



## Deploying Network Registrar

---

Cisco CNS Network Registrar is a full featured, scalable Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Trivial File Transfer Protocol (TFTP) implementation for medium to large IP networks. It provides the key benefits of stabilizing the IP infrastructure and automating networking services, such as configuring clients and provisioning cable modems. This provides a foundation for policy-based networking. Service provider and enterprise users can better manage their networks to integrate with other network infrastructure software and business applications.

### Target Users

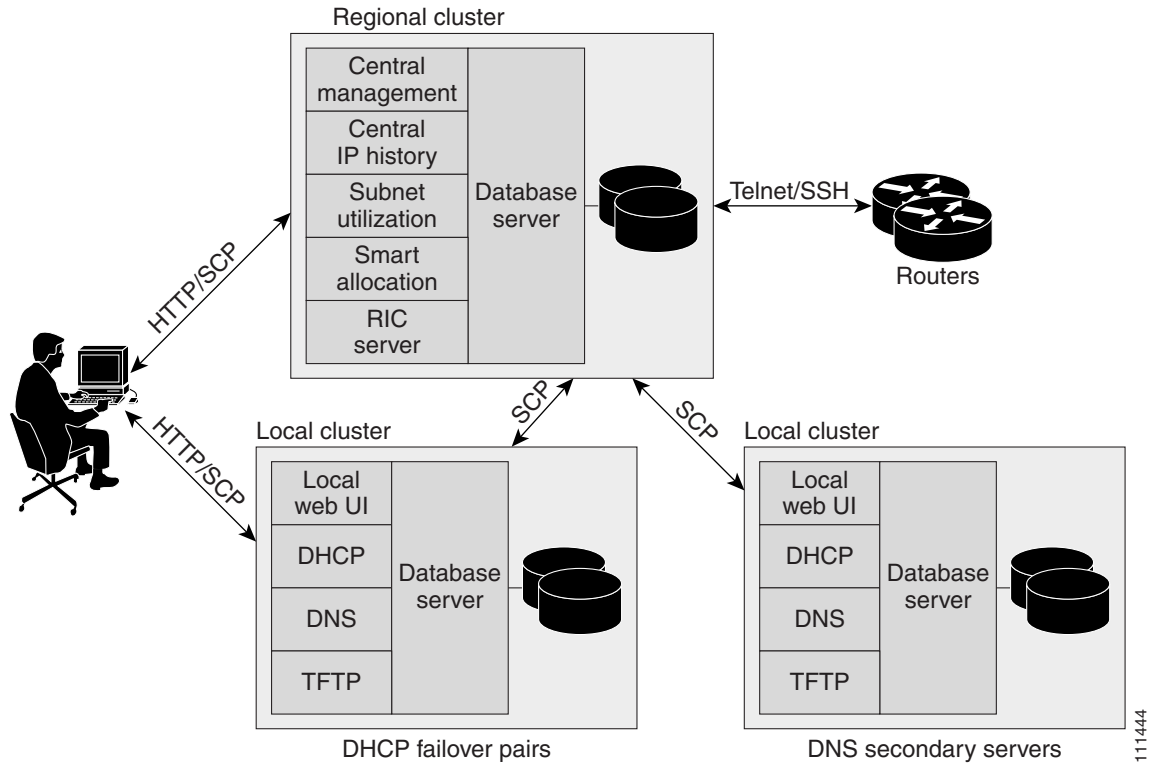
Network Registrar is designed for these users:

- Internet service providers (ISPs)—Helps ISPs drive the cost of operating networks that provide leased line, dialup, and DSL (Point-to-Point over Ethernet and DHCP) access to customers.
- Multiple service operators (MSOs)—Helps MSOs provide subscribers with Internet access using cable or wireless technologies. MSOs can benefit from services and tools providing reliable and manageable DHCP and DNS services that meet the Data Over Cable Service Interface Specification (DOCSIS). Network Registrar provides policy-based, robust, and scalable DNS and DHCP services that form the basis for a complete cable modem provisioning system.
- Enterprises—Helps meet the needs of single- and multisite enterprises (small-to-large businesses) to administer and control network functions. Network Registrar automates the tasks of assigning IP addresses and configuring the Transport Control Protocol/Internet Protocol (TCP/IP) software for individual network devices. Forward-looking enterprise users can benefit from class-of-service and other features that help integrate with new or existing network management applications, such as user registration.

### Regional and Local Clusters

Network Registrar 6.2 extends the work of building on the local address server and address management architecture of earlier releases by providing additional features at the regional cluster (see [Figure 3-1 on page 3-2](#)). This regional cluster acts as an aggregate management system for up to a hundred local clusters. Address and server administrators interact at the regional and local clusters through the regional and local Web-based user interfaces (Web UIs), and local cluster administrators can continue to use the command line interface (CLI) at the local cluster. The regional cluster consists of a Central Configuration Management (CCM) server, Router Interface Configuration (RIC) server, Tomcat web server, servlet engine, and server agent.

Figure 3-1 Network Registrar User Interfaces and Server Clusters



A typical deployment is one regional cluster at a customer's network operation center (NOC), the central point of network operations for an organization. Each division of the organization includes a local address management server cluster responsible for managing a part of the network. The System Configuration Protocol (SCP) communicates the configuration changes between the servers.

The regional cluster can also manage a RIC server responsible for end point cable modem termination systems (CMTSs). (See [Chapter 10, "Managing Router Interface Configurations."](#))

## Deployment Scenarios

The Network Registrar regional cluster Web UI provides a single point to manage any number of local clusters hosting DNS, DHCP, or TFTP servers. The regional and local clusters also provide administrator management so that you can assign administrative roles to users logged on to the application.

This section describes two basic administrative scenarios and the hardware and software deployments for two different types of installations—a small-to-medium local area network (LAN), and a large-enterprise or service-provider network with three geographic locations.

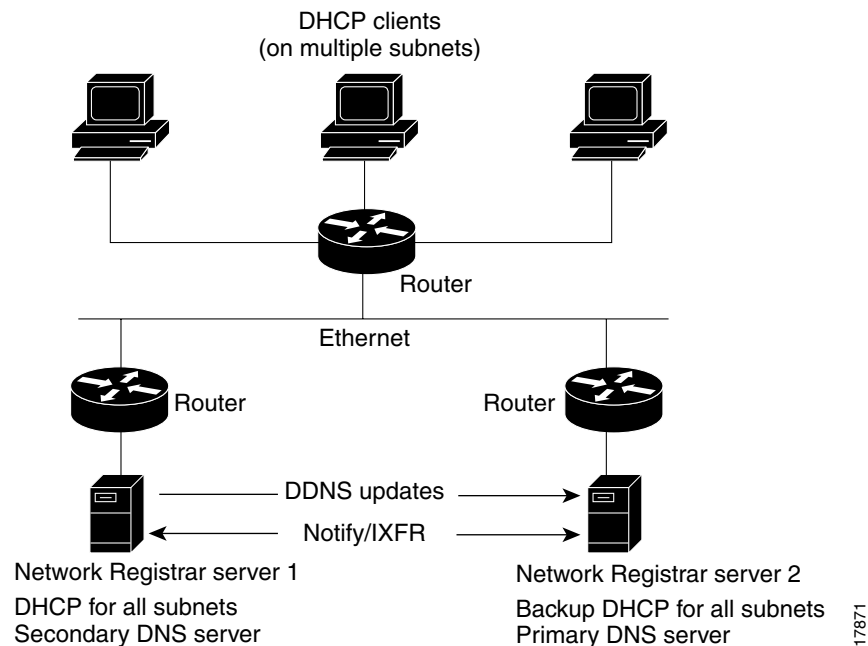
## Small-to-Medium-Size LANs

In a small-to-medium LAN serving fewer than 50,000 DHCP clients, you can deploy Network Registrar without a regional cluster component. In this scenario, low-end Windows, Solaris, or Linux servers are acceptable. You can also use systems with EIDE disk, although Cisco recommends Ultra-SCSI disks for dynamic DNS update. [Figure 3-2](#) shows a configuration that would be adequate for this network. Recommendations include:

Recommendations include:

- Windows—Single-processor Pentium III, Windows 2003, 512 MB of RAM, 18-GB disk.
- Solaris—Sunfire v120, Solaris 8 or 9, 512 MB of RAM, 18-GB disk.
- Linux—Pentium III, Red Hat Linux 7.3 (kernel version 2.4) or Red Hat Linux Enterprise ES or WS 2.1 (kernel 2.4.9-e.24), with RPM Package Manager (RPM) 4.0.4 or later, 512 MB of RAM, 18-GB disk.

**Figure 3-2 Small-to-Medium LAN Configuration**



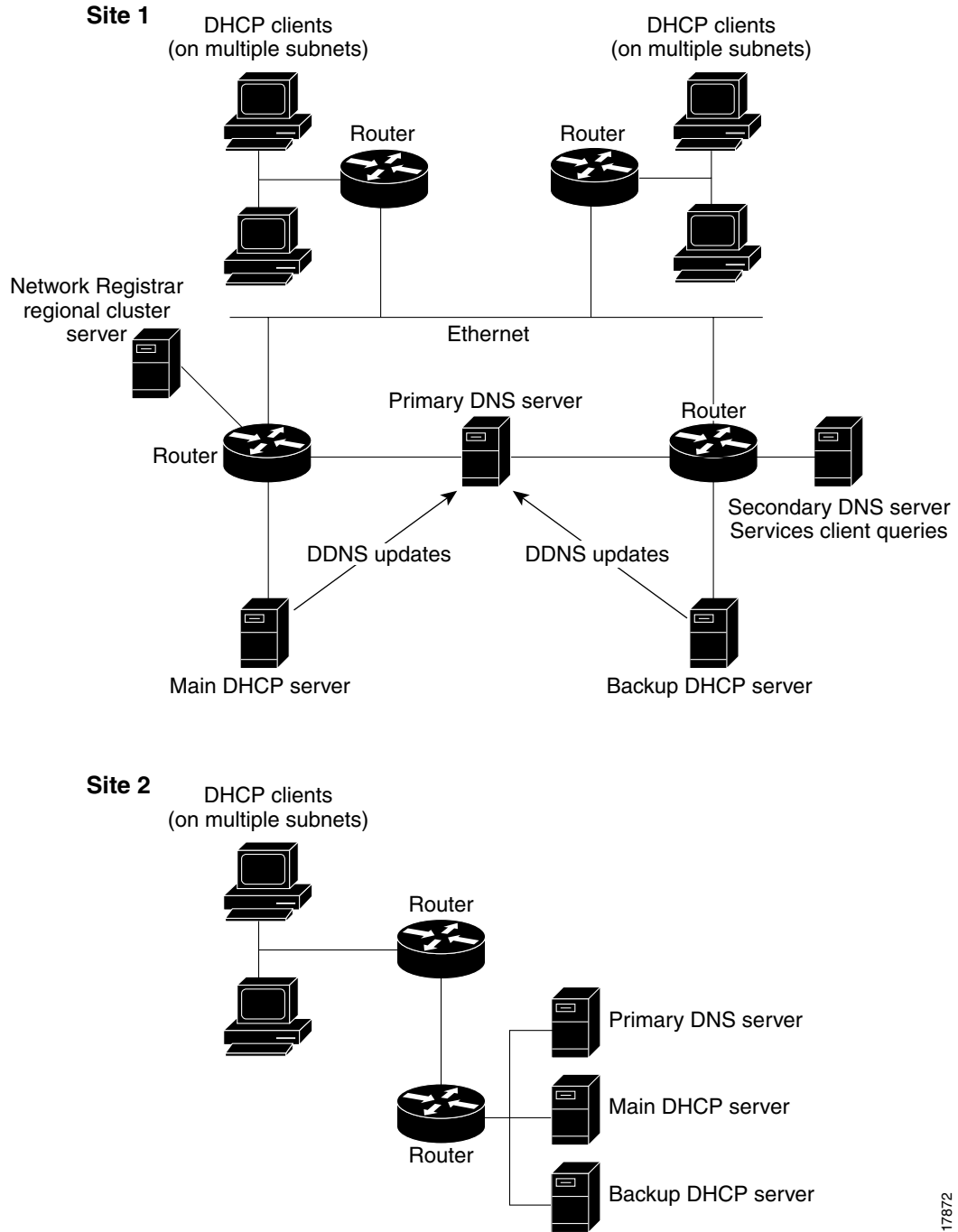
## Large Enterprise and Service Provider Networks

In a large enterprise or service provider network serving over 500,000 DHCP clients, use mid-range Sun, Windows, or Linux servers. Put DNS and DHCP servers on different systems. [Figure 3-3 on page 3-4](#) shows the hardware that would be adequate for this network. Recommendations include:

- Windows—Dual-processor Pentium III plus, Windows 2003 Server, 2 GB of RAM, 36-GB disk (10,000 RPM).
- Solaris—Dual-processor Sunfire v240, Solaris 8 or 9, 2 GB of RAM, 36-GB disk (10,000 RPM).
- Linux—Dual-processor Pentium III plus, Red Hat Linux 7.3 (kernel version 2.4) or Red Hat Linux Enterprise ES or WS 2.1 (kernel 2.4.9-e.24), with RPM Package Manager (RPM) 4.0.4 or later, 2 GB of RAM, 36-GB disk.

When supporting geographically dispersed clients, locate DHCP servers at remote locations to avoid disrupting local services if wide-area connections fail. Install the Network Registrar regional cluster to centrally manage the distributed clusters.

**Figure 3-3 Large Enterprise or Service Provider Network Configuration**



17872

# Configuration and Performance Guidelines

Network Registrar is an integrated DHCP, DNS, and TFTP server cluster capable of running on a Windows 2003, Solaris, or Linux workstation or server.

Because of the wide range of network topologies for which you can deploy Network Registrar, you should first consider the following guidelines. These guidelines are very general and cover most cases. Specific or challenging implementations could require additional hardware or servers.

## General Configuration Guidelines

The following suggestions apply to most Network Registrar deployments:

- Configure a separate DHCP server to run in remote segments of the wide area network (WAN)—Ensure that the DHCP client can consistently send a packet to the server in under a second. The DHCP protocol dictates that the client receive a response to a DHCPDISCOVER or DHCPREQUEST packet within four seconds of transmission. Many clients (notably early releases of the Microsoft DHCP stack) actually implement a two-second timeout.
- In large deployments, separate the secondary DHCP server from the primary DNS server used for dynamic DNS updates—Because lease requests and dynamic DNS updates are persisted to disk, server performance is impacted when using a common disk system. So that the DNS server is not adversely affected, run it on a different cluster than the DHCP server.
- Include a time server in your configuration to deal with time differences between the local and regional clusters so that aggregated data at the regional server appears in a consistent way. See the [“Polling Subnet Utilization and Lease History Data”](#) section on page 5-8.
- Set DHCP lease times in policies to four to ten days—To prevent leases from expiring when the DHCP client is turned off (overnight or over long weekends), set the DHCP lease time longer than the longest period of expected downtime, such as seven days. See [Chapter 21, “Managing Leases.”](#)
- Locate backup DNS servers on separate network segments—DNS servers are redundant by nature. However, to minimize client impact during a network failure, ensure that primary and secondary DNS servers are on separate network segments.
- If there are high dynamic DNS update rates in the network, configure separate DNS servers for forward and reverse zones.
- Use NOTIFY/IXFR—Secondary DNS servers can receive their data from the primary DNS server in two ways: through a full zone transfer (AXFR) or an incremental zone transfer (NOTIFY/IXFR, as described in RFCs 1995 and 1996). Use NOTIFY/IXFR in environments where the namespace is relatively dynamic. This reduces the number of records transferred from the primary to the secondary server. See the [“Enabling Incremental Zone Transfers \(IXFR\)”](#) section on page 16-7.

## Special Configuration Cases

The following suggestions apply to some special configurations:

- When using dynamic DNS updates for large deployments or very dynamic networks, divide primary and secondary DNS and DHCP servers across multiple clusters—Dynamic DNS updates generate an additional load on all Network Registrar servers as new DHCP lease requests trigger dynamic DNS updates to primary servers that update secondary servers through zone transfers.
- During network reconfiguration, set DHCP lease renewal times to a small value—Do this several days before making changes in network infrastructure (such as to gateway router and DNS server addresses). A renewal time of eight hours ensures that all DHCP clients receive a changed DHCP option parameter within one working day. See [Chapter 21, “Managing Leases.”](#)

## Interoperability with Earlier Releases

[Table 3-1](#) shows the interoperability of Network Registrar features on the regional CCM server with versions of the local cluster.

**Table 3-1 CCM Regional Feature Interoperability with Server Versions**

Feature	Local Cluster Version			
	6.0	6.1	6.1.1	6.2
Central push and pull:				
Address space	x	x	x	x
Scope templates, policies, client-classes	x	x	x	x
Zone data and templates	x	x	x	x
Groups, owners, regions	x	x	x	x
Resource records (RRs)	x	x	x	x
Local cluster restoration	x	x	x	x
Host administration	x	x	x	x
Extended host administration				x
Administrators and roles			x	x
Administrator:				
Single sign-on		x	x	x
Password change			x	x
IP history reporting:				
Central lease history		x	x	x
Detail lease history			x	x
Utilization reporting:				
Central subnet utilization history		x	x	x
Current subnet and scope utilization			x	x