



CHAPTER 10

Configuring Address Pools

Service providers concerned with the efficient management of IP address space are challenged to implement an address assignment mechanism that efficiently assigns addresses to remote users from address pools and effectively manages those pools. Such deployment requires a strategy for dealing with poorly utilized address pools and pools that run out of addresses. Each remote user assigned an address must have a route to the remote user configured in the corresponding virtual routing and forwarding (VRF) instance. Configuration becomes further complicated by the fact that a single PE router can support hundreds of VRFs, and the provider's network can have hundreds or thousands of PE routers. The total number of routes in all VRFs and in the default routing table on a single PE router can grow enormously, highlighting the need for an address mechanism that provides for route summarization.

To enhance IP address space management, the Cisco 10000 series router supports the following address pool features:

- [On-Demand Address Pool Manager, page 10-4](#)—Provides an address assignment mechanism that dynamically resizes address pools and permits efficient route summarization.
- [Overlapping IP Address Pools, page 10-16](#)—Enables you to use multiple IP address spaces and reuse IP addresses among different VPNs supported on the Cisco 10000 series router.

This chapter describes the advantages and disadvantages of address assignment mechanisms currently deployed, the On-demand Address Pool Manager feature, and the Overlapping IP Address Pools feature:

- [Address Assignment Mechanisms, page 10-1](#)
- [On-Demand Address Pool Manager, page 10-4](#)
- [Overlapping IP Address Pools, page 10-16](#)

Address Assignment Mechanisms

Typically, service providers deploy the following address assignment mechanisms:

- [Local Address Pool, page 10-2](#)
- [RADIUS-Based Address Assignment, page 10-2](#)
- [DHCP-Based Address Assignment, page 10-3](#)

The following sections describe the advantages and disadvantages of the address assignment mechanisms.

Local Address Pool

A local address pool is a pool of IP addresses statically configured on a PE router. The pool name identifies the address pool. When a PPP session requests an address from a specific pool, the pool manager assigns an unused address from the pool. When the PPP session returns the address, the pool manager puts the address back into the pool from which it was taken.

A common group identifier identifies a group of pools. In an MPLS VPN network architecture, each pool group is used to assign addresses to remote users belonging to a particular VPN. Though not officially associated with a VRF, the address pool is unofficially tied to the VRF because each VPN associated with an address pool is also associated with a specific VRF.

The ability to assign overlapping addresses provides a significant benefit to VPN customers who use private addresses. Two address pools in different groups can have overlapping IP addresses, but two pools in the same group cannot contain overlapping addresses.

Benefits of a Local Address Pool

The main benefit of a local address pool is the ability to efficiently summarize routes:

- The total number of routes configured on a single PE router can grow enormously. Route summarization avoids lengthy VRF and default routing tables.
- Summarized routes correspond to all subnets present in the address pool.
- The summarized routes are configured in the VRF associated with the address pool.

Limitations of a Local Address Pool

A drawback to local address pools is that because they are statically configured, the pool might be poorly utilized or it might run out of addresses. The provider's ISP customers have a limited number of public addresses and are particularly affected by poorly managed pools. For example, for the same ISP it is possible that one PE router is underutilizing its local pool while another PE router has exhausted its local pool.

RADIUS-Based Address Assignment

RADIUS is a distributed client/server system that secures networks against unauthorized access. In addition to providing authentication, authorization, and accounting (AAA) services, RADIUS also provides IP address assignment by using user defined static routes and IP pool definitions on the RADIUS server.

In the Cisco 10000 series router implementation, a RADIUS client runs on the router and queries a central RADIUS server for a remote user's static route or an IP address from the RADIUS IP pool definitions. Typically, the RADIUS server assigns addresses from a separate pool of addresses for each VPN associated with a particular PE router. This allows the server to assign contiguous addresses to remote users who are in the same VPN and who connect to the same PE router. The RADIUS server uses the remote user's domain name to identify the VPN.

Benefits of RADIUS-Based Address Assignment

RADIUS is an effective mechanism for providing IP address assignment for remote users:

- One benefit of RADIUS-based address assignment is its ability to effectively manage the IP address pools configured on the server. RADIUS can dynamically resize pools as needed, removing addresses from poorly utilized pools and adding them to pools that run out of addresses.
- RADIUS supports route summarization and uses profiles configured on the server to provide efficient addressing and AAA services.
- RADIUS can also attach a fixed IP address to a remote user's login.

Limitations of RADIUS-Based Address Assignment

When deciding upon an addressing mechanism, you must weigh the limitations and benefits of RADIUS-based address assignment. The following are some of the limitations of RADIUS-based address assignment:

- Using RADIUS for address assignment can increase the load on the server and slow the server's performance.
- As remote users log on and off, route summarization can become less efficient because it becomes more difficult for the PE router to have a contiguous set of IP addresses that the PE can summarize to the RADIUS server.
- Each time a user logs on or off, the Border Gateway Protocol (BGP) sends update information to the PE routers to update the VRFs configured on each router.
- Remote users have limited connectivity during the time it takes for BGP to propagate a newly configured route to all PE routers.

DHCP-Based Address Assignment

Dynamic Host Configuration Protocol (DHCP) servers allocate IP addresses to remote users, eliminating the need to configure users individually. DHCP also provides all the parameters that user systems require to operate and exchange information on the Internet network to which they connect. DHCP is based on a client/server model. The client software runs on the user system and the server software runs on the DHCP server.

DHCP uses a lease mechanism that offers an automated, reliable, and safe method for distributing and reusing addresses in networks, with little need for administrative intervention. As a system administrator, you can tailor the lease policy to meet the specific needs of your network.

Leases are grouped together in an address pool called a *scope*. The scope defines the set of IP addresses available for requesting hosts. A lease can be reserved (the host always receives the same IP address) or dynamic (the host receives the next available, unassigned lease in the scope).

Benefits of DHCP-based Address Assignment

One of the most significant benefits of DHCP is that it can dynamically configure user systems with IP addresses and associate leases with the assigned addresses. DHCP also provides for multiple servers. You can configure redundant DHCP servers so that if one server cannot provide leases to requesting clients, the other one can take over. Existing DHCP clients can continue to keep and renew their leases without knowing which server is responding to their requests.

Limitations of DHCP-Based Address Assignment

DHCP-based address assignment has route summarization problems similar to the problems encountered with RADIUS-based address assignment. Route summarization becomes less efficient as remote users log on and off, and users have limited connectivity while BGP updates all of the PE routers with newly configured routes.

For more information, see the [“RADIUS-Based Address Assignment”](#) section on page 10-2.

On-Demand Address Pool Manager

The On-demand Address Pool Manager feature is a mechanism for assigning and managing IP addresses.

On-demand address pools (ODAPs) use a central server to manage a block of addresses for each customer. The central server can be a Dynamic Host Configuration Protocol (DHCP) server or a RADIUS server. After the ODAP is configured, the central server populates the ODAP with one or more subnets leased from the central server. The central server divides each address pool into subnets and assigns the subnets to PE routers upon request.

**Note**

The Cisco Network Registrar (CNR) DHCP server and the Cisco Access Registrar (CAR) RADIUS server support ODAPs.

The customer site connects to a provider edge (PE) router in the provider network. When an ODAP is configured, the pool manager for the PE router initiates a request to the central server for an initial subnet for a specific ODAP. The pool manager then monitors the utilization of the ODAP.

If the utilization of the pool exceeds a high-utilization threshold (high-utilization mark), the pool manager requests an additional subnet from the central server and adds it to the ODAP. Similarly, if the utilization of the pool decreases below the low-utilization threshold (low-utilization mark), the pool manager returns one or more subnets to the central server from which it was originally leased. Each time subnets are added to or removed from the ODAP, the summarized routes for each leased subnet must be inserted or removed from the corresponding VRF.

The On-demand Address Pool Manager feature is described in the following topics:

- [Feature History for On-Demand Address Pool Manager](#), page 10-5
- [Address Allocation for PPP Sessions](#), page 10-5
- [Subnet Releasing](#), page 10-5
- [On-Demand Address Pools for MPLS VPNs](#), page 10-5
- [Benefits On-Demand Address Pool Manager](#), page 10-6
- [Prerequisites for On-Demand Address Pool Manager](#), page 10-6
- [Required Configuration Tasks for On-Demand Address Pool Manager](#), page 10-6
- [Optional Configuration Tasks for On-Demand Address Pool Manager](#), page 10-10
- [Verifying On-Demand Address Pool Operation](#), page 10-12
- [Configuration Examples for On-Demand Address Pool Manager](#), page 10-14
- [Monitoring and Maintaining an On-Demand Address Pool](#), page 10-15

Feature History for On-Demand Address Pool Manager

Cisco IOS Release	Description	Required PRE
12.2(15)BX	This feature was introduced on the Cisco 10000 series router.	PRE2
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7)XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Address Allocation for PPP Sessions

For individual address allocation for PPP sessions, the pool manager searches for a free address beginning with the very first leased subnet. If a free address is not available in the first subnet, the pool manager searches the second leased subnet, and so on until a free address is found. This method of address allocation allows for efficient subnet release and route summarization. However, it differs from the normal DHCP address selection policy in which the IP address of the receiving interface is taken into account. The on-demand address pool manager feature provides an IP address pooling mechanism for PPP that allows the DHCP server to distinguish between a normal DHCP address request and an address request for a PPP client.

Subnet Releasing

The pool manager releases subnets beginning with the last leased subnet. The pool manager searches for a releasable subnet—a subnet with no addresses currently being leased. If it finds a releasable subnet, it releases the subnet and removes the summarized route for that subnet. If more than one releasable subnet exists, the pool manager releases the most recently allocated subnet. The pool manager takes no action if it does not find a releasable subnet. If the high utilization mark is reached by releasing the subnet, the pool manager does not release the subnet. Regardless of the instantaneous utilization level, the pool manager never releases the first leased subnet until it disables the ODAP.

On-Demand Address Pools for MPLS VPNs

The on-demand address pool manager feature provides support for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environments. This feature automates the resizing of address pools, reducing network loading and manual configuration.

Each ODAP is configured and associated with a specific MPLS VPN. Each VPN is associated with one or more VRFs. The VRF maintains a routing table and other information associated with a specific customer VPN site. The utilization of the on-demand address pool occurs as described in the [“On-Demand Address Pool Manager” section on page 10-4](#), except that address allocation occurs within the VRF associated with a particular VPN.

Only the ODAP associated with a specific VPN can allocate addresses to PPP sessions belonging to that VPN. The PE router on which the ODAP is configured terminates the PPP sessions and maps the remote user to the corresponding MPLS VPNs.

**Note**

For more information about ODAPs, see the [“On-Demand Address Pool Manager” section on page 10-4](#). For information about configuring MPLS VPNs, see the Remote Access to MPLS VPN chapter or see the *Cisco IOS Switching Services Configuration Guide*, Release 12.2.

The On-demand Address Pools for MPLS VPNs feature is described in the following topics:

Benefits On-Demand Address Pool Manager

The on-demand address pool manager feature provides:

- Dynamic resizing of IP address pools, increasing or reducing the size of the pool as needed
- Automated control of address assignment
- Easy monitoring capabilities, enabling the pool manager to assess address utilization
- Support for MPLS VPNs with addresses assigned per subnet, per interface (see the [“On-Demand Address Pools for MPLS VPNs” section on page 10-5](#))
- Simplified VPN setup, enabling the pool manager to request an initial subnet from the address pool server upon configuration of the on-demand address pool (ODAP)

Prerequisites for On-Demand Address Pool Manager

The on-demand address pool manager feature has the following requirements:

- You can choose to specify a VRF for an ODAP. If you do, you must configure the VRF first and then configure the VRF in the ODAP. If you do not configure a VRF in the pool, the pool is assumed to be in the global address space.
- The VRF of the PPP session must match the VRF configured in the pool. To ensure that it does, configure a virtual template interface using the **ip vrf forwarding** command. If you use AAA to authorize the PPP user, you can include the VRF in the user profile configuration on the RADIUS server.

**Note**

For more information about configuring AAA, see the *Cisco IOS Security Configuration Guide*, Release 12.2.

Required Configuration Tasks for On-Demand Address Pool Manager

To configure the on-demand address pool manager feature, perform the following required configuration tasks:

- [Defining DHCP ODAPs as the Global Default Pooling Mechanism, page 10-7](#)
- [Configuring the DHCP Pool as an ODAP, page 10-7](#)
- [Configuring the AAA Client, page 10-8](#)
- [Configuring RADIUS, page 10-9](#)

Defining DHCP ODAPs as the Global Default Pooling Mechanism

To specify on-demand address pooling as the global default mechanism, enter the following command in global configuration mode:

Command	Purpose
Router(config)# ip address-pool dhcp-pool	Enables on-demand address pooling as the global default IP address mechanism for PPP remote access sessions into MPLS VPNs. Locally configured VRF-associated DHCP pools allocate IP addresses.



Note

The DHCP server needs to be able to distinguish between a normal DHCP address request and an address request for a PPP client. For more information, see the [“Address Allocation for PPP Sessions” section on page 10-5](#).

Example 10-1 enables on-demand address pooling as the mechanism to service address requests from PPP clients. The locally configured VRF-associated DHCP pool named `Green_pool` provides the IP addresses.

Example 10-1 Defining DHCP ODAPs as the Global Default Pooling Mechanism

```
!
ip address-pool dhcp-pool
!
ip dhcp pool Green_pool
!
```

Configuring the DHCP Pool as an ODAP

To configure a DHCP pool as an on-demand address pool, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip dhcp pool name	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 2	Router(config-dhcp)# vrf name	Associates the address pool with a VRF.
Step 3	Router(config-dhcp)# origin {dhcp aaa ipcp} [subnet size initial size [autogrow size]]	Configures an address pool as an on-demand address pool.
Step 4	Router(config-dhcp)# utilizationmark low percentage-number	Sets the low utilization mark of the pool size. The default value is zero percent.
Step 5	Router(config-dhcp)# utilization mark high percentage-number	Sets the high utilization mark of the pool size. The default value is 100 percent.

Example 10-2 configures two on-demand DHCP address pools: `green_pool` and `red_pool`. The `green_pool` address pool is associated with the `Green` VRF and the `red_pool` address pool is associated with the `Red` VRF. Both pools obtain their subnet addresses from an external DHCP server.

Example 10-2 Configuring the DHCP Pool as an ODAP

```

!
ip dhcp pool green_pool
  vrf Green
  utilization mark high 60
  utilization mark low 40
  origin dhcp subnet size initial /24 autogrow /24
!
ip dhcp pool red_pool
  vrf Red
  origin dhcp
!
ip vrf Green
  rd 200:1
  route-target export 200:1
  route-target import 200:1
!
ip vrf Red
  rd 300:1
  route-target export 300:1
  route-target import 300:1
ip address-pool dhcp-pool
!
interface Virtual-Template1
  ip vrf forwarding Green
  ip unnumbered Loopback1
  ppp authentication chap
!
interface Virtual-Template4
  ip vrf forwarding Red
  ip unnumbered Loopback2
  ppp authentication chap
!

```

Configuring the AAA Client

To allow an ODAP to obtain subnets from the RADIUS server, enter the following commands in global configuration mode. These commands configure the AAA client on the Cisco 10000 router:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA access control.
Step 2	Router(config)# aaa authorization configuration default group radius	Downloads static route configuration information from the AAA server using RADIUS.
Step 3	Router(config)# aaa accounting network default start-stop radius or Router(config)# aaa accounting network default stop-only radius	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. Sends a <i>start</i> accounting notice at the beginning of a process. Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. Sends a <i>stop</i> accounting notice at the end of the requested user process.
Step 4	Router(config)# aaa session-id common	Ensures that the same session ID is used for each AAA accounting service type within a call.

For an example of how to configure AAA, see [Example 10-3](#) in the “Configuring RADIUS” section on [page 10-9](#).

Configuring RADIUS

To configure RADIUS on the Cisco 10000 router, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip radius source-interface <i>subinterface-name</i>	Forces the Cisco 10000 router to use the IP address of the specified interface for all outgoing RADIUS packets.
Step 2	Router(config)# radius-server host <i>ip-address</i> auth-port <i>port-number</i> acct-port <i>port-number</i>	Specifies a RADIUS server host.
Step 3	Router(config)# radius server attribute 32 include-in-access-req	Sends RADIUS attribute 32 (NAS-Identifier) in an access request or accounting request.
Step 4	Router(config)# radius server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in an access request or accounting request.
Step 5	Router(config)# radius-server vsa send accounting	Configures the Cisco 10000 router, acting as the network access server (NAS), to recognize and use vendor-specific accounting attributes.
Step 6	Router(config)# radius-server vsa send authentication	Configures the Cisco 10000 router (NAS) to recognize and use vendor-specific authentication attributes.

[Example 10-3](#) configures an address pool named *Green* and a RADIUS server from which the *Green* address pool obtains its subnets. The RADIUS server is located at the IP address 172.16.1.1.

Example 10-3 Configuring AAA and RADIUS

```

!
aaa new-model
!
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa session-id common
!
ip subnet-zero
!
ip dhcp ping packets 0
!
ip dhcp pool Green
    vrf Green
    utilization mark high 50
    utilization mark low 30
    origin aaa subnet size initial /28 autogrow /28
!
ip vrf Green
    rd 300:1
    route-target export 300:1
    route-target import 300:1
!
interface Ethernet1/1
    ip address 172.16.1.12 255.255.255.0
    duplex half

```

```

!
interface Virtual-Template1
  ip vrf forwarding Green
  no ip address
!
ip radius source-interface Ethernet1/1
!
!IP address of the Radius server host
radius-server host 172.16.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 32 include-in-access-req
radius-server attribute 44 include-in-access-req
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication

```

Optional Configuration Tasks for On-Demand Address Pool Manager

To configure the on-demand address pool manager feature, perform any of the following optional configuration tasks:

- [Defining ODAPs on an Interface, page 10-10](#)
- [Configuring ODAPs to Obtain Subnets Through IPCP Negotiation, page 10-11](#)
- [Disabling ODAPs, page 10-11](#)

Defining ODAPs on an Interface

To configure the on-demand address pool manager feature on an interface, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>name</i>	Specifies the interface and enters interface configuration mode.
Step 2	Router(config-if)# peer default ip address dhcp-pool	Specifies to return an IP address from an on-demand address pool to a remote peer connecting to the interface. This command supports only remote access (PPP) sessions into MPLS VPNs.



Note

When you configure the on-demand address pool mechanism on an interface-by-interface basis, the ODAP overrides the global default address pool mechanism configured on the interface.

Configuring ODAPs to Obtain Subnets Through IPCP Negotiation



Note

When you assign an IP address pool to customer premise equipment (CPE), the pool manager assigns IP addresses to the CPE devices and to a DHCP pool. To use the ODAP functionality requires the following:

- The Cisco IOS CPE device must be able to request and use the subnet.
- The RADIUS server using AAA must be able to provide the subnet and insert the framed route into the proper VRF table.
- The PE router must be able to facilitate providing the subnet through IPCP.

To configure an on-demand address pool with the IP Control Protocol (IPCP) as the subnet allocation protocol, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip dhcp pool <i>name</i>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 2	Router(config-dhcp)# import all	Imports option parameters into the Cisco IOS DHCP server database.
Step 3	Router(config-dhcp)# origin ipcp	Configures an address pool as an on-demand address pool by using IPCP as the subnet allocation protocol.
Step 4	Router(config-dhcp)# exit	Exits DHCP pool configuration mode.
Step 5	Router(config)# interface <i>type</i>	Selects an interface and enters interface configuration mode.
Step 6	Router(Config-if)# ip address pool <i>name</i>	Indicates to automatically configure the interface's IP address from the specified pool. Note The pool must be populated with a subnet from IPCP.

Disabling ODAPs

To disable an ODAP from a DHCP pool, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip dhcp pool <i>name</i>	Enters DHCP pool configuration mode for the DHCP address pool indicated.
Step 2	Router(config-if)# no origin { dhcp aaa ipcp }	Disables the ODAP



Note

When you disable an ODAP, all leased subnets are released. If active PPP sessions are using addresses from the released subnets, those sessions are reset. DHCP clients leasing addresses from the released subnets are not able to renew their leases.

Example 10-4 disables the on-demand DHCP pool named *test_pool*.

Example 10-4 Disabling ODAPs

```
!
ip dhcp pool test_pool
  import all
  no origin ipcp
!
```

Verifying On-Demand Address Pool Operation

To verify ODAP operation, enter the following commands in privileged EXEC mode:

Command	Purpose
Router# show ip dhcp pool	Displays information about all pools configured, such as high and low utilization mark, subnet size, VRF name, total addresses, and leased addresses.
Router# show ip dhcp pool name	Displays information about the specified pool, such as high and low utilization mark, subnet size, VRF name, total addresses, and leased addresses.
Router# show ip dhcp binding	Displays binding information for pools associated with a VRF, such as IP address, hardware address, lease expiration, and type of pool.

Example 10-5 uses the **show ip dhcp pool** command to display information for two DHCP pools: *Green* and *Global*. The *Green* pool configuration indicates:

- Autogrow—Obtain more subnets when the high-utilization mark is reached.
- Subnet size—Indicates the initial and incremental subnet sizes that the *Green* pool can request. These are the values configured using the **origin** command.
- VRF name—Indicates that the *Green* pool is associated with the *Green* VRF.
- Total addresses—Count of all the usable addresses in the pool.
- Leased addresses—Total count of the number of bindings created from the pool.
- Pending event: subnet request—Indicates that a subnet request is pending for the pool. The subnet request was scheduled because the Leased addresses count exceeds the high-utilization mark of the pool.
- Current index—Indicates the subnet address to be allocated next to the pool. In Example 10-5, three subnets are currently added. The Current index for the first two subnets is 0.0.0.0, indicating that each of these subnets has used all its available addresses.



Note The *Green* pool and the *Global* pool have the same 172.16.0.1 subnet allocated, which is acceptable because the *Green* pool is associated with the *Green* VRF and the *Global* pool is configured in the global address space.

- IP address range—Indicates the range of usable addresses from the subnet.
- Leased addresses—Indicates the individual count of bindings created from each subnet.

Example 10-5 show ip dhcp pool Command

```
Router# show ip dhcp pool

Pool Green :
  Utilization mark (high/low): 50 / 30
  Subnet size (first/next): 24 / 24 (autogrow)
  VRF name: Green
  Total addresses: 18
  Leased addresses: 13
  Pending event subnet request
  3 subnets are currently in the pool :
  Current indexIP address rangeLeased addresses
  0.0.0.0178.16.0.1- 172.16.0.66
  0.0.0.0172.16.0.9- 172.16.0.146
  172.16.0.17172.16.0.17- 172.16.0.221
Pool Global :
  Utilization mark (high/low): 100 / 0
  Subnet size (first/next): 24 / 24 (autogrow)
  Total addresses: 6
  Leased addresses: 0
  Pending event: none
  1 subnet is currently in the pool :
  Current indexIP address rangeLeased addresses
  172.16.0.1172.16.0.1- 172.16.0.60
```

Example 10-6 uses the **show ip dhcp binding** command to display the bindings from the *Green* pool. The example indicates the following:

- **Type: On-demand**—Indicates that the address binding is created for a PPP session.
- **Lease expiration: Infinite**—Indicates that the binding is valid as long as the session is up. If a subnet must be released back to the leasing server while the session is still up, the session is reset so that it is forced to obtain a new IP address.
- **Hardware address**—Indicates the session identifier that PPP detected for an on-demand entry.

**Note**

Example 10-6 does not display any bindings from pools not associated with a VRF because the global pool has not allocated any addresses.

Example 10-6 show ip dhcp binding Command

```

Router# show ip dhcp binding
Bindings from all pools not associated with VRF :
IP addressHardware addressLease expirationType

Bindings from VRF pool Green :
IP addressHardware addressLease expirationType
172.16.0.15674.312d.7465.7374.InfiniteOn-demand
2d38.3930.39
172.16.0.25674.312d.7465.7374.InfiniteOn-demand
2d38.3839.31
172.16.0.35674.312d.7465.7374.InfiniteOn-demand
2d36.3432.34
172.16.0.45674.312d.7465.7374.InfiniteOn-demand
2d38.3236.34
172.16.0.55674.312d.7465.7374.InfiniteOn-demand
2d34.3331.37
172.16.0.65674.312d.7465.7374.InfiniteOn-demand
2d37.3237.39
172.16.0.95674.312d.7465.7374.InfiniteOn-demand
2d39.3732.36
172.16.0.105674.312d.7465.7374.InfiniteOn-demand
2d31.3637
172.16.0.115674.312d.7465.7374.InfiniteOn-demand
2d39.3137.36
172.16.0.125674.312d.7465.7374.InfiniteOn-demand
2d37.3838.30
172.16.0.135674.312d.7465.7374.InfiniteOn-demand
2d32.3339.37
172.16.0.145674.312d.7465.7374.InfiniteOn-demand
2d31.3038.31
172.16.0.175674.312d.7465.7374.InfiniteOn-demand
2d38.3832.38
172.16.0.185674.312d.7465.7374.InfiniteOn-demand
2d32.3736.31

```

Configuration Examples for On-Demand Address Pool Manager

This section provides the following configuration examples:

- [Configuring DHCP ODAPs on an Interface, page 10-14](#)
- [Configuring ODAPs to Obtain Subnets Through IPCP Negotiation, page 10-15](#)

Configuring DHCP ODAPs on an Interface

[Example 10-7](#) defines ODAPs on a virtual template interface named *Virtual-Template1*. Remote peers connecting to an interface on which *Virtual-Template1* is applied obtain their IP addresses from the ODAP.

Example 10-7 Defining DHCP ODAPs on an Interface

```

!
interface Virtual-Template1
  ip vrf forwarding green
  ip unnumbered loopback1
  ppp authentication chap
  peer default ip address dhcp-pool

```

Configuring ODAPs to Obtain Subnets Through IPCP Negotiation

[Example 10-8](#) creates a DHCP address pool named *my_pool*, configures the pool as an on-demand address pool using IPCP as the subnet allocation protocol, and configures the Ethernet0 interface to automatically obtain its IP address from the *my_pool* address pool.

Example 10-8 Enabling ODAPs to Obtain Subnets Through IPCP Negotiation

```

!
ip dhcp pool my_pool
  import all
  origin ipcp
!
interface Ethernet0
  ip address pool my_pool
  ip verify unicast reverse-path
  shutdown
  hold-queue 32 in
!

```

Monitoring and Maintaining an On-Demand Address Pool

To monitor and maintain an ODAP, enter the following commands in privileged EXEC mode:

Command	Purpose
Router# clear ip dhcp [<i>pool name</i>] binding {* <i>address</i> }	Deletes an automatic address binding or objects for a specific pool from the DHCP server database.
Router# clear ip dhcp [<i>pool name</i>] conflict {* <i>address</i> }	Clears an address conflict(s) for a specific pool from the DHCP server database.
Router# clear ip dhcp [<i>pool name</i>] subnet {* <i>address</i> }	Clears all currently leased subnets in the specified DHCP pool or in all DHCP pools if you do not specify a specific pool.
Router# debug dhcp details	Monitors subnet allocation and subnet releases for the on-demand address pools.
Router# debug ip dhcp server events	Reports DHCP server events, such as assignments and database updates.
Router# show ip dhcp import	Displays the option parameters imported into the DHCP server database.

Command	Purpose
Router# show ip interface [<i>type number</i>]	Displays the usability status of interfaces configured for IP.
Router# show ip dhcp pool <i>name</i>	Displays DHCP address pool information. Use this command to check that the DHCP pool assigns an IP address for each incoming PPP session and associates the address with the correct VRF.

**Tip**

- By default, the Cisco IOS DHCP server that the pool manager uses verifies address availability by using the **ping** command before allocating the address; the default DHCP ping configuration waits two seconds for an ICMP echo reply. As a result of this default configuration, the DHCP server services one address request every two seconds. You can configure the number of ping packets sent and the ping timeout timer. To reduce the address allocation time, reduce either the timeout timer value or the number of ping packets sent.

**Note**

While reducing the address allocation time improves address allocation, the reduced time inhibits the DHCP server's ability to detect duplicate addresses.

- Each ODAP retries up to four times to obtain a subnet from the DHCP server or the RADIUS server. If unsuccessful, the subnet request automatically starts when another individual address request is made to the pool (for example, a newly brought up PPP session makes an address request). If the address allocation server has not allocated any subnets to a pool, you can force the subnet request process to restart by using the **clear ip dhcp pool name subnet *** command in privileged EXEC mode.

Overlapping IP Address Pools

The Overlapping IP Address Pools feature enables you to use multiple IP address spaces and reuse IP addresses among different VPNs supported on the Cisco 10000 router. Duplicate IP addresses cannot reside in the same IP address space.

To uniquely place IP addresses within a given IP address space, multiple address spaces are assigned to IP address groups. This also allows for the verification of nonoverlapping IP address pools within an IP address group. Within the Cisco 10000 router, use unique pool names. Each pool name has an implicit group identifier to ensure that it is associated with only one group.

The Cisco 10000 router considers pools without an explicit group name as members of a base system group and processes these pools as if the IP addresses belong to a single IP address space. You cannot assign a given IP address multiple times from the pool of a single IP address space.

Existing configurations are not affected by the Overlapping IP Address Pools feature. The processing of pools that are not specified as a member of a group is unchanged from the existing implementation.

The Overlapping IP Address Pools feature is useful in the following deployment models:

- Managed L2TP Network Server
- PPP Terminated Aggregation (PTA) to VRF
- Remote Access (RA) to MPLS VPN

The Overlapping IP Address Pools feature is described in the following topics:

- [Feature History for Overlapping IP Address Pools, page 10-17](#)
- [Restrictions for Overlapping IP Address Pools, page 10-17](#)
- [Configuration Tasks for Overlapping IP Address Pools, page 10-17](#)
- [Verifying Local Pool Groups for IP Overlapping Address Pools, page 10-18](#)
- [Configuration Examples for Overlapping IP Address Pools, page 10-18](#)

Feature History for Overlapping IP Address Pools

Cisco IOS Release	Description	Required PRE
12.2(4)BZ1	This feature was introduced on the Cisco 10000 series router.	PRE1
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7)XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for Overlapping IP Address Pools

The software checks for duplicate addresses on a per-group basis. This means that you can configure pools in multiple groups that could have possible duplicate addresses. You should only use this feature in environments such as MPLS VPN where multiple IP address spaces are supported.

Configuration Tasks for Overlapping IP Address Pools

To configure the IP overlapping address pools feature, configure a local pool group as described in [“Configuring a Local Pool Group for IP Overlapping Address Pools”](#).

Configuring a Local Pool Group for IP Overlapping Address Pools

To configure a local pool group, enter the following command in global configuration mode:

Command	Purpose
Router(config)# ip local pool <i>pool-name</i> <i>start-IP</i> [<i>end-IP</i>] [group <i>group-name</i>] [cache-size <i>size</i>]	Configures a group of local IP address pools, gives the group a name, and specifies a cache size.

Verifying Local Pool Groups for IP Overlapping Address Pools

To verify that you have successfully configured a pool group, enter the following commands in privileged EXEC mode and check the resulting output for the pool group name:

Command	Purpose
Router# show ip local pool [<i>pool-name</i> [<i>group group-name</i>]]	Displays statistics for defined IP address pools.
Router# show ip local pool	Displays statistics for all pools configured.
Router# show ip local pool <i>pool-name</i>	Displays statistics for a specific pool you specify.
Router# show ip local pool <i>group</i>	Displays statistics for all pools in a base system group.
Router# show ip local pool <i>group group-name</i>	Displays all pools in a specified group.

Configuration Examples for Overlapping IP Address Pools

This section provides the following configuration examples:

- [Generic IP Overlapping Address Pools Example, page 10-18](#)
- [IP Overlapping Address Pools for VPNs and VRFs Example, page 10-19](#)

Generic IP Overlapping Address Pools Example

The following example shows the configuration of two pool groups and includes pools in the base system group. In this example:

- Pool group grp1 consists of pools p1_g1, p2_g1, and p3_g1.
- Pool group grp2 consists of pools p1_g2 and p2_g2.
- Pools lp1 and lp2 are members of the base system group.
- The IP address 10.1.1.1 overlaps grp1, grp2, and the base system group.
- No overlapping addresses occur within any group including the unnamed base system group, which consists of pools lp1 and lp2.

```
ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```



Note

The preceding example shows pool names that provide an easy way to associate a pool name with a group (when the pool name stands alone). This association is an operational convenience. There is no required relationship between the names used to define a pool and the name of the group.

IP Overlapping Address Pools for VPNs and VRFs Example

The following example is a general IP address configuration that VPNs and VRFs might use. This example shows pool names that provide a way to associate a pool name with a VPN (when the pool name stands alone). This association is an operational convenience. There is no required relationship between the names used to define a pool and the name of the group. In this example:

- Pool group vpn1 consists of pools p1_vpn1, p2_vpn1, and p3_vpn1.
- Pool group vpn2 consists of pools p1_vpn2, p2_vpn2.
- Pools lp1 and lp2 are members of the base system.
- The IP address 10.1.1.1 overlaps vpn1, vpn2, and the base system group.
- No overlapping addresses occur within any group including the unnamed base system group, which consists of pools lp1 and lp1.

```
ip local pool p1_vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2_vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1_vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2_vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

