



IP Address Management and DNS Management

A white paper by Incognito Software
February, 2006

IP Address Management and DNS Management

Automated IPAM for Risk Management	2
The Complete IPAM Lifecycle	3
Cost-Effective IP Address Expansion	3
Fast Integration with Business Processes and Systems	3
Efficient RIR Reporting	4
Large-Scale DNS Management	4
Fast Domain Updates and Distribution	4
DNS Management Interfaces with Diagnostics and Roll-Back	5
Conclusions	5

IPAM software can substantially reduce risk for organizations that depend on IP-based networks to operate.

Automated IPAM for Risk Management

Organizations today – service providers, large enterprises, or government agencies – depend on IP-based networks to operate. They cannot afford the risks or productivity hits from problems related to network reliability, security, or downtime. Complete DHCP, DNS, and IP address management (IPAM) software can substantially reduce those risks if it offers a strategic approach to network management including centralized databases, diagnostics, auditing, provisioning, and automated reporting.

IPAM involves the analysis, assignment, and tracking of IP addresses and DNS (Domain Name System) records. A 2004 report from Forrester Research states that most network downtime is due to manual errors in IP addresses and DNS records. Gartner analysts also found that IP management can reduce the cost of administering IP addresses by as much as 83%. Nevertheless, 45% of \$1 billion-plus companies still manage their IP address space manually with spreadsheets or other tools, 25% use software developed in-house, 10% don't have any solution, and only 20% have full-fledged, industry-tested IPAM software.

The risks associated with the lack of automated IPAM are significant. Worldwide, IP networks are increasing in complexity as users demand more communications features from the billions of electronic devices now deployed. This amplifies the impact of manual IPAM errors on network reliability, security, customer service, user access, and IT department productivity.

An IPAM solution also needs to perform fast, secure, and reliable DNS updates so that an organization can easily reach new customers and prevent security attacks, and customers can remain confident in the company's ability to manage information.

All these factors are making the topic of IPAM impossible for organizations to ignore.

The Complete IPAM Lifecycle

IP addresses and DNS records are used by every device on a network: laptops, servers, printers, VoIP phones, cable and DSL modems, multimedia terminal adapters (MTAs), and more. The IP addresses provide unique network identifiers so that devices can communicate with each other, and DNS information gives devices human readable names so that a user can simply type in the name, such as www.incognito.com, without knowing the specific IP address. If one device needs to contact another through a domain name, a DNS server gets involved by associating the domain name with its IP address.

True IPAM software automatically manages the complete IPAM lifecycle.

True IPAM software automatically manages the complete IPAM lifecycle. This includes synchronization of DHCP and DNS servers with verification of IP address space during DNS record changes and DNS updates during IP address assignments. It also comprises enterprise-wide analysis, monitoring, and reporting on IP address usage and DNS operations.

Although open-source IPAM software is available, it requires extensive support and maintenance for long-term use because IP networks are continuing to evolve.

Network administrators need to plan, assign, and track IP address space accurately, efficiently, and reliably using industry-tested software that is upgradeable as IP networks change.

An automated IPAM solution can meet the needs of either broadband or enterprise networks. The solution must allocate blocks of address space for specific uses, track individual IP address assignments, update DNS servers, report on IP address space utilization, and audit all changes made in the system.

Cost-Effective IP Address Expansion

IPAM tools help organizations continually evaluate how their current IP address space is being used and justify the need for more.

As IP networks grow at an exponential rate, organizations need to continually evaluate how their current space is being used and justify the need for more. Requesting additional IP address space from service providers or RIRs can be time-consuming and costly.

Proper IPAM tools should provide a way to do this efficiently. They must automatically report on utilization, easily re-number IP addresses, and update network elements such as DHCP, DNS, and routers associated with this space.

Additionally, an IPAM software investment needs to last into the future as your business grows with scalability to millions of domains, IPs, and subnets.

Fast Integration with Business Processes and Systems

IPAM software should allow users to customize network views, delegate administration, and integrate with existing infrastructure.

There are two aspects to integration: processes and infrastructure.

First, for maximum efficiency, organizations need to view their IP address space and domain names in a way that is meaningful to them. An IPAM solution should allow users to customize views of IP address space and domain names and delegate administration by region, department, domain, customer, or other custom topologies.

Then various administrators can be responsible for managing selected address blocks and domain groups according to assigned permissions for viewing, requesting space, assigning nodes, and other actions.

Second, to provide an end-to-end IPAM solution, the software must support integration with a company's existing information infrastructure such as back-office OSS, billing, and SIP proxy systems using tools like Java and CORBA APIs.

Efficient RIR Reporting

Due to limited IPv4 address space, RIRs have very strict reporting and justification policies. Organizations that have received address space directly from RIRs must produce detailed reports about their use of existing space and reasons for requiring additional space.

An IPAM solution should simplify this process through automated collection of IP address information as well as SWIP updates and reports to RIRs such as ARIN and RIPE. It saves staff many hours or even months of time from having to learn the intricacies of those specialized requirements, and avoids the possibility of an RIR denying more IP space because of inadequately updated WHOIS entries or poorly documented justifications.

Large-Scale DNS Management

Before the widespread use of IP networks, DNS was the responsibility of the IT department's web or email support group and was typically implemented using BIND. Many DNS solutions offered administrative tools that looked at DNS in a patchwork manner, making DNS modifications easier but not addressing DNS stability for the entire organization.

Now the time has come where having a centralized, robust DNS solution is a necessity. A solid DNS solution must offer centralized domain management of multiple servers as well as data integrity verification, auditing, and diagnostics. It should perform domain updates across multiple zones without any need for server re-starts. It should also use a centralized database for enterprise-wide distribution and synchronization of domain data. Unlike BIND, which usually relied on a single administrator to make updates, a centralized system using a high-throughput SQL server can manage simultaneous updates by multiple users, ensuring that the information conforms to best practices, and distributing the information to various DNS servers all over the network.

High-performance voice and video applications also require that DNS systems integrate with third-party software via a multi-threaded API such as Java, or use a highly flexible communication architecture such as CORBA, which support multiple tasks running in parallel inside the same process.

Fast Domain Updates and Distribution

In order for a DNS system to operate in a fast, secure manner, all DNS servers must use consistently-defined parameters for security settings and domain values.

RIRs require detailed utilization reports as well as SWIP updates.

A solid DNS solution must offer centralized domain management of multiple servers as well as verification of data integrity.

Parameters include DDNS security permissions and zone transfer settings. There are also Start-of-Authority (SOA) records, which identify the authoritative DNS server(s) that publishes information about a domain and DNS servers with information about domains "beneath" it in the naming hierarchy (eg., www.incognito.com is located "beneath" incognito.com). Through this hierarchy, information about a change in a domain name's IP address is recorded on one DNS server and transmitted to other DNS servers when necessary. A local DNS server can resolve a domain's IP address by recursively requesting information from a series of DNS servers with progressively more information. The local DNS server works on the domain name from right to left, starting with a question for the root nameserver, which is responsible for top-level domains such as .com or .org. That server delegates the question to another DNS server, which has information about the next domain level in the name. Each server delegates a question on to the next server in the hierarchy until the proper IP address is found.

Domain profiles, which associate a set of domains with a list of local DNS resolvers, also allow for mass editing and automatic distribution of domain data. Any updates to domains are automatically distributed to the servers on the associated list, and new name servers added to the list are populated with the associated domain data.

DNS Management Interfaces with Diagnostics and Roll-Back

Advanced diagnostics, auditing, and roll-back are necessary for fast resolution of any DNS-related network issues.

If email distribution stops, an organization needs to track down the root cause and precise timing of the problem. For example, with the right diagnostics and auditing tools, the IT department may trace the problem to a change an administrator made to an authoritative name server at a specific time, and then roll back the server to its previous settings. Built-in diagnostics can also prevent an administrator from modifying or creating a mail record that points to a non-existent host.

Conclusions

The only way to manage the huge number of IP-based devices and services in operation today is through automated IPAM software. Productivity dramatically increases when valuable staff transition away from manual IP address administration and on to more strategic projects, helping the entire organization achieve more.

Resolution of common issues like email failures require advanced diagnostics to pinpoint problem sources.

Contact:

Incognito Software Inc. www.incognito.com
Phone: 604.688.4332 or US/Canada toll free 800.877.1856
Email: sales@incognito.com