Cisco Prime Network Registrar

Contents

IP is everywhere, in use in most aspects of everyone’s daily lives. We live in a world with an ever- increasing number of connected users, and an explosive growth of connected devices, each needing one or more IP addresses. Managing this IP addressability through manual assignment of IP addresses, and furthermore addressing connected devices through pre-knowledge of their IP addresses, are practices from bygone days.

- **DHCP:** In modern networks the devices learn their assigned addresses dynamically when they join the network. This is put into practice using the Dynamic Host Configuration Protocol (DHCP).
- **DNS:** Once devices have learned their assigned addresses through DHCP, they must learn the addresses of the hosts or other devices with which they want to communicate. For this, the standards have provided us with the Domain Name System, which translates human-friendly host names into the numeric IP addresses that are used by the routing systems to enable communication.

Cisco Prime™ Network Registrar provides the market-leading solution that delivers both these DHCP and DNS services.

Product overview

Cisco Prime Network Registrar is a scalable, high-performance, extensible solution that provides services for Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) acting as an Authoritative DNS, and Caching DNS which allows for additional efficiency and speed in providing domain name translations by being deployed closer to the client population and taking on considerable load that would otherwise go to the Authoritative DNS.

These functionalities are generic for all access types (Mobiliy, WiFi, Cable, BNG). Furthermore, for cable providers, Cisco Prime Network Registrar provides integration with the Cisco Prime Cable Provisioning product to provide reliable, scalable DNS and DHCP services for millions of devices.

Key technologies

PNR provides service across all access technologies. Whether your end users are connecting through Cable, BNG, WiFi, Mobile, or any of their derivative technologies, PNR can provide the Standards-compliant IP addressability services needed.

DHCP is a core network access technology - every device must be assigned a unique address when connected to the network, a virtually impossible task to undertake manually. Given the increasing number of connected users and connected devices as well as the growth in demand for network services driven by rich-media applications, automating the tracking and control of users and devices with a high-capacity DHCP server is imperative.

DNS is a core IP enabling service that is considered mission critical in today's service provider and enterprise networks. Without a fast, reliable, and secure DNS service, subscribers' Internet access will be compromised. If DNS fails, the Internet will fail. In addition, many network providers have created a dynamic service delivery infrastructure based on DNS. Service quality and delivery help build competitive advantage and new revenue-generating opportunities. Therefore, high-performing, reliable, scalable, and secure DNS is an important requirement.

Some customers require also IPAM services. Cisco has chosen not to provide this function on our price list. Instead, we maintain a partner relationship with BT Diamond were we reference sell their IPAM product for use with PNR.

Features and benefits

Cisco Prime Network Registrar provides the following features and benefits:

- **Fast and scalable:**
  - **DHCP:** With an extremely fast DHCP server, Cisco Prime Network Registrar has the ability to assign well over 20,000 DHCP leases per second. The solution is also the industry's most scalable DHCP server – supporting more than 130 million devices across multiple servers in a single customer deployment.
  - **DNS:** The recursive, extremely fast, Cisco Prime Network Registrar DNS caching server offers significant acceleration of DNS query throughput.
- **Integrated load balancing of DHCP Lease Renewals:** Smoothing server load by redistributing lease renewals, allowing better utilization across deployed clusters.
- **Reliable:** Cisco Prime Network Registrar helps address unique challenges in large-scale deployments of DHCP and DNS by offering multiple levels of redundancy with DHCPv4 and DHCPv6 simple failover and support for High-Availability DNS (HA-DNS). Our patented discriminating rate limiter provides unsurpassed DHCP avalanche prevention to reduce downtime after network outages.
- **Consolidated IPv4 and IPv6 address management:** Cisco Prime Network Registrar includes integrated, full lifecycle management for IPv4 and IPv6 and allows dual-stack addressing deployments on a single server. The full-featured DHCPv6 server provides support for address assignment, both stateless and stateful configuration, prefix delegation, and prefix stability. DNS64 functionality allows access to the IPv4 Internet and servers for hosts that have only an IPv6 address. By helping to automate the transition from IPv4 to IPv6, Cisco Prime Network Registrar mitigates IP address scarcity, facilitates deployment of new revenue-generating services, and lowers IP address management overhead.
- **Extensible:** Powerful, industry-leading extension support for both IPv4 and IPv6 allows network operators to alter and customize DHCP server operations for IPv4 and IPv6, improving network security, network performance, and third-party application integration. Extensions easily create new solutions such as billing, security, and lawful interception.
- **Health Checks:** Health checking for DHCP and for DNS to allow early detection and bypass of failed target systems. For DHCP, PNR can be configured to monitor relay agents for reliable operations in a failover configuration. For DNS, PNR can be configured to check that the destination server is a viable choice for the DNS assignment.
- **Secure:** DNSSEC, DNS firewall, TSIG, Protection against DNS Poisoning Attacks and DNS over TLS to help protect against DNS vulnerabilities. Smart Cache for DNS Caching server protects against outages when an external DNS has been compromised.

Table 1 lists additional detailed features and benefits of Cisco Prime Network Registrar.

Table 1. Detailed Features and Benefits

Feature	Benefit
Rapid Time to Value	
DNS and DHCP setup wizards	Using the basic configuration mode with setup wizards for the DHCP and DNS components, users can easily perform DHCP and DNS configuration by entering the parameters that are essential for the configuration. An advanced configuration mode is available for users with more in-depth experience with DHCP and DNS configuration. Users can quickly set up and configure Cisco Prime Network Registrar DHCP and DNS properly to facilitate IP-based services such as VoIP, LAN, and so on.
Full visibility into lease history for IPv4 and IPv6	Cisco Prime Network Registrar DHCP provides the ability to query DHCP lease history for IPv4 and IPv6. Searching of lease history is possible both at the local and regional cluster level and is compliant with European Union privacy regulations.
Simplified Dashboard, Tracking, and Reporting Capabilities	
Real-time server status dashboards	The DNS, DNS caching, and DHCP component dashboards provide at-a-glance, real-time indicators of the server health, system metrics, alarms and alerts, and inventories of the respective Cisco Prime Network Registrar servers. The dashboards display graphs for monitoring DHCP and DNS general information, throughput, and error data that can affect network operations. To measure address usage over time, the DHCP component dashboard can collect DHCP utilization information for a time period and present graphs showing trends that are useful for capacity planning. Benefits include improved network maintenance and increased uptime.
Resource notification and alerts	The ability to set two levels of resource utilization notifications – warning and critical. Threshold levels can be defined by the administrator. Settings can: • Provide an indication in the web User Interface (UI) and CLI when one or more monitored resources exceed their critical or warning levels. • Provide a report on the current state of the monitored resources in the Web UI and CLI. • Provide a means to reset the peak monitored resource values. • Generate traps when monitored resources exceed their critical or warning levels, and return to reasonable values. • Provide a means to adjust the critical and warning levels for each monitored resource. SNMP is supported and traps can be sent for these notifications.
Global search capability	Operators can quickly search for any full or partial IP address or any DNS name.
Centralized DNS/DHCP Server Configuration	
Automated configuration	Operators can significantly reduce downtime with more accurate DNS/DHCP configurations.
Advanced configuration support	Support for multitiered addressing, multihomed hosts (to model multiple IP addresses on a given device), DHCP client classes, MAC address processing, client ID, dynamic DNS, and more – all helping to meet complex network operator needs.
DHCP configuration verification and preview	Verification and preview capabilities help limit network outages and IP conflicts.

Feature	Benefit
Static IP Address Management	
Carrier-class lease reservation performance	For users with needs for static IP address assignment, Cisco Prime Network Registrar DHCP can handle up to 500,000 lease reservations. Because Cisco Prime Network Registrar supports failover deployment, the enhanced lease reservation synchronizes the lease reservation between the main and the backup server to ensure that any update to the configuration will be populated between these servers. Modification to the reserved lease configuration can be done through the web UI, a CLI, and the Java Software Development Kit (SDK).
Full-Featured DHCP Server	
Dynamic lease notification	With dynamic lease notification, network operators can request perpetual or time-bounded external system notification whenever Cisco Prime Network Registrar DHCP issues a DHCPv4 or DHCPv6 lease.
DHCPv4 and DHCPv6 failover	A simple failover model using TCP provides support for IP address, prefix, and variable-length prefix failover. This allows a backup DHCP server to take over for a main server if the main server is taken off the network for any reason.
Client reservations	Cisco Prime Network Registrar DHCP provides client reservations for IPv4 and IPv6 addresses as well as IPv6 prefix delegation. This capability allows the DHCP server to reserve a permanent IP address assignment. These reservations can be stored internal to Cisco Prime Network Registrar (through the Cisco Prime Network Registrar client entries) or external to Cisco Prime Network Registrar - either in Lightweight Directory Access Protocol (LDAP) or supplied through the DHCP server's extension interface from other external sources. This avoids the need to synchronize data with Cisco Prime Network Registrar's internal databases and provides for a much more dynamic and scalable reservation-based service.
Client class support	Cisco Prime Network Registrar DHCP can classify incoming client packets in three ways for greater flexibility: • Look up clients in a database (internal or external). • Apply a customer-defined algorithm or algorithms based on incoming packet content. • Call custom extensions or use third-party extensions written in C/C++ or Tool Command Language (Tcl). The client class can specify the options supplied to the client - which subnet or prefix to use for address allocation, which DNS server to update, and how to generate the host name, and more - as required for the various device types and service classes in the network. For example, device types could include cable modems, Customer Premises Equipment (CPE), and Media Terminal Adapters (MTAs) in a cable network, and service types could include the various classes of Internet service offered. In an enterprise, device types might be phones, printers, and desktop computers.
Extensions	Cisco Prime Network Registrar DHCP provides powerful extension support to allow for DHCP server processing customization. Extensions can be used to classify client types, add/remove/modify options in packets, query or update an external database, and much more. Extensions are flexible enough to be written in the service provider or enterprise development environment - they are written in either Tcl or C/C++ and support all operating platforms and all devices.

Feature	Benefit
Gracefully handles difficult client situations	The DHCP server will handle an avalanche of DHCP client requests by prioritizing and processing the most important requests using a patent-pending discriminating rate limiter. The DHCP server will not collapse under any load, no matter how extreme – it will rapidly work through any backlog and get the network back up as quickly as possible. Also, through the use of an extension, the Chatty Client Filter, the DHCP component handles misbehaving clients. For clients that do not have multiple packets outstanding but still frequently send requests to the DHCP server, the extension will automatically disable such clients and then, if their behavior improves, automatically re-enable them. In customer situations this has been shown to decrease packet traffic by more than 50 percent.
Bulk lease query support for DHCPv6	The DHCP server will respond to lease query requests for a large number of DHCPv6 leases using standards-compliant bulk lease query functionality.
Prefix stability for IPv6	Prefix stability allows a client to retain a delegated IPv6 address prefix when the client changes location – for example, during network maintenance, when an operator performs node splits, or during load-balancing events. • Cable Modem Termination System (CMTS) prefix stability supports the DOCSIS 3.0 requirements for prefix stability and allows a subscriber to retain his or her delegated prefix when an operator performs a load-balancing or reconfiguration event within a CMTS group. CMTS prefix stability must be deployed on a single DHCP server. • Universal prefix stability allows subscribers to retain a delegated prefix anywhere in the network. Use of this feature requires administrative assignment of the delegated prefixes and use of a client or lease reservation. It can be deployed across multiple DHCP servers.
Prefix allocation groups	Prefix allocation groups allow users to define multiple prefixes that do not result in multiple lease assignments to clients and to control the order in which the prefixes are used.
DNS Features	
Standards-compliant DNS Authoritative server	Cisco Prime Network Registrar DNS is a standards-compliant authoritative DNS server that offers an advanced feature set, with support for incremental zone transfers, dynamic updates, and notifications. To secure DNS services, the DNS component supports Transactional Signature (TSIG) to authenticate DNS zone transfer and update requests.
DNS caching server	The DNS caching server is optimized for its specific role, performing the actual recursion to resolve a given name, resulting in greater simplicity and better performance overall. The server improves speed/performance of high volume recursive queries, and operators can expect increased performance in end-user applications. The server stores DNS query results locally, which helps to improve efficiency and reduce DNS traffic across the Internet.
DNSSEC support	The Cisco Prime Network Registrar DNS caching server performs DNSSEC validation and authenticates DNS data as being published by zone administrators. This helps to ensure the authenticity and integrity of DNS records and servers being accessed. Specifically, DNSSEC validation provides assurance to end-user resolvers that DNS query responses are accurate for signed zones. The DNSSEC server validates signatures of each resource record ultimately to the root zone in accordance with standard DNSSEC protocol. DNSSEC also protects resource records against DNS vulnerabilities such as DNS cache poisoning.
DNS over TLS	The Cisco Prime Network Registrar DNS functionality supports encrypting and delivery of Domain Name System (DNS) queries and answers via the Transport Layer Security (TLS) protocol to increase user privacy and security by preventing eavesdropping and manipulation of DNS data via man-in-the-middle attacks.

Feature	Benefit
DNS64 functionality	The Cisco Prime Network Registrar DNS caching server 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.
DNS views support	Cisco Prime Network Registrar provides simplified implementation support for and management of DNS views. DNS views allow presentation of alternate resource record sets (different "views" of the same data) based on the source or destination of the query and whether the query is recursive or not. End users only have to remember a single URL rather than an internal versus external URL. Operators can realize operating expense savings through the ability to have a single primary DNS server for both internal and external view servers. 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 resolutions - for enhanced security for systems within a campus LAN.
DNS firewall	Uses RPZ to define lists of fully qualified domain names, IPs, subnets, and prefixes of end nodes for blocked and allowed listing. DNS administrators can optimize the user experience by helping users get to a predefined URL. The DNS server can be configured to modify response to queries to redirect clients away from known risky web sites. Administrators can block a domain or list of domains, redirecting the user to a notification page. The DNS firewall supports zone transfers from a third party RPZ provider.
NXDOMAIN redirect	Network operators can assist users when they query an invalid domain name (that is, the server has no entry) by returning an "NXDOMAIN" response, meaning nonexistent Internet or intranet domain name.
Internationalized domain name support	Supports the use of the full Unicode character set to name DNS domains from the Cisco Prime Network Registrar web UI. This allows administrators to use localized domain names in the web UI.
DNS E.164 Number Mapping (ENUM) configuration	ENUM allows telephone numbers to be resolved to URLs using a DNS-based architecture. Cisco Prime Network Registrar offers an easy way to input and manage ENUM records. By placing telephone numbers into the DNS server, ENUM can facilitate interoperability for a wide range of applications including VoIP, video, presence, and instant messaging.
External Systems Integration and Support	
Representational State Transfer (REST)/RESTful API	An industry standard web services REST API for lightweight, maintainable, and scalable web based services. Support includes get, add, modify, or delete operations, as allowed for each class. REST APIs are beneficial in supporting cloud-based implementations.
Integration with external systems	Users are able to streamline intersystem workflow using robust API/CLIs for communication between related asset inventory and network management systems.
Integration with Cisco Prime Cable Provisioning	Integration between Cisco PNR DHCP and Cisco PCP enabling zero touch provisioning of cable modems for DOCSIS environments.

Standards

DHCP RFCs supported:

RFC	Description
RFC 1350	THE TFTP PROTOCOL (REVISION 2)
RFC 1497	Vendor Extension Options
RFC 1531	Dynamic Host Configuration Protocol
RFC 1533	DHCP Options and BOOTP Vendor Extensions
RFC 1534	Interoperation Between DHCP and BOOTP
RFC 1541	Dynamic Host Configuration Protocol
RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DHCP Options and BOOTP Vendor Extensions
RFC 2241	DHCP Options for Novell Directory Services
RFC 2322	Management of IP numbers by peg-dhcp
RFC 2347	TFTP Option Extension
RFC 2348	TFTP Blocksize Option
RFC 2485	DHCP Option for The Open Group's User Authentication Protocol
RFC 2489	Procedure for Defining New DHCP Options
RFC 2563	DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients
RFC 2610	DHCP Options for Service Location Protocol
RFC 2855	DHCP for IEEE 1394
RFC 2937	The Name Service Search Option for DHCP
RFC 2939	Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types
RFC 3004	The User Class Option for DHCP
RFC 3011	The IPv4 Subnet Selection Option for DHCP
RFC 3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6 For Temporary addresses - Temporary addresses solve a privacy issue with IPv6 (see RFC 3041).
RFC 3046	DHCP Relay Agent Information Option
RFC 3074	Attributes for DHCP Related Failover Servers.

RFC	Description
RFC 3256	DOCSIS (Data-Over-Cable Service Interface Specifications) Device Class DHCP (Dynamic Host Configuration Protocol) Relay Agent Information Sub-option
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3319	DHCPv6 Options for SIP Servers
RFC 3361	Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers
RFC 3396	Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)
RFC 3397	Dynamic Host Configuration Protocol (DHCP) Domain Search Option
RFC 3442	The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4
RFC 3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
RFC 3495	Dynamic Host Configuration Protocol (DHCP) Option for Cable Labs Client Configuration
RFC 3527	Link Selection sub-option for the Relay Agent Information Option for DHCPv4
RFC 3594	Packet Cable Security Ticket Control Sub-Option for the DHCP Cable Labs Client Configuration (CCC) Option
RFC 3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC 3634	Key Distribution Center (KDC) Server Address Sub-option for the Dynamic Host Configuration Protocol (DHCP) Cable Labs Client Configuration (CCC) Option
RFC 3646	DNS Configuration options for DHCPv6
RFC 3679	Unused Dynamic Host Configuration Protocol (DHCP) Option Codes
RFC 3736	Stateless DHCP Service for IPv6
RFC 3825	Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information
RFC 3898	Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3925	Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)
RFC 3942	Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options
RFC 3993	Subscriber-ID Sub option for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option
RFC 4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Sub option for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option
RFC 4030	The Authentication Sub option for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option
RFC 4039	Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)

RFC	Description
RFC 4075	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
RFC 4076	Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 4174	The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service
RFC 4242	Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 4243	Vendor-Specific Information Sub option for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option
RFC 4280	Dynamic Host Configuration Protocol (DHCP) Options for Broadcast and Multicast Control Servers
RFC 4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 4388	DHCP Lease query specification
RFC 4390	Dynamic Host Configuration Protocol (DHCP) over InfiniBand
RFC 4477	DHCP IPv4 and IPv6 Dual-Stack Issues
RFC 4578	Dynamic Host Configuration Protocol (DHCP) Options for the Intel Preboot eXecution Environment (PXE)
RFC 4580	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option
RFC 4649	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option
RFC 4676	Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information
RFC 4701	A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)
RFC 4702	The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option
RFC 4703	Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients
RFC 4704	The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option
RFC 4776	Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information
RFC 4833	Time zone Options for DHCP
RFC 4994	DHCPv6 Relay Agent Echo Request Option
RFC 5007	DHCPv6 Lease query
RFC 5010	The Dynamic Host Configuration Protocol Version 4 (DHCPv4) Relay Agent Flags Sub option
RFC 5071	Dynamic Host Configuration Protocol Options Used by PXELINUX

RFC	Description
RFC 5107	DHCP Server Identifier Override Sub option
RFC 5192	DHCP Options for Protocol for Carrying Authentication for Network Access (PANA) Authentication Agents
RFC 5223	Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)
RFC 5417	Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option
RFC 5460	DHCPv6 Bulk Lease query
RFC 5859	TFTP Server Address Option for DHCPv4
RFC 5908	Network Time Protocol (NTP) Server Option for DHCPv6
RFC 5970	DHCPv6 Options for Network Boot
RFC 6148	DHCPv4 Lease Query by Relay Agent Remote ID **Note:** Supported only for Bulk
RFC 6153	DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery
RFC 6221	Lightweight DHCPv6 Relay Agent
RFC 6225	Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information **Note:** Must enter data in blob format
RFC 6276	DHCPv6 Prefix Delegation for Network Mobility (NEMO)
RFC 6334	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite
RFC 6355	Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)
RFC 6422	Relay-Supplied DHCP Options
RFC 6440	The EAP Re-authentication Protocol (ERP) Local Domain Name DHCPv6 Option
RFC 6603	Prefix Exclude Option for DHCPv6-based Prefix Delegation
RFC 6607	Virtual Subnet Selection Options for DHCPv4 and DHCPv6
RFC 6656	Description of Cisco Systems' Subnet Allocation Option for DHCPv4
RFC 6842	Client Identifier Option in DHCP Server Replies
RFC 6853	DHCPv6 Redundancy Deployment Considerations
RFC 6925	The DHCPv4 Relay Agent Identifier Sub-Option

RFC	Description
RFC 6926	DHCPv4 Bulk Lease query **Note:** Pre-RFC implementation
RFC 6939	Client Link-Layer Address Option for DHCPv6
RFC 7031	DHCPv6 Failover Requirements
RFC 7083	Modification to Default Values of SOL_MAX_RT and INF_MAX_RT
RFC 7291	DHCP Options for the Port Control Protocol (PCP) **Note:** Supported for DHCPv6. For DHCPv4 must be entered as blob data.
RFC 7550	Issues and Recommendations with Multiple Stateful DHCPv6 Options
RFC 7653	DHCPv6 Active Lease query **Note:** Pre-RFC implementation
RFC 7724	Active DHCPv4 Lease Query **Note:** Pre-RFC implementation
RFC 8156	DHCPv6 Failover Protocol **Note:** Pre-RFC implementation
RFC 8168	DHCPv6 Prefix-Length Hint Issue
RFC 8357	Generalized UDP Source Port for DHCP Relay
RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 8520	Manufacturer Usage Description Specification
RFC 8925	IPv6-Only Preferred Option for DHCPv4
RFC 8973	Distributed-Denial-of-Service Open Threat Signaling (DOTS) Agent Discovery

DNS RFCs supported:

RFC	Description
RFC 952	DOD INTERNET HOST TABLE SPECIFICATION
RFC 1034	DOMAIN NAMES - CONCEPTS AND FACILITIES
RFC 1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
RFC 1101	DNS Encoding of Network Names and Other Types
RFC 1536	Common DNS Implementation Errors and Suggested Fixes
RFC 1706	DNS NSAP Resource Records

RFC	Description
RFC 1982	Serial Number Arithmetic
RFC 1995	Incremental Zone Transfer in DNS
RFC 1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
RFC 2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC 2181	Clarifications to the DNS Specification
RFC 2308	Negative Caching of DNS Queries (DNS NCACHE)
RFC 2317	Classless IN-ADDR.ARPA delegation
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)
RFC 2845	Secret Key Transaction Authentication for DNS (TSIG)
RFC 3110	RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS
RFC 3226	DNSSEC and IPv6 A6 aware server/resolver message size requirements
RFC 3258	Distributing Authoritative Name Servers via Shared Unicast Addresses
RFC 3492	Punycode:A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
RFC 3493	Basic Socket Interface Extensions for IPv6
RFC 3596	DNS Extensions to Support IP Version6
RFC 3597	Handling of Unknown DNS Resource Record (RR) Types
RFC 3645	Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)
RFC 3833	Threat Analysis of the Domain Name System (DNS)
RFC 4033	DNS Security Introduction and Requirements
RFC 4034	Resource Records for the DNS Security Extensions
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 4074	Common Misbehavior Against DNS Queries for IPv6 Addresses
RFC 4159	Deprecation of " ip6.int"
RFC 4343	Domain Name System (DNS) Case Insensitivity Clarification
RFC 4367	What's in a Name: False Assumptions about DNS Names
RFC 4408	Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1
RFC 4592	The Role of Wildcards in the Domain Name System

RFC	Description
RFC 4641	DNSSEC Operational Practice
RFC 4701	A DNS Resource Record (RR) for Encoding DHCP Information
RFC 5011*	Automated Updates of DNS Security (DNSSEC) Trust Anchors
RFC 5452	Measures for Making DNS More Resilient against Forged Answers
RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
RFC 6116	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation
RFC 6147*	**DNS64:** DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers **Note:** Not compliant for section 5.1.4 and section 5.1.7 TTL calculation
RFC 6195	Domain Name System (DNS) IANA Considerations
RFC 6605*	Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
RFC 6672*	DNAME Redirection in the DNS
RFC 6840	Clarifications and Implementation Notes for DNS Security (DNSSEC)
RFC 6844	DNS Certification Authority Authorization (CAA) Resource Record
RFC 6891	Extension Mechanisms for DNS (EDNS(0))
RFC 7553	The Uniform Resource Identifier (URI) DNS Resource Record
RFC 7858	DNS over TLS
RFC 7871*	Client Subnet in DNS Queries
RFC 8020	NXDOMAIN: There Really Is Nothing Underneath
RFC 8145*	Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)
RFC 8198*	Aggressive Use of DNSSEC-Validated Cache
RFC 8375*	Special-Use Domain 'home.arpa.'
RFC 8467*	Padding Policies for Extension Mechanisms for DNS (EDNS(0))
RFC 8484*	DNS Queries over HTTPS (DoH)
RFC 8509*	A Root Key Trust Anchor Sentinel for DNSSEC
RFC 8624*	Algorithm Implementation Requirements and Usage Guidance for DNSSEC
RFC 8767*	Serving Stale Data to Improve DNS Resiliency
RFC 9156*	DNS Query Name Minimisation to Improve Privacy

RFCs marked with '*' are supported only on the DNS Caching server.

System Requirements

Cisco PNR 11 is a Linux application which runs on Intel-based servers. The required operating environment consists of:

- Linux OS (Red Hat Enterprise Linux, or equivalent)
- Bare metal Intel-architecture hardware -or- VMware ESXi -or- Docker Container

The software is tested within Cisco on Red Hat Enterprise Linux running on Cisco UCS Servers, as well as on VMware ESXi and Openstack. Cisco PNR uses Red Hat UBI for building the Docker Container form factor.

The Cisco PNR software is generally not sensitive to the RHEL and virtualization software levels used, so upgrades performed by the customer are not restricted. Customers are entitled to upgrade their OS and Hypervisor independently from any Cisco action, and are supported directly by their respective vendors if the customer has the proper licenses from those vendors. Note that RHEL 8.0 introduced some changes and so is only supported starting with PNR 11.0. Cisco PNR 11.0 was tested with RHEL 8.2. New PNR releases are tested with newer versions of RHEL and VM. Please refer to the PNR Release Notes and Installation Guide for a listing of the latest versions that were tested with the PNR release.

For minimum system requirements for running Cisco PNR, please refer to the Cisco Prime Network Registrar Installation Guide.

Licensing

PNR 11 uses Capacity-based metering for licensing.

- DHCP is licensed based on number of IP Leases to be supported.
- DNS is licensed based on number of Resource Records to be supported.
- Caching DNS is licensed per instance (e.g., per server, per VM, or per Container)

PNR licensing is offered in the following tiers, so that the customer can select the level of feature richness desire:

License Tiers	
Essentials Feature Set	Core features offered by the individual component
Advantage Feature Set	This refers to extended features for the product that are licensed as add-ons. These features provide additional capabilities and are purchased in addition to the Essential feature set (refer to the PID list for details).

Within each Tier, the customer must select the base license(s) for the components desired, and the Capacity meter licenses needed for each selected component.

License Meters	
Base License	RTU (Right to Use) license for the software component, entitling the minimal level capacity.
Capacity Licenses	This license extends the purchased capacity beyond the initial capacity provided with the base license.

Additional licenses may apply.

PNR 11 supports PAK-based licensing or Smart licensing. Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Ordering Information

To place an order, visit the Cisco® Ordering Homepage. See the Cisco Prime Network Registrar Ordering Guide for a list of Cisco Prime Network Registrar product numbers and upgrade product numbers as well as detailed licensing information. To download software, visit the Cisco Software Center.

Cisco Services

The Cisco technical support is limited to the Cisco PNR Application software. For support on other components, such as, but not limited to, Linux, Hypervisor, non-Cisco hardware, the customer must obtain entitlement and support licenses from the respective vendors.

Cisco offers a wide range of services programs to accelerate customer success. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Customer Experience.

Cisco Capital

Financing to Help You Achieve Business Outcomes

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information about 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.

Document history

New or revised topic	Described in	Date
Added updates covering PNR 11.2 release	PNR 11.2 product documentation	January 08, 2024

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 **https://www.cisco.com/go/offices**.

Printed in USA C78-729989-04 01/24