White Paper

Cisco Prime Network Registrar DNS Service Enhancements

What You Will Learn

The Domain Name System (DNS) protocol is a dynamic database that provides mapping between host names, IP addresses, text records, mail exchange (MX) records, name server (NS) records, and security key information. Cisco Prime™ Network Registrar is a high-performance, scalable, integrated DNS, Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM) (DDI) solution that supports both IPv4 and IPv6 deployments on a single server. The latest release of the product (version 8.2) includes several new DNS capabilities, including support for DNS views, Domain Redirect, NXDOMAIN Redirect, and ENUM configuration. This white paper includes an overview of these new capabilities along with a summary of other advanced features within this high-performance, scalable, reliable DNS service from Cisco.

Introduction

DNS is an essential component of Internet functionality, and the protocol's first specifications were published by the Internet Engineering Task Force (IETF) in 1983. Since then, DNS features have evolved both as open source and proprietary technology. Cisco has dedicated extensive time and resources to development of its DNS functionality, which is a component of Cisco Prime Network Registrar.

One major area of differentiation between the Cisco® implementation of DNS and open source DNS products such as Internet Systems Consortium (ISC) Berkeley Internet Name Domain (BIND) is that of database architecture. File-based products such as BIND require a complete database reload when resource records are added or removed. This can delay new deployments for individual users by up to a day. By contrast, Cisco Prime Network Registrar updates individual DNS records in its database in real time, providing a significant performance benefit.

Advanced DNS Features Introduced in Cisco Prime Network Registrar Version 8.0

Cisco Prime Network Registrar DNS is standards compliant, supports both IPv4 and IPv6, and is reliable with support for High-Availability DNS (HA-DNS). High-performance DNS caching delivers query throughput that far exceeds competitive solutions. Advanced DNS features included the following.

Support for High-Availability DNS

With HA-DNS, a second primary server can be made available as a hot standby that shadows the main primary server. The Cisco Prime Network Registrar web UI and command-line interface (CLI) have features that allow duplication of the primary setup for the server pair. The server pair is responsible for detecting communication failures, power outages, and other network issues. Once HA-DNS is configured, shadowing and error detection are automatic.

HA-DNS is used with Dynamic DNS (DDNS). When a DHCP server issues a lease, it can add corresponding DNS host records to the DNS authoritative server, using the DDNS protocol. This maps a client host name to the leased IP address. Without DDNS support, DHCP performance may be affected.

Centralized Management

Cisco Prime Network Registrar DNS Version 8.0 introduced centralized management (using the regional server) of domains versus having to configure each local server cluster individually. From the regional server you can:

- Manage DNS zones and templates, hosts, resource records, and secondary servers and create subzones and reverse zones
- Manage DNS update policies, access control lists (ACLs), and encryption keys
- Synchronize DNS zones and HA server pairs, manage zone distributions, pull replica zone data, and push update maps

Dedicated DNS Caching Server

Version 8.0 of Cisco Prime Network Registrar also introduced a separation of the DNS caching server from the authoritative server. Separating DNS caching greatly improves the performance of high-volume recursive queries as the dedicated DNS caching server provides significant acceleration of DNS query throughput compared to other implementations - with up to 170,000 queries per second.

For organizations that require higher levels of protection, the dedicated DNS caching server caches all addresses resolved by the authoritative server. The caching server also provides greater security by insulating the authoritative server from the rest of the network.

DNSSEC Support

The Cisco Prime Network Registrar DNS Caching Server also performs Domain Name System Security Extensions Security (DNSSEC) validation to authenticate the origin DNS data to protect against DNS vulnerabilities from network attacks. This set of extensions to DNS provides DNS resolvers (clients) with origin authentication of DNS data, authenticated denial of existence, and DNS data integrity to combat denial of service attempts. Used in the caching service, DNSSEC checks the Internet route to resolve a domain name, ensuring that it is a trusted source. DNSSEC provides protection for domains signed using DNSSEC from:

- Spoofing/packet interception/man-in-the-middle attacks (where contents of a DNS response are modified to falsify information to the resolver)
- Name chaining/cache poisoning (poisoning of the cache with malicious query information)

Cache poisoning examples include the Kaminsky attack, ID guessing, and query prediction. The Cisco Prime Network Registrar DNS Caching Server prevents a cache attack through port randomization.

DNS64 Support

The Cisco Prime Network Registrar DNS Caching Server also supports DNS64, synthesizing AAAA (IPv6) records from A (IPv4) records in order to provide an IPv6-only client access to an IPv4-only resource. This capability helps facilitate the migration of IPv4 to IPv6. Note: In order for a DNS64 IPv6 client to resolve an IPv4 address, NAT64 is required.

RFC Compliance

Cisco Prime Network Registrar DNS is RFC compliant with approximately 45 RFCs. Two highly sought-after RFCs include:

- Dynamic update support
- Zone transfer support

This standards compliance means that Cisco Prime Network Registrar DNS is heterogeneous in its support of industry-standard DNS implementations, such as ISC BIND.

New DNS Features Introduced with Cisco Prime Network Registrar Version 8.2

DNS Views

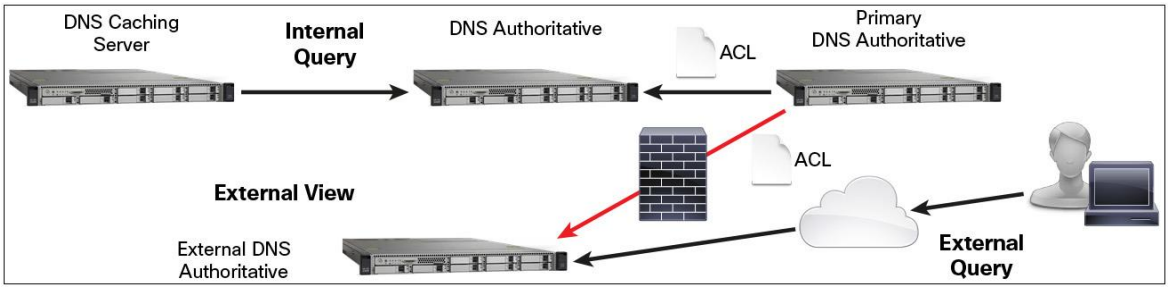
Cisco Prime Network Registrar provides implementation support for and management of DNS views. DNS views allow the presentation of alternate resource record sets (different views of the same data) to different clients based on the source or destination of the query and whether the query is recursive or not.

With DNS views, URL redirection can be implemented with one server inside of the firewall instead of two separate authoritative systems, one inside and the other outside of the firewall. Operators can realize operational savings through the ability to have a single primary DNS server for both internal and external view servers.

Another benefit is that an enterprise domain could apply this concept to name spaces outside of the campus environment to create a true set of internal (on-campus) versus external (Internet-based clients) DNS name resolution.

Using ACLs that show location and identity, users can be redirected to multiple resources based on internal and external access privileges (Figure 1).

Figure 1. Cisco Prime Network Registrar DNS Views



Domain Redirect

DNS administrators can use the Domain Redirect feature to optimize the user experience by helping users get to a predefined URL. If the user types in an incorrect URL, the Domain Redirect feature compares it to a database of URLs and redirects the domain used in the URL to an IP address that has been specified in the ACL.

The feature can be used to blacklist a domain or list of domains, redirecting the user away from risky websites to a notification page.

NXDOMAIN Redirect

This new DNS feature is related to Domain Redirect. It is used to return a response where DNS has no entry for a specified host. When a user queries an invalid domain name, an “NXDOMAIN” (error indicating nonexisting domain name) response is received.

ENUM Functionality

E.164 Number Mapping (ENUM) allows telephone numbers to be resolved to URLs using a DNS-based architecture. The Cisco Prime Network Registrar DNS UI offers an easy way to input and manage ENUM records. ENUM-compliant records can be accessed manually or using web services Simple Object Access Protocol (SOAP).

By placing telephone numbers into the DNS server, ENUM can facilitate interoperability for a wide range of applications including voice over IP (VoIP), video, presence, and instant messaging.

Summary

Cisco Prime Network Registrar includes a variety of important and useful DNS features. Cisco's unique product architecture updates individual DNS records in its database in real time instead of requiring a complete database reload when resource records are added or removed. Now Cisco Prime Network Registrar also provides support for HA-DNS and includes centralized management of domains so each local server cluster does not need to be configured individually. Version 8.0 introduced separate DNS caching and authoritative servers to increase query throughput and provide greater security by insulating the authoritative server from the rest of the network. Other important features include DNSSEC validation to protect against Cisco DNA vulnerabilities from network attacks, DNS64 support, and compliance with 45 RFCs. New DNS features in version 8.2 include implementation support for and management of DNS views. DNS views allow different "views" of the same data based on the source or destination of the query - offering enhanced security and operational expenses (OpEx) savings. Also support for domain and NXDOMAIN redirection helps users avoid “risky” websites and assists users when they query an invalid domain name, and support for ENUM allows telephone numbers to be resolved to URLs and can facilitate interoperability for a wide range of applications including VoIP, video, presence, and instant messaging.

These advanced DNS features complement the many other DNS, DHCP and IPAM features available with Cisco Prime Network Registrar.

For More Information

For more information on Cisco Prime Network Registrar, visit http://www.cisco.com/go/networkregistrar, contact your local account representative, or send an email to ask-networkregistrar@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-730186-00 11/13