record updates from the master(s) via zone transfers.

IP Name Services Management Best Practices

The following are best practices for IP name services management.

Best Practice

<p><input checked="" type="checkbox"/> Centralize the DNS server configuration to improve configuration accuracy and consistency.</p>	<p>Utilizing a single interface and database to configure a number of DNS servers provides the ability to enter configuration parameters once, and deploy the appropriate master or slave configuration to multiple DNS servers, then aggregate dynamic updates to keep the centralized inventory up-to-date. This provides a centralized view into the overall DNS configuration across your network for DNS servers, domains, zones, and views.</p>
<p><input checked="" type="checkbox"/> Run multiple DNS servers on different subnets for each zone to maximize availability of critical DNS services to end users.</p>	<p>Deploy DNS servers to eliminate common points of failure and maximize reachability from internal resolvers and to the Internet. Trade off the simplicity of running a single master DNS server for each zone versus the more complex deployment of multi-master DNS. Single master zones ease configuration by requiring updates to one master server; however, take care to minimize exposure to unauthorized updates to this master. Multi-master configurations have less vulnerability but require careful management of the dynamic update process to reduce cyclic updates.</p>
<p><input checked="" type="checkbox"/> Periodically validate DNS configuration files to check for syntax errors, lame delegations, and other errors that can reduce the accuracy and effectiveness of the DNS infrastructure.</p>	<p>This configuration verification should be done prior to reloading a zone or entire server configuration, as well as on a periodic basis for audit and validation purposes. A backup copy of at least the most recent working version of each server's configuration files should be maintained to allow roll back should a corrupted or misconfigured file end up being deployed.</p>
<p><input checked="" type="checkbox"/> Configure external, internal, and perhaps other "views" of your name space.</p>	<p>This can be accomplished either by configuring separate views on separate name servers (e.g., an external set of DNS servers and a separate internal set of DNS servers) or on a single set of DNS servers utilizing the "views" feature of BIND 9. This provides an external version of externally exposed domains to keep resolvable hostnames to a manageable number, large or small. Meanwhile, a different version of domains can be provided to those querying DNS from internal networks. This simple dual view example can be extrapolated to multiple views, allowing granular configuration of which host names get resolved with what if any, IP address(es).</p>
<p><input checked="" type="checkbox"/> Tighten security by configuring ACLs, transaction signatures for dynamic updates, zone transfers and control messages, and specifying particular TCP/UDP ports for queries, updates and zone transfers.</p>	<p>BIND code offers a variety of configurable options that allow specification of ACLs, pair-wise server transaction signatures, and IP address/port specifications. While these options provide the flexibility for configuring these capabilities, the key is to accurately configure each server with its corresponding ACLs, keys, and IP addresses/port numbers. For a large number of servers, this can be cumbersome and error-prone to configure manually.</p>
<p><input checked="" type="checkbox"/> In high performance environments, configure caching-only DNS servers to handle large volumes of DNS queries.</p>	<p>Caching-only servers are simply name servers not configured as authoritative for any zones. All queries to caching-only servers result in a lookup in cache with escalation to the DNS root servers as necessary. Over time, these servers build up a substantial cache and can respond directly from cache for those records with "still alive" TTLs.</p>

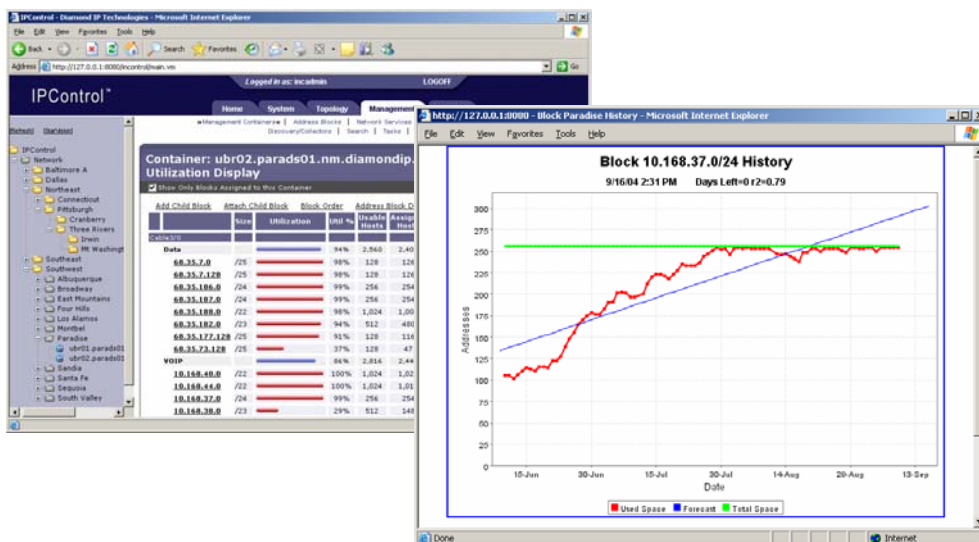
Simplifying Best Practice Implementation with IPControl™

Given the tight relationship between IP address space management and its implication on DHCP and DNS server configuration, employment of a centralized IP management tool that supports the latest DHCP/DNS server technologies can simplify implementation of these best practices and reduce IP management resource requirements while reducing configuration errors. INS's innovative IPControl software product provides a comprehensive centralized IP management solution for managing IP address space and capacity, as well as DNS and DHCP server configurations. IPControl provides support for sophisticated DNS/DHCP services, including DNS views, logging configuration, transaction signature support, DHCP client classes, and much more.

IP Address Inventory – streamline IP inventory functions

- ▶ IPControl provides a centralized IP address inventory database, from which IP space can be consistently assigned and capacity managed, and DNS and DHCP servers can be configured.
- ▶ IPControl helps automate subnet allocations, simplifying the allocation process to a few mouse clicks and reducing binary arithmetic errors. Actual configuration information can be collected from network devices to enable reconciliation with the database plan vs. network actuals.
- ▶ IPControl enables you to model your network topology via its innovative container construct (Figure 3). Containers allow you to define a hierarchy and track address space allocations in accordance with routing topology to model route aggregation.
- ▶ IPControl's address allocation templates allow you to reserve subnet addresses for each subnet for routers, servers, and other elements common to your subnets, breaking down each pre-allocation by static, dynamic DHCP, automatic DHCP and manual DHCP address ranges.
- ▶ IPControl provides unparalleled user definability, including user-defined device types. Each device type can have its own attributes via Information Templates and naming policies for DNS updates. In addition, container policies can be set to define allowable device types per container, and per-container Information Templates to allow per device/per container attributes.
- ▶ IPControl collects data from network devices and DHCP servers to gather actual IP address utilization information across the network. User defined alerts warn you of impending address pool exhaustions.

Figure 3: IPControl's Innovative Containers and Graphical Interface



IP Address Assignment – automate accurate address assignment

- ▶ IPControl enables you to centralize your DHCP server configuration to improve configuration accuracy and consistency.
- ▶ IPControl provides multiple secure DHCP mechanisms, including client filtering by MAC address, client class, user authentication, and/or device verification callouts.
- ▶ IPControl provides user-definable option sets and policy sets, which can be applied across multiple DHCP servers to promote configuration consistency.
- ▶ IPControl enables simple configuration of DHCP failover for high availability address assignment services, whether using shared scopes or double scopes.
- ▶ IPControl automates tracking of dynamic address assignments and monitor utilization of address pools, including shared subnets, to proactively manage address pool utilization.
- ▶ IPControl maintains address pool history data along with linear regression trending to present pool utilization in an easy to understand graphical format. At a glance, you can determine address pool usage trends, communicate this among multiple organizational levels, and take proactive action.

Name Services Configuration – simplify accurate DNS configuration while enabling advanced features

- ▶ IPControl enables you to centralize your DNS server configuration to improve configuration accuracy and consistency.
- ▶ IPControl can support nearly any configuration of multiple master/slave DNS configurations from a few servers to several hundred servers. IPControl agents can be deployed throughout your network to facilitate scalable deployments, promoting maximum flexibility and unconstrained DNS server network design.
- ▶ IPControl provides a feature to validate your DNS configuration files prior to deploying them to production DNS servers in your network. This enables you gain an extra level of assurance of the validity of your DNS configuration files. Should an erroneous configuration be deployed from IPControl or direct configuration file edits, IPControl enables the added assurance of configuration rollback if needed.
- ▶ IPControl is the first software product to support configuration of DNS views from a GUI interface. IPControl enables you to create separate views on separate name servers (e.g., an external set of DNS servers and a separate internal set of DNS servers) or on a single set of DNS servers utilizing the “views” feature of BIND 9.
- ▶ IPControl enables you to tighten security by configuring ACLs, transaction signatures for dynamic updates, zone transfers and control messages, and specifying particular TCP/UDP ports for queries, updates and zone transfers.
- ▶ Configuring caching only DNS servers is a snap with IPControl. In general, DNS server templates allows administrators to define DNS servers for virtually any application, whether for caching-only, internal root or authoritative name servers and more.

IPControl Differentiators

Previous generation products were of great assistance for managing IP address space at the time they were introduced, that is, when IP networks were relatively unsophisticated. However, IP networks have evolved to support more hierarchical topologies, multimedia services beyond best-effort data, and in the level of sophistication of DHCP and DNS technologies they require. These previous generation products have not kept pace with the way you need to manage the evolved IP networks of today. IPControl was developed with this evolved IP network in mind. IPControl provides the following unique features, which enable incomparable next-generation IP address management:

- ▶ Hierarchical, multi-tiered, centralized IP address inventory
 - IPControl is the only software product that enables modeling of multi-tiered, hierarchical IP networks in its centralized inventory. This is enabled by its patent-pending container structure.
- ▶ Simplified DNS/DHCP configuration
 - While many other tools support centralized or distributed configuration of DNS servers, IPControl is the only product today that supports BIND 9 views, TSIG, DDNS, controls, logging, option/server templates, and much more—all within the GUI interface. This simplifies and improves the accuracy of DNS configurations.
 - IPControl also provides a unique DHCP policy set to define behavioral aspects of DHCP servers under management. In addition, DHCP failover configuration is vastly simplified using either the traditional approach on a per-server or per-subnet basis
- ▶ Data collection from the network
 - Only IPControl integrates the automated data collection of configuration and active lease information from network services to reconcile the inventory database's version of network and server configuration (“planned”) vs. the actual configuration.
 - In addition IPControl is the only product that tracks historical address utilization data for reporting in intuitive, easy to read graphical reports on address utilization and trending. User defined thresholds and alerts enable you to define conditions for alerting you of impending address depletions so you can proactively allocate address capacity where it's needed before it runs out.
- ▶ Unsurpassed user definability
 - IPControl allows you to manage your IP address space the way you want to manage it, not in accordance with a rigid software tool. You can define user defined fields in the system of various data types (text, radio button, text box, drop down list, and more), whether required or not, along with other attributes. Groups of user-defined fields, called Information Templates, can then be associated with containers, subnets, and devices to allow you to track this additional information with the corresponding system element.
 - IPControl also supports user defined device types and the most flexible device naming policies on the market. You can define and concatenate free text, IP address, incrementors, and more to define policies per device type.
 - Policies for containers, which can map to your network topology or geography, can be established in terms of allowable address types and device types, and associated Information Templates to enable you to attach different information to a particular device type in one area differently from another if desired.
 - Thresholds and alerts can be activated to define the conditions required to fire an alert, along with the associated criticality, for container-level, address block level, and DHCP server level alerts.
- ▶ Integrated IPv4 and IPv6

- IPControl is the only IP address management product that supports both IPv4 and IPv6 in one integrated product. This allows you to plan out and either experiment with IPv6 in a non-production environment or fully institute and complete a migration from IPv4 to IPv6 over time. IPv6 is coming, so any IP management software investment you make today should incorporate this “next generation” IP.
- ▶ Affordability
 - With this superior feature set, you might expect to pay more for IPControl than you would for previous generation products. But next generation thinking goes beyond product features. IPControl provides exceptional value by providing these key differentiating features for next generation IP address management, at less than half the price of comparable competing solutions.

Conclusion

INS IPControl™ software provides an advanced next generation IP management solution that enables you to automate many tedious, error-prone, yet crucial IP management functions. IPControl provides unsurpassed extensibility and user-definability to enable you to manage your IP address space the way you want to manage it, all at an affordable price. Please email us at diamondip@ins.com to learn more about how IPControl can automate more of the IP management functions you need at an exceptional ROI.

About INS

INS (International Network Services Inc.) provides IT infrastructure consulting services, software, and solutions to help companies build, secure, and manage business-critical networks. Our end-to-end consulting solutions address customers’ needs in IT Strategy and Planning, IT Infrastructure, Operating Systems and Directory Services, Storage Systems and Services, Security, Network and Systems Management, and Project Management helping them optimize their businesses to better face competitive challenges and meet future demands. The Diamond IP™ family of software from INS provides flexible and scalable solutions for today's complex IP networks. We are one of the world's largest independent IT infrastructure consulting solutions providers with a track record of thousands of successful engagements. INS is headquartered in Santa Clara, Calif. and has offices across the U.S. and Europe. For additional information, please contact INS at 1-888-767-2788 in the U.S., 44 (0) 1628 503000 in Europe, or 1-408-330-2700 worldwide, or visit www.ins.com

Diamond IP and IPControl are trademarks of International Network Services Inc.

Copyright © 2004, International Network Services Inc.

This is an unpublished work protected under the copyright laws.
All trademarks and registered trademarks are properties of their respective holders.
All rights reserved.