White Paper

Cisco Prime IP Express: DDI

Deploying a Scalable, Resilient, High-Performance DDI Solution

Overview

With the bring-your-own-device (BYOD) trend, enterprises are seeing an explosion of connected devices in the workplace - smartphones, tablets, video cameras, card readers, and much more. And the Internet of Things (IoT), a rising tide of billions of new connected devices that will come online over the next several years, is also bringing an onslaught of wireless devices and services to enterprise networks.

At the same time, the growing trend toward virtualization exponentially increases the complexity of the network, adding more network management points, more systems to be managed, and many more IP addresses consumed per physical machine.

All of those physical and virtual devices need fast, reliable connectivity to the enterprise network. And all of them depend on basic Domain Name System (DNS), Dynamic Host Control Protocol (DHCP), and IP address management (IPAM) services to provide that connectivity. But is your current DNS, DHCP, and IPAM (DDI) framework ready to deliver it? Ask yourself the following questions:

- Can you easily scale DDI services across all of your sites and manage them centrally and automatically? Or are you relying on a patchwork of basic “freeware” solutions and spreadsheets that have to be managed manually at each site?
- Do you have a rock-solid, highly available framework for the core DDI services that are the bedrock of your business connectivity? Or are you vulnerable to an outage or DNS attack in one segment of the network cutting off hundreds or thousands of employees from critical business applications?
- Are your DDI platform and processes ready to transition to IPv6 when the coming wave of new IoT and network connections makes it a basic business requirement? Or will you have to overhaul your systems?

Despite the reality that DDI is the foundation of your business’s Internet and network connectivity, many enterprises still rely on aging, localized, and largely manual DDI tools. These systems are barely equipped to keep pace with today’s higher network traffic volumes and the growing number of connected devices - much less meet the connectivity needs of tomorrow. Fortunately, there’s a better solution: Cisco Prime™ IP Express.

Cisco Prime IP Express

Cisco Prime IP Express provides a highly reliable, scalable, and centrally managed DDI solution for enterprise networks. Based on the same Cisco Prime Network Registrar DNS and DHCP technology used in many of the world’s largest service provider networks, it brings industrial-strength performance and security, massive scalability, and high availability to your enterprise DDI services.

Cisco Prime IP Express includes the following high-performance components and their respective services, all of which are standards compliant, and all of which support both IPv4 and IPv6:

- **High-capacity DHCP** to efficiently connect and manage all of the devices operating in the modern enterprise and fully integrate with Microsoft Active Directory (AD) authentication systems
- **Comprehensive DNS** services for centralized IP address translation and service delivery
- **Advanced DNS caching server** that provides high-performance forwarding and DNS recursion, as well as DNS Security Extensions (DNSSEC) to prevent cache poisoning and other DNS attacks
- **A powerful, comprehensive IPAM system** that integrates DNS and DHCP configuration and automates and simplifies management of the entire dual-stack IP address space
- **Captive BYOD portal,** included with DHCP or DNS suites, that simplifies, accelerates, and tightly controls the onboarding of employee devices

Cisco Prime IP Express supports external authentication using Active Directory, so you can continue to use AD as the single source for authentication and enforcement of network controls and security policies. You can migrate to Cisco Prime IP Express with confidence, improving the scalability, resiliency, and manageability of your DDI services without worrying about potential access or security errors, or negatively affecting your existing procedures or operating costs.

A Modular, Flexible DDI Solution That Grows with Your Business

With Cisco Prime IP Express, you can deploy these high-performance DDI solutions individually or as part of a preintegrated DNS or DHCP suite. And, because they are modular and standards-compliant, you can deploy any or all of them over time, centralizing the specific DDI functions you need as it makes sense for your business.

For example, you can start with a centralized DHCP solution that fully integrates with your existing Microsoft or other third-party DNS systems that operate at the local level. Or, you could deploy the Cisco® IPAM solution to centrally manage the IP address space for your entire business, even as you continue to use third-party and localized DNS and DHCP systems.

This flexibility is especially important for enterprises looking at transitioning to IPv6 down the road. Even if your current DNS/DHCP systems function well enough at present, you may not be able to rely on them when you migrate, as they likely do not provide IPv6 failover capabilities. Instead, you can implement a phased plan to centralize your DNS, DHCP, and IPAM services with Cisco dual-stack, standards-compliant DDI solutions over the coming months and years. So when you do begin using IPv6, you can make the transition easily, with no disruption to your processes or operations, and without compromising the performance or availability of your network.

The same holds true for enterprises transitioning to virtualized environments. Cisco Prime IP Express provides extensive support for virtual machines (VMs) and virtualized network functions (VNFs), including automating the provisioning and administration of associated IP addresses. This simplifies your transition to a virtualized environment, whether you're doing it now or plan to in the future. In addition, all elements of Cisco Prime IP Express can be deployed virtually, so you can add Cisco performance and manageability to your DDI operations right away, and take advantage of the scalability and resiliency of virtualization whenever you're ready.

Deploying Cisco Prime IP Express for Optimal Scalability and Resiliency

Your employees may not spend much time thinking about DHCP, DNS, and IP addresses. But without scalable, always-available DDI services, there is no network connectivity and no Internet.

What does a state-of-the-art, highly available enterprise DDI platform look like? And how can you deploy Cisco Prime IP Express to achieve optimal performance and manageability for your business? The following sections provide a closer look.

Cisco Prime IP Express Architecture

For larger and more complex networks (typically with more than 5000 IP addresses), building the Cisco Prime IP Express DDI architecture begins by deploying the management layer of the full DDI solution, the Cisco Prime Network Registrar IPAM server. The IPAM server is the central database for configuration of IP blocks, subnets, IP addresses, and DNS zones and records. It provides:

- Centralized planning and management of the complete address space down to the individual IP address level
- Centralized DNS and DHCP configuration management
- IPv4 and IPv6 support
- Automated address utilization collection and reporting
- Address utilization forecasting and trending analysis
- APIs and command-line interfaces (CLIs) for integration with any type of system (for example, workflow systems, provisioning systems, change management systems, or network management systems)

Unlike other tools that maintain IP name and address data as discrete information maintained uniquely and separately, Cisco Prime Network Registrar IPAM interacts with network devices and services to:

- Verify that the actual network matches the information in Cisco Prime Network Registrar IPAM
- Capture and record utilization information to be able to establish historical trends
- Reclaim inactive addresses

In a full DDI solution, the Cisco Prime Network Registrar IPAM is installed separately from the DHCP and DNS components. By separating IPAM and DNS/DHCP services components, the solution provides flexibility and modularity that allow enterprises to deploy just the specific DDI elements they require for their business at that time. Additional elements can easily be added later.

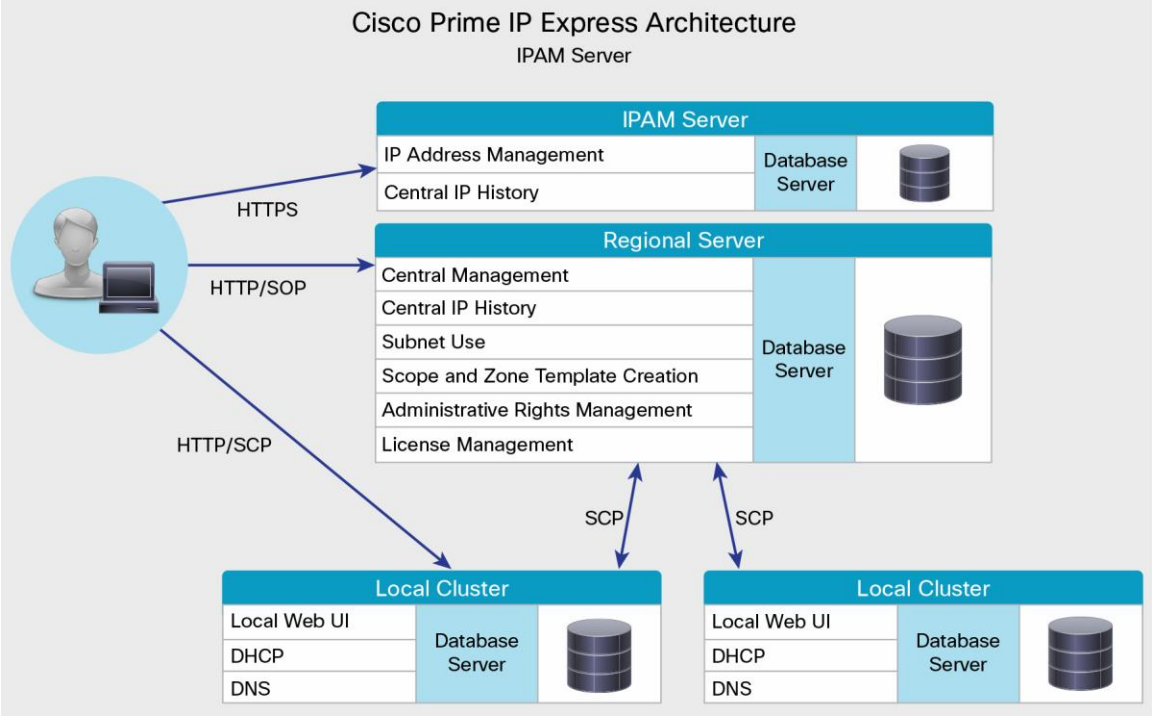
For example, what if you have a smaller or less complex network and don’t need IPAM right now? What if you want to use Cisco DNS and DHCP solutions to control your IP address services more efficiently (implementing just a “DD” solution rather than “DDI”), while you continue to manage the address space with spreadsheets or another tool? With Cisco Prime IP Express, you have the flexibility to do this.

In a network that does not include the Cisco IPAM component, a regional server is the central point of control for DNS and DHCP services. It provides:

- **Cluster connectivity** with a single sign-on (SSO) for a central administrator to manage all local clusters
- **Configuration of common DHCP and DNS objects**[1] such as:
  - Administrators, groups, and tenants
  - DHCP policies, client classes, DNS zones, and failover pairs
  - Scope templates and prefix templates
- **DHCP and DNS server license management** (for multiple sites across the company) from a single interface

In either type of deployment - with or without IPAM - the regional server communicates with local clusters that are deployed in your network to deliver DNS and DHCP services. Figure 1 shows an overview of the basic Cisco Prime IP Express architecture for a full DDI implementation.

Figure 1. Cisco Prime IP Express Architecture with IPAM

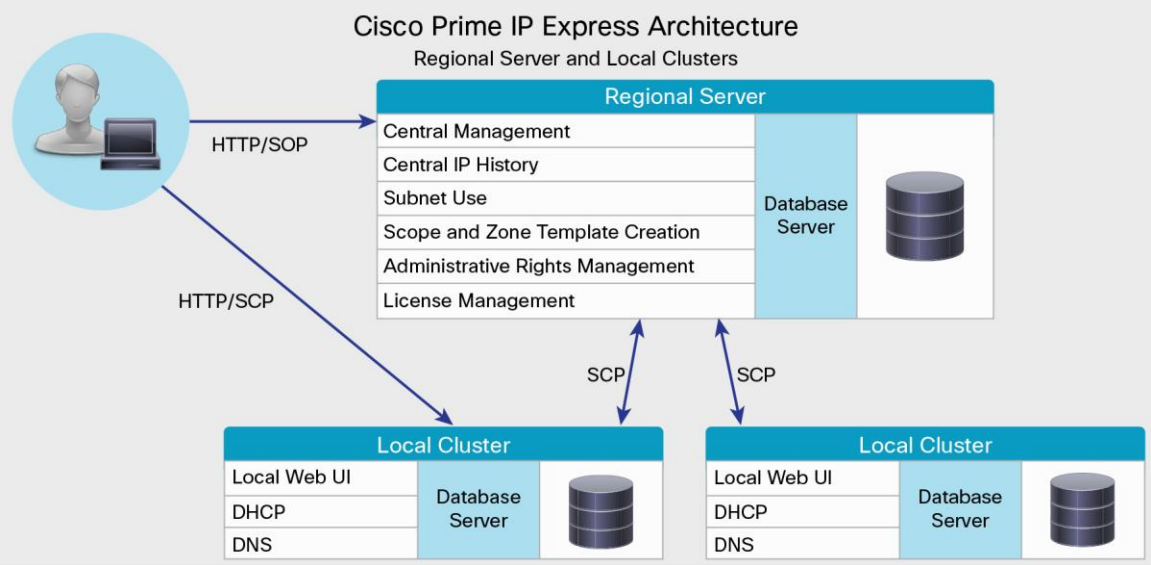


Here, you can see servers for DHCP, DNS, Caching DNS (CDNS), and IPAM. All of these servers - both in the regional server and local clusters - can be controlled centrally through a single interface, using either the solution's intuitive web-based GUI or CLI.

[1] Note: In a full Cisco Prime IP Express DDI solution, these functions are performed in the IPAM server.

Figure 2 illustrates the same basic architecture in a DD-only deployment.

Figure 2. Cisco Prime IP Express Architecture without IPAM



The regional server in a DD solution, or the IPAM in a DDI solution, centrally manages the local cluster servers, providing an aggregated view of DHCP address spaces and DNS zones. From this regional server or IPAM a central administrator can:

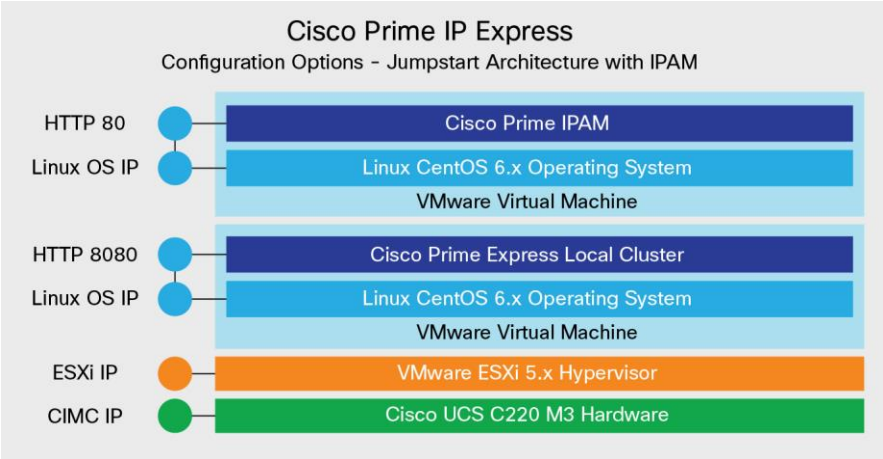
- Manage the distributed address space, zones, scopes, and DHCPv6 prefixes and links
- Manage users
- Manage licenses
- Push and pull DHCP and DNS configuration objects from the local clusters
- Obtain subnet utilization and IP lease history data from local clusters

Cisco Prime IP Express Logical Architecture and Configuration

The heart of Cisco Prime IP Express scalability and resiliency is its modular architecture, in which individual DDI solutions can be deployed and scaled independently and run in a virtualized environment. This modularity allows you to use DHCP failover and DNS high-availability capabilities to deploy highly reliable, rock-solid DDI services - even in large, high-growth networks.

Figure 3 shows an overview of the logical architecture of a Cisco Prime IP Express server deployment using the Cisco Jumpstart appliance - a preintegrated Cisco Prime IP Express server solution. However, you can deploy the solution's components on any standards-based x86 platform. This figure highlights a deployment using DHCP, DNS, and IPAM solutions, but the same basic architecture and resiliency principles apply to deployments with just one or two of these elements.

Figure 3. Cisco Prime IP Express Jumpstart Architecture with IPAM



The three layers of this logical architecture - hardware, hypervisor, and virtual machines running DHCP/DNS and IPAM - can be controlled independently and remotely, with each maintaining its own independent connection to the network. In this way, you can scale each element as needed and retain total flexibility in assuring availability of any or all components.

Cisco Prime IP Express Scalability and High-Availability Deployment in Action

Using the previous Cisco Jumpstart example as a model, the following sections walk through the ways an enterprise can deploy Cisco Prime IP Express across two sites, adding individual elements one by one to provide a full suite of DDI solutions.

These illustrations are based on Cisco and industry best practices for deploying critical DDI services in high-growth enterprise networks, to achieve optimal performance and availability. Each service instance shown here is deployed as a VM running on a Cisco Unified Computing System™ (Cisco UCS®) C220 M3 server.

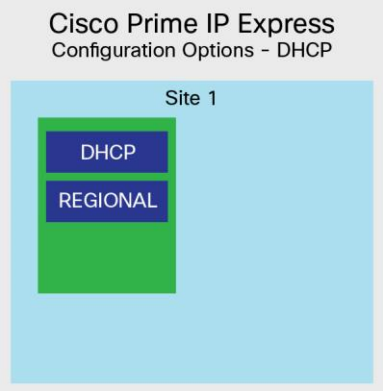
A single Cisco Prime IP Express installation can be installed with both a local cluster and a regional server. In local mode, the local cluster can provide DHCP and DNS services based on the licensing option, with local management features to administer the cluster.

For large deployments, best practice is to deploy only one service - either DHCP or DNS - on a single local cluster server. For smaller deployments, however (less than 20,000 DHCP leases), a regional server and local cluster can be deployed on the same physical server without diminishing performance.

Deploying DHCP

Figure 4 shows one possible first step in a Cisco Prime IP Express deployment, deploying a DHCP server at one site.

Figure 4. DHCP Configuration



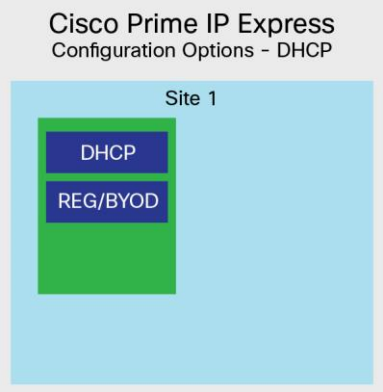
Note that while a regional server is required in the solution to manage licensing, the regional server does not participate in DHCP or DNS processes. If the regional server in this illustration fails, for example, you can install a new regional server, which can derive its configuration from the connected local clusters. However, best practices also dictate backing up the regional server regularly, using the included backup utility.

Adding BYOD

The Cisco Prime IP Express solution illustrated in this example includes a captive BYOD portal at no additional charge. The solution automates the onboarding of employee devices to the network and is fully integrated with the DDI solution.

Figure 5 shows the installation of the BYOD portal on the regional server at Site 1.

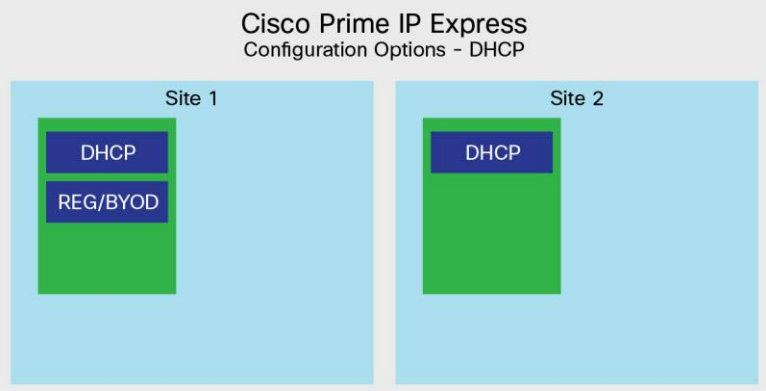
Figure 5. DHCP with BYOD



Adding a Second Site for Resiliency

In Figure 6, the enterprise has deployed the failover DHCP server at a second site (Site 2) to provide a highly resilient DHCP solution. This allows administrators to build scope templates, policies, and failover pair configurations once and deploy them on the regional server where they can be distributed to each connected DHCP instance, instead of having to build those configurations separately for each server.

Figure 6. DHCP Server Pair

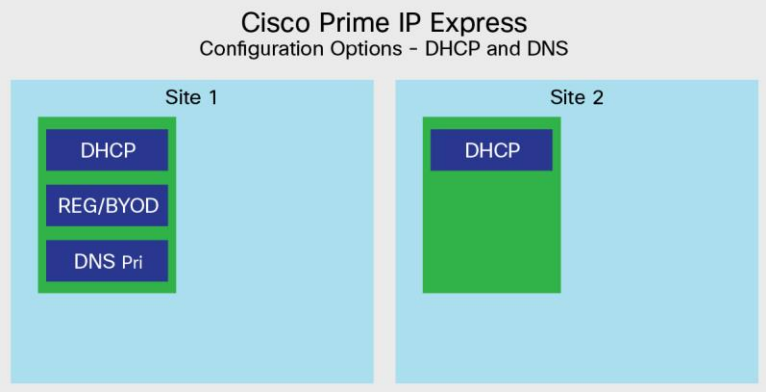


Each DHCP appliance or failover pair can handle up to 750,000 configured IP leases and up to 500,000 active IP leases. The DHCP failover pair communicates across the network through Transmission Control Protocol (TCP) and supports DHCP failover for both IPv4 and IPv6 address spaces.

Adding DNS

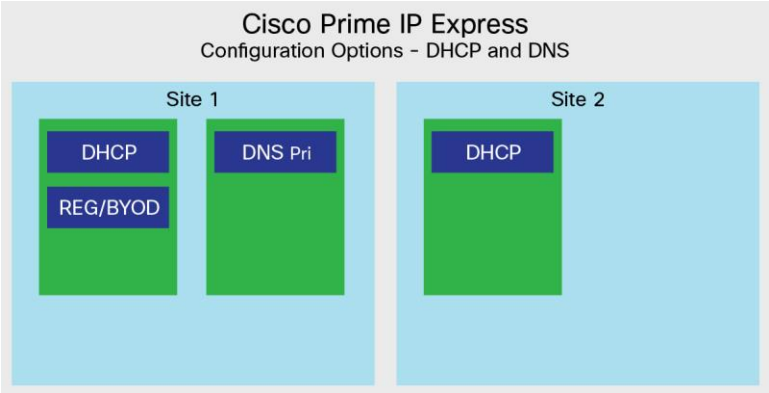
Figures 7 and 8 show the enterprise now adding DNS to the solution. In small networks (up to approximately 10,000 configured DHCP leases), DNS and DHCP can be deployed in the same appliance (Figure 7).

Figure 7. DHCP with DNS on One Server



For larger networks, best practice is to deploy DNS and DHCP on separate appliances to assure optimal performance and scalability (Figure 8).

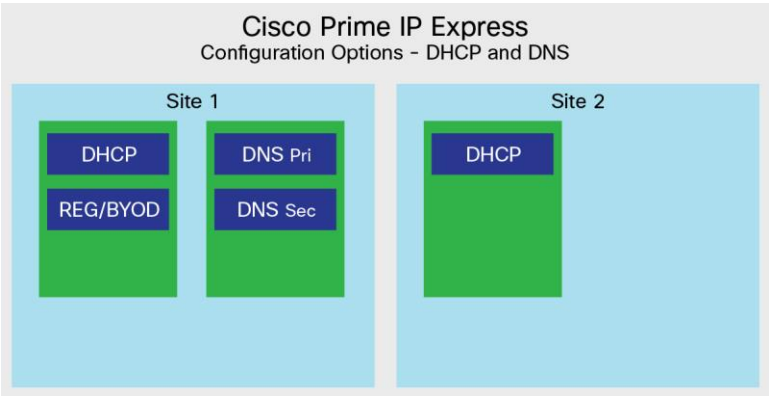
Figure 8. DHCP and DNS on Separate Servers



Best practices for scalability and security also dictate separating DNS servers into primary and secondary instances. The DNS primary server is the authoritative DNS server, where all zones and records are maintained. The DNS primary server then distributes that information through updates to DNS secondary servers. These secondary servers are the published name servers and accessible to users. In this way, authoritative DNS records are protected from DNS attacks. Even if an intruder can access and compromise the secondary DNS server, the authoritative data is never exposed.

Figure 9 shows the solution with both primary and secondary DNS servers. As illustrated here, both DNS primary and secondary servers can be installed within the same physical appliance.

Figure 9. Primary and Secondary DNS Servers

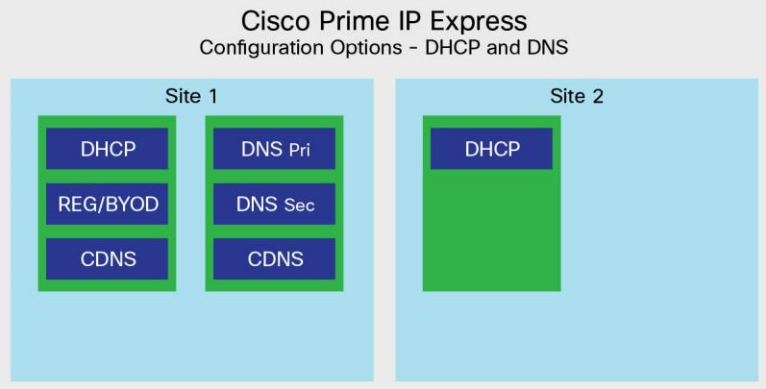


By installing the DNS primary server in a separate VM, it is “hidden” from users, with the only cost for this additional security being VM resources.

Adding Caching DNS Servers

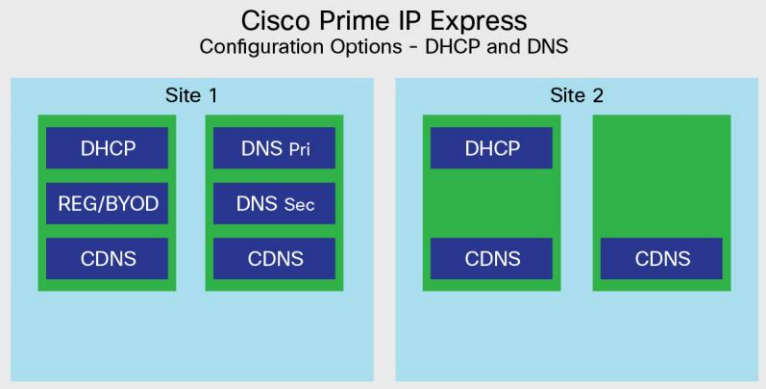
Within Cisco Prime IP Express, the Caching DNS server provides DNS forwarding and recursion functions (Figure 10). CDNS servers contain no authoritative DNS records, only cached results from both recursive and exception queries. Often, enterprises opt for secondary or tertiary DNS resolution in order to reduce the number of onsite CDNS servers. When deployed along with the captive BYOD portal, the CDNS servers are also used to forward designated subnets to the BYOD server for authentication.

Figure 10. Caching DNS Servers



To achieve optimal resiliency of DNS forwarding and recursion functions, best practice is to deploy two CDNS servers per site in separate appliances, as illustrated in Figure 10. For optimal performance, enterprises should install CDNS servers at each location (Figure 11), once again, deploying two separate CDNS servers per site.

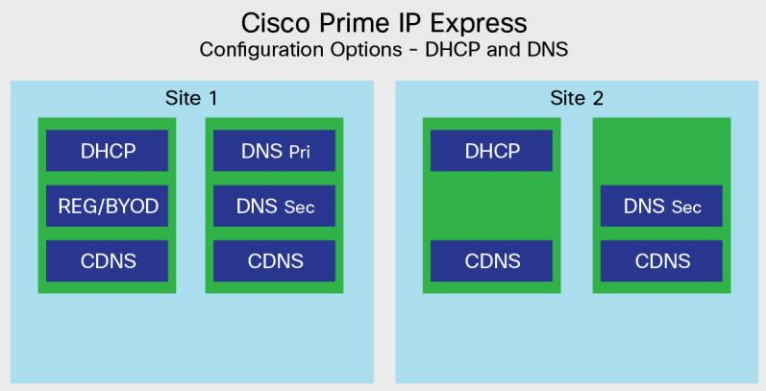
Figure 11. CDNS Servers at Multiple Sites



Adding Local DNS Services at Remote Sites

To optimize performance in growing networks, enterprises can deploy DNS servers at local sites. Figure 12 shows the deployment of a DNS secondary server at Site 2.

Figure 12. Secondary DNS Server at a Remote Site

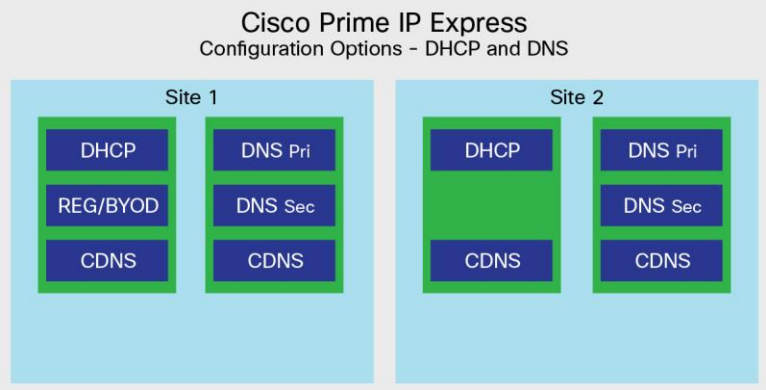


In this deployment the DNS secondary server at Site 2 is an authoritative server. It receives zone updates from the DNS primary server at Site 1 (resulting from both manual changes and dynamic DNS updates from DHCP servers), and assures that authoritative DNS records are locally available at all sites.

DNS High Availability

In addition to deploying an authoritative DNS secondary server at remote sites, enterprises can also deploy a mirrored DNS primary server at secondary sites to achieve optimal resiliency (Figure 13).

Figure 13. Mirroring DNS Primary Server at Secondary Sites

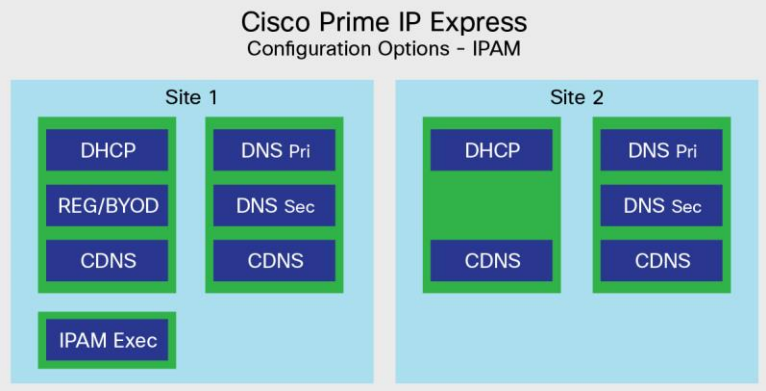


In Dynamic DNS (DDNS) environments, DHCP servers can only update a primary DNS server. By adding a DNS primary server to a second site, enterprises can assure that DHCP servers can always dynamically assign new DNS addresses - even if the connection to the DNS primary server at the central site is unavailable.

Deploying IPAM

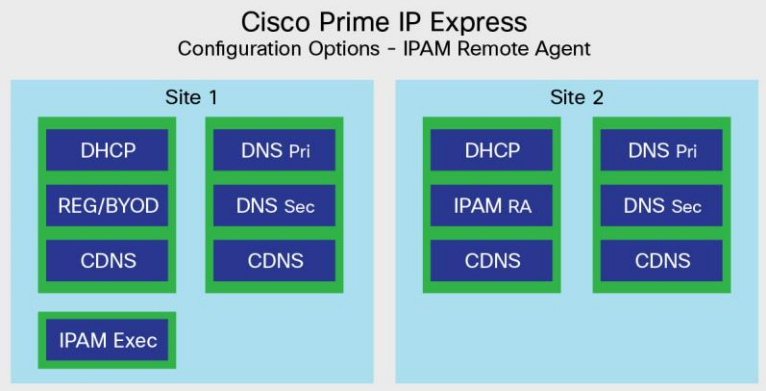
Figure 14 shows the final piece in deploying a comprehensive, highly scalable, and resilient DDI solution for larger and more complex networks: deploying IPAM. (As discussed, enterprises can deploy Cisco Prime IP Express DNS and DHCP services without IPAM, or even deploy an IPAM-only solution.)

Figure 14. Deploying IPAM



The Cisco Prime Network Registrar IPAM solution can be deployed in both an “executive” instance at a central site and as a distributed “remote agent” at each remote location (Figure 15).

Figure 15. IPAM with Distributed Remote Agent (IPAM RA)

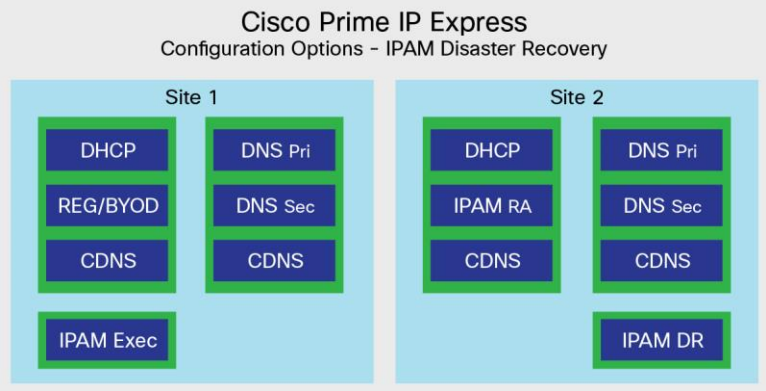


The executive instance provides the interface for administrators to configure and execute IPAM tasks. The remote agent executes IPAM tasks delegated by the executive instance and returns results. For example the remote agent will respond with data such as DHCP utilization, or the results of a configuration update on a remote DHCP or DNS server.

As illustrated, best practice for performance and scalability is to deploy the IPAM executive instance on a separate physical server. At distributed sites, IPAM remote agent instances can be deployed on the same server as other Cisco Prime IP Express services.

The solution also supports a disaster recovery design to assure resiliency of IPAM services in the event of an outage (Figure 16).

Figure 16. IPAM Disaster Recovery Design



To implement disaster recovery (DR) capabilities, enterprises should deploy the IPAM DR instance on a separate server at the remote site. The IPAM executive periodically updates the IPAM DR server. In the event of a failure of the IPAM executive server, the IPAM DR server can be activated to take over as the executive instance. In this manner, all elements of the DDI solution - DNS, DHCP, IPAM, and the captive BYOD portal - provide optimal performance and resiliency for critical business connectivity services.

Conclusion

As your enterprise adapts to changing business requirements in the coming months and years, yesterday's basic, localized, and largely manual DDI processes cannot scale to meet your needs. With your employees and critical applications depending on the basic business connectivity that DNS and DHCP enable, you need more advanced, industrial-strength DDI capabilities.

Cisco Prime IP Express delivers the scalability and resiliency you need, even in the largest and fastest-growing enterprise networks. It provides a modular, standards-compliant dual-stack solution that can grow and evolve with your business. And it gives you a central point of administration to simplify all connectivity and IP address space functions across your distributed enterprise.

To learn more about what Cisco Prime IP Express can do for your business, visit http://www.cisco.com/go/prime-ipexpress.

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 C11-733373-00 11/14