



Cisco Prime Network Registrar IPAM 8.3 User Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Prime Network Registrar IPAM 8.3 User Guide
Copyright © 2016 Cisco Systems, Inc. All rights reserved

Contents

Chapter 1 Introduction	1
Overview	1
Major Functions	2
Record Information about Subnets	2
Individual IP Address Inventory	3
DNS Configuration Management	4
DHCP Configuration Management	6
Dynamic DNS	7
Address Utilization and Tracking	7
Administrator Controls	7
Components	8
License Key Support	8
Chapter 2 Getting Started	9
How to Begin	9
Logging into the IPAM Web User Interface	10
Logging in for the First Time	10
The Menu Bar	11
About Page	11
The License Block	11
Quick Links	12
Administrator Features	12
Administrator Preferences	13
Administrator Portal	14
Adding a page to the portal	14
Removing a page from the portal	14
Minimizing a page	14
Maximizing a page	14
Configuring the Portal	15
Portal Preferences	15
Logging Off	15
Displaying IPV6 Capacities	15
Internationalized Domain Names (IDN) Support	15
UI Treatment	16
Search and IDN	16
Column Selection	16
Column Sorting	17
Page Size Preference	17
Home Page	18
Page Navigation History	18
Toggle to freeze heading on tabular displays	18
Exporting Output	18
Chapter 3 Managing IP Addresses	21
Container View	21

Understanding the screen layout.....	21
Organization of Container Data	22
Table Display.....	23
Logical Container Functions	25
Add Root Block	25
Add Site.....	27
Add Child Block	28
Address Pool Allocation.....	32
Attach Child Block	32
Utilization Display	33
Block Chart.....	34
History Chart.....	35
Device Container Functions.....	35
Add Site.....	35
Add Child Block	36
Defining a Default Gateway	37
Attach Child Block	38
Detach a Block	39
Delete a Block	40
Network Switch Functions	41
IP Management.....	41
Adding Individual IP Addresses	42
Edit IP Address.....	49
Editing Interface Address Types	49
Editing Resource Records.....	49
Net Elements Tab	49
Ports Tab.....	50
Adding a Range of IP Addresses	50
Adding an IP Address Pool	52
Adding a Prefix Pool.....	56
Show Dynamic Leases	58
Planned vs Actual	59
Subnet/Block View.....	60
Understanding the screen layout.....	60
Editing Blocks.....	62
Root Block	62
Child Block	64
Delete Block	65
Split Block	65
Join Block.....	66
Move Block.....	66
Block type edit.....	66
Pending Approvals.....	67
My Approvals	67
My Submissions	69
Discovery	69
Discovery/Collector Task Definition Options	69
On-demand (Immediate) Collection Task	71
Scheduled Collection Task.....	71
Recurring Collection Task.....	71
Address Space Reclaim.....	72
Manual Reclaim.....	72
Automatic Reclaim	73
Ignoring Specific Device Types during Subnet Reclaim	73
IP Address Space Reclaim.....	73

Performing Manual IP Address Reclaim	73
Performing a Manual Subnet Reclaim	75
Performing Automatic Reclaim Tasks	76
Container Maintenance	77
Container Maintenance Layout	77
Edit Container	77
Detach Container	77
Delete Container	78
Add Child Container	78
Clone Container	80
Reparent/Move this Container	80
Attach Network Service to Container	81
Detach Network Service from Container	81
Attach Switch	82
Detach Switch	82
Network Elements/Devices	82
Adding a Network Element	83
Editing a Network Element	84
Editing Interfaces	84
Server Pairs	85
Adding a Network Service Pair	85
Editing a Network Service Pair	88
Restoring Deleted Items	88
Restoring Deleted Devices	89
Restoring Deleted Resource Records	90
Chapter 4 Managing DNS	93
Servers/Services	93
Managing DNS Servers/Services	93
Adding a DNS Network Service	95
Zones on a DNS Server	102
Configuring DNS Views on a DNS Server	106
Configuring Zone Templates on a DNS Server	108
Configuration/Deployment	111
Configuration/Deployment Task Definition Options	111
On-demand (Immediate) Config/Deployment Task	113
Scheduled Config/Deployment Task	114
Recurring Config/Deployment Task	114
Domains	115
Managing DNS Domains	115
Adding a DNS Domain	117
Editing a DNS Domain	118
Managing Resource Records	119
Galaxies	121
Adding a DNS Galaxy	122
Log Channels	123
Adding a Logging Channel	124
Editing a Logging Channel	125
Server Templates	125
Managing Server Templates	125
Adding a DNS Server Template	126
DNS Domain Types	130
Managing DNS Domain Types	130
Address Match Lists	132
Managing Address Match Lists	132

Adding an Address Match List.....	132
Editing an Address Match List.....	134
Update Policies	135
Managing DNS Update Policies	135
Adding a DNS Update Policy	135
Editing a DNS Update Policy	136
Adding a DNS Update Policy Detail	136
Editing a DNS Update Policy Detail	137
Transaction Keys.....	137
Managing Transaction Keys	137
Adding a Transaction Key	138
DNS Option Vendor Dictionary.....	139
Managing DNS Option Vendor Dictionaries	139
Editing Syntax for DNS Options	140
DNS Option Master Dictionary.....	141
Managing the DNS Option Master Dictionary.....	141
DNS Software Products.....	141
Managing DNS Software Products	142
Adding a Software Product.....	142
Chapter 5 Managing DHCP	145
Servers/Services	145
Managing DHCP Servers/Services	145
Adding a DHCP Server.....	147
General Tab.....	147
Collection Tab.....	148
Management Tab	149
Configuration Tab	150
Failover Peer Tab – CNR, INS, and ISC DHCPv4.....	151
Failover Peer Tab – Microsoft Windows 2012 DHCP.....	153
Extensions Tab	155
DHCP Utilization View	155
Utilization Display.....	156
Address Pool Details.....	157
Block Details.....	157
Network Links.....	158
Managing Network Links.....	159
Adding a Network Link.....	159
Editing a Network Link.....	160
Configuration/Deployment	160
Configuration/Deployment Task Definition Options	160
Immediate Config/Deployment Task	161
Scheduled Config/Deployment Task	161
Recurring Config/Deployment Task	162
Policy Sets.....	163
Adding a DHCP Policy Set.....	163
Working with DHCP Policy Set Policies	164
Viewing Policy Assignments.....	166
Option Sets.....	166
Adding a DHCP Option Set.....	167
Deleting a DHCP Option Set	167
Copying a DHCP Option Set.....	167
DHCP Option Set Options	168
Viewing All Options Assigned to This Option Set.....	168
Same as Subnet Options.....	169

Editing Values of Options Assigned to an Option Set.....	169
Removing Options from an Option Set.....	170
Viewing Option Set Assignments.....	170
Client Classes.....	170
Adding a DHCP Client Class	172
Editing a DHCP Client Class	173
Deleting a DHCP Client Class	174
Option Vendor Dictionary	175
Adding New Options to DHCP Product	175
Removing Options from an DHCP Option List.....	176
Option Master Dictionary.....	177
Adding a DHCP Master Option.....	177
Editing a DHCP Master Option.....	178
Deleting a DHCP Master Option.....	178
DHCP Software Products	179
Adding a Product.....	179
Editing a Software Product.....	180
Deleting a Software Product.....	180
Chapter 6 Producing Reports.....	181
Reports Overview	181
Filters	181
Container Utilization Report.....	182
Creating a Container Utilization Report.....	182
Container Utilization Report Output.....	184
Block Utilization Report	185
Creating a Block Utilization Report	185
Block Utilization Report Output	187
Low Pool.....	188
Creating a Low Pool Report	188
Low Pool Report Output.....	188
Container Audit Report.....	189
Creating a Container Audit Report.....	189
Container Audit Report Output.....	190
Block Audit Report.....	191
Creating a Block Audit Report	191
Block Audit Report Output.....	191
Device Audit Report.....	193
Creating a Device Audit Report.....	193
Device Audit Report Output.....	193
DNS Domain Audit Report.....	194
Creating a DNS Domain Audit Report	194
DNS Domain Audit Report Output.....	195
Resource Record Audit Report.....	197
Creating a Resource Record Audit Report.....	197
Resource Record Audit Report Output.....	198
Administrator Definition Audit Report	198
Creating an Administrator Definition Audit Report	198
Administrator Definition Audit Report Output	200
Administrator Activity Audit Report.....	200
Creating an Administrator Activity Audit Report.....	200
Administrator Activity Audit Report Output.....	201
Login Audit Report.....	201
Creating a Login Audit Report.....	202
Login Audit Report Output.....	202

Delegated Prefix Audit Report	202
Creating a Delegated Prefix Audit Report	203
Delegated Prefix Audit Report Output	203
Tasks	205
Tasks Screen Layout.....	205
Task Details	206
Alert Log.....	209
Working with the Alert Log.....	209
Logged-In Administrators Report.....	210
Accessing the Logged-In Administrators Report	210
Logged-In Administrators Report Output.....	210
RIR Summary Report	210
Accessing the RIR Summary Report.....	210
RIR Summary Report Output.....	211
SWIP/Net Name Report.....	211
Creating a SWIP/Net Name Information Report.....	212
SWIP/Net Name Information Report Output.....	212
DNS Zone Report	214
DNS Zone Report Output	214
Chapter 7 Setting Up System Policies, Agents, and Importing Data	215
System Policies/Options.....	215
Agents.....	220
Import Wizard	222
Select Import Type.....	222
Select Import File	223
Validate Import File Data	224
Import Data.....	224
Search	225
Saving Search Criteria	229
Loading a Saved Search	229
Editing a Search Filter.....	230
Chapter 8 Working with Blocks and Subnets	231
Allocation Reason Codes	231
Block Types	231
Initial Container Rules	233
Constraining Block Sizes.....	233
Address Pool Allocation Templates.....	233
Adding a new address allocation template	234
Searching for an address allocation template.....	237
Deleting an existing address allocation template	237
Site Allocation Templates	237
Site Allocation Template Functions	238
Site Allocation Template Prerequisites	238
Adding a Site Allocation Template.....	239
Editing a Site Allocation Template.....	243
Deleting a Site Allocation Template.....	243
RIR Organization IDs	244
Chapter 9 Working with IP/Devices	247
Vendor/Models	247
Vendor Maintenance	247
Model Maintenance	248

Device Types.....	248
Adding a Device Type	249
Naming Policies.....	249
Editing a Naming Policy for a Device Type.....	250
Device Interface Template Maintenance	251
Adding a Device Interface Template	251
Editing a Device Interface Template	252
Chapter 10 Using Other Tools.....	253
Threshold Sets	253
Creating a Threshold Set.....	253
Adding a Threshold to a Threshold Set	253
Block Threshold Alerts	255
Setting Up a Block Threshold Alert	255
Container Threshold Alerts.....	255
Setting Up a Container Threshold Alert.....	256
Network Services Threshold Alerts	256
Setting Up a Network Service Alert	257
User-Defined Fields.....	258
Adding a User-Defined Field	258
Creating Radio Button and List Values	259
Information Templates	260
Adding an Information Template.....	260
IDN Converter	261
UI Treatment.....	261
Converting a Domain Name to IDN.....	261
Search and IDN	262
Chapter 11 Managing Administrators	263
Administrator Definition	263
Adding an Administrator.....	263
Assignable Roles	264
Administrator-specific Policies.....	265
Determining Effective Rights for an Administrator	265
Authorized Functions	265
Access Control List	265
Block Type Access.....	266
Device Type Access	266
Policies	266
Domain Access Control	266
Net Service Access Control	267
Resource Record Type Access	267
Address Type Access	267
Administrator Roles	267
Adding an Administrator Role	268
Administrator Role Policies	268
Authorized Functions Tab.....	269
Access Control Lists.....	269
Block Type Access Tab	270
Device Type Access Tab	271
Policies Tab.....	271
Domain Access Control Tab.....	272
Net Service Access Control Tab.....	273
Resource Record Type Access Control Tab.....	273
Address Type Access Tab	274

Chapter 12 Performing Advanced Administration Activities	275
Configuring INS DNS for Selected or Changed Zone Push	275
Configuring IPAM to use External Authentication	276
Input.....	277
Output	277
Configuration Steps.....	277
Interfacing with Microsoft Active Directory and Microsoft DNS.....	278
BIND DNS	279
BIND Redundancy.....	279
Microsoft DNS	280
BIND DNS and Microsoft DNS Compared	281
Joint Implementation Scenarios	282
Case 1: BIND DNS Supporting Non-DNS AD Environment	282
Case 2: IPAM Centralized Inventory of AD DNS Environment	284
Case 3: AD Multi-Master DNS with BIND DNS Slave	286
Case 4: BIND DNS Master with a Microsoft DNS Slave	287
Case 5: PeerMaster – Effective BIND-Microsoft Multi-Master DNS	288
Creating GSS-TSIG enabled account in Microsoft MMC.....	290
Overview	290
Microsoft Active Directory.....	290
IPAM	291
Other Considerations.....	291
IPAM Management of Windows DHCP Server	291
Overview	291
Prerequisites.....	292
Windows Server Procedures.....	292
IPAM Procedure.....	293
Configuring DHCP Failover	294
Failover Scenarios.....	294
Simple Failover.....	294
Many to One Failover.....	295
Failover Checklist	295
Configuring Failover within IPAM	296
Configuring IPAM for Failovers.....	296
Administrator Access Control Use Cases	297
Use Case - Regional Administrators.....	297
Use Case - Specific Block Access Required	298
Use Case - DNS Administrator.....	299
Use Case - Third Party Access	299
Supported RFCs	300
Appendix A: Resource Records and Workflow.....	301

Chapter 1 Introduction

Overview

Welcome to the Cisco Prime Network Registrar IPAM 8.3 Address Management System. IPAM is a comprehensive software solution that helps organizations plan and maintain their IP address space and leverages that information for use by IP services such as DNS and DHCP.

No matter what size or type of organization, anyone that runs an IP network needs to manage their IP address space effectively. However, the Internet Protocol specifications do not provide any tools that help with this process. Some people may say that DHCP provides “automated IP address assignment”, but the scopes that are assigned to a DHCP server must still be allocated out of larger blocks used by the company. Some products that track IP addresses have been around for the last decade, but they are considered first generation tools that do not adequately address the needs of enterprises and service providers in the 21st century.

IPAM is a next generation tool that offers advanced functionality:

- 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 for integration with any type of system. Examples are work-flow 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 IPAM.
- Capture and record utilization information to be able to establish historical trends.
- Reclaim inactive addresses.

This interaction not only maintains consistency between the planned and deployed network, but allows proactive modification to the network to adjust for IP address shortages and overages.

IPAM is one product that is part of a complete and robust IP Address Management Suite. Collectively, these products form the IPAM IP Address Management Suite. When multiple products are installed, they appear and function seamlessly.

Note: CPNR IPAM 8.3 and later versions will not support Solaris. Refer to earlier versions of IPAM documents if you want to use IPAM with Solaris support.

Major Functions

IPAM has the following general functions:

- Record information about subnets.
- Individual IP Address inventory and asset management.
- Centralized DNS (Domain Name System) configuration and management.
- Centralized DHCP configuration and management.
- Updates DNS Dynamically for DHCP clients and for immediate changes to the IP Address Inventory.
- Captures address utilization and tracks it over time by the periodic and recurring retrieval of DHCP information, enabling trending and regression analysis to extrapolate when an IP address block will be exhausted.
- Creation of unique administrators that only allow access to those parts of the system authorized for that individual.

Record Information about Subnets

The basic building block of modern IP networks is the subnet. Yet, how are companies tracking information about those subnets? What are all the IP addresses eligible to be a “default gateway” for hosts on that subnet? What is the proper subnet mask for a subnet? It is not surprising that many companies rely on routing tables to obtain this information, or at least to use them to verify the accuracy of manually maintained information.

IP Addressing rules, such as verifying and enforcing bit-boundary rules when defining subnets are standard in IPAM. Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM) are fully supported.

In keeping with the dynamics of growing networks, many organizations have had to resort to having duplicate IP network numbers. Mergers have often forced IT departments into this practice. IPAM can easily handle this situation, helping companies keep these duplicate iterations of address space separate and distinct.

Before individual IP addresses can be recorded and managed, subnets must be declared. When a subnet is declared in IPAM, it is tagged as either an IPv4 subnet or an IPv6 subnet. Once declared, that subnet is supported in its native form, either IPv4 or IPv6. That subnet

must exist in a network of that address type and all the individual IP addresses in that subnet will be of that type.

IPAM provides a central repository for all subnet information; it verifies the accuracy of that information by “reading” the network and comparing it to the repository. The result is a single, correct picture of what is deployed on the network.

Individual IP Address Inventory

Historically, IP Addresses have been recorded as being used with a number of different methods. These include spreadsheets and logs. Some organizations have used DNS files or DHCP configurations to track which IP addresses were assigned and which ones were available. Common to all these techniques was a single view of the information. These processes only looked at the information in one way regardless of how those addresses were actually deployed on the network. DNS looked at it strictly from a DNS resource-record view.

IP addresses do not live by themselves. They are always equated with something, specifically some device or host on the network.

IPAM’s design took this into consideration. IPAM keeps track of a number of elements that represent real aspects of an IP network. These elements are:

- IP Addresses
- Devices
- DNS Information
- DHCP Information
- Services
- Users
- Logical or Physical representations of how a network is organized.

Relationships are then established between these elements in such a way that represent real network situations. Examples are:

- IP addresses are associated with devices
- Devices can have any number of DNS Resource Records
- Users own devices
- Devices reside at physical locations
- Subnets reside at physical locations
- Subnets form a logical network topology
- Services execute on Devices

A comprehensive IP Address Management System not only tracks the IP addresses themselves, but also how those addresses affect, and are affected by, other things on the network. For example, if a network management system such as HP Openview discovers a router, it will report on all the subnets that are attached to that device. It is the IP Address Inventory System that is the source for data needed to translate the HP Openview

discovered data into meaningful information. The IP Address Inventory System can answer such questions as:

- Are the IP addresses and subnets on that router correct based on the plan, design and architecture of the network?
- What are the physical locations of those subnets and routers?
- Are the proper names registered in DNS for that device and all the IP addresses on that device?

IPAM not only provides a source for such information, but can periodically verify it to insure its accuracy.

An extremely useful feature of IPAM is the general way that it allows a company to organize its IP Address information. IPAM uses “Containers” to create any type of hierarchical topology. Address information can then be placed into these Containers. The flexibility of a hierarchy allows the rendering of information in almost any fashion, allowing the company to represent the IP address information in the way that makes the most sense for that company.

Access to the IPAM Address Inventory is not just through a human Graphical User Interface (GUI). It is also accessible through Command Line Interfaces (CLI) and Application Programming Interfaces (API). This allows other systems and programs to get to IP Address Inventory information for automatic population of those other systems and programs, leveraging the Address Inventory for any number of uses.

Views of the elements are summarized wherever possible to reduce the amount of information that must be scrolled. This is especially important for companies that have a very large address space or numerous DNS elements. Whenever there is a relationship between IPAM elements (addresses, devices, DNS records, etc.), those relationships can be easily displayed from any of the elements. For example, can we see all the IP addresses associated with a device? Or, what are all the DNS records that will be generated for a given IP address? IPAM provides this information from an easy to use interface.

DNS Configuration Management

Without an automated, centralized IP Address Management System, there can be considerable duplication of data for different uses. The person tracking IP address using one method, such as a spreadsheet, would provide that information to a DNS administrator. The administrator would enter the same information, but in a different context and syntax, into a different system, specifically DNS configuration (i.e. zone) files.

IPAM eliminates this additional administrative task. IPAM takes the information that is used to record IP address and device information and builds the needed DNS records automatically, populating the DNS configurations in real time using dynamic DNS (RFC 2136) updates. It can also build, or rebuild, a complete set of DNS configuration files that are compliant with ISC’s BIND Versions 8 and 9 DNS servers, as well as a number of 3rd party DNS servers including Microsoft’s and Cisco’s. These DNS configuration files (boot and zone db files) are remotely loaded onto DNS servers distributed on the network.

IPAM's DNS configuration feature allows the easy entry and management of some of BIND's newer features, reducing those feature's complexity and making it easier to implement and deploy them, and in much less time. Some of these features are:

- BIND Views
- TSIG support (for dynamic updates and zone transfers)
- Nested Access Control Lists (ACLs)
- Configuration for remote management via the RNDNC command
- Zone types of forward, stub and delegate-only
- Multiple masters per zone

BIND 8 and 9 are exceptionally feature-rich. However, with that increased functionality comes configuration complexity. There are a daunting number of options, parameters and keywords that can be coded in the DNS configuration files. IPAM minimizes this complexity by hiding all options that may not pertain in a specific environment. A customer has complete control on which BIND options are made visible and externalized, and which ones should take defaults and not be shown. A master DNS dictionary contains every possible BIND option available. Subsets are defined and associated with DNS server "models" or "templates". These models can then be applied to a real server definition, almost eliminating the need to specify options for that server. A high level DNS administrator can define these models once, and then let them be applied to any number of server definitions by less experienced administrators.

What are some of the other ways that IPAM can make administration of DNS servers easier?

- Automatic generation of **key** statements between two DNS servers to insure that they have consistent private keys between them.
- Definition of **server** statements that insure correct communication between different DNS servers.
- Creation of **control** statements that facilitate external communication to the DNS server from only authorized sources.
- Proper inclusion of ACLs in the configuration files whenever they are referenced.

Even though IPAM reduces the complexity of these definitions, they are all still accessible and configurable, giving complete flexibility in those situations that demand the advanced DNS features implemented. The philosophy of IPAM is simple: make configuration easy, but don't compromise functionality.

Another unique feature of IPAM's DNS Configuration Management is the ability to have multiple domains per DNS zone. For example, a DNS domain called **company.com** exists as a delegated domain with its DNS resource records in a single db zone file. Child domains to company.com might be **newyork.company.com** and **california.company.com**. The DNS resource records for these child domains can exist as delegated domains in unique zone files (with their own SOA records) or in the parent's db zone file. IPAM fully supports this model.

Prior to activating any new DNS configuration, it is checked for syntax and consistency to make sure that DNS configuration files are built correctly. This will ensure that DNS servers always initialize properly.

In addition to supporting BIND Versions 8 and 9, any DNS server that is compliant with BIND 8/9 is supported. Support for Microsoft's Windows 2008 DNS server is also provided.

DHCP Configuration Management

Another service that benefits from the common central repository of IP address information is DHCP. Addresses assigned to DHCP servers (scopes) come out of the overall management of the address space that is part of the IP Address Inventory feature of IPAM.

As with DNS, address information needs to be manually replicated in a DHCP server configuration without the aid of an IP Address Management System. With IPAM, the actual configuring of scopes is completely hidden from the administrator.

Ranges of addresses are defined with an attribute of "dynamic". They are then assigned to a DHCP server. The DHCP servers are defined before-hand to IPAM, along with operational parameters for those servers. IPAM includes a software based DHCP server that can run on Windows 2003/2008 or Linux (RedHat, Enterprise 5 or 6). A variety of other DHCP servers are also supported, including Microsoft's and Cisco's.

Rather than link DHCP options (the IP parameters sent by the server to the DHCP client) to address ranges or scopes, options are defined as sets. These sets are then associated with a rule. If the information provided by the DHCP client in the process of obtaining an IP address matches the rule, those options are sent, regardless of the subnet from which an address is provided to the client. This way, a limited set of option lists can be maintained, even for the largest of networks. Options don't have to be defined and associated for each and every subnet or scope. Broad policies can dictate what options a client will get, disassociated from the address pools that are appropriate for the client based on their network location.

IPAM's DHCP server supports "failover", a high availability option where two DHCP servers work in concert to provide a single appearance of DHCP services to the DHCP client. This DHCP server implements the IETF DHCP Failover Protocol Internet Draft and allows very flexible primary/secondary DHCP server deployment designs. With the IPAM DHCP server you can:

- Declare one server as a primary and one as a backup for a given subnet.
- Have one DHCP server act as a backup for any number of primaries.

These capabilities allow limitless combinations that can effectively provide for high availability and redundancy of the DHCP configuration while maximizing the use of address space.

Dynamic DNS

IPAM has full support of updating the DNS name space with RFC 2136 compliant dynamic UPDATE packets. There are two sources for these updates:

- The IPAM DHCP server
- Changes made directly to the IP Address Inventory repository for static address changes

The result is a DNS name space that is synchronized with the IP Address Inventory. Dynamic updates are performed in two different ways:

- Immediately
- Batched to combine a number of dynamic updates in a single operation

BIND Version 9 brings true dynamic DNS operation as the primary mechanism for maintaining the DNS space. Unlike earlier versions of this DNS server, which used modifications to zone db files as the definitive update mechanism, BIND 9 relies almost exclusively on dynamic DNS to keep its domain information current. IPAM fully supports this model. Zone db files are only updated by the IP Address inventory initially, and in disaster situations. At all other times, dynamic updates are used to update zone information.

Name and address binding information from a DHCP server is verified before a dynamic DNS update is performed using the method outlined in the IETF Internet Draft “Resolution of DNS Name Conflicts among DHCP Clients”. This method does not rely on the IP Address Management Repository for name and address information, but rather DNS itself, allowing that data to be replicated for a much more robust availability model.

Address Utilization and Tracking

Planning and recording of IP addresses in a central repository is a unidirectional approach to IP address management. It is not a complete solution for an IP Address Management System. That is why IPAM is multi-directional system. It not only plans and records information about the IP address space, but it also interacts with the actual network to read, verify and compare configurations and utilizations on the network against the IP Address Inventory repository. IPAM will go out to the network and:

- Verify the use of a statically defined address
- Ensure that free addresses in the repository are not in use on the network
- Capture information about DHCP clients.

These three features provide the raw data to report and trend address utilization. This can be displayed as current snapshots, or historically, providing trending information at any level of the IP address hierarchy.

Administrator Controls

IPAM is a multi-administrator system. Access to the system is limited based on rights and privileges given to that administrator. These rights can be very broad, or limited to a very narrow set of conditions. To any element and/or Container in IPAM, an administrator can

be allowed read access, write access, or create/delete access. Options within the Graphical User Interface can be exposed or withheld. The use of the CLIs and APIs can be denied or allowed.

Components

IPAM is a highly scalable, distributed solution that consists of four major components:

- **IPAM Executive** – The central management system responsible for initiating work requests or recording the results of completed requests. There is typically one IPAM Executive per IPAM system.
- **IPAM Agents** – Lightweight, distributed processes that execute work requests from the IPAM Executive. The IPAM Agents are the entities that interface directly with DHCP servers, DNS servers, or Network Devices such as routers. There can be any number of IPAM Agents distributed on a network. They may be located wherever is optimal for the network topology.
- **IPAM Database** – The central repository that stores information and auditing data about IP network space. This database is under the control of the IPAM Executive.
- **IPAM Administrative Interface** – A Web-based Graphical User Interface (GUI), hosted on the IPAM Executive that allows administrators to control the IPAM system.

License Key Support

IPAM requires you to enter a license key the first time you log in to the product. The license key determines how many IP Addresses, devices, and/or agents that can be managed.

To obtain your license key, contact Cisco Software Support at www.cisco.com

Chapter 2 Getting Started

How to Begin

Note: For information on installing IPAM, refer to *Cisco Prime Network Registrar IPAM 8.3 Installation Guide*.

To start using the IPAM Management System, all IPAM services, and the IPAM database must be started.

Windows: To start IPAM services, use the Windows Services Controller, and start the following services:

- MySQL Relational Database
- InControl ActiveMQ Service
- InControl Task Manager Service
- InControl Result Manager Service
- InControl Log Manager Service
- InControl File Manager Service
- InControl Callout Manager Service
- Incontrol DNS Listener Service
- Incontrol Management Server Service
- InControl Agent
- Tomcat

Table 2-1 Description of IPAM Services

Windows service	What does it do?	Running on
MySQL	Provides the relational database system that supports the IPAM system.	IPAM Executive server only.
InControl Task Manager Service	Provides scheduling functions and controls the tasks (units of work) that are sent to the InControl Agents.	IPAM Executive server only.
InControl Result Manager Service	Collects task result information from all InControl Agents and places that information into the IPAM database.	IPAM Executive server only
InControl ActiveMQ Service	Provides reliable message transport between the InControl Task Manager, the Result Manager, and the Agent.	IPAM Executive server, and all InControl Agents

Windows service	What does it do?	Running on
InControl Log Manager Service	Provides a centralized log message collection system.	IPAM Executive server only.
InControl Callout Manager Service	Provides a mechanism to invoke customer defined scripts after certain events are triggered within the system.	IPAM Executive server only.
InControl Agent	Communicates with servers and devices to gather statistics.	InControl Agent server(s) only.
InControl File Manager Service	Provides file transport capabilities.	IPAM Executive server only.
InControl DNS Listener Service	Listens for changes to the DNS environment and updates IPAM with the appropriate DNS Resource Records.	IPAM Executive server only.
InControl Management Server Service	Executes pings for IP addresses and DHCP releases, when those functions are performed in the GUI.	IPAM Executive server and Agents
Tomcat	Provides the http web server and serves the IPAM web interface.	IPAM Executive server.

Logging into the IPAM Web User Interface

You need to log into the IPAM Web user interface to perform all functions. Before you log into IPAM for the first time, you need to be assigned a user name and password from your IPAM administrator.

IPAM is administered via a Web browser. If you are administering IPAM from the same server you installed IPAM on, you will find a shortcut in your Programs folder (**Start > Programs > InControl > InControl Supervisor**). Otherwise, follow the directions in the next section.

Logging in for the First Time

To log into IPAM, follow these steps:

1. Open your Web browser.
2. In the Address bar, type the following URL:
`http://xxx.xxx.xxx.xxx:8080/incontrol`
 where `xxx.xxx.xxx.xxx` is the IP address of the IPAM Executive.
 One example might be: **`http://172.16.32.50:8080/incontrol`**
 You may also use the DNS name of the IPAM server, such as:
`http://ncexec.mycompany.com:8080/incontrol`
3. You see the following login screen.
4. Enter the Login name and Password assigned to you by your IPAM administrator, and click **Log In**.

Note: The first time you log into the IPAM system, use the user name **incadmin**, and the password **incadmin**. Refer to “Changing Password” on page 13 for instructions on changing the password of this user.

Note: The attribute “autocomplete=off” is set for the password field to prevent the saving of passwords. This attribute is now ignored for password fields by Internet Explorer as of version 11 and Chrome as of version 34, and these browsers will still offer to save passwords if the feature is enabled in the browser.

The Menu Bar

The bar across the top of the browser display is called the menu bar. There are four menu lists in the IPAM Supervisor interface:

- Home
- Management
- Reports
- Tools

The menu options are described in detail in the sections below.

About Page

The **About Page** displays the current status of your system and some quick links for easy navigation. It is accessible under the menu bar under Tools->System->About.

The License Block

Several key pieces of information are shown on the **Home** screen:

Version and Build number

The version and build number of Cisco Prime Network Registrar will be displayed here. You need to know this when getting support for IPAM. For support, refer to the links and phone numbers in the Product Support Information section.

Address Block Information:

- **Current Public IPv4 Space** - This is the size of public IPv4 address space (blocks and subnets) currently defined in the system. A “public” address is one that is not within the ranges defined in [RFC1918](#).
- **Current Private IPv4 Space** - This is the size of private IPv4 address space (blocks and subnets) currently *used* (has a status of “in-use”) in the system. A “private” address is one that lies within the address ranges defined in [RFC1918](#).

- **Current total IPv4 Space** – This is the sum of the public and private IPv4 address space counters above.
- **Maximum Allowed IPv4 Space** - This is the total IPv4 space (subnets and blocks) allowed by your license key.
- **Current Number of IPv6 /64 Blocks** - If you have licensed IPv6 support, this counter shows the number of /64 subnets defined.
- **Maximum Allowed IPv6 /64 Blocks** - The total number of /64 blocks allowed by your license.

Individual IP Address Information:

- **Maximum Allowed Used IP Addresses** - The total number of used IPv4 and IPv6 addresses allowed by your license key.
- **Current Number of Used IP Addresses** - The total number of used IPv4 and IPv6 addresses within the system. This count includes devices with the following status; Static, Manual DHCP, Dynamic DHCP with an active lease, and Automatic DHCP with an active lease.
- **Maximum Allowed Defined IP Addresses** - The total number of defined IPv4 and IPv6 addresses that allowed by your license key.
- **Current Number of Defined IP Addresses** - The total number of defined IPv4 and IPv6 addresses within the system. This count includes devices with the following status; Static, Manual DHCP, Dynamic DHCP, Automatic DHCP, and Reserved.

Other Key Information:

- **Expiration of License Key:** The date on which your license key for IPAM expires.

Quick Links

Quick Links provide you with direct links to some of the more commonly used functions. Use these to save time navigating through the other tabs. You can add up to four custom links in **Policies and Options** on the **Tools** menu.

Administrator Features

Administrator Features provides you with convenient links to several commonly used functions.

Pending Approvals

Displayed when Device or Resource Record Workflow is enabled, the Pending Approvals screen allows you to view two sets of data related to device and resource record workflows.

To review the status of device changes that either need your approval or that you have submitted for approval, click the **Pending Approvals** link. The Pending Approvals screen opens, as described in “Pending Approvals” on page 67.

Changing Password

To change your password, click the **Change Password** link. The Change Password screen opens.

Enter a new password in the **New Password** field and then confirm the password by retyping it in the **Verify New Password** field. Click **Submit** to complete the procedure.

Adding an Administrator

Refer to “Adding an Administrator” on page 263.

Logoff

Choose this link to exit the system.

Administrator Preferences

Some settings are stored in the IPAM Database and remembered on a per administrator basis. Administrator Preferences are retained in the IPAM and loaded by the GUI on login. When administrator changes one of these settings, IP Control will update the administrator’s preference in the IPAM database. The following table lists preferences that are currently remembered by the IPAM GUI:

Preference	Description
Navigation(Left) Pane Sizing	Changing the size of the navigation pane.
Help Panel(Right) Pane Sizing	Changing the size of the help pane.
Page Size per Tabular Page	Changing the page size. Each type of Tabular page will remember its own page size.
Advanced Search	The last search an administrator performed will be remembered and automatically launched when returning to the advanced search page.
Home Page	Select a home page to display on login and clicking the home icon.
Columns	The columns selected for display via the column chooser dialog will automatically be remembered when the administrator makes changes.
Sort Order	When the user changes the sort order of a tabular page.

Preference	Description
Container Classic vs. Table Display	When the administrator navigates to the container table display (or back to the classic view), this will automatically be remembered as a preference. When a new container is visited, the table display will now be shown first. If the administrator returns to the classic view, the classic view will be shown first.

Administrator Portal

Every administrator has a default portal which defaults to a view with the same information as the about page presented as two portal windows.

The portal is divided into individual portal windows that display pages that have been added to the portal. These pages support all of the functions of the original page, except in a more compact view. A maximum of 10 pages can be added to the portal for each administrator. List pages will only display 5 rows of data at a time in the portal.

Adding a page to the portal

Many pages within IPAM can be added to the administrator portal. Pages that can be added to the portal will have a (★) icon in the upper right corner of the page. To add a page to the portal, navigate to the desired page in IPAM and click on the icon. After clicking on the icon, it will change to (★) to indicate that the page is now in the portal. Clicking on this icon again will remove the page from the portal.

Removing a page from the portal

Pages can be removed from the portal by clicking on the (✕) icon in the top right corner of the portal window.

Minimizing a page

Pages can be minimized by clicking on the (–) icon. When the window is minimized it can be returned to normal by clicking on the restore (☐) icon.

Maximizing a page

Pages can be maximized by clicking on the (☐) icon. Maximizing a page takes you to the full view of that page.

Configuring the Portal

The position of the portal windows can be configured by clicking on the ( [Configure](#)) link at the top of the portal. Clicking this link minimizes all windows and adds the portal move icons to move items left() , right() , up() , and down() . Use these buttons to position portal windows as desired. Windows can also be removed from the portal by clicking on the () icon. Click the ( [Configure](#)) link again to put the portal back to its normal view.

Portal Preferences

Each portal page is individually configurable based on an administrator's preferences. By default, preferences for each portal page will be inherited from the preferences configured in the page's full view. However, if the portal page is configured directly in the portal, the individual portal page will remember its own preferences.

Logging Off

To exit the system, choose one of the following:

- Click the **Logout** link at the top of the screen.
- Click the **Logoff** link in the Administration Features section of the **Home** menu.

You are logged out of the system and returned to the initial login screen.

Displaying IPV6 Capacities

IPV6 subnets are extremely large. Displaying these numbers is challenging because the numbers are so large that they lose meaning. IPAM enables you to display these numbers in one of three different formats, so their values are easier to interpret. The formats are:

- **CIDR** – The number is displayed in terms of a CIDR value, e.g., 1 /64
- **Full** – The full decimal number is displayed, e.g., 18446744073709551616
- **Exponential** – The number displayed as a power of 10, e.g., 1.8x10¹⁹

A small gear icon () appears above the columns where these numbers are displayed. Click on the gear to change the display format. The fields that will be affected are marked with a shaded triangle in the upper right-hand corner (). Pause the cursor over the triangle to see the value in all formats, as shown in the sample container utilization display.

Internationalized Domain Names (IDN) Support

Internationalized Domain Names use characters drawn from a large repertoire (Unicode). IDNA (Internationalized Domain Names for Applications) as described in RFC 3490 allows the non-ASCII characters to be represented using only the ASCII characters already allowed in so-called host names today. This backward-compatible representation is required in

existing protocols like DNS, so that IDNs can be introduced with no changes to the existing infrastructure.

IDNA is only meant for processing domain names, not other text.

IPAM supports IDNA as defined in RFC 3490. It allows for data to be entered using Unicode characters and ASCII characters both when entering domain names. IPAM also gives the users the ability to switch between IDN and ASCII when viewing the data. The underlying data is always stored as ASCII or ASCII Compatible encoding (ACE).

For example, for Internationalized Domain name 'bücher.com', the ACE equivalent is 'xn--bcher-kva'.

UI Treatment

Screens involving domain names, FQDNs and hostnames in case of domains/zones and owner and RDATA fields in case of resource records get special treatment for IDN support.

If an internationalized domain name is entered, an  icon appears on the screen. You can click on the icon to switch between IDN (Unicode character set) and ACE (ASCII compatible encoding) views. Hover the cursor over domain names to see the value in the alternate format.

Search and IDN

Domain and resource record searches in IPAM are performed using the ASCII representations. If you have Internationalized Domain Names, type a full IDN domain name or full/partial ASCII domain name in the search box to get back the desired result. Partial IDN search does not work.

For example, to search domain "bücher.com", you can enter "bücher.com" or "xn--bcher-kva" (ASCII Compatible representation) or any part of the ASCII compatible name (for example, "bch") and get back the desired result.

However, putting "büc" does not return the domain "bücher.com" since the searches are performed using the ASCII equivalent.

Column Selection

In addition to being able to filter report data selection criteria, you can select which columns you want to view in lists and reports where the  icon is displayed.

To change the column selection, follow these steps.

1. Click on one of the  icons. The Column Selection dialog opens, showing all columns selected.
2. Choose from the following actions.

To ...	Then ...
--------	----------

To ...	Then ...
Remove a currently displayed column	<ol style="list-style-type: none"> 1. Select the column in the Selected list. 2. Click . The column is moved to the Columns list.
Remove all currently selected columns	Click  . All columns in the Selected list are moved to the Columns list.
Add a column that is not currently selected to the report output	<ol style="list-style-type: none"> 1. Select the column in the Columns list. 2. Click . The column is moved to the Selected list.
Add all columns that are not currently selected to the report output	Click  . All columns now appear in the Selected list.
Move a column leftward in the report output	<ol style="list-style-type: none"> 1. Select the column in the Selected list. 2. Click  until the column is located in the position you want it to appear in the output.
Move a column rightward in the report output	<ol style="list-style-type: none"> 1. Select the column in the Selected list. 2. Click  until the column is located in the position you want it to appear in the output.

3. Click **OK** to implement your changes or **Cancel** to restore the previous column display. The selected columns will be stored in the database as an administrator preference.

Column Sorting

Many columns in lists and reports can be sorted. Sortable columns are distinguished by their black headings, in contrast to gray column headings that cannot be sorted.

To sort a column, click the heading. The  icon appears besides the heading as the data is sorted. To reverse the sort order, click the heading a second time. The  icon appears besides the heading as the data is resorted. The sort column and sort order are stored in the database as an administrator preference.

Page Size Preference

Tabular pages enable setting the page size once. When you revisit the page, the same page size will be selected. As a result, you do not need to set the page size every time the page is revisited. When you select a new size from the “Show:” drop-down box, the setting will be updated. The page size is saved as an administrator preference in the IPAM database.

Home Page

By default, an administrator on logging in will be directed to the container view if they have permissions to access the container view, otherwise they will be directed to the Tools -> System -> About page. Also by default, an administrator clicking on the home icon on the mega menu will be directed to the administrator portal. An administrator can choose their own home page, which will replace these defaults with the administrator's choice. A home icon is displayed on pages that are available to be set as a default home page. By default, it will be an empty house (🏠). Clicking on the icon will change the house to blue (🏠), and will make that page the administrator's home page. The administrator can restore the defaults by clicking on the icon again, which will remove the page as the administrator's home page.

Page Navigation History

When an administrator navigates from a list page to an edit page via a hyperlink or action, the GUI remembers the state of the page, i.e. filter criteria selected, search criteria entered, current page, etc. After an operation is performed on the edit page, i.e. submit or cancel, and the user is returned to the current page, the page will display as it was before navigating to the edit page.

Toggle to freeze heading on tabular displays

IPAM provides an ability to scroll only the rows of a given tabular display. The column headings remain in place while each row scrolls up or down.

This feature will be activated when a user has enough results in the table to add a scroll bar to the right hand side. When the user scrolls down and when the header row (with the column names) hits the top of the page, the header row will lock in place at the top and results will continue to scroll underneath it. This feature is dynamic and depends on the space width allocated to the table and the number of columns in the table. If the table columns are too narrow and there is not enough space to display their titles, the row header cannot be locked at the page top. The table header can automatically lose or gain its ability to freeze if you

- resize the browser window
- close, open, resize the left/right sliding panels
- add, remove columns by using the Column Selection .

Exporting Output

Once you have customized a list or report by modifying the filters and columns, you may want to save the output for analysis or review. IPAM provides the following export formats:

- PDF
- Excel
- CSV
- XML

Firefox only: the browser does not have an application associated with the text/XML or application/XML mime types to open XML attachments in XML format. The browser handles XML attachments as HTML documents. If you try to open an XML export file in Firefox and select any browsers installed in your system from the “Open with” option, the Firefox saves the file with “htm” extension in Temp directory. As result, the selected browser displays the file without any XML formatting. For Firefox, we recommend the following options:

- select any text editor to open XML export file.
- save XML export and open it with any default application.

This page intentionally left blank.

Chapter 3 Managing IP Addresses

In IPAM 8.3, all the features you need to perform IP address management are located in the IPAM section of the **Management** menu. This chapter describes how to use each selection.

- Container View
- Subnet/Block View
- Pending Approvals (displayed when Device or Resource Record Workflow is enabled)
- Discovery
- Address Space Reclaim
- Container Maintenance
- Network Elements/Devices
- Server Pairs
- Restore Deleted Items

Container View

The Container View option allows you to view and manage IP address space by using a user-defined management hierarchy. Day to day management of IP address space is accomplished using the Container View option. Using this option, blocks are added, deleted, split, joined, attached, detached, and moved. IP addresses are added, deleted, and allocated to network services. IPAM adheres to strict CIDR rules and maintains referential integrity of your address space.

Understanding the screen layout

When you select the Container View function, a view of your management containers is available in the left frame of your browser. You may select individual containers and drill down into child containers that were created with Container Maintenance. You may note two different colored containers in the left pane. Gray containers indicate that the container does not have blocks assigned to it. Yellow containers indicate blocks have been assigned.

Two container types exist: logical containers and device containers. Device containers are linked to a network element, which means that a discovery can be performed against the IP

of that net element and the results written onto the associated device container. Logical containers, however, are not attached to a network element.

On the right side of the screen, you will see details about the container that is currently selected in the tree view in the left frame.

The default container displayed is the Root Container, or **InControl**.

- In the **Container Tree** frame, you can click **Refresh** to refresh the content of the container tree.
- In the **Container View Details** frame, address block details about the selected container are displayed.

Organization of Container Data

The blocks that are displayed in the container view are organized within the container by block type. Block types are user defined, and are created using the **Block Types** option in the SUBNET/BLOCK section of the **Tools** menu (described on page 231).

Table 3-1 Detailed Container View Screen Elements

Field	Description
Block By Type	Shows the blocks assigned to this container organized by Block Type.
 Edit	Edit the properties of this block.
Child Block	The starting address of the child blocks.
Size	The size in CIDR notation of the block.
Root	If this block is a Root block, then “Yes” will be displayed in this column.
Status	The current status of this block.
Container	The name of the container that holds this block.
Parent Block	The starting address and size of the Parent Block of the current block. The parent block is the block that this block was derived from.
Create Date	The date this block was created.
Creator	The administrator that created this block.
Create Reason	The reason code entered when this block was created.
User Defined Fields	The User Defined Fields associated with this block.

Detailed Container View

In the **Detailed Container View** frame, there are several selections available depending on the selected container:

- **Add Site** – Click this link to add a number of blocks using a site allocation template.
- **Add Child Block** – Click this link to add a child block to this container.
- **Attach Child Block** – Click this link to model connections between devices.

- **Add Root Block** – Click this link to add a root block to this container. This link can optionally be suppressed for this container based on the rules defined for this container in the “Container Maintenance” option.
- **Utilization Display** – Click this link to display the utilization information for the blocks in this container. Be sure a Global Utilization Rollup discovery has been performed to see the most current utilization (described in Table 3-26 on page 69).
- **Table Display** – Click this link to display the container view in a tabular display with sorting, searching, filtering, and exporting capabilities (described in Table Display).
- **Block Chart** – Click this link to display the block allocation graph for the blocks located within this container.
- **History Chart** – Click this link to display the chart of this container showing the overall history of address space allocated to this container.

Table Display

The Table Display for containers provides the same features as a regular container view (except folding capability) plus sorting, searching, filtering, exporting, and pagination. The Filters depend on the container type (logical/device) and the status of the “Show Only Blocks Assigned to this Container” checkbox.

Table 3-2 Filters for logical and device containers

Container Type	Filters, “Show Only...” checkbox is on	Filters, “Show Only...” checkbox is off
Logical	<ul style="list-style-type: none"> • Block Type – all block types specific for the container • Status – all available statuses excluding Free 	<ul style="list-style-type: none"> • Block Type – all block types specific for the container • Status – all available statuses including Free
Device	<ul style="list-style-type: none"> • Interface - all interfaces specific for the container • Block Type – all block types specific for the container • Status – all available statuses excluding Free 	<ul style="list-style-type: none"> • Interface - all interfaces specific for the container • Block Type – all block types specific for the container • Status – all available statuses including Free

The “Show Only Blocks...” checkbox status is synchronized between the regular and tabular views. To return to the regular view, click on the Container View link.

When an administrator navigates to the container view or table display, this is remembered as a preference. If an administrator has navigated to the table display, anytime a container is shown it will now default to the table display. To return to the regular container view, click the “Container View” link from the Table Display to return to the Container View. The container view will now be shown by default.

Table 3-3 Detailed Logical/Device Container Table Screen Elements

Field	Description	Container Type
Block	Block name	Logical/Device
Child Block	The starting address of the child blocks.	Logical
Interface	Interface of the block	Device
Block Type	Type of the block	Logical/Device
Child Block Type	Type of the child block	Logical
Size	The size in CIDR notation of the block.	Logical/Device
Root	If this block is a root block, then <input checked="" type="checkbox"/> will be displayed in this column.	Logical/Device
Primary Subnet	If this block is primary Subnet, then <input checked="" type="checkbox"/> will be displayed in this column.	Device
Status	The current status of this block.	Logical/Device
IP Address	The IP address of the interface	Device
Container	The name of the container that holds this block.	Logical
Parent Block	The starting address and size of the Parent Block of the current block. The parent block is the block this block was derived from.	Logical/Device
Create Date	The date the block was created.	Logical/Device
Creator	The administrator who created this block.	Logical/Device
Create Reason	The reason code entered when this block was created.	Logical/Device
User Defined Fields	The User Defined Fields associated with this block.	Logical/Device

Logical Container Functions

This section describes the functions available to manage the Logical Container.

Note: Device containers contain the same options as Logical Containers plus some extra device-specific features. These differences are outlined in “Device Container Functions” on page 35.

Add Root Block

The Add Root Block display is used to initially define address space to IPAM. This includes initial allocations of space from an internet registry such as ARIN, or private [RFC 1918](#) address space. Once this space has been defined to IPAM, you use “Add Site” (see the next section) or “Add Child Block” (see page 28) options to allocate space from this block to your network.

Table 3-4 Add Root Block Parameters

Field	Description
Address Space	<p>Enter the starting address for the block of addresses that you are defining.</p> <ul style="list-style-type: none"> For IPv4 addresses, use standard dotted decimal notation (x.x.x.x) such as 10.0.0.0. For IPv6 addresses, use the 2 standard text conventions as defined in RFC 2373 below. <ol style="list-style-type: none"> The preferred form is x:x:x:x:x:x:x:x, where each x is the hexadecimal value of the eight 16-bit pieces of the address, such as: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 Or 1080:0:0:0:8:800:200C:417A <p>Note: It is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2).</p> <ol style="list-style-type: none"> Due to some methods of allocating certain styles of IPv6 addresses, it is common for addresses to contain long strings of zero bits. To make writing addresses containing zero bits easier, a special syntax is available to compress the zeros. The use of :: indicates multiple groups of 16-bits of zeros. The :: can only appear once in an address. The :: can also be used to compress the leading and/or trailing zeros in an address. For example, the following address: 1080:0:0:0:8:800:200C:417A may be represented as: 1080::8:800:200C:417A
Block Type	Select from the user-defined block types that have been defined in the Block Types option in the SUBNET/BLOCK section of the Tools menu.

Field	Description
IP Address Version	Select the version of IP Address space that you are adding to the system, IPv4 or IPv6 . Note: The license key controls which versions of IP Address space are supported within the product.
Block Size	Select the block size that you are adding. The block sizes are listed in CIDR notation.
Block Name	Enter the name of a block, or use the system supplied name of {Address space/BlockSize}. Note: The block name appears on the Container screen.
Block Description	Enter a description of the block.
Current Status	The current status of this block: Aggregate – This block is an aggregate block. Note: All root blocks have an aggregate status.
Create Reverse DNS Domain(s)	If this option is checked, the system will automatically create an in-addr.arpa reverse domain for this address space. You may optionally select the “type” if you have overlapping address space. Domain “Types” are defined in the Domain Types option in the DNS section of the Management menu.. Note that you must still assign this domain to a DNS server or a DNS galaxy in the DNS section of the Management menu. This option only creates the reverse domain for you.
Block Type	Select from the user defined block types that have been defined in the system. This assigns this block a specific type. The list that is displayed in the “block type” list is controlled by rules defined in the container maintenance option.
Allow Overlapping Address Space	If this option is checked, this address space may be defined multiple times within the system. This allows for overlapping address space if needed. Any overlapping space must not be in the same container or any of its parents. It is recommended that you do not check this option, unless you specifically want to define duplicate address space within the product.
Internet Registry	If this is public IP Address space, select the Internet Registry from which you received this block. If this is private IP Address space, select RFC1918 . For any other types of blocks, select Generic Root Block .
Organization ID	Default is None . Select an ID that has already been defined in RIR Organization IDs in the SUBNET/BLOCK section of the Tools menu.
SWIP/Net Name	Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container in Container Maintenance require the SWIP/Net Name.
Reason for Allocation	Select the reason why this block is being allocated. Reasons are defined by your IPAM administrator. For more information, refer to “Allocation Reason Code” on page 231.
Reason Description	Enter an optional description that outlines why this block is being allocated.

Add Site

Use the Add Site screen to select a previously defined site allocation template to apply to the currently selected container. For more information on creating site allocation templates, refer to “Searching for an address allocation template” on page 237.

To add a site with a site allocation template, follow these steps.

1. Select a logical container in the Container Tree.
The Address Block Details screen for the selected container opens.
2. Click the **Add Site** link.
The Add Site to Container screen opens.
3. Select the site allocation template you want to use from the **Site Allocation Template** drop-down list. Only site allocation templates defined for logical containers are listed.
A sequenced list of blocks in the selected template appears.
4. Enter block-specific data in the fields, as described in the table, below:

Table 3-5 Add Site Parameters

Field	Description
SWIP/Net Name	Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container require the SWIP/Net Name.
Allocation Reason	Select the reason why this block is being allocated. Reasons are defined by your IPAM administrator. For more information, refer to “Allocation Reason Code” on page 231.
Allocation Reason Description	<i>Optional.</i> Enter a description that outlines why this block is being allocated.

5. If an address allocation template is included in the site template, click  and enter any data required for the address template, for example, network service.
6. If user-defined fields are associated with a block, click the **UDFs** button and enter the required data. Click **Submit** to save the UDF data.
7. Click **Submit**.
The Add Address Pool Details screen closes.
8. Click **Submit**.
The subnet is added to the Address Block Details list.

Add Child Block

The Add Child Block display is used to define sub-allocations of address space to IPAM. Sub-allocations are taken from parent address space. This space is allocated from the parent, and then marked with the status that has been selected.

General Tab

For Logical Containers, the **General** tab shows:

Table 3-6 General Tab Parameters

Field	Description
Block Type	Select a block type from the user-defined block types that are defined in Block Types (in the SUBNET/BLOCK section of the Tools menu). The contents of the drop-down list are further determined by Valid Block Types policies for the current container. For more information, refer to “Container Maintenance” on page 77.
IP Address Version	Select the version of IP Address space that you are adding to the system, IPv4 or IPv6. Note that the license key controls which versions of IP Address space are supported within the product. Note: The list of Address Allocation columns at the bottom of the screen reflects which IP Address Version you select. Only templates that match the selected version are displayed in the Allocation Template list.
Block Size	Select the block size that you are adding. The block sizes are listed in CIDR notation. The block sizes that are displayed in this drop-down list are controlled by Valid Block Sizes settings in the Block Type tool, as well as the Block Sizes link in the Administrator Policies Block Type Access tab in the Administrator Roles tool.
Parent Block	<ul style="list-style-type: none"> To use the automated “best fit” allocation routine, select the “Best fit” option. To use the automated “random” (IPv6 only) allocation routine, select the “Random” option. To use the automated “sparse” (IPv6 only) allocation routine, select the “Sparse” option. To manually select the parent block to use for the space allocation, select “Manual”. The field will be populated with space that can be used for the allocation based on the version, size, and type entered above. <p>In either case the selection of allocation candidate blocks follows the rules defined for the container.</p>
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.

Field	Description
Discovery Agent	<p>Allows you to specify the IPAM Agent that will be used to “discover” hosts on this subnet/block.</p> <p>Inherit from Parent Block – Indicates that the agent specified on the parent block will be used for discovery.</p> <p>Inherit from Container – Indicates that the agent specified on the container will be used for discovery.</p> <p>Select Agent – allows you to select and specify a specific agent that will perform discovery for this subnet/block.</p>
Address Space	<p>Enter the starting address for the block of addresses that you are defining.</p> <ul style="list-style-type: none"> • For IPv4 addresses, use standard dotted decimal notation (x.x.x.x) such as 10.0.0.0. • For IPv6 addresses, use the 2 standard text conventions as defined in RFC 2373 below. <ol style="list-style-type: none"> 1) The preferred form is x:x:x:x:x:x:x:x, where each x is the hexadecimal value of the eight 16-bit pieces of the address, such as: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 1080:0:0:0:8:800:200C:417A <p>Note: It is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2).</p> <ol style="list-style-type: none"> 2) Due to some methods of allocating certain styles of IPv6 addresses, it is common for addresses to contain long strings of zero bits. To make writing addresses containing zero bits easier, a special syntax is available to compress the zeros. The use of :: indicates multiple groups of 16-bits of zeros. The :: can only appear once in an address. The :: can also be used to compress the leading and/or trailing zeros in an address. For example, the following address: 1080:0:0:0:8:800:200C:417A may be represented as: 1080::8:800:200C:417A
Block Name	<p>Enter a name of the block (manual parent block selection only), or use the system supplied name of {Address space/BlockSize}.</p> <p>Note: The block name appears on the container screen.</p>
Block Description	<p>Enter a description of the block.</p>
Current Status	<p>The current status of this block:</p> <ul style="list-style-type: none"> • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP Addresses are fully utilized. • Reserved – This block is reserved for future use.
Primary Subnet	<p>When using Network Links, select this check box if the block you are creating should be the primary subnet in the share.</p>

Field	Description
Non-Broadcast	When True, indicates that this block is not in a broadcast domain. As such the subnet and broadcast addresses (i.e., the first and last address in the block) are available for assignment. Typically this flag is set to False. This flag is only valid for IPv4 In Use/Deployed blocks.
Create Reverse DNS Domain(s)	If this option is checked, the system will automatically create a in-addr.arpa reverse domain for this address space. You may optionally select the “type” if you have overlapping address space. Domain “Types” are defined in Tools > IP/Devices > Device Types . Note that you must still assign this domain to a DNS server or a DNS galaxy using the Management menu. This option only creates the reverse domain for you.
SWIP/Net Name	Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container require the SWIP/Net Name.
Reason for Allocation	Select the reason why this block is being allocated. Reasons are defined by your IPAM administrator. For more information, refer to “Allocation Reason Code” on page 231.
Reason Description	Enter an optional description that outlines why this block is being allocated.

Policies Tab

The **Policies** tab provides further Child Block configuration options:

Table 3-7 Policies Tab Parameters

Field	Description
Network Links	For use with shared subnets only -- that is, when more than one subnet is attached to the same physical network segment. When using device containers, the physical network links are automatically managed by IPAM. When using logical containers, select the network segment which this subnet will share. Logical network links are defined in Network Links in the DHCP section of the Management menu, as described in “Network Links”.
Default Gateway	The IP Addresses of the default gateway for this subnet (IPv4 only). Used to provide this information to DHCP for Dynamic Address types. You may specify multiple IP Addresses by typing them in a comma-separated format, for example: 192.168.1.1,192.168.1.2 For more information on defining a default gateway, refer to “Defining a Default Gateway”.
Primary DHCP Server	Select the Primary DHCP server that serves this address space.
Failover DHCP Server	Select the Failover DHCP server that serves this address space (IPv4 only). Note that this field is only displayed after DHCP failover is set up under the DHCP server profile’s Failover tab.
Primary WINS Server	The IP Addresses of the Primary WINS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. You may specify multiple IP Addresses by typing them in a comma separated format, for example: 192.168.1.1,192.168.1.2
DHCP Policy Set	Select the default DHCP Policy set to assign to dynamic devices on this subnet.
DHCP Option Set	Select the default DHCP Option set to assign to dynamic devices on this subnet. To create a set specifically for this subnet, select Subnet Specific Option Set . Use the View/Edit link to edit the set.
Effective DHCP Options	Edit Child Block Only. When editing an existing In-Use/Deployed Child Block (that is, a Subnet), a button is available on the Policies tab that shows a popup page displaying the currently saved DHCP options which are effective for this subnet. The effective options for the subnet are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the subnet with options from the current DHCP Option Set assigned to this subnet.
Forward Domains	Click the Add Domains link and select the default DNS Forward domains for this subnet from the DNS Domains screen. If multiple domains are specified, then the default that is used when adding objects is the first one in the list (an arrow appears next to the default).
Reverse Domains	Click the Add Domains link and select the default DNS Reverse domains for this subnet from the DNS Domains screen. This domain is used to hold DNS PTR records. Note that this is optional; if no default is specified, the system automatically calculates the correct reverse zone for DNS PTR records. If multiple domains are specified, the default that is used when adding objects is the first one in the list (an arrow appears next to the default).

Field	Description
DNS Servers	Click the Add DNS Server link and select the default DNS Servers for this subnet from the DNS Servers/Services screen. Used to provide this information to DHCP for Dynamic Address types. If multiple DNS servers are specified, the default that is used when adding objects is the first one in the list (an arrow appears next to the default).

Important Note: For flexibility, IPAM optionally allows for the creation of the same domain name (both forward and reverse) multiple times within the system. It is required that each of these domains be placed in a separate “DNS Domain Type” namespace. An example of this is when you have overlapping private address space being managed by two different DNS servers. It is required that if you are using the same domain name more than once, you must specify the “default domains” on the subnet’s “policies” screen above. This permits the system to place the automatically generated DNS Resource Records in the correct domain(s) for this subnet.

Address Pool Allocation

If you select a Block Status of **In Use/Deployed**, the form displays additional input fields for the creation of **Address Pools**.

This allows you to create **Address Pools** from the newly created block. To do so, select an Allocation Template from the **Allocation Template** field. See “Address Pool Allocation Template” on page 233 for instructions on creating these templates.

After you select a template, the screen refreshes with a new set of rows, one for each row in the template.

Attach Child Block

The **Attach Child Block** function allows for the same block to exist in multiple locations. An attached block is not constrained by the container type so that a block created in a Device container can be attached to a Logical container, and vice versa.

Table 3-8 Attach Child Block Fields

Field	Description
Block Size	Select the CIDR size of the block you wish to attach.
Block Type	Select the Block Type to attach. Note that this list is limited to those block types that have the Blocks of this type can be attached setting selected. It is further limited by the administrator’s Block Type permissions. Refer to “Block Types” for instructions on setting up Attachable block types.

Field	Description
Select Block to Attach	Select the <i>existing</i> block to attach. If you choose the Select Block from List option, the drop-down displays a list of candidate blocks that match the Block Size and Block Type and have an available IP Address. If you choose the Specify Block option, you can type in the starting address of a block. The specified block must match the specified block size and type.

There are several rules that govern when blocks may be attached to each other.

When you try to pick the block from the list, the list is filtered on the following:

- The block type must be marked as Attachable to multiple containers.
- The block type must be allowable in the container to be attached.
- The block size must be allowable in the container to be attached.
- The block must already exist.
- If the block resides in a Logical container, it must be allocated as In Use/Deployed.
 - ▶ There is no restriction on the block status if the pre-existing block resides in a Device container, although it is recommended you only attach In-Use/Deployed blocks together.
- If you do not select a block from the list, the validations are:
 - ▶ The block type must be marked as Attachable to multiple containers.
 - ▶ The block type must be allowable in the container to be attached.
 - ▶ The block must already exist.

Utilization Display

The **Utilization Display** link is used to display the details about the utilization of the selected container. This information is updated each time a Global Utilization Rollup discovery task is performed.

Table 3-9 Utilization Display Screen Elements

Field	Description
	Changes the display format of IPV6 hosts. See “Displaying IPV6 Capacities” on page 15 for more information.
	Edit the properties of this block.
Child Block	The starting address of the child blocks.
Size	The size in CIDR notation of the block.
Utilization	A graph of the current utilization of the block.
Util %	The percentage of this block that is currently utilized.
Usable Hosts	The number of usable hosts that are contained within the current block

Field	Description
Assigned Hosts	The number of hosts that are in use in this block.
Dynamic Hosts	The number of dynamic hosts within the subnet or block. This is inclusive of the “locked” hosts.
Locked	The number of Locked addresses in this block.
Static	The number of Static addresses in this block.
Leasable Hosts	The number of dynamic addresses available to DHCP for allocation.
Lease %	The percentage of dynamic addresses leased to clients.
Subnet Loss	The number of addresses lost due to subdivision of this block.
History	Click this link to display a history graph of the utilization for the current block.

Block Chart

The block chart option allows you to graph the allocations of address space to a specific container. It can be used to quickly visualize the details of the blocks, and to show contiguous areas of space. The chart defaults to a pie chart but you can change the display to a bar chart by selecting **Bar Chart**.

History Chart

The **History Chart** link graphs the history of address space utilization over time for this container. It allows you to visualize overall address space, used space, and provides a forecast of space usage based on the history data.

Table 3-10 History Chart Screen Elements

Field	Description
Forecast	Enter the number of periods (past the current date) that you want to create a forecast for.
Periods	Enter the number of history periods that you want to be included in the graph. Select the “Periods” in the drop-down list. <ul style="list-style-type: none"> • Days – View the history data by days. • Weeks – View the history data by weeks. • Months – View the history data by months. • Years – View the history data by years.
Use Dynamic Data	Checked indicates the data for the graph is filtered to only show data for the Dynamic hosts for the given history period. The days left calculation is also relative to the dynamic host numbers.
Width	The Width in pixels of the graph.
Height	The Height in pixels of the graph.
Zero Min. Y	When checked, always includes zero on the Y axis.

Device Container Functions

Add Site

Use the Add Site screen to select a previously defined site allocation template to apply to the currently selected device container. For more information on creating site allocation templates, refer to “Site Allocation Templates” on page 237.

To add a site with a site allocation template, follow these steps.

1. Select the site allocation template you want to use from the **Site Allocation Template** drop-down list. Only site allocation templates defined for device containers are listed.
A sequenced list of blocks in the selected template appears.
2. Enter block-specific data in the fields, as described in the following table.

Table 3-11 Site Allocation Template Block Parameters

Field	Description
Interface	Select the Interface that the address space will be allocated to from the drop-down list.

Field	Description
SWIP/Net Name	Enter the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE). This is an optional field unless the rules specified on this container require the SWIP/Net Name.
Allocation Reason	Select the reason why this block is being allocated. Reasons are defined by your IPAM administrator. For more information, refer to “Allocation Reason Code” on page 231.
Allocation Reason Description	Enter an optional description that outlines why this block is being allocated.

3. If an address allocation template is included in the site template, select the link and enter any data required for the address template, for example, network service.
4. If user-defined fields are associated with a block, click **UDFs** and enter the required data. Click **Submit** to save the UDF data.
5. Click **Submit**.
The Add Address Pool Details screen closes.
6. Click **Submit**.
The subnet is added to the Address Block Details list.

Add Child Block

When you allocate child blocks on a Device Container, you must assign at least one interface on the network element to an IP address in the child block. If you use an address allocation template to allocate child blocks on a Device Container, IPAM ensures that you do not use a template that would create devices with the same IP addresses as those assigned to the network element interfaces.

When allocating space to a Device container, you must first select the Interface to which the space will be attached, and then specify the Interface Address for that space.

The Add Child Block screen for allocating space to a device container has all the fields that are available for logical containers, with the addition of some device-specific information.

Table 3-12 Additional Device Child Block Fields

Field	Description
Interface	Select the Interface that the space will be allocated to.
Interface IP Address	Number of IP Addresses Choose the number of IP addresses this block will have on this interface. Typically, this will be one. However, there are some high-availability configurations where more than one is needed. If you are not sure, leave this at one.
	Auto allocate Select this radio button to have IPAM calculate the Interface IP Address using the Offset From Start field.
	Offset From Start Use this in conjunction with Auto allocate to have IPAM calculate the Interface Address. If selected, the Interface Address is the Block Starting address plus this Offset.
	Manual Select this radio button if you wish to enter the Interface IP address manually.
	IP Address This field is enabled only when Manual is selected. Fill in the desired Interface IP Address. The supplied address must be within the allocated block and cannot conflict with interface addresses already in use by other devices.
	Default Gateway Select this option to designate that the Interface IP Address is the default Gateway address. For more information, refer to “Defining a Default Gateway” following.

Defining a Default Gateway

IPAM supports three methods that you can use to specify that an interface IP address be designated as the Default Gateway when you allocate a child block:

1. Explicitly list the default gateway IP(s) on the **Subnet Policies** tab (if administrator privileges allow), as described in “Policies Tab” on page 30.

Note: If this method is used, IPAM does not let you use the following two methods.

2. Use an Address Allocation Template with the **Default Gateway** option, as described in “Address Pool Allocation Templates” on page 233.
3. Select the **Default Gateway** checkbox on one or more interface IPs, when allocating a block on a Device Container, as described above in “Add Child Block”.

Methods 2 and 3 can be used together, but with the following restrictions:

- If the IPs allocated by the address template conflict or overlap with the IPs assigned to the network element interfaces, an error is generated.

- If the IPs do not conflict or overlap, then the **Default Gateway** field for the Subnet Policies is populated with the interface IPs in which the **Default Gateway** checkbox is selected, followed by any default gateway IPs created by the address allocation template.

In most cases, the router addresses that are assigned to DHCP clients (that is, the default gateways) are simply the interface IP addresses. In these cases, the **Default Gateway** field on the Subnet Policies screen should be populated with the IP addresses assigned to the network element interfaces.

Attach Child Block

The **Attach Child Block** function allows for the same block to exist in multiple locations. An attached block is not constrained by the container type so that a block created in a Device container can be attached to a Logical container, and vice versa.

The **Attach Child Block** function for Device containers links an *existing* block to a specified interface on the current device container.

Table 3-13 Attach Child Block Fields

Field	Description
Block Size	Select the CIDR size of the block you wish to attach.
Block Type	Select the Block Type to attach. Note that this list is limited to those block types that have the Blocks of this type can be attached setting selected. It is further limited by the administrator's Block Type permissions. Refer to "Block Types" for instructions on setting up Attachable block types.
Select Block to Attach	Select the <i>existing</i> block to attach. If you choose the Select Block from List option, the drop-down displays a list of candidate blocks that match the Block Size and Block Type and have an available IP Address. If you choose the Specify Block option, you can type in the starting address of a block. The specified block must match the specified block size and type.
Attach to Interface	<i>For blocks being attached to Device containers only.</i> Select the Device Interface to which this block will be attached.
Number of IP Addresses	<i>For blocks being attached to Device containers only.</i> Choose the number of IP addresses this block will have on this interface. Typically, this will be one. However, there are some high-availability configurations where more than one is needed. If you are not sure, leave this at one.
Auto allocate	<i>For blocks being attached to Device containers only.</i> Select this radio button to have IPAM calculate the Interface IP Address using the Offset From Start field.

Field	Description
Offset From Start	<i>For blocks being attached to Device containers only.</i> Use this in conjunction with the Auto allocate selection to have IPAM calculate the Interface Address. If selected, the Interface Address will be the Block Starting address plus this Offset. Note: This offset cannot conflict with the Interface Addresses already in use by other devices.
Manual	<i>For blocks being attached to Device containers only.</i> Select this radio button if you wish to enter the Interface IP address manually.
IP Address	<i>For blocks being attached to Device containers only.</i> This field is enabled only when the Manual option is selected. Enter an IP Address for the interface. The address must be within the allocated block and cannot conflict with interface addresses already in use by other devices.
First Available From Start	<i>For blocks being attached to Device containers only.</i> Select this radio button if you wish IPAM to determine the first unused IP address from the beginning of the block to use as the interface address.
First Available From End	<i>For blocks being attached to Device containers only.</i> Select this radio button if you wish IPAM to determine the first unused address from the end of the block to use as the interface address.

There are several rules that govern when blocks may be attached to each other.

When you try to pick the block from the list, the list is filtered on the following things:

- The block type must be marked as Attachable to multiple containers.
- The block type must be allowable in the container to be attached.
- The block size must be allowable in the container to be attached.
- The block must already exist.
- If the block resides in a Logical container, it must be allocated as In Use/Deployed.
 - ▶ There is no restriction on the block status if the pre-existing block resides in a Device container, although it is recommended you only attach In-Use/Deployed blocks together.
- If you do not select a block from the list, the validations are:
 - ▶ The block type must be marked as Attachable to multiple containers.
 - ▶ The block type must be allowable in the container to be attached.
 - ▶ The block must already exist.
 - ▶ The block must be already assigned to a Device container.

Detach a Block

You can detach a child block that has been attached to a device container. Interface IP addresses that are listed in **Interface IP Addresses** are also removed. If a virtual IP address has been attached to the interface, it changes to non-virtual status but remains an interface IP

address. Note that if a virtual IP address is a shared address with more than 2 interfaces, it will remain virtual until it is detached from all interfaces but 1.

To detach a child block, follow these steps.

1. Select the device container from which you want to detach a child block.
2. In Address Block Details, click  beside the block you want to detach.
The Edit Block screen opens.
3. Click **Detach Block**.
4. In response to the confirmation message, click **OK**.
The block is removed from the Address Block Details screen.

Delete a Block

You can delete a child block that has been attached to device containers. Interface IP addresses, along with any virtual addresses will all be removed. Anywhere this block resided will be removed/deleted along with any IPs in the block.

Network Switch Functions

Selecting a network switch icon within the Container Hierarchy causes the display in the right pane to change to a view of the ports that have been discovered on the switch using the “Discover Switch Ports” task in the Discovery/ Collectors section. For more information, refer to “Discovery/Collector Task Definition Options” on page 69.

To view more address information, pause the cursor on an address link. To edit an address, click on the link to open the Edit IP Address screen. For more information, refer to “Edit IP Address” on page 49.

IP Management

Use the Subnet screen to maintain your inventory of IP addresses. In Container View, when you select a block/subnet link with a status of **In-Use/Deployed**, the Subnet screen opens with a complete list of all individual IP addresses within that subnet (if the subnet is an IPv6 subnet, an additional **Add Prefix Pool** link is displayed).

In the Subnet screen, you can perform the following functions:

- Add a new IP address
- Edit an existing IP address
- Delete an IP address
- Add an IP Address Range
- Add/Modify/Delete an IP Address Pool
- Add/Modify/Delete a Prefix Pool (IPv6 blocks only)
- Move Objects
- Export data in PDF/XLS/CSV/XML format

Adding Individual IP Addresses

To add a single IP address in the Subnet screen, follow these steps.

1. Choose one of the following:
 - To define a specific address, select the address link in the IP Address list. The Add IP Address screen opens, and the Address Options drop down has “Manual” selected. Scroll to other tabs as needed.
 - Select the **Add IP Address** link, and choose an option from the Address Options drop down list: Next Available From Subnet Start, Next Available Before Subnet End, Random, or Manual.

The Add IP Address screen opens.

2. On the **General** tab, define the address, as described in Table 3-14 Add IP Address Screen Elements.

Table 3-14 Add IP Address Screen Elements

Field	Description
Subnet	<i>Read only.</i> Displays the subnet that you are currently working within.
Container	<i>Read only.</i> Displays the container that you are currently working within.
General Tab	
Address Options	Determines how the system selects an IP address to add: <ul style="list-style-type: none"> - Next Available from Subnet Start: Selects the first available address in the subnet. - Last Available Before Subnet End: Selects the last available address in the subnet. - Random: Selects a random address in the subnet. - Manual: Allows the user to type in the address they wish to use. - Modified EUI-64 (IPV6 only for blocks with a subnet length less than or equal to 64): Form the address based on the specified MAC as described in RFC 4291.
IP Address	The IP Address that you are adding. Click the Ping button to check if the address is already in use. Note that the ping will be sent by the Discovery Agent assigned to the In-Use/Deployed block or subnet. The Validate button can be used to validate your input. If the input is not a valid IP address, the error message will be displayed. If the entered address is not available, the application will generate the next available after the requested IP address. You can modify the IP address further. Modified EUI-64 option: to generate an IP address the HW Address field must be populated.
Virtual	<i>Read only.</i> Checked if the IP address is being reused because it has been attached to more than one device.

Field	Description
Address Type	<p>Specify the address type to be created.</p> <p>IPv4 only</p> <ul style="list-style-type: none"> • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Manual DHCP – DHCP Address assigned to a specific HW Address, unlimited lease. <p>IPv4 and IPv6</p> <ul style="list-style-type: none"> • Static – Statically addressed device. • Reserved – Reserved for future use. <p>IPv6 only</p> <ul style="list-style-type: none"> • Dynamic NA DHCPv6 – Typical DHCPv6 lease types used by most clients. These are non-temporary addresses requested by the client that are leased for a limited amount of time. • Dynamic TA DHCPv6 – Atypical DHCPv6 lease types used by some clients, most often for PPP or dial-up connections. These are temporary addresses requested by the client that are leased for a limited amount of time. • Automatic NA DHCPv6 – Typical DHCPv6 lease types, most often for PPP or dial-up connections. These are non-temporary addresses requested by the client that are leased for an unlimited amount of time. • Automatic TA DHCPv6 – Atypical DHCPv6 lease types. These are temporary addresses requested by the client that are leased for an unlimited amount of time.
Device Type	Specify the device type being assigned to this IP Address. Device types are created in the Device Types function in the IP/DEVICES section of the Tools menu.
Hostname	The hostname of this device. If you are using Naming Policies, the system generates a unique name based on the policy that you have defined. You may use this generated name, or you may overwrite the system-generated name.
Domain	Select a DNS Domain Name to associate to this device. This list box is initially populated with domains configured in the Subnet Policy, but any domain in the system can be chosen by clicking Search .
Description	Enter a description of this device.
OS	The operating system in use with this device, for example, “Windows 7” or “Red Hat Enterprise Linux 5”.

Field	Description
DUID	<p>Enter the DHCP Unique Identifier that is generated for the device. There are four types of DUID:</p> <ul style="list-style-type: none"> • DUID-LLT - the Link-Layer address of one of the device's network interfaces, concatenated with a timestamp. • DUID-EN - an Enterprise Number plus additional information specific to the enterprise. • DUID-LL - the Link-Layer address of one of the device's network interfaces. • DUID-UUID - a Universally Unique IDentifier (UUID), designed to be used across multi-boot hosts (for example, PXE). <p>Note that all DUIDs are intended to be generated once and stored in stable storage if possible. If there is no stable storage on the device, then it should use DUID-LL.</p>
Interface Name	Enter a name for this interface.
Create Default DNS Resource Records	<p>Checked indicates that the system will automatically create DNS A and PTR records for this object. See the note in this section regarding defining default domains (forward and reverse) for this subnet.</p> <p>Unchecked indicates that you must manually create any DNS records that you may want for this device.</p>
HW Type	Ethernet or Token Ring. If a HW Type is chosen, then a HW Address is mandatory.
HW Address	<i>Mandatory if HW Type is chosen.</i> Enter the MAC Address of this device in hex format.
Exclude from Discovery	Select if you want this address space to be ignored during the discovery process.
Primary DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Primary DHCP server that will serve this address space.
Failover DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Failover DHCP server that will serve this address space.
DHCP Policy Set	<i>Only applicable for Dynamic Address Types.</i> Select the DHCP Policy set to assign to this device. You may choose “—Same As Subnet—” to use the policy set that you have defined at the subnet level.
DHCP Option Set	<i>Only applicable for DHCP address types.</i> Select the DHCP Option set to assign to this device. You may choose “—Same As Subnet—” to use the option set that you have defined at the subnet level. To create a set specifically for this device, select “IP Address Specific Option Set”. Use the View/Edit link to edit the set.

Field	Description
Effective DHCP Options	<i>Edit Only.</i> When editing an existing DHCP address, a button will be available which will show a popup page displaying the currently saved DHCP options which are effective for this address. The effective options for the address are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the address (or subnet, if Same as Subnet) with options from the current DHCP Option Set assigned to the subnet which contains this address, and with the options from the current DHCP Option Set assigned to this address.
User-defined Fields	If any information templates are associated with the chosen device type, then User Defined Fields appear. For more information, refer to “User-Defined Fields” on page 258.

- When you have completed the **General** tab, click on other tabs as needed. Refer to descriptions of each tab in the following sections as you complete your IP address definition.
- After you have provided the necessary information in all the IP Address tabs, click **Submit** to save your changes.

Interfaces Tab

Only available for static addresses. Use the **Interfaces** tab to select the interface that the static IP address will use, as displayed below. The list displays the interface you entered in **Interface Name** on the **General** tab but you can add other interfaces as needed and select one of them instead.

Click **Add Interface** to add an interface to the list.

Refer to Table as you define the interface.

Table 3-15 Add InterfaceScreen Elements

Field	Description
Interface Name	Enter a name for the interface.
Interface Type	Select from Ethernet or Token Ring.
Hardware Address	Enter a physical address for the device
IP Address	Enter the IP address for the device.
Exclude from Discovery	Select if you want this address space to be ignored during the discovery process.
Address Type	Only static addresses are allowed.

Click **Submit** to save your new interface definition.

To use the interface, select the interface in the **Interfaces** tab.

Resource Records Tab

Use the **Resource Records** tab to select or create a resource record for the IP address.

Important Note: For flexibility, IPAM optionally allows for the creation of the same domain name (both forward and reverse) multiple times within the system. It is required that each of these domains be placed in a separate “DNS Domain Type” namespace. An example of this is when you have overlapping private address space being managed by two different DNS servers. If you are using the same domain name more than once, you *must* specify the “default domains” on the subnet’s “policies” screen (see “Add Child Block” on page 27). This permits the system to place the automatically generated DNS Resource Records in the correct domains for this subnet.

To add a new resource record, click **Add Resource Record**. The Add Resource Record screen opens.

To add a resource record, select from the **Resource Record Type** drop-down list. All standard DNS resource record types are available, as well as **OTHER (Other Resource Record)**. You can select this Resource Record type to enter any type of resource record, including experimental options, in a free format text area.

Resource Records and Workflow

If RR Workflow is enabled, when you add or edit a resource record, resource record approval access is checked on the domain for the resource record. If you have the required access, the record is added and is eligible for deployment. If the required access is not granted to you, the record is added in a “Pending” approval state. In this state, it will need an approval from an administrator with resource record approval access on the given domain to be eligible for pushing/deployment. The same behavior applies when you try to edit or delete a resource record. In effect, the Pending Action on a resource record may be ‘Create’, ‘Update’ or ‘Delete’ or empty. An empty value for Pending Action means that the record has been approved or does not require approval.

Aliases Tab

If you select a Domain on the **General** tab, the **Aliases** tab appears.

To add an alias, click the **Add Alias** link. The following screen appears where you enter a new alias and select a domain from the **Select domain** drop-down list. To search additional domains, click the **Search** button and select the domain you want from the **DNS Domains** screen. This step is equivalent to creating a CNAME resource record which points to the hostname of the device being edited. Once added, the CNAME record can be seen in the Resource Record tab of the same device.

To save the alias, click **Submit**.

Edit IP Address

An individual IP Address may be edited using the links on the Subnet display.

You can change the properties on the main page and/or various tabs and click **Submit** to save the changes. All the changes from various tabs are collected as one record and saved when you click **Submit**.

When RR workflow is enabled, changing the IP Address, Domain or Hostname on the **General** tab is not allowed if there are resource records associated with the IP Address that are pending approval. When you try to submit such a change, a message is displayed indicating that the pending changes need to be approved or rejected before proceeding with further changes.

Editing Interface Address Types

The following rules apply when you are editing addresses with an Interface address type:

1. The IP address cannot be deleted using the Subnet list, as you can with other existing IP addresses.
2. The Address Type cannot be modified.
3. Interface addresses are removed when the block is detached from a Device container. Virtual interface addresses, however, may remain after the block is detached.
4. The Interface IP address itself cannot be changed on the Edit IP Address screen. Instead, use the Edit Block screen for a device container.

Editing Resource Records

Resource records can be edited by clicking on the link inside the **Owner** field.

In the case where RR Workflow is enabled:

- If an approver edits a resource record that is pending approval, their change is saved. The disposition of the pending change depends on the state and pending action on the resource record as detailed in “Resource Records and Workflow” on page 47.
- If a non-approver edits a resource record that is pending approval, their change is saved but the record remains in the pending state.

Net Elements Tab

The **Net Elements** tab is displayed only for addresses with an address type of Interface that were added by Add Child Block and Attach Child Block to a device container. All the associated network elements for the IP address are listed.

To edit a network element, select it in the **Network Element** list. The Edit Network Element screen is displayed. For more information, refer to “Network Elements/Devices” on page 82.

Ports Tab

The **Ports** tab displays read only information gathered during a Discover task. It displays the interface this IP address is associated with, and the switch and port where the device was discovered.

Adding a Range of IP Addresses

Use the **Add IP Range** option to add a range of IP Address that share common attributes within the system. This option creates multiple individual IP Addresses (as opposed to a pool of addresses), which allows you to maintain the details of each device if needed.

Table 3-16 Add IP Range Screen Elements

Field	Description
Address Options	Determines how the system selects a range of IP addresses to add: <ul style="list-style-type: none"> - Next Available from Subnet Start: Selects the first available address range in the subnet. - Last Available Before Subnet End: Selects the last available address range in the subnet. - Random: Selects a random address range in the subnet. - Manual: Allows the user to type in the address range they wish to use.
Start Address	Enter the starting IP Address within the range that you are adding. Note: You can only add a range of IP Addresses within a subnet. You cannot create a range that spans subnets or overwrites in-use IPs.
End Address	Enter the ending IP Address within the range that you are adding.
Range Size	Enter the number of IP Addresses to create. For example, if the “Start Address” was 10.0.0.1, and the “Size” is 3, then the following IP Addresses will be created: 10.0.0.1, 10.0.0.2, 10.0.0.3. Clicking “Generate” will populate the address fields based on the value of the “Address Options”.

Field	Description
Address Type	<p>Specify the address type to be created.</p> <p>IPv4 only</p> <ul style="list-style-type: none"> • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Manual DHCP – DHCP Address assigned to a specific HW Address, unlimited lease. <p>IPv4 and IPv6</p> <ul style="list-style-type: none"> • Static – Statically addressed device. • Reserved – Reserved for future use. <p>IPv6 only</p> <ul style="list-style-type: none"> • Dynamic NA DHCPv6 – Typical DHCPv6 lease types used by most clients. These are non-temporary addresses requested by the client that are leased for a limited amount of time. • Dynamic TA DHCPv6 – Atypical DHCPv6 lease types used by some clients, most often for PPP or dial-up connections. These are temporary addresses requested by the client that are leased for a limited amount of time. • Automatic NA DHCPv6 – Typical DHCPv6 lease types, most often for PPP or dial-up connections. These are non-temporary addresses requested by the client that are leased for an unlimited amount of time. • Automatic TA DHCPv6 – Atypical DHCPv6 lease types. These are temporary addresses requested by the client that are leased for an unlimited amount of time.
Device Type	Specify the Device Type being assigned to these IP Addresses. Device Types are created in the Tools menu.
DHCP Policy Set	<i>Only applicable for Dynamic Address Types.</i> Select the DHCP Policy set to assign to these devices. You may choose —Same As Subnet— to use the policy set that you have defined at the subnet level.
DHCP Option Set	<i>Only applicable for Dynamic Address Types.</i> Select the DHCP Option set to assign to these devices. You may choose —Same As Subnet— to use the option set that you have defined at the subnet level.
Primary DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Primary DHCP server that will serve this address space.
Failover DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Failover DHCP server that will serve this address space.
Example Host Name:	<i>Read Only:</i> Example hostname that will be generated for each IP Address based on a specified naming policy. If you are using Naming Policies, the system generates a unique name based on the policy that you have defined for each IP Address.
Domain	Select a DNS Domain Name to associate to these devices. Use Search to search for any domain defined within the system.

Field	Description
Create A Records for All	Checked indicates that the system will automatically create “A” DNS records for each object. See note below. Unchecked indicates that you must manually create any “A” DNS records that you may want for these objects.
Create PTR Records for All	Checked indicates that the system will automatically create “PTR” DNS records for each object. See note below. Unchecked indicates that you must manually create any “PTR” DNS records that you may want for these objects.
Ignore Duplicate Warnings	If the policy Allow Duplicate Hostname Checking or Allow Duplicate A Record (Owner) Checking for the administrator is set to Warn, adding the IP Address will fail if any duplicate warnings occur unless you select this option to ignore any duplicate warnings.

Important Note: For flexibility, IPAM optionally allows for the creation of the same domain name (both forward and reverse) multiple times within the system. It is required that each of these domains be placed in a separate “DNS Domain Type” namespace. An example of this is when you have overlapping private address space, being managed by two different DNS servers. It is required that if you are using the same domain name more than once, then you must specify the “default domains” on the subnet’s Policies screen (refer to “Add Child Block” on page 28). This permits the system to place the automatically generated DNS Resource Records in the correct domains for this subnet.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding an IP Address Pool

Use the **Add IP Address Pool** option to add an IP Address Pool to the system. An Address Pool encompasses a range of IP addresses, but unlike individual IP addresses, you manage the attributes of a Pool as a whole.

For example, if you create an IP Address Pool from 10.0.0.1-10.0.0.10, you cannot change the attributes of the individual IP Addresses. When you change the attribute of an IP Address Pool, the change affects all IP addresses within that pool. IP Address Pools are very helpful when you are creating large DHCP address pools or scopes, or creating large blocks of “static” or “reserved” space, that you do not need to individually manage.

IPv4 Address Pool

If you select **Dynamic DHCP** or **Automatic DHCP** for the **Address Type** and select a primary DHCP server, additional DHCP-specific fields are displayed.

Table 3-17 Add IPv4 Address Pool Screen Elements

Field	Description
Address Options	Determines how the system selects a pool of IP addresses to add: <ul style="list-style-type: none"> - Next Available from Subnet Start: Selects the first available address pool of the specified length in the subnet. - Last Available Before Subnet End: Selects the last available address pool of the specified length in the subnet. - Random: Selects a random address pool of the specified length in the subnet. - Manual: Allows the user to type in the address pool they wish to use.
Start Address	Enter the starting IP Address of the pool that you are adding. Note: You can only add a pool of IP Addresses within a subnet. You cannot create a pool that spans subnets.
End Address	Enter the ending IP Address of the pool that you are adding.
Name	Enter a unique name for this Address Pool. The default name is <StartAddress>-<EndAddress>.
Size	Enter the number of IP Addresses to create. For example, if the “Start Address” was 10.0.0.1, and the “Size” is 3, then the following IP Addresses will be included in the pool (10.0.0.1, 10.0.0.2, 10.0.0.3). If “Next Available”, “Last Available”, or “Random” is selected as the Address Option, then clicking the generate button after selecting a size will calculate the IP address pool addresses to use.
Address Type	Specify the address type to be created. <ul style="list-style-type: none"> • Static – Statically addressed device. • Reserved – Reserved for future use. Note: The above address types are only allowed on individual addresses. <ul style="list-style-type: none"> • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Manual DHCP – DHCP Address assigned to a specific HW Address, unlimited lease.
DHCP Policy Set	Only applicable for Dynamic Address Types. Select the DHCP Policy set to assign to these devices. You may choose “—Same As Subnet—” to use the policy set that you have defined at the subnet level.
DHCP Option Set	Only applicable for DHCP address types. Select the DHCP Option set to assign to these devices. You may choose “—Same As Subnet—” to use the option set that you have defined at the subnet level. To create a set specifically for this address pool, select “Address Pool Specific Option Set”. Use the View/Edit link to edit the set.

Field	Description
Effective DHCP Options	<i>Edit Only.</i> When editing an existing address pool, a button will be available which will show a popup page displaying the currently saved DHCP options which are effective for this address pool. The effective options for the address pool are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the address pool (or subnet, if Same as Subnet) with options from the current DHCP Option Set assigned to the subnet which contains this address pool, and with the options from the current DHCP Option Set assigned to this address pool.
Primary DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Primary DHCP server that will serve this address space. The servers listed are IP version specific. For example, for an IPv4 address, only IPv4 DHCP servers and DHCP servers supporting 'IPv4 and IPv6 both' are listed.
Failover DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Failover DHCP server that will serve this address space. The servers listed are IP version specific.
Allow Client Classes	<i>Only applicable for Dynamic Address Types.</i> Select the client classes that are ALLOWED to receive an IP Address from this pool. Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.
Deny Client Classes	<i>Only applicable for Dynamic Address Types.</i> Select the client classes that are DENIED from receiving an IP Address from this pool. Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

IPv6 Address Pool

Selecting **Add IP Address Pool** displays.

If you select **Dynamic/Automatic NA DHCPv6** or **Dynamic/Automatic TA DHCPv6** for the **Address Type** and select a primary DHCPv6 server, additional DHCP-specific fields are displayed.

Table 3-18 Add IPv6 Address Pool Screen Elements

Field	Description
Address Options	Determines how the system selects a pool of IP addresses to add: <ul style="list-style-type: none"> - Next Available from Subnet Start: Selects the first available address pool of the specified length in the subnet. - Last Available Before Subnet End: Selects the last available address pool of the specified length in the subnet. - Random: Selects a random address pool of the specified length in the subnet. - Manual: Allows the user to type in the address pool they wish to use.

Field	Description
Start Address	Enter the starting IP Address of the pool that you are adding. Note: You can only add a pool of IP Addresses within a subnet. You cannot create a pool that spans subnets.
Name	Enter a unique name for this Address Pool. The default name is <StartAddress>/<Size>.
Size	Pools must reside on a CIDR/octet boundary. To add an address pool to a V6 block, select a block size up to /128 from the dropdown list. If “Next Available”, “Last Available”, or “Random” is selected as the Address Option, then clicking the generate button after selecting a size will calculate the IP address pool addresses to use.
Address Type	Specify the address type to be created. <ul style="list-style-type: none"> • Static – Statically addressed device. • Reserved – Reserved for future use. Note: The above address types are only allowed on individual addresses. <ul style="list-style-type: none"> • Dynamic NA DHCPv6 – Typical DHCPv6 lease types used by most clients. These are non-temporary addresses requested by the client that are leased for a limited amount of time. • Dynamic TA DHCPv6 – Atypical DHCPv6 lease types used by some clients, most often for PPP or dial-up connections. These are temporary addresses requested by the client that are leased for a limited amount of time. • Automatic NA DHCPv6 – Typical DHCPv6 lease types, most often for PPP or dial-up connections. These are non-temporary addresses requested by the client that are leased for an unlimited amount of time. • Automatic TA DHCPv6 – Atypical DHCPv6 lease types. These are temporary addresses requested by the client that are leased for an unlimited amount of time.
DHCP Policy Set	Only applicable for Dynamic Address Types. Select the DHCP Policy set to assign to these devices. You may choose “—Same As Subnet—” to use the policy set that you have defined at the subnet level.
DHCP Option Set	Only applicable for DHCP address types. Select the DHCP Option set to assign to these devices. You may choose “—Same As Subnet—” to use the option set that you have defined at the subnet level. Note: “Address Pool Specific Option Set” only applies to IPv4 address pools.
Effective DHCP Options	Edit Only. When editing an existing address pool, a button will be available which will show a popup page displaying the currently saved DHCP options which are effective for this address pool. The effective options for the address pool are determined by combining DHCP options from the option set assigned to the current Primary DHCP Server for the address pool (or subnet, if Same as Subnet) with options from the current DHCP Option Set assigned to the subnet which contains this address pool, and with the options from the current DHCP Option Set assigned to this address pool.

Field	Description
Primary DHCP Server	<i>Only applicable for Dynamic Address Types.</i> Select the Primary DHCP server that will serve this address space. The servers listed are IP version specific. For example, for an IPv4 address, only IPv4 DHCP servers and DHCP servers supporting 'IPv4 and IPv6 both' are listed.
Allow Client Classes	<i>Only applicable for Dynamic Address Types.</i> Select the client classes that are ALLOWED to receive an IP Address from this pool. Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.
Deny Client Classes	<i>Only applicable for Dynamic Address Types.</i> Select the client classes that are DENIED from receiving an IP Address from this pool. Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.
Overlap Interface IP	<i>Only applicable for Dynamic Address Types.</i> Flag to allow the DHCPv6 pool to overlap an interface address. This is enabled only if the pool is managed by a CNR DHCPv6 server.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a Prefix Pool

In IPv6 networking, use the Add Prefix Pool option to create an IPv6 Prefix Delegation pool for a delegating router. The delegating router uses this pool to delegate (sub) prefixes (delegated prefixes) to the requesting router.

The Add Prefix Pools screen opens.

Refer to the following table for information on the fields.

Table 3-19 Add Prefix Pool Screen Elements

Field	Description
Address Options	Determines how the system selects a pool of IP addresses to add: <ul style="list-style-type: none"> - Next Available from Subnet Start: Selects the first available prefix pool of the specified length in the subnet. - Last Available Before Subnet End: Selects the last available prefix pool of the specified length in the subnet. - Random: Selects a random prefix pool of the specified length in the subnet. - Manual: Allows the user to type in the address of the prefix pool they wish to use.
Start Address	Enter the starting IP Address of the pool that you are adding.

Field	Description
Size	<p>Select the prefix pool size from the drop-down list. It is recommended that prefixes be split on 4-bit boundaries, so if you were to delegate prefixes of size /64, you would have a pool of at least size /60, or perhaps /56. If your delegated prefixes were of size /48, then you would create a prefix pool of at least /40, or perhaps /36.</p> <p>Note: Although ISC and CNR servers have different ways of specifying the prefix address in conf files (ISC states the start and end address whilst CNR states the start address and prefix/size), IPAM limits the prefix address to be only on CIDR boundaries and calculates the end address based on start address and size.</p> <p>If “Next Available”, “Last Available”, or “Random” is selected as the Address Option, then clicking the generate button after selecting a size will calculate the prefix pool address to use.</p>
Name	Enter a unique name for this Prefix Pool. The default name is <StartAddress>/<Size>.
Address Type	<p>Specify the address type to be created:</p> <ul style="list-style-type: none"> • Dynamic PD DHCPv6 – DHCPv6 IP Address with a lease • Automatic PD DHCPv6 – DHCPv6 IP Address unlimited lease
Delegated Prefix Length	Enter the default delegated prefix length for this prefix pool.
Shortest Prefix Length	<i>CNR DHCPv6 only.</i> Enter the shortest delegated prefix length allowed for this prefix pool.
Longest Prefix Length	<i>CNR DHCPv6 only.</i> Enter the longest delegated prefix length allowed for this prefix pool.
Primary DHCP Server	Select the Primary DHCPv6 server that will serve this address space.
DHCP Policy Set	Select the DHCP Policy set to assign to these devices. You can choose “—Same As Subnet—” to use the policy set that you have defined at the subnet level.
DHCP Option Set	Select the DHCP Option set to assign to these devices. You can choose “—Same As Subnet—” to use the option set that you have defined at the subnet level.
Effective DHCP Options	Click Show Currently Saved DHCP Options to review the DHCP options that are currently in effect for the selected server.
Allow Client Classes	<p><i>Only applicable for Dynamic Address Types.</i> Select the client classes that are ALLOWED to receive an IP Address from this pool.</p> <p>Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.</p>
Deny Client Classes	<p><i>Only applicable for Dynamic Address Types.</i> Select the client classes that are DENIED from receiving an IP Address from this pool.</p> <p>Note: The selected Client Class must also be assigned to the DHCP server within the DHCP server definition.</p>
Overlap Interface IP	<i>Only applicable for Dynamic Address Types.</i> Flag to allow the DHCPv6 pool to overlap an interface address. This is enabled only if the pool is managed by a CNR DHCPv6 server.

After a discovery task (Collect DHCP Utilization), you can review delegated prefixes by clicking the  icon next to a prefix pool in an IPv6 subnet list. Such pools are identified as either Dynamic or Automatic PD DHCPv6 address types.

To edit a prefix pool, select the prefix pool link that you want to modify. The Edit Prefix Pool screen opens where you can modify fields.

Show Dynamic Leases

Use the **Dynamic Leases** tab to view DHCP lease information that has been collected from the DHCP server. Collecting active lease information is accomplished through the **Discovery** option in the IPAM section of the **Management** menu. For more information, refer to “Discovery” on page 68.

Show Only Leased Addresses checkbox: If this checkbox is checked, only active leases (IP Addresses with status "Leased" and Lease End time greater than the current time) are shown.

The Release button can be used to send a DHCP Release packet to the DHCP server from which the leases were collected. For DHCPv4, the Release will be sent by the Executive Agent to the DHCPv4 server (this is because DHCPv4 servers do not listen on the loopback interface, and therefore will ignore packets that are sent by the Agent assigned to the DHCPv4 server). For DHCPv6, the Release will be sent by the Agent assigned to the DHCPv6 server. Note that DHCP Collection task must be run again to update the IPAM GUI with the new lease information after the Release has been issued.

Table 3-20 Show Dynamic Leases Screen Elements

Field	Description
IP Address	The IP Address of this lease record.
Host Name	The hostname of this device as defined within IPAM.
Domain Name	The Domain name of this device as defined within IPAM.
HW Address	The MAC Address of this device in hex format.

Field	Description
Address Type	<p>The address type of this lease:</p> <p>IPv4:</p> <ul style="list-style-type: none"> • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Manual DHCP – DHCP IP address that has been directly assigned to this client via MAC address. <p>IPv6:</p> <ul style="list-style-type: none"> • Dynamic NA DHCPv6 – Non-temporary address requested by the client, leased for a limited amount of time. • Dynamic TA DHCPv6 – Temporary address requested by the client, leased for a limited amount of time. • Automatic NA DHCPv6 – Non-temporary address requested by the client, leased for an unlimited amount of time. • Automatic TA DHCPv6 – Temporary address requested by the client, leased for an unlimited amount of time.
Device Type	The Device Type being assigned to this IP Address. Device Types are created in Tools > IP/Devices > Device Types .
Device Status	The current Device Status.
Lease Start	The lease start time for this IP Address.
Lease End	The lease end time for this IP Address.
Client Hostname	The hostname of the device as it was collected directly from the active lease file.
Last Update	The last date/time that this lease record was updated.
Circuit ID	The value of the relay agent circuit ID (if any) as it was collected directly from the active lease file.
Remote ID	The value of the relay agent remote ID (if any) as it was collected directly from the active lease file.

Planned vs Actual

Use the **Planned vs Actual** tab to view planned vs. actual of what has been defined within IPAM vs. what has been discovered on the subnet using the integrated discovery agent. You must first run a discovery task against this subnet to populate this screen. You can then selectively choose which updates you want to apply.

You can use this option to effectively find and record devices that appear on the network without knowledge or assignment of the IPAM administrator. For updates on existing devices, the discovery may yield updates for devices that are pending approval. Such devices will not be updated from the Planned vs Actual tab. Users see a message indicating that the records should be approved/rejected before the update can be applied. If a non-approver is doing the update from the Planned vs Actual tab, the update happens but the record is pending approval.

Click  to save any changes you have made, or  to refresh the display.

Subnet/Block View

The Subnet/Block View option allows you to view and manage IP Address space by CIDR block. This feature allows you to quickly see how a specific CIDR block has been allocated throughout your network.

Understanding the screen layout

When you select **Subnet/Block View** from the IPAM section of the **Management** menu, a view of your address blocks is available in the left frame of your browser. You can select individual blocks and drill down into child blocks that are derived from the CIDR block. On the right side of the screen, you see details about the block that is currently selected in the tree view in the left frame.

In the **Detailed Block View** frame, the details about the specific block that is selected in the block tree are displayed.

The top of the display shows the details about the current block, such as size, name and status.

Table 3-21 Block View Screen Elements

Field	Description
Block	The starting address of the CIDR block.
	Edit the properties of this block.
Size	The size in CIDR notation of the block.
Status	The current status of this block: <ul style="list-style-type: none"> • Free – The block is available for use or allocation. • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP addresses are fully utilized. • Reserved – This block is reserved for future use.
Usable	The number of usable IP addresses in this block.
Assigned	The number of hosts that have been assigned (are in use) in this block.
Available	The number of hosts in this block that are available to be assigned.
Utilized	The percent of the block that is used.
User Defined Fields	The User Defined Fields affiliated with this block
	Displayed when IPV6 address pools are listed. Used to change the display format of IPV6 hosts. See “Displaying IPV6 Capacities” on page 15 for more information.

The bottom of the display shows the details about any child blocks that have been derived from this block.

Table 3-22 Children Block Details Screen Elements

Field	Description
Block	The starting address of the CIDR block.
	Edit the properties of this block.
Size	The size in CIDR notation of the block.
Status	The current status of this block: <ul style="list-style-type: none"> • Free – The block is available for use or allocation. • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP addresses are fully utilized. • Reserved – This block is reserved for future use.
Name	The name that has been assigned to this block. By default, IPAM sets the name to the address/size.
Container	The name of the container that holds this block.
Usable	The number of usable IP addresses in this block.
Assigned	The number of hosts that have been are in use in this block.

Field	Description
Available	The number of hosts in this block that are available to be assigned.
Utilized	The percent of the block that is used.
User Defined Fields	The User Defined Fields affiliated with the block.

Editing Blocks

Note the edit icon () next to the block address. Click on the edit icon to see the Edit Block page.

The Edit Block screen varies, depending on whether you are viewing a Root Block or a Child Block.

Root Block

Use this form to edit the root block, and to perform other operations on it.

Table 3-23 Edit Root Block Screen Elements

Field	Description
Block Name	The Name of the block. This defaults to the Address/Size. If you edit this, the address and size do <i>not</i> change, just the name.
Block Description	A description field for your use.
Current Status	Root blocks can only be type Aggregate.
Primary Subnet	<i>Applicable to Device Container Only.</i> Checkbox to indicate this is the primary subnet.
Interface IP Address	<i>Applicable to Device Container Only.</i> Listing of the interface IP addresses created by the Add Child Block and Attach Child Block functions. <ul style="list-style-type: none"> • Container – The device container to which the IP address belongs. • Interface – The interface on which this address was added or attached. • IP Address – The IP Address hyperlink allows you to edit or delete the address. Note that an IP Address in this context can only be deleted if there is more than one.
SWIP/Net Name	For Internet Registry reporting.
Reason for Allocation	Populated if an Allocation Reason was specified when the block was created.
Internet Registry	Choose the Internet Registry this address was allocated from, or leave as Generic Root Block for private space.
Organization ID	Default is None . Select an ID that has already been defined in Tools > Subnet/Block > RIR Organization IDs .
Block Type	The current Block Type.
Address Space	The block starting address.
Block Size	The CIDR Size.
Number of Addresses	The total addresses in the block.
Start Address	The first usable address in the block.
End Address	The last usable address in the block.
Parent Block	The parent block from which this block was created.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	There are three options for selecting the Discovery Agent: <ul style="list-style-type: none"> • Inherit from Parent Block – Inherits the Discovery Agent from the Parent Block • Inherit from Parent Container - Inherits the Discovery Agent from the Parent Container • Select Agent – Allows user to select Discovery Agent from the system list of Agents.
Root Block	Indicates whether this is a Root Block or not.

Field	Description
Allow Overlapping Address Space	If checked, this block can co-exist with another that overlaps its address range, as long as the overlapping block is not in the same container, or any of its parent containers.
Created On	The block creation date.
Last Modified on	The date/time of last modification.
Last Modified by	The administrator who last changed the block.

At the bottom of the form, a row of buttons allows you to perform several operations on blocks. Some of these buttons might be suppressed if the operation is not applicable. For more information, see the following sections of this chapter.

Child Block

Table 3-24 Child Block Screen Elements

Field	Description
General	General information about the block.
Block Name	The Name of the block. This defaults to the Address/Size. If you edit this, the address and size do <i>not</i> change, just the name. The block name will then appear in the block list.
Block Description	A description field for your use.
Current Status	Choose one of Aggregate, Reserved, Free, In-Use/Deployed, In-Use/Fully Assigned. Note that your choices might be constrained according to how the block was allocated. In some cases you will not be able to change the Status once assigned (that is, you cannot later change an In-Use block to Aggregate).
Primary Subnet	<i>Applicable to Device Container Only.</i> Checkbox to indicate this is the primary subnet.
Non-Broadcast	When True, indicates that this block is not in a broadcast domain. As such the subnet and broadcast addresses (i.e., the first and last address in the block) are available for assignment. Typically this flag is set to False. This flag is only valid for IPv4 In Use/Deployed blocks.
Interface IP Address	This appears for Device Containers. It displays the Containers, Interfaces, and IP Addresses in use for this block.
SWIP/Net Name	For Internet Registry reporting.
Reason for Allocation	Populated if an Allocation Reason was specified when the block was created.
Organization ID	Not selectable in a child block.
Block Type	The current Block Type.
Address Space	The block starting address.
Block Size	The CIDR Size.
Number of Addresses	The total addresses in the block.
Start Address	The first usable address in the block.

Field	Description
End Address	The last usable address in the block.
Parent Block	The parent block from which this block was created.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	There are three options for selecting the Discovery Agent: <ul style="list-style-type: none"> • Inherit from Parent Block – Inherits the Discovery Agent from the Parent Block • Inherit from Parent Container - Inherits the Discovery Agent from the Parent Container • Select Agent – Allows user to select Discovery Agent from the system list of Agents.
Root Block	Indicates that this is not a root block.
Allow Overlapping Address Space	Indicates whether overlapping address space is allowed.
Created On	The block creation date
Last Modified On	The date/time of last modification
Last Modified By	The administrator who last changed the block
Allocation Template	The name of a template to be applied to a Deployed block, or to be applied when modifying the block status to Deployed. See “Address Pool Allocation Template” on page 233 for instructions on creating these templates.
Policies	Policy settings used when defining individual IP addresses in this block and when generating DHCP configuration files.
Vlans	Provides read-only VLAN details when a Switch Discovery runs and updates the database successfully.

At the bottom of the form, there is a row of buttons that allow you to perform several operations on blocks. Some of these buttons might be suppressed if the operation is not applicable. For more information, see the following section of this chapter.

Delete Block

Click this button to delete the block from the system. You are prompted for a confirmation. When you delete a block, IPAM automatically reclaims free space, and merges adjacent free space into larger blocks.

Split Block

Click this button to split the current block into smaller pieces. You see the screen below:

Select the size of the smallest block you need. IPAM keeps the remaining blocks as large as possible while ensuring the smallest block size is available.

Join Block

Click this button to merge the current block with an adjacent block of the same size.

To be successful, the combined block must satisfy the following criteria:

- Must be of identical size
- Must be contiguous
- Must reside in the same container
- Must have the same block type

Move Block

This operation moves the current block to a new container.

Select the target container. If you select a Device container, another field appears for the target Interface. Click **Submit** to move the block. Note that the Block must be allowed in the target container, according to its Block Type rules. In addition, you cannot move blocks between Logical and Device containers.

If using the feature of IPAM where you attach network services (DHCP servers) to containers, then you can optionally select a DHCP server, which is valid for the target container, to be assigned to any subnets, address pools, or individual devices in the block being moved which are assigned to a DHCP server that would no longer be valid as a result of the move.

Block type edit

A block's block type may be changed under certain conditions. A block type must first be accessible to the current user for it to be available as the new block type. Rules governing Block Type access can be found in "Block Type Access" on page 266. Below are the conditions when a block's block type can be edited and to what block types it can be changed.

Business rules governing *when* a block's block type may be modified:

- A block's block type may be modified when it contains no children *or* only children of block status 'Free'.

Business rules governing *what* block types are available to a block being modified:

- Only block types allowed by rules governed by Admin ACLs are available.
- The block type of a root block can be modified to any block type in the system, as long as the container it resides in is configured to allow it as a root block type.
- The block type of a non-root block can be modified to its parent's block's block type or this block type's children.

Block type edit example

Assume the following block types are defined in the system, the current user has no Admin ACL restrictions, and the block's block type may be modified.

- A root block could be changed to any block type in the system, as long as the container is configured for that block type (in the **Allow Root Block Creation** tab in Container Maintenance).
- A child block whose parent's block's block type is 'Any' could be changed to:
 - ▶ Any
 - ▶ Any_East
 - ▶ Any_West
 - ▶ Private
- A child block whose parent's block's block type is 'Any_East' could be changed to:
 - ▶ Any_East
 - ▶ 3rdGen

Pending Approvals

The Pending Approvals menu item only exists when either Resource Record or Device Workflows are enabled and pending records exist in the system. Otherwise this functionality does not apply. The Pending Approvals screen allows you to view two sets of data related to device workflow:

- Devices that require your approval
- Devices you have submitted for approval

You can filter the display results by the Create and Delete actions. If there are Internationalized Domain Names, an  icon appears on the far right of the display, where you can select how you want the Domain Name column to be displayed.

To access the Pending Approvals screen, select **Pending Approvals** from the IPAM section of the **Management** menu. In the case of Device Workflow being enabled, a list of device changes submitted for your approval appears in the **My Approvals** tab.

My Approvals

Refer to Table 3-25 for a description of the columns in the **My Approvals** tab.

Table 3-25 My Approvals Columns

Field	Description
IP Address	The IP address assigned to the device.
Host Name	The host name of the device.
Domain Name	The domain on which the device is located.
HW Address	The MAC address of the device.
Type	The IP address type.

Field	Description
Device Type	The device type assigned to the device. Device Types are maintained in the IP/DEVICES section of the Tools menu.
Description	The description (if any) that was entered for the device.
Date/Time	Date and time of the action that was performed on the device.
Block	The block where the device is located.
Container	The container where the device is located.
Action	The action that is awaiting approval (that is, Create, Delete or Update)
Approvers	<i>My Submissions tab only.</i> Click  to display the Login ID of the administrator who can approve the action taken on the device. Click  to remove the name from the display.
Admin	<i>My Approvals tab only.</i> Displays the Login ID of the administrator that last modified the device.

You can take the following actions on changes that require your approval:

To ...	Then ...
Approve a submission	<ol style="list-style-type: none"> 1. Select the actions that you want to approve. 2. Click . The Approval Reason dialog opens. 3. Enter up to 256 alphanumeric characters to indicate why you approve the action taken on the selected devices. 4. Click Save.
Reject a submission	<ol style="list-style-type: none"> 1. Select the actions that you want to reject. 2. Click . The Rejection Reason dialog opens. 3. Enter up to 256 alphanumeric characters to indicate why you reject the action taken on the selected devices. 4. Click Save.
Review more details of a specific entry	<ol style="list-style-type: none"> 1. Select the IP address link of the device. The Edit IP Address screen opens. 2. Choose from the following actions: <ol style="list-style-type: none"> a. To approve, click Approve. The Approval Reason dialog opens. Enter up to 256 alphanumeric characters to indicate why you approve of the action taken on the device and click Approve. b. To reject, click Reject. The Rejection Reason dialog opens. Enter up to 256 alphanumeric characters to indicate why you reject the action taken on the selected devices and click Reject.

My Submissions

To review the device changes that you have submitted for approval from another administrator, select the **My Submissions** tab.

Discovery

The Discovery option allows you to create on-demand, scheduled, or recurring scheduled tasks for collection of utilization, configuration information on network devices (such as routers), and host information on your network. IPAM can capture the following actual configuration information and then compare it with the planned view that is defined in the database:

- Network elements (such as which subnets have been configured on a router)
- Network services (such as what address pools are configured on a DHCP server)
- Hosts on a specific subnet
- IP and MAC addresses (by scanning the ARP table on network elements, such as routers and switches)
- Ports configured on a network switch including port names, speeds, VLAN membership, and devices attached to the ports

Discovery/Collector Task Definition Options

To collect host, configuration, or utilization information from the network, select the “task type”, “network element” or “network service”, and then specify when to run the task. Depending upon the selection of when you will be running the task, different options will be displayed on the screen for you to select. Refer to the sections below for additional information about each option. Note that once you click **Submit**, a new task is created, and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Table 3-26 Discovery/Collector Task Definition Screen Elements

Field	Description
Task Type	<p>Select the type of task that you would like to run.</p> <ul style="list-style-type: none"> • Collect DHCP Utilization collects utilization information from the DHCP server by address pool. Note that Fully Qualified Domain names can be collected for Windows 2003/2008 DHCP servers, but not MS Windows 2000 Servers. • Discover Router Subnets discovers subnets for an individual Network Element or all Network Elements, using SNMP to query the router. Receives information on interfaces, network address, network size and creates a snapshot in the database. • Discover Switch Ports collects information about the ports defined on a network switch or all of the switches defined within a branch of the container hierarchy. • Discover Subnet Hosts discovers the hosts that are connected

Field	Description
	<p>to a single subnet, or all the hosts for all subnets within a Container.</p> <ul style="list-style-type: none"> • Discover V4 and V6 Router ARP Hosts discovers V4 and V6 hosts that are connected to a network element such as a router or switch, by scanning the ARP tables defined on the element. If a container scope is selected, discovers all hosts on all subnets on all network elements below the selected container in the container hierarchy. • Global Utilization Rollup performs the rollup of all utilization data. This includes the following steps: <ul style="list-style-type: none"> ○ Address Pool utilization rolled into associated blocks. ○ Block utilization rolled up into root blocks. ○ All block utilization rolled into container utilization by block type (and interface for device containers) ○ Address pool history snapshot taken ○ Block history snapshot taken ○ Container history snapshot taken ○ Address pool days left regression ○ Block days left regression ○ Block and Address Pool Threshold checks • Global Synchronization of DHCP Servers collects utilization information from all DHCP servers that participate in Global Synchronization, that is, have the Include during Global Synchronization Task field checked. • Global Synchronization of Network Elements discovers all Network Elements that have the Include during Global Synchronization Task field checked. Used to query the current state of the network and perform difference analysis to compare actual deployment with the topology modeled in IPAM.
The following options are based on which type of task is selected	
Container	Select Search and select a container to perform this task against.
Create History Records	Check this option to create history records as a part of the task.
Ignore Duplicate Warnings	If duplicate host name information is found while adding new hosts, you can choose this option to ignore any warnings.
Include Alert Threshold Checking	Check this option to include alert threshold checking during the task process.
Lookup Hostname	Check this option to perform a DNS lookup during host discovery.
Network Element	Select Search and select a network element to perform this task against.
Network Service	Select Search and select a network service to perform this task against.
Perform Net Host Additions	Check this option to automatically add new hosts that are found during discovery. Note: This option only adds new hosts to the system. It does not automatically overwrite existing hosts defined within the system.
Perform Net Resource	Check this option to automatically add DNS resource records for

Field	Description
Records Additions	new hosts that are found during discovery. Note: This option only adds resource records for new hosts to the system, and does not automatically overwrite existing host resource record information defined within the system.
Ping Hosts	Check this option to ping hosts during discovery.
Regression Periods	Enter in the regression number of periods, and select the regression period type.
Run Snapshot Import When Complete	Imports interfaces and blocks discovered by either a Discover Router Subnets or Global Synchronization of Network Elements task. Reads the snapshot records from the task and creates address blocks (subnets).
Detach Stale Interface Addresses	Only available when the “Run Snapshot Import When Complete” option is selected. For blocks with multiple interface addresses on a given interface, it will find existing interface addresses that were not discovered. It will then “detach” these interface addresses from the interface.
Subnet Address	Select Search and select a subnet to perform this task against.
Update Reclaim Statistics	Update the last discovered counters for blocks and hosts defined within a network element for purposes of including this discover in the reclaim criteria. This option is provided because an ARP discover is less accurate than the Subnet Host Discover in determining if a host is up or not.

On-demand (Immediate) Collection Task

To define an immediate task, define the task parameters, and select **Immediate** from the **When to run task** options. Click on **OK** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled Collection Task

To schedule a future task, define the task parameters, and select **Scheduled** from the **When to run task** selections. Schedule options are displayed .

To select the future date to run the task, click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 69.

After all parameters have been entered, click **Submit**. A new task is created, and submitted to the system. After tasks have been created, you can manage them using the **Task** menu option.

Recurring Collection Task

A recurring task enables you to define tasks to run on a pre-determined schedule. This option allows you to define tasks (such as Utilization Collection) that will occur at regular intervals, providing you with up to date information. To schedule a recurring task, set the

task parameters, and select **Recurring** from the **When to run task** selections. Recurring options are displayed.

Select the date and time that this recurring task is to begin. This is the first occurrence of the recurring task. Click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 69.

Table 3-27 Discovery/Collector Task Definition Screen Elements

Field	Description
Sub-Daily	Select this option if the task is to occur more than once per day.
Daily	Select this option if the task is to occur once per day at the specified time.
Weekly	Select this option if the task is to run weekly, or on the specified day(s).
Monthly	Select this option to run this task on a specified day of the month.
Yearly	Select this option to run this task on a specified day of the year.

After all the parameters have been selected or entered, click **OK**. A new task is created and submitted to the system. After tasks have been created, you can manage them using the **Task** menu option.

Address Space Reclaim

The Reclaim option allows you to free unused IP addresses and subnets from the IPAM database.

IP Address managers need to monitor the actual usage of IP Addresses. “Actual” means that a particular IP Address is configured on a device interface, and used for network traffic. It is not uncommon for an administrator to allocate addresses to a user and those addresses are never used. Addresses can also become stale and unused over time. This does not refer to Dynamic DHCP addresses, which are managed by the DHCP server. Address reclaim is targeted at static and Manual DHCP addresses only. An Administrator needs to identify allocated addresses that are unused, and reclaim them for use by other users. In some cases, entire subnets are allocated for use only during a limited period of time. In such cases, this feature supports reclaiming entire subnets (in-use/deployed blocks) when it is discovered that there are zero hosts on that subnet.

IPAM provides two methods for performing reclaim – manual and automatic.

Manual Reclaim

Manual reclaim allows the administrator to selectively reclaim objects that meet the given criteria. This operation involves these basic steps:

1. Run network discovery tasks periodically. Select **Discover** from the IPAM section of the **Management** menu, and then select **Discover Subnet Hosts** from the **Task Type** drop-down list.

Note: The task must *not* include the **Determine Host Operating System** option.

2. Choose from a number of criteria and filters and then run a report that analyzes the results of Step 1 and proposes individual addresses or subnets for reclaim.
3. Choose from suggested output and reclaim addresses or subnets. Freed subnets are returned to the free block pool. Freed addresses are deleted and available for other allocations.

Automatic Reclaim

Automatic reclaim allows the administrator to schedule tasks to perform automatic reclaim of objects that meet the given criteria. This operation involves these basic steps:

1. Run network discovery tasks periodically. Select **Discover** from the IPAM section of the **Management** menu, and then select **Discover Subnet Hosts** from the **Task Type** drop-down list.

Note: The task must *not* include the **Determine Host Operating System** option.

2. Run an Automatic Reclaim task – immediate, scheduled, or recurring – where the parameters for a reclaimable addresses or subnets are supplied and applied in bulk.
3. Review the results of the reclaim task in the Task display.

Ignoring Specific Device Types during Subnet Reclaim

When creating or editing Device Types, you can specify which device types can be ignored for the purposes of Subnet discovery by selecting the **Ignore devices of this type for Subnet Reclaim** check box.

When a Host Discovery is run for a subnet, devices of the specified type are not counted towards the number of devices discovered. For example, if the Router device type had been set up to be ignored and was the only IP address found during discovery, then that subnet could be reclaimed. This does *not* affect the IP Address Reclaim feature, which supports Device Type filtering. Note that the number of ignored hosts is counted and tracked for the subnet.

IP Address Space Reclaim

To reclaim address space, select **Address Space Reclaim** from the IPAM section of the **Management** menu. The Reclaim screen appears, where you can choose between Manual/Automatic reclaim types, and IP Addresses/Subnets reclaim objects.

Performing Manual IP Address Reclaim

To perform a manual reclaim on IP addresses, ensure that the Manual Reclaim Type and the IP Addresses option buttons are selected.

IP Address reclaim supports the following criteria and filters:

Reclaim Criteria (required)

- **Scope** - The Scope of the IP Address Reclaim may be either a Block or a Container, interpreted as follows:
 - ▶ If the scope is a Block without children, then the reclaim analysis will be performed on the IP addresses in that Block only if it is an In-Use/Deployed Block (that is, a Subnet), otherwise an error will be displayed.
 - ▶ If the scope is a Block with children, then the reclaim analysis will be performed on IP addresses in all child Subnets under the selected aggregate Block.
 - ▶ If the scope is a Container without children, then the reclaim analysis will be performed on IP addresses in all Subnets in the selected Container.
 - ▶ If the scope is a Container with children, then the reclaim analysis will be performed on IP addresses in all Subnets in the selected Container and its sub-containers.
- **Days Since Last Contact** - Defines the window to look for unreachable hosts. That is, the number of days that have elapsed since the last time that an IP address was found to be online.
- **Minimum Discover Attempts** - The minimum number of Discover Subnet Hosts tasks that have been run within the window defined by Days Since Last Contact. That is, the number of times that a Discover Task has been run over the last X number of days, where X is the value of the Days Since Last Contact.

Additional Filters (optional)

- **Block Type** - Default is ALL types. If scope is Block, then list includes the selected Block's type and any sub-types.
- **Address Status** - Default is ALL statuses. Generally useful only for Manual DHCP objects.
- **Device Type** - Default is ALL types.
- **Hostname match** - Default is any hostname but you can enter a string and select from **Begins With**, **Contains**, or **Ends With** options.

After you have entered criteria, click **Submit**. The reclaim analysis is performed and a list is displayed showing all reclaimable addresses. Note that an additional **Pending Approval Status** column is displayed if Device Workflow is enabled.

You can then select some or all of the addresses and click the **Reclaim Selected** button. By default, the list is ordered by IP Address, but you can choose a different sort order by clicking on the appropriate column header. The columns specific to the reclaim analysis are as follows:

- **Last Update** – this is the date/time stamp of the time this device was created or last updated. If this column is blank, then the device was created before this information was tracked in IPAM.
- **Last Reachable** – this is the date/time stamp of the time this device was last determined to be “up” via a Subnet Host Discovery task.

- **Discover Attempts** – this is the number of Subnet Host Discover tasks that have been attempted for this device since the Last Reachable date.

Performing a Manual Subnet Reclaim

To perform a manual subnet reclaim, select the Subnet option button in the Reclaim screen. The screen updates to show subnet reclaim settings.

Subnet reclaim supports the following criteria and filters:

Reclaim Criteria (required)

- **Scope** - The Scope of the Subnet Reclaim may be either a Block or a Container.
 - ▶ If the scope is a Block without children, reclaim analysis is performed on that Block only if it is an In-Use/Deployed Block (that is, a Subnet); otherwise an error is displayed.
 - ▶ If the scope is a Block with children, reclaim analysis is performed on all child Subnets under the selected aggregate Block.
 - ▶ If the scope is a Container without children, reclaim analysis is performed on all Subnets in the selected Container.
 - ▶ If the scope is a Container with children, reclaim analysis is performed on all Subnets in the selected Container and its sub-containers.
- **Days Since Last Contact** - Defines the window to look for unused subnets. That is, the number of days that have elapsed since the last time that at least one IP address in the subnet was found to be online.
- **Minimum Discover Attempts** - The minimum number of Discover Subnet Hosts tasks that have been run the since the device was last reachable. That is, the number of times that a Discover Task has been run over the last X number of days, where X is the value of the Days Since Last Contact.

Additional Filters (optional)

- **Block Type** - Default is ALL types. If scope is Block, then list includes selected Block's type and any sub-types.

After you have entered your criteria and clicked **Submit**, reclaim analysis is performed and a list is displayed showing all reclaimable subnets.

You can then select some or all of the subnets and click the **Reclaim Selected** button. By default, the list is ordered by Subnet name, but you can choose a different sort order by clicking on the appropriate column header. The columns specific to the reclaim analysis are as follows:

- **Last Update** – this is the date/time stamp of the time this block was created or last updated. If this column is blank, then the device was created before this information was tracked in IPAM.

- **Last Reachable** – this is the date/time stamp of the time a device on this subnet was last determined to be “up” via a Subnet Host Discovery task, and that device was not a device type that is to be ignored as described above.
- **Hosts Ignored** – this is the number of devices that were determined to be “up” during the last Subnet Host Discover task, but were ignored because their device type was defined to be ignored as described above.
- **Discover Attempts** – this is the number of Subnet Host Discover tasks that have been attempted for this subnet since the Last Reachable date.

Performing Automatic Reclaim Tasks

Choosing the Automatic reclaim type allows the administrator to create a task that performs reclaim processing automatically on an immediate, scheduled, or recurring basis. Automatic Reclaim is supported for both IP Address and Subnet reclaim. In both cases, the additional task scheduling parameters appear at the bottom of the page.

Immediate Reclaim

To run a reclaim task now, select **Immediate** from the **When to run task** options. Click on **OK** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled

To schedule a future reclaim task, select **Scheduled** from the **When to run task** selections.

To select the future date to run the task, click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 69.

Once all parameters have been entered, click **Submit**. A new task is created and submitted to the system. After tasks have been created, you can manage them using the **Task** menu option.

Recurring

A recurring reclaim task enables you to define the reclaim task to run on a pre-determined schedule. To schedule a recurring task, select **Recurring** from the **When to run task** selections.

Select the date and time that this recurring task is to begin. This is the first occurrence of the recurring task. Click on the calendar icon and select a date, as described in “Discovery/Collector Task Definition Options” on page 69.

After all the parameters have been selected or entered, click **Submit**. A new task is created and submitted to the system. Once tasks have been created, you can manage them using the **Task** menu option.

Container Maintenance

The Container Maintenance menu option allows you to maintain IPAM containers. Containers are organizational units that IPAM administrators use to create a hierarchy of their company's network structure. Rules that govern the IP Address allocation policies of your organization are assigned to each container.

Container Maintenance Layout

When you select **Container Maintenance** from the IPAM section of the **Management** menu, your network tree is displayed in the left frame of your browser. IPAM recommends that you click the **Refresh** link above the hierarchy display after adding or deleting containers.

The right-hand side of the screen lists the container maintenance options, described in Table 3-28. Refer to the following sections for information on each option.

Table 3-28 Container Maintenance Features

Option	Description
Edit Container	Edit the currently selected container.
Delete Container	Delete the currently selected container.
Add Child Container	Add a container below the currently selected container. The currently selected container becomes a parent of the new container.
Clone Container	Clone a container adjacent to the original container in the container tree.
Reparent/Move this Container	Move this container underneath a different parent.
Attach Network Service to Container	Attach a DHCP Server to this container. The DHCP Server must have previously been defined in the Topology -> Network Services module.
Detach Network Service from Container	Remove a DHCP Server assignment from this container.
Attach Switch	Attaches a switch to this container. A Network Element with an Element Type of "Switch" must be defined first.
Detach Switch	Detaches a switch from this container.

Edit Container

Use the **Edit Container** option to edit the attributes of a container. Note that you cannot change a container type after you have created it. For information on the fields in each tab, refer to Table 3-29 and Table 3-30 on page 79.

Detach Container

If the container is a device container which is attached to multiple parents in the logical container hierarchy, then the option available will be to Detach Container. If the container is

a logical container or a device container with a single parent, the option available will be to Delete Container (see next section).

When you detach a device container which it attached to multiple parents, then you will be presented.

If you are using the feature of attaching network services to containers (see below), then the operation of detaching a device container from one portion of the logical container hierarchy may result in removing one or more DHCP servers from the list available to objects within this device container. In this instance, you can choose to reassign those subnets, address pools, or individual device objects to a DHCP server that would be valid after the detachment.

Delete Container

Use the **Delete Container** option to delete a container. Note that deletes are not allowed in the following cases:

- Container is the root container (top of the container hierarchy)
- Container has child containers

Note: If child containers are moved or deleted first, the container can then be deleted.

- Container has blocks assigned within it

When you select this option, an *Are you sure you want to delete this container?* confirmation window displays. Select **OK** to delete the container or **Cancel** to leave the container unchanged.

Add Child Container

Select the **Add Child Container** option to create a child container for the parent container you have selected in the container hierarchy. The Add Child Container screen shown, below, appears.

This screen is divided into two sections: General Information and Rules tabs.

General Information Section

The General Information section captures basic information about the new child container.

Table 3-29 General Information Parameters

Option	Description
Type	Select Logical or Device . Logical containers are user-defined organizational views of how your address space is managed (such as regions, divisions, ISP, organizations, and so on.). Device containers represent actual Network Devices such as Routers and CMTSs. To add a Device, click the Search button and select a Device from the IPAM Device Search window, where you can search on a specific text or IP address string if necessary. The device you select appears in the Name field and its IP address is shown in the Device Specific Information area.
Name	Provide a name for the new container, which is displayed in the container tree.
Discovery Agent	Select the IPAM Agent (defined in Agents in the System section of the Tools menu) to be used to perform Network Discovery for blocks within this container.
Description	Provide a description for the new container.
IP Address	<i>Read-only for Device containers.</i> Displays the IP Address of the Network device selected in the IPAM Device Search window.
Information Template	Choosing an Information Template for this container adds the User Defined Fields in that Information Template to this container. The fields from the selected Information Template appear on the right side of the screen.
Maintain History Records	If checked, Container History and Block History records will be kept for all appropriate block types. The history records are created each time the Global Utilization Rollup task is run.

Rules Tabs

The tabs allow policies or rules to be established for this container. The rules established for a container govern the use and allocation of address space for this container.

Table 3-30 Rules

Rule	Description
Valid Block Types	Selecting one or more block types on this policy allows child blocks of these types to be created in this container. All other block types are prohibited.
Valid Device Types	Selecting one or more device types on this policy allows devices of these types to be created in subnets that are defined within this container. All other device types are prohibited.
Allow Root Block Creation	<i>Not applicable for device containers.</i> Selecting one or more block types on this policy allows root blocks of these types to be created in this container. All other block types are prohibited.

Rule	Description
Allow Allocation from Parent	<i>Not applicable for device containers.</i> Selecting one or more block types on this policy allows child containers to search in this container's Parent for blocks of the selected types. For all non-selected block types, the search is not allowed to proceed beyond this container.
Require SWIP/Net Name	Selecting one or more block types on this policy makes entry of the SWIP/Net Name parameter a required field for these block types, within this container. For all non-selected block types, entry of the SWIP/Net Name parameter is not required.
Block Type Information Template	Choosing an Information Template for a block type adds the User Defined Fields in that Information Template to any block of that type within this container. You can see the fields from the Information Template on the Add Child Block screen.
Device Type Information Template	Choosing an Information Template for a device type adds the User Defined Fields in that Information Template to any device of that type within this container. You can see the fields from the Information Template on the Add IP Address screen.

Clone Container

Use the **Clone Container** option to create a clone of a container. This would place the cloned container adjacent to the original container in the container tree. All fields would be prepopulated with values from the original container and you can modify them. Note that you cannot change a container type. For logical containers, the container name would be prefixed with "Copy of", we recommend to modify the name. For a device container, use the "Search" button on the clone container screen to enable necessary selection of a network element. For information on the fields in each tab, refer to Table 3-29 and Table 3-30 on page 79.

Reparent/Move this Container

Select the **Reparent/Move this Container** option to move this container (and the blocks associated with it) to another parent. The Reparent/Move Container screen opens.

Click the **Select New Parent** button to display the Container Search dialog box.

Navigate the tree, expanding nodes as needed, and then check the new parent container. Note that you can only check a single container. Once you have selected a container, click the **Select Container** button. The name of the new parent is displayed in the **Move Container to this parent** field. Click **Submit** to move the container to this new parent, or click **Cancel** to return to the Container Maintenance screen.

If you are using the feature of attaching network services to containers (see below), then the operation of moving a container may result in objects within that container becoming invalid with respect to the available DHCP servers for the target container. In this instance, you can choose to reassign those subnets, address pools, or individual device objects to a DHCP server that would be valid after the move. Therefore, you may optionally choose to have this

replace DHCP server operation affect device containers which may have multiple attachments in the logical container hierarchy.

Attach Network Service to Container

Use this option to attach Network Services (DHCP servers) to this container. By attaching one or more network services to this container, you establish the set of Primary DHCP servers available for this container and its children containers. That is, when assigning a Primary DHCP server to a subnet, address pool, or individual object, the list of DHCP servers will be limited to those servers attached to the container. If the immediate container has no attached network services, then the next closest ancestor container with attached network services will be used to establish the list of available DHCP servers. If no network services are attached to any of the containers up to the root container, then all DHCP servers defined in IPAM will be in the list, and available for assignment.

Important Note: This feature should be used with caution. By limiting the available DHCP servers in portions of the container hierarchy, IPAM will be required to enforce these limits. Therefore, operations which involve moving containers, blocks, or devices are impacted by the set of available DHCP servers for the portion of the container hierarchy to which the object is moved.

To attach a network service to the container, check the select box of the network services to attach, and then click on **Attach Selected**. You can limit the display of network services by using the search filter, or by clicking on the **Only Show Services not attached to any container** check box.

As part of the attach operation, you may wish to update existing objects within the container and its children with respect to their Primary DHCP server assignment. If subnets, address pools, or individual devices below this container are assigned to a different DHCP server than those that are currently attached or being attached to this container, then use the “Replace DHCP servers defined in this container and children with” option to select one of the attached DHCP servers which will be used to update the assignments on those subnets, address pools, or devices. Since device containers may have multiple parents in the logical container hierarchy, it may be possible for two distinct sets of DHCP servers to be available for assignment at that device and below. Therefore, you may optionally choose to have this replace DHCP server operation affect device containers which may have multiple attachments in the logical container hierarchy.

Detach Network Service from Container

Please see the section above on Attach Network Service to Container. Use this option to remove an attached network service from this container.

As part of the detach operation, you may wish to update existing objects within the container and its children with respect to their Primary DHCP server assignment. If subnets, address pools, or individual devices below this container are assigned to the DHCP server which is being detached, then use the “Replace detached DHCP servers with” option to select one of

the remaining, attached DHCP servers which will be used to update the assignments on those subnets, address pools, or devices. Since device containers may have multiple parents in the logical container hierarchy, it may be possible for two distinct sets of DHCP servers to be available for assignment at that device and below. Therefore, you may optionally choose to have this replace DHCP server operation affect device containers which may have multiple attachments in the logical container hierarchy.

Attach Switch

Select the **Attach Switch** option to attach a Switch to the container previously selected in the container hierarchy.

To search for a particular Switch, enter a search string into the text block and click **Search**. To filter your search criteria to only Switches in the system that are not attached to a Container, click the **Only show Switches not attached to any container** checkbox.

To attach one or more Switches, click the checkbox in the **Select** column for each item you wish to attach, and click **Attach Selected**. Click **Cancel** to cancel and return to the previous screen.

Detach Switch

Use the Detach Switch option to detach a Switch from a container.

This menu allows you to detach one or more Switches from a Container. All Switches currently attached to the selected Container in the tree view are listed.

To detach one or more Switches, click the checkbox in the Select column for each item you wish to detach, and click **Detach Selected**. You are prompted for confirmation. Click **OK** to detach the selected Switch, or **Cancel** to return to the previous screen.

Network Elements/Devices

The Network Elements/Devices screen allows you to maintain network elements (managed devices) within the IPAM system. A network element represents a physical device on your network such as a router. IPAM can be used to manage and plan the IP Address space that is allocated to a physical device. This planned allocation can then be compared to the device's actual configured address space by using the collection facility provided by IPAM.

To search for a particular Network Element, enter a search string into the text block and click **Search**.

To delete one or more Network Element, select the checkbox next to each item you want to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected Network Elements.

Adding a Network Element

To add a network element, click the **Add Network Element** link. The Add Network Element screen appears.

Table 3-31 Add Network Element Parameters

Field	Description
Name	Enter the name of the device. Typically, this will be the fully qualified domain name.
Description	Enter a description of this device.
IP Address	Enter the IP Address of this device. This is required if you will use IPAM to collect configuration information from this device.
Element Type	Select the type of this device.
Vendor	Select the vendor of this device.
Model	Select the model of this device.
Telnet Username	Enter the Telnet user name used to telnet into this device. This user name will be used to optionally update the device's configuration with changes in the address space. <i>This feature is not implemented.</i>
Telnet Password	Enter the Telnet password used to telnet into this device. <i>This feature is not implemented.</i>
Enable Password	Enter the Enable password. <i>This feature is not implemented.</i>
SNMP Version	Select the SNMP Version being used. Choosing V3 will display additional fields required by V3.
SNMP Read Community String	Enter the SNMP read community string used to read the device's MIB II information. This is required if you will use IPAM to collect configuration information for planned vs. actual comparisons.
SNMP Timeout (milliseconds)	Enter the number of milliseconds the SNMP Agent will wait without receiving any messages from its partner before it assumes that the connection to its partner has failed.
SNMP Retries	Enter the number of connection retries that the SNMP Agent will attempt.
Collection Agent	Select the Agent that will be used to collect information from this device. This is required if you want to use IPAM to collect configuration information for planned vs. actual comparisons. Click  or select the Add Agent link to open the Agents screen where you can select an agent from the Agent Name list, as described in "Agents" on page 220.
Include during Global Synchronization Task	Select if you want to include this device in the global synchronization task. The device's configuration information is then collected when the task runs.
Device Interface Template	Select a device interface template to assign to this device. The device template is used to model and attach interfaces to this device. If a template is selected, and there are interfaces defined for this device, interfaces are displayed and can be assigned a status of ENABLED, DISABLED, or BEING DEPLOYED, as described in "Adding a Device Interface Template" on page 251.

Click **Submit** to save your changes. The new network element appears in the **Network Element Name** list.

Editing a Network Element

To modify an existing network element, click on the network element name in the Network Element List. The Edit Network Element screen opens.

Edit the network element fields as needed. You can change the attributes of the network element, or add and remove interfaces using the **Interfaces** tab. Click **Submit** to save your changes.

Editing Interfaces

To modify an existing network interface, click on the **Interfaces** tab in the Edit Network Element screen. The Interfaces tab opens with a list of interface names.

This screen displays a list of interfaces associated with a network element. Choose from the following actions:

- To add an interface, click on **Add Interface**.
- To modify an interface, select it in the Interface Name list and modify the name or status in the Edit Network Element Interface (name) popup.
- To delete an interface, select the checkbox next to it and click . You are prompted for confirmation. Click **OK** to delete the selected Network Element Interface.

Creating a Network Element Interface

To create the interface associated with a network element, follow these steps.

1. Click **Add Interface**.

The Create Network Element Interface popup opens.

2. Refer to the following table as you fill in the fields.

Table 3-32 Network Element Interface Parameters

Field	Description
Interface Name	Enter a name for the interface.
Status	Select one of the following: <ul style="list-style-type: none"> • Enabled (available for block allocation / attachment) • Disabled (Not available for block allocation / attachment) • Being Deployed (Defined in IPAM, not yet defined on actual Network Element)

3. Click **Save**.
The interface is added to the **Interface Name** list.

Server Pairs

The Server Pairs screen allows you to maintain network service to network service communications. It allows you to configure the following:

- Transaction keys that are used to secure communications between ISC BIND-based DNS servers.
- Transaction keys that are used to secure dynamic updates from ISC-based DHCP servers to ISC BIND-based DNS servers.
- GSS Credentials that are used to secure dynamic updates from IPAM to Microsoft DNS servers.
- Override of default behavior of BIND-based DNS server communications, such as turning off incremental zone transfers.

To delete one or more server to server definitions, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected pairs, or **Cancel** to return to the previous screen.

Adding a Network Service Pair

To add a Net Service Pair, click the **Add Net Service Pair** link. The Add Net Service Pair screen appears.

Table 3-33 Net Service Pair Parameters

Field	Description
Net Service	<p>Select the network service that you wish to add server to server communications statements.</p> <p>If “IP Control” is selected, you are configuring the security credentials for dynamic DNS updates to a remote DNS Server. You must select a DNS server for the Remote Net Service option. If the remote DNS server is BIND based, then you choose a TSIG key. If the DNS server is Microsoft based, you choose GSS TSIG credentials.</p> <p>If a DHCP server is selected, you are configuring the transaction key to be used for dynamic DNS updates from this DHCP server to the DNS server selected in the Remote Net Service option. You must select a DNS server for the Remote Net Service option.</p> <p>If a DNS server is selected, you can configure the server to server configuration settings between this DNS server and the entity that you select in the Remote Net Service option.</p> <ul style="list-style-type: none"> • If the Remote Net Service option is “IP Control”, you are configuring the server to server configuration between the DNS server and the InControl DNS Listener. • If the Remote Net Service option is another DNS server, you are configuring the server to server configuration between these two DNS servers. <p>When configuring DNS to DNS server pairs, a list of DNS options is displayed. These options are used to configure the “Server” configuration section of the named.conf file. If the servers are BIND 9.10 and later, the new DNS options available since BIND 9.10 will be displayed</p>
Remote Net Service	<p>Select the remote network service that you want to communicate with the “Net Service”.</p> <p>If “IP Control” is selected, you are configuring the server to server configuration between the DNS server (specified in the “Net Service” selection) and the InControl DNS Listener.</p> <p>If a Bind based DNS server is selected, you can configure the server to server configuration settings between this DNS server and the entity that you select in the Net Service option. If the Net Service option is another DNS server, you are configuring the server to server configuration between these two DNS servers.</p> <p>If a Microsoft DNS server is selected, you can configure the GSS TSIG credentials to use for dynamic updates.</p>
Enable TSIG Key	Checked indicates that communications between these two network services should use Transaction Keys.

Field	Description
TSIG Key	Choose a Key from the list of keys, or Generate a Key on the fly by entering in a key name. The key name must conform to fully qualified domain name rules, including a trailing dot for example: <i>key45.ins.com</i> .
Bogus	If you discover that a remote server is giving out bad data, marking it as bogus will prevent further queries to it. The default value of bogus is no.
EDNS	The edns clause determines whether the local server will attempt to use EDNS when communicating with the remote server. The default is yes.
Support IXFR	IXFR requests to servers that do not support IXFR will automatically fall back to AXFR. Therefore, there is no need to manually list which servers support IXFR and which ones do not; the global default of yes should always work. The purpose of the provide-ixfr and request-ixfr clauses is to make it possible to disable the use of IXFR even when both master and slave claim to support it, for example if one of the servers is buggy and crashes or corrupts data when IXFR is used.
Provide IXFR	The provide-ixfr clause determines whether the local server, acting as master, will respond with an incremental zone transfer when the given remote server, a slave, requests it. If set to yes, incremental transfer will be provided whenever possible. If set to no, all transfers to the remote server will be non-incremental. If not set, the value of the provide-ixfr option in the view or global options block is used as a default.
Request IXFR	The request-ixfr clause determines whether the local server, acting as a slave, will request incremental zone transfers from the given remote server, a master. If not set, the value of the request-ixfr option in the view or global options block is used as a default.
Number of Transfers	Number of Transfers is used to limit the number of concurrent inbound zone transfers from the specified server. If no transfers clause is specified, the limit is set according to the transfers-per-ns option.
Transfer Format	The server supports two zone transfer methods <ul style="list-style-type: none"> • one-answer - uses one DNS message per resource record transferred. • many-answers - packs as many resource records as possible into a message. many-answers is more efficient, but is only known to be understood by BIND 9, BIND 8.x, and patched versions of BIND 4.9.5. <p>You can specify which method to use for a server with the transfer-format option. If transfer-format is not specified, the transfer-format specified by the options statement will be used.</p>
Enable GSS	This is a Microsoft only DNS Parameter: Checked indicates that the communications between these two network services should be secured using GSS TSIG.

Field	Description
Realm Name	This is a Microsoft only DNS Parameter: For GSS TSIG, enter the Microsoft Realm name. This is typically the same as the Microsoft AD domain name. By convention, it is entered in uppercase.
Principal Name	This is a Microsoft only DNS Parameter: For GSS TSIG, enter the principal name that has authorization to update zones the chosen DNS Server. By convention, this name has the format: "host/<agent-hostname>", where <agent-hostname> is the FQDN of the agent associated with this Net Service. This field should match the Principal name configured in Active Directory.
Principal Password	This is a Microsoft only DNS Parameter: Enter the password associated with the Principal name in Active Directory.
Confirm Password	This is a Microsoft only DNS Parameter: Confirm the Principal password by re-entering it here.

Enter the desired attributes once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen. If the Net Service Pair was successfully added, the new product appears in the Net Service Pair list.

Editing a Network Service Pair

To modify an existing Network Service Pair definition, follow these steps.

1. On the Net Service Pairs screen, click on a service name link in the Net Service list. The Edit Net Service Pair screen opens.
2. Edit the pair definition as needed. Refer to Table 3-33 for information on the fields or check boxes you wish to update.
3. Choose one of the following actions:
 - Click **Submit** to save your changes.
 - Click **Cancel** to return to the previous screen.

Restoring Deleted Items

The Restore Deleted Items screen allows you to restore device or resource records that have been deleted. To access the Restore Deleted Items screen, select Restore Deleted Items from the IPAM section of the Management menu or by clicking the Restore link in the top left corner of the screen next to Tasks | Alerts link. The screen has two tabs, Device and Resource Records. Number of entries eligible for restore is determined by System Policy 'Maximum Records to Retain in the Restore List per User'. The limit is per user. Once the limit is reached, oldest items in the list will be deleted as new items are added.

Restoring Deleted Devices

Devices that have been deleted and are eligible for restore are listed on the Device tab. You may click the IP Address field hyperlink to view the details of the deleted device that are not shown in the list, for ex. Resource records, interfaces etc.

Refer to 3-34 for a description of the columns in the **Device** tab.

Table 3-34 Restore Deleted Device Columns

Field	Description
IP Address	The IP address assigned to the deleted device.
Host Name	The host name of the deleted device.
Block	The block where the deleted device was located.
Container	The container where the deleted device was located.
Device Type	The device type assigned to the device. Device Types are maintained in the IP/DEVICES section of the Tools menu.
Address Type	The IP address type.
HW Addr	The MAC address of the deleted device.
Description	The description (if any) that was entered for the device.
Domain	The domain on which the device was located.
DUID	DUID of the deleted device
Admin	Admin who deleted the device.
Date/Time	Date and time when the device was deleted.

Ignore Duplicate Warning checkbox:

The admin policy may be set to ‘warn’ in case of duplicate hostname or duplicate hardware address.

- If the checkbox is unchecked, the restore will fail if the restore results in a device with duplicate hostname or hardware address.
- If the checkbox is checked, the duplicate warning will be ignored, and the restore will be successful.

To restore one or more devices from the list, click the checkbox in the Select column for each item you wish to restore, and click .

To delete one or more devices from the list, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the device from the list, or **Cancel** to return to the previous screen.

The list may be filtered based on the following columns (Filter panel on the left):

- IP Address
- Hostname

- Block
- Container
- Device Type
- Address Type
- HW Addr
- Admin (Master Administrators only)

Restoring Deleted Resource Records

Resource records that have been deleted and are eligible for restore are listed on the Resource Records tab.

Note: If a resource record is deleted from a device or domain it will appear on this list. However if the whole device is deleted, the resource records associated with the device will not appear in this list. They are part of the deleted device and may be restored along with the Device from the Device tab.

Refer to 3-35 for a description of the columns in the **Resource Records** tab.

Table 3-35 Restore Deleted Resource Record Columns

Field	Description
Owner	The Owner field of the deleted resource record.
Class	The Class field of the deleted resource record.
Type	Type of the deleted resource record.
TTL	Time to live value for the deleted resource record.
Data	The RDATA field of the deleted resource record.
Domain	The domain on which the deleted resource record was located.
IP Address	If the deleted resource record was associated with a device, then the IP Address of the device.
Hostname	If the deleted resource record was associated with a device, then the hostname of the device.
Admin	Admin who deleted the resource record
Date/Time	Date and time when the resource record was deleted.

Ignore Duplicate Warning checkbox:

The admin policy may be set to 'warn' in case of duplicate Owner.

- If the checkbox is unchecked, the restore will fail if the restore results in a resource record with duplicate owner field.

- If the checkbox is checked, the duplicate warning will be ignored if a duplicate owner field is encountered during restore, and the restore will be successful.

To restore one or more resource record from the list, click the checkbox in the Select column for each item you wish to restore, and click .

To delete one or more resource record from the list, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the resource record from the list, or **Cancel** to return to the previous screen.

The list may be filtered based on the following columns (Filter panel on the left):

- Owner
- Type
- Data
- Domain
- IP Address
- Hostname
- Admin (Master administrators only)

This page intentionally left blank.

Chapter 4 Managing DNS

In Cisco Prime Network Registrar IPAM 8.3, all the features you need to set up DNS servers is located in the DNS section of the Management menu. This chapter describes how to use each selection on the DNS menu.

- Servers/Services
- Configuration/Deployment
- Domains
- Galaxies
- Log Channels
- Server Templates
- Domain Types
- Address Match Lists
- Update Policies
- Transaction Keys
- Option Vendor Dictionary
- Option Master Dictionary
- DNS Software Products

Servers/Services

The **Servers/Services** option in the DNS section of the **Management** menu allows you to define and maintain a layer 3 network DNS service. Use IPAM to manage and plan the IP address space, policies, options, and/or resource records that are allocated to your DNS network service. Then use IPAM to create the configuration files necessary for DNS services.

Managing DNS Servers/Services

To manage your DNS servers and services, follow these steps.

1. Select **Servers/Services** from the DNS section of the **Management** menu. The DNS Servers/Services window appears and the hierarchy changes to display your existing domain structure.
2. Choose from the following actions.

To ...	Then ...
Search for a particular DNS Network Service	<ol style="list-style-type: none"> 1. Enter a search string into the text block. 2. Click Search. The list of servers changes to match the search string.
Add a DNS Network Service	Refer to “Adding a DNS Network Service” on page 94.
Edit a DNS Network Service	<ol style="list-style-type: none"> 1. Click on the service entry in the Service Name list. The Edit DNS Server screen opens. 2. Edit fields and tab entries as needed. Refer to the descriptions in the following sections for more information.
Add or edit a zone on an existing DNS Network Service	Refer to “Editing a DNS Zone” on page 105.
Add or edit a DNS View on an existing DNS Network Service	Refer to “Configuring DNS Zones” on page 106.
Add or edit a DNS Template on an existing DNS Network Service	Refer to “Configuring Zone Templates on a DNS Server” on page 108.
Add or edit a DNS64 configuration on a CNR Caching 8.3 server	Refer to “DNS64 Settings”, later in this chapter.
Delete one or more DNS Network Services	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Network Services, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen. If the DNS server was successfully added or modified, the DNS server appears in the **Service Name** list.

Adding a DNS Network Service

To add a DNS Network Service, follow these steps:

1. Select the **Add Network Service** link. The Choose DNS Template screen appears, as shown below.
2. Select a DNS template from the drop-down list or **None** to begin with a clean slate. For more information on DNS Server templates, refer to “Server Templates” on page 125.
3. Click **Submit**. The Add DNS Server from template <DNS Template Name> screen appears.

Note: Different tabs are displayed for Cisco Network Registrar servers:

- CNR DNS Authoritative: **General, Zones, Options, and HA Pair**
 - CNR DNS Caching: **General, Root Hints File, Zones, Options, DNSSec, and DNS64.**
-

General Tab Settings

Table 4-1 General Tab Parameters

Field	Description
Name	Enter the name of this DNS Server. Typically, this is the fully qualified domain name of the system where the service is running.
IPv4 Address	Enter the IPv4 address of this service. This is required if you use IPAM to collect configuration information from this service, or create configuration files for this service.
V6 IP Address	Enter the IPv6 address of this service, if any. This is optional, however if option 23 is set to “Same as Subnet” on any IPv6 address pool, then this field will be required for any DNS servers on the IPv6 Subnet Policies tab.
Create db.127.0.0 Loopback Address File	Check this box to automatically create the db.127.0.0 loopback file during a DNS Configuration File creation task. This file contains the information that is needed by the server for it to direct traffic to itself.
Configuration Directory	Enter the fully qualified pathname where the configuration file named .conf is created. Typical entries are listed below: UNIX DNS: /opt/incontrol/dns/etc Windows DNS: C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\dns\db
Data Directory	Enter the fully qualified pathname where the data files (zone files) are created. Typical entries are listed below: UNIX DNS: /opt/incontrol/dns/db Windows DNS: C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\dns\db
Product	Select the Product from the drop-down list of DNS products available within this system. Use the DNS Software Products option on the Management > DNS menu to manage products defined within the system.

Field	Description
Agent	Select the Agent that is used to collect and distribute information to this service. This is required if you use IPAM to collect configuration information for planned <i>vs.</i> actual comparisons. Usually the agent selected is the agent residing on the system where the DNS Service is running.
Start Script	The script that is used to start the DNS server. This script is called by IPAM to start a DNS server. UNIX: /opt/incontrol/etc/named_start Windows: C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\etc\named_start.bat
Stop Script	The script that is used to stop the DNS server. This script is called by IPAM to start a DNS server. UNIX: /opt/incontrol/etc/named_stop Windows: C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\etc\named_stop.bat
Configuration File Check Script	The script that verifies the DNS server's configuration file (named.conf). When creating a configuration task for this server, an administrator can have IPAM call this script to ensure that a valid configuration has been generated for the server. The configuration file is copied to the DNS server and the check script runs against the file in a temporary directory. If the check is successful, the server is stopped and the new configuration file replaces the existing file, and the DNS server is restarted.
Zone File Check Script	The script that verifies the DNS server's zone files. When creating a configuration task for this server, the administrator can have IPAM call this script to ensure that valid zone files have been generated for the server. The zone files are copied to the DNS server and the check script runs against the files in a temporary directory. If the check is successful, the server is updated with the new zone files.
CNR Userid	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Enter the user ID required to allow execution of the nrcmd and/or cnr_exim utilities for this cluster.
CNR Password	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Enter the password required to allow execution of the nrcmd and/or cnr_exim utilities for this cluster.
Confirm CNR Password	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Confirm the CNR password.
Port	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Enter the port that the CNR SDK listens on. The default is 1234.
Nrcmd Directory	<i>CNR DNS Authoritative only.</i> Enter the full pathname where the nrcmd command is located. Default locations are: UNIX: /opt/nwreg2/local Windows: C:\Program Files (x86)\Network Registrar\Local\bin

Logging Tab Settings

The **Logging** tab allows the configuration of the logging statements for the DNS server. Logging for BIND DNS servers is accomplished with two main concepts: *channels* and *categories*. A channel specifies where logged data goes (that is, syslog, to a file, and so on). A category specifies what data is logged. In a BIND-based DNS server, most messages are categorized by function.

The **Logging** tab displays when you edit a server only.

This option allows you to select logging channels for each category that is defined for the server.

To add a channel to a category, click the **Choose** button next to the category. The Logging Channels screen opens.

Click the checkbox next to the Channels that you want to assign to this category, and once finished, click **Submit** to save your changes.

Extensions Tab Settings

Click the **Extensions** tab to display the configuration file extensions area. The extensions area allows you to create free form text to add to the beginning or the end of the named.conf configuration file.

Table 4-2 Extensions Tab Parameters

Field	Description
Start of named.conf	A free text area that will appear at the beginning of the named.conf file when the file is automatically generated. Note: The extensions are limited to 32000 characters.
End of named.conf	A free text area that will appear at the end of the named.conf file when the file is automatically generated. Note: The extensions are limited to 32000 characters.

Root Hints Tab Settings

Click on the **Root Hints** tab to display the configuration of the Root Hints file. The Root Hints file tells the DNS server where the name servers for the root zone are.

Table 4-3 Root Hints Tab Parameters

Field	Description
Create Root Hints File	Check this item on if you want to automatically create the Root Hints file when generating the DNS Configuration files.
Use Standard InterNIC supplied content	Only valid if you have checked the Create Root Hints file option. Select this option if you would like to use the InterNIC supplied content when generating this file.
Use Custom Root Hints file	Only valid if you have checked the Create Root Hints file option. Select this option if you would like to use custom content that you enter for the Roots Hints file.

Zone Tab

Click on the **Zones** tab to display the zones associated with this DNS server. This tab is read-only. To add, edit, or delete zones associated with this DNS server, click on its **Zones** link on the Servers/Services window, selected from the DNS section of the Management menu.

Advanced Tab Settings

Click on the **Advanced** tab to display the available advanced options. These options include configuration of the “controls” section of the configuration file.

Traditionally, DNS administrators controlled the BIND DNS server with UNIX signals. The DNS server interprets certain signals as an instruction to take a particular action, such as reloading changed zones. Due to a limited number of signals, BIND has introduced a method of controlling the name server by sending messages to it on a special control channel. The control channel can be either a UNIX socket, or a TCP port that the name server listens on for messages.

Table 4-4 Advanced Tab Parameters

Field	Description
TCP Port Control Channel Settings:	Select this option to send messages to the name server via a TCP/IP Port.
Listen on IP Address	Enter the IP Address for the name server to listen on for messages.
Listen on Port	Enter the Port that the name server will listen on for messages. Typically, this is port 953.
Allow Message From	Enter an IP Address or Address Match List name that specifies where messages are allowed to come from.
UNIX Domain Socket Channel Settings:	Select this option to send messages to the name server via a UNIX Domain Socket.
UNIX Domain Socket	Enter the name of the socket that will be used for communicating with the name server. Typically this is <code>/var/run/ndc</code> , though some operating systems use a different pathname. The socket is usually owned by root and readable and writable only by the owner.
Permissions (in Octal Format)	The permission value must be specified as an Octal number (with a leading zero to indicate an octal quantity). For example; 0660
Owner (in Numeric Format)	Enter the Owner identifier.
Group (in Numeric Format)	Enter the Group identifier.

Options Tab Settings

Click on the Options tab to display the options and directives that are available. The options displayed are dependent upon the Product selected and the items configured in the Option Vendor Dictionary. For more information on DNS option vendors, refer to “DNS Option Vendor Dictionary”.

To view all available options for this product, select **Show All Product Options**. All options configured for the product selected on the **General** tab are displayed.

Configure each option that you want to appear in the named.conf configuration file.

HA Pair Tab Settings

On a CNR DNS Authoritative server, an HA DNS server pair is a symmetric backup system where both servers are masters for their zones.

1. Click on the **HA Pair** tab to define a failover server for a CNR DNS Authoritative server.

Note: The HA Pair CNR DNS Authoritative server defined here does not require the IPAM Agent software like the main CNR DNS Authoritative server does.

2. Enter the required values, as described in the following table.

Table 4-5 HA Pair Parameters

Field	Description
Backup Server IP Address	Enter the IP address of the failover server.
Backup Server Admin Name	Enter the admin user name to connect to the failover server.
Backup Server Password	Enter the password for the admin user name and then validate it in the Verify Password field.
Backup Server Port	Enter the port number that IPAM should use to communicate with the failover to have it sync. The port number default is 1234.

3. If needed, check **Show All Product Options** and enter the following values.

Table 4-6 HA Pair Options

Field	Description
ha-dns main server	The IP address to use for the HA DNS protocol on the main server. If this value is not set, the address specified for the main cluster is used. In general, it should only be set if the server is configured with different interfaces for configuration management and update requests. The HA DNS protocol should always be configured with the interface used to service updates.
ha-dns backup server	The IP address to use for the HA DNS protocol on the backup server. If this value is not set, the address specified for the backup cluster is used. In general, it should only be set if the server is configured with different interfaces for configuration management and update requests. The HA DNS protocol should always be configured with the interface used to service updates.
ha-dns	Click Yes to enable or No to disable HA on the DNS server.

4. If your administrator role has the required expert permission, you may need to expand the **Expert Options** section and enter values for the following options.

Table 4-7 HA Pair Expert Options

Field	Description
ha-dns port	Specifies the TCP port number used for HA servers communication. The value of this attribute must be consistent for both HA servers.
ha-dns max-batch-count	The HA main server batches RR edits before dispatching them to the backup server. To maintain a manageable history list containing the RR changes that need to be dispatched to the backup server, the main server will discontinue accepting DNS updates/administrative sourced RR edits once the number of RRs undispached/unknowledged (to/by the backup server) exceeds this value.
ha-dns poll-interval	On the HA main server, this is the interval at which the HA server will check if keep alive heartbeat message requests need to be send to the HA partner. The request will be sent if the last time the server received a request or response from its partner was more than ha-dns-comm-timeout. On the HA backup server, this is the interval at which the HA server sends a heartbeat request.
ha-dns comm-timeout	This time interval specifies the amount of time which is allowed between sending a HA message and a successful acknowledgement from the HA partner. Expiration of this time interval causes the HA server to assume its partner is unreachable, triggering a HA state transition (into Communication-Interrupted state).
ha-dns max-interrupted-edits	This value defines a percentage that the HA server uses to allow its edit list to grow in the persisted changed-names DB while in the communication-interrupted state. If the number of name-set records exceeds this percentage of the total size of the zone, the zone will be purged from the changed names DB. During zone synchronization, the HA server can only provide its entire zone to its partner. Though this value bounds a zone in the changed-names DB during communication-interrupted state, it will require a full zone exchange during zone synchronization. The probability of losing RR changes during synchronization gets enhanced by decreasing this value. Note, a value of 100 retains all name-set records for the zones and zones will not be purged.

DNSSec Tab Settings

On a CNR DNS Caching server, the **DNSSec** tab enables you to establish DNS Security settings.

1. Click on the **DNSSec** tab to define DNS security options.
2. Check **Show All Product Options** and enter values as needed. Refer to the section DNS Option Master Dictionary for instructions on getting the description of each option.
3. If your administrator role has the required expert permission, you may need to expand the **Expert Options** section and enter values for the options. Refer to the DNS Option Master Dictionary for a description of each option.

DNS64 Settings

CNR Caching 8.1 and 8.2 Servers

On a CNR DNS Caching 8.1 or 8.2 server, the **DNS64** tab enables you to establish DNS64 settings.

1. Click on the **DNS64** tab to define DNS64 options.
2. Check **Show All Product Options** and enter the following values.

Table 4-8 DNS64 Options

Field	Description
Prefix	Specifies the IPv6 prefix to use for synthesizing AAAA records. The prefix length must be 32, 40, 48, 56, 64, or 96, and bits 64-71 of the prefix must be zero.
Enable DNS64	Determines whether or not to enable DNS64 processing. DNS64 synthesizes AAAA records from A records, when a client queries for AAAA records, but none are found.

3. If your administrator role has the required expert permission, you may need to expand the **Expert Options** section and enter values for the following options.

Table 4-9 DNS64 Expert Options

Field	Description
Suffix	Specifies the IPv6 suffix to use for synthesizing AAAA records. The suffix is ignored if the dns64 prefix is 96 bits long.
DNS64 Name	The name of the DNS64 configuration instance.
Synthesize-all	Forces DNS64 to always synthesize AAAA records from A records when they are requested.

CNR Caching 8.3 Server

On a CNR DNS Caching 8.3 server, the DNS64 link on the DNS Servers/Services list page enables you to establish DNS64 option settings. This server release implements a new “Match Clients ACL” attribute, supporting multiple DNS64 configurations. The options are the same as described in the previous section, with the addition of the Match Clients ACL. Also, the DNS64 Name is now entered as the name of the DNS64 configuration.

Statistics Tab Settings

Click on the **Statistics** tab to configure statistics channels for BIND 9.5 servers and newer. Click “Add Statistics Channel” to add a new channel. Multiple channels can be configured per server.

Table 4-10 Statistics Channel Options

Field	Description
Listen On IP Address	IP Address on which the server will listen for statistics access. Use * to listen on all configured V4 addresses and :: to listen on all configured V6 addresses

Field	Description
Listen On Port	The port on which the server will listen for statistics access.
Allow Message From	Address match lists allowed to request statistics.
Keys	Keys required for statistics access.

Zones on a DNS Server

DNS Zones are the mechanism that is used to link DNS domains to DNS servers. IPAM provides you with complete control over DNS zones in order to provide you with the capability to model complex DNS infrastructure if needed. Click on the **Zones** link on the Network Services List to display the DNS Zones for the selected server.

Choose from the following actions.

- To delete one or more DNS Zones from this server, click the checkbox in the **Select** column for each item you wish to delete, and click . At the confirmation prompt, click **OK** to delete the selected zones, or **Cancel** to not delete any zones.
- To refresh the DNS Zones list, click .
- To exit the DNS Zones list and return to the list of servers, click .
- To add a DNS Zone, refer to the following section.
- To edit a DNS Zone, refer to “Editing A Zone” on page 105.

Adding a DNS Zone

To add a DNS Zone, follow these steps.

1. Click the **Add DNS Zone** link. The Add Zone screen appears.
2. In the **Zone Type** fields. Select the type of zone you want to create. The choices are:
 - a. master
 - b. slave
 - c. forward (except CNR Authoritative Servers)
 - d. stub (except CNR Authoritative Servers)
 - e. static-stub (since BIND 9.8)
 - f. redirect (since BIND 9.9)

The **Show All Product Options** checkbox is automatically selected and different zone options appear depending on the selected zone type.

3. In the **Domain** field, select the domain you want to attach to the DNS server. Click **Search** to open the Domain Search screen, where you can refine your search to **Forward** and **Reverse** domains, in addition to **All**.

Redirect zones only:

- The "Domain Name" search will be hidden, and the page will instead show a Domain Type down, if there are multiple domain types defined, otherwise the Domain Type field will be read-only and set to the "Default" domain type. The zone itself will be the "." domain for the given type.
 - The "View" selection (if applicable) is available, but the limit is one Redirect per view.
4. *Optional for non-master zones.* Enter the filename to contain the DNS zone data that is automatically created. The data can be overwritten, if necessary.
 5. Choose from the following actions.
 - ▶ If you select **master**, enter the data described in Table 4-11.

Table 4-11 Master Zone Type Parameters

Field	Description
Automatic Generation of NS/Glue Records	Checked indicates that you will let IPAM automatically create the NS and Glue Records for this zone/domain. If you uncheck this option, the IPAM system will not automatically create these records, and you may enter your own NS and Glue records. Please refer to your DNS administrative manual for correct creation of the required records. Failure to create the proper NS and Glue records potentially will prohibit the DNS server from starting, or loading this zone.
Include Server in NS List for this Zone	If this is checked, an NS record will be created for this server in this zone. If it is unchecked, this server will be stealth and not listed in the NS records for this zone.
Use Alternative MNAME	Select this checkbox to indicate that you want to use an alternative MNAME within the SOA record. Enter that MNAME in the Alternative MNAME field.
Allow DNS Listener to Accept Zone Transfers	Select this checkbox to ensure that the IPAM DNS Listener accepts zone transfers from this server for this zone, if the zone is dynamic.
Enable Dynamic Updates	Select this checkbox to indicate that this zone will use dynamic updates. Select the option, Update Policy or Allow Update, which will be used. One of these options must be specified.
Update Policy	An option for dynamic zones that specifies an update policy, already defined in the system, which includes detailed rules. Click Policy List to select a policy or policies.
Allow Update	An option for dynamic zones that defines an address match list of IP addresses that are allowed to send updates to the zone. Click Address List to select a match list or lists. You can also enter the match list in the text area.

- ▶ If you select **slave** or **stub**, enter the IP addresses of the master DNS servers for this slave/stub zone in the **Masters** field. These addresses map to the “masters” option on the zone. For example: 10.0.0.2; 10.0.0.6.

6. Select the necessary zone options. If you need information on a zone option, follow these steps:
 - a. Select the vendor Options link () in **Management > DNS > Option Vendor Dictionary**.
 - b. Click the option link in the **Name** column that you want information on. The Edit DNS Dictionary Option screen contains a **Description** field.
7. To add zone extensions, click the **Zone Extensions** tab and enter extension data as needed in the **Insert Prior to Resource Records** and **Insert After Resource Records** columns.
8. When your definition of the zone for the selected server is complete, click **Submit** to save your changes.

Editing a DNS Zone

To modify an existing DNS Zone, click on the Zone name in the DNS Zone List. The Edit DNS Zone screen opens.

Edit the DNS Zone as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Configuring DNS Views on a DNS Server

DNS Views are very useful in a firewalled environment since they allow you to present one name server configuration to one community of hosts and a different configuration to another community. This is particularly handy if you are running a name server on a host that receives queries from both internal and external hosts. Click on the **Views** link on the Network Services List to display the DNS Views for the selected server.

Choose from the following actions:

- To refresh the DNS Views list, click .
- To exit the DNS Views list and return to the list of servers, click .
- To add a DNS View, refer to the following section.
- To edit a DNS View, refer to “Editing a DNS View” on page 107.
- To delete one or more DNS Views, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected DNS View, or **Cancel** to not delete the selected DNS View.

Adding a DNS View

To add a DNS View, click the **Add DNS View** link. The Add DNS View screen opens.

Table 4-12 Add DNS View Parameters

Field	Description
General Tab	
Name	Enter a unique name for the DNS View.
Class	Select the appropriate Class that will be assigned to this view.
Match Clients	Specify the hosts that will “see” the view using this statement. Any hosts that are part of this group will see this view. You may use an ACL name to make this option more readable. This option checks the source IP Address of the host.
Match Destinations	Specify the hosts that will “see” the view using this statement based on the destination IP Address of the packet.
Match Recursive Only	Checked indicates that only recursive requests from matching clients will match this view. BIND Only.
Options Tab	
Show All Product Options	Click on this option to display all DNS options that are available to be associated with this view. Many of the options are described in Management > DNS > Option Vendor Dictionary . BIND Only.
Zones Tab	
Search	Displays the zones that are associated with this view. Use the Search function to filter the list of zones that are displayed on this page. To associate a zone with a view, select it in the list. BIND Only.
Extensions Tab	
Insert at beginning of view definition	Enter custom text to write into named.conf at the beginning of each view definition. BIND Only.
Append at end of view definition	Enter custom text to write into named.conf at the end of each view definition. BIND Only.
Add Server Link	
Server IP	IP Address of the remote server that this server will interact with within this view. BIND Only.
TSIG Key	Choose a TSIG Key from the list of keys defined in IPAM that will be used in communication with the remote server defined in the Server IP field. BIND Only.

Enter the desired attributes once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Once created, you may reorder the DNS Views by pressing the corresponding **Up** and **Down** buttons.

Editing a DNS View

To modify an existing DNS View, click on the view name in the DNS View List. The Edit <viewname> screen opens.

Edit the DNS View as needed. Refer to Table 4-12 for information on fields on the different tabs. When you have completed your changes, click **Save** to implement your changes, or **Cancel** to undo your changes and return to the previous screen.

Note that the default view for CNR Authoritative DNS servers is read only and cannot be moved from the last place in the view list.

Configuring Zone Templates on a DNS Server

In some cases, if you are dealing with large numbers of domains, you may want to create a “template” zone data file that allows you to use a single data file for multiple zones. IPAM supports this feature using the “template” domain menu item. It allows you to create a “template” domain, associate resource records within that domain, and then utilize that single domain over and over for various zones.

Make sure that all of the owner names of records within the zone are “@” (short for origin), or relative, and do not include a trailing dot. Click on the **Templates** link on the Network Services List to display the DNS Zone Templates for the selected server.

Choose from the following actions:

- To delete one or more DNS Zone Templates, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected channels, or **Cancel** to not delete the selected channels.
- To refresh the DNS Zone Templates list, click .
- To exit the DNS Zone Templates list and return to the list of servers, click .
- To add a DNS Zone Template, refer to the following section.
- To edit an existing DNS Zone Template, click on the zone name link in the template list. The Edit Zone <zonename> screen opens. Make changes as described in “Adding a DNS Zone Template”, in the next section.
- To add an alias domain to attach to a DNS Zone Template, or view a list of existing alias domains, click the **Aliases** link. For more information, refer to “DNS Zones Template Aliases” on page 109.

Adding a DNS Zone Template

To add a DNS Zone Template, click the **Add DNS Zone Template** link. The Add DNS Zone Template screen opens.

1. In the **Domain** field, select the domain you want to attach to the DNS server. Click **Search** to open the DNS Domains screen, where you can refine your search to **Forward** and **Reverse** servers, in addition to **All**.
2. In the **Filename** field, a default filename to contain the DNS zone data is automatically displayed. You can change the filename if desired.
3. Refer to Table 4-11 on page 103 to complete the remaining zone template fields.
4. In the **Zone Options** tab, select the necessary zone options. If you need information on a zone option, follow these steps:
 - a. Select the vendor Options link () in **Management > DNS > Option Vendor Dictionary**.
 - b. Click the option link in the **Name** column that you want information on. The Edit DNS Dictionary Option screen contains a **Description** field.
5. To add zone extensions, click the **Zone Extensions** tab and enter extension data as needed in the **Insert Prior to Resource Records** and **Insert After Resource Records** columns.
6. When your definition of the zone for the selected server is complete, click **Submit** to save your changes.

DNS Zones Template Aliases

To view existing domain aliases for a DNS Zone Template, click the **Aliases** link beside the desired zone template in the DNS Zone Templates list. The DNS Zones Template Aliases for <zonename> screen opens.

Choose from the following actions:

- To add a DNS Zones Template Alias, follow these steps:
 - a. Click the **Add DNS Zones Template Alias** link.
 - b. In the DNS Domains Search window, select the domain alias you want in the list.
The domain alias is added to the Aliases list
- To delete one or more DNS Zones Template Aliases, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected aliases, or **Cancel** to not delete the selected aliases.
- To refresh the DNS Zones Template Aliases list, click .

- To exit the DNS Zones Template Aliases list and return to the list of servers, click 

Configuration/Deployment

The Configuration/Deployment option allows you to create on-demand, scheduled, or recurring scheduled tasks for deployment of configuration information to your DNS network services.

Configuration/Deployment Task Definition Options

To deploy configuration information to a network service, select the “task type”, select the “network service”, and then specify when to run the task. Depending upon the selection of when you will be running the task, different options will be displayed on the screen for you to select. Refer to the sections below for additional information about each option. Note that once you click **Submit**, a new task will be created, and submitted to the system. Once tasks have been created, they can be managed using the **Tasks** menu option.

Table 4-13 Configuration/Deployment Screen Elements

Field	Description
Network Service	<ol style="list-style-type: none">1. Click the Search button. The DNS Servers/Services screen opens.2. Select a DNS server from the list. To restrict your search, enter search criteria and click the Search button. The selected server is displayed in the Network Service field.

Field	Description
Task Type	<p>Select the type of task that you want to run.</p> <ul style="list-style-type: none"> • DNS Configuration – All Files creates all configuration files (configuration and zones) for the DNS server that you selected. • DNS Configuration – Changed Zones Only creates the configuration file and only the changed zone files for the DNS server that you selected. • DNS Configuration – Selected Zones Only creates the configuration file and only the selected zone for the DNS server that you have selected. <p>Note: For more information, refer to “Configuring INS DNS for Selected or Changed Zone Push” on page 275.</p> <ul style="list-style-type: none"> • DNS Configuration – Configuration Only creates only the configuration file for the DNS server that you selected. • DNS Configuration – Changed Resource Records Only (via DDNS) sends all changed resource records to the selected DNS server via RFC2136 dynamic DNS updates. • DNS Configuration – All Resource Records (via DDNS) sends all resource records for the selected zone, or all zones, for the selected DNS server via RFC2136 dynamic DNS updates. • DNS Configuration - - All User-created Resource Records (via DDNS) is similar to the previous option. However, the resource records selected are limited to those created on IPAM via the GUI or a CLI/API. This enables the refreshing of these records in Microsoft AD DNS to prevent their scavenging, while not interfering with the intended scavenging of dynamic records. <p>CNR Authoritative server</p> <ul style="list-style-type: none"> • Update Configuration for Changed Zones Only creates new zones (including RRs), as well as updates the configuration of any zones that have changed. There is <i>no</i> overwrite option with this deployment type. • Update Configuration creates new zones and populate them with RRs and updates the configuration only for existing zones. If Overwrite Zones is checked, all zones will be removed and recreated with the current RRs for those zones. You can select either All Zones or a specific zone to update. • Update Changed Resource Records sends all changed resource records to the selected server. This task sends deletes and adds of resource records via standard Dynamic DNS update protocol (RFC 2136) in order to change the records as required. • Update All Resource Records sends all resource records for the selected zone, or all zones, for the selected server. This task sends adds of all resource records defined for the zone in IPControl via standard Dynamic DNS update protocol (RFC 2136). It is used to completely refresh the zone in situations where the authoritative server has been replaced.

Field	Description
Task Type	<ul style="list-style-type: none"> • Update User Created Resource Records sends resource records that are created in IP Control via the GUI or a CLI/API. This task sends adds of resource records defined for the zone in IPControl via standard Dynamic DN update protocol (RFC2136). These records are a subset of those sent for the Update All Resource Records task, and do not include records that that were “learned” by IPControl via the DNS Listener. <p>CNR Caching server Full Server Configuration creates all configuration files (configuration and zones) for the selected server.</p>
The following options are based on which type of task is selected	
Perform DNS configuration file check	If checked, then the configuration file check script specified when the DNS net service was created will be run against the <code>named.conf</code> file created for DNS Configuration tasks.
Perform DNS zone file check	If checked, then the zone file check script specified when the DNS net service was created will be run against the zone files created for DNS Configuration tasks.
Stop on Critical Errors	For DNS Configuration tasks, if either the Perform DNS Configuration File Check or Perform DNS Zone File Check options are selected, selecting this task option causes the configuration task to abort if either of the check scripts returns a non-zero value, indicating an error has been found in the configuration or zone file. If aborted, the DNS server is not stopped or restarted, and the current DNS configuration remains unchanged.
Hold files for preview	If checked, the configuration files will be created, but not deployed. You can view the files from the Task List.
Delete Task if No Zones to Generate	If checked, indicates that the task will be deleted when there are no changes to the configuration.
Delete Task if No Resource Records to Generate	If checked, indicates that the task will be deleted when there are no changes to the configuration.
When to run task	<ul style="list-style-type: none"> • Immediate – Run the task immediately • Scheduled – Run the task on the predetermined date and time specified • Recurring – Run this task multiple times

On-demand (Immediate) Config/Deployment Task

To define an immediate task, define the task parameters and select **Immediate** from the **When to run task** options. Click **Submit** to create the task. A new task is created and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled Config/Deployment Task

To schedule a future task, define the task parameters and select **Scheduled** from the **When to run task** selections. Schedule options are displayed.

To select a future date to run the task, type in the desired date in mm/dd/yyyy format or click the calendar icon to select a date. A calendar is displayed, with today's date selected by default.

You can use the following navigation links to change to another month and/or year and then select a date in the month to close the utility:

 Previous Year

 Previous Month

 Next Year

 Next Month

Select the hours, minutes, and AM or PM to schedule a specific time for the task.

Once all parameters have been entered, click **Submit**. A new task is created, and submitted to the system. Once tasks have been created, they can be managed using the **Tasks** menu option on the **Tools** menu.

Recurring Config/Deployment Task

A recurring task enables you to define tasks to run on a pre-determined schedule. This option allows you to define tasks (such as DNS Configuration) that will occur at regular intervals, providing you with up to date information. To schedule a recurring task, set the task parameters and select **Recurring** from the **When to run task** selections. Recurring options are displayed.

Select the date and time that the recurring task is to begin. This is the first occurrence of the recurring task. Click on the calendar icon to display a calendar. Refer to “Scheduled Config/Deployment Task” on page 114 for information on using the calendar utility.

Select the **Frequency** for the recurring task:

- Sub-Daily
- Daily
- Weekly
- Monthly
- Yearly

Once all the parameters have been selected or entered, click **Submit**. A new task is created and submitted to the system. Once tasks have been created, you can manage them using the **Tasks** menu option on the **Tools** menu.

Domains

DNS's distributed database is indexed by domain names. Each domain name is essentially just a path in a large inverted tree, called a domain name space. The tree's hierarchical structure is similar to the structure of the UNIX file system. The tree has a single root at the top. This is called the root directory, represented by a slash. DNS simply calls it "the root". Like a file system, DNS's tree can branch out any number of ways at each intersection point (or node). Each node of the tree has a text label that can be up to 63 characters long.

If you have Internationalized Domain Names, the  icon will appear. Click on the icon to change how domain names are displayed. Hover over the cells marked with a  to see domain names in alternative formats.

Managing DNS Domains

To work with DNS domains, follow these steps.

1. Select **Domains** from the DNS section of the **Management** menu. The hierarchy refreshes to show the zones in the root container and a list of domains appears.
2. Choose from the following actions.

To ...	Then ...
Search for a particular DNS Domain	<ol style="list-style-type: none"> 1. Select the type of search in the drop down to the left of the search box. This specifies if the search string Contains, Begins With, Ends With, or Is Exactly what is specified. Note: Domain searches in IPAM are performed using the ASCII representations. If you wish to search Internationalized Domain Names, select Is Exactly and type a full IDN domain name or to do a partial search using Contains, Begins With or Ends With type full/partial ASCII domain name in the search box to get back the desired result. Partial IDN search does not work. 2. Select All, Forward, or Reverse from the Search drop-down list. 3. Enter a search string in the text block. 4. Click on the filters icon  to display optional filters. This allows you to select one or more domain types to limit the search by. This is only applicable if you have configured domain types within IPAM. 5. Click Search. The list of domains changes to match the search string.
Add a DNS Domain	Click on the Add DNS Domain link to open the Add DNS Domain page.

To ...	Then ...
Refresh the DNS Domain list	Click  .
Edit a DNS Domain	<ol style="list-style-type: none"> 1. Click on the domain name in the Domain list. The Edit DNS Domain <domainname> screen opens. 2. Edit fields and tab entries as needed. Refer to “Editing a DNS Domain” on page 118.
Delete one or more DNS Domains	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Domains, or Cancel to return to the previous screen.

3. After you have finished entering the desired attributes for Add or Edit, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a DNS Domain

To add a DNS Domain, follow these steps.

1. Click the **Add DNS Domain** link. The Create DNS Domain screen appears.
2. Type the requisite values in the fields, as described in Table 4-14.

Table 4-14 Create DNS Domain Parameters

Field	Description
Name	Enter a unique name for this Domain.
Managed	Checked indicates that this domain/zone is fully defined in IPAM. That is, all resource records and all other definitions about this domain/zone will be completely described in the IPAM product. A “Managed” Type (and only a Managed Type) can be associated to a DNS server as a DNS “Master”. It can also be associated to an IPAM DNS server as a “Slave”, “Stub”, or “Forward” zone, but only if the zone is associated to at least one “Master” IPAM DNS server. For example, a zone, company.com, can be defined as a Master on server DNS1, a Slave, on server DNS2 (pointing to DNS1 as its Master), a Stub on DNS3 (pointing back to DNS1 and DNS2 as authoritative), and a Forward on DNS4 (forwarding to DNS1 and DNS2). Also, a Managed domain/zone can be associated to multiple IPAM DNS servers as “Masters”. A “Delegate-Only” zone is treated exactly like a Master, but a BIND 9.2.3 server (or higher) would only respond with delegation (referral) information for child zones defined, not with any authoritative information from the zone itself. Unchecked indicates that this domain/zone is “Un-Managed”– This domain/zone is declared to IPAM as falling outside the scope of IPAM definition. It is a way to get a zone statement into a DNS server that is a Slave, Stub or Forward for a zone defined outside of IPAM. For example, if there is a business partner that has the domain anothercompany.com, and nothing is known about this zone in IPAM, yet an IPAM DNS server will need to have some information about it, an Un-Managed domain in IPAM will allow the proper zone statement to be built in the boot file to get information from a DNS Server outside the IPAM definition sphere.
Delegated	Checked indicates that this domain may be associated directly with a zone file. If the delegated flag is turned off, this domain and its resource records will be written in a zone file that is associated with a parent domain.
Reverse	Checked indicates that this is a reverse domain.

Field	Description
Derivative	The role of this domain. <ul style="list-style-type: none"> • Standard – indicates a standard domain. • Template – indicates that this domain is a template and can be used as a template domain for when you want to use a single data file for multiple zones. • Alias – indicates that this domain is aliased to a specified template. In this case, no resource records are attached to the alias, all resource records are inherited from the template domain. When this type of domain is specified, the user must select a “template” domain to associate with this alias.
Serial Number	DNS Serial number for this domain.
Refresh	The refresh interval tells a slave for the zone how often to check that the data for this zone is up to date.
Retry	If the slave fails to reach the master name server after the refresh interval (the host could be down), it starts trying to connect every <i>RETRY</i> seconds.
Expire	If the slave fails to contact the master name server for <i>EXPIRE</i> seconds, the slave expires the zone.
Negative Cache TTL	TTL stands for “Time to Live”. This value applies to all negative responses from the name servers authoritative for the zone.
Default TTL	The default Time to Live value. For BIND 8.2 and later, this will be the \$TTL value that is written in the zone file.
Contact	The contact email address in dotted format. For example, an email address of ‘ root@ins.com ’, would be represented as <code>root.ins.com</code>
Information Template	Choosing Information Template will add the User Defined Fields in that Template to this domain. Default selection is “—None—”.
Created On	Date and time this domain was created. Read only, appears on edit screen.
Last Modified On	Date and time this domain was modified. Read only, appears on edit screen.
Last Modified By	Name of the administrator who last modified the domain. Read only, appears on edit screen.

Editing a DNS Domain

To modify an existing DNS Domain, follow these steps.

1. Click on the domain name in the DNS Domain List. The Edit DNS Domain screen opens.
2. Type the requisite values in the fields, as described in Table 4-14.
3. Choose from the following actions.

To ...	Then ...
Modify values for the currently selected domain	Refer to Table 4-14 on page 117 for information as you make your edits.
Add additional information template data	<ol style="list-style-type: none"> 1. Click Set Information Template. The Set/Remove Information Template opens. 2. Select one of the information templates to add additional fields to the DNS Domain record. For more information on Information Templates, refer to “Information Templates” on page 260. 3. Click Submit. Extra fields for the selected information template are added to the DNS Domain record.
View and edit the DNS resource records that are associated with the current domain	Click the Resource Records tab. For more information on Resource Records, refer to the section below.

Managing Resource Records

Resource records can be maintained from the Resource Records Tab.

To search for a resource record, enter a search string into the search box and hit search. To delete one or more resource records, click the checkbox in the select column for each item you wish to delete, and click the delete icon. You will be prompted for confirmation. Click OK to delete the selected resource record(s), or cancel to return to the previous screen. To add a resource record, click the Add Resource Record Link. The Add Resource Record screen will appear. To edit an existing record, click on the link in the owner column to open the Edit Resource Record screen.

If you enter/edit Internationalized Domain Names, the  icon will appear. Click on the icon to change how the owner and data fields are displayed. Hover over the cells marked with a  to see the fields in alternative formats.

Table 4-15 Resource Records Tab Screen Elements

Field	Description
Device	Indicates if this resource record was created from a device.
Owner	The owner of the resource record. Note that this section is specific to the type of resource record. Refer to the appropriate RFC for the exact text that should be entered.
Class	The class of the resource record.
Class Type	The type of the resource record.
TTL	The time to live of the resource record.

Field	Description
Data	The data field of the resource record. Note that this section is specific to the type of the resource record. Refer to the appropriate RFC for the exact text that should be entered.

About Resource Records and Workflow

When you add or edit a resource record, resource record approval access is checked on the domain for the resource record. If you have the required access, the record is added and is eligible for pushing/deployment. If the required access is not granted to you, then the record is added in a “Pending” approval state. In this state it will need an approval from an administrator with resource record approval access on the given domain to be eligible for pushing/deployment. The same behavior applies when you try to edit or delete a resource record. In effect, the Pending Action on a resource record may be ‘Create’, ‘Update’ or ‘Delete’ or empty. An empty value for Pending Action means that the record has been approved or does not require approval.

In addition to the fields associated with a resource record such as Owner, Class, Type, and so on, this list has two additional fields, as described in Table 4-16.

Table 4-16 Resource Records Tab Screen Elements

Field	Description
Device	
Pending Changes	<p>This field can have the following values.</p> <ul style="list-style-type: none"> • Empty – An empty field indicates this is an approved record. • Create – Creation of a new record is awaiting approval. • Delete – A delete on an existing record is awaiting approval. • Update – An update to an existing record is awaiting approval.
Details	<p>When you click on the Details icon, a pop-up appears with the details regarding the record. The fields in the pop-up include:</p> <p>Last Update time – time of the last update to the record.</p> <p>Admin – login name of the user that last updated the record.</p> <p>Create Source – source of record creation, for example, GUI, API, Host discovery.</p> <p>Update Source – source of last update, for example, GUI, API, Host discovery.</p> <p>Approvers – A list of administrators that are eligible to approve this record. This field is displayed only in the case of a pending record. An administrator needs to have resource record approval access on a given domain to be an approver.</p> <p>To close the pop-up, click the Details icon again.</p>

Adding a Resource Record

You can define a resource record for the current domain. Note that resource records for IP Addresses (devices) can be generated automatically when IP Addresses are added to the system.

To add a Resource Record, follow these steps.

1. Click on the **Add Resource Record** link. The Add Resource Record screen opens.
2. Select the record type from the **Resource Record Type** drop-down.
3. Enter the fields associated with the resource record type, such as Owner, Class, and Data.
4. Click **Save Resource Record** to save your changes, or **Cancel** to return to the previous screen.

Editing a Resource Record

To edit a resource record, follow these steps.

1. Locate the record you want to edit. You can locate a record quickly by entering search criteria and selecting either **Owner** or **RDATA** from the **Search** drop-down.
2. Select the **Owner** link for the resource record you want to edit.
3. Make changes as required. You can change the Resource Record Type, Owner, TTL and RDATA fields.
4. Click **Save Resource Record** to save your changes, or **Cancel** to return to the previous screen.

Deleting a Resource Record

To delete resource records, click on the checkbox next to the items that you want to delete, and click .

Galaxies

A DNS Galaxy is a management technique that can be used to help automate the task of assigning Domains to DNS Servers. The concept is that you may define a group of DNS servers (known as a Galaxy) that includes a master DNS server and one or more slave DNS servers. Once the Galaxy is defined, you may assign Domains directly to a Galaxy, and when DNS configuration is generated by the system, all DNS servers will include an entry for the domain.

This saves the DNS administrator the step of having to assign the domain to each of the DNS servers individually. If your organization uses a large number of DNS servers, or manages a large number of DNS Domains, this feature helps save considerable administrative effort.

Use this menu item to maintain DNS Galaxies within the system.

To delete one or more DNS Galaxy, click the checkbox in the **Select** column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected domains, or **Cancel** to not delete the selected domains.

Adding a DNS Galaxy

To add a DNS Galaxy, click the **Add DNS Galaxy** link. The Create DNS Galaxy screen appears.

Table 4-17 Add DNS Galaxy Parameters

Field	Description
Name	Enter a unique name for this Galaxy.
Description	Enter a description for this Galaxy.

Enter the desired attributes once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing DNS Views for Galaxy

DNS Views are a mechanism that is very useful in a firewalled environment. Views allow you to present one name server configuration to one community of hosts and a different configuration to another community. This is particularly handy if you are running a name server on a host that receives queries from both internal and external hosts.

To add or modify DNS Views for this Galaxy, click the **Views** option from the DNS Galaxy List, shown on Figure 4-31.

The DNS View List for this Galaxy opens. By default, a DNS View named **GalaxyDefault** is created for each Galaxy. You can add additional views, and order them accordingly by clicking on the **Up** or **Down** buttons. View parameters can be edited from here by clicking on the view name. These parameters include view options and extensions as described in the “Configuring DNS Views on a DNS Server” section. You can also delete Views from the Galaxy by selecting the View you want to delete and clicking .

Editing DNS Server Profiles for Galaxy

To add or modify the DNS servers that are associated with this Galaxy, click on the **Profiles** option from the DNS Galaxy List. The DNS Profile List for this Galaxy opens. Using this screen, you can add, delete, and modify the list of DNS servers.

When you select the **Add DNS Galaxy Profile** option, you can select the DNS server, product, and specify Zone options for these servers. Use this screen to manage the list of Master and Slave Servers for this Galaxy, as well as the zone options that are available for these servers.

Table 4-18 Add DNS Galaxy Profile Parameters

Field	Description
Product	The DNS product type that you have selected for this group of servers.
Type	Select the type of DNS server(s) that you will be adding to this Galaxy.
Masters	Only appears if “slave” or “stub” is selected. Enter the IP addresses of the master DNS servers for this slave/stub, separated by semicolons. Maps to the “masters” option on the zone. For example: 10.0.0.2;10.0.0.6
Generate Filename Option	Indicates whether the “file” option should be generated for Galaxy Profiles of type Slave or Stub.
Location	Enter the relative directory name of where the zone files for this group of servers will be created on the DNS servers. This “location” ends up as part of the path (appended to the configuration directory). Note: It needs to end with a \ or / or else it becomes part of each zone file name. For example: galaxyslave/
DNS Servers	Click Add DNS Server and select a DNS server to add to this Galaxy from the Service Name list in the Available DNS Servers screen. If this is to be a stealth server, uncheck “Include this Server in NS Record List” and for master profiles, specify an alternate mname.
Zone Options	Add any zone options that you want to have associated to this Galaxy for this type of server.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Log Channels

The Logging Channels screen allows you to maintain DNS Log Channels. Logging for BIND DNS servers is accomplished with two main concepts: *channels* and *categories*. A channel specifies where logged data goes (that is, syslog, to a file, and so on.). A category specifies what data is logged. In a BIND-based DNS server, most messages that the name server logs are categorized according to the function of the code they relate to.

Select the **Log Channels** option to enable you to define global (system-wide) logging channel definitions that you can use throughout the system.

To delete one or more logging channels, select the checkbox beside each item you wish to delete, and click . At the confirmation prompt, click **OK** to delete the selected channels, or **Cancel** to return to the previous screen.

Note: Make sure that the logging channels that you are deleting are not associated with a DNS server.

Adding a Logging Channel

To add a logging channel, click the **Add Logging Channel** link. The Add Logging Channel screen appears.

Table 4-19 Create Logging Channels Parameters

Field	Description
Channel Name	Enter a unique name for the Logging Channel.
Output Destination	Select the destination where you want to send the log output: <ul style="list-style-type: none"> • Disk File – A disk based file(s) • System Log (syslog) – The system Log • Standard Error Output (stderr) – Stderr as defined by the DNS server. • Null – Nowhere. Messages sent to this channel will be discarded.
Syslog Facility	This option is only applicable if you have selected “System Log (syslog)” as the Output Destination. Select the appropriate syslog facility based on your operating system and configuration.
File Path	This option is only applicable if you have selected “Disk File” as the Output Destination. Enter the fully qualified path and file name that will receive the log information. Example “file.msgs”
File Versions	This option is only applicable if you have selected “Disk File” as the Output Destination. Enter the number of versions of the file to keep at any point in time. For example, if you specify “3” as the File Versions, and “file” as the File Path, each time the server is stopped and restarted, it will copy the current version to a backup copy. It will increment a number and append that number to the file name of the backup file(s). Over time, you will end up with file, file.0, file.1, and file.3.
File Size	This option is only applicable if you have selected “Disk File” as the Output Destination. Specifies the maximum file size of the log channel. The name server will stop writing to this channel if the maximum size is reached. You can enter the size of the file using a scaling factor such as “k” to indicate kilobytes, and “m” to indicate megabytes, or “g” to indicate gigabytes of the file. For Example; “10k” – 10 kilobyte file size limit, “10m” = 10 megabyte file size limit

Field	Description
Severity	Channels allow you to filter messages based on severity. Use this option to specify what severity of message will be hosted by this channel. Here is a list of the supported severities sorted by most severe to least severe: <ul style="list-style-type: none"> • Critical • Error • Warning • Notice • Info • Debug (note: only level 1 is currently supported)
Print Category	If Yes, the Category of the message is printed within the log message.
Print Time	If Yes, the date/time of the message is printed within the log message.
Print Severity	If Yes, the severity of the message is printed within the log message.

Enter the desired attributes once finished, click **Submit** to save your changes, or **Cancel** to return to the Logging Channels screen.

Editing a Logging Channel

To modify an existing logging channel, click on the channel name in the Logging Channel List. The Edit Logging Channel screen opens.

Edit the logging channel as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the Logging Channels screen.

Server Templates

Use the DNS Server Templates screen to maintain Domain Name Server (DNS) definition templates. These templates allow you to standardize the definitions that are used to create DNS servers. When you create new DNS servers, you may alternately create them using one of the defined DNS Server Templates. This allows you to standardize on complex configuration settings, and apply them to servers in a “cookie cutter” manner.

Managing Server Templates

To work with DNS Server Templates, follow these steps.

1. Select **Server Templates** from the DNS section of the **Management** menu. The DNS Server Templates list appears.
2. Choose from the following actions.

To ...	Then ...

To ...	Then ...
Search for a specific server template	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The list of server templates changes to match the search string.
Define a new server template	Refer to “Adding a DNS Server Template” following.
Modify an existing server template	<ol style="list-style-type: none"> 1. Select the template name in the Template list that you want to modify. The Edit DNS Server Template screen opens, with an additional tab for Logging. 2. Edit the DNS Server template fields and tabs as needed. Refer to the following sections for more information on fields and tabs.
Delete one or more server templates	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you wish to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected server templates, or Cancel to return to the previous screen.

3. Once you have finished working with a DNS Server Template, click **Submit** to save it, or click **Cancel** to return to the previous screen.

Adding a DNS Server Template

To add a new DNS Server Template, follow these steps.

1. Click the **Add DNS Server Template** link. The Add DNS Server Template screen appears.

General Tab

2. Type values in the **General** tab, as described in Table 4-20.

Table 4-20 Add DNS Server Template Parameters

Field	Description
Template Name	The name of the DNS Server Template. This name appears in a select list when you are creating DNS Servers.
Create db.127.0.0 Loopback Address File.	If this option is checked, the system automatically creates the db.127.0.0 loopback address file. Name servers need this file to be sure that they can resolve localhost correctly.
Configuration Directory	The directory where the DNS configuration file, “named.conf”, is created.
Data Directory	The directory of where the DNS data files (that is, zone files) are created.

Field	Description
Product	Select the DNS Server product from the list. This controls the options that are available within this template.
Start Script	The script that is executed by the IPAM Agent to start the DNS server.
Stop Script	The script that is executed by the IPAM Agent to stop the DNS server.
Configuration File Check Script	The script that is executed to verify the Configuration File.
Zone File Check Script	The script that is executed to verify the Zone File.
CNR Userid	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Enter the user ID required to allow execution of the nrcmd and/or cnr_exim utilities for this cluster.
CNR Password	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Enter the password required to allow execution of the nrcmd and/or cnr_exim utilities for this cluster.
Confirm CNR Password	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Confirm the CNR password.
Port	<i>CNR DNS Authoritative and CNR DNS Caching only.</i> Enter the port that the CNR SDK listens on. The default is 1234.
Nrcmd Directory	<i>CNR DNS Authoritative only.</i> Enter the full pathname where the nrcmd command is located. Default locations are: UNIX: /opt/nwreg2/local Windows: C:\Program Files (x86)\Network Registrar\Local\bin

Extensions Tab

- Click on the **Extensions** tab to display the configuration file extensions area. The extensions area allows you to create free form text that is added to the beginning or the end of the *named.conf* configuration file.
- Type text as needed in the **Start of Named.conf** and **End of Named.conf** text areas, as described in Table 4-21.

Table 4-21 DNS Server Template Extensions Parameters

Field	Description
Start of Named.conf	A free text area that appears at the beginning of the <i>named.conf</i> file when the file is automatically generated. Note: The extensions are limited to 32000 characters.
End of Named.conf	A free text area that appears at the end of the <i>named.conf</i> file when the file is automatically generated. Note: The extensions are limited to 32000 characters.

Root Hints Tab

- Click on the **Root Hints** tab to display the configuration of the Root Hints file. The Root Hints file tells the DNS server where the name servers for the root zone are located.
- Select the **Create Root Hints File** check box, if required. Refer to Table 4-22 for more information.

Table 4-22 Root Hints Parameters

Field	Description
Create Root Hints File	Check this item on if you want to automatically create the “Root Hints” file when generating the DNS Configuration files.
Use Standard InterNIC supplied content	Only valid if you have checked the “Create Root Hints” file option. Select this option if you would like to use the InterNIC supplied content when generating this file.
Use Custom Root Hints file	Only valid if you have checked the “Create Root Hints” file option. Select this option if you would like to use custom content that you enter for the Roots Hints file.

Advanced Tab

- Click on the **Advanced** tab to display the advanced options that are available. These options include configuration of the “controls” section of the configuration file. Traditionally, DNS administrators have controlled the BIND DNS server with UNIX signals. The DNS server interprets the receipt of certain signals as an instruction to take a particular action, such as reloading zones that have changed. Because there are a limited number of signals, BIND has introduced a method of controlling the name server by sending messages to it on a special control channel. The control channel can be either a UNIX socket, or a TCP port the name server listens on for messages.
- Type values in the **Advanced** tab fields, as described in Table 4-23.

Table 4-23 Advanced Tab Parameters

Field	Description
TCP Port Control Channel Settings:	Select this option to send messages to the name server via a TCP/IP Port.
Listen on IP Address	Enter the IP Address for the name server to listen on for messages.
Listen on Port	Enter the Port that the name server will listen on for messages. Typically, this is port 953.
Allow Message From	Enter an IP Address, or the name of an Address Match List that specifies where messages are allowed to come from.
Keys (Used by rndc)	Select the key to be used by rndc.
UNIX Domain Socket Channel Settings:	Select this option to send messages to the name server via a UNIX Domain Socket.

Field	Description
UNIX Domain Socket	Enter the name of the socket that will be used for communicating with the name server. Typically this is <code>/var/run/ndc</code> , though some operating systems use a different pathname. The socket is usually owned by root and readable and writable only by the owner.
Permissions (in Octal Format)	The permission value must be specified as an Octal quantity (with a leading zero to indicate an octal quantity). For example; 0660
Owner (in Numeric Format)	Enter the Owner identifier.
Group (in Numeric Format)	Enter the Group identifier.

Options Tab

- Click on the **Options** tab to display the options and directives that are available. The options that are displayed are dependent upon the Product Selected, as well as the items configured in the Vendor Option Dictionary.

To view all available options for this product, click on **Show All Product Options**. All options that have been configured for the product selected (on the **General** tab) are displayed.

- Configure each option that you want to appear in the `named.conf` configuration file.

HA Pair Tab

On a CNR DNS Authoritative server, an HA DNS server pair is a symmetric backup system where both servers are masters for their zones.

- Click on the **HA Pair** tab to define a failover server for a CNR DNS Authoritative server.
- Enter the required values, as described in the following table.

Table 4-24 HA Pair Parameters

Field	Description
Backup Server IP Address	Enter the IP address of the failover server.
Backup Server Admin Name	Enter the admin user name to connect to the failover server.
Backup Server Password	Enter the password for the admin user name and then validate it in the Verify Password field.
Backup Server Port	Enter the port number that IPAM should use to communicate with the failover to have it sync. The port number default is 1234.

- If needed, check **Show All Product Options** and enter values, as described in Table 4-6 on page 99.
- If your administrator role has the required expert permission, you may need to expand the **Expert Options** section and enter values for the options, as described in Table 4-7 on page 100.

DNSSEC Tab

On a CNR DNS Caching server, the **DNSSEC** tab enables you to establish DNS Security settings.

1. Click on the **DNSSEC** tab to define DNS security options.
2. Check **Show All Product Options** and enter values as needed. Refer to the section DNS Option Master Dictionary for instructions on getting the description of each option.
3. If your administrator role has the required expert permission, you may need to expand the **Expert Options** section and enter values for the options. Refer to the DNS Option Master Dictionary for a description of each option.

DNS64 Tab

On a CNR DNS Caching server, the **DNS64** tab enables you to establish DNS64 settings.

1. Click on the **DNS64** tab to define DNS64 options.
2. Check **Show All Product Options** and enter values, as described in Table 4-8 on page 101.
3. If your administrator role has the required expert permission, you may need to expand the **Expert Options** section and enter values, as described in Table 4-9 on page 101.

Logging Tab

The **Logging** tab only appears when you modify a server template.

This option allows you to select logging channels for each category that is defined for the server. To add a channel to a category, follow these steps.

1. Click the **Choose** button next to the category you have selected. The Logging Channels screen opens.
2. Select the channels you want.
3. Click **Submit**. The channels you selected appear beside the category you selected in Step 1.

DNS Domain Types

The DNS Domain Types screen allows you to maintain DNS Domain Types. Domain types allow you to distinguish between domains that are used within your system. For example, if you are using the same domain name more than once within your system, you would place each domain in a different DNS Domain Type.

Managing DNS Domain Types

To work with DNS Domain Types, follow these steps.

1. Select **Domain Types** from the DNS section of the **Management** menu. The DNS Domain Types screen opens.
2. Choose from the following actions.

To ...	Then ...
Search for a particular DNS Domain Type	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The list of domains changes to match the search string.
Add a DNS Domain Type	<ol style="list-style-type: none"> 1. Click the Add Domain Type link. The Add Domain Type screen appears. 2. In the Name field, type the name of the DNS Domain Type you want to add.
Edit a DNS Domain Type	<ol style="list-style-type: none"> 1. Click on the domain type in the Name list. The Edit DNS Domain Type screen opens. 2. Edit the Name as needed.
Delete one or more DNS Domains Types	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Domain Types, or Cancel to return to the previous screen.

3. Click **Submit** to add the Domain Type, or **Cancel** to return to the previous screen.

Address Match Lists

Use the Address Match List screen to maintain Address Match lists. Domain Name Servers (DNS) use address match lists for nearly every security feature and even for some features that are not security-related at all. An Address Match List is a list of terms that specifies one or more IP addresses. The elements in the list can be individual IP addresses, IP Prefixes, or a named address match list.

IP prefixes have the format of (Network in dotted-octet format/bits in net mask). For example, 15.0.0.0 with a network mask of 255.0.0.0 can be represented as 15/8.

A named address match list is just that, a list of IP Addresses, IP Prefixes, and/or other named address match lists that have been associated with a name. For example; “my internal servers” name list could contain (15/8, 10.1.1.20, and 10.2.1.21).

Managing Address Match Lists

To maintain global Address Match Lists that can be used in various points within the system, follow these steps.

1. Select **Address Match Lists** from the DNS section of the **Management** menu. The Address Match List screen opens.
2. Choose from the following actions.

To ...	Then ...
Search for a specific Address Match List	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The Address Match list changes to match the search string.
Add an Address Match List	Refer to “Adding an Address Match List” following.
Edit an Address Match List	Refer to “Editing an Address Match List” on page 134.
Delete one or more Address Match Lists	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Address Match Lists, or Cancel to return to the previous screen.

3. Click **Submit** to add the new or modified Address Match List, or **Cancel** to return to the previous screen.

Adding an Address Match List

To add a new Address Match List, follow these steps.

1. Click the **Add Address Match List** link. The Add Address Match List screen opens.
2. In the **Address Match List Name** field, enter a name for this address match list. This name is displayed in drop-down lists when you are defining options.
3. In the **Description** field, enter a description of this address match list.
4. Click on **Add to Match List** to add actual values. The Add Address Match Entry screen opens.
5. Enter values in the fields, as described in Table 4-25.

Table 4-25 Add Address Match Entry Parameters

Field	Description
IP Address/Range	When selected, adds the single IP address that you enter to the match list. Note: You can use the exclamation mark “!” to create an exclusion, such as “!10.0.0.1”.
Address Match List	When selected, enables you to add a reference to a previously created match list.
TSIG Key	When selected, enables you to add a TSIG Key to the match list from the drop-down list.
Net Service	When selected, enables you to add a network service to the match list.
GeoIP	When selected, enables you to add a GeoIP lookup field and value to the match list. You may also select a GeoIP database (optional) to search to find a match. Note that GeoIP address match lists will only be pushed out to servers that allow support of geoip. That would include all BIND 9.10 and higher based servers.
Negate this Match	When checked, negates the query options you have previously selected. For example, if you have selected TSIG Key and chosen “rndc-key.” from the drop-down list, checking Negate this Match includes all TSIG Keys <i>except</i> “rndc-key.”

6. Once you have completed entering the Address Match List Name and Match List, click **Submit** to create the match list, or **Cancel** to return to the previous screen.

Editing an Address Match List

To modify an existing Address Match List, follow these steps.

1. Select the match list name in the **Address Match List** that you want to modify. The Edit Address Match List screen opens.
2. Choose from the following actions.

To ...	Then ...
Change the order of how match lists are written to the configuration file	Click the Up button to move the match entry up or click the Down button to move the match entry down.
Add to an Address Match List	Click on Add to Match List to add actual values. The Add Address Match Entry screen opens.
Edit a Match Entry	<ol style="list-style-type: none"> 1. Select the item in the Match Entry list you want to edit. The Edit Address Match Entry screen opens. 2. Make changes to the values, as described in Table 4-25 on page 133. 3. Click Submit.
Remove a Match Entry	Click the Delete button for each entry you want to remove.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Update Policies

The DNS Update Policies screen enables you to define update policy statements to apply to zone statements of type master.

Managing DNS Update Policies

To work with DNS Update Policies, follow these steps.

1. Select **Update Policies** from the DNS section of the **Management** menu. The DNS Update Policies screen opens.
2. Choose from the following actions.

To ...	Then ...
Search for a specific Update Policy	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The DNS Update Policy Details list changes to match the search string.
Add a DNS Update Policy	Refer to “Adding a DNS Update Policy” following.
Edit a DNS Update Policy	Click on a policy detail name in the DNS Update Policy Details list. The Edit DNS Update Policy screen opens.
View Details	Click  to open the “<policyname>: DNS Update Policy Details” page
Delete a DNS Update Policy	<p>Note: Make sure that the update policy that you are deleting is not associated with a DNS server.</p> <ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected DNS Update Policy, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a DNS Update Policy

To add a DNS Update Policy, follow these steps.

1. In the DNS Update Policies screen, click the **Add DNS Update Policy** link. The Add DNS Update Policy screen appears.
2. In the **Update Policy Name** field, enter a unique free form text string.

3. Click **Submit**. The new policy is added to the DNS Update Policy list.

Editing a DNS Update Policy

To modify an existing DNS Update Policy, click on a DNS Update Policy name link in the DNS Update Policies list. The Edit DNS Update Policy screen opens.

1. Edit the DNS Update Policy name as needed. **Name** must be *unique* amongst all update policies.
2. Once the desired attributes are finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a DNS Update Policy Detail

1. Add a policy detail by clicking  on the DNS Update Policy screen or the **Edit Details** link on the Edit DNS Update Policy screen. The <policyname> DNS Update Policy Details screen opens.
2. Click the **Add DNS Update Policy Detail** link. The <policyname>: Add DNS Update Policy Detail screen opens.
3. Type values in the fields, as described in Table 4-26.

Table 4-26 Add DNS Update Policy Detail Parameters

Field	Description
Action	Can be grant or deny. <ul style="list-style-type: none"> • Grant - allows an update if the rest of the rule matches. • Deny - denies an update if the rest of the rule matches.
Updater (ACL List/Identity)	A list of one or more IP addresses, network addresses, keys and/or named ACL references. Note key names must be prefixed with "key " (that is. "key key.example").
Match Type	Select from the dropdown list.
Value	A list of one or more ip addresses, network addresses, keys and/or named acl references. Note key names must be prefixed with "key", for example, key key.example . The supported wildcard characters are: <ul style="list-style-type: none"> • * Matches zero or more characters. For example, the pattern dhcp-* matches all strings with the dhcp- prefix including the string dhcp-. • ? Matches a single character. For example, the pattern zone?.com matches zone1.com, zone2.com, and so on but does not match zone.com • [...] Matches any characters listed within the brackets. For example, you can provide a range such as 0-9 or a-z. If the pattern also includes the - character, make it the first character in the list (for example, dhcp[-a-z]*)
RR Types	A comma delimited list of RR types for this rule. Each RR type can also be negated using the exclamation point (for example, !A,!TXT).

Field	Description
	You can also specify all types with an asterisk *.

- Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing a DNS Update Policy Detail

To modify an existing DNS Update Policy Detail, follow these steps:

- On the <policyname>: DNS Update Policy Details screen, click . The <policyname>: Edit DNS Update Policy Details screen opens.
- Follow instructions in “Adding a DNS Update Policy” to modify the settings.

Transaction Keys

The Transaction Keys screen allows you to define system wide global Keys, and use these throughout the system to provide DNS security. The keys that are defined within this option can be used to help secure the following:

- Dynamic DNS updates from the INS DHCP server to an INS or BIND DNS Server.
- Dynamic DNS updates from the ISC DHCP server to an INS or BIND DNS Server.
- Dynamic DNS updates from IPAM to CNR Servers or INS/BIND DNS Servers.

The Transaction Keys are used to sign DNS messages with a Transaction Signature (TSIG).

Managing Transaction Keys

To work with Transaction Keys, follow these steps.

- Select **Transaction Keys** from the DNS section of the **Management** menu. The Transaction Keys screen opens.
- Choose from the following actions.

To ...	Then ...
Search for a specific Transaction Key	<ol style="list-style-type: none"> Enter a search string in the text block. Click Search. The Transaction Key list changes to match the search string.
Add a Transaction Key	Refer to “Adding a Transaction Key” following.

To ...	Then ...
Edit a Transaction Key	<ol style="list-style-type: none"> 1. Click on the Key name in the Transaction Keys list. The Edit Transaction Key screen opens. 2. Edit the key as needed. Refer to Table 4-27 for information on the fields.
Delete a Transaction Key	<p>Note: Make sure that the keys that you are deleting are not associated with a DNS server.</p> <ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Transaction Keys, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a Transaction Key

To add a Transaction Key, follow these steps.

1. In the Transaction Keys screen, click the **Add Transaction Key** link. The Add Transaction Key screen appears.
2. Type values in the fields, as described in Table 4-27.

Table 4-27 Add Transaction Key Parameters

Field	Description
Key Name	Enter a unique name for the Transaction Key. From a syntax perspective, it must have the same naming rules as a fully qualified domain name, including the trailing dot. Example: tkey1.ins.com.
Key Algorithm	Select the key algorithm to be used for this key: HMAC-MD5 – one way hash function variant of MD5.
Secret	Shared secret that is used to sign the transactions when using this key. This is a base 64 encoded value. You can use the Generate button to automatically generate a base 64 secret. If you choose your own secret, you must put in the base 64 equivalent of the secret.
Confirm Secret	Confirm the shared secret.
Unmask Secret	Unchecked indicates that the Secret and Confirm Secret fields are masked. Checked indicates that the Secret and Confirm Secret fields are not masked and you can see the secrets on the screen. You can use this option to cut and paste secrets.

Field	Description
Generate a Secret	Use the Generate button to generate a random secret in base 64 encoding. Select the number of Bits to use to generate the key.

DNS Option Vendor Dictionary

Use the DNS Option Vendor Dictionary screen to maintain DNS Vendor Options within the system. Vendor Options are DNS options that are specific to a vendor or type of DNS server. This menu item allows you to select a set of options (from the DNS Master Option List) that are available for use with a specific type of DNS server. In addition, the syntax for this option is (as written to the configuration file) is specified using this menu item as well.

When you access the DNS Option Vendor Dictionary screen, the existing DNS Products are shown. You can add, modify, and delete DNS Products using **DNS Software Products** on the Management menu.

Managing DNS Option Vendor Dictionaries

To work with DNS Option Vendor Dictionaries, follow these steps.

1. Select **DNS Option Vendor Dictionary** from the DNS section of the **Management** menu. The DNS Option Vendor Dictionary screen opens.
2. To modify the options associated with a DNS Product, click the **Options** icon () next to the DNS product that you want to change. The DNS Options for <DNS Product> screen opens.
3. Choose from the following actions.

To ...	Then ...
Change the parameters for an enabled option	Refer to Table 4-28 as you decide which option to apply.
Add a new option to the product	<ol style="list-style-type: none"> 1. Select the Show all options checkbox. All the options in the system are displayed. 2. Select the Enabled checkbox beside the option you want to add. 3. Select the appropriate checkboxes in the Option Applies To section, as described in Table 4-28.
Edit the syntax for an enabled option	Refer to “Editing Syntax for DNS Options” on page 140.
Remove an option from a DNS product	Uncheck the Enabled checkbox next to the option that you wish to remove from this option set.

- Once finished, click **Save** to save your changes, or **Cancel** to return to the previous screen.

Table 4-28 DNS Options Screen Columns

Field	Description
Enabled	Indicates whether this DNS Option is enabled for this DNS Product.
Name	The name of the DNS Option.
Option Applies To:	
Options	Option can be used when defining an “options” statement within the “named.conf” file.
View	Option can be used when defining a “view” statement within the “named.conf” file.
Zone Master	Option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “master”.
Zone Slave	Option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “slave”.
Zone Stub	Option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “stub”.
Zone Forward	Option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “forward”.
Zone Static Stub	Option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “static-stub”.
Zone Redirect	Option can be used when defining a “zone” statement within the “named.conf” file for a zone type of “redirect”.
HA Pair	Option can be used when defining an “HA Pair” statement within the “named.conf” file.
DNSSec	Option can be used when defining a “DNSSec” statement within the “named.conf” file.
DNS64	Option can be used when defining a “DNS64” statement within the “named.conf” file.
Option Syntax	Shows a sample of the syntax that is used when writing this option to the DNS configuration file. To edit the syntax, click on the option Name link.

Editing Syntax for DNS Options

To edit the syntax for an option, follow these steps.

- Click on the option name in the **Name** column. The Edit DNS Dictionary Option screen opens.
- Use this screen to model the syntax for this DNS option, and click **Submit** to save your changes, or click **Cancel** to return to the list.

DNS Option Master Dictionary

Use the DNS Option Master Dictionary screen to maintain DNS Master Options within the system. Master Options are predefined with all available options that are normally configured with a BIND 8.x or a BIND 9.x server, but may be modified for your environment.

In addition, you can add your own options if they are not already defined within the system.

Managing the DNS Option Master Dictionary

To work with the DNS Option Master Dictionary, follow these steps.

1. Select **Option Master Dictionary** from the DNS section of the **Management** menu. The DNS Option Master Dictionary screen opens.
2. Choose from the following actions.

To ...	Then ...
Search for a specific string	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The Name list changes to match the contents of the search string.
Add a Master DNS Option	<ol style="list-style-type: none"> 1. Select the Add to DNS Master Dictionary link. The Add Master DNS Option screen appears. 2. Enter a name and optional description in the Name and Description fields.
Edit a Master DNS Option	<ol style="list-style-type: none"> 1. Click on the Option name in the Name list. The Edit Master DNS Option screen opens. 2. Edit the name and description as needed.
Delete a Master DNS Option	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Options, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

DNS Software Products

Use the DNS Software Products screen to define DNS products and the attributes that are associated with them.

A set of pre-defined products are included with the system. These products include all the definitions, options, and business logic that are needed to properly manage these network services. Additional products may be added to the system, as long as these newer products

are derived from existing product definitions (that is, they share the same attributes, and so on).

Managing DNS Software Products

To work with a DNS Software Product, follow these steps.

1. Select **DNS Software Products** from the DNS section of the **Management** menu. The DNS Software Products screen opens.
2. Choose from the following actions.

To ...	Then ...
Search for a specific Product string	<ol style="list-style-type: none"> 1. Enter a search string in the text block. 2. Click Search. The Name list changes to match the contents of the search string.
Add a Product	Refer to “Adding a Software Product” following.
Edit a DNS Software Product	<ol style="list-style-type: none"> 1. Click on the Product name in the Name list. The Edit Product screen opens. 2. Edit the values as needed. Refer to Table 4-29 on page 142.
Delete a DNS Software Product	<p>Note: Make sure that this Product is not assigned to any DNS Server (Network Service) before you delete it.</p> <ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Products, or Cancel to return to the previous screen.

3. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Adding a Software Product

To add a software product, follow these steps.

1. Click on the **Add Product** link. The Add Product screen opens.
2. Enter values in the appropriate fields, as described in Table 4-29.

Table 4-29 Create Product Parameters

Field	Description
Name	The DNS Product Name that you want to create. This is a mandatory field.
Description	A description of this product. This is an optional field.
Vendor	Select the Vendor of this product.
Type	<i>Read only.</i> The DNS product type is selected.

Field	Description
Configuration Type	<p>Used to tell the system which type (or syntax) of configuration files should be created during a configuration/deployment task:</p> <p>Supported DNS Types:</p> <p>BIND9 - Indicates that servers that are defined as this product type utilize BIND 9 DNS syntax for their configuration files.</p> <p>BIND8 – Indicates that servers that are defined as this product type utilize BIND 8 DNS syntax for their configuration files.</p> <p>MSFT - Indicates that servers that are defined as this product type utilize Microsoft DNS syntax for their configuration files.</p> <p>CNR – Indicates that servers that are defined as this product type utilize Cisco Network Registrar Command syntax for their configuration files. This applies to CNR DHCP and CNR Caching servers.</p> <p>CNRAUTH - Indicates that servers that are defined as this product type are CNR Authoritative servers.</p>
Collection Type	<p>Used to tell the system which type of collection mechanism should be used to collect information from this service. There are no supported DNS collection types, so the value is set to NONE.</p>

This page intentionally left blank.

Chapter 5 Managing DHCP

In IPAM 8.3, all the features you need to set up DHCP servers are located in the DHCP section of the Management menu. This chapter describes how to use each selection on the DHCP menu.

- Servers/Services
- Utilization View
- Network Links
- Configuration/Deployment
- Policy Sets
- Option Sets
- Client Classes
- Option Vendor Dictionary
- Option Master Dictionary
- DHCP Software Products

Servers/Services

The **Servers/Services** option in the DHCP section of the **Management** menu allows you to define and maintain a layer 3 network DHCP service. Use IPAM to manage and plan the IP address space, policies and options that are allocated to your DHCP network service. Then use IPAM to create the configuration files necessary for DHCP services.

Managing DHCP Servers/Services

To manage DHCP servers and services, follow these steps.

1. Select **Servers/Services** from the DHCP section of the **Management** menu. The list of DHCP Servers/Services opens.
2. Choose from the following actions.

To ...	Then ...
Search for a particular DHCP Network Service	<ol style="list-style-type: none">1. Enter a search string into the text block.2. Click Search. The list of servers changes to match the search string.

To ...	Then ...
Add a DHCP Network Service	Refer to “Product Change Rules for Assigned DHCP Servers” Refer to “Adding a DHCP Server”
Edit a DHCP Network Service	<ol style="list-style-type: none"> 1. Click on the service entry in the Service Name list. The Edit DHCP Server screen opens. 2. Edit fields and tab entries as needed. Refer to the descriptions in the following sections for more information. 3. If the DHCP server is not assigned yet, it is allowed to change the product freely. 4. If a DHCP server is already in use somewhere (i.e. assigned to a subnet) the user will be limited in changing the product. We do allow updating of a product type to the same or a newer version from the same vendor, e.g. <ol style="list-style-type: none"> a. CNR 8.2 to CNR 8.3 b. ISC 4.2 to ISC 4.3 5. The label "(Server is assigned)" under the server name indicates an assigned server. 6. Refer to “Product Change Rules for Assigned DHCP Servers”.
Delete one or more DHCP Network Services	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Network Services, or Cancel to return to the previous screen.

Product Change Rules for Assigned DHCP Servers:

Current Product Collection Type	Available Product Versions or Products
DHCP ISC	
DHCP INS 3x	INS 3x INS 4.1 INS 4.2 INS 4.3
DHCP INS 4.1	INS 4.1 INS 4.2 INS 4.3
DHCP INS 4.2	INS 4.2 INS 4.3
DHCP INS 4.3	INS 4.3
DHCP CNR	

DHCP CNR 8.0	CNR 8.0 CNR 8.1 CNR 8.2 CNR 8.3
DHCP CNR 8.1	CNR 8.1 CNR 8.2 CNR 8.3
DHCP CNR 8.2	CNR 8.2 CNR 8.3
DHCP CNR 8.3	CNR 8.3
DHCP MSFT	
DHCP MSFT 2003	MSFT 2003 MSFT 2008 MSFT 2012
DHCP MSFT 2008	MSFT 2008 MSFT 2012
DHCP MSFT 2012	MSFT 2012
DHCP ADC and QIP	The same product
Any Custom Product	The same product

Adding a DHCP Server

In the Servers/Services screen, select the **Add Network Service** link. The Add DHCP Server screen opens on the **General** tab.

Select a product from the **Product Name** drop-down list. The screen changes to show you available options for the server product type that you selected and displays additional tabs, described in the next sections.

Note: Failover is not currently supported in DHCPv6.

General Tab

This tab applies to all server product types.

Table 5-1 General Tab Parameters

Field	Description
Name	Enter the name of this DHCP Server. Typically, this is the fully qualified domain name of the system where the service is running.
IP Address	Enter either an IPv4 or IPv6 IP Address depending on the DHCP Version type you are creating. This is required if you use IPAM to collect configuration information from this service, or create configuration files for this service.

Product Name	Select the Product Name from the drop-down list of DHCP products available within this system. Use the Management > DHCP Software Products menu option to manage products defined within the system.
DHCP Version	Specify whether the server hosts services for DHCPv4 only, DHCPv6 only, or DHCPv4 and DHCPv6 (CNR 8.0 and 8.1 only).
Agent	Select the Agent that will be used to collect and/or distribute information to/from this service.
Default Scope Utilization Warning Threshold	The default threshold (in percent) that is used to provide warnings when usage of a pool assigned to this service is exceeded.
Include during Global Synchronization Task	Select this checkbox if you want to include this service in the global synchronization task. If this service is included in the global synchronization task, the service's configuration and utilization information will be collected when the task runs.
Configuration File Path:	Enter the fully qualified pathname of the configuration file. The typical entries are listed below: <ul style="list-style-type: none"> • INS/ISC DHCPv4: /opt/incontrol/dhcpd/dhcpd.conf • INS/ISC DHCPv6: /opt/incontrol/dhcpd/dhcpd6.conf • Lucent QIP: /opt/qip/dhcp/dhcpd.conf • Fastflow: /etc/dhcpd.conf
Lease File Path:	Enter the fully qualified pathname of the lease file for this DHCP server. The typical entries are listed below: <ul style="list-style-type: none"> • INS/ISC DHCPv4: /opt/incontrol/dhcpd/dhcpd.leases • INS/ISC DHCPv6: /opt/incontrol/dhcpd/dhcpd6.leases • Lucent QIP: /opt/qip/dhcp/dhcpd.leases • Fastflow: /etc/dhcpd.leases
Start Script	The script called by IPAM to start a DHCP server. INS/ISC DHCP: /opt/incontrol/etc/dhcpd_start
End Script	The script called by Cisco Prime Network Registrar IPAM to stop a DHCP server. INS/ISC DHCP: /opt/incontrol/etc/dhcpd_stop

Collection Tab

Click on the **Collections** tab to display the collection information. This area allows you to select a collection type, enter login information, and set the port used for collection. Note that this tab only appears when you are configuring ADC, INS, ISC and QIP servers.

Table 5-2 Collection Tab Parameters

Field	Description
Collection Type	Select the method that will be used to collect information about this service. Select “File Transfer Protocol – FTP” to use the FTP protocol. Select “Secure Copy – SCP” to use the SCP protocol. If you select SCP, you must manually configure SSH on the system that is running the service. Note that SCP is not supported by default on Windows systems.
Username	Enter the user id that will be used for the protocol that you selected (FTP or SCP). The Agent uses this credential when communicating with the server on which the Net Service is running.
Password	Enter the password that will be used for the protocol that you selected (FTP or SCP). The Agent uses his credential when communicating with the server on which the Net Service is running.
Confirm Password	Confirm the password that will be used for the protocol that you selected (FTP or SCP).
Port	Enter the port that will be used to connect to the service (FTP or SCP). The default port for FTP is 21; the default port for SCP is 22. The defaults may be overridden if different ports are used within your network for security purposes.

Management Tab

Click on the **Management** tab to enter Cisco Network Registrar server configuration options. Note that this tab only appears when you are configuring CNR servers.

Table 5-3 Management Tab Parameters

Field	Description
Collect via CNR SDK	When checked, indicates that the IPAM Agent uses the Cisco Network Registrar SDK (available separately from Cisco) to retrieve configuration and lease information from the CNR DHCP server.
CNR Userid	Enter the user ID required to allow execution of the <code>nrcmd</code> and/or <code>cnr_exim</code> utilities for this cluster.
CNR Password	Enter the password required to allow execution of the <code>nrcmd</code> and/or <code>cnr_exim</code> utilities for this cluster.
Confirm CNR Password	Confirm the CNR password.
Port	Enter the CNR DHCP server port number.
Perform Summary Collections	When checked, indicates that the IPAM Agent does not get individual leases from the CNR DHCP server, but instead retrieves only the utilization summary from the server. CNR DHCP maintains the utilization summary information at the subnet or prefix level only. Therefore, address pool utilization numbers are not available using this option.

Field	Description
Include Interface and Block Type in Collection Task Differences	<p>For use by cable operators. The CNR DHCP server's 'selection-tag' scope attribute can be mapped to specific block types defined in IPAM. In addition, this option enforces that the CNR DHCP scopes match the configuration of the child blocks attached to the network element (usually a CMTS) interface.</p> <p>Note: Only use this selection under the guidance of Cisco support support staff.</p>
Path to the CNR Binary Executable Directory.	<p>Visible when "Collect via CNR SDK" is unchecked.</p> <p>Enter the full path of where the CNR nrcmd and cnr_exim executables are located. Example: /opt/nwreg2/local</p>
CNR Cluster Name	<p>Visible when "Collect via CNR SDK" is unchecked.</p> <p>Enter the CNR cluster name for this server.</p>
Collect Failover Backup Subnets	<p>Visible when "Collect via CNR SDK" is unchecked.</p> <p>Unchecked indicates that the collection will ignore any subnets that this DHCP server is failover for. Typically, if you are collecting DHCP information from all your DHCP servers, collection of data for those subnets would be accomplished when you are performing collection against the primary DHCP server.</p> <p>Checked indicates that you will collect data for any subnets that this server is failover for.</p> <p>Typically you would leave this unchecked, so that you do not collect duplicate information from both the primary and failover DHCP servers.</p>

Configuration Tab

Click on the **Configuration** tab to display the configuration options. This area allows you to select different DHCP Server configuration options. Note that this tab only appears when you are configuring CNR, INS, ISC and Microsoft servers.

Table 5-4 Configuration Tab Parameters

Field	Description																		
Perform Dynamic DNS Updates	<p>Select a dynamic DNS update. The default Dynamic DNS update is “none” or “off”. Other selections indicate that the system will send RFC2136 dynamic DNS updates to the primary DNS server when a lease is given out.</p> <table border="1"> <thead> <tr> <th>Product Family</th> <th>Default Dynamic DNS Update</th> <th>Dynamic DNS Update Selections</th> </tr> </thead> <tbody> <tr> <td>CNR</td> <td>off</td> <td>off on</td> </tr> <tr> <td>INS DHCP 4.3</td> <td>none</td> <td>none interim standard lastin</td> </tr> <tr> <td>INS DHCP 4.2</td> <td>none</td> <td>none interim lastin</td> </tr> <tr> <td>INS DHCP (excluding 4.2 and 4.3)</td> <td>none</td> <td>none interim</td> </tr> <tr> <td>Microsoft</td> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Product Family	Default Dynamic DNS Update	Dynamic DNS Update Selections	CNR	off	off on	INS DHCP 4.3	none	none interim standard lastin	INS DHCP 4.2	none	none interim lastin	INS DHCP (excluding 4.2 and 4.3)	none	none interim	Microsoft	N/A	N/A
Product Family	Default Dynamic DNS Update	Dynamic DNS Update Selections																	
CNR	off	off on																	
INS DHCP 4.3	none	none interim standard lastin																	
INS DHCP 4.2	none	none interim lastin																	
INS DHCP (excluding 4.2 and 4.3)	none	none interim																	
Microsoft	N/A	N/A																	
DHCP Policy Set	Select a default Policy Set for this server. Policies assigned at the server level are used system wide. It can contain items such as default lease times, and so on.																		
DHCP V4 Option Set	Select the default DHCPv4 option set for this server. This field appears if the server supports the DHCPv4 protocol. Options assigned at the server level are used system wide.																		
DHCP V6 Option Set	Select the default DHCPv6 option set for this server. This field appears if the server supports the DHCPv6 protocol. Options assigned at the server level are used system wide.																		
DHCP Client Classes	<p>Select the superset of DHCP Client classes that are available for use by this DHCP server. The selection of the DHCP Client classes is DHCPv4/ DHCPv6 specific.</p> <p>Note: DHCPv6 servers: the feature is available for CNR and DHCP 4.3 servers only.</p> <p>Note: When an administrator wants to assign Allow/Deny access to an IP Address or Prefix Pool managed by this server by client class, those client classes must be associated with the server here first!</p>																		

Failover Peer Tab – CNR, INS, and ISC DHCPv4

Click on the **Failover** tab to display the failover information. This area allows you to identify the server’s failover server. Note that this tab only appears when you are configuring CNR, INS and ISC DHCPv4 servers. Failover is not currently supported in DHCPv6.

Table 5-5 Failover Peer Tab Parameters

Field	Description
Failover IP Address	Enter the IP Address of this server that will be used for failover communications to other DHCP servers.
Failover Port	Enter the port number that will be used for failover communications. Typically, this is 847 for primary servers or 647 for failover servers.
My Failover Peers	<p>Peer Server – Select the failover peer server(s) that will be used to implement DHCP failover for this server. Refer to “Configuring DHCP Failover” on page 294 for more information regarding DHCP Failover. Select Add Failover Peer, and enter the following:</p> <p>Contact Timeout – Determines how long a server will wait without receiving any messages from its partner before it assumes that the connection to its partner has failed.</p> <p>Max Pending Updates – The maximum number of pending updates that the server can accept without blocking the input.</p> <p>Max Client Lead Time (MCLT) – The amount of time by which either server can extend a lease without contacting the other server.</p> <p>Max Lease Misbalance – The percentage threshold beyond which a server will commence to achieve balance with its failover peers.</p> <p>Max Lease Ownership – The percentage threshold beyond which a server will no longer need to transfer leases to its failover peers to achieve balance.</p> <p>Max Balance – Specifies the maximum number of seconds before the server initiates load balance analysis.</p> <p>Min Balance – Specifies the minimum number of seconds before the server initiates load balance analysis.</p> <p>Load Balance Split – Tells the primary server what portion of all clients it should serve in a load balancing scenario.</p> <p>A value of “255” indicates that the primary server serves all clients and the failover server serves no clients (this is the typical primary and failover behavior without load balancing).</p> <p>A value of “128” indicates that approximately 50% of the clients will be served by the primary server, and 50% of the clients will be served by the failover server.</p> <p>Load Balance Override – Determines when the primary or failover server will bypass load balancing and respond to the client even if the client is supposed to be served by the other server. Every message from a DHCP client includes a field that indicates for how many seconds the DHCP client has been trying to contact the DHCP server. If the value of that field is higher than the configured “Load Balance Override” seconds, the DHCP server always attempts to respond to the client, regardless of the “Load Balance Split”.</p>

Field	Description
My Primary Peers	<p>Peer Server – Select the primary peer server(s) that will be used to implement DHCP failover for this server. Refer to “Configuring DHCP Failover” on page 294 for more information regarding DHCP Failover. Select Add Primary Peer, and enter the following:</p> <p>Auto Partner Down Delay - Specifies the delay time in seconds that a server should wait before entering the partner-down state after detecting a communications interruption with its failover peer. In general, this feature should only be used in deployments where the failover servers are directly connected to one another, such as by a dedicated hardwired link ("a heartbeat cable").</p> <p>Contact Timeout – Determines how long a server will wait without receiving any messages from its partner before it assumes that the connection to its partner has failed.</p> <p>Max Pending Updates – The maximum number of pending updates that the server can accept without blocking the input.</p> <p>Max Client Lead Time (MCLT) – The amount of time by which either server can extend a lease without contacting the other server.</p> <p>Max Lease Misbalance – The percentage threshold beyond which a server will commence to achieve balance with its peers.</p> <p>Max Lease Ownership – The percentage threshold beyond which a server will no longer need to transfer leases to its peers to achieve balance.</p> <p>Max Balance – Specifies the maximum number of seconds before the server initiates load balance analysis.</p> <p>Min Balance – Specifies the minimum number of seconds before the server initiates load balance analysis.</p> <p>Load Balance Split – Tells the primary server what portion of all clients it should serve in a load balancing scenario.</p> <p>A value of “255” indicates that the primary server serves all clients and the failover server serves no clients (this is typical primary and failover behavior without load balancing).</p> <p>A value of “128” indicates that approximately 50% of the clients will be served by the primary server, and 50% of the clients will be served by the failover server.</p> <p>Load Balance Override – Determines when the primary or failover server will bypass load balancing and respond to the client even if the client is supposed to be served by the other server. Every message from a DHCP client includes a field that indicates for how many seconds the DHCP client has been trying to contact the DHCP server. If the value of that field is higher than the configured “Load Balance Override” seconds, the DHCP server always attempts to respond to the client, regardless of the “Load Balance Split”.</p>

Failover Peer Tab – Microsoft Windows 2012 DHCP

Click on the **Failover** tab to display the failover information. This area allows you to identify the server’s failover server.

Table 5-6 Failover Peer Tab Parameters – Microsoft Windows 2012 DHCP

Field	Description
My Failover Peers	<p>Peer Server – Select the failover peer server(s) that will be used to implement DHCP failover for this server. Select Add Primary Peer, and enter the following:</p> <p>State Switch Interval in seconds – Specifies the time interval for which the DHCP server service operates in the COMMUNICATION INTERRUPTED state before transitioning to the PARTNER DOWN state.</p> <p>Max Client Lead Time (MCLT) in seconds – Specifies the maximum client lead time for the failover relationship.</p> <p>Reserve Percent – Specifies the percentage of free IPv4 addresses in the IPv4 address pool of the scope which should be reserved on the standby DHCP server service. In the case of a failover, the IPv4 address from this reserved pool on the standby DHCP server service will be leased to new DHCP clients.</p> <p>Failover Mode – Two DHCP failover modes are available to use when you create a DHCP failover relationship:</p> <p style="padding-left: 40px;">Hot standby mode: This mode provides redundancy for DHCP services.</p> <p style="padding-left: 40px;">Load balance mode: This mode allocates DHCP client leases across two servers.</p>
My Primary Peers	<p>Peer Server – Select the failover peer server(s) that will be used to implement DHCP failover for this server. Select Add Primary Peer, and enter the following:</p> <p>State Switch Interval in seconds – Specifies the time interval for which the DHCP server service operates in the COMMUNICATION INTERRUPTED state before transitioning to the PARTNER DOWN state.</p> <p>Max Client Lead Time (MCLT) in seconds – Specifies the maximum client lead time for the failover relationship.</p> <p>Reserve Percent – Specifies the percentage of free IPv4 addresses in the IPv4 address pool of the scope which should be reserved on the standby DHCP server service. In the case of a failover, the IPv4 address from this reserved pool on the standby DHCP server service will be leased to new DHCP clients.</p> <p>Failover Mode – Two DHCP failover modes are available to use when you create a DHCP failover relationship:</p> <p style="padding-left: 40px;">Hot standby mode: This mode provides redundancy for DHCP services.</p> <p style="padding-left: 40px;">Load balance mode: This mode allocates DHCP client leases across two servers.</p>

Extensions Tab

Click on the **Extensions** tab to display the configuration file extensions area. This area allows you to create free form text to add to the beginning or the end of the `dhcpd[6].conf` configuration file. Note this tab only appears when you are configuring INS, ISC and Microsoft servers.

Table 5-7 Extensions Tab Parameters

Field	Description
Insert at beginning of configuration file	Enter any free text options that you want to appear at the beginning of the configuration file. Note: The extensions are limited to 32000 characters.
Append to end of configuration file	Enter any free text options that you want to appear at the end of the configuration file. Note: The extensions are limited to 32000 characters.

Click **Submit** to save your changes. If the DHCP server was successfully added, the new DHCP server appears in the DHCP Servers/Services list.

DHCP Utilization View

The DHCP Utilization View feature provides a summary of the IP infrastructure managed by a DHCP server (Network Service). Separate views of Block and Address Pool information are supported. You can also review a chart showing the allocation history of available vs. used space for a selected DHCP server.

To review network usage details for a DHCP server, select **Utilization View** from the DHCP section of the **Management** menu. The DHCP TOPO Network Services List screen is displayed.

Table 5-8 DHCP TOPO Network Services List Parameters

Field	Description
Server Name	Displays the DHCP server name.
IP Address	Displays the server address.
TOPO Details	Enables you to review the network usage details. Click the TOPO Details icon associated with the Service Name you want to review, or search for a specific Service Name as follows: <ol style="list-style-type: none"> 1. Type a search string in the text block. 2. Click Search. 3. Click the TOPO Details icon of the server you want to review from the search results. The Utilization Display appears.

Utilization Display

The columns in the Utilization Display are described in Table 5-9.

Table 5-9 Network Service Utilization Display Elements

Field	Description
Address Pool	The starting and ending address of the address pool, or the “shared network” name of a group of address pools.
Pool Type	The block type of the pool.
Usable Hosts	The number of usable hosts that are contained within the current block
Utilization	A graph of the current utilization of the block.
Percent Used	The percentage of this block that is currently utilized.
History	Select this link to display a history graph of the utilization for the current address pool.
 and 	Displayed when IPV6 address pools are listed. Used to change the display format of IPV6 hosts. See “Displaying IPV6 Capacities” on page 15 for more information.

To return to the DHCP TOPO Network Services List, click **Cancel**. To review a chart showing the allocation of available vs. used space across an entire DHCP server, click the **History** link beside the pool you want to review. The Address Pool History chart appears. To exit, scroll down and click **Cancel**.

Address Pool Details

To display detailed information about the address pools associated with a DHCP server, click **Address Pool Details**. The Address Pool Details screen opens.

The columns in the Address Pool Details screen are described in Table 5-10.

Table 5-10 Address Pool Details Display Elements

Field	Description
Network Link Name	The name of the network link.
Address Pool	The starting and ending address of the address pool, or the shared network name of a group of address pools.
Pool Type	The block type of the pool.
Usable Hosts	The number of usable hosts that are contained within the current block. This is inclusive of the “locked” hosts.
Assigned Hosts	The number of assigned hosts that are contained within the current block.
Locked Hosts	The number of locked hosts that are contained within the current block. Locked hosts are typically hosts that a DHCP server will mark as in use, although the DHCP server has not assigned or leased the IP Address. This can occur if a DHCP server detects a static IP Address assignment, before the IP address is leased by the DHCP server.
Percent Used	The percentage of this block that is currently utilized.
Last Updated	The date the address pool was last updated with data from a collection task.

Block Details

To display detailed information about the blocks associated with a DHCP server, click **Block Details**. The Block Details screen opens.

The columns in the Block Details screen are described in Table 5-6.

Table 5-6 Block Details Display Elements

Field	Description
Block	The name of the block
Block Type	The block type of the block.
Leasable Hosts	The number of dynamic addresses available to DHCP for allocation.
Dynamic Hosts	The number of dynamic hosts within the subnet or block. This is inclusive of the “locked” hosts.
Locked Hosts	The number of locked addresses in this block.
Utilization	The percentage of this block that is currently utilized.
Lease %	The percentage of dynamic addresses leased to clients.
History	Click on this link to view a history graph of the utilization information for this block.

To return to the Network Service List, click **Cancel**. To review a chart showing the allocation of available vs. used space across an entire DHCP server, click the **History** link beside the block you want to review. The Block History chart appears.

Network Links

The Network Links option allows you to define network segments. A network segment generally corresponds to a subnet. However, it is possible to have multiple subnets on a single network segment. This is referred to as “shared subnets” or “shared networking”. You can define a logical network link to be shared amongst subnets in a logical container, whereas a physical network link is automatically created when more than one subnet is attached to the same interface of a device container.

Managing Network Links

To manage your Network Links, select **Network Links** from the DHCP section of the **Management** menu. The Network Links screen is displayed.

The Network Links screen allows you to maintain DHCP network links in the IPAM system.

Note: Since physical network links are automatically managed by IPAM, they cannot be added or deleted from the Network Links screen.

Choose from the following actions.

To ...	Then ...
Search for a particular DHCP Network Link	<ol style="list-style-type: none"> 1. Enter a search string into the text block. 2. Click Search. The list of Network Links changes to match the search string.
Add a DHCP Network Link	Refer to “Adding a Network Link”.
Edit a DHCP Network Link	Refer to “Editing a Network Link”.
View a subnet	Click on a Subnet name in the Subnets (Block Type) list. The Subnet screen is displayed.
View DHCP Option Set	Click on a DHCP Option name in the DHCP Option Set(s) List. The View Option Set screen is displayed.
View DHCP Policy Set	Click on a DHCP Policy name in the DHCP Option Set(s) List. The View Policy Set screen is displayed.
Delete one or more Network Links	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Network Links, or Cancel to return to the previous screen.

Adding a Network Link

To add a network link, follow these steps.

1. Click **Add Network Link**.

The Add Logical Network Link screen opens.

2. Enter a unique name for the network link in the **Name** field..
3. Enter up to *n* alphanumeric characters to describe the network link in the **Description** field, (up to 60 characters fit comfortably).

4. Click **Add Dhcp Policy Set** to choose a previously created DHCP Policy Set. Use the Search function to restrict the list to a subset that meets your search criteria.
5. Click **Add Dhcp Option Set** to choose a previously created DHCP Option Set. Use the Search function to restrict the list to a subset that meets your search criteria.
6. Click **Submit**.

Editing a Network Link

To modify an existing network link, follow these steps:

1. Click on the network link name in the Network Link list. The Edit Network Link screen opens.
2. Edit field entries as needed. Refer to the descriptions in the previous section for more information.
3. Click **Submit**.

Configuration/Deployment

The Configuration/Deployment option allows you to create on-demand, scheduled, or recurring scheduled tasks for deployment of configuration information to your DHCP network services.

Configuration/Deployment Task Definition Options

To deploy configuration information to a network service, select the **Task Type**, **Network Service** and **When to run task** on this screen. Depending upon the selection of when you will be running the task, different options will be displayed on the screen for you to select. Refer to the sections below for additional information about each option. Note that once you click **Submit**, a new task will be created, and submitted to the system. Once tasks have been created, they can be managed using the **Task** menu option.

Select **DHCP Configuration – All Files** from the **Task Type** drop-down. The screen expands to display additional fields, described in Table 5-7.

Table 5-7 Configuration/Deployment Screen Elements

Field	Description
Network Service	Select Search and select a network service, previously configured on the DHCP Servers/Services screen, to perform this task against.

Field	Description
Stop on Errors and Warnings	<p>Checked indicates that the system will not complete the selected task if any errors or warnings are encountered during its execution. Best practice suggests you enable this option whenever you are performing a distribution task to avoid pushing an invalid configuration to a network service.</p> <p>Unchecked allows the task to proceed regardless of issues. This allows you the opportunity to ignore errors or warnings deemed to be benign.</p>
Update Failover Servers	<p>Checked indicates that when you distribute configuration information to a DHCP server, if that server has failover servers, then the system should also automatically push an appropriate configuration file to those servers as well.</p> <p>Unchecked indicates that only the selected DHCP server will be sent its configuration files.</p>
Push only if configuration changed	<p>If checked, indicates that the push task should only occur if there are changes to the configuration.</p>
Delete task if no changes	<p>If checked, indicates that the task should be automatically deleted if no changes to the configuration are detected. This feature is enabled by and only works in conjunction with the “Push only if configuration changed” checkbox.</p>
Hold files for preview	<p>If checked, the configuration files will be created, but not deployed. You can view the files from the Task List.</p>
When to run task	<ul style="list-style-type: none"> • Immediate – run the task immediately • Scheduled – run the task on the predetermined date and time specified • Recurring – Run this task multiple times

Immediate Config/Deployment Task

Select **Immediate** from the **When to run task** options to run a task on demand. Clicking **Submit** will immediately build the required configuration file and move the task to the head of the task execution queue. Once tasks have been created, they can be managed using the **Task** menu option.

Scheduled Config/Deployment Task

Select **Scheduled** from the **When to run task** options to schedule a task to run in the future. Schedule options are displayed.

To select a future date to run the task, type in the desired date in MM/DD/YYYY format or click the calendar icon to select a date. A calendar is displayed, with today’s date selected by default.

You can use the following navigation links to change to another month and/or year and then select a date in the month to close the utility:



Previous Year

 Previous Month

 Next Year

 Next Month

Select the hours, minutes, and AM or PM to schedule a specific time for the task.

Once all parameters have been entered, click **Submit**. A new task is created, and submitted to the system. Once tasks have been created, they can be managed using the **Tasks** menu option on the **Reports** menu.

Recurring Config/Deployment Task

Select **Recurring** from the **When to run task** options to schedule a task to run at regular intervals. Schedule options are displayed.

To set up a recurring task, follow these steps:

1. Select the date and time that you want the recurring task to begin.
2. Click on the calendar icon to display a calendar. Refer to “Scheduled Config/Deployment Task” on page 114 for information on using the calendar utility.
3. Select the frequency for the recurring task.
 - ▶ Sub-Daily
 - ▶ Daily
 - ▶ Weekly
 - ▶ Monthly
 - ▶ Yearly
4. Click **Submit**.

A new task is created and submitted to the system.

After tasks have been created, you can manage them using the **Task** menu option.

Policy Sets

Use the DHCP Policy Sets screen to maintain DHCP Policy Sets. DHCP Policy Sets are groups of DHCP vendor-specific policies that you implement to affect the behavior of the DHCP server.

By using DHCP Policy Sets, you can simplify the configuration steps that are needed. DHCP Policy Sets allow you to group logical sets of policies together for specific purposes, and then allow you to apply the Policy Sets at different areas within your DHCP infrastructure.

To work with DHCP Policy Sets, select **Policy Sets** from the DHCP section of the **Management** menu. The DHCP Policy Sets screen opens.

Choose from the following actions:

To ...	Then ...
Copy one or more DHCP Policy Sets	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you wish to copy. 2. Click .
Add a DHCP Policy Set	Refer to “Adding a DHCP Policy Set” on page 163.
Edit a DHCP Policy Set	<ol style="list-style-type: none"> 1. Click on the policy set entry in the Name list. The Edit DHCP Policy Set screen opens. 2. Edit fields and tab entries as needed. Refer to Table 5-8 for more information.
Delete one or more DHCP Policy Sets	<ol style="list-style-type: none"> 1. Select the checkbox beside each item you want to delete. 2. Click . 3. At the confirmation prompt, click OK to delete the selected Policy Sets, or Cancel to return to the DHCP Policy Sets screen. <p>Note: You cannot delete a Policy Set that is assigned to a DHCP Server (Network Service), Subnet, Network Link, IP Address/Pool, or Client Class without deleting these associations first.</p>

Adding a DHCP Policy Set

To add a DHCP Policy Set, click the **Add DHCP Policy Set** link. The Add DHCP Policy Set screen appears as follows:

Fill in the appropriate fields, as described in Table 5-8.

Table 5-8 Add DHCP Policy Set Parameters

Field	Description
Name	Mandatory. The DHCP Policy Set Name that you want to assign to this policy set (for example, 'Server Policy', 'VoIP Scope Policy'). This is a mandatory field.
Description	Optional. Enter a description of the DHCP Policy Set.
Product	Select the DHCP Vendor Product that the DHCP Policy Set represents.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the DHCP Policy Sets screen.

Working with DHCP Policy Set Policies

To review, edit, add or remove policies for an existing Policy Set, select the **Policies** link associated with a policy set name on the DHCP Policy Sets. The DHCP Policies for Policy Set screen opens.

Table 5-9 DHCP Policies for Policy Set Parameters

Field	Description
Show all policies	When checked, the superset of all available policies associated with the selected server product family is displayed. Otherwise, only the policies currently assigned to this policy set are shown.
Select	When checked, the policy is associated/enabled with this DHCP policy set. Unchecking a policy will remove it from the set.
Name	The name of the policy, displayed as a link to a DHCP Policy screen.
Value(s)	The values that have been assigned to this policy. If the text “— Same as Subnet—” appears in this field, the actual value is inherited from the Subnet’s value at the time that the configuration file is created.
Applies To	Indicates where the policy can be used within the “dhcpd[6].conf” file structure. The locations displayed here will vary by server product family. For example ISC servers support; Server, Subnet, Client Class, Link, Pool and Host. CNR servers support; Server, Subnet, Client Class, Prefix and Link. Pushing a configuration file with policies configured at an inappropriate level can cause the DHCP push to fail.

Choose from the following actions:

To ...	Then ...
Add new policies to a selected policy set	<ol style="list-style-type: none"> 1. Select the Show all policies check box. All the policies that are defined within the system for that server family are displayed. 2. Click on the name of the policy to assign a value. The DHCP Policy screen appears. 3. Type in the requisite values. Possible data types are described in Table 5-10. 4. Click Submit. The Select checkbox is checked and values are shown in the Value(s) column.
Edit the value of a policy	<ol style="list-style-type: none"> 1. Click on the policy set entry in the Name list. The DHCP Policy screen opens. 2. Edit values as needed. 3. Click Submit. The new values are shown in the Value(s) column.
Remove policies from a policy set	<ol style="list-style-type: none"> 1. Uncheck the checkbox next to the policy that you want to remove. 2. Click Submit.

Table 5-10 DHCP Policies Data Types

Data Type	Description
blob	Indicates this policy will accept a binary large object value (for example, Server DUID).
boolean	Indicates this policy requires a true or false value.
date	Indicates this policy requires a date formatted '[weekday] mon day hh:mm[:ss] year' value. For example, 'Dec 31 23:59 2006'.
expr	Indicates this policy will accept an expression as a means to set its value (for example, Client Class Lookup ID).
int100	Indicates this policy requires a decimal formatted per cent value (for example, Event Roll Store Percentage).
ip6addr	Indicates this policy requires a IPv6 formatted address value.
ipaddress	Indicates this policy requires a IPv4 formatted address value.
mstime	Indicates this policy requires an integer representing a milliseconds value.
numeric	Indicates this policy requires an integer representing a raw number or count.
optionid4	Indicates this policy requires an integer representing a IPv4 DHCP Option Code.
optionid6	Indicates this policy requires an integer representing a IPv6 DHCP Option Code.
percent	Indicates this policy requires an integer representing a per cent value.

prefix	Indicates this policy requires an integer representing a IPv6 network prefix.
quoted-string	Indicates this policy requires a quoted string value.
selectlist	Indicates this policy can only be assigned a value from the accompanying drop-down list.
string	Indicates this policy requires a non-quoted string value.
time	Indicates this policy requires a time formatted value such as 24h or 60m.

Viewing Policy Assignments

Select the **Assignments** link associated with a policy set name on the DHCP Policy Sets screen in order to view where in IP Control the policy set is in use. The DHCP Policies Set Assignments List screen opens, as shown below:

The DHCP Policy Set Assignments view provides a list of objects in your system using a specific DHCP policy set. DHCP policy sets can be assigned to the following objects in IP Control: DHCP servers, subnets, address pools, devices, network links, and client classes. The following table explains the details listed for each object:

Table 5-11 DHCP Policy Set Assignment Display Fields

Field	Description
Object	Client Class, Device, Network Link, Pool, Server, or Subnet
Name	The name of the object, with the following exceptions: For a device, this is the hostname. For a subnet, this is the start address in CIDR notation.
Type	The object type. This varies by object type, and is not displayed for client classes and subnets.
IP Address	The IP address of a device.
Block Name	The name of the block containing the listed device, address pool or subnet.
Container	The block's container for devices, address pools, and subnets.

Option Sets

Use the DHCP Option Sets screen to maintain DHCP Option Sets. DHCP Option Sets are groups of DHCPv4 and DHCPv6 options that you implement to affect the behavior of the DHCP server. These include DHCP RFC options that are used to send to a DHCP or Bootp client (or host).

DHCP can provide other configuration parameters in addition to an IP Address to a client. In fact, several additional parameters must be provided to a client before that host can communicate with other hosts. At a minimum, a host must be provided:

- Its local subnet mask

- The IP address of at least one router on its subnet
- The IP address of a Domain Name Server (DNS)

There are two types of option sets that can be configured for the DHCP server:

- “Server-specific” options that effect the configuration of the DHCP server itself.
- “Scope-specific” options that effect individual IP Address or IP Address pools

Using IPAM, you can simplify the configuration steps that are needed, by using DHCP Option Sets. DHCP Option Sets allow you to group logical sets of options together for specific purposes, and then apply the Option Sets at different areas within your DHCP infrastructure.

Adding a DHCP Option Set

To add a DHCP Option Set, click the **Add DHCP Option Set** link. The Add DHCP Option Set screen appears.

Table 5-12 Add DHCP Option Set Parameters

Field	Description
Name	The DHCP Option Set Name that you want to assign to this option set (for example, ‘Windows Clients’, ‘VoIP Devices’). This is a mandatory field.
Description	An optional description of this option set.
Type	Specify which option set version you want: DHCPv4 or DHCPv6.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Deleting a DHCP Option Set

To delete one or more DHCP Option Sets, select the checkbox beside each item you wish to delete, and click . You are prompted for confirmation.

Note: You cannot delete an Option Set that is assigned to a DHCP Server (Network Service), Subnet, Network Link, IP Address/Pool, or Client Class without deleting these associations first.

Click **OK** to delete the selected DHCP Option Sets, or **Cancel** to return to the previous screen.

Copying a DHCP Option Set

To copy one or more DHCP Option Sets, select the checkbox beside each item you wish to copy, and click .

DHCP Option Set Options

To review, edit, add or remove options for an existing Option Set, select the **Options** link associated with an option set name on the DHCP Option Sets screen. The DHCP Options for Option Set screen opens.

Table 5-13 DHCP Options for Option Set Parameters

Field	Description
Show all options	When checked, the superset of all available options associated with the selected DHCP server version is displayed. Otherwise only the options currently assigned to this option set are shown.
Enabled	When checked, this option is associated with this DHCP option set.
Code	The option code as defined by the RFC. Refer to RFC 2132 .
Name	The name of the option.
Value(s)	The values that have been assigned to this option. If -Same as Subnet- appears in this field, the actual value is inherited from the Subnet's value as the configuration file is created.

Once finished, click **Submit** to save all changes on this Options screen, or **Cancel** to discard all changes and return to the previous screen.

Viewing All Options Assigned to This Option Set

When you first enter this screen, any options that are already assigned to this set have their **Enabled** checkbox selected. To add new options to the set, click on the **Show all options** checkbox at the top of the screen. This displays all the options defined within the system for the given DHCP version.

From here you can click on an option's **Enabled** checkbox or on its **Name** link to open a value assignment window. For example, clicking on the DHCPv6 "Preference" option link will pull up the DHCP Option screen.

Table 5-14 DHCP Option Parameters

Field	Description
Option name	The DHCP Option name assigned to this option.
Code	The option code as defined by the RFC. Refer to RFC 2132 .
Description	A description of this option.
Data Type	The data type that is required for this option, as described in Table 5-10.
Minimum Value	Numeric data types only – the minimum value that is allowed.
Maximum Value	Numeric data types only – the maximum value that is allowed.
Same as Subnet Policy	On some specific options where it is appropriate, the value of the option can be set with the expression "Same as Subnet". This will cause the value to be resolved during the configuration file creation. For more information, refer to "Same as Subnet options" below.

Field	Description
Multiple Values Allowed	Specifies if multiple values are allowed for this option. True indicates that multiple values are allowed. False indicates that multiple values are not allowed. If multiple values are allowed, then the button “Append Value” will appear. Click on this button to append values to this option. For multi-valued options, you can reorder the option using the Up or Down buttons, and delete individual options by clicking Delete .
Value(s)	Enter the value for this option.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Same as Subnet Options

DHCPv4 Option Sets can include five common options that can support a special value of “Same as Subnet”. The “Same as Subnet” value indicates that the actual value will be determined from the Policies tab of a subnet defined in IPAM. A subnet is a block with a status of “In-Use/Deployed”.

Note: Options configured this way are supported only if the Option Set is attached to the subnet or the address pool. Server and Link level option sets cannot use this special value.

The five policies that support “Same as Subnet” include the following:

1. Subnet Mask (DHCPv4 option code 1) – derived from the block size of the subnet.
2. Routers (DHCPv4 option code 3) – the value of the Default Gateway field of the subnet Policies tab.
3. Domain Name Servers (DHCPv4 option code 6) – the list of DNS servers attached to the subnet Policies tab.
4. Domain Name (DHCPv4 option code 15) – the list of Forward Domains attached to the subnet Policies tab.
5. NetBIOS over TCP/IP Name Servers (DHCPv4 option code 44) – the Primary WINS Server field of the subnet Policies tab.

Editing Values of Options Assigned to an Option Set

To edit the value of an option assigned to this option set, click on its **Name** link in the option list. For example, clicking on the DHCPv4 “Routers” option link will pull up the DHCP Option screen.

Edit the value of the option and click **Submit** to save your changes, or click **Cancel** to return to the list.

Removing Options from an Option Set

To remove options from an option set, uncheck the **Enabled** checkbox next to the options that you wish to remove and click **Submit**, or **Cancel** to discard your changes and return to the previous screen.

Viewing Option Set Assignments

Select the **Assignments** link associated with an option set name on the DHCP Option Sets screen in order to view where in IP Control the option set is in use. The DHCP Options Set Assignments List screen opens.

The DHCP Option Set Assignments view provides a list of objects in your system using a specific DHCP option set. DHCP option sets can be assigned to the following objects in IP Control: DHCP servers, subnets, address pools, devices, network links, and client classes. The following table explains the details listed for each object:

Table 5-15 DHCP Option Set Assignment Display Fields

Field	Description
Object	Client Class, Device, Network Link, Pool, Server, or Subnet
Name	The name of the object, with the following exceptions: For a device, this is the hostname. For a subnet, this is the start address in CIDR notation.
Type	The object type. This varies by object type, and is not displayed for client classes and subnets.
IP Address	The IP address of a device.
Block Name	The name of the block containing the listed device, address pool or subnet.
Container	The block's container for devices, address pools, and subnets.

Client Classes

The DHCP Client Classes screen allows you to maintain criteria that are used to group clients together for applying specific conditional behavior to the device, such as sending specific options to the device.

For example, sometimes it is useful to be able to provide an IP Address for a client from a specific address pool (or range) based on the type of client (or device). Or, you may need to provide extra DHCP options to a device because it is a specific type of device, such as sending special options to a VoIP phone. Or, you may need to supply a short lease time only to a specific group of MAC addresses, because you are moving these devices to another area within the network.

IPAM supports this capability in a powerful way, by allowing groups of devices to be specified either by MAC Address, Client Identifier, Hostname, User Class Identifier, Vendor Class Identifier, or by a custom expression.

Using DHCP Client Classes you can accomplish the following types of tasks:

- You can use this feature to create groups of included or excluded devices based on MAC Address, Client Identifier, Hostname, User Class Identifier, or Vendor Class Identifier.
- You can use this feature to provide specific options to groups of devices.
- You can use this feature to change lease times for specific groups of devices.
- You can use this feature to specify a logical expression that can be used to evaluate the attributes of a specific client, and then apply specific policies or options to that client.
- You can use this feature to implement various “Quality of Service” schemes based on selecting which address pool (with corresponding options and policies) will service a specific client.

Adding a DHCP Client Class

To add a Client Class, click the **Add DHCP Client Class** link. The Add DHCP Client Classes screen will appear.

Table 5-16 Add DHCP Client Class Parameters

Field	Description
Name	The name associated with this DHCP Client Class.
DHCP Version	Specify which DHCP Version you want to support: DHCPv4 or DHCPv6. The DHCP Version cannot be changed after entry.
Type	The type of client class restriction. This cannot be changed after entry. Valid types are: <ul style="list-style-type: none"> • MAC Address (DHCPv4 only) • Client Identifier (DHCPv4 only) • DUID (DHCPv6 only) • Hostname • User Class Identifier • Vendor Class Identifier • Custom Expression
DHCP Policy Set	<i>Optional.</i> The DHCP Policy Set that will apply to clients in this DHCP Client Class.
DHCP Option Set	<i>Optional.</i> The DHCP Option Set that will apply to clients in this DHCP Client Class.
Option Definition	<i>Only available for client classes defined by a Vendor Class Identifier.</i> This should be set to the Vendor Specific Information Option (VSIO) definition that corresponds to the vendor. VSIO definitions are created using the Option Master Dictionary and Option Vendor Dictionary menu selections and include those option definitions for DHCPv4 option code 43 and its suboptions or DHCPv6 option code 17 and its suboptions.
Statement/Expression	<i>Only available for client classes defined by a Custom Expression.</i> A free form text field where a service access expression that can be understood by the DHCP server can be entered.
Add <Restriction Flag>	<i>Based on client class restriction type.</i> Click button to add a restriction flag to this client class.

Field	Description
Filter Criteria	<p><i>Based on client class restriction type.</i> String fragment of an entity identifier in the IPAM infrastructure that can serve as a client class “allow/deny” access flag. Use the corresponding radio buttons to determine how the string fragment will be utilized to search for matching entity identifiers. The options are:</p> <ul style="list-style-type: none"> • Begins With – the entity identifier must begin with the string fragment. • Contains – the entity identifier must contain the string fragment. • Exact – the entity identifier must match the string fragment exactly.
Restriction Flag	<p><i>Based on client class restriction type.</i> String fragment of an entity identifier in the IPAM infrastructure that can serve as a client class “allow/deny” access flag.</p>
Restriction Flag Options	<p><i>Based on client class restriction type.</i> Specify how the restriction flag should be utilized by the DHCP server to decide when to apply the client class to the IP address infrastructure under management. The options are:</p> <ul style="list-style-type: none"> • Begins With – the entity identifier must begin with the string fragment. • Exact Match – the entity identifier must match the string fragment exactly.

Enter the desired attributes and once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing a DHCP Client Class

To modify an existing Client Class, click on the name in the Client Class List to open the Edit DHCP Client Class screen.

Edit Client Classes as needed. Choose from the following actions:

- To add another restriction flag, click the **Add [MAC Address | Client Identifier | DUID | Hostname | User Class | Vendor Class]** button. A new data entry row will appear where you can enter a type appropriate value. Repeat as needed. In the special case of a **Custom Expression** restriction, only one may be used per client class.
- To remove an identifier entry, select **Delete**.
- To search for identifiers that match your criteria, enter a string in the **Filter Criteria** field, choose from one of the **Identifiers** options and click **Search**. The Identifiers list is refreshed to match your criteria.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Deleting a DHCP Client Class

To delete one or more DHCP Client Classes, click the checkbox in the Select column for each item you wish to delete, and click .

Note 1: You cannot delete a Client Class that is assigned to a DHCP Server (Network Service) or IP Address Pool without deleting these associations first.

Note 2: Any client class you want to use to govern how a DHCP server interacts with its managed IP infrastructure must be associated to the DHCP server on the **Management > DHCP > Server/Services > (Service Name Link) > Edit > Configuration** screen.

Option Vendor Dictionary

Use the Option Vendor Dictionary screen to maintain DHCP Vendor Options within the system. Vendor Options are DHCP options that are specific to a vendor or type of DHCP server. This menu item allows you to select a set of options (from the DHCP Master Option List) that are available for use with a specific type of DHCP server. In addition, the syntax for this option (as written to the configuration file) is specified using this menu item as well.

When the DHCP Option Vendor Dictionary icon or link is selected, the existing DHCP Products will be shown. DHCP Products can be added, modified, or deleted, using the **DHCP Software Products** menu item from the **Management** menu.

To modify the options associated with this DHCP Product, click the **Options** icon next to the DHCP product that you want to maintain. The DHCP Vendor Option Dictionary screen appears.

Table 5-17 DHCP Vendor Option Dictionary Parameters

Field	Description
Show All Options	When checked, the superset of all available options associated with the selected DHCP server version is displayed. Otherwise only the options currently assigned to this vendor dictionary are shown.
Enabled	When checked, indicates that this DHCP Option is enabled for this DHCP Product.
Code	The code or number of the option as defined by RFC2132 or an RFC draft.
Name	The name of the DHCP Option.
Type	<i>Supported only for INS/ISC DHCP 4.2 and CNR DHCP 8.0 or 8.1 servers.</i> Indicates whether the DHCP Option is IPv4 or IPv6. You can display DHCP Options of a specific type only by selecting from the drop-down list at the top of the screen. The default setting is Both IPv4/IPv6 .
Option Tag	The tag for this option that is written to the configuration file when a DHCP deployment task is created. Note that when viewing a CNR Vendor Dictionary, all the Option Tag and Suffix fields are blank. This is because CNR only pays attention to option codes and is configured through an API rather than by reading a “dhcpd[6].conf” file as an ISC DHCP server would.
Suffix	The suffix for this option, which is written to the configuration file after the “Option Tag” and “value” have been written.
Render Definition	Toggle to render the option definition in the DHCP push. Typically used for custom definitions, since the default set are understood by default.

Adding New Options to DHCP Product

To add new DHCP options to this option set, click on the **Show all options** checkbox at the top of the screen. This displays all DHCP options that are defined within the system.

To add a new option to this DHCP Product, click the **Enabled** checkbox next to the option that you want to add to this DHCP vendor.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Removing Options from an DHCP Option List

To remove options from a DHCP product, uncheck the **Enabled** checkbox next to the option that you wish to remove from this option set.

Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Option Master Dictionary

Use the DHCP Option Master Dictionary to maintain DHCP Master Options within the system. Master Options are predefined with all available options that are normally configured with an IPv4 and IPv6 DHCP server, but may be modified for your environment. DHCPv6 options are currently associated with five DHCP server products:

- CNR 8.0
- CNR 8.1
- INS DHCP 4.2
- ISC DHCP 4.2

In addition, you may add your own options if they are not already defined within the system.

When the DHCP Option Master Dictionary icon or link is selected, the existing DHCP Master options and associated descriptions will be shown.

Adding a DHCP Master Option

To add a DHCP Master Option, click the **Add DHCP Option Dictionary Entry** link. The Add Master DNS Option screen appears.

Table 5-18 Add DHCP Option Dictionary Parameters

Field	Description
Option Type	Indicate whether the option is for DHCPv4 or DHCPv6.
Parent Option	Select the parent option only if the option you are creating is a suboption. None – Indicates that this is not a suboption.
Option Name	The name of the option. This name appears in lists within the user interface.
Short Description	The short description for this option. This description appears in tooltips. Only use alphanumeric characters.
Full Description	The full description for this option. Only use alphanumeric characters.
Option Code	The numeric option code.
Option Value Type	Select the type of option: <ul style="list-style-type: none"> • IPv4 Address • IPv6 Address • Numeric • String • Boolean • IP Address Pair • Hex String • Composite (Use for a parent with sub-options) • Unquoted String

Field	Description
Minimum	Used for validation when Option Value Type is set to Numeric. Enter the minimum allowed value for this option.
Maximum	Used for validation when the Option Value Type is set to Numeric. Enter the maximum allowed value for this option.
Required	Checked indicates that a value for this option is required.
Multi-Valued	Checked indicates that this option can have more than one value, for example, when Option Value Type is set to IP Address Pair..

Once you have completed defining the DHCP option, click **Submit** to save the option, or **Cancel** to return to the previous screen. If the option was successfully added, the list shows the new option within the list.

Editing a DHCP Master Option

To modify an existing DHCP Master Option, click on the option name in the DHCP Master Option List. The Edit DHCP Master Option screen is displayed.

Edit the DHCP master option fields as needed. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Deleting a DHCP Master Option

To delete one or more DHCP Master Options, select the checkbox beside each item you wish to clear, and click the “Delete Selected” button. You are prompted for confirmation. Click **OK** to delete the selected master options, or **Cancel** to return to the previous screen.

DHCP Software Products

Use the DHCP Software Products screen to maintain DHCP products that can be managed by IPAM. IPAM was built as a platform that can manage multiple DHCP products. This screen is used to define these products, and the attributes that are associated with them.

A set of pre-defined products are included with the system. These products include all the definitions, options, and business logic that are needed to properly manage these network services. Additional products may be added to the system, as long as these newer products are derived from existing product definitions (that is, they share the same attributes, and so on).

Adding a Product

To add a software product, click the **Add Product** link. The Add Product screen opens.

Table 5-19 Create Product Parameters

Field	Description
Name	<i>Mandatory.</i> Enter the DHCP Product Name that you want to create.
Description	<i>Optional.</i> Enter a description of this product.
Vendor	Select the Vendor of this product.
Type	DHCP is displayed.
Configuration Type	<p>Informs the system which type (or syntax format) of configuration file should be created by the configuration/deployment task for this service.</p> <p>Supported DHCP Types:</p> <ul style="list-style-type: none"> • NONE – Indicates that this product will not support the creation of DHCP configuration files. • ISC – Indicates that servers that are defined as this product type utilize ISC DHCP 3.0 syntax for their configuration files. • ISCV6 – Indicates that servers that are defined as this product type utilize ISC DHCP 4.2 syntax for their configuration files. • MSFT – Microsoft 2008 DHCP Servers • CNR – Cisco CNR 8.x DHCP Servers

Field	Description
Collection Type	<p>Informs the system which type of collection mechanism should be used to collect information from this service.</p> <ul style="list-style-type: none"> • NONE – No DHCP collection will enabled for this product. • ISC – The system will use the ISC 3.x or 4.x collection mechanism. • QIP – The system will use the Alcatel-Lucent VitalQIP collection mechanism. Supported DHCP servers include the DHCP servers included with VitalQIP 5.x, and VitalQIP 6.x. • CNR – The system will use the Cisco CNR collection mechanism. Supported DHCP servers include the DHCP servers included with CNR 8.x. • ADC – The system will use the ADC/Bigband Fastflow collection mechanism. • MSFT – The system will use the Microsoft DHCP server collection mechanism. Supported DHCP servers include Windows 2008.

Fill in the appropriate fields. Once finished, click **Submit** to save your changes, or **Cancel** to return to the previous screen.

Editing a Software Product

To edit the attributes of a Software product, click on the name of the product.

The Edit Product screen appears. Edit the values for the product, as described in Table 5-19.

Once finished, click **Submit** to save all changes on this Options screen, or **Cancel** to discard all changes and return to the previous screen.

Deleting a Software Product

To delete one or more DHCP Products, select the checkbox beside each item you wish to delete, and click . You are prompted for confirmation.

Note: Make sure that this Product is not assigned to any DHCP Server (Network Service) before you delete it.

Click **OK** to delete the selected Products, or **Cancel** to return to the previous screen.

Chapter 6 Producing Reports

Reports Overview

IPAM reports are grouped into three categories:

Utilization	Audit	Other
<ul style="list-style-type: none"> • Container 	<ul style="list-style-type: none"> • Container 	<ul style="list-style-type: none"> • Tasks (<i>same as link below Cisco Prime Network Registrar IPAM menu</i>)
<ul style="list-style-type: none"> • Subnet/Block 	<ul style="list-style-type: none"> • Subnet/Block 	<ul style="list-style-type: none"> • Alerts (<i>same as link below Cisco Prime Network Registrar IPAM menu</i>)
<ul style="list-style-type: none"> • Low Pool 	<ul style="list-style-type: none"> • IP/Device • Domain • Resource Record • Administrator Activity • Administrator Login • Delegated Prefix 	<ul style="list-style-type: none"> • Appliance Dashboard • Logged-In Administrators • RIR Summary • SWIP/Net Name Information • DNS Zone Report

Administrator access to reports can be controlled in Administrator Policies **Authorized Functions** tab in both Administrator Definition and Administrator Roles. These functions are located in the ADMINISTRATORS section of the **Tools** menu.

Filters

Many reports allow you to filter the data that are displayed to suit your own requirements. When you select these reports from the **Reports** menu, the left pane displays a set of filters that allows you to select what data you want to view. Report output refreshes dynamically, based on the filter criteria you select.

Filters are also organized in a similar fashion to a folder hierarchy, so you can collapse and expand elements as required by clicking the  and  icons respectively.

Descriptions of the filter elements for each report are available throughout this chapter.

In addition to filtering the content of a report, you can change which columns appear, as well as their order sequence. Columns can be sorted and are distinguished by their black headings. For further details, refer to “Column Sorting” on page 17.

Note: Changes made to filter criteria and column selection cannot be saved for reuse at a later date. If you wish to save results of a specific criteria and column selection for analysis and review, IPAM recommends you use one of the output Export options, as described in “Exporting Output” on page 18.

Container Utilization Report

The Container Utilization Report provides summarized utilization information about specific block types within the system based on the container hierarchy. It allows you to report on the utilization within a container based on any utilization criteria that you desire. Run a Global Utilization Rollup to see the most current data (described in Table 3-26 on page 69).

Creating a Container Utilization Report

To create a Container Utilization Report, follow these steps.

1. Select **Container** from the UTILIZATION section of the **Reports** menu. The Filters pane and default content and layout for the Container Utilization Report open.
2. Customize the report by making selections in the Filters pane, as described in **Table 6-1**.

Table 6-1 Container Utilization Report Filter Elements

Filter	Description
Container	
Branch	<i>Optional.</i> Click the “Search” button to select a starting container for filtering report results. The report will be generated for this container and all of its descendants.
Total IP	
IPs Available	Select the radio button next to this option to filter the report by blocks that have less than the specified number of IP Addresses free. Enter the “Available IPs” and blocks that have the specified amount to be displayed in the report.
% free	Select the radio button next to this option to filter the report by blocks that have less than the specified percent free space. Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).

Filter	Description
Days Remaining and R Squared	Select the radio button next to this option to filter the report by blocks that have less than the specified days remaining before running out of address space. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space will be displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPAM.
Dynamic IPs Available	Select the radio button next to this option to filter the report by blocks that have less than the specified number of dynamic IP Addresses free. Enter the "Available IPs" and blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic % Free	Select the radio button next to this option to filter the report by blocks that have less than the specified percent of dynamic free space. Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic Days Remaining and Dynamic R Squared	Select the radio button next to this option to filter the report by blocks that have less than the specified days remaining before running out of dynamic address space. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPAM.
Usables	Select the radio button next to this option to filter by the number of usable hosts in the container.
Allocated	Select the radio button next to this option to filter by the number of allocated hosts in the container.
Unallocated	Select the radio button next to this option to filter by the number of unallocated hosts in the container.
Reserved	Select the radio button next to this option to filter by the number of reserved hosts in the container.
Assigned	Select the radio button next to this option to filter by the number of assigned hosts in the container.
Locked	Select the radio button next to this option to filter by the number of locked hosts in the container.
Alloc %	Select the radio button next to this option to filter by the percentage of allocated hosts out of the total number of utilized hosts.
Util %	Select the radio button next to this option to filter by the percentage of assigned hosts out of the total number of available hosts.

Filter	Description
IP Version	
v6 v4	Choose whether v4 or v6 will be used as a filter.
Container Type	
Logical Device	<i>Optional.</i> Select a container type if you wish to filter report output for Logical or Device containers.
User Defined Fields	
UDF Name	Select the name of the User Defined Field to be used as a filter. Note: User defined fields are defined in the User Defined Fields tool on the Tools menu.
UDF Value	Select the value that appears in the User Defined Fields column.
Block Type	
<Site Dependent>	Select the Block Type that you want to report against. Block types are defined in the Block Types tool on the Tools menu.

Container Utilization Report Output

The default Container Utilization Report.

Columns in the report output are described in **Table 6-2**.

Table 6-2 Container Utilization Report Output Elements

Field	Description
Container	The Container Name that contains the utilization criteria that you selected. Click on the link to open the Address Block Details screen for the container.
History	Click on this link to view a history graph of the utilization information for this address pool.
Interface	The interface name (if any) associated with the utilization criteria that was selected.
Total IP	The total IP addresses of this address block.
In Use	The total IP Addresses within this block that are in use.
IPs Available	The number of IP Addresses that are available within this block.
Last Update	The last date and time that this block was updated during a Global Utilization Rollup task.
% Free	The percent of free space available within this block.
Dynamic % Free	The percent of dynamic free space available within this block.
R Squared	Displays the correlation coefficient for predicting the number of days remaining for all IP addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Dynamic IPs Available	Indicates the number of dynamic IP addresses currently available.

Field	Description
Dynamic R Squared	Displays the correlation coefficient for predicting the number of days remaining for dynamic addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Days Remaining	Indicated the number of days remaining before running out of address space.
Dynamic Days Remaining	Indicates the number of days remaining before running out of dynamic address space. Enter the specified days, and the correlation coefficient (r2).
Usables	The number of usable hosts in the container.
Allocated	The number of allocated hosts in the container.
Unallocated	The number of unallocated hosts in the container.
Reserved	The number of reserved hosts in the container.
Assigned	The number of assigned hosts in the container
Locked	The number of locked IP Address(es). IP Addresses that have been reported as being locked by a DHCP server during a “ping before assign” check.
Alloc %	The percentage of allocated hosts out of the total number of usable hosts.
Util %	The percentage of assigned hosts out of the total number of available hosts.
IP Version	Indicates whether the IP addresses are v4 or v6 format.
Container Type	Indicates whether the container is a logical or device container.
User Defined Fields	The user defined fields affiliated with this block.
Block Type	The Block type associated with this block.

Block Utilization Report

The Block Utilization Report provides utilization information about specific blocks within the system. It allows you to report on blocks based on any utilization criteria that you desire.

Creating a Block Utilization Report

To create a Block Utilization Report, follow these steps.

1. Select **Subnet/Block** from the UTILIZATION section of the **Reports** menu. The Filters pane and default content and layout for the Block Utilization Report open.
2. Customize the report by making selections in the Filters pane, as described in **Table 6-3**.

Table 6-3 Block Utilization Report Filter Elements

Field	Description
Block Type	

Field	Description
<Site Dependent>	Select the Block Type that you want to report against. Block types are defined in the Block Types tool on the Tools menu.
Total IP	
% Free	Select the radio button next to this option to filter the report by blocks that have the specified percent free space. Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
IPs Available	Select the radio button next to this option to filter the report by blocks that have the specified number of IP Addresses free. Enter the “IPs Available” and blocks that have the specified amount to be displayed in the report.
Days Remaining and R Squared	Select the radio button next to this option to filter the report by blocks that have the specified days remaining before running out of address space. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r ²). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPAM.
Dynamic % free	Select the radio button next to this option to filter the report by blocks that have the specified percent free space for dynamic devices only (Manual DHCP, Automatic DHCP, and Dynamic DHCP). Enter the percent free (1-100) blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic IPs Available	Select the radio button next to this option to filter the report by blocks that have the specified number of IP Addresses free for dynamic devices only (Manual DHCP, Automatic DHCP, and Dynamic DHCP). Enter the “IPs Available”, and blocks that have the specified amount to be displayed in the report. You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>).
Dynamic Days Remaining and Correlation Coefficient	Select the radio button next to this option to filter the report by blocks that have the specified days remaining before running out of address space for dynamic devices only (Manual DHCP, Automatic DHCP, and Dynamic DHCP). You can also modify your filter criteria from the default is less than (<) to equals (=) or is greater than (>). Enter the specified days, and the correlation coefficient (r ²). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPAM.
IP Version	
v6 v4	Choose whether v4 or v6 will be used as a filter.

Field	Description
User Defined Fields	
UDF Name	Select the name of the User Defined Field to be used as a filter. Note: User defined fields are defined in the User Defined Fields tool on the Tools menu.
UDF Value	Select the value that appears in the User Defined Fields column.

Block Utilization Report Output

The default Block Utilization Report.

Columns in the report output are described in **Table 6-4**.

Table 6-4 Block Utilization Report Output Elements

Field	Description
Block	The Block in CIDR notation.
History	Click on this link to view a history graph of the utilization information for this address pool.
Block Type	The Block type associated with this block.
Total IP	The total IP addresses of this address block.
In Use	The total IP Addresses within this block that are in use.
Locked	The number of locked IP Address(es). IP Addresses that have been reported as being locked by a DHCP server during a “ping before assign” check.
IPs Available	The number of IP Addresses that are available within this block.
Last Update	The last date and time that this block was updated during a Global Utilization Rollup task.
% Free	The percent of free space available within this block.
Dynamic % Free	The percent of dynamic free space available within this block.
R Squared	Displays the correlation coefficient for predicting the number of days remaining for all IP addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Dynamic IPs Available	Indicates the number of dynamic IP addresses currently available.
Dynamic R Squared	Displays the correlation coefficient for predicting the number of days remaining for dynamic addresses (between 0.0 and 1.0), and indicates the confidence in the regression. A 1.0 specifies a perfect fit.
Days Remaining	Indicated the number of days remaining before running out of address space.
Dynamic Days Remaining	Indicates the number of days remaining before running out of dynamic address space. Enter the specified days, and the correlation coefficient (r2).
IP Version	Indicates whether the IP addresses are v4 or v6 format.
Container	Displays the containers with which a block is associated. Click on the link to open the Address Block Details screen for the container.

Field	Description
User Defined Fields	The User Defined Fields affiliated with this block.

Low Pool

The Low Pool Report displays the address pools or blocks that are high in utilization, and/or have a low number of IP addresses available.

Creating a Low Pool Report

To create a Low Pool Report, follow these steps.

3. Select **Low Pool** from the UTILIZATION section of the **Reports** menu. The Filters pane and default content and layout for the Low Pool Report open.
4. Customize the report by making selections in the Filters pane, as described in **Table 6-5**.

Table 6-5 Low Pool Report Filter Elements

Field	Description
Block Type	Select a specific block type to report against, or select “All Block Types”.
% Free	Select the radio button next to this option to filter the report by blocks that have less than the specified percent free space. Enter the percent free (1-100) blocks that have less than the specified amount to be displayed in the report.
IPs Available	Select the radio button next to this option to filter the report by blocks that have less than the specified number of IP Addresses free. Enter the “Available IPs”, and blocks that have less than the specified amount to be displayed in the report.
Days Remaining and Correlation Coefficient	Select the radio button next to this option to filter the report by blocks that have less than the specified days remaining before running out of address space. Enter the days remaining, and the correlation coefficient (r2). The correlation coefficient is between 0.0 and 1.0 and indicates the confidence in the regression. A 1.0 specifies a perfect fit. Blocks that have less than the specified number of days remaining with free space are displayed in the report. This option uses the regression analysis and the forecasting algorithm that is built into IPAM.
IP Version	Choose whether IPv4 or IPv6 is used as a filter.

Low Pool Report Output

The default Low Pool Report.

Columns in the report output are described in **Table 6-6**.

Table 6-6 Low Pool Report Output Elements

Field	Description
History	Click on the link to view a history graph of the utilization information for this address pool.
Pool	The pool starting and ending IP Addresses or the shared network name.
Block Type	The Block type associated with this pool.
Total IP	The total IP addresses of this address pool.
In Use	The total IP Addresses within this pool that are in use.
Locked	The number of IP Addresses that have been reported as being locked by a DHCP server during a “ping before assign” check.
IPs Available	The number of IP Addresses that are available within this pool.
IP Version	Indicates which IP version the pool uses: IPv4 or IPv6.
Last Update	The last date and time that this block was updated during a Global Utilization Rollup task.
Container	Displays the container with which a block is associated. Click on the link to open the Address Block Details screen for the container.
% Free	The percent of free space available within this pool. (Filter dependent)
Days Left	The predicted number of days left until the available space is exhausted. (Filter dependent)
r2	The R Squared coefficient of the days left calculation. Values closer to 1 indicate a higher reliability. (Filter dependent)

Container Audit Report

The Container Audit Report provides audit information about changes that have occurred within a specific container.

Creating a Container Audit Report

To create a Container Audit Report, follow these steps.

5. Select **Container** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Container Audit Report open.
6. Customize the report by making selections in the Filter pane, as described in **Table 6-7**.

Table 6-7 Container Audit Report Filters

Field	Description
Date/Time	

Field	Description
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Container Audit Report Output

The default Container Audit Report.

Use the “Container Search” link to select a container to audit.

Columns in the report output are described in **Table 6-8**.

Table 6-8 Container Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Container	The container that this event occurred in.
Event Type	The event type that took place: Create Container – A container was created Modify Container – A container was changed Delete Container – A container was deleted Add Block – a block has been added to this container Delete Block – a block has been deleted from this container.
Additional Information	Additional information related to the specific task.

Block Audit Report

The Block Audit Report provides audit information about changes that have occurred to a specific block.

Creating a Block Audit Report

To create a Block Audit Report, follow these steps.

7. Select **Subnet/Block** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Block Audit Report open.
8. Customize the report by making selections in the Filter pane, as described in **Table 6-9**.

Table 6-9 Block Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
Block Size	
Selected Block Size	Select the size of the block in CIDR notation from the drop-down list, or leave at Select All to display all blocks.
IP Version	
v4	Select to filter on IPv4 blocks.
v6	Select to filter on IPv6 blocks.
Reason Code	
Select Reason Code	Select one of the allocation reason codes defined in Tools > SUBNET/BLOCK > Allocation Reason Codes , or leave at Select All to display all blocks.

Block Audit Report Output

The default Block Audit Report.

Columns in the report output are described in **Table 6-10**.

Table 6-10 Block Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Block	The block on which this event occurred.
Block Size	The size of the block in CIDR notation.
Event Type	The event type that took place: Create – a block has been added Delete – a block has been deleted Move – a block has been moved Update – a block has been updated
IP Version	The type of IP address: v4 or v6.
Reason Code	The Reason Code assigned to this block when it was allocated, if any.
Additional Info	Additional information related to the specific task, such as information in the Block Profile that was modified on an Update action.

Device Audit Report

The Device Audit Report provides audit information about changes that have occurred to a specific device. You may run this report for a specific IP Address or a specific MAC Address.

Creating a Device Audit Report

To create a Device Audit Report, follow these steps.

9. Select **IP/Device** from the **AUDIT** section of the **Reports** menu. The Filters pane and default content and layout for the Device Audit Report open.
10. Customize the report by making selections in the Filter pane, as described in **Table 6-11**.

Table 6-11 Device Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
IP Address	
Enter IP Address	Enter the IP Address to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
Hardware Address	
Enter Hardware Address	Enter the hardware address (MAC Address) to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .

Device Audit Report Output

The default Device Audit Report.

Columns in the report output are described in **Table 6-12**.

Table 6-12 Device Audit Report Output Screen Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Host Name	The host name for this device.
Event Type	The event type that took place: Create, Delete, or Modify
IP Address	The IP Address for this device.
Hardware Address	The MAC Address for this device.
Address Type	The Address type that was assigned to this device when the audit record was created.
Additional Information	Additional information related to the specific task.

DNS Domain Audit Report

The DNS Domain Audit Report provides audit information about creates, updates and deletes of DNS Domains.

Creating a DNS Domain Audit Report

To create a DNS Domain Audit Report, follow these steps.

1. Select **Domain** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the DNS Domain Audit Report open.
2. Customize the report by making selections in the Filter pane, as described in **Table 6-21**.

Table 6-13 DNS Domain Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Field	Description
Derivative	Select 'Standard', 'Alias' or 'Template' if you want to filter the report based on the derivative.
Managed	Filter options include 'All', 'Managed' or 'Non-managed'
Delegated	Filter options include 'All', 'Delegated' or 'Not Delegated'
Reverse	Filter options include 'All', 'Reverse' or 'Forward'

DNS Domain Audit Report Output

The default DNS Domain Audit Report is shown below.

Columns in the report output are described below.

Table 6-14 DNS Domain Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Domain	The delegated prefix on which this event occurred.
Event Type	The event type that took place: Create – a delegated prefix has been added Delete – a delegated prefix has been deleted Update – a delegated prefix has been updated
Derivative	Indicates whether the domain that was added or deleted is a standard domain, a template or an alias.
Managed	Indicates whether the domain that was added or deleted is 'Managed'(fully defined in IPAM).
Delegated	Indicates whether the domain that was added or deleted is 'Delegated'(domain is associated directly with a zone file.)
Reverse	Indicates whether the domain that was added or deleted is a reverse in-addr.arpa or ip6.arpa domain.
Additional Info	Additional information related to the specific event. This specifies the updates to domain in the form: "Property Name: Old Value->New Value".

Resource Record Audit Report

The Resource Record Audit Report provides audit information about changes that have occurred to DNS Resource Records. You may run this report for a specific FQDN, DNS Owner, and Resource Record Type.

Creating a Resource Record Audit Report

11. Select **Resource Record** from the **AUDIT** section of the **Reports** menu. The Filters pane and default content and layout for the Resource Record Audit Report open.
12. Customize the report by making selections in the Filter pane, as described in **Table 6-15**.

Table 6-15 Resource Record Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
FQDN	Enter the Fully Qualified Domain Name (Host name . domain name) of the resource records for which you want to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
Owner	Enter the DNS “Owner” field, as specified in DNS Resource Record definitions, that will be used to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .
RR Type	Enter the Resource Record Type (that is, A, PTR, CNAME, and so on) if you are trying to limit the report to a specific Resource Record Type.
Data	Enter the DNS “RData” field, as specified in DNS Resource Record definitions, that will be used to display audit information. You can use the default criterion of an exact match (Is Exactly), or use the drop-down to select Begins with or Contains .

Field	Description
IP Address	Enter the IP Address for which to display audit information. You should only use this filter for A and PTR records.

Resource Record Audit Report Output

The default Resource Record Audit Report.

Columns in the report output are described in **Table 6-16**.

Table 6-16 Resource Record Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
FQDN	The Fully Qualified Domain Name for this record.
Event Type	The event type that took place: Create, Delete, Update, Pending Create, Pending Delete, Pending Update, Create Approved, Update Approved, Delete Approved.
Domain	The Domain where this Resource Record is assigned.
Owner	The DNS “Owner” Information of this record.
RR Type	The DNS Resource Record Type of this device.
Data	The DNS “RData” Information of this record.
IP Address	The IP Address for this device.
Additional Information	Additional information related to the specific task.

Administrator Definition Audit Report

The Administrator Definition Audit Report provides audit information about administrator creates, deletes, updates and role changes.

Creating an Administrator Definition Audit Report

Select **Administrator Definition** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Administrator Definition Audit Report open, as shown in below.

You may customize the report by making selections in the Filter pane, as described in table below

Administrator Definition Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.
Admin Type	Select one of the options from the drop-down to see all, normal, master or read only admin types.
First Name	Enter the first name or few characters from the first name to filter the report against.
Last Name	Enter the last name or few characters from the last name to filter the report against.
Role	Enter the role or few characters from the role to filter the report against.

To filter the report based on the ‘LoginID’ field, use the search box in the top left corner of the report.

Administrator Definition Audit Report Output

The default Administrator Definition Audit Report is shown below.

Columns in the report output are described in table below **Table 6-18**.

Administrator Definituin Audit Report Output Screen Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
LoginID	The login id of the administrator that was added, deleted or modified
Event Type	The event type that took place. One of the following: <i>Create</i> : An administrator was added. <i>Delete</i> : An administrator was deleted <i>Update</i> : An administrator definition was updated <i>Add Role</i> : A role was assigned to the administrator <i>Delete Role</i> : A role was deleted from administrators profile <i>Add Assignable Role</i> : An assignable role was assigned to the administrator <i>Delete Assignable Role</i> : An assignable role was deleted from administrators profile
Admin Type	Type assigned to the admin, one of 'Normal', 'Master' or 'Read Only'.
First Name	First Name of the Administrator.
Last Name	Last Name of the Administrator.
Role	Role assigned to (or removed from the profile of) the administrator. This field is populated only for 'role' related event types.
Additional Information	Additional information related to the specific event. Updates to the administrator are displayed in the form: "Property Name:Old Value->New Value".

Administrator Activity Audit Report

The Administrator Activity Audit Report provides a combined view of the audit activities from all the other audit reports. It allows you to see all the activities of a user from login to logoff or all the changes made to the system for a particular time.

Creating an Administrator Activity Audit Report

13. Select **Administrator Activity** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Administrator Audit Report open.
14. Customize the report by making selections in the Filter pane, as described in **Table 6-17**

Table 6-17 Administrator Activity Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Administrator Activity Audit Report Output

The default Administrator Activity Audit Report.

Columns in the report output are described in **Table 6-18**.

Table 6-18 Administrator Activity Audit Report Output Screen Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Scope	Categorization based on the area of activity. For example: Changes to container have the scope container Changes to device are under device scope. The sub-columns under Details change based on the scope.
Event Type	The event type that took place: Login, Logoff, Create, Add Block, Update and so on.
Details	Details column has sub-columns based on the scope and provides additional information related to the activity. For example: Login scope has Session ID and Client IP Address sub-columns under Details. Container scope has Container Name and Additional Info sub-columns.

Login Audit Report

The Login Audit Report provides audit information about system access activities like login, logout, session timeout, and so on.

Creating a Login Audit Report

15. Select **Administrator Login** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Login Audit Report open.
16. Customize the report by making selections in the Filter pane, as described in **Table 6-19**.

Table 6-19 Login Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Login Audit Report Output

The default Login Audit Report.

Columns in the report output are described in **Table 6-20**.

Table 6-20 Login Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Event Type	The event type that took place: Login, Logoff, Session timed out
Session ID	Session ID associated with this particular session. This is useful when an admin has multiple application sessions open.
Client IP Address	IP address of the client or last proxy that the Admin logged in from.

Delegated Prefix Audit Report

The Delegated Prefix Audit Report provides audit information about changes that have occurred to delegated prefix blocks. This information is supplied from Discovery data when the **Audit Delegated Prefixes** system policy is set to **Yes**. Additionally, if a delegated prefix

is moved to another subnet, any leases attached get deleted, which should initiate an entry in this report.

Creating a Delegated Prefix Audit Report

To create a Delegated Prefix Audit Report, follow these steps.

3. Select **Delegated Prefix Report** from the AUDIT section of the **Reports** menu. The Filters pane and default content and layout for the Delegated Prefix Audit Report open.
4. Customize the report by making selections in the Filter pane, as described in **Table 6-21**.

Table 6-21 Delegated Prefix Audit Report Filter Elements

Field	Description
Date/Time	
Start date	Select the Start Date field to display the calendar, and select the starting date for which to filter the audit report. The format of the start date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of start date. Select the start time using the drop-down menus.
End date	Select the End Date field to display the calendar, and select the ending date for which to filter the audit report. The format of the end date is “mm/dd/yyyy”. If you leave this field blank, all items are returned regardless of end date. Select the end time using the drop-down menus.
Admin	
<Site Dependent>	Select the administrators that you want to filter the report against.

Delegated Prefix Audit Report Output

The default Delegated Prefix Audit Report is shown below.

Columns in the report output are described below.

Table 6-22 Delegated Prefix Audit Report Output Elements

Field	Description
Date/Time	The date and time that the audit event took place.
Admin	The administrator that initiated the event.
Address	The delegated prefix on which this event occurred.
Event Type	The event type that took place: Create – a delegated prefix has been added Delete – a delegated prefix has been deleted Update – a delegated prefix has been updated
Prefix Type	Indicates whether the prefix is Dynamic PD DHCPv6 or Automatic PD DHCPv6.
Start Lease	Indicates the start lease time.

Field	Description
Preferred End Lease	Indicates the preferred end lease time.
Valid End Lease	Indicates the valid end lease time.
DUID	Displays the DHCP Unique Identifier of the device to which the prefix was delegated.
IAID	Displays the Identity Association ID for this delegated prefix lease.
Additional Info	Additional information related to the specific task.

Tasks

The **Tasks** option allows you to view and manage tasks that have been created in the system. You may use this option to view the status of the tasks, as well as view specific results from the task itself.

The reports that are created in the task display provide you with planned vs. actual views of the configuration (IP Address space allocations) to your network services and network elements.

Tasks Screen Layout

When you select **Tasks** from the OTHER section of the **Reports** menu, a Filters pane appears in the left pane, and a view of your tasks is displayed within the main browser window.

To delete tasks, select the checkbox next to the task ID you want to delete and click .

To refresh, choose from the following actions.

To refresh immediately, click .

To select other refresh intervals, select an interval from the **Refresh** drop-down list:

You can also sort most columns by clicking on the column header. Columns in the report output are described in **Table 6-23**.

Table 6-23 Task List Screen Elements

Field	Description
ID	A unique task id that is assigned by the system.
Status	Graphical representation of the status of the task. Complete –  Complete w/Errors –  Error –  Fail w/Retry –  In Progress -  Not Started –  Preview Ready –  Preview Ready w/Errors –  Queued – 
Select	Check this box to select this task for deletion.
Start Time	The date and time that the task started.
Completed Time	The date and time that the task completed.
Scheduled	The scheduled interval for the task to run (Immediate, Scheduled, or recurring).

Field	Description
Scope	Task type specific; the specific scope for this task. Depending upon which type of task this is, this could be the network service or network element.
Type	The type of task.
Admin	Identifies the administrator who initiated the task.

Task Details

When you click on the **Task ID** link on a specific task in the task list, the task details are displayed as shown below. This display shows you summary information about the task, such as how long the task took to run.

Click **Back to Task List** to return to the task list display.

Locate Queued/In-Progress Task Messages

For tasks with a status of Queued or In Progress, the Task Details page provides a troubleshooting button for locating task messages within the IPAM task and result queues.

The status of each message located within the task and result queues is displayed in the corresponding read-only text area. If multiple lines are displayed, then more than one message was found. The following is a list of the message statuses that can appear.

Task has not started.

No queued messages exist for tasks that have not started.

Task has completed.

No queued messages exist for tasks that have completed.

No task messages found for ID=###

If this is a parent task, check the child tasks. If this is a child task, the Agent is working on it. No queued messages exist for parent tasks.

Queued(ActiveMQ) for 3.x Agent: x.x.x.x

A task message has been posted to the ActiveMQ task queue, and the message is waiting for the IPAM 3.x Agent identified by IP address 'x.x.x.x' to process the message.

Queued(ActiveMQ) for 3.x Result Manager

A result message has been posted by the IPAM 3.x Agent that was responsible for the task, and the message is waiting for the IPAM 3.x Result Manager to process the message.

Previewing Configuration Files

When you click on the **Details** link for a task with status "Preview Ready", the child task details are displayed. When you click on the **Details** link for that child task, the task summary results section includes a list of configuration and zone files that were created.

To view a file, select either the **PDF** or **Text** link for that file. A new window displays the file contents in the format you selected. The **Deploy** button enables you to continue the deploy process using the files held for preview.

Router Subnet Differences

The Discover Router Subnets task generates child tasks to perform the actual discovery. If the Discover Router Subnets task was run against a particular network element, there will be one child task generated for the network element. If the Discover Router Subnets task was run against a container, one child task will be generated for each network element that is associated with a device container that is a child of the specified container. Which network element the task was run against will be displayed in the Scope column. When each task has completed, a differences button will be displayed on the task details page to view the differences that have been discovered. Clicking on this differences button for the parent task will display the differences for all of the child tasks that were executed, which may contain multiple network elements. Each child task will also have a differences link which you can click to view the differences for that child task only (which will only display the results for the particular network element for which that child task was run against). You can also click on the details link to view the child task details, and then click on the differences button there to view its differences. The differences are displayed on the Router Subnet Differences page.

This screen shows the differences between the plan (what is defined in the system), and the actual configuration that is on a router or device based on the data that was collected. It displays information on interfaces, network addresses, and network sizes. If a difference is found, the actual value will be highlighted in yellow. The search box is used to search for a specific subnet address. The combo box next to the search box is used to filter by a particular difference type.

Field	Description
Net Element Name	The name of the network element to which the difference applies. The page may contain multiple network elements if the Discover Router Subnets task was run against a container, and you chose to view the differences from the parent task.
Difference Type	The type of difference. <ul style="list-style-type: none"> • Configured but not planned - The IP Address, Subnet, and Interface information that has been found on a device (through discovery), but has not been defined within the system. • Planned but not configured - The Subnet information that has been defined within the system, but was not configured on the actual device (through discovery). • Planned and Configured but Difference - The Information about subnets or interfaces where the plan vs the actual information does not match. Differences will be highlighted in yellow.

Field	Description
Subnet Address	The address of the subnet.
I/F Address	The interface address on the router.
Block Size	The size of the subnet.
I/F Name	The name of the interface on the router.

Alert Log

The Alert Log informs the administrator of thresholds that have been crossed in the system. Use this screen to view, search, or delete outstanding alerts.

Working with the Alert Log

- To work with the Alert Log, select **Alerts** from the OTHER sections of the **Reports** menu, or simply click the **Alerts** link below the IPAM logo. The Filters pane and default content and layout for the Alert Log open.

Table 6-24 Alert Log Filter Elements

Field	Description
Date/Time	
Start Date	Fill in this field to limit the output to alerts raised after this date and time.
End Date	Fill in this field to limit the output to alerts raised before this date and time.
Severity	
	Select from the following choices: <ul style="list-style-type: none"> • Critical • Warning • Info

Columns in the report output are described in **Table 6-25**.

Table 6-25 Output Fields

Field	Description
Selected	Check the box in this column for delete operations.
Date/Time	The Date and Time the alert was raised.
Severity	Displays icons that indicate the severity of the alert: <ul style="list-style-type: none">  Information  Warning  Error
Object	Displays the Object that raised the Alert. <p>A Container alert shows the container name, followed by the Block Type specified on the Threshold. The container name displayed as a fully qualified path from the root of the container tree.</p> <p>An Interface Alert shows the Device container name, followed by the Interface name, followed by the block type configured on the Threshold.</p> <p>A Block Alert shows the name of the Block in CIDR notation.</p> <p>A Network Service alert shows the name of the Network Service, followed by Address Pool or Address Pool share name that raised the alert.</p>

Field	Description
Criteria	The Criteria that caused the alert.
Observed Value	The Value that caused the alert.
Confidence	The Confidence value if Criteria tested “Days Left”

Logged-In Administrators Report

The Logged-In Administrator Report provides information on the administrators that are currently logged-in to the system.

Accessing the Logged-In Administrators Report

To access the report, select **Logged-In Administrators** from the OTHER section of the **Reports** menu.

Logged-In Administrators Report Output

The default Logged-In Administrator report.

Columns in the report output are described in **Table 6-26**.

Table 6-26 Logged-In Administrators Report Output Elements

Field	Description
Login Time	The date and time that the user logged in.
Admin	The administrator that logged in.
Session ID	Session ID associated with this particular session. This is useful when an admin has multiple application sessions open.
Client IP Address	IP address of the client or last proxy that the Admin logged in from.

RIR Summary Report

The RIR Summary Report creates a report that can be used to provide utilization information to a Regional Internet Registry such as ARIN or APNIC.

Accessing the RIR Summary Report

To access the report, follow these steps.

Select RIR Summary from the OTHER section of the Reports menu. A Filters pane appears in the left pane, and a view of your block allocation is displayed within the main browser window.

RIR Summary Report Output

The default Regional Internet Registry Report.

Columns in the report output are described in **Table 6-27**.

Table 6-27 RIR Report Screen Elements

Field	Description
Internet Registry	The internet registry assigned to the block.
Organization ID	The organization ID assigned to the block.
Block	The root block and CIDR size.
Usables	The total number of addresses in this block.
Allocated	The number of IP Addresses in sub-blocks (of this block) that have a status of InUse/Deployed or InUse/Fully Assigned.
Unallocated	The number of IP Addresses that are still available for allocation from this block.
Reserved	The number of IP Addresses from this block that have a reserved status.
Assigned	The number of IP Addresses from this block that has been assigned either dynamically, statically, or is in a locked state.
Locked	The number of IP Addresses that are locked.
IP Version	The IP version of the block (v4 or v6)
Alloc %	The percent of this block that is allocated. This is equal to the $(\text{number allocated} / \text{blocksize hosts}) * 100$.
Util %	The percent of this block that is utilized. This is calculated by taking the $(\text{number assigned} / \text{number of addressable hosts}) * 100$. Number of addressable hosts is determined by taking the total blocksize and subtracting all addresses lost due to subnet assignment, such as the subnet and broadcast address.

SWIP/Net Name Report

The SWIP Report provides a report that shows the SWIP ([Shared WHOIS Project](#)) information that is needed to assist in reporting to the ARIN internet registry. Internet Service Providers (ISPs) that receive IP address space from ARIN directly or indirectly (as a downstream customer of another ISP) MUST use either Shared WHOIS Project known as SWIP or a Referral WHOIS server known as RWhois to provide reassignment information for /29 and larger blocks to ARIN.

SWIP is a process used by ISPs to submit customer IP reassignment information to ARIN's WHOIS database. It ensures the effective and efficient maintenance of records for IP address space. All utilization templates must be submitted in ASCII format via e-mail. [RFC 2050](#) Section 2.2 provides a brief description on the submission of Reassignment information.

SWIP is intended to:

Provide information to identify the organizations utilizing each sub-delegated IP address block.

Provide registration information for each IP address block.

Track utilization of allocated IP address blocks to determine if additional allocations may be justified.

Creating a SWIP/Net Name Information Report

To create a SWIP/Net Name Information Report, follow these steps.

18. Select SWIP/Net Name Information from the OTHER section of the Reports menu. A Filters pane appears in the left pane, and a view of your block allocation is displayed within the main browser window.
5. Customize the report by making selections in the Filter pane, as described in **Table 6-28**.

Table 6-28 SWIP/Net Name Report Filter Elements

Field	Description
Root Block Type	
Root Block Type	Select the Regional Internet Registry block type you want to report against. Choices are ARIN or RIPE.
IP Version	
	Select from the following choices: <ul style="list-style-type: none"> • v4 • v6

SWIP/Net Name Information Report Output

The default SWIP Report.

Columns in the report output are described in **Table 6-29**.

Table 6-29 SWIP/Net Name Information Report Output Elements

Field	Description
Block Name	The block name consisting of the starting point of the block and the CIDR size.
SWIP Name	The SWIP name that has been assigned to this block.
Addressable Hosts	The number of hosts that are addressable within this block.
Allocated	The number of IP Addresses that are allocated from this block.
Unallocated	The number of IP Addresses that have not been allocated from this block and are free.
Reserved	The number of hosts that are reserved within this block.
Assigned	The number of hosts that are in use in this block.
Locked	The number of IP Addresses that are locked.

Field	Description
Alloc %	The percent of this block that is allocated.
Util %	The percent of this block that is utilized.
Internet Registry	The Internet Registry assigned to the block.
IP Version	The IP version of the block (v4 or v6).

DNS Zone Report

The DNS Zone Report lists all the zones defined in the system and their related information. For each zone associated with a DNS server(s), this report lists each zone (one line per server assigned) with the following information: Zone, DNS Server, View, Type (master, slave, etc.), Galaxy, Domain (Domain Type if applicable), and flags indicating values for 'Published NS for the server', 'DNS Listener accepting Zone Transfers' and 'Dynamic Updates Enabled'. The report allows filtering, sorting and column rearranging and exports in various formats.

DNS Zone Report Output

A sample DNS Zone Report output is shown below.

Columns in the report output are described in table below.

Table DNS Zone Report Output elements

Field	Description
Zone	Name of the zone.
DNS Server	DNS Server that the zone is defined on.
View	View that the zone is associated with.
Zone Type	Type of the zone.
Galaxy	Name of the galaxy if the DNS Server is part of a galaxy.
Domain	Domain described by the zone.
Publish NS Server for this server	Checked indicates that IPAM will automatically include the server in its calculation of NS and Glue records for this zone/domain.
DNS Listener accepting Zone Transfers	Checked indicates that the IPAM DNS Listener will accept zone transfers from this server for this zone, if the zone is dynamic.
Dynamic Updates Enabled	Checked indicates that this is a dynamic zone.

Chapter 7 Setting Up System Policies, Agents, and Importing Data

System Policies/Options

System Policies are policies that affect your interaction with IPAM system-wide. There are several configurable system policies. To work with System Policies, select **Policies and Options** from the **Tools** menu. The policies are described in Table 7-1 on page 215.

Table 7-1 System Policies/Options Parameters

Field	Description
License Key	The license key you received from BT for Cisco Prime Network Registrar IPAM.
About Page Custom Link "#" Label	Use these numbered fields to add customized hyperlinks to the Home tab. The Label is the value displayed in the Home tab.
About Page Custom Link "#" URL	Use these numbered fields to add customized hyperlinks to the Home tab. The URL is the site (e.g., http://www.companyhelpdesk.com) to be directed to.
Allow Block Allocation from Non-writable Containers	Determines whether users can allocate space from an aggregate block in a container to which the user does not have Write permission.
Allow Block Allocation from the Same Container	When set to Yes, allows a child block to be allocated in the same container as its root block. Wait at least 60 seconds for this change to take effect.
Allow Dots in Host Names	Allows for system-wide permit or deny of dots (.) in hostnames.
Allow Duplicate CNAME Owners	Specifies if you wish to include duplicate CNAME owners. Typically, you should set this option to NO since BIND 9.x does not allow duplicate CNAME owners by default, and discards the zone if you attempt to add duplicates to it.
Allow Overlapping Public Blocks	If Allow Overlapping Public Blocks is set to Yes, then the system will allow creation of overlapping non-RFC1918 root blocks. This is typically not necessary, except in some specialized cases. Thus the default is No.
Allow Underscores in Host Names	Allows for system-wide permit or deny of underscores in hostnames.
Audit Block Changes	Set to Yes to track changes (add, delete, and modify) to a Block.
Audit Container Changes	Set to Yes to track changes (add, delete, and modify) to a Container.

Audit Delegated Prefixes	When set to Yes , allows auditing of delegated prefixes to occur. The audit data can then be reviewed in the Delegated Prefix Report, as described in “Delegated Prefix Audit Report” on page 202.
Audit Device/IpAddress Changes	Set to Yes to track changes (add, delete, and modify) to a Device.
Audit DNS Resource Record Changes	Set to Yes to track changes (add, delete, and modify) to Domain level Resource Records.
Block Folding Threshold	Sets the number of blocks in a container that triggers the folded display instead of the standard list for easier navigation. For example, if there are more than 500 blocks in a container, the folded display is used.
Case Sensitive Password Check	When set to Yes, the login password validation is case sensitive.
Classless in-addr.arpa Notation	Style used when creating classless in-addr.arpa (RFC 2317) domains. Currently only CIDR Usable Range is supported.
Container Folding Threshold	Sets the number of containers that can appear in a tree before the list of containers is folded into ranges for easier navigation. For example, a value of 500 indicates that the folded display is used if there are more than 500 children under a given container.
Field	Description
Count “Other Available” leases for CNR DHCP collections	<i>For CNR Summary Collections Only.</i> If this policy is True, leases marked as “Other Available” are counted as unavailable or locked in the utilization.
Default Allocation Algorithm	The default allocation algorithm to use for automatic block allocation. <ul style="list-style-type: none"> • Select Use Best fit Allocation to set as default the best fit algorithm. • Select Use Random Allocation to set as default the random algorithm (IPv6 only). • Select Use Sparse Allocation to set as default the sparse algorithm (IPv6 only)
Default Domain Contact	Specifies the policy for forming the domain contact. Select from the following: <ul style="list-style-type: none"> • Use Admin’s Email Address to use the administrator’s email address. • Use Explicit Email Address to use the email address specified in the Domain Contact Email system property • Use Explicit Email Address in Current Domain to use the user entered DNS Domain Name appended to the email address specified in the Domain Contact Email system property.
Default Dynamic Address Pool Alert Threshold	The value, in percent, at which administrators will be alerted that a dynamic address pool (DHCP) is filling up.

Default Host Discovery Ping type	The default 'Ping Host' type initialized when defining a Subnet Hosts Discovery task in the Discover Subnet Hosts screen. <ul style="list-style-type: none"> • Select Ping Only to set as default the option which sends ICMP packet, then only does portscan if reply is received. • Select Ping with TCP port 80 packet to set as default the option that sends ICMP and TCP packet on port 80, then waits for reply.
Default Number of Periods for Pool Regression	The default number of periods (based on Period Type – i.e., “90” Days) that will be used when calculating the pool regression. The number of periods entered will be used for creating the forecasting values for utilization information.
Default Period Type for Pool Regressions	The Period type that will be used to calculate the pool regression. Days, Weeks, Months, or Years.
Domain Contact Email	The Domain contact email address used in the Default Domain Contact system policy.
Enable Block Callout Policy	Governs whether changes to a block are sent to the Callout Manager. The policy is set to False to minimize the amount of unneeded traffic that is sent to the Callout Manager. Set this policy to True if you want changes (add, delete, and modify) to be sent to the Callout Manager.
Field	Description
Enable Device Callout Policy	This policy governs whether changes to a device are sent to the Callout Manager. The policy defaults to False to minimize the amount of traffic that is sent to the Callout Manager. This policy can be set to either IP Address or Device if you want changes (add, delete, and modify) to be sent to the Callout Manager. Setting the policy to IP Address enables an IP Address centric format that is compatible with pre 7.0 versions of IP Control. This format will only display information for a single IP Address. Setting the policy to Device enables a Device centric format that will contain information on all IP Addresses associated with the Device.
Enable Domain Callout Policy	This policy governs if changes to a domain are sent to the "Callout Manager". This is implemented as a policy in order to minimize the amount of unneeded traffic that is sent to the Callout Manager. Set this policy to TRUE if you want changes (add, delete, modify) to be sent to the callout manager.
Enable Task Callout Policy	When set to True, the Callout Manager is notified upon completion of a task (Configuration/Deployment or Discovery/Collectors). The default value is False due to the large overhead that can occur, particularly with DDNS Update tasks.
Enable Workflow Callout Policy	This policy governs if workflow changes are sent to the "Callout Manager". If Workflow is enabled (through Workflow Type System Policy) and the Enable Workflow Callout policy is set to True, pending approval submissions (adds, edits or deletes needing approvals) and approvals or rejections will be sent to the callout manager. Note: If an approving admin updates a resource record that is pending approval or deletes a device or resource record that is pending approval instead of approving or rejecting it, it is not considered a ‘workflow’ operation and as such a Workflow Callout will not be generated.

Enterprise or Service-Provider Constructs	Determines how certain components of the user interface are rendered. Select Enterprise if you are an Enterprise customer, select Service Provider if you are an ISP, Service Provider, or broadband operator.
Executive Copy Method	The protocol used by IPAM Agents to move files back to the Executive. SCP and FTP are the choices. Note: incadmin's \$HOME environment variable must be set to <code>/opt/incontrol/ftproot</code> if the Executive resides on a UNIX platform, when using the SCP copy method. Check <code>/etc/passwd</code> on the Executive to confirm this setting. Note: SCP is not supported by default on Windows systems.
Executive Copy Port	The port number used by IPAM Agents to move files back to the Executive. Typically, 21 for FTP, 22 for SCP.
Executive Copy Username	The user name used by IPAM Agents when moving files back to the Executive.
Executive Copy Password	The password used by IPAM Agents when moving files back to the Executive.
Executive FTP Copy Passive Mode	If the Executive Copy Method is FTP, then this policy can be used to control whether or not the FTP connection from the Agent to the Executive is established using passive mode.
Executive IPv4 Address	The IPv4 Address of the Executive, used by IPAM Agents when moving files.
Executive IPv6 Address	The IPv6 Address of the Executive, used by IPAM Agents when moving files.
Field	Description
External Authentication Script	The full path and name of the external authentication script that is used for authentication of users during login. Refer to “Configuring IPAM to use External Authentication” on page 276. You can override the standard user authentication using this option. For example: <code>C:\perl\bin\perl.exe "C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\test.pl"</code>
File Manager Default Path	The default path for files uploaded to the File Manager.
File Manager FTP Port	The port number used by the File Manager to listen for incoming FTP connections from Agents. The File Manager is not used if the Executive Copy Method is SCP.
File Manager Username	The Username used by remote Agents to log in to the File Manager. Generally you will not need to change this setting.
File Manager Password	The Password used by remote Agents to log in to the File Manager. Generally you will not need to change this setting.
Force Change Password Value	Allows the administrator to set a password that <i>must</i> be changed by the user when they next logon. For example, if this policy is set to <code>changeme</code> , then any user whose password is <code>changeme</code> is required to change it at their next logon. If the policy is blank, users are not affected.

Limit Container Tree Display	<p>Governs the display of containers in the tree display within the Management >Container and Container Maintenance displays, as well as in various Search popup windows.</p> <ul style="list-style-type: none"> • Select Admin Readable to limit the container tree to display only those containers (and its ancestors) to which the current Administrator has at least Read privileges. This is the default behavior. • Select All Containers to allow all Administrators to see all containers in the tree regardless of privileges. However, if an administrator clicks on a container in the tree to which he/she does not have at least Read privilege, an Access Denied message is displayed.
Limit Display of Blocks by Blocktype Access	<p>Governs the display of blocks in various lists based on Blocktype Access Control settings. When set to Yes (the default), blocks of the selected type do not appear in lists when access for an administrator in the Blocktype Access Control tab is turned off.</p> <p>When set to No, blocks of the selected type appear in lists but an administrator may not have Write access.</p> <p>Examples of these block lists are Management > Container View, Management > Subnet/Block View, and various Search lists where only Read access is required.</p>
Maximum records to export from User Interface	<p>Determines the maximum number of records that can be exported through the UIs, such as Audit reports. Care should be taken when changing this setting since the export of records consumes considerable system resource. Export of a very large number of records can result in an out of memory error that requires the web server to be restarted. The threshold at which the error may occur varies by systems but is dependent on the total memory and the system load when the report is run.</p>
Field	Description
Maximum Records to Retain in the "Restore List" Per User	<p>This policy determines the maximum number of entries allowed in the Restore list (Device and Resource records combined) per user. Once this limit is reached, as new items are added to the list, the oldest items will be deleted (First in First Out).</p>
Perform Regression During Global Rollup	<p>Controls whether regression analysis is performed during the global rollup task. The regression analysis includes: 1) Address Pool utilization, 2) Block Utilization (Overall), 3) Dynamic Address Block Utilization, 4) Container Utilization (Overall), 5) Dynamic Address Container Utilization.</p> <p>History records collected during the rollup are used as the input to the regression analysis. The result is a "days left" metric, which indicates how many days the remaining space will last. Since this analysis can slow down the system, you can set this option to False and disable computed metrics, and thereby improve performance.</p>
Polling Interval of Task Manager (seconds)	<p>The number of seconds the task manager will wait between polls to check if any tasks need to be processed. Typically this is set to 15 seconds.</p>
Require SWIP Names to be Unique	<p>When set to true, this policy requires the SWIP name (specific to the ARIN Internet Registry) or the Net Name (specific to RIPE) to be unique within IPAM.</p>

SOA Serial Number Format	<p>Default format for DNS SOA Serial numbers. Numerical format is recommended for dynamic zones.</p> <p>Numerical – Instructs the system to use numeric SOA serial numbers when writing zone files.</p> <p>Date (YYYYMMDDxx) – Uses the date format of YYYYMMDDxx for the SOA number. Note the xx is a numeric sequence number, so if you plan on having more than 99 updates in a single day (or more than 99 dynamic DNS updates), you must use the “Numerical” SOA serial number format.</p>
Task Manager Address	The IP address of the Task Manager module; usually this is the same IP address as that of the IPAM Executive.
Task Manager Port	The port number on which the Task Manager service will listen.
Use View Name with Galaxy Zone Filenames	<p>Set to Yes to append the View name to the end of the Galaxy zone’s filename when it is written to the DNS server, for example:</p> <p>LocationNamedb.domain.com.ViewName</p>
Workflow Type	<p>Master Administrators only. Determines the workflow type. Settings are as follows:</p> <p>None – Workflow is disabled and IPAM works as in previous releases.</p> <p>Resource Records – Enables users to control resource record approvals at the domain level. The Resource Record Approval Access check box is enabled for all administrators on the Domain Access Control tab in Administrator Policies. You can then control access by disabling for specific administrators or by assigning a role in which the right is disabled.</p> <p>Device – Enables users to control device/IP address approvals at the container or block level. The Device Approve Access check box is enabled for all administrators on the Access Control List tab in Administrator Policies. You can then control access by disabling for specific administrators or by assigning a role in which the right is disabled.</p>

Agents

Use the Agents screen to manage the Agents used by IPAM. Agents are used to perform various tasks such as gathering subnet information or statistics, transporting network service configuration, or communicating to network devices to capture configuration information. Agents have direct interaction with DNS servers, DHCP servers, routers, and/or switches.

When you select **Agents** from the SYSTEM section of the **Tools** menu, a list of existing agents is shown in the Agents screen.

To search for a particular agent, enter a search string into the text block and click **Search**.

To delete one or more agents, click the checkbox next to each item you want to delete, and click . At the confirmation prompt, click **OK** to delete the selected agents, or **Cancel** to undo your selections.

To add a new agent, click the **Add Agent** link. The Add Agent screen appears.

Table 7-2 Agent Parameters

Field	Description
IPAM Agent Name	The name of the agent, in either simple or fully-qualified form.
IP Address	The IP address of the agent. This is used by the IPAM Executive to connect to the Agent.

Click **Submit** to add the agent, or **Cancel** to return to the previous screen.

Import Wizard

The Import Wizard allows you to import the following data types into your IPAM database in a four-step process:

- Root Block
- Child Block
- Address Pool
- Device
- Device Resource Record
- Domain
- Domain Resource Record

Note: The size of the import file cannot exceed 2MB.

The four steps are:

1. Select the type of file to import.
2. Select the Comma Separated Value (CSV) or Microsoft Excel Workbook (.xls or .xlsx) file from your local machine and upload it to the IPAM server.
3. Validate the data in the import file.
4. Import the import file data.

To access the Import Wizard, select **Import Wizard** from the SYSTEM section of the **Tools** menu. The IPAM Import Wizard Step 1 screen opens.

Select Import Type

Select Import Type to define the type of data import that you want to perform, as described in

Table 7-3. Refer to the *Cisco Prime Network Registrar IPAM CLI and API Guide* for more details about each import type. When you have selected an **Import Type**, click **Next**.

Table 7-3 Import Types

Import Type	Description
Import Root Block	Allows import of root blocks into IPAM. Attributes for each root block including user defined fields may be specified for each block. For more information, refer to the ImportRootBlock CLI.

Import Type	Description
Import Child Block	Allows import of child blocks into IPAM. Attributes for each child block including user defined fields may be specified for each block. Each child block to be imported must reside within an existing root block defined within IPAM. For more information, refer to the ImportChildBlock CLI. By checking the “Overwrite existing records” box, existing devices can also be modified via the Import Wizard. Refer to the ImportChildBlock CLI –o parameter and the section, “Import with overwrite using expanded format and the !BLANK! keyword”.
Import Address Pool	Allows import of address pools into IPAM. Option and policy sets for each pool may be defined, as well as allow and deny client classes. Address ranges comprising each pool must exist with In-Use/Deployed subnet(s) within IPAM. For more information, refer to the ImportAddrpool CLI.
Import Device	Allows import of IP devices into IPAM. Attributes for each device including user-defined fields may be specified for each device. Each IP address associated with imported devices must exist within In-Use/Deployed subnet(s) within IPAM. For more information, refer to the ImportDevice CLI. By checking the “Overwrite existing records” box, existing devices can also be modified via the Import Wizard. Refer to the ImportDevice CLI –o parameter and the section, “Import with overwrite using expanded format and the !BLANK! keyword”.
Import Device Resource Record	Allows import of IP device resource records into IPAM. Each record must be associated with an existing device in IPAM. For more information, refer to the ImportDeviceResourceRecord CLI.
Import Domain	Enables importing of DNS domains into IPAM. Attributes for each domain including user-defined fields may be specified for each domain. Specified non-default domain types must already exist within IPAM. For more information, refer to the ImportDomain CLI.
Import Domain Resource Record	Allows import of DNS domain resource records into IPAM. Each record must be associated with an existing domain in IPAM. For more information, refer to the ImportDomainResourceRecord CLI.

Select Import File

In Select Import File, you specify which file to use for the import type you selected in Select Import Type.

Note: The required file format for the selected import type is shown, displaying **Column, Field, Accepted Value** and **Required** information in a scrollable section.

To select a file, follow these steps:

1. Type the full path to the file you want to upload, or click **Browse** to locate the file in the file selection window.
2. Click **Upload** to copy your file to the central server.

3. Click **Next** to continue. To return to the previous step, click **Back**.

The file format is validated as it is copied to the server, and the result of the validation is shown in the Validate Import File Data display.

Validate Import File Data

Validate Import File Data displays the results of a spot check of the first record in the selected file to verify that the required fields and submitted data conform to the expectations of the selected import type. Fields that will assume a default value if not specified are so noted.

If validation is successful, the Validate Import File Data screen indicates that there were no detected errors.

If validation is not successful, the Validate Import File Data screen indicates that the file contains errors and indicates where the error occurred.

If validation is successful, click **Next** to continue to **Import Data**. Otherwise, click **Back** so you can open the file and fix errors before you upload the file another time.

Import Data

Import Data appears after successful validation of the selected import type data file has occurred.

You can now decide whether to import the data file immediately, or schedule it to run later.

To select a future date to import the data file, select the **Scheduled** option button. The screen refreshes to show scheduling fields.

Enter the desired date in mm/dd/yyyy format or click the calendar icon to select a date. A calendar is displayed, with today's date selected by default.

You can use the following navigation links to change to another month and/or year and then select a date in the month to close the utility:



Previous Year



Previous Month



Next Year



Next Month

Select the hours, minutes, and AM or PM to schedule a specific time for the task.

Once all scheduling parameters have been entered, click **Done**. A new task is created, and submitted to the system. Once tasks have been created, they can be managed using the **Tasks** option. To view Import Tasks, select from the tasks shown in the **Type** Filters hierarchy:

The results are displayed in the Tasks List.

To review the results of a completed import task, select the **Task ID**. The Task Summary screen opens.

If errors occur during the task execution phase the [Rejects](#) and [Errors](#) links shown in the Task Summary Results table will provide access to the respective rejected records (in CSV format) and associated error messages, as shown below and in Figure 7-14.

Rejects:

??,??,,Owner66,666,IN,A,10.0.0.66,66 IDN Standard,

Errors:

Line 40: Domain not found: Default/??,??: ??,??,,Owner66,666,IN,A,10.0.0.66,66 IDN Standard,

You can copy rejected records to a new file for subsequent editing to correct errors and re-import them.

As with CLI/API transactions, you can review relevant audit records on import wizard activity by reviewing Audit reports for the IP infrastructure type that corresponds to the Import Type. For example, if you are importing Device Resource Records, then run a Resource Record Audit Report and check for entries that correspond to the date you scheduled the import.

Search

The **Search** option allows you to search for the following objects in the IPAM database:

- Individual Objects
- Subnets/Blocks
- DNS Resource Records
- Containers
- Domains

When you select one of these options in the **Search For** field, the screen is updated with the respective search criteria for that selection.

To perform a search, follow these steps.

1. In the **Search For** drop-down list, choose one of the following search types:
 - ▶ **Individual Objects**
 - ▶ **Subnet/Blocks**
 - ▶ **DNS Resource Records**
 - ▶ **Containers**
 - ▶ **Domains**
2. Choose one of the following actions.

If you are searching for ...	Then ...
Individual Object	<ol style="list-style-type: none"> 1. Choose one of the following search criteria: <ul style="list-style-type: none"> ▶ IP Address ▶ Host Name ▶ Hardware Address ▶ User Defined Fields ▶ Specific text in the Description ▶ Shared/Virtual IP ▶ Circuit ID as ASCII ▶ Remote ID as ASCII ▶ Circuit ID as Hex ▶ Remote ID as Hex 2. Select Search ALL Device Types, or refine your search further by choosing a specific Device Type from the drop-down list. 3. Select Search ALL Address Types, or refine your search further by choosing a specific address type from the drop-down list. 4. UDF only. If you selected User Defined Fields in Step 1, select a UDF from the UDF drop-down list. 5. Click Search Container and specify the container in which to search. 6. Enter a string in the Search Value field. 7. For search criteria other than IP Address, choose from the following options: <ul style="list-style-type: none"> ▶ Begins With ▶ Contains ▶ Exact Match

If you are searching for ...	Then ...
Subnet/Block	<ol style="list-style-type: none"> 1. Choose one of the following search criteria: <ul style="list-style-type: none"> ▶ CIDR Address ▶ Specific text in the Name ▶ Specific text in the Description ▶ User Defined Fields ▶ IP Address contained within block 2. Select Search ALL Block Types, or refine your search further by choosing a specific Block Type from the drop-down list. 3. Select Search ALL Block Statuses, or refine your search further by choosing a specific Block Status from the drop-down list. 4. <i>UDF only.</i> If you selected User Defined Fields in Step 1, select a UDF from the UDF drop-down list. 5. Choose one of the following actions: <ul style="list-style-type: none"> ▶ <i>CIDR Address only.</i> Enter a CIDR format address in the Address/Size field. ▶ Enter a string in the Search Value field. 6. For search criteria other than IP Address and CIDR Address, choose from the following options: <ul style="list-style-type: none"> ▶ Begins With ▶ Contains ▶ Exact Match
DNS Resource Record	<ol style="list-style-type: none"> 1. Select Search ALL Resource Record Types, or refine your search further by choosing a specific Resource Record Type from the drop-down list. 2. Limit the search by searching: <ul style="list-style-type: none"> ▶ OWNER field only ▶ RDATA field only ▶ Search Comment field only ▶ OWNER, RDATA and Comment fields 3. Enter a string in the Search Value field. 4. Choose from the following options: <ul style="list-style-type: none"> ▶ Begins With ▶ Contains ▶ Exact Match

If you are searching for ...	Then ...
Container	<ol style="list-style-type: none"> 1. Choose one of the following search criteria: <ul style="list-style-type: none"> ▶ Specific text in the Name ▶ Specific text in the Description ▶ User Defined Fields 2. Select Search ALL Container Types, or refine your search further by choosing Logical or Device container types from the drop-down list. 3. Choose one of the following search options: <ul style="list-style-type: none"> ▶ Begins with ▶ Contains ▶ Exact Match
Domain	<ol style="list-style-type: none"> 1. Choose one of the following search criteria: <ul style="list-style-type: none"> ▶ Select Specific text in the Name or User Defined Fields ▶ Select Search ALL Domain Types, or refine your search further by choosing a domain type ▶ Select Search ALL Forward and Reverse Domains, or refine your search further by choosing Forward Domains, Reverse Domains ▶ Select Search ALL Domain Derivatives, or refine your search further by choosing Standard, Template, Alias ▶ Select Search ALL Managed/Not Managed Domains, or refine your search further by choosing Managed Domains or Not Managed Domains ▶ Select Search ALL Delegated/Not Delegated Domains, or refine your search further by choosing Delegated Domains or Not Delegated Domains 2. Enter a string in the Search Value field. 3. Choose one of the following search options: <ul style="list-style-type: none"> ▶ Begins with ▶ Contains ▶ Exact Match

3. Click **Search**. The system is searched for the specified criteria, and records that match the query are displayed.
4. To start over with different search criteria, click **Reset**.

5. If searching for either Subnets/Blocks or Individual Objects, the search results include an extra toolbar button called “Export for Editing”. Pressing this button will generate a .CSV file that is compatible with the ImportChildBlock or ImportDevice CLIs. The file will then automatically download via the user’s browser.
6. After a search has been run, this search will be remembered as a preference. The next time the advanced search screen is accessed the last search will automatically be run.

Saving Search Criteria

To save time, you can save search criteria and retrieve them or edit them the next time you want to perform a search.

To save a search, follow these steps.

1. Click **Save Search**.
The Save Search Criteria for <searchtype> screen opens.
2. Fill in fields, as described in the following table.

Table 7-4 Save Search Criteria Parameters

Field	Description
Search Name	Enter a unique name for the search.
Description	<i>Optional.</i> Enter text to help identify the search content.
Public Search	Checked indicates that the search is available to all administrators. Unchecked, indicates that the search is restricted to the administrator who created it.

3. Click **Save**.

Loading a Saved Search

To use a saved search, follow these steps.

1. In the Search screen, click **Load Saved Search**.
The Saved Search Filters screen opens.
2. Choose from the following actions.
 - ▶ To check the content of a search filter, click . A Details window opens. Valid filters are indicated by . Invalid filters are indicated by . You cannot use or edit saved searches that contain an invalid filter.
Click anywhere outside the Details screen to close.
 - ▶ To load a search filter, select the search name in the list. The Search Result screen opens.

Editing a Search Filter

To edit a search filter, follow these steps.

1. In the Search window, click **Edit Saved Search**.
The Edit Search Filters screen opens.
2. Choose from the following actions.
 - ▶ To delete a search filter, select the filter to be deleted and click .
 - ▶ To check the content of a search filter, click .
 - ▶ To modify a filter, select it from the **Name** list. The Edit Search screen opens, where you can modify the original filter values and click **Save** to save your changes.

Chapter 8 Working with Blocks and Subnets

Allocation Reason Codes

The Allocation Reason Codes screen allows you to maintain the reason why IP Address allocations are made. **Allocation reasons** enable IPAM administrators to record a reason why additional address space was allocated. Examples might include “Site Growth”, if your company has a site that has outgrown their current address allocation or “Customer Growth” if you are a service provider with clients that periodically request more addresses. Allocation reasons can be tailored to your organization’s particular needs.

Choose from the following actions:

- To search for an allocation reason code, enter a search string into the text block and hit Search.
- To delete one or more allocation reason code, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected reasons, or **Cancel** to undo your selections.
- To add a reason code, click the **Add Reason Code** link. The Add Reason screen appears.

Table 8-1 Allocation Reason Code Parameters

Field	Description
Reason Code	The text of the allocation reason you wish to add.

Click **Submit** to add the allocation reason, or **Cancel** to return to the previous screen.

Block Types

Use the Block Types screen to maintain block types. Use block types to differentiate your IP address space by function or role. For example, you may want to distinguish between blocks based on how they will be used (customer space, internal topology, loopback space, gold level of service space, etc.). This powerful feature enables the IPAM allocation engine to

distinguish between different types of space when performing IP Address space auto allocation. In addition, the use of block types allows administrators to tightly control how the IP Address space is allocated, and where that type of address space can be deployed.

Note: The **Any** block type cannot be deleted.

Choose from the following actions

- To search for a particular block type, enter a search string into the text block and click **Search**.
- To delete one or more block types, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected block types, or **Cancel** to undo your selections. Note that the **Any** block type cannot be deleted.
- To add a block type, click the **Add Block Type** link. The Add Block Type screen appears. Fill in the fields, as described in the following table.

Table 8-2 Add Block Type Parameters

Field	Description
Block Type Name	The name of the block type.
Parent Block Type	A block type can be a child of other block types including Any. A block type with parent block type “None” is not a child to any other block type. When a block type has a parent, during auto allocation the IPAM allocation algorithm will include blocks of its own type, and of its parent type in the result list.
Blocks of this type can be attached to multiple containers	If this box is checked, this block type can be associated with more than one container. This feature allows blocks that are assigned this specific block type to belong to multiple containers. This feature is useful for modeling blocks assigned to multiple physical network devices (that is, routers), such as loopback or point-to-point space.
Include in Regression Analysis	If this box is checked, blocks assigned this block type are included in the regression analysis. For many block types (such as point to point, or loopback), it does not make sense to calculate regression analysis for trending purposes. Because the regression analysis is CPU intensive, in a large deployment it is important to calculate the regression analysis only against blocks that need the trending.
Maintain History Records	If checked, Container History and Block History records will be kept for this block type. The history records are created each time the Global Utilization Rollup task is run.
Blocks of this type can have Shared Interface addresses	If this box is checked, blocks assigned this block type support virtual IP addresses.
Valid Block Sizes	A block type can be constrained to discrete sizes of an address block for block allocation. Select the “Root Block Sizes” link to constrain block sizes for root block allocation for the block type. Select the “Child Block Sizes” link to constrain block sizes for child block allocation for the block type.

Initial Container Rules

The Add Block Type screen also enables you to configure how the new block rules are applied to the existing container hierarchy. The system root container is displayed initially to ensure that the new rules are applied to every container in the system. For this reason, the **Apply to Children** check box is locked.

To modify the rule set for other containers in the hierarchy, click **Add Container(s)**. The Container Search screen opens.

Select containers from the hierarchy and click **Select Container(s)**. The container is added to the Initial Container Rules list where you can modify the rule set for any selected container. You can also select the **Apply to Children** check box for logical containers where you want to propagate their rules to their descendants.

Constraining Block Sizes

To constrain block allocation for the block type to discrete sizes of an address block, select either the **Root Block Sizes** link for root block allocation or **Child Block Size** link for child block allocation. Selecting either link opens the Edit Block Sizes screen.

Select all block sizes allowable for allocation for the block type. All unchecked block sizes will not be allowed for allocation. Use the **IPv4** tab to edit settings for IPv4 block size addressing. Use the **IPv6** tab to edit settings for IPv6 block size addressing. After you have selected the block sizes you want, scroll down and click **Ok**.

Note: Whether or not a block type is allowed, block allocation for a specific size will be determined by examining the block size constraint rules defined at the block type definition and rules defined at the administrator for all roles owned by the user seeking to allocate blocks. See the block type policies **Block Type Size Allocation Rules** for further details on this. Note that if a block type is constrained by a block size at the block type definition, it may not be unconstrained at the administrator role block type policy. Block types may only be further constrained by block size at the administrator role policy level, not the other way around.

Click **Submit** to add the block type, or **Cancel** to return to the previous screen.

Address Pool Allocation Templates

Use the Address Allocation Template List screen to maintain IPv4 and IPv6 address allocation templates. Address allocation templates enable you to define standard policies that govern the allocation of address space or address pools within a subnet. For example, you can create a template that reserves the first address in a subnet for a static router assignment, and then reserves all remaining space for dynamic assignment. When you add an address block (that is, subnet) to a container, you can assign that block an address pool allocation template that ensures not only that address pools and/or individual IP addresses are created,

but also that network services, such as DHCP servers, are assigned. Using templates enables you to plan your space allocations to your network services more efficiently.

Use the Address Allocation Template List screen to:

- Add a new template
- Search for an existing template
- Delete one or more existing templates

Adding a new address allocation template

To add an address allocation template, follow these steps:

1. Click the **Add Address Allocation Template** link. The Add Address Allocation Template screen appears.
2. Enter a name of up to 255 alphanumeric characters in the **Address Allocation Template Name** field.
3. In **IP Version**, click **IPv4** to create an IPv4 address allocation template or click **IPv6** to create an IPv6 address allocation template. When you select IPv6, the column headings change:
4. Select the **Add Address Allocation** link.
If IP Version is set to IPv4, the Add Address Allocation screen is displayed.
If IP Version is set to IPv6, the Add Address Allocation screen is displayed.
5. Refer to Table 8-3 as you define the allocation parameters for the template you are designing.

Table 8-3 Address Allocation Parameters

Field	Description
Object Type	For IPv4 addresses, select either Address Pool or Individual IP Objects. For IPv6 addresses, select from Address Pool, Individual IP Objects, or Prefix Pool. Fields are displayed and enabled/disabled depending on your selection.

Field	Description
Address Type	<p>Select the type of address to be created by the template from the list.</p> <p>IPv4 only</p> <ul style="list-style-type: none"> • Dynamic DHCP – DHCP IP Address with a lease. • Automatic DHCP – DHCP IP Address unlimited lease. • Manual DHCP – DHCP Address assigned to a specific HW Address, unlimited lease. <p>IPv4 and IPv6</p> <ul style="list-style-type: none"> • Static – Statically addressed device. • Reserved – Reserved for future use. <p>IPv6 only</p> <ul style="list-style-type: none"> • Dynamic NA DHCPv6 – Typical DHCPv6 lease types used by most clients. These are non-temporary addresses requested by the client that are leased for a limited amount of time. • Dynamic TA DHCPv6 – Atypical DHCPv6 lease types used by some clients, most often for PPP or dial-up connections. These are temporary addresses requested by the client that are leased for a limited amount of time. • Automatic NA DHCPv6 – Typical DHCPv6 lease types, most often for PPP or dial-up connections. These are non-temporary addresses requested by the client that are leased for an unlimited amount of time. • Automatic TA DHCPv6 – Atypical DHCPv6 lease types. These are temporary addresses requested by the client that are leased for an unlimited amount of time.
Starting Offset	<p><i>All IPv4 object type and IPv6 Individual IP object type only.</i></p> <p>Specify the number of IP addresses you want to offset from beginning or end of the subnet. 0 is only valid for IPv6.</p>
Starting Offset From	<p><i>All IPv4 object type and IPv6 Individual IP object type only.</i></p> <p>Choose whether you want this offset to start from the beginning or the end of the subnet.</p> <p>IPv4 examples:</p> <ol style="list-style-type: none"> 1) For a /24, 1 from the beginning is x.x.x.1 2) For a /24, 1 from the end is x.x.x.254 3) For a /24, if you create a template using the end of the subnet, Starting Offset=>3 from the end, and Ending Offset=>1 from the end, the expected pool is 252-254.
Ending Offset	<p><i>All IPv4 object type and IPv6 Individual IP object type only.</i></p> <p>Specify the number of IP addresses you want to offset from the beginning or end of the subnet. 0 is only valid for IPv6.</p>

Field	Description
Ending Offset From	<p><i>All IPv4 object type and IPv6 Individual IP object type only.</i></p> <p>Choose whether you want this offset to start from the beginning or the end of the subnet.</p> <p>Examples for IPv4:</p> <ol style="list-style-type: none"> 1) For a /24, 1 from the beginning is x.x.x.1 2) For a /24, 1 from the end is x.x.x.254 3) For a /24, if you create a template using the end of the subnet, Starting Offset=>3 from the end, and Ending Offset=>1 from the end, the expected pool is 252-254.
Create Resource Record	<p>Enabled only when Individual IP Objects is selected.</p> <p>Checked indicates that IP Control will create default DNS Resource Records for IP Address(es) when created.</p>
Device Type	<p>Enabled only when Individual IP Objects is selected.</p> <p>Select the default device type for IP Address(es).</p>
Default Gateway(s)	<p>Enabled when the Address Type is Static and Individual IP Objects is selected. When checked, indicates that default gateway address(es) are available on the block. If selected, the Starting Offset From value and Ending Offset From value must be the same. For more information on specifying the default gateway, refer to “Defining a Default Gateway” on page 37.</p>
Pool Size	<p><i>For V6 address pools and prefix pools only.</i></p> <p>Select an IPv6 address pool size from a CIDR/octet boundary of /7 to /128.</p>
Offset	<p><i>For V6 address pools and prefix pools only.</i></p> <p>Specify the offset that determines the multiple of the pool size that the pool should start from. For example, for a /64 pool size, an offset of 0 from start indicates that the pools starts at the starting address of the block, whereas an offset of 1 indicates that the pools will start at the second /64 location in the block.</p>
from start/from end	<p><i>For V6 address pools and prefix pools only.</i></p> <p>Choose whether the offset you specified should be calculated from the start or the end of the block.</p>
Delegated Prefix Length	<p><i>For V6 prefix pools only.</i></p> <p>Specify the default delegated prefix length for the prefix pool.</p>
Shortest Prefix Length	<p><i>For V6 prefix pools only.</i></p> <p>Specify the shortest delegated prefix length allowed for the prefix pool.</p>
Longest Prefix Length	<p><i>For V6 prefix pools only.</i></p> <p>Specify the longest delegated prefix length allowed for the prefix pool.</p>
Overlap Interface IP	<p><i>For V6 address pools and prefix pools only.</i></p> <p>Allow the DHCPv6 pool to overlap an interface address.</p>

6. Once the fields are completed, click **Submit**. The Add Allocation Template screen is updated to display the allocation you just defined and the **Edit** and **Delete** buttons appear.

7. Choose from the following actions.
 - ▶ To make additional allocations within the same template, click the **Add Address Allocation** link and repeat steps 4 and 5.
 - ▶ To delete an allocation, click its **Delete** button. The entry is removed from the template.
 - ▶ To edit an allocation, click its **Edit** button. The Address Allocation screen opens for you to make your changes.
 - ▶ To discard your address allocations and return to the Address Pool Allocation Template List, click **Cancel**.
 - ▶ To save your changes, click **Submit**. The new address allocation template appears in the Address Allocation Template List.

Searching for an address allocation template

To search for a particular address allocation template, follow these steps:

1. Enter a search string in the text block.
2. Click **Search**.

Deleting an existing address allocation template

To delete one or more address allocation templates, follow these steps:

1. Select the checkbox in the Select column beside each template you wish to delete.
2. Click . A dialog opens with the message Are you sure you wish to delete the selected rows?
3. Choose one of the following actions:
 - ▶ Click **OK** to delete the selected allocation templates.
 - ▶ Click **Cancel** to return to the previous screen.
4. The templates are removed and the message Address Pool Template *<template name>* deleted appears.

Site Allocation Templates

The Site Allocation Templates feature allows you to define a site template so that you can allocate multiple address blocks in one step. This is especially useful for larger organizations where a new site may require several subnets. Use the **Site Allocation Templates** option on the **Tools** menu to define a site template, and then invoke the template when creating a site under the **Management > Container View** menu.

Site Allocation Template Functions

You can choose from the following functions:

- Create a new site allocation template. For more information, refer to “Adding a Site Allocation Template” on page 239.
- Modify an existing site allocation template. For more information, refer to “Editing a Site Allocation Template” on page 243.
- Delete a site template. For more information, refer to “Deleting a Site Allocation Template” on page 243.

Site Allocation Template Prerequisites

Before you can manage site allocation templates, the root/aggregate blocks need to be created. For more information, refer to “Add Root Block” on page 25.

Administrators need to have specific Administrator and Container policies set up to use the Site Allocation Template feature.

Administrator Policies

In **Tools > Administrator Roles**, access the Administrator Policies for the administrator role to which you want to grant Site Allocation Template privileges.

- On the **Authorized Functions** tab, ensure that the following checkboxes are selected:
 - ▶ In the System Setup section: **Site Allocation Templates**
 - ▶ In the Management section: **Management Containers** and **Add Sites**
- On the **Access Control List** tab, ensure that Write permission is enabled so that administrators can write blocks to the container.
- On the **Block Type Access** tab, ensure that administrators have access to the block types they will be using in the sites that they create.
- On the **Device Type Access** tab, ensure that administrators have access to the device types they will be using in the sites that they create.
- On the **Domain Access Control** tab, ensure that **Resource Record Write Access** checkbox is selected. This permits administrators to access the domains where resource records are created in any address allocation template in the site template.
- On the **Net Service Access Control** tab, if the **Enable Net Service Access Controls for this Administrator** option button is selected, ensure that the **Write** checkbox is selected for servers in the Net Service Access list.

For more information on administrator roles, refer to “Administrator Role Policies” on page 268.

Container policies

In **Management > Container Maintenance**, access the Edit Container (or Add Child Container) screen for the container where a Site Allocation Template is to be applied.

- On the **Valid Block Types** tab, ensure that selected block types match the block types specified in the Site Allocation Template you want to apply.
- On the **Valid Device Types** tab, ensure that the device types to which you want nested address allocation templates to be applied are selected.
- On the **Allow Allocation from Parent** tab, ensure that selected block types match the block types specified in the Site Allocation Template you want to apply.
- On the **Require SWIP/NetName** tab, select block types for which you want the same requirement in corresponding block types being added in this container by the site template.
- On the **Block Type Information Templates** tab, select UDFs you want entered on the Add Site screen for the Block Types specified in the Site Allocation Template.
- On the **Device Type Information Templates** tab, select UDFs you want entered on the Add Site screen for the Block Types specified in the Site Allocation Template.

Adding a Site Allocation Template

To add a site allocation template, follow these steps:

1. In the SUBNET/BLOCK section of the **Tools** menu, select **Site Allocation Templates**.
The Site Allocation Templates screen opens.
2. Select the **Add Site Allocation Template** link.
The Add Site Allocation Template screen opens.
3. Enter a name for the template in the **Site Allocation Template Name** field.
4. Designate whether the template is for a **Logical** or **Device** container type.
5. Click **Submit**.
The template name is added to the Site Allocation Templates list.
6. Click the Details icon ()
The Details of Site Allocation Template <Name> screen opens.
7. Click the **Add Detail** link.
The Add Site Template Detail screen opens.

Note: If you select **Device** container type, the Block Sequence screen displays an additional parameter, **Interface IP Address**, in the **General** tab.

Note: The allocation column details are dependent on what IP Address Version is selected.

8. Fill out the parameters in the **General** tab, as described in the following table.

Table 8-4 Add Block Parameters

Field	Description
Block Type	Select from the user-defined block types that have been defined in the system. This assigns this block a specific type. The list that is displayed in the block type list is controlled by rules defined in the container maintenance option.
IP Address Version	Select the version of IP Address space that you are adding to the system, IPv4 or IPv6 . Note that the license key controls which versions of IP Address space are supported within the product.
Block Size	Select the block size that you are adding. The block sizes are listed in CIDR notation.
Allocation Strategy	Choose one of the following: <ul style="list-style-type: none"> • To use the automated best fit allocation routine, select the Best fit option. • <i>IPv6 only</i>. To use the automated random allocation routine, select the Random option. • <i>IPv6 only</i>. To use the automated sparse allocation routine, select the Sparse option.
Exclude from Discovery	Select this checkbox if you want this address space to be ignored during the discovery process.
Discovery Agent	Allows you to specify the IPAM Agent to be used to discover hosts on this subnet/block. Choose one of the following: <ul style="list-style-type: none"> • Inherit from Parent Block – Indicates that the agent specified on the parent block is used for discovery. • Inherit from Parent Container – Indicates that the agent specified on the container is used for discovery. • Select Agent – Allows you to select and specify a specific agent that performs discovery for this subnet/block.
Interface IP Address	<p><i>Device Containers only.</i></p> <p>Interface IP Address(es) – Choose the number of IP addresses this block has on this interface. Typically, this is 1. However, there are some high-availability configurations where more than 1 is needed. If you are not sure, leave this at 1.</p> <p>Offset From Start – Specify the number of IP addresses you want to offset from the beginning of the subnet. The Interface Address is the Block Starting address plus this Offset. The default is 1.</p> <p>Default Gateway – Select this option to designate that the Interface IP Address is the default Gateway address.</p>

Field	Description
Block Name	<p>Enter a name for the block. In addition to text, you can use the following tokens that are substituted after a site template is applied to a container:</p> <p>%containername% %parentblocktype% %blocktype% %startaddrstring% %blocksize%</p> <p>For example, the standard CIDR name for a block could be formed using: %startaddrstring%/%blocksize%</p> <p>Note: The block name appears on the container screen.</p>
Block Description	Enter a description of the block. In addition to text, you can use the tokens listed above.
Current Status	<p>The current status of this block. Choose one of the following:</p> <ul style="list-style-type: none"> • Aggregate – This block is an aggregate block. • In-Use/Deployed – The block is in use as a subnet. • In-Use/Fully Assigned – The block is in use and all IP Addresses are fully utilized. • Reserved – This block is reserved for future use.
Primary Subnet	Select this check box if the subnet you are creating should be the primary subnet. Otherwise, leave blank.
Non-Broadcast	<p>When True, indicates that this block is not in a broadcast domain. As such the subnet and broadcast addresses (i.e., the first and last address in the block) are available for assignment. Typically this flag is set to False.</p> <p>This flag is only valid for IPv4 In Use/Deployed blocks.</p>
Create Reverse DNS Domain(s)	<p>When checked, the system automatically creates an in-addr.arpa or ip6.arpa reverse domain for this address space. You may optionally select the “type” if you have overlapping address space. DNS Domain Type values are defined within the System tab of the system.</p> <p>Note: This option only creates the reverse domain. You must still assign this domain to a DNS server or a DNS galaxy.</p>
Allocation Template	Select the allocation template to be used with the site allocation template. The allocation name and rules appear.

9. Select the **Policies** tab.

10. Fill out the parameters, as described in the following table:

Table 8-5 Add Block Sequence Policies Parameters

Field	Description
Primary DHCP Server	Select the Primary DHCP server that serves this address space from the drop-down list.
Failover DHCP Server	Select the Failover DHCP server that serves this address space from the drop-down list.

Field	Description
Primary WINS Server	Enter the IP address of the Primary WINS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. You may specify multiple IP addresses by typing them in a comma-separated format, for example: 192.168.1.1,192.168.1.2
DHCP Policy Set	Select the default DHCP Policy set to assign to dynamic devices on this subnet from the drop-down list.
DHCP Options Set	Select the default DHCP Option set to assign to dynamic devices on this subnet.
Forward Domains	Select the default DNS Forward domains for this subnet. These appear in the drop-down list when defining devices. If multiple domains are specified, then the default (indicated by an arrow) that is used when adding objects is the first one in the list. For more information on adding a forward domain, refer to “Searching for a Domain or a DNS Server.”
Reverse Domains	<i>Optional.</i> Select the default DNS Reverse domains for this subnet. This domain is used to hold DNS PTR records. If multiple domains are specified, then the default (indicated by an arrow) for adding objects is the first one in the list. If no default is specified, the system automatically calculates the correct reverse zone for DNS PTR records. For more information on adding a reverse domain, refer to “Searching for a Domain or a DNS Server.”
DNS Servers	Select the default DNS Servers for this subnet. Used to provide this information to DHCP for Dynamic Address types. If multiple DNS servers are specified, then the default that is used when adding objects is the first one in the list (an arrow appears next to the default). For more information on adding a DNS Server, refer to “Searching for a Domain or a DNS Server.”

11. Click **Submit**.

The block is added to the Add Site Allocation Template list.

12. Choose from the following actions:

- ▶ To add another block, click **Add Detail** and refer to step 5 above.

- ▶ To save the template, click **Save**.

The message

Successfully saved Site Allocation Template:

<templatename>

appears, and the template is added to the list in the Details of Site

Allocation Template <Name> screen.

For information on invoking the template to create a site under the **Management > Management Containers** menu, refer to “Add Site” on page 27 (for Logical Containers) or “Add Site” on page 35 (for Device Containers).

Searching for a Domain or a DNS Server

To search for a domain or a DNS server in the **Policies** tab, follow these steps:

1. Click **Add Domains** or **Add DNS Server**.
2. Enter search criteria or leave blank to return all domains or all servers.
3. Click **Search**.
4. Select the **Add** check box beside each domain or server you want.
5. Click **Submit**.

The domain or DNS servers you selected appear in the **Policies** tab. If you selected more than one domain or server:

- ▶ To change the default, use the **Up** or **Down** buttons.
- ▶ To remove an entry altogether, click **Delete** beside the entry you no longer want.

Editing a Site Allocation Template

You can modify a site allocation template that no longer suits your original design. You can change the name, add new blocks, or modify and/or delete existing blocks. You cannot change the container type.

Note: Blocks already created using a specific site template will not change. Only new block allocations are affected by changes you make when you edit a site allocation template.

To edit a site allocation template, follow these steps:

1. Select the site template in the **Name** column that you want to modify.
The Edit Site Allocation Template screen opens.
2. Choose from the following actions:
 - ▶ To add another block, select **Edit Details**, and follow the instructions in “Adding a Site Allocation Template” on page 239.
 - ▶ To modify an existing block, click  beside the block you want to change. Follow the instructions in “Adding a Site Allocation Template” on page 239.
 - ▶ To delete an existing block, click the checkbox beside the block you no longer want and click . A dialog opens with the message
Are you sure you wish to delete the selected rows?
Click **OK** to confirm.
3. Click **Submit** to save your changes.
4. Click  to return to the list of site allocation templates.

Deleting a Site Allocation Template

You can delete a site allocation template that you no longer need.

Note: Blocks already created using a specific site template will not be deleted.

Follow these steps:

1. Select the check box next to the site template in **Name** column that you want to delete.
2. Click .

The message *Are you sure?* appears.
3. Click **OK**.

The site template is removed from the Site Template Name column.

RIR Organization IDs

This section describes the setup and maintenance of Regional Internet Registry Organizations. RIR Organizations are used to organize and define information that is associated to your address space. This includes information that is needed and/or required for reporting purposes by internet registries such as ARIN or RIPE. When an organization gets a new allocation of IP Address space from an Regional Internet Registry (RIR), the address space is essentially registered to that organization. The RIR assigns an identification number to each organization, which is sometimes referred to as an Organization ID (OrgID) or “organization”. This OrgID needs to be associated with the root block and all subsequent descendant blocks to facilitate tracking and proper utilization reporting. For instance, showing utilization by OrgID helps an organization when it becomes time to request more space from the RIR.

When the Regional Internet Registry Organizations icon or link is selected, the existing Organizations, if any, are shown.

Choose from the following actions.

- To delete one or more organizations, click the checkbox in the Select column for each item you wish to clear, and click . You are prompted for confirmation. Click **OK** to delete the selected Organizations, or cancel to return to the previous screen.
- To add a new Organization, click the **Add Organization** link. The Add Organization screen appears.

Table 8-6 Add Organization Parameters

Field Name	Usage
Organization Name	The name of this organization. The organization (or division within an organization) who manages the network.
Organization ID	(OrgID) A unique identifier of an organization.
Registry	Select the internet registry that this Organization will apply to.
Description	Enter a free text description for this Organization.
Address	Enter the address information for this Organization.
City	Enter the city of this Organization.
State/Province	Enter the state/province of this Organization.

Field Name	Usage
Postal Code	Enter the postal code for this Organization.
Country Code	Enter the country code for this Organization.
Admin Contact	Enter the administrative contact information for this Organization.
Tech Contact	Enter the technical contact information for this Organization.
Authorization Type	When submitting an update that requires authorization, authentication information valid for this organization should be supplied. Different methods require different authentication information. Refer to the Internet Registry Documentation for additional details.
Password	Required for an Authentication Type of MD5-PW.
Confirm Password	Required for an Authentication Type of MD5-PW.
Email Update to	Email address to send updates that occur to blocks assigned to this organization.
Notify Email to	Notify email address to send updates that occur to blocks assigned to this organization.

Fill in the fields with the desired values, and click **Submit** to store the definition, or click **Cancel** to return to the previous screen.

This page intentionally left blank.

Chapter 9 Working with IP/Devices

Vendor/Models

Use the Vendor List screen to maintain the list of networking equipment vendors and their models. This section is divided into two parts: Vendor Maintenance and Model Maintenance. Vendors are maintained in the Vendor List, while types and models of equipment are maintained by selecting a specific vendor.

Vendor Maintenance

When you first choose **Vendor/Models** from the **Tools** menu, you are presented with a list of the vendors in the system.

You can see at a glance which types of equipment you have that are associated with this vendor. In the figure above, for example, 3Com has one or more CMTSs associated with it, and no routers, VPN gateways, or network switches. The same applies to ADC and Arris.

Choose from the following actions:

- To search for a particular vendor, enter a search string into the text block and click **Search**.
- To delete one or more vendors, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected vendors.

Note: When you delete a vendor, all models associated with the vendor are also deleted.

Adding a Vendor

To add a vendor, follow these steps.

1. Click the **Add Vendor** link.
The Add Vendor screen opens.
2. In Vendor Name, enter the equipment manufacturer.
3. Click **Submit** to add the vendor.

The vendor is added to the **Vendor Name** list, where you can add the models that should be associated with it.

Model Maintenance

Models of equipment are related to vendors.

Adding a Model

To add an equipment model associated with a vendor, follow these steps:

1. In the **Vendor Name** list, click  beside the vendor for which you want to add equipment.

The Models of Vendor <name> screen opens.

2. Click **Add Model**.

The Add Model screen opens.

3. Select a **Device Type** from the list of previously defined device types.

4. In **Model Name**, enter a name for the model.

5. Click **Submit** to add the device

The new model appears in the Models of Vendor <name> screen.

6. Click  to return to the list of vendors, where the device type of the model you added is indicated by a checkmark.

Modifying a Model

To modify a model in the model list, follow these steps:

1. In the Model of Vendor <name> screen, click the name of the model.

The Edit Model screen appears.

2. Modify the model name and device type as desired.

3. Click **Submit**.

Deleting a Model

To delete one or more models in the model list, follow these steps:

1. In the Model of Vendor <name> screen, select the checkbox beside each model you want to delete.

2. Click .

You are prompted for confirmation.

3. Click **OK** to delete the selected model.

Device Types

Use this screen to maintain Device Types. Use **Device Types** to differentiate your individual IP addresses by function, type, or role. For example, you may want to distinguish between printers, routers, or standard laptops. This powerful feature enables the IPAM

engine to distinguish between different types of devices when creating default host names, displaying user defined fields, and for reporting purposes. In addition, the use of device types allows administrators to tightly control how the IP Address space is allocated, and where that type of device can be deployed.

Choose from the following actions:

- To add a device type, refer to “Adding a Device Type”.
- To refresh the display, click .
- To modify a device type, select its name in the **Device Type Name** list and modify fields as needed.
- To delete one or more device types, click the checkbox next to each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected device types.

Adding a Device Type

To add a device type, follow these steps.

1. Click the **Add Device Type** link.
The Add Device Type screen appears.
2. Enter values in the fields, as described in the following table.

Table 9-1 Device Type Parameters

Field	Description
Name	The name of the device type. This name appears in drop-down lists and on reports.
Description	An optional description that describes the device type.
Ignore devices of this type for Subnet Reclaim	When checked, devices defined with this Device type will be overlooked during a Subnet Reclaim.

3. Click **Submit** to add the device type.

Naming Policies

Use the Device Naming Policies screen to maintain Device Type Naming Policies. These policies allow you to standardize device names within your organization based on the device type. Using naming policies allows you to ensure unique host names for devices throughout your network. This is important if you are using DNS to help resolve the name to IP Address for your devices. A unique naming policy can optionally be assigned to each device type. When you create a device (by allocating an IP Address), IP Control can auto-generate the next available host name based on the naming policies you have established.

When you select **Naming Policies** from the IP/DEVICES section of the **Tools** menu, the existing device types and associated Naming Policy, if any, are displayed.

All device types are listed in this display. The **Example** column shows the currently defined naming policy.

Choose from the following actions.

- To edit a naming policy for a device type, refer to “Editing a Naming Policy for a Device Type”.
- To delete a naming policy so you can create a new one, click the checkbox next to the device type you want to clear, and click . Click **OK** to confirm the deletion.

Editing a Naming Policy for a Device Type

A naming policy is usually a combination of static text, mixed with dynamic (system generated) components. The dynamic components ensure uniqueness of the host name.

To edit a naming policy for a device type, follow these steps.

1. In the **Device Type** column, select the device type for which you want to edit a naming policy. The Edit Naming Policy screen opens.
2. You build up a naming policy by adding several components together. Choose from the following actions.
 - ▶ Click **Delete** on a line to remove a specific component of a naming policy.
 - ▶ Click **Insert Row Above** to insert a new component of a naming policy above the current line.
 - ▶ Click **Insert Row Below** to insert a new component of a naming policy below the current line.
 - ▶ Click **Append Policy** to add a naming policy at the end of existing components.
3. Add or modify components by selecting from the following parameter list.

Table 9-2 Device Naming Policy Parameters

Field	Description
Container Name	Displays the name of the container. The container name is used during the generation of the policy.
Free Text	Static text that is used during the generation of the policy.
IPv4 – Zero Filled	A dynamically generated component that is the IPv4 Address of a fixed sized, padded with zeros, without the dotted decimal notation. For example; 10.0.0.3 would generate the string 010000000003 198.200.121.2 would generate the string 198200121002

Field	Description
IPv4 – Dash Separated	A dynamically generated component that is the IPv4 Address, with dashes instead of dotted decimal notation. For example; 10.0.0.3 would generate the string 10-0-0-3 198.200.121.2 would generate the string 198-200-121-2
Incrementor	A dynamically generated global incrementor specifically unique for this naming policy. Each time this policy is used, a unique number will be generated.
Incrementor – Zero Filled	A dynamically generated global incrementor specifically unique for this naming policy. Each time this policy is used, a unique number is generated. This field is padded to a fixed size of 5 characters. For example; 12 generates the string 00012 1232 generates the string 01232

- Click **Submit** to save the naming policy.
The modified naming policy is displayed in the **Example** column.

Device Interface Template Maintenance

The Device Interface Templates List screen allows you to maintain device interface templates. A device interface template enables the IPAM administrator to define standard equipment interface configurations, and then duplicate those interface configurations easily across multiple devices (“Network Elements/Devices” on page 82) in IPAM.

To access the Device Interface Template List, select **Interface Templates** from the IP/DEVICES section of the **Tools** menu. The Device Interface Templates List screen opens.

Choose from the following actions:

- To search for a particular device template, enter a search string into the text block and hit Search.
- To delete one or more device templates, click the checkbox next to each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected device templates.
- To add a device template, refer to next section.
- To edit a device template, refer to “Editing a Device Interface Template” below.

Adding a Device Interface Template

To add a device interface template, follow these steps.

- Click the **Add Device Template** link. The Add Device Template screen opens.
- In **Template Name**, enter the desired template name.

3. Click on **Append Interface** to add an interface to the template.
4. In **Interface 1**, enter a unique name to the interface.
5. To add more interfaces, choose from the following actions.
 - ▶ Click **Insert Row Above** to add a row above.
 - ▶ Click **Insert Row Below** to add a row below.
 - ▶ Click **Delete** to remove an interface,
6. Click **Submit** to save your changes.

Editing a Device Interface Template

To modify an existing device interface template, click on a template name in the **Template Name** list. The Edit Device Interface Template screen opens.

Edit the template fields as needed. You can change the name of the template in the **Template Name** field, or add and remove interfaces using the **Delete** or **Insert Row** buttons. Click **Submit** to save your changes.

Chapter 10 Using Other Tools

Threshold Sets

Thresholds and Threshold Sets alert administrators when a particular condition occurs within IPAM. For example, you can configure IPAM to alert an administrator when the allocated IP addresses in a block exceed 90% of its capacity.

To use this feature, there are three steps:

1. Define a Threshold Set.
2. Add one or more thresholds to the Threshold Set.
3. Associate a Threshold Set with a container/block type pair, a block, or a network service. This section describes steps 1 and 2. Refer to “Block Threshold Alert” on page 255 for instructions on Step 3.

Creating a Threshold Set

To add a threshold set, click the **Add Threshold Set** link. The Create Threshold Set screen opens, as shown.

In **Set Name**, enter the desired name and click **Submit**. The new Threshold Set is added to the **Set Name** list, where you can choose from the following actions.

- To add a threshold to a Threshold Set or modify a Threshold Set name, refer to “Adding a Threshold to a Threshold Set”.
- To delete a threshold set, select the checkbox next to the item you want to remove and click . You are prompted for confirmation. Click **OK** to delete the selected Threshold Set..

Adding a Threshold to a Threshold Set

After you have created a Threshold Set, you need to add individual Thresholds. Follow these steps:

1. Click on a **Set Name** link to display the **Edit Threshold Set** screen.
2. Click on **Add Threshold**. The Create Threshold screen opens.
3. Make your field selections, as described in Table 10-1.

Table 10-1 Create Threshold Parameters

Field Name	Usage
Severity	Choose one of Critical , Warn , or Info to indicate the importance of this condition.
Variable	Choose one of the following: <ul style="list-style-type: none"> • Allocated, Assigned, and Available refer to the number of IP addresses in those categories in a block or address pool. • Days Left refers to the calculated time remaining before the block or address pool runs out of space. • Dynamic Available refers to the number of dynamic IP addresses that are available. • Dynamic Days left refers to the calculated time remaining before the block or address pool runs out of dynamic space.
Type	Choose one of Percent or Absolute . This tells IPAM how to interpret the Value field.
Comparator	Choose one of > , >= , = , < , <= . This specifies the comparison between Variable and Value that triggers the Threshold.
Value	Enter the value that triggers the Threshold. If the Type is Percent , enter a value between 1 and 100.
Confidence	Specify a number between 0.0 and 1.0. This only applies when the Variable is Days Left . It specifies that the threshold is crossed <i>only</i> if the comparison of Days Left and Value is true <i>and</i> the confidence calculated (R2 or R-Squared) for Days Left is greater than this number.

4. Click **Submit** to add the threshold to the Threshold Set.
5. Choose from the following actions:
 - ▶ To edit a threshold, click the **Edit** button beside the threshold you want to edit.
 - ▶ To delete a threshold, click the **Delete** button beside the threshold you want to delete. At the confirmation prompt, click **OK**.
 - ▶ To return to the Threshold Set page, click **Cancel**.

Block Threshold Alerts

Use the Block Threshold Alerts screen to enable a block alert. An alert is raised when the total space for a given block triggers the conditions in the Threshold Set. Refer to “Threshold Set” on page 253 for instructions on defining Threshold Sets and Thresholds. Refer to “Alert Log” on page 209 for instructions on viewing pending alerts.

To access Block Threshold Alerts, select **Block Threshold Alerts** from the OTHER section of the **Tools** menu. The Block Threshold Alerts screen opens.

Choose from the following actions.

- To add a block threshold alert, refer to “Setting Up a Block Threshold Alert”.
- To remove an existing alert, select the checkbox next to the alert you no longer need and click . You are prompted for confirmation. Click **OK** to delete the selected alert.

Setting Up a Block Threshold Alert

When an Alert is defined for a Block, an alert is raised when the variables in that Block trigger the conditions in an associated Threshold Set.

To set up a block threshold alert, follow these steps.

1. In the Block Threshold Alerts screen, click **Add Alert**.
The Add Block Threshold Alert screen opens.
2. Select a threshold set from the **Threshold Set** list.
3. Select the checkbox beside the block in the block hierarchy to which you want to assign the selected threshold set. Expand the hierarchy as needed to locate a specific block.
3. Click **Submit**.
The selected block appears in the **Block** list.

Container Threshold Alerts

Use the Container Threshold Alerts screen to enable Container alerts. An alert is raised when the total space for a given container triggers the conditions in the Threshold Set. Refer to “Threshold Set” on page 253 for instructions on defining Threshold Sets and Thresholds. Refer to “Alert Log” on page 209 for instructions on viewing pending alerts.

To access Container Threshold Alerts, select **Container Threshold Alerts** from the OTHER section of the **Tools** menu. The Container Threshold Alerts screen opens.

Choose from the following actions.

- To add a container threshold alert, refer to “Setting Up a Container Threshold Alert”.

- To remove an existing alert, select the checkbox next to the alert you no longer need and click . You are prompted for confirmation. Click **OK** to delete the selected alert.

Setting Up a Container Threshold Alert

To set up a Container Alert, follow these steps.

1. Click on the **Add Alert** link. The Add Container Threshold Alert screen opens.
2. Check the **Apply to Children** box if you wish the alert to apply to the container and all its children. Leave it unchecked to have it apply only to the container.
3. Select the **IP Address Version** to which the threshold set applies.
4. Select the **Block Type** to which the threshold set applies.

Note: **Any** is a Block Type of its own, and does *not* mean that all Block Types are included.

5. Select the checkbox beside the container in the hierarchy to which you want to assign the selected threshold set. Expand the hierarchy as needed to locate a specific container.
6. Click **Submit**.
The container with the threshold alert appears in the **Container Name** list.

Network Services Threshold Alerts

Use the Network Services Threshold Alerts screen to enable Network Service alerts. An alert is raised when any of the address pools managed by that Network Service triggers the conditions in the Threshold Set. If there are shared address pools, they are aggregated before testing the threshold. Refer to “Threshold Set” on page 253 for instructions on defining Threshold Sets and Thresholds. Refer to “Alert Log” on page 209 for instructions on viewing pending alerts.

To access Network Services Threshold Alerts, select **Network Services Threshold Alerts** from the OTHER section of the **Tools** menu. The Network Services Threshold Alerts screen opens.

Choose from the following actions.

- To add a network services threshold alert, refer to “Setting Up a Network Service Alert”.
- To remove an existing alert, select the checkbox next to the alert you no longer need and click . You are prompted for confirmation. Click **OK** to delete the selected alert.

Setting Up a Network Service Alert

To set up a Network Service threshold alert, follow these steps.

1. In the Network Services Threshold Alerts screen, click **Add Alert**.
The Add DHCP Network Services Alert screen opens.
2. In **Threshold Set**, choose a threshold set from the list.
3. Select the checkbox beside the **Network Service** in the list to which you want to assign the threshold set you have selected.
4. Click **Submit**.
The threshold alert is added to the **Network Service** list.

User-Defined Fields

User-Defined fields enable users to attach arbitrary data elements to containers, subnets, and IP addresses. For example, you can define a field called Customer ID to track blocks allocated to a particular customer, or a field called Asset Tag to track asset information about a specific device using an IP address.

There are three steps to defining user-defined fields and attaching them to subnets or IP addresses:

1. Create the user-defined field.
2. Create the Information Template and select the desired user-defined fields.
3. Attach the Information Template to a Container-Block (Subnet) pair, or a Container-IP Address (via Device Type) pair.

To access the User-Defined Field list, select **User Defined Fields** from the OTHER section of the **Tools** menu.

Adding a User-Defined Field

To add a user-defined field, follow these steps.

1. Click on **Add User-Defined Field**.
The Add User-Defined Field screen opens.
2. Fill in the fields with the desired values, as described in Table 10-2.

Table 10-2 Add User-Defined Field Parameters

Field Name	Usage
Display Title	The label displayed on input forms for this field.
Field Name/Tag	The name of this field. This name must be unique from other User-Defined Fields and must follow the XML naming rules: <ul style="list-style-type: none"> • Names can contain letters, numbers, and other characters • Names cannot start with a number or punctuation character • Names cannot start with the letters xml (or XML, or Xml, etc) • Names cannot contain spaces • Any name can be used, no words are reserved
Value Data Type	Controls how the data element is displayed on input forms. Choose one of Text, Checkbox, Radio Button, Text area, List, Hidden, or URL .
Default Value	Choose the default value for this field if the user does not supply one on an input form. Note: This field is required if the Read-Only option is selected, or if the Data Type is Hidden.

Field Name	Usage
URL Template	<p>Only visible if Data Type is URL. Enter the URL that will be used to call a different web screen. You may use FIELD TOKENS to represent the data of other fields on the screen. For example:</p> <pre>%custid%</pre> <p>Valid field tokens include:</p> <ul style="list-style-type: none"> • Device Level Tokens: hostname, description, fqdn, hwaddr, deviceTypeString, hostOperatingSystem, domainName, ipaddress <p>Note: All user-defined fields using the “Field name/Tag”</p> <ul style="list-style-type: none"> • Block Level Tokens: name, blockstatus, blocksize, blocksizehosts, rootblock, rootblocktype, privateaddrspace, startaddrstring, servicetype, swipname <p>Note: All user defined fields using the “Field name/Tag”</p> <ul style="list-style-type: none"> • Container Level Tokens: name, type, notes, createAdmin, createdate <p>Note: All user defined fields using the “Field name/Tag”</p>
Read Only	<p>Check this box for a read-only field.</p> <p>Note: The Default value is required for this option.</p>
Required	<p>Check this box if the field cannot be left blank.</p>

3. If you have already defined some information templates, select the checkbox next to the template with which you want to associate the UDF. For more information on information templates, refer to “Information Template” on page 260.
4. Click **Submit** to save the definition.

Creating Radio Button and List Values

If you choose a **Value Data Type** of Radio Button or List, you must provide a list of acceptable values for the field in the Define Options for Radio Button or Define Options for List Box screen.

Follow these steps.

1. In **Label**, enter the form label for one of the allowed values.
2. In **Value**, enter its associated value. The contents of **Value** is what is actually saved when a Block is saved. The "Value" should be a unique value (case insensitive) that identifies the label.
3. Click **Add new option** to add the Label-Value pair to the acceptable values for this field. It appears in the list below.
4. Choose one of the following actions.
 - ▶ To add additional options, repeat the process.
 - ▶ To change the label sequence, check the **Select** option for that row, and click **Up** to move a label up the list or **Down** to move a label down the list.

- ▶ To edit existing options, change the contents of the **Label** or **Value** fields on the desired row.
 - ▶ To delete an option, check the **Select** option for that row, and click **Delete**.
5. To save the additions, changes, and deletions, click **Save**.

Information Templates

Information templates are groups of user-defined fields. A user-defined field can only be associated with a block through an information template.

To access the information templates, select **Information Templates** from the OTHER section of the **Tools** menu.

Adding an Information Template

To add an information template, follow these steps.

1. Click the **Add Information Template** link. The Add Information Template screen opens.
2. In **Information Template Name**, enter a name.
3. To attach a user defined field to the template, click **Append User Defined Field**. The Append UDFs (User Defined Fields) to Information Template screen opens.
4. Select the checkbox next to the fields to append to the template.
5. Scroll down and click **Submit**. The Add Information Template opens.
6. Choose how the UDFs are displayed, as described in Table 10-3.

Table 10-3 Add Information Template Parameters

Field Name	Usage
Field Name	The name of the user-defined field.
List Display?	Determines whether this user-defined field is displayed on main-level lists, such as the block list in the Management Containers screen, or the subnet list when viewing individual IP addresses.
Sequencing	Use the Up and Down buttons to arrange the order in which user-defined fields are displayed on the screen. Use the Delete button to remove a UDF entry from a template.

7. Click **Submit** to save the new template. The template is added to the **Information Template Name** list.

After you have saved the new template, you can activate it by choosing the template in the Edit Container screen (**Container Maintenance** in the IPAM section of the **Management**

menu). There, you can choose a template to be associated with a given block type within that container.

Refer to “Rules Tabs” on page 79 for further information. The next time you create or edit a block of that type in that container, the user-defined fields appear on the input form.

IDN Converter

Internationalized Domain Names use characters drawn from a large repertoire (Unicode). IDNA (Internationalized Domain Names for Applications) as described in RFC 3490 allows the non-ASCII characters to be represented using only the ASCII characters already allowed in so-called host names today. This backward-compatible representation is required in existing protocols like DNS, so that IDNs can be introduced with no changes to the existing infrastructure.

IDNA is only meant for processing domain names, not other text.

IPAM supports IDNA as defined in RFC 3490. It allows for data to be entered using Unicode characters and ASCII characters both when entering domain names. IPAM also gives the users the ability to switch between IDN and ASCII when viewing the data. The underlying data is always stored as ASCII or ASCII Compatible encoding (ACE).

For example, for Internationalized Domain name ‘bücher.com’, the ACE equivalent is ‘xn--bcher-kva’.

UI Treatment

Screens involving domain names, FQDNs and hostnames in case of domains/zones and owner and RDATA fields in case of resource records get special treatment for IDN support.

If an internationalized domain name is entered, hover the cursor over the IDN (Unicode character set) to see the ACE equivalent.

Whenever an Internationalized Domain Name is displayed, a  icon is visible. Additionally,  is displayed on the **DNS Domain** tab, where you can choose to have the name displayed in ACE or IDN format.

Converting a Domain Name to IDN

To access the IDN Converter, select **IDN Converter** from the OTHER section of the **Tools** menu. The IDN Converter screen opens.

To convert a domain name to IDN, follow these steps.

1. Enter the domain you want to convert.
2. Choose one of the following actions.
 - ▶ Click **To IDN** to review the name converted to IDN format.
 - ▶ Click **To ACE** to review the name converted to ACE format.

The converted domain name is displayed.

Search and IDN

Domain and resource record searches in IPAM are performed using the ASCII representations. If you have Internationalized Domain Names, put full IDN domain name or full/partial ASCII domain name in the search box to get back the desired result. Partial IDN search will not work.

For example, to search domain “bücher.com”, you may enter “bücher.com” or “xn--bcher-kva” (ASCII Compatible representation) or any part of the ASCII compatible name (for example, "bch") and get back the desired result.

However, putting “büc” does not return the domain “bücher.com” since the searches are performed using the ASCII equivalent.

Chapter 11 Managing Administrators

Administrator Definition

Use the Administrator List screen to maintain IPAM administrators. Administrators have their own login credentials, and are assigned to specific Administrator Roles which control access to the system components.

To access the Administrator List, select **Administrator Definition** from the ADMINISTRATORS section of the **Tools** menu. The Administrator List screen opens.

Choose from the following actions:

- To add an administrator, refer to “Adding an Administrator”.
- To search for a particular administrator, type a search string in the text block and click **Search**.
- To create copies of one or more administrators, select the checkbox next to each administrator you want to copy, and click . A copy of each selected administrator will be created, with the name “Copy of *loginId*”. If multiple copies of an administrator are created, each will be named with a sequence number, for example, “Copy(2) of *loginId*”. The new administrator will have the same attributes and policies as the selected administrator. The password will be set to the loginId.
- To delete one or more administrators, click the checkbox in the Select column for each item you wish to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected administrators, or **Cancel** to return to the Administrator List screen.

Adding an Administrator

To add an administrator, follow these steps.

1. Click **Add Administrator**,
The Add Administrator screen opens.
2. Enter a Login ID and a Password,
3. Verify the password and enter information in other fields as needed.
4. Click **Add Administrator Role** to select a role for the administrator.

Table 11-1 Add Administrator Parameters

Field	Description
Login ID	Required. New administrator's login ID (for example, jsmith).
Password	Required. New administrator's password.
Verify Password	Required. Re-enter the new administrator's password for verification purposes.
First Name	First (given) name of new administrator.
Last Name	Last (family) name of new administrator.
Address	Mailing address of new administrator.
Email	Email address of new administrator (for example, juser@example.com).
Phone	Phone number of new administrator.
Pager	Pager number of new administrator.
Fax	Fax number of new administrator.
Authorize Externally	Disabled when Administrator Type is set to MASTER. When this administrator logs in, use the external authorization callout for authentication purposes. This feature allows you to use corporate-wide authentication, such as LDAP, RADIUS, or TACACS.
Enabled	Determines whether the user can access the IPAM system.
Administrator Type	Choose from MASTER, NORMAL, or READONLY. <ul style="list-style-type: none"> • MASTER users have full control over the entire IPAM system. • NORMAL users have ordinary read-write permissions, and may be restricted to working with only certain portions of the IPAM system. • READONLY users have read-only access to IPAM, and may be restricted to seeing only certain portions of the IPAM system.
Role	Click Add Administrator Role and select an Administrator Role from the roles that you have previously defined. Note: You can select more than one role.
Assignable Role	Select the Administrator Assignable Role from the roles that you have defined. Assignable Roles are roles that the administrator you are creating can assign to another administrator if they have Superuser privileges. <p>Note: Only administrators with Superuser privileges can administer Assignable Roles.</p>
Last Modified on	Displays the last date and time this administrator's record was modified.

5. Click **OK** to save your changes.

The new administrator appears in the administrator list.

Assignable Roles

The basic premise is that a Superuser creates all the roles in the system and grants authority to another administrator to assign all or a subset of these roles to other administrators. An

administrator can have zero to many roles *assignable* to another administrator. Administrators without Superuser privileges cannot assign a role to themselves.

Administrator-specific Policies

Policies for an administrator are set using the **Policies** link in the Administrator List screen. The Administrator Policies screen opens.

The Administrator Policies screen works exactly as described in “Administrator Role Policies” on page 268. The only difference is that the policies set are assigned only to the Administrator being modified.

Note: It is important to note that the Administrator-specific policies are combined with the policies defined for all of the Administrator Roles to which the Administrator is assigned.

Determining Effective Rights for an Administrator

When an Administrator is assigned to multiple roles or is assigned to a single role but has Administrator-specific policies defined it may not be apparent as to what the effective rights or policies are applied to the given Administrator. This section explains how these “effective” rights are computed.

When reading the descriptions, keep in mind that the Administrator-specific Policies are treated the same as the policies defined for a defined Administrator Role.

The general rule of thumb is that if the access right is “on” for any of the roles assigned to an Administrator, then the policy is considered “on” for the Administrator. For the **Policies** tab, the general rule of thumb is that the most restrictive policy will apply.

Authorized Functions

For the Authorized Functions, the rule is that if the Function is authorized for any role assigned to the Administrator, then the Function is authorized for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for “Container Maintenance”, while Role B is not authorized for this. The effective right is that the Administrator is authorized for “Container Maintenance”.

Access Control List

For the Access Control Lists, the rule is that if the action on a specific Container (or Block) is authorized for any role assigned to the Administrator, then that action on that Container (or Block) is authorized for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized to Read and Write to Container “Region A”, while Role B is authorized for only Read access to “Region A”. The effective right is that the Administrator is authorized to Read and Write for the “Region A” container.

Block Type Access

For the Block Type Access, the rule is that if access is granted for a Block Type for any role assigned to the Administrator, then that access is granted to that Block Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Block Types “Any” and “Loopback”, while Role B is authorized only for Block Type “Point to Point”. The effective right is that the Administrator is authorized for “Any”, “Loopback”, and “Point to Point”.

Device Type Access

For the Device Type Access, the rule is that if access is granted for a Device Type for any role assigned to the Administrator, then that access is granted to that Device Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Device Types “PC” and “Printer”, while Role B is authorized for only for Device Type “Router”. The effective right is that the Administrator is authorized for “PC”, “Printer”, and “Router”.

Policies

For the Policies, the rule is that the most restrictive policy defined for any role assigned to the Administrator will be honored.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for “Allow Command Line Interface Access” and the “Allow Duplicate Hostnames Checking” policy is set to “Fail”, while Role B is not authorized for “Command Line Interface Access” and the “Allow Duplicate Hostnames Checking” is set to “Warn”. The effective policies are that the Administrator is **not** authorized for Command Line Interface Access and the Duplicate Hostnames Checking policy will be to “Fail”.

Domain Access Control

For the Domain Access Control Lists, the rule is that if the action on a specific Domain is authorized for any role assigned to the Administrator, then that action on that Domain is authorized for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized to Read and Write to Domain “ins.com”, while Role B is authorized for only Read access to Domain “ins.com”. The effective right is that the Administrator is authorized to Read and Write for the “ins.com” container.

Net Service Access Control

For the Net Service Access, the rule is that if access is granted for a Net Service for any role assigned to the Administrator, then that access is granted to that Net Service for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized to Read and Write to Net Service “DNS1”, while Role B is authorized for only Read access to Net Service “DNS1”. The effective right is that the Administrator is authorized to Read and Write for the Net Service “DNS1”.

Resource Record Type Access

For the Resource Record Type Access, the rule is that if access is granted for a Resource Record Type for any role assigned to the Administrator, then that access is granted to that Resource Record Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Resource Record Types “A”, “PTR” and “MX”, while Role B is authorized for only for Resource Record Type “A”. The effective right is that the Administrator is authorized for “A”, “PTR” and “MX”.

Address Type Access

For the Address Type Access, the rule is that if access is granted for an Address Type for any role assigned to the Administrator, then that access is granted to that Address Type for the Administrator.

For example, assume an Administrator is assigned to Role A and Role B. Role A is defined to be authorized for Address Types “Static” and “Reserved”, while Role B is authorized for only for Address Type “Static”. The effective right is that the Administrator is authorized for “Static” and “Reserved”.

Administrator Roles

Use the Administrator Roles screen to maintain Administrator Roles. Administrator Roles allow policies to be created for specific purposes. Once these policies are created, you may assign individual administrators to a role or multiple roles. Use Administrator Roles to define the following:

- Which management containers and/or blocks within the system can be accessed
- Which menu items are displayed to a user
- Which block types an administrator can manage
- Which device types an administrator can manage
- Which domains an administrator can manage
- What policies are applied to this user

You define administrator roles, and associate one or more users to a specific administrator role. This allows you to change an attribute of the administrator role and have it apply to all administrators that are assigned to that the role. This provides you an effective way to manage large groups of administrators, and allows you to manage groups of administrators in a consistent manner.

To access the Administrator Roles List, select **Administrator Roles** from the ADMINISTRATORS section of the **Tools** menu. The Administrator Roles screen opens.

Choose from the following actions:

- To add an administrator role, refer to “Adding an Administrator Role”.
- To search for a particular administrator role, type a search string in the text block and click **Search**.
- To create copies of one or more administrator roles, select the checkbox next to each role you want to copy, and click . A copy of each selected role will be created, with the name “Copy of *role*”. If multiple copies of a role are created, each will be named with a sequence number, for example, “Copy(2) of *role*”. The new role will have the same name, description, and policies as the selected role.
- To delete one or more administrator roles, select the checkbox next to each role you want to delete, and click . You are prompted for confirmation. Click **OK** to delete the selected administrator roles.

Note: Ensure that no administrators are assigned to a role before you delete it.

Adding an Administrator Role

To add an administrator role, follow these steps.

1. Click **Add Administrator Role**,
The Add Administrator Role screen opens.
2. **Required.** In **Role Name**, enter the name of the administrator role, for example, ‘Region A Admin Roles’.
3. In **Description**, enter a description of the role.
4. Click **Submit** to save your changes.
The role is added to the **Administrator Role** list.

Administrator Role Policies

Policies for an administrator role are set using the **Policies** link in the Administrator Role List screen.

Click **Policies** to open the Administrator Policies screen on the **Authorized Functions** tab.

Authorized Functions Tab

Each function corresponds to a menu item. To allow an administrator to use that menu function, place a check in the box next to the description. To disallow a function, uncheck the checkbox.

Access Control Lists

Select the **Access Control List** tab to what containers and blocks are accessible to NORMAL or READONLY administrator types; by definition, MASTER administrators cannot be restricted.

Note: Administrator types are defined in “Adding an Administrator” on page 263.

Access controls allow you to define which management containers a specific administrator or a group of administrators may access.

Any existing Access Control Lists (ACLs) are shown. To add containers to the ACL for the currently selected administrator role, click **Add Container(s)**. The Container Search popup window.

Place checkmarks next to the containers this administrator role can access. Once finished, click **Select Container(s)** to return to the Administrator Roles Policies screen, where the containers you selected are added to the Access Control List for the administrator role.

You can now specify the privileges that apply to the added container for the role, as described in Table 11-2.

Table 11-2 Access Control List Parameters

Field	Description
Read	Administrator can view attributes of this container and all blocks assigned to this container.
Write	Administrator can write to this container and all blocks (and IP Addresses) assigned to this container. This includes deleting blocks and IP Addresses.
Delete	Administrator can delete this container.
Apply to Children	Determines whether the Read, Write, and Delete privileges also apply to the children of this container.

Adding Blocks to an Administrator Role ACL

In addition, you can add access control policies for individual blocks assigned to a container for which there is an access control policy specifically defined for this Role. To do this, click on the **Add Block** button next to the container where the block resides. The Subnet/Block Search Results popup window opens with a list of the blocks in the container.

Click on the name of the block you want to add to the Access Control List for the selected administrator role. The block is added to the Block Name list, where you can specify the privileges to apply to this block for the selected role, as described in Table 11-3.

Table 11-3 Block Name Parameters

Field	Description
Read	Administrator can view attributes of this block including IP Addresses.
Write	Administrator can change attributes of block. Also permitted to add, modify, and/or delete IP Addresses assigned to this block.
Delete	Administrator can delete this block.

You typically add blocks to an administrator role ACL when you want to override the privileges defined on the container for a specific block. For instance, if you want to “hide” a specific block from an administrator role while allowing access to all other blocks in the container, then give the administrator role full rights to the container, but then add the specific block and remove all rights. Thus when the administrator assigned to this role views the container, the specific block does not even appear in the list of container blocks.

Block Type Access Tab

The **Block Type Access** tab allows you to limit the **Block Types** that this administrator can manage. It limits the block types available on Add Child Block, Add Root Block and Attach Block operations. The net effect is that by limiting block types for an administrator, they can see blocks of any type, but can only create blocks of types for which they have permission.

To enable Block Type Access Controls for an administrator role, click the **Allow Full Access to All Block Types for this Administrator** option button. If you wish to specify certain block types for access restriction, choose the **Limit Access By Selected Block Type(s)** option button and check the box next to each Block Type for which create permission is desired. To check or uncheck all block types shown, select **Check/Uncheck All Block Types** check box.

Block Type Size Constraints

To further constrain the block type to discrete sizes of an address block, select the **Block Sizes** link next to the selected block type. The Edit Block Sizes dialog box opens for the given block type. Block size constraints are only effective if the **Limit Access By Selected Block Type(s)** button is selected and the block type is checked. All constraints defined here are applied to both child and root block allocation.

Select all block sizes allowable for allocation by the administrator role for the block type. Any unchecked block sizes are not allowed for allocation. Use the **IPv4** tab to edit settings for IPv4 block size addressing. Use the **IPv6** tab to edit settings for IPv6 block size addressing.

Block Type Size Allocation Rules

Whether or not an administrator is allowed block allocation of a certain size for a block type will be determined by first examining the block size constraints defined at the block type definition. If there are no constraints defined for the definition, then the administrator

block type policy rules are examined. If a user owns multiple administrator roles, the block type size constraints defined for the **least** restrictive role are used.

Block Type Definition Rules

The block type will be allowed block allocation for the block size if there are no constraints defined for the block size. Note if the block size is defined as not allowable by the block type definition, then the user will not be allowed allocation **regardless** of the constraints defined at any administrator role level.

Administrator Block Type Policy Rules

The block type will be allowable for allocation for the block size if any of the following conditions apply:

- The block type is **not** selected as “Limit Access By Selected Block Type(s)”.
- The block type **is** selected as “Limit Access By Selected Block Type(s)” **and** the block size is defined as allowable for the block type.

Note: If “Limit Access By Selected Block Type(s)” is selected **and** “Abstain and leave block sizes ‘undefined’” is flagged, the administrator role will defer to another role owned by the administrator. In the case where there are no other roles defined, the block type definition rules will be used. In other words, if there are no other roles defined, all block sizes are allowed. When the “abstain” box is checked, there is no need to check any of the block sizes, and those settings will be ignored.

Device Type Access Tab

The **Device Type Access** tab allows you to limit the Device Types that this administrator can manage. It limits the device types available on the Add IP Address, or the Add IP Address Range screens. The net effect is that by limiting device types for an administrator, they can view devices of any type, but can only create, edit, or delete devices of types for which they have permissions.

To enable Device Type Access Controls for an administrator role, click the **Allow Full Access to All Device Types for this Administrator** option button. If you wish to specify certain device types for access restriction, choose the **Limit Access By Selected Device Type(s) for this Administrator** option button and check the box next to each Device Type for which create permission is desired. To check or uncheck all device types shown, select the **Check/Uncheck All Device Types** check box.

Policies Tab

The **Policies** tab allows you to assign miscellaneous administrator policies to the current administrator role.

Table 11-4 Administrator Policies Parameters

Field	Description
Allow Command Line Interface Access for this Administrator	When checked, this administrator is permitted to use Command Line Interfaces to IPAM. Otherwise, this administrator is denied access to the Command Line Interfaces.
Allow Duplicate Hostnames Checking	Ignore – Ignores duplicate hostname checking for this administrator. Warn – When a duplicate hostname is encountered, provides a warning to this administrator. Fail - Does not allow this administrator to add duplicate hostnames.
Duplicate Hostname Checking Style	Fully Qualified Domain Name – Allows administrator to check for duplicate hostnames using the fully qualified domain name. Hostname Only – Allows administrator to check for duplicate hostnames using the hostname only.
Allow Duplicate A Record (Owner) Checking	Ignore – Ignores duplicate A record checking for this administrator. Warn – When a duplicate A record is encountered, provides a warning to this administrator. Fail - Does not allow this administrator to add duplicate A record.
Allow Duplicate Hardware Address (MAC) Checking	Ignore – Ignores duplicate MAC Address checking for this administrator. Warn – When a duplicate MAC Addresses are encountered on distinct devices, provides a warning to this administrator. Fail - Does not allow this administrator to add duplicate MAC Addresses on distinct devices. Note that duplicate MAC addresses are always allowed on multiple interfaces on the same device.

Domain Access Control Tab

Domain Access Control allows you to define which domains a specific administrator or a group of administrators may access.

Any existing Domain Access Control Lists (ACLs) are shown. To add domains to this user's ACL, click **Add Domain(s)**. This brings up a window prompting you to select the domain this administrator role can access.

Select the domain link that this administrator role can access. The domain is added to Domain Access Control list, where you can specify the privileges that apply to this administrator role, as described in Table 11-5.

Table 11-5 Domain Access Control Parameters

Field	Description
Read	Administrator can view attributes of this domain excluding resource records. This also includes viewing attributes of zones for this domain.
Write	Administrator can make modifications to this domain. This effectively means that the administrator can: <ul style="list-style-type: none"> • Change SOA values (where appropriate) for this domain. • Create child domains

Field	Description
	<ul style="list-style-type: none"> Create zones for this domain.
Delete	Administrator can delete this domain.
Resource Record Access	Administrator can read resource records within this domain.
Resource Record Write Access	Administrator can modify resource records within this domain.
Resource Record Approve Access	<i>Displayed only when Resource Records Workflow is enabled.</i> Administrator can approve/reject resource records added by others for this domain. Also if this option is checked, resource records added by the administrator in this domain do not require approval.
Apply to Children	Determines whether these privileges also apply to the children of the domain in the Domain field.

Net Service Access Control Tab

The **Net Service Access Control** tab controls allow you to define which Net Services a specific administrator or a group of administrators may access.

To **enable** Net Service Access Controls for an administrator, click on the button labeled “Enable Net Service Access Controls for this Administrator”. When this selection is enabled, only those Net Services listed will be accessible to the administrator. If the selection is **disabled**, all Net Services in the system will be accessible with full permissions (Read, Write, Deploy).

Any existing Net Service Access Control Lists (ACLs) are shown. To add Net Services to this user’s ACL, click **Add Net Service(s)**. This brings up the Network Service Search screen where you to select the Net Services this administrator role can access.

Select the Net Service link you want this administrator role to access. The Administrator Net Service Access Control screen opens with the selected Net Service added to the Net Service table, where you can specify the permissions that apply to this administrator for the specified Net Service.

Table 11-6 Net Service Access Control Parameters

Field	Description
Read	Administrator can view attributes of this Net Service.
Write	Administrator can make modifications to this Net Service.
Deploy	Administrator can deploy to this Net Service.

Resource Record Type Access Control Tab

The **Resource Record Type Access Control** tab allows you to limit the Resource Record Types that this administrator can manage. It limits the Resource Record types available on the Add Resource Record screens. The net effect is that by limiting resource record types for an administrator, they can only create, edit, or delete resource records of types for which they have permissions.

To enable Resource Record Type Access Controls for an administrator role, click the **Allow Full Access to All Resource Record Types for this Administrator** option button. If you wish to specify certain resource record types for access restriction, choose the **Limit Access By Selected Resource Record Type(s) for this Administrator** option button and check the box next to each Resource Record Type for which create permission is desired. To check or uncheck all resource record types shown, select the **Check/Uncheck All Resource Record Types** check box.

Address Type Access Tab

The **Address Type Access** tab allows you to limit the Address Types that this administrator role can manage. It limits the Address types available on the Add IP Address, Add IP Range and Add IP Address pool screens. The net effect is that by limiting address types for an administrator, they can only create, edit, or delete IP Address of Address types for which they have permissions.

To enable Address Type Access Controls for an administrator role, click the **Allow Full Access to All Address Types for this Administrator** option button. If you wish to limit access by selected address type, choose the **Limit Access By Selected Address Type(s) for this Administrator** option button and check the box next to each Address Type where access is desired. To check or uncheck all address types shown, select the **Check/Uncheck All Address Types** check box.

Once finished, click **Submit** to save all changes on the Administrator Policies screen, or **Cancel** to discard all changes and return to the Administrator Roles screen. If the Administrator Policy was successfully updated, the Administrator List screen displays Policy for <admin-role> saved.

Chapter 12 Performing Advanced Administration Activities

This chapter provides administrators with “how to” information on common operational functions that need to be accomplished within the product.

Configuring INS DNS for Selected or Changed Zone Push

IPAM has the ability to perform selective DNS zone configurations using the Configuration/Deployment menu option.

Specific Configuration/Deployment options include the following:

- **DNS Configuration - Changed Zones Only** - when an administrator makes a change to a resource record in a domain, all zones associated with that domain are marked as “dirty”. The IPAM administrator can then schedule a “Changed Zones Only” deployment push, and only zones that have changed since the last file generation are created and sent to the DNS server.
- **DNS Configuration - Selected Zones Only** - an administrator may want to immediately push changes to a specific zone to a specified DNS server, without necessarily pushing every changed zone.

To support either of these configuration/deployment options, some additional configuration is required on the DNS server. This is because these tasks make use of the “rndc” utility to only load the selected zones, instead of forcing the DNS service to completely stop and start. This provides seamless loading of new data without affecting name resolution for your users.

To configure the INS DNS server for this support, perform the following steps:

1. Choose from the following actions.

Server Type	Steps
Windows	<ol style="list-style-type: none">1. Run the following command: <code>C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\dns\bin\rndc-confgen -a -k rndc-key.</code>2. Open the C:\Program Files\Cisco\Cisco Prime Network Registrar IPAM\dns\etc\rndc.key in a text editor (such as Notepad).

Server Type	Steps
UNIX	<ol style="list-style-type: none"> As the 'root' user, run the command: <code>/opt/incontrol/dns/sbin/rndc-confgen -a -k rndc.key.</code> Open or cat the file <code>/etc/rndc.key</code>.

- Copy the secret part of the file, excluding quotes. For example:
f72ISy9MFntJ4In1sSRtOQ==
- In IPAM, select **Transaction Keys** from the DNS section of the **Management** menu.
- In the Transaction Keys screen, select **Add Transaction Key**. The Add Transaction Key screen opens.
- In the **Key Name** field, type `rndc-key.` (Note the trailing period).
- Paste the key from step 3 into the **Secret** field. (To review the string, select the **Unmask Secret** checkbox.)
- Repeat for the **Confirm Secret** field.
- Click **Submit** to save the key.
- Select **Servers/Services** from the DNS section of the **Management** menu.
- Select the DNS Server to which you are performing a Changed or Selected Zone push.
- Click on the **Advanced** tab. In the **Allow Messages From** list box, make sure **localhost** is selected. In the **Keys (Used by rndc)** section, select the `rndc-key.` key you created above.
- Click **Submit** to save the server.

Your server is now configured for Changed or Selected Zone pushes.

Configuring IPAM to use External Authentication

IPAM can use an external authentication mechanism when users log into the system. This allows you the ability to establish administrative roles within the system, and then use an external authentication data store for password credentials.

There are two approaches to using external authentication.

- The first is to define each administrator (USERID) within IPAM, assign an administrator role to that admin, and then only use the external authentication mechanism for password authentication purposes. This allows you the ability to control admin rights at a very granular level, while still leveraging a single sign on method.

- The second approach involves creating a small set of userids (administrators) within the IPAM system, and assigning unique roles to each. You can then use your external script to map the userid attempting to login to IPAM, to a specific user within IPAM. This allows you to control your administrative roles at a higher level, and allows you to leverage your external authentication system to help control access.

You must create a script, or use/modify one of the scripts that have been provided with your installation. By default, the installation routine copies a number of PERL based scripts to the `$INCHOME/etc/support/sample-scripts` directory. Sample scripts that are included are:

- `extauth-ldap.pl` – LDAP Authentication
- `extauth-msad.pl` – Microsoft Active Directory Authentication
- `extauth-tacacs.pl` – Cisco TACACS authentication

Please refer to these scripts as examples and note the input and outputs to these scripts.

Input

When this script is executed, IPAM passes three variables to the script:

- The `USERID` entered on the IPAM login page
- The `PASSWORD` entered on the IPAM login page
- The Product name “IPAM”

Output

On a successful authentication:

- When your script executes, it should send to `STDOUT`, the line “SUCCESS”, and then the `USERID` that is used by IPAM to establish administrative roles (that is, the `USERID` to look up within IPAM). You can optionally change the `USERID` that is returned to IPAM: it does not necessarily have to be the `USERID` entered by the user on the IPAM login page.

On an unsuccessful authentication:

- Your script should send the line “FAILURE”, followed by a line of text that appears on the login page. You can use this second line to send a reason why the login failed. The message appears on the IPAM Login page.

Configuration Steps

To configure the system to use external authentication, perform the following steps:

1. Select **Policies and Options** from the **SYSTEM** section of the **Tools** menu. The System Policies/Options screen opens.
2. In the **External Authentication Script** field, type the authentication script name and click **Submit**.

Note 1: If you are using PERL, you must enter the path and name of the PERL interpreter, as well as the script name, for example: `c:\perl\bin\perl test.pl`

Note 2: To call an external authentication script that resides in a directory with a space in the directory name, you must enclose the full path and script name in quotes, for example:
`c:\cygwin\bin\perl.exe "c:\Program Files\success.pl"`

3. After you have saved the script name, click the **Test** button next to the **External Authentication Script** field to run a test.
4. The test dialog appears. If necessary, enter a different userid and password to exercise the script, and then click **Test**.
5. After the script executes, a success or failure message is provided back to the script.
6. After you are sure your script is operating correctly, set an administrator option for each administrator that you want to have use this external authentication method. Select **Administrators** from the ADMINISTRATORS section of the **Tools** menu and select the administrator entry you want to edit.
7. Select the **Authorize Externally** check box to turn on external authentication for this user and click **Submit**.

Interfacing with Microsoft Active Directory and Microsoft DNS

Many enterprise IT organizations find themselves faced with the challenge of managing a dichotomy of two Domain Name System (DNS) technologies: the original Internet standards-based BIND (Berkeley Internet Name Domain) and Microsoft Windows DNS. While these two DNS technologies are very similar and even interoperate in some ways, they are at the same time vastly different.

This section provides an overview of each technology and discusses various interoperable configurations supported within standard Microsoft Windows and Internet Systems Consortium BIND. It also reviews deployment configurations supported with the help of IPAM software, from pure Microsoft Active Directory DNS configurations to a mix of Microsoft and BIND DNS.

IPAM IP address management software system is designed to provide centralized IP address management (IPAM) features for customers who manage a number of DHCP and DNS servers from various suppliers, including ISC and Microsoft. The benefits that can be derived from supplementing Microsoft and BIND DNS deployments with IPAM's IP address management functions include:

- **Centralized IP address inventory** - The IPAM centralized IP management system can serve as a centralized IP address inventory database across both technologies.
- **Unified IP inventory and DNS configuration** - IPAM can leverage IP inventory information and associate it with corresponding DNS domains, zones, and options. This inherent association reduces errors and saves time by reducing duplicate entries

of similar information in multiple systems (for example, in a BIND text file and in a Microsoft DNS server).

- **Simplified IP management** – Manually configuring and managing DNS configurations and resource record updates is complex enough when using either BIND or Microsoft. When using both, the technical challenges of performing these updates accurately and efficiently are potentially overwhelming. IPAM supports the consistent deployment of DNS configuration information across multi-vendor DNS servers including BIND and Microsoft.
- **High availability services** – While Microsoft’s multi-master architecture is targeted to provide high availability, using IPAM, you can incorporate BIND servers into the multi-master mix.
- **Extensive user definability** – Centrally defining policies and implementing them across an IP network can promote consistency, reduce configuration errors, and allow tracking of additional information with the elements of the IP network. IPAM can define device types, define naming policies per device type, and associate a rich set of user definable fields with each device type and address type to allow individualized management of the IP network.

The following sections explain the different configuration options that are available using IPAM with Microsoft Active Directory and Microsoft DNS.

BIND DNS

Internet-standardized DNS servers have historically been based on an IETF (Internet Engineering Task Force) RFC 1034-5 (and its successors) reference implementation known as BIND (Berkeley Internet Name Domain). BIND is currently supported and maintained by the Internet Systems Consortium (ISC) and supports storage of name server and zone configuration information in text files stored on each DNS server. BIND has been extended significantly over the years, including a total rewrite of BIND with version 9, and provides extensive flexibility in terms of configurability. As is often the case, with the benefit of increasing flexibility comes increasing complexity. IPAM software can ease the complexity of configuring these very enabling features.

BIND Redundancy

BIND provides for redundancy using a master/slave relationship. A single master DNS server maintains the authoritative, administrator-created and -modified copy of information for a particular DNS domain. DNS slaves acquire their information from the master using a special copy mechanism called a zone transfer. There are two types of zone transfers: a full transfer, called AXFR, and a partial or incremental transfer (changed information only since the last full transfer), called IXFR.

AXFR Zone Transfer

The single master DNS server domain information can be manually edited by an administrator. The administrator must also update the zone serial number. When this

update is complete, the slaves detect a change in the domain's configuration via their periodic "zone refresh" polling of the master DNS server's Start of Authority (SOA) record, which contains the current serial number. Upon detecting a serial number change, the slave may then request a full or incremental zone transfer.

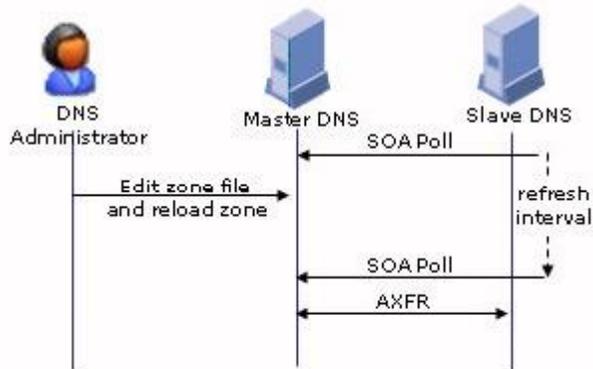


Figure 12-1 AXFR Zone Transfer

IXFR Zone Transfer

Updates may also be made dynamically from a DHCP server, for example. In this scenario, upon providing a device an IP address via DHCP, the DHCP server can dynamically update the master DNS server with the IP address to host name/domain name mapping (A and PTR records). When the master receives and accepts such a dynamic update, it will initiate a notify message to its slaves. The notify message instructs the slaves to request an IXFR to receive the dynamic updates sooner than they otherwise may have received it via zone refresh polling.

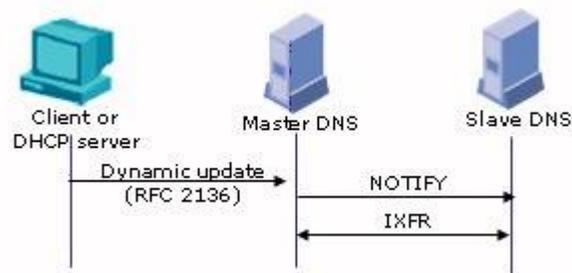


Figure 12-2 IXFR Zone Transfer

Microsoft DNS

Microsoft Windows 2003 Server and 2008 Server products provide DNS services, which support Internet standard name resolution in accordance with RFCs 1034-5. This allows standard resolver clients, Windows-based or otherwise, to query Microsoft DNS as they would BIND DNS. As we shall see, there are some areas where Microsoft supports Internet standard interfaces, such as for dynamic updates, and other areas where Microsoft supports a variation, though in some cases also Internet standards-based (for example, GSS-TSIG [Generic Security Specification Transaction Signature] *vs.* TSIG).

Microsoft's DNS services can be configured via Windows Registry, configuration files stored on the server, or AD integration of DNS zones on specially configured Windows 2003/2008 servers called Domain Controllers (DCs). The Active Directory implementation option is the most common approach as it provides the ability to run multiple master DNS servers, which can be kept in close synchronization via Active Directory replication.

Domain Controller Query

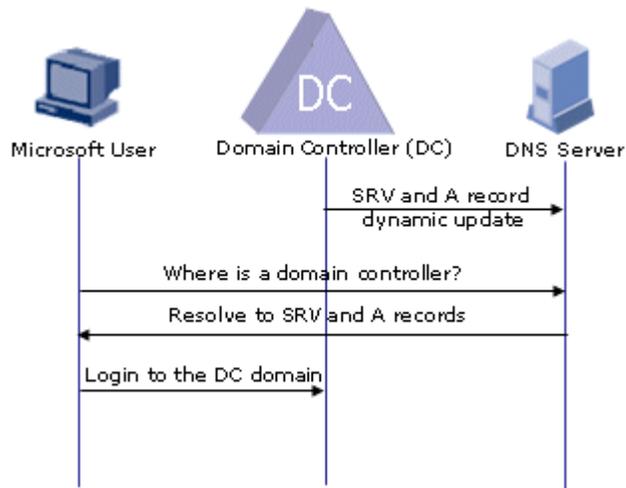


Figure 12-3 Domain Controller Query

Microsoft's AD is based on a replicated LDAP compliant directory and is used for provisioning of all authentication and network services. This AD resides on DCs. When Windows AD participating clients connect to the network, they must find a DC for validation and to access a catalog of Windows services (mainly file and print). A DC is located by querying a DNS server for a number of specialized DNS records called SRV records. Although SRV records are a standard part of the DNS system, the information returned in these records for AD are specific to Microsoft. The DNS domain in which these SRV records reside must be the same as the AD Primary Domain name in which the Microsoft client participates. (The DNS domain and the Windows Primary Domain are not the same thing; they are, however, named the same.)

These SRV records are dynamically added to the DNS space by the Windows 2003/2008 DCs using standard dynamic DNS updates, as described by the IETF RFC 2136. Beyond this element of commonality, the "normal" or standardized DNS servers begin to have a problem with Microsoft's requirements for Active Directory and DCs.

BIND DNS and Microsoft DNS Compared

The BIND master/slave philosophy is very different from Microsoft's approach to AD, where every copy of the directory is identical and replicated frequently to keep them synchronized; each AD copy is a peer to all the others. Where BIND DNS updates always go to the master first, updates to the AD can go to any peer copy. That instance of the AD then initiates a replication of that information to all other copies.

The following table highlights a few of the key differences and similarities of BIND 9 DNS and Microsoft AD-integrated DNS. Note that there are hundreds of attributes that could be compared; the point here is that each implementation of DNS brings its relative advantages with respect to the other. In most situations today, you either need to pick one implementation or the other in all but the most trivial scenario of BIND DNS supporting an Active Directory environment that itself is not running DNS. But IPAM can help expand the possibilities by supporting additional BIND and Microsoft configurations highlighted in this section.

Table 12-1 Feature Comparison

Feature	BIND 9 DNS	Microsoft AD-Integrated DNS
Dynamic Update via RFC 2136	Yes	Yes
Support for AXFR/IXFR	Yes	Yes
Multi-Master DNS	No	✓ Yes
Slave DNS	✓ Yes	No
TSIG Support	✓ Yes	No
GSS-TSIG Support	No	✓ Yes
Standard configuration file format	✓ Yes	No
LDAP-based replication	No	✓ Yes
SRV Record support (RFC 2782)	Yes	Yes
Split DNS	✓ Yes	No
Hints file	Yes	Yes

Joint Implementation Scenarios

With both technologies bringing respective advantages, coordinated support of both technologies in various scenarios can provide significant benefits for your DNS infrastructure. IPAM software facilitates this joint technology approach by providing support for both technologies in various implementation scenarios. This section reviews five such scenarios outlining IPAM's support of standalone and mixed BIND and Microsoft DNS deployments.

Case 1: BIND DNS Supporting Non-DNS AD Environment

This case is the simplest of scenarios and requires no special interworking per se, as the DNS service resides only on BIND DNS servers. The AD environment leverages the BIND DNS server as its DNS repository and domain controllers send SRV record updates to the master DNS server when it boots. This allows Windows clients to locate their domain controller for login. Utilizing IPAM in such an environment provides the benefits of centralized configuration and leverages the many BIND configuration parameters supplied by IPAM.

IPAM can be used to not only define the servers, views, domains, and associated configuration, but additionally for centralized IP inventory. Thus, when a new IP address is assigned to a static device for example, the IP inventory can be updated via IPAM. IPAM can then automatically send a dynamic update to the master DNS server for the associated zone if desired, thereby keeping DNS information in synch with the IP inventory. Note that this update can be unsigned or signed for added security. IPAM enables simplified

transaction signature (TSIG) key creation and association with pair-wise server connections, including DNS-DNS, DHCP-DNS, and IPAM-DNS connections.

As a dynamic device receives an IP address via DHCP, the DHCP server can send a dynamic update to the master DNS server on behalf of the client. The master DNS server can send a notify message to each of its slaves. The master would also be configured to also-notify IPAM (DNS Listener service) for the purpose of capturing such notify messages and executing IXFRs to capture changes or updates to the DNS information and IP inventory in IPAM. In this manner, the IPAM centralized inventory can be kept up-to-date and accurate with respect to static device entries as well as dynamic clients obtaining IP addresses.

Figure 12-4 illustrates this configuration and these update scenarios.

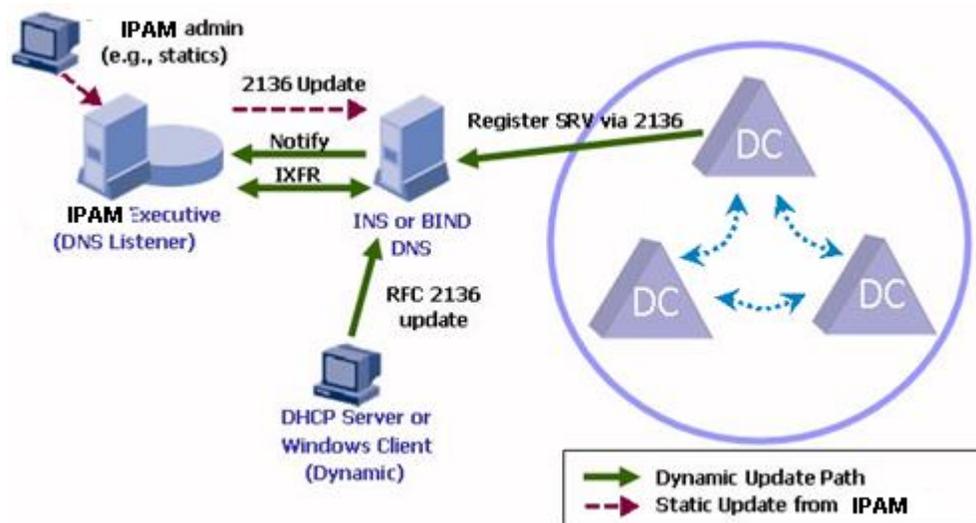


Figure 12-4 BIND DNS Supporting Non-DNS AD Environment

Reviewing Figure 12-4, following the magenta dash arrows (static update from IPAM), IPAM administrators can enter static addresses into the system, and it can automatically update the master DNS server via an RFC 2136 dynamic update (TSIG-signed or unsigned). The master can then notify its slaves of the update and perform IXFRs with each (not shown in the figure). For dynamic devices such as clients or domain controllers, they can either update the master DNS server directly or clients can update via DHCP servers as shown via the green solid arrows (dynamic update path) above. The master DNS server notifies its slaves and also-notifies the IPAM DNS Listener. The slaves and the DNS Listener perform IXFRs to get updated zone information. IPAM can then update its database with the host name, domain name, and IP address information.

Configuring Case 1 in IPAM

INS DNS (and BIND 8.x/9.x) can accept dynamic updates of SRV records from AD servers, and accept dynamic updates (A/PTR) from AD clients. Any dynamic updates accepted by INS DNS can be forwarded to IPAM (to update the IPAM database) via Notify/IXFR to the DNS Listener. Minimally, this requires that DNS options for Allow Update, Also Notify, and Allow Transfer be set appropriately for any dynamic zones

To configure Case 1 within the IPAM system, follow these steps:

1. Create an Address Match List (select **Address Match Lists** in the DNS section of the **Management** menu) that contains all the IP addresses of your AD servers, IPAM Agents, DHCP Servers, and any specific AD clients that are updating DNS.
2. Configure the **Allow update** option on the zone to allow updates from your known Microsoft Domain Controllers, DHCP Servers, and/or IPAM Agents. Select the **Address Match List** that you defined in step 1.
3. Configure the **Allow transfer** and **Also notify** options to allow transfers of data to the IPAM DNS Listener. In this example, the IPAM Executive (DNS Listener) is at IP address 10.10.10.1.
4. Distribute the new DNS configuration to your DNS server using the **Configuration/Deployment** option, and the server will now accept updates from Active Directory, and update the IPAM as well.

Case 2: IPAM Centralized Inventory of AD DNS Environment

The next case could be viewed as the converse of Case 1. Instead of using a pure BIND DNS approach to support DNS services for an AD environment, this case utilizes a pure AD-integrated DNS approach to supporting DNS services. Case 1 demonstrated the entry of static IP addresses into IPAM, and propagation to the master Microsoft DNS server. While this scenario still applies in this case, many organizations employing AD-integrated DNS desire to alternatively have their AD administrators update AD DNS with static entries. These two “static update” scenarios are broken out in Figure 12-5.

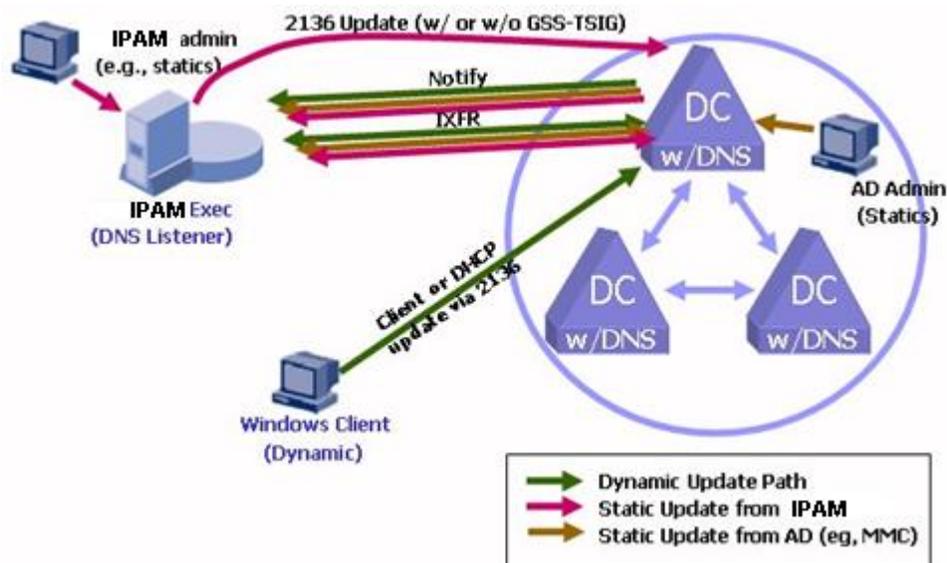


Figure 12-5 IPAM Centralized Inventory of AD DNS Environment

Static Update from IPAM

The magenta arrows once again illustrate entry of static IP addresses via IPAM. As in Case 1, IPAM can automatically update the master DNS server, which in this case is an AD domain controller running DNS. The update can be signed or unsigned, though Microsoft does not support TSIG as supported by BIND. Microsoft supports GSS-TSIG for update signing. Microsoft's implementation of GSS-TSIG utilizes Kerberos for key distribution. IPAM can participate in obtaining a key via Kerberos to sign updates to AD DNS.

Static Update from AD

The brown arrow represents static address updates from a Windows administrator, for example, via the Microsoft Management Console (MMC). The updating of IPAM with this information requires the Microsoft DNS server to have the IPAM DNS Listener configured for also-notify. When a record is updated via MMC, the AD-integrated DNS servers synchronize the update via LDAP replication and also-notify IPAM, which in turn performs an IXFR and inventory update. In this manner, organizations may manage IP inventory with IPAM, whether static devices are entered via IPAM or Windows MMC.

Dynamic Updates

Dynamic addresses would be updated in AD DNS via RFC 2136 updates from domain controllers, DHCP servers, or directly from Windows clients. Following the green arrows in Figure 12-5, this update is replicated among the AD DNS servers and the IPAM DNS Listener is also-notified. IPAM then updates its database with this dynamic host name, domain name, and IP address information.

Configuring Case 2 in IPAM

To configure Case 2 within the IPAM system, follow these steps:

1. You must first define the DNS Master Zone within Microsoft AD using the supplied Microsoft DNS "New Zone" wizard.
2. Follow the wizard to create a new Primary Zone Active Directory integrated zone.
3. Select how you want to replicate zone data throughout your Active Directory Replication scope.
4. Enter the zone name of your new zone.
5. Select the dynamic update options for this zone. Select **Allow only secure updates** if you are using the GSS-TSIG secure update support within IPAM, or select **Allow both nonsecure and secure dynamic updates** if you are not using GSS-TSIG.
6. Complete the creation of your new zone by selecting **Finish**.
7. Once the zone has been created, you must allow zone transfers to the IPAM DNS listener. Use the **Zone Transfers** tab of the DNS Management Console to configure the IP Address of the IPAM DNS Listener on the zone.
8. Note that the above configuration explicitly lists the IP address of the IPAM DNS Listener (10.10.10.1). Alternatively, the **To any server** option could be selected.

However, **Only to servers listed on the Name Servers tab** is not a good selection, because then the DNS Listener would need to be listed as an actual DNS server for this domain, which is not correct, since it cannot respond to queries. The DNS Listener should also be explicitly listed in the Notify list as follows. Use the **Notify** tab of the DNS Management Console to configure the IP Address of the IPAM DNS Listener.

9. Make sure you configure and define the Domains that you are managing within IPAM system.

Case 3: AD Multi-Master DNS with BIND DNS Slave

This case is the first of the mixed technology scenarios with one or more BIND DNS slave servers supporting AD DNS multi-master servers. The benefits of deploying this configuration include:

- **Technology diversity** – minimize implementation specific issues and reduce upgrade outages
- **Platform diversity** – especially if you run your BIND servers on Linux; minimizes OS vulnerabilities
- **Flexible network design** – depending on design, it may make sense to deploy low end boxes running BIND in remote offices while running DCs “on the backbone.”

As displayed in Figure 12-6, this scenario is similar to Case 2, with the addition of one (or more, not shown) BIND slaves. In fact, one variation on this case is one exactly as in Case 2, with the additional also-notify for each BIND slave configured in each AD DNS server. However, referring to Figure 12-6, static IP device entries may be made either via IPAM or Windows MMC.

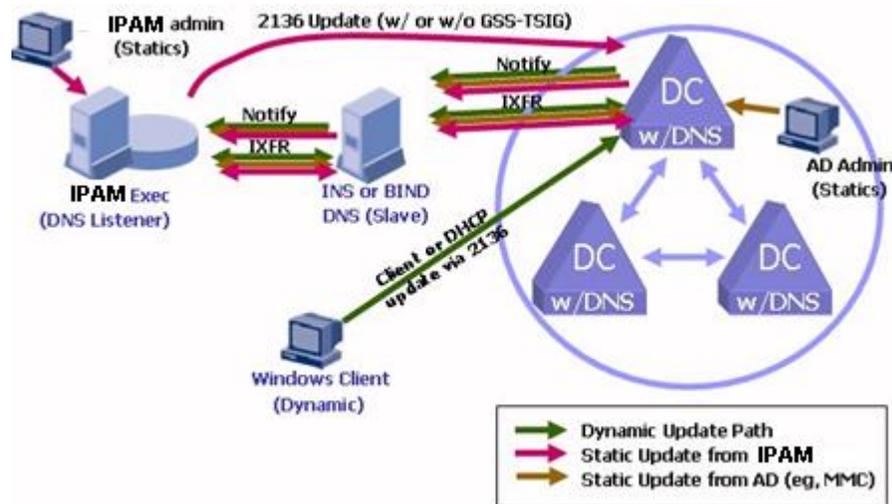


Figure 12-6 AD Multi-Master DNS with BIND DNS Slave

Updates from IPAM, following the magenta arrows (static update from IPAM) in the figure, are forwarded via signed or unsigned updates to a master domain controller. The DC

updates its fellow-AD-integrated DNS servers and also-notifies the BIND DNS slaves. The BIND slaves perform an IXFR to refresh their zone data with the new static address and associated host and domain name information. The slave BIND server can in turn also-notify the DNS Listener, which in this case ignores the update given that it originated it.

Note that a variation on this case employs non-AD integrated DNS from Microsoft as master with BIND DNS as slaves. With a Microsoft file- or registry-based DNS server performing as master, updates would follow the same path described in this section, with the exception that no multi-master support and no LDAP replication would be provided. The master DNS server would receive updates statically from a Microsoft administrator or via dynamic updates from clients, DHCP servers or IPAM. The notify/IXFR process would then be invoked to update BIND or other Microsoft DNS servers acting as slaves.

Configuring Case 3 in IPAM

To configure Case 3 within the IPAM system, follow these steps:

1. Configure your domain within your Microsoft DNS infrastructure. Refer to the Microsoft documentation to create a new domain.
2. Create a slave domain within IPAM.

Case 4: BIND DNS Master with a Microsoft DNS Slave

The same basic motivations driving Case 3 also apply to Case 4. Use of diverse technologies, platforms, and design reduce exposure to particular implementations' vulnerabilities or nuances. Case 4 highlights the use of a BIND DNS server as master for a set of zones, with Microsoft DNS as slave servers. Note that AD-integrated DNS only functions as multi-master; it cannot function in a slave configuration. However, when using Microsoft's file- or registry-based implementation, Microsoft DNS servers can function as slaves.



Figure 12-7 BIND DNS Master with a Microsoft DNS Slave

As illustrated in Figure 12-7, static addresses are configured via IPAM, which drives a signed or unsigned dynamic update to the master BIND server (magenta line). The master server utilizes notify/IXFR to update the Microsoft (and/or BIND) slaves as well as the DNS Listener, which ignores this update. A dynamic client's IP address to host/domain name

mapping is updated in the master BIND server by the DHCP server or client itself. Utilizing the same notify/IXFR mechanism, Microsoft (and/or BIND) slaves are updated, as is IPAM via its DNS Listener service.

Configuring Case 4 within IPAM

To configure Case 4 within the IPAM system, follow these steps:

1. Configure your domain within your IPAM infrastructure.
2. Using the Domain wizard available on the Microsoft Windows 2003/2008 server GUI, create a secondary zone on your Microsoft DNS infrastructure.
3. Select **Secondary zone** and click **Next**. The Zone Name screen appears.
4. Enter the name of your domain name, and click **Next**. When prompted for the addresses of the master servers, enter the IP Address of the INS DNS server that is master for the zone.
5. In the IPAM GUI, the IP Address of the Microsoft DNS slave must be added to the **Allow transfer** and **Also notify** lists of the INS DNS master server. In the following example, the IP address of the MS DNS slave is 11.11.11.1.
6. Note that alternatively, the IP address of the MS DNS slave (11.11.11.1) could be added to an Address Match List along with either the IP address of the IPAM DNS Listener or the name of a TSIG key which identifies IPAM. The named Address Match List could then be referenced in the Allow Transfer option.
7. Push your configuration file to your DNS secondary server, using the Deployment options from the IPAM system.

Case 5: PeerMaster – Effective BIND-Microsoft Multi-Master DNS

The last case is another unique case where IPAM provides substantial value in maximizing the flexibility of DNS deployments. The PeerMaster approach effectively provides multi-master DNS using both Microsoft AD DNS and BIND servers. This means that updates to either the AD DNS master or the BIND DNS “master” will be communicated to the other masters automatically.

This configuration requires use of BIND 9.2 or later. The BIND server is actually configured as a slave, but with 9.2 or later, BIND supports update-forwarding. This allows updates to be sent to the BIND slave as if it were a master, while allowing other masters to be updated automatically. This is the most complex yet enabling configuration presented to maximize the benefits of managing BIND and AD-integrated DNS together. Figure 12-8 illustrates this configuration with the four update methods:

- Static update via IPAM
- Static update via Windows (MMC)
- Dynamic update to Windows DNS
- Dynamic update to BIND DNS

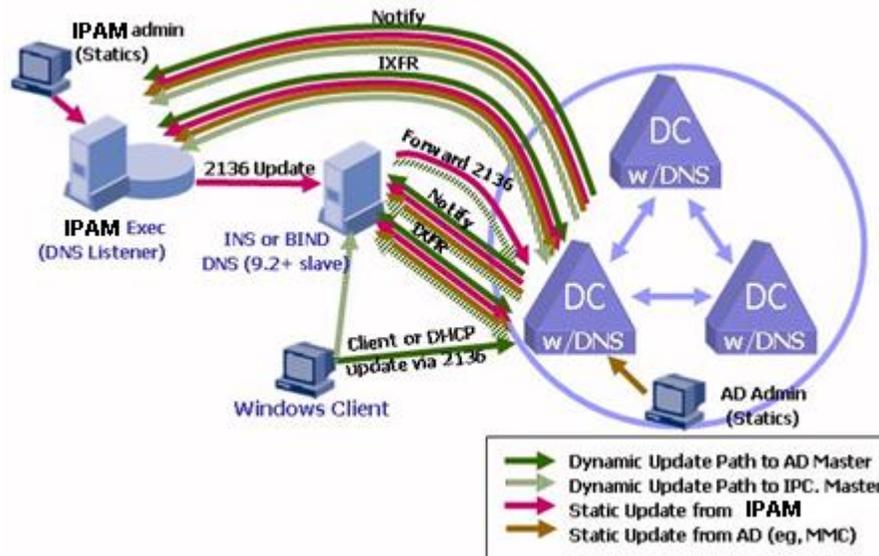


Figure 12-8 PeerMaster – Effective BIND-Microsoft Multi-Master DNS

Static Update via IPAM

If an organization’s policy is to drive static address assignments via IPAM, two sub-scenarios exist for this case. Only one is shown in Figure 12-8 to keep it relatively simple. Following the magenta arrows (static updates from IPAM) in the figure, when the IPAM database is updated with the new device information, IPAM can then issue a dynamic update to a master DNS server. The first sub-scenario consists of an IPAM signed or unsigned update to a BIND slave server. With update forwarding on, the BIND slave forwards the update to its master, an AD-integrated master DNS server. The second sub-scenario comprises IPAM sending a signed or unsigned update directly to a master AD DNS server. At this point, both sub-scenarios converge, and the AD DNS server replicates the update to its AD peers, and then executes also-notify to the BIND slaves and IPAM’s DNS Listener.

Static Update via Windows (MMC)

The brown arrows in Figure 12-8 indicate the flow of information when updating an AD master DNS directly via Windows, for example, via MMC. The AD master replicates to its peer AD masters via LDAP, and executes also-notify to the BIND slaves and IPAM DNS Listener, each of which initiate an IXFR to capture the update.

Dynamic Update to AD DNS

The green arrows in Figure 12-8 highlight the update path for dynamic updates to AD DNS. The master AD DNS server replicates this update to other AD masters and executes also-notify to its BIND slaves and IPAM’s DNS Listener for updating of IPAM’s database.

Dynamic Update to BIND DNS

The hashed green arrows in Figure 12-8 illustrate the flow for a DHCP server or client update to a BIND DNS server, appearing as a master but technically a slave. The BIND server is configured to forward updates to an AD DNS server. The AD DNS server

performs its replication of the data to peer AD masters and executes also-notify to slave BIND DNS servers and IPAM's DNS Listener.

Configuring Case 5 within IPAM

To configure Case 5 within the IPAM system, follow this step:

- Configure your domains within the Microsoft DNS system. The zone should be created and defined as master for a zone, and an INS IPAM DNS server as slave for the same zone. In the slave zone definition, you need to use the “Allow Update Forwarding” option. There are two possible values to support the PeerMaster configuration:
 - ▶ **Any** - This allows any updates sent to the slave to be forwarded to the master. Any such forwarded updates are assumed to be unsecured. This is because the Microsoft AD DNS server provides only secure (GSS-TSIG) or unsecured updates as options for dynamic zones. The INS IPAM DNS slave cannot negotiate GSS-TSIG with MS AD, so the zone must be configured for unsecured updates.
 - ▶ **Authorized updaters only** - Authorized updaters include IPAM Agents and Microsoft Domain Controllers (DC). This configuration places the security enforcement on the slave; however the zone master must still be configured for unsecured updates. The security on the slave is unfortunately static by nature, so as new IPAgents and/or DCs are added to the environment, the Allow Update Forwarding ACL on the slave must be updated.

Creating GSS-TSIG enabled account in Microsoft MMC

Overview

IPAM can exchange GSS-TSIG signed messages with Microsoft DNS. To make use of this mechanism, a user ID must be created on the Microsoft side, and this account must have certain attributes.

Microsoft Active Directory

Follow these steps:

1. Launch MMC and open the Users and Computers snap-in.
2. Create a new user and set the password.
3. Once user is created, right-click on the user and choose **Properties**.
4. Choose the **Account** tab.
5. Select the following checkboxes:
 - ▶ Use DES encryption types for this account

- ▶ Do not require Kerberos preauthentication

Note: Due to various configuration options with MS AD security, if IPAM cannot authenticate with MS AD, and you receive `SERVFAIL` messages in the IPAM Agent log file when performing a DDNS Configuration/Deployment, you must deselect **Use DES encryption types for this account** and **Do not require Kerberos preauthentication**.

6. Save the changes by clicking **OK**.
7. Right-click on the user and choose **Reset Password**, and set the password again.

IPAM

Follow these steps:

1. Navigate to System >Management > IPAM> Server Pairs.
2. Create a server pair and ensure the following:
 - ▶ Realm name is in all capital letters
 - ▶ Realm name matches the realm used in Active Directory
 - ▶ User name and password match the case used in Active Directory

Other Considerations

Follow these steps:

1. If the Executive is running on UNIX, ensure that the FQDN of the AD server appears *before* the short hostname in `/etc/hosts`. Ex:
10.30.8.46 adsrvr.example.com adsrvr
2. The AD account can be either a normal user or a service account
3. The AD account must be allowed “Full Control” to each domain that is to be dynamically updated.
4. Target server must be in Notify List
5. Target server must be in Zone Transfer list.

IPAM Management of Windows DHCP Server

Overview

IPAM has the ability to create Microsoft Windows DHCP Server configuration information, providing an alternative management console that can be used enterprise wide for DHCP configuration. Dynamic objects can be defined within IPAM and then “pushed” to the remote MS Windows Server. All active lease information from MS Windows Server is

displayed within the IPAM console. IPAM can also be used to create the policy that governs how the Microsoft DHCP Server performs dynamic DNS updates.

Prerequisites

- In the IPAM Executive
 - ▶ Configured Address Pools, and so on.
- On the Microsoft Windows 2003/2008 Server
 - ▶ DHCP Server running
 - ▶ IPAM Agent installed

Windows Server Procedures

Install DHCP Service

Use the Configure My Server window to add DHCP if it is not already installed. It is accessible via **Start > Control Panel > Administrative Tools > Configure Your Server Wizard**.

Run DHCP Configurator

Start the DHCP configuration tool using the Start Menu. This application allows you to authorize DHCP and monitor all scopes, address pools, and options.

Verify Server is Authorized

If the server is a member of an AD Domain, the DHCP server must be authorized for the domain if it is not already. A green arrow appears on the DHCP server icon if the server is authorized. A red arrow appears if it is not authorized.

MS DHCP is now ready to be configured. This is done automatically from within IPAM – you do not have to manually add scopes from within the Microsoft application.

Non-AD Domain Agent Configuration

Microsoft DHCP servers do not need to be a member of an AD Primary Domain. However, the IPAM Agent *must* be running as an account that is authorized to read and modify the DHCP options and parameters. Since a Windows Service, by default, runs as a “System” account, this authorization is not implicitly defined. Therefore, you must configure the Agent to run as an account that is authorized to access the DHCP server. This account can be a Domain user or it could be a local user, just as long as the DHCP authorizations allow that local or domain account “Write” or “Full Control” access to the DHCP server.

To modify what account a service runs as, follow these steps.

1. Open up the Window Services dialog (**Start > Program Files > Administrative Tools > Services**).

2. Highlight the IPAM Agent, right-click and select **Properties**.
3. Select the **Log On** tab.
4. Select the **This Account** option, and enter the user account and password for either a Windows Domain Account or a Local User that has access rights to the DHCP server.
5. Click **OK**.

Running the Agent as something other than the local SYSTEM account should not have an adverse effects on other Agent functions. IPAM is not impeded by and does not use or rely on Windows authentication.

IPAM Procedure

To manage the Windows DHCP configuration, a new Network Service and Agent must be added within IPAM. Follow these steps

Add Agent for MS Windows Server

Within IPAM, the Agent for the Windows Server box must be registered.

1. Select **Agents** from the Tools menu and click on **Add Agent**. Define an MS DHCP Agent and assign an IP address.

Create the DHCP Network Service

2. Define the MS DHCP network service by selecting **Servers/Services** from the DHCP section of the **Management** menu.
3. Select **Add Network Services** and add the path for the DHCP configuration and lease files in the **General** tab. You can choose either Microsoft DHCP or Microsoft 2008 DHCP as the Product Name.
4. In the **Configuration** tab, select the Microsoft Windows choices for the Option and Policy sets.

Create Address Pools

5. Address Pools need to be created for dynamic assignment. Refer to “Address Pool Allocation Template” on page 233 for more information.

Deployment

6. Once the DHCP Network Service and Remote Agent are defined, initiate the DHCP Push task by selecting **Configuration/Deployment** from the DHCP section of the **Management** menu and selecting **DHCP Configuration – All Files** as the **Task Type**.

Configuring DHCP Failover

DHCP failover is a protocol designed to allow a backup (Failover) DHCP server to take over for a main DHCP server (Primary) if the primary server is taken off the network for any reason. You can use DHCP failover to configure two DHCP servers to operate as a redundant pair (failover peers).

Note: DHCP failover is not currently supported for DHCPv6 servers.

The INS DHCP server, working in conjunction with a powerful management tool such as IPAM, offers the unprecedented ability to configure simple or complex failover scenarios that are easy to manage.

As always, best practices for DHCP failover is to make your configuration as simple as possible, based on your unique requirements for your network.

Failover Scenarios

There are two basic scenarios for DHCP failover:

- **Simple Failover** - One server acting as the primary, and its partner acting as backup.
- **Many to One Failover** - Two or more primary DHCP servers having the same failover (backup) server.

Simple Failover

Simple failover involves a single primary server and a single failover server pair. In this example, both servers are configured with the same DHCP Scopes.

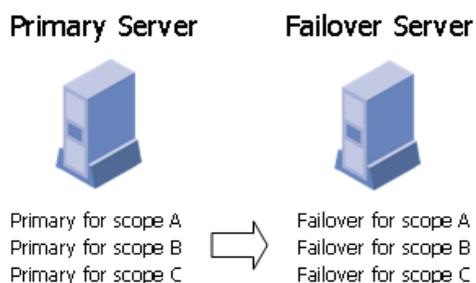


Figure 12-9 Simple Failover

The advantages of simple failover over the other scenarios are:

- You can set the failover properties within IPAM at the subnet level and you do not need to worry about managing failover settings at the individual IP Address, or IP Address Pool (scope) level.
- It is the easiest to manage as the network changes, as it is the simplest to understand, configure, and has the fewest messages.
- Provides the greatest performance benefits.

Many to One Failover

Many to One failover involves two (or more) primary DHCP servers that share a single failover server.

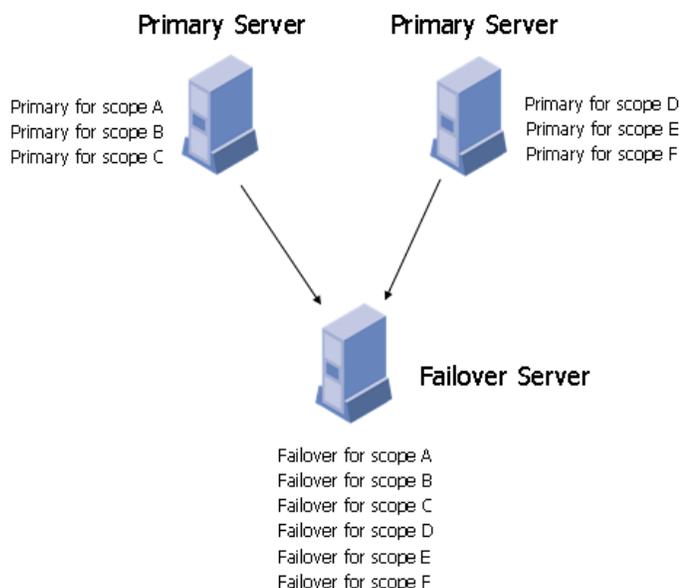


Figure 12-10 Many to One Failover

The advantages of many to one failover over the other scenarios are:

- It reduces the number of servers managed. You do not need to put a pair of servers (both primary and failover) in each location where you want to utilize failover.

There are some disadvantages of many to one failover over the other scenarios which include:

- The backup server must be sized to handle the sum of the configurations.

Failover Checklist

Use this checklist to prepare for an effective failover configuration:

- Design your failover strategy by selecting which type of failover scenario you will be using.
- Define your common DHCP Options Sets and DHCP Policy Sets.
- Decide on the Peering relationships that you will be using, and decide on the communication parameters that will be used between the peers.
- Duplicate the scope, policy, DHCP option, and address configurations on the partner servers. This is accomplished automatically when you perform a configuration creation task utilizing IPAM.
- Ensure that both partners are configured with a wide enough range of addresses so that the failover server can provide leases while the primary server is down for a reasonable amount of time.

- If you change any of the following configurations on the primary server, also change them on the failover server:
 - ▶ IP Addresses, IP Address Pools, IP Address Ranges
 - ▶ Subnet Profiles for subnets containing Dynamic DHCP Addresses
 - ▶ DHCP Policy Sets
 - ▶ DHCP Option Sets
 - ▶ Peer Relationship communication parameters
 - ▶ User Classes / Client-classes
 - ▶ Dynamic DNS update policies
 - ▶ DHCP extensions
- If you use BOOTP /DHCP relays (IP helpers), configure all BOOTP/DHCP relay agents to point to both partners. This cannot be detected by IPAM or by the DHCP server. You can only detect BOOTP/DHCP configuration errors by performing live tests in which you periodically take the primary server out of service to verify that the failover server is available to DHCP clients.

Configuring Failover within IPAM

You can use the IPAM web interface to configure DHCP failover server pairs. The types of configuration options supported by managing failover server pairs are:

- Policy properties and DHCP options, including vendor-specific options
- DHCP server properties
- Scope properties and ranges
- Clients and client-classes
- DHCP Extensions

To add a failover pair, you must set the failover attributes on the DHCP server or scope level.

Configuring IPAM for Failovers

To configure IPAM for failover servers, perform the following steps:

1. Choose from the following actions.

To configure a...	Then...
Simple Failover	Define two DHCP servers (select Servers/Services from the DHCP section of the Management menu).
Many to One Failover	Define at least three DHCP servers (select Servers/Services from the DHCP section of the Management menu).

2. Create and assign the same DHCP Policy Sets, DHCP Option Sets, and DHCP Client Classes for each server. **Policy Sets**, **Option Sets**, and **Client Classes** are all created from the DHCP section of the **Management** menu.
3. Within each Primary Server's configuration, define the DHCP Failover Peer. In the My Failover Peers section of the **Failover Peer** tab, select the **Add Failover Peer** link.
The Add Failover Peer screen opens.
4. Select the failover peer server from the **Peer Server** drop-down list. Note that the failover server must already be defined as a DHCP server within IPAM, before you can assign it to a primary as a peer.
5. Define a Block/Subnet to hold the DHCP address scopes (select **Container View** from the **Management** menu and after you have selected a Container in the hierarchy, click **Add Child Block**). In the **Policy** tab, select the **Primary DHCP Server** and **Failover DHCP Server** to be used for this subnet. Also select the **DHCP Policy Set** and **DHCP Option Set** to be used for this subnet. Click **Submit** to save.
6. Select the container you just created by clicking on the IP Address. Select Define IP Addresses, IP Address Ranges, or IP Address Pools to make the desired IP address configuration. Note that you do not need to select the Primary DHCP Server, Failover DHCP Server, DHCP Policy Set, or DHCP Option Set. These can all default from the Subnet Profile that was defined in step 3, which simplifies your management over these IP Addresses. For example, if you want change any of the settings for all IP Addresses within this subnet; you can simply change the subnet profile to effect the change on all IP Addresses.
7. Perform a DHCP Configuration File Generation by selecting **Configuration/Deployment** from the DHCP section of the **Management** menu and creating configuration files for the primary and failover DHCP servers.

Administrator Access Control Use Cases

This section outlines some general Access Control use cases and how to configure either Administrator or Administrator Role policies to handle them.

Use Case - Regional Administrators

Problem

You have administrators that should only have access to Containers and Blocks within a specific region, say North America. Furthermore, some administrators should be able to modify items within North America, but require Read-only access to both Europe and Asia.

Solution

1. Create a role that specifies the Authorized Functions for this type of administrator, but specifies no other Access Control Lists or Domain Access. Call this `Regional Functions`.
2. Create another role that contains no Authorized Functions, but specifies North America in the Access Control List with full rights (that is, Read, Write, Delete, and Apply to Children). No other containers are listed in the Access Control List. Call this `Regional North America - Full Access`.
3. Create another role that contains no Authorized Functions, but specifies Europe in the Access Control List with only Read and Apply to Children access specified. No other containers are listed in the Access Control List. Call this `Regional Europe - Read Only`.
4. Create another role that contains no Authorized Functions, but specifies Asia in the Access Control List with only Read and Apply to Children access specified. No other containers are listed in the Access Control List. Call this `Regional Asia - Read Only`.
5. Create one or more Administrators using the combination of these four roles.

Benefits

- All Regional administrators would be given the same set of Authorized Functions. And changing this set of Authorized Functions once would propagate to all Regional Administrators automatically.
- The Administrators defined with this set of roles would have Full Access to blocks and containers within North America, and would be able to view all of the blocks and containers within Europe and Asia but could not modify them.
- Following this pattern of roles, different types of Administrators could be created easily with a mix of Full vs. Read Only access rights to each region.

Use Case - Specific Block Access Required

Problem

An administrator who is not to be granted access to a particular block type on a global basis needs access to a specific block of the denied type.

For instance, the administrator is denied access to blocks of type “Infrastructure”, but needs access to the specific block 192.168.2.0/24 in container “Miami”.

Solution

Using one of the roles specified for the given administrator (or create a new role and assign it to the Administrator), add the Container “Miami” to the Access Control List with only Read access turned on. Then add the block “192.168.2.0/24” and grant full rights.

Benefits

Using this approach the Administrator will gain access to the block necessary, but at the same time be restricted from accessing other Infrastructure blocks.

Use Case - DNS Administrator

Problem

The customer has administrators that solely handle DNS administration and they would like to assign specific Domains to groups of DNS Administrators.

One group of DNS Administrators controls all domains under “subsidiary1.com” and the “23.43.in-addr.arpa” reverse domain. Another group controls all domains under “company.com” and the “43.in-addr.arpa” reverse domain.

Solution

A privileged administrator would create a “functional” role that defined Authorized Functions which limited the user to mainly DNS related functions. We’ll call this role “DNS Functional” as an example. This role has no Containers or Domains specified in its Access Control Lists.

Another role would be created with all Authorized Function check boxes turned off and only the “subsidiary1.com” and “23.43.in-addr.arpa” domains specified on the Domain Access Control tab. This role would be called “DNS Domain subsidiary1.com” for example.

Another role would be created with all Authorized Function check boxes turned off and only the “company.com” and “43.in-addr.arpa” domains specified on the Domain Access Control tab. This role would be called “DNS Domain company.com” for example.

Finally, one set of Administrators would be created with the Administrator Roles of “DNS Functional” and “DNS Domain subsidiary1.com”. While the second set would be created using the roles of “DNS Functional and “DNS Domain company.com”.

Benefits

- This approach saves the privileged administrator from having to remember to set each of the “DNS Domain *” roles with the same Authorized Functions since the “DNS Functional” role is shared by all DNS Administrators.
- Following this pattern, if an administrator needed access to both subsidiary1.com and company.com as well as the reverse domains, the above roles could easily be added to that administrator’s profile and the administrator would immediately gain access to these domains.

Use Case - Third Party Access

Problem

Some organizations, especially ISPs, may wish to allow their customers to have access to IPAM in an effort to let them manage their own address blocks or domains. However, they

do not wish to create an Administrator Role and an Administrator for each client. Furthermore, it is likely to be the case that these third party administrators would all have the same functional access, but would differ only on the objects (Blocks, Domains, Containers, etc.) they could access.

Solution

Create a “Customer Function” role that defined just the Authorized Functions to be assigned to 3rd party administrators. Then, for each customer, create an Administrator using the Customer Function role. In addition, assign the appropriate objects (Blocks, Domains, and / or Containers) to the Administrator itself.

Benefits

- All 3rd party administrators would automatically get the same level of functional access to the system. Changes made once would be propagated to all administrators using the role.
- The need to create a separate Administrator Role for each Administrator is eliminated.

Supported RFCs

IP Addressing

- [RFC2373](#) IP Version 6 Addressing Architecture
- [RFC1918](#) Address Allocation for Private Internets

DHCP

- [RFC2131](#) Dynamic Host Configuration Protocol
- [RFC2132](#) DHCP Options and BOOTP Vendor Extensions
- [RFC3315](#) Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- [RFC3633](#) IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

DNS

- [RFC1034](#) Domain Names – Concepts and Facilities
- [RFC1035](#) Domain Names – Implementation and Specifications
- [RFC1995](#) Incremental Zone Transfer in DNS
- [RFC1996](#) Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- [RFC2136](#) Dynamic Updates in the Domain Name System (DNS UPDATE)
- [RFC2317](#) Classless IN-ADDR.ARPA delegation
- [RFC2782](#) A DNS RR for specifying the location of services (DNS SRV)

Other

- [RFC 2050](#) Internet Registry IP Allocation Guidelines

Appendix A: Resource Records and Workflow

Table A 1 Approver Actions

Current State	Admin Action	Result
Free (non-existent)	Create	A new record is created that does not need approval.
Approved	Update	The updated record is saved and does not need approval.
Approved	Delete	The record is deleted and does not need approval.
Pending Create	Update	Approver's changes are saved and record is approved.
Pending Create	Delete	Record is deleted.
Pending Update	Update	Approver's changes are merged with pending changes and record is approved. In case of conflicts, approver's changes prevail.
Pending Update	Delete	Record is deleted.
Pending Delete	Update	Approver's changes are saved and the pending Delete is in effect rejected.
Pending Delete	Delete	Record is deleted.

Table A 2 Non-Approver Actions

Current State	Admin Action	Result
Free(non-existent)	Create	A new record is created that requires approval, new state is Pending Create.
Approved	Update	A new record with updated values is created with the state as Pending Update.
Approved	Delete	The record is marked for deletion and needs approval.
Pending Create	Update	The pending record is updated with the new values but the state is still Pending Create.
Pending Create	Delete	The pending record is deleted.
Pending Update	Update	The pending record is updated with the new values but the state is still Pending Update.
Pending Update	Delete	State is changed from a pending update to a pending delete and it needs approval.
Pending Delete	Update	State is changed from a pending delete to a pending update and it needs approval.
Pending Delete	Delete	No change.