Conquering the Challenges of IP Network Management with DHCP and DNS

A white paper by Incognito Software
Conquering the Challenges of IP Network Management with DHCP and DNS

Introduction ............................................................................................................... 2
Challenges of IP Networks ............................................................................................ 2
  Manual Host Configuration ..................................................................................... 3
  Lack of HostName-to-IP Address Mapping ............................................................ 3
  Limited Reliability ................................................................................................. 3
  Limited IP Address Space ....................................................................................... 3
Evolution of IP Networking Standards............................................................................. 3
  DHCP for Assignment of IP Addresses ..................................................................... 4
  DNS, the Domain Name System ............................................................................. 4
  Dynamic DNS (DDNS) for Hostname- to-IP Address Mapping .................................... 5
  DHCP Failover for Maximum Reliability ................................................................... 5
Implementation Choices ............................................................................................... 5
  Windows NT® Implementations .............................................................................. 5
  UNIX® Implementations ......................................................................................... 6
Critical DHCP and DNS Features for Today’s IP Networks................................................... 7
  Integrated DHCP and DNS Management Interfaces ............................................... 7
  Uniform Addressing Policies and Domain Preferences ........................................... 7
  Standards-Based Hostname-to-IP Address Mapping .............................................. 7
  Delegated Resource-Based Administration ............................................................ 7
  Redundancy and Reliability .................................................................................... 7
  Platform Independence ......................................................................................... 8
  Import Utilities ..................................................................................................... 8
  Advanced Diagnostics Utilities ............................................................................. 8
Future of IP Network Management ................................................................................. 8

Introduction
Integrated DHCP and DNS management is critical to maintaining reliable TCP/IP network and Internet operation. With the increasing use of Internet-based technologies, networks have grown in size and complexity, as have the challenges for network management. While IP networks have become more sophisticated, the tools that most organizations use to manage them have remained primitive.

To minimize the time spent overseeing IP networks, administrators must use efficient DHCP and DNS management tools and open standards-based solutions. These software tools eliminate error-prone manual methods, reduce administrative costs, increase reliability, and improve security.

This paper describes the background of DHCP and DNS technologies, open standards for managing IP networks, and current industry trends.

Challenges of IP Networks
Administrators of TCP/IP networks commonly encounter issues such as manual host configuration, hostname-to-IP address mapping, reliability, and limited IP address space.
Manual Host Configuration

In a TCP/IP network, each network device must have a unique IP address based on its local segment, plus a default gateway, subnet mask, and a DNS server, all to interact with other network devices. Traditionally, this required an administrator to manually maintain a detailed list of these parameters, but this process was very time consuming and prone to errors.

Lack of HostName-to-IP Address Mapping

TCP/IP networks do not inherently provide automatic hostname-to-IP address mapping. A hostname is the human-readable name by which a network device (like a computer, server, modem, or printer) is identified on a network. The hostname corresponds to an IP address and, ultimately, a unique hardware MAC address. Without hostname-to-IP address mapping, network administrators would need to look up the location of devices manually, a very time-consuming process.

On a LAN, a hostname is often a single word such as "Computer1." On the Internet, a hostname is usually a combination of the host's local name and its parent domain's name, (for instance, www.incognito.com includes the host label "www" and the domain name, incognito.com). This type of hostname, also known as a Fully Qualified Domain Name or FQDN, is translated into an IP address via the local host's file or a DNS server (discussed later).

Limited Reliability

Fault tolerance and redundancy are crucial to the success of IP networks. They must be available without interruption, which translates to 5-nines reliability, or less than 8 hours of downtime per year.

Limited IP Address Space

The IPv4 specification provides 32-bits of address space, which represents over 4 billion addresses. However, only a small percentage are available for use, partly because of the tremendous growth of Internet use worldwide, and partly because of inefficient assignment of addresses in the early years. Although the upcoming IPv6 revision will greatly expand the pool of available IP addresses to 128 bits, the limitations of IPv4 will remain.

Evolution of IP Networking Standards

The Internet Engineering Task Force (IETF) committee drafts standards, known as Requests For Comment (RFCs), to introduce new capabilities to the Internet. In 1985, the IETF defined the BOOTP protocol to allow a diskless workstation to receive an IP address and a limited number of configuration options (subnet mask, default gateway, and others) based on its MAC address at boot time.

Although useful, the BOOTP protocol was primitive and only handled static IP addresses, which did not allow for the rapidly expanding number of hosts on the Internet and continually changing network configurations.
DHCP for Assignment of IP Addresses

To overcome the limitations of BOOTP, in 1993 the IETF defined DHCP (Dynamic Host Control Protocol), which became the de facto standard when it was included in Microsoft® Windows 95.

DHCP is a client/server protocol. A DHCP server assigns an IP address as well as a set of configuration parameters to a network device (the DHCP client) so it can participate on an IP network. Configuration parameters are called DHCP options and include subnet mask, default gateway, and domain name.

DHCP is an extension to the BOOTP protocol. Its distinguishing feature is the ability to allow DHCP clients to receive IP addresses for a lease period that can be renewed on an ongoing basis.

To request an IP address, a DHCP client generates a “DISCOVER” message by sending a broadcast on the local network segment. If a DHCP server is on the local segment, it will try to service the request by sending back an "OFFER" message. If a DHCP server is not on the local subnet, the request is forwarded through a router acting as a relay agent. The relay agent is responsible for inserting its IP address into the packet (known as the giaddr field), to indicate the location of the client, and forwarding it onto other subnets that may have DHCP servers.

Since the client may receive OFFERs from several DHCP servers, it must decide which server to use – typically, the first response it receives. The client then sends a “REQUEST” message to the selected DHCP server, which replies with an “ACK” message that contains the IP address, a lease time, and the requested DHCP options.

DNS, the Domain Name System

DNS (Domain Name System) is the name service for the Internet and provides a name lookup facility that correlates each domain name with an IP address.

A DNS server can resolve the IP address of a domain outside its name space by recursively requesting information from a series of other 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.

To support this functionality, DNS relies on a hierarchal, distributed system of name servers and a standardized language to query these servers. A resolving server can look up a name in its own name space or query other DNS servers to take part in searches for domains outside its space.
Each domain has one primary DNS server and at least one secondary server for backup.

DNS servers store a domain’s namespace in zone files. Zone files contain information such as hostname-to-IP address mappings, and mail and name server locations.

**Dynamic DNS (DDNS) for Hostname- to-IP Address Mapping**

With the exponential increase in the number of hosts on the Internet, it became evident that DNS had two drawbacks.

First, the DNS system was designed to read zone files, which were editable but the changes would not take effect until the DNS server was stopped and re-started. Second, primary DNS servers could only update slave servers through processes called zone transfers. Traditional full zone transfers are inefficient because they occur on a scheduled basis instead of occurring as changes are made. These full transfers also involve transfer of all the records in a zone regardless of how many are changed.

The DNS standard needed to support dynamic configuration and a mechanism to send updates to slave servers immediately. To address these problems, the IETF defined Dynamic DNS (DDNS) protocol in RFC 2136, zone change notification in RFC 1996, and incremental transfers in RFC 1995. DDNS allows DHCP servers to send updates to primary DNS servers, removing the need for administrator intervention. Additionally, when a change is made on the master server, a zone change notification is promptly sent to the slave servers, with only the changed records being transferred.

**DHCP Failover for Maximum Reliability**

Since DHCP has become such a critical network application, DHCP servers need to be highly reliable. A new IETF draft addresses this issue. The DHCP Failover protocol allows a DHCP server to have a shadow service that is constantly updated with both configuration and data files. The shadow service polls the primary service to determine its status. If the primary service goes down, the shadow service becomes the primary. When the primary comes back online, the shadow updates the primary and resumes control.

**Implementation Choices**

Despite the wide acceptance of IETF standards, several DHCP/DNS solutions are still available without RFC compliance and may lack enterprise-wide management capabilities.

**Windows NT® Implementations**

Networks using Microsoft DHCP and DNS services have limitations in managing name spaces and IP addresses. Without an up-to-the-minute, detailed view of enterprise-wide address space, it is difficult to accurately assess address usage or manage address allocations efficiently. This challenge is compounded if the organization has an address shortage.
• No Resource-Based Administration – Windows NT DHCP and DNS services rely on an exclusive adminlist to provide configuration access. This has prompted individual locations in some large enterprises to implement their own DHCP server, resulting in less control of address space – a costly and inefficient way to operate. With resource-based administration, central administrator can manage all address space and provide site-based administrative rights for specific address ranges.

• Limited Hostname to IP Mapping – WINS provides hostname to IP address mapping using the NETBIOS namespace. WINS is known to cause broadcast storms and lose records. WINS provides a Microsoft-only solution, whereas DDNS is an open standards-based solution.

• Lack of Diagnostic and Auditing Tools – Windows NT’s solution only tracks active addresses. It does not maintain log or audit trails, making it difficult to diagnose problems or determine IP address usage from a historical perspective.

• Lack of RFC Support - The DDNS and DHCP Failover protocols are not supported, which severely limits MS DHCP’s ability to operate in a heterogeneous environment and provide reliable services. Its lack of DDNS support prevents Microsoft’s DHCP servers from updating domain name servers.

**UNIX® Implementations**

Whereas Windows NT is a common DHCP platform, UNIX is a common platform for DNS. This is due to TCP/IP networks originating from the UNIX environment.

Most UNIX implementations use a DNS program called BIND (Berkeley Internet Name Domain). BIND has been so pervasive that compatibility with it is considered essential for any competitive DNS product. Some of the drawbacks of UNIX platforms are:

• No GUI - UNIX-based DHCP and DNS implementations still rely on text files for configuration information. Without a GUI, it is very easy to mistype or use improper syntax. Typical DNS problems stem from an administrator forgetting to fully qualify a domain name for an MX record and as a result halting all mail operations.

• Lack of Resource-Based Administration - Because most UNIX systems are running other important software (such as payroll, HR, and more) as well as DNS and DHCP, UNIX administrators may not give access to other network administrators for security reasons. As a result, many simple DNS changes, including BIND updates, must wait until the UNIX administrator has time.

• Diagnostic Tools - Diagnosing network problems is difficult and may require involvement from the UNIX administrator due to access restrictions. BIND’s logs are also very cryptic and difficult to follow.
Critical DHCP and DNS Features for Today’s IP Networks

Through DDNS capabilities, DHCP Failover, GUIs, diagnostics tools, and delegated resource-based administration, standards-based DHCP and DNS services make the management of entire IP networks more cost-effective, efficient, and reliable.

Integrated DHCP and DNS Management Interfaces

An integrated DHCP/DNS interface with setup wizards can provide administrators with unprecedented flexibility and ease of configuration. For example, a setup wizard can configure a DHCP service to automatically update the DNS service with any changes to hostname-to-IP address mappings. The wizard steps through the configuration process to enable DDNS support in the DHCP and DNS, adds the IP address of the DHCP service to the DDNS security lists, and generates the appropriate in-addr.arpa domains for the network ranges configured in the DHCP service. Additionally, an administrator can select DNS records and drag them to the DHCP service to make those records “static” entries.

Uniform Addressing Policies and Domain Preferences

These features simplify configuration and minimize administrative errors. A DHCP service should use policies to quickly generate address ranges based on object types. For example, every network segment may have the first 20 addresses reserved for servers, the next 10 addresses for printers, the next 10 for laptop users and the remaining for PCs. Domain preferences allow administrator to set domain security settings for zone transfers, DDNS, notify, lookup and configuration.

Standards-Based Hostname-to-IP Address Mapping

This capability allows a DHCP service to update any RFC 2136-compliant DNS service whenever an IP address is assigned. This ensures that any client with a dynamically assigned IP address can be identified by its hostname. When the IP address of a host is changed, its DNS information is dynamically updated by DDNS to associate the existing host name with the new IP address. This process allows you to eliminate WINS from your network and provide an all inclusive view of your network.

Delegated Resource-Based Administration

This type of administration allows various groups of administrators to manage specific IP address ranges and domains. The benefit is that a central administrator can control all address space, and in turn, control costs, while permitting remote locations to manage their own address ranges. Otherwise, an organization’s remote offices may set up their own DHCP service with little regard to the rest of the network.

Redundancy and Reliability

Fault tolerance and redundancy are crucial to the success of an IP and DNS management solution. Any commercially available DHCP solution must support the latest IETF draft for DHCP Failover.
Platform Independence
DHCP and DNS management software should run on Windows, Solaris, and Linux environments with a web-based management utility to monitor, configure, and manage services from any operating system.

Import Utilities
Utilities should be available to allow you to easily import your existing DNS and DHCP data into a management console, whether that data is located in an existing Novell DHCP Server file, a Novell BOOTP file, or a BIND DNS master file.

Advanced Diagnostics Utilities
Diagnostics utilities provide the following capabilities:
- Fast troubleshooting of DHCP, BOOTP, and DNS issues
- Auditing of when, where, and who received an IP address or made domain changes
- Multi-level logs to display requests and service processing
- Color-coded views of IP address status in selected ranges with indications for free, active, reserved, offered, and unused addresses, as well as who is using the address
- High-water marks for tracking the numbers of allocated addresses against pre-set limits, with warning emails if the limit is exceeded

Future of IP Network Management
IP address and domain management are essential to maintaining a secure, reliable and robust network. New generations of DHCP and DNS management software allow IT professionals to meet the demand for more IP-based services and efficiently manage the traffic on their growing networks. Upcoming DHCP and DNS services will likely include the following features:
- IP Allocation and Hostname Mapping Based on User Authentication – Currently, DHCP services map a hostname to IP address. Machines and network devices receive IP addresses, not the user. In proprietary network operating systems, it was necessary for a user to become authenticated prior to receiving an address and gaining access to network resources.
- Dynamic White Pages Based on Organizational Units – A user should be able to dictate which directories are updated. For example, if an employee is away from the office, they should be able to receive an IP address from their ISP and update their corporate DNS server with this information. This functionality requires user authentication facilities.
- Service-Based Location Vs. Server-Based Location – Windows 2000 updates DNS with service information and Windows 2000 clients query to find needed network services. All operating systems will need to include this capability for DNS to become a full-scale directory.
• PKI-Based Security — Without security and authentication mechanisms in place, DNS and DHCP cannot become all encompassing directory and network tools. Since PKI is a published and implemented standard, it is the most likely candidate for security.

• Directory-Enabled Applications. The entire industry is in the middle of a push towards directory-enabled applications, and IP management software is no exception. There are currently several packages available that use an LDAP-based directory server for their central data store, rather than a relational database. We expect this trend to continue.