



DHCP Server—On-Demand Address Pool Manager

Feature History for DHCP Server—On-Demand Address Pool Manager

Release	Modification
12.2(8)T	This feature was introduced.
12.2(15)T	This feature was enhanced to support non-MPLS VPN address pools.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

This document describes the DHCP Server—On-Demand Address Pool Manager feature and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Monitoring and Maintaining the ODAP, page 10](#)
- [Configuration Examples, page 11](#)
- [Command Reference, page 16](#)
- [Glossary, page 41](#)

Feature Overview

The DHCP Server—On-Demand Address Pool Manager is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. On-demand address pools (ODAPs) support address assignment using the Dynamic Host Configuration Protocol (DHCP) for customers using private addresses. Each ODAP is configured and associated with a



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2001–2005 Cisco Systems, Inc. All rights reserved.

particular Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). Cisco IOS Release 12.2(15)T introduces support for non-MPLS VPN address pools by adding pool name support to the **peer default ip address dhcp-pool *pool name*** command.

For MPLS VPNs, each VPN is associated with one or more VPN routing and forwarding instances (VRFs). The VRF is a key element in the VPN technology because it maintains the routing information that defines a customer VPN site. This customer site is attached to a provider edge (PE) router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

Once configured, the ODAP is populated with one or more subnets leased from a source server and is ready to serve address requests from DHCP clients or from PPP sessions. The source server can be a remote DHCP server or a RADIUS server (via AAA). Currently, only the Cisco Access Registrar RADIUS server supports ODAPs. Subnets can be added to the pool when a certain utilization level (high utilization mark) is achieved. When the utilization level falls below a certain level (low utilization mark), a subnet can be returned to the server from which it was originally leased. Summarized routes for each leased subnet must be inserted or removed from the related VRF with each addition or removal of subnets into the ODAP.

A PPP session belonging to a specific VPN is only allocated an address from the ODAP associated with that VPN. These PPP sessions are terminated on a Virtual Home Gateway (VHG)/PE router where the ODAP is configured. The VHG/PE router maps the remote user to the corresponding MPLS VPNs.

For PPP sessions, individual address allocation from an ODAP follows a First Leased subnet First (FLF) policy. FLF searches for a free address beginning on the very first leased subnet, followed by a search on the second leased subnet if no free address is available in the first subnet, and so on. This policy provides the benefit of grouping the leased addresses over time to a set of subnets, which allows an efficient subnet release and route summarization.

However, the FLF policy differs from the normal DHCP address selection policy. Normal DHCP address selection takes into account the IP address of the receiving interface or the gateway address if it is nonzero. To support both policies, the DHCP server needs to be able to distinguish between a normal DHCP address request and an address request for a PPP client. The DHCP Server—On-Demand Address Pool Manager feature introduces a new IP address pooling mechanism for PPP that allows the DHCP server to distinguish between a normal DHCP address request and a request from a PPP client.

Subnet release from an ODAP follows a Last Leased subnet First (LLF) policy, which prefers the last leased subnet to be released first. This LLF policy searches for a releasable subnet (a subnet with no addresses currently being leased) starting with the last leased subnet. If a releasable subnet is found (candidate subnet), it is released, and the summarized route for that subnet is removed. If more than one releasable subnet exists at that time, only the most recently allocated is released. If there are no releasable subnets, no action is taken. If by releasing the candidate subnet, the high utilization mark is reached, the subnet is not released. The first leased subnet is never released (regardless of the instantaneous utilization level) until the ODAP is disabled.

Benefits

Efficient Address Management

The ODAP Manager allows customers to optimize their use of IP addresses, thus conserving address space.

Efficient Route Summarization and Update

The ODAP Manager inserts a summarized route when a subnet is added to the ODAP.

Restrictions

Currently, the **ip dhcp excluded-address** global configuration command cannot be used to exclude addresses from VRF associated pools.

The **vrf** DHCP pool configuration command is currently not supported for host pools.

Attribute inheritance is not supported on VRF pools.

Related Features and Technologies

- IPCP subnet mask negotiation
- DHCP proxy client and local IP address pooling mechanisms

Related Documents

- *Cisco IOS IP Configuration Guide, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*
- *Cisco IOS Security Command Reference, Release 12.2*
- *Cisco IOS Security Configuration Guide, Release 12.2*. Refer to the chapters “Configuring Authentication,” “Configuring Authorization,” “Configuring Accounting,” and “Configuring RADIUS.”
- *Cisco IOS Switching Services Command Reference, Release 12.2*
- *Cisco IOS Switching Services Configuration Guide, Release 12.2*. Refer to the chapters “Multiprotocol Label Switching Overview” and “Configuring Multiprotocol Label Switching” in the part “Multiprotocol Label Switching.”
- *Introduction to Cisco MPLS VPN Technology*
- *Release Notes for the Cisco 820 Series Routers for Cisco IOS Release 12.2(1)XD1*. Refer to “IPCP Subnet Mask Delivery” in the “New and Changed Information” section
- *MPLS VPN ID, Release 12.2(8)T*

Supported Platforms

Refer to feature navigator for the latest platform information as referenced below.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgt/cmtk/mibs.shtml>

RFCs

- RFC 3046, *DHCP Relay Information Option*
- RFC 2685, *Virtual Private Networks Identifier*

Prerequisites

Before configuring the DHCP Server—On-Demand Address Pool Manager feature, you must configure standard MPLS VPNs unless you intend to use non-MPLS VPNs.

In order for the IP address pooling mechanism to work correctly, the VRF of the PPP session must match that configured on the pool. Typically this matching is done either by configuring the **ip vrf forwarding vrf-name** command on the virtual template interface, or if AAA is used to authorize the PPP user, it can be part of the user's profile configuration.

For more information on configuring MPLS VPNs, refer to the *Cisco IOS Switching Services Configuration Guide*, Release 12.2. For more information on configuring AAA, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.

- [Defining DHCP ODAPs as the Global Default Mechanism](#) (required)
- [Defining DHCP ODAPs on an Interface](#) (optional)
- [Configuring the DHCP Pool as an ODAP](#) (required)
- [Configuring ODAPs to Obtain Subnets Through IPCP Negotiation](#) (optional)
- [Configuring AAA](#) (required)
- [Configuring RADIUS](#) (required)
- [Disabling ODAPs](#) (optional)
- [Verifying ODAP Operation](#) (optional)

Defining DHCP ODAPs as the Global Default Mechanism

IP addressing allows configuration of a global default address pooling mechanism. The DHCP server needs to be able to distinguish between a normal DHCP address request and an address request for a PPP client.

To specify that the global default mechanism to use is on-demand address pooling, use 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 remote access (PPP) sessions into MPLS VPNs, IP addresses are obtained from locally configured VRF-associated DHCP pools.

Defining DHCP ODAPs on an Interface

You can also configure the on-demand address pooling mechanism on an interface-by-interface basis, which overrides the global default mechanism on that interface. To enable DHCP on-demand address pooling assignment on an interface, use 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 [<i>pool name</i>]	Specifies an IP address from an on-demand address pool to be returned to a remote peer connecting to this interface. The <i>pool name</i> argument is mandatory if the session is not associated with any VRF. Multiple pool names can be accepted.

Configuring the DHCP Pool as an ODAP

To configure a DHCP pool as an on-demand address pool, use 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)# vrf <i>name</i>	(Optional) Associates the address pool with a VRF name. Only use this command for MPLS VPNs.
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.

	Command	Purpose
Step 4	Router(config-dhcp) # utilization mark low <i>percentage-number</i>	Sets the low utilization mark of the pool size. The default value is 0 percent.
Step 5	Router(config-dhcp) # utilization mark high <i>percentage-number</i>	Sets the high utilization mark of the pool size. The default value is 100 percent.

Configuring ODAPs to Obtain Subnets Through IPCP Negotiation

You can assign IP address pools to customer premises equipment (CPE) devices, which, in turn, assign IP addresses to the CPE and to a DHCP pool. This functionality has three requirements:

- The Cisco IOS CPE device must be able to request and use the subnet.
- The RADIUS server (via AAA) must be able to provide that subnet and insert the framed route into the proper VRF table.
- The PE router must be able to facilitate providing the subnet through IP Control Protocol (IPCP) negotiation.

To configure your router to use subnets obtained through IPCP negotiation, use 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 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>	Configures an interface and enters interface configuration mode.
Step 6	Router(config-if) # ip address pool <i>name</i>	Specifies that the interface IP address will be automatically configured from the named pool, when the pool is populated with a subnet from IPCP.

Configuring AAA

To allow ODAP to obtain subnets from the RADIUS server, the AAA client must be configured on the VHG/PE router. To configure AAA on the VHG/PE router, use the following commands in global configuration mode:

	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	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. Sends a "start" accounting notice at the beginning of a process.
	or	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 "stop" accounting notice at the end of the requested user process.
Step 4	Router(config)# aaa session-id common	Ensures that the same session ID will be used for each AAA accounting service type within a call.

Configuring RADIUS

To configure RADIUS, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip radius source-interface <i>subinterface-name</i>	Forces RADIUS to use the IP address of a 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 network access server (NAS) to recognize and use vendor-specific accounting attributes.
Step 6	Router(config)# radius-server vsa send authentication	Configures the NAS to recognize and use vendor-specific authentication attributes.

Disabling ODAPs

When an ODAP is disabled, all leased subnets are released. If active PPP sessions are using addresses from the released subnets, those sessions will be reset. DHCP clients leasing addresses from the released subnets will not be able to renew their leases. To disable an ODAP from a DHCP pool, use the following command in DHCP pool configuration mode:

Command	Purpose
Router(config-dhcp)# no origin {dhcp aaa ipcp}	Disables the ODAP.

Verifying ODAP Operation

Step 1 Enter the **show ip dhcp pool [name]** command:

The following output is for two DHCP pools: Green and Global. Pool Green is configured with a high utilization mark of 50 and a low utilization mark of 30. The pool is also configured to obtain more subnets when the high utilization mark is reached (autogrow). The Subnet size field indicates the values configured in the **origin** command as the initial and incremental subnet sizes that would be requested by the pool named Green. The Total addresses field is a count of all the usable addresses in the pool. The Leased addresses field is a total count of how many bindings were created from the pool. The Pending event field shows subnet request, which means that a subnet request is pending for the pool. The subnet request was scheduled because the Leased addresses count has exceeded the high utilization level of the pool. Subnets currently added to pool Green are shown in sequence. The Current index column shows the address that would be allocated next from this subnet. The IP address range column shows the range of usable addresses from the subnet. The Leased addresses column shows individual count of bindings created from each subnet. Three subnets are currently added to pool Green. The first two subnets have used all their addresses and thus the Current index is showing 0.0.0.0.

Notice that pool Green and pool Global can have the same subnet (172.16.0.1-172.16.0.6) because pool Green is configured to be in VRF Green, while pool Global is configured to be in the global address space.

```
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 index      IP address range      Leased addresses
  0.0.0.0            172.16.0.1      - 172.16.0.6      6
  0.0.0.0            172.16.0.9      - 172.16.0.14     6
  172.16.0.18        172.16.0.17     - 172.16.0.22     1

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 index      IP address range      Leased addresses
  172.16.0.1         172.16.0.1      - 172.16.0.6      0
```

Step 2 Enter the **show ip dhcp binding** command:

The output following shows the bindings from pool Green. The Type field shows On-demand, which

indicates that the address binding was created for a PPP session. The Lease expiration field shows Infinite, which means 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 will be forced to obtain a new IP address. The Hardware address column for an On-demand entry shows the identifier for the session as detected by PPP. There are no bindings shown under the Bindings from all pools not associated with VRF field because the Global pool has not allocated any addresses.

Router# **show ip dhcp binding**

Bindings from all pools not associated with VRF:

IP address	Hardware address	Lease expiration	Type
Bindings from VRF pool Green:			
IP address	Hardware address	Lease expiration	Type
172.16.0.1	5674.312d.7465.7374. 2d38.3930.39	Infinite	On-demand
172.16.0.2	5674.312d.7465.7374. 2d38.3839.31	Infinite	On-demand
172.16.0.3	5674.312d.7465.7374. 2d36.3432.34	Infinite	On-demand
172.16.0.4	5674.312d.7465.7374. 2d38.3236.34	Infinite	On-demand
172.16.0.5	5674.312d.7465.7374. 2d34.3331.37	Infinite	On-demand
172.16.0.6	5674.312d.7465.7374. 2d37.3237.39	Infinite	On-demand
172.16.0.9	5674.312d.7465.7374. 2d39.3732.36	Infinite	On-demand
172.16.0.10	5674.312d.7465.7374. 2d31.3637	Infinite	On-demand
172.16.0.11	5674.312d.7465.7374. 2d39.3137.36	Infinite	On-demand
172.16.0.12	5674.312d.7465.7374. 2d37.3838.30	Infinite	On-demand
172.16.0.13	5674.312d.7465.7374. 2d32.3339.37	Infinite	On-demand
172.16.0.14	5674.312d.7465.7374. 2d31.3038.31	Infinite	On-demand
172.16.0.17	5674.312d.7465.7374. 2d38.3832.38	Infinite	On-demand
172.16.0.18	5674.312d.7465.7374. 2d32.3735.31	Infinite	On-demand

Troubleshooting Tips

By default, the Cisco IOS DHCP server on which the ODAP Manager is based attempts to verify an address availability by performing a ping operation to the address before allocation. The default DHCP ping configuration will wait for 2 seconds for an ICMP echo reply. This default configuration results in the DHCP server servicing one address request every 2 seconds. The number of ping packets being sent and the ping timeout are configurable. Thus, to reduce the address allocation time, you can reduce either the timeout or the number of ping packets sent. Reducing the timeout or the ping packets being sent will improve the address allocation time, at the cost of less ability to detect duplicate addresses.

Each ODAP will make a finite number of attempts (up to four retries) to obtain a subnet from DHCP or AAA. If these attempts are not successful, the subnet request from the pool automatically starts when there is another individual address request to the pool (for example, from a newly brought up PPP session). If a pool has not been allocated any subnets, you can force restarting the subnet request process by using the **clear ip dhcp pool *name* subnet *** EXEC command.

Monitoring and Maintaining the ODAP

To monitor and maintain the ODAP, use the following EXEC commands:

Command	Purpose
Router# clear ip dhcp [<i>pool name</i>] binding { <i>*</i> <i>address</i> }	Deletes an automatic address binding or objects from a specific pool from the DHCP server database.
Router# clear ip dhcp [<i>pool name</i>] conflict { <i>*</i> <i>address</i> }	Clears an address conflict or conflicts from a specific pool from the DHCP server database.
Router# clear ip dhcp [<i>pool name</i>] subnet { <i>*</i> <i>address</i> }	Clears all currently leased subnets in the named DHCP pool or all DHCP pools if <i>name</i> is not specified.
Router# debug dhcp details	Monitors the subnet allocation/releasing in the on-demand address pools.
Router# debug ip dhcp server events	Reports DHCP server events, like address assignments and database updates.
Router# show ip dhcp import	Displays the option parameters that were imported into the DHCP server database.
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.

Note the following behavior for the **clear ip dhcp binding**, **clear ip dhcp conflict**, and **clear ip dhcp subnet** commands:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified binding/conflict/subnet.
- If you do not specify the **pool name** option and the ***** option is specified, it is assumed that all automatic/ or on-demand bindings/conflicts/subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the ***** option, all automatic or on-demand bindings/conflicts/subnets in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified binding/conflict or the subnet containing the specified IP address will be deleted from the specified pool.

Configuration Examples

This section provides the following configuration examples:

- [Defining DHCP ODAPs as the Global Default Mechanism Example](#)
- [Defining DHCP ODAPs on an Interface Example](#)
- [Configuring the DHCP Pool as an ODAP Example](#)
- [Configuring the DHCP Pool as an ODAP for Non-MPLS VPNs Example](#)
- [IPCP Subnet Mask Delivery Example](#)
- [Configuring AAA and RADIUS Example](#)

Defining DHCP ODAPs as the Global Default Mechanism Example

The following example shows that the on-demand address pooling mechanism will be used to serve an address request from a PPP client.

```
!  
ip address-pool dhcp-pool  
!  
ip dhcp pool Green-pool  
!
```

Defining DHCP ODAPs on an Interface Example

The following example shows how to configure an interface to retrieve an IP address from an on-demand address pool:

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

Configuring the DHCP Pool as an ODAP Example

The following example shows two ODAPs configured to obtain their subnets from an external DHCP server:

```
Router# show running-config  
  
Building configuration...  
  
Current configuration : 3943 bytes  
!  
version 12.2  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname Router  
!
```

```

no logging console
enable password lab
!
username vpn_green_net1 password 0 lab
username vpn_red_net1 password 0 lab
ip subnet-zero
!
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 cef
ip address-pool dhcp-pool
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
    ip address 1.1.1.1 255.255.255.255
!
interface Loopback1
    ip vrf forwarding Green
    ip address 100.10.10.1 255.255.255.255
!
interface Loopback2
    ip vrf forwarding Red
    ip address 110.10.10.1 255.255.255.255
!
interface ATM2/0
    no ip address
    shutdown
    no atm ilmi-keepalive
!
interface ATM3/0
    no ip address
    no atm ilmi-keepalive
!
interface Ethernet4/0
    ip address 10.0.105.12 255.255.255.224
    duplex half
!
interface Ethernet4/1
    ip address 150.10.10.1 255.255.255.0
    duplex half
!
interface Ethernet4/2
    ip address 120.10.10.1 255.255.255.0
    duplex half
    tag-switching ip

```

```
!  
interface Virtual-Template1  
  ip vrf forwarding Green  
  ip unnumbered Loopback1  
  ppp authentication chap  
!  
interface Virtual-Template2  
  ip vrf forwarding Green  
  ip unnumbered Loopback1  
  ppp authentication chap  
!  
interface Virtual-Template3  
  ip vrf forwarding Green  
  ip unnumbered Loopback1  
  ppp authentication chap  
!  
interface Virtual-Template4  
  ip vrf forwarding Red  
  ip unnumbered Loopback2  
  ppp authentication chap  
!  
interface Virtual-Template5  
  ip vrf forwarding Red  
  ip unnumbered Loopback2  
  ppp authentication chap  
!  
interface Virtual-Template6  
  ip vrf forwarding Red  
  ip unnumbered Loopback2  
  ppp authentication chap  
!  
router ospf 100  
  log-adjacency-changes  
  redistribute connected  
  network 1.1.1.1 0.0.0.0 area 0  
  network 120.10.10.0 0.0.0.255 area 0  
  network 150.10.10.0 0.0.0.255 area 0  
!  
router bgp 100  
  no synchronization  
  bgp log-neighbor-changes  
  neighbor 3.3.3.3 remote-as 100  
  neighbor 3.3.3.3 update-source Loopback0  
  !  
  address-family ipv4 vrf Red  
    redistribute connected  
    redistribute static  
    no auto-summary  
    no synchronization  
    network 110.0.0.0  
  exit-address-family  
  !  
  address-family ipv4 vrf Green  
    redistribute connected  
    redistribute static  
    no auto-summary  
    no synchronization  
    network 100.0.0.0  
  exit-address-family  
  !  
  address-family vpnv4  
    neighbor 3.3.3.3 activate  
    neighbor 3.3.3.3 send-community extended  
  exit-address-family
```

```

!
ip classless
ip route 172.19.0.0 255.255.0.0 10.0.105.1
no ip http server
ip pim bidir-enable
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password lab
login
!
end

```

Configuring the DHCP Pool as an ODAP for Non-MPLS VPNs Example

The following example shows how to configure an interface to retrieve an IP address from an on-demand address pool. In this example, two non-VRF ODAPs are configured. There are two virtual-templates and two DHCP address pools, `usergroup1` and `usergroup2`. Each virtual-template interface is configured to obtain IP addresses for the peer from the associated address pool.

```

!
ip dhcp pool usergroup1
origin dhcp subnet size initial /24 autogrow /24
lease 0 1
!
ip dhcp pool usergroup2
origin dhcp subnet size initial /24 autogrow /24
lease 0 1
!
interface virtual-template1
ip unnumbered loopback1
peer default ip address dhcp-pool usergroup1
!
interface virtual-template2
ip unnumbered loopback1
peer default ip address dhcp-pool usergroup2

```

IPCP Subnet Mask Delivery Example

The following example shows a Cisco 827 router configured to use IPCP subnet masks:

```

Router# show running-config

Building configuration...

Current configuration :1479 bytes
!
version 12.2

```

```
no service single-slot-reload-enable
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname Router
!
no logging buffered
logging rate-limit console 10 except errors
!
username 6400-nrp2 password 0 lab
ip subnet-zero
ip dhcp smart-relay
!
ip dhcp pool IPPOOLTEST
    import all
    origin ipcp
!
no ip dhcp-client network-discovery
!
interface Ethernet0
    ip address pool IPPOOLTEST
    ip verify unicast reverse-path
    shutdown
    hold-queue 32 in
!
interface ATM0
    no ip address
    atm ilmi-keepalive
    bundle-enable
    dsl operating-mode auto
    hold-queue 224 in
!
interface ATM0.1 point-to-point
    pvc 1/40
    no ilmi manage
    encapsulation aal5mux ppp dialer
    dialer pool-member 1
!
!
interface Dialer0
    ip unnumbered Ethernet0
    ip verify unicast reverse-path
    encapsulation ppp
    dialer pool 1
    dialer-group 1
    no cdp enable
    ppp authentication chap callin
    ppp chap hostname Router
    ppp chap password 7 12150415
    ppp ipcp accept-address
    ppp ipcp dns request
    ppp ipcp wins request
    ppp ipcp mask request
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
no ip http server
!
dialer-list 1 protocol ip permit
line con 0
    exec-timeout 0 0
    transport input none
```

```

stopbits 1
line vty 0 4
login
!
scheduler max-task-time 5000
end

```

Configuring AAA and RADIUS Example

The following example shows one pool "Green" configured to obtain its subnets from the AAA (RADIUS) server located at IP address 172.16.1.1:

```

!
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

```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

New Commands

- [aaa session-id](#)
- [clear ip dhcp subnet](#)
- [ip address pool \(DHCP\)](#)
- [ip dhcp aaa default username](#)
- [origin](#)
- [show ip dhcp pool](#)
- [utilization mark high](#)
- [utilization mark low](#)
- [vrf](#)

Modified Commands

- [clear ip dhcp binding](#)
- [clear ip dhcp conflict](#)
- [ip address-pool](#)
- [peer default ip address](#)

aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

```
aaa session-id [common | unique]

no aaa session-id [unique]
```

Syntax Description	common	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is common .
	unique	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID.
		Accounting-requests for each service will have a different session ID.

Defaults The **common** keyword is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)B	This command was introduced.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines The **common** keyword behavior allows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model** command is configured.



Note

The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique keyword *must* be specified. The session ID may be included in RADIUS access requests by

configuring the **radius-server attribute 44 include-in-access-req** command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

Related Commands

Command	Description
aaa new model	Enables AAA.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

clear ip dhcp binding

To delete an automatic address binding from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp binding** command in privileged EXEC mode.

```
clear ip dhcp [pool name] binding [* | address]
```

Syntax Description

pool name	(Optional) Name of the DHCP pool.
*	Clears all automatic bindings.
address	The address of the binding you want to clear.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	The pool name keyword and argument combination was added.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Typically, the address denotes the IP address of the client. If the asterisk (*) character is used as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp pool** global configuration command to delete a manual binding.

Note the following behavior for the **clear ip dhcp binding** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified binding.
- If you do not specify the **pool name** option and the * option is specified, it is assumed that all automatic or on-demand bindings in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the * option, all automatic or on-demand bindings in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified binding will be deleted from the specified pool.

Examples

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Router# clear ip dhcp binding 10.12.1.99
```

The following example deletes all bindings from all pools:

```
Router# clear ip dhcp binding *
```

The following example deletes all bindings from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 binding *
```

The following example deletes address binding 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool red binding pool2
```

Related Commands

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

clear ip dhcp conflict

To clear an address conflict from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp conflict** command in privileged EXEC mode.

```
clear ip dhcp [pool name] conflict { * | address }
```

Syntax Description

pool name	(Optional) Name of the DHCP pool.
*	Clears all address conflicts.
address	The IP address of the host that contains the conflicting address you want to clear.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(8)T	The pool name keyword and argument combination were added.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If the asterisk (*) character is used as the address parameter, DHCP clears all conflicts.

Note the following behavior for the **clear ip dhcp conflict** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified conflict.
- If you do not specify the **pool name** option and the * option is specified, it is assumed that all automatic/ or on-demand conflicts in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the * option, all automatic or on-demand conflicts in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified conflict will be deleted from the specified pool.

Examples

The following example shows an address conflict of 10.12.1.99 being deleted from the DHCP server database:

```
Router# clear ip dhcp conflict 10.12.1.99
```

The following example deletes all address conflicts from all pools:

```
Router# clear ip dhcp conflict *
```

The following example deletes all address conflicts from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 conflict *
```

The following example deletes address conflict 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 conflict 10.13.2.99
```

Related Commands

Command	Description
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

clear ip dhcp subnet

To clear all currently leased subnets in the Cisco IOS Dynamic Host Configuration Protocol (DHCP) pool, use the **clear ip dhcp subnet** command in privileged EXEC configuration mode.

```
clear ip dhcp [pool name] subnet { * | address }
```

Syntax Description

pool name	(Optional) Name of the DHCP pool.
*	Clears all leased subnets.
address	Clears a subnet containing the specified IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

A PPP session that is allocated an IP address from the released subnet will be reset.

Note the following behavior for the **clear ip dhcp subnet** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified subnet.
- If you do not specify the **pool name** option and the ***** option is specified, it is assumed that all automatic or on-demand subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the ***** option, all automatic or on-demand subnets in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the subnet containing the specified IP address will be deleted from the specified pool.



Caution

Use this command with caution to prevent undesired termination of active PPP sessions.

Examples

The following example releases the subnet containing 10.0.0.2 from any non-VRF on-demand address pools:

```
Router# clear ip dhcp subnet 10.0.0.2
```

The following example clears all leased subnets from all pools:

```
Router# clear ip dhcp subnet *
```

The following example clears all leased subnets from the address pool named pool3:

```
Router# clear ip dhcp pool pool3 subnet *
```


The following example clears the address 10.0.0.2 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 subnet 10.0.0.2
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

ip address-pool

To enable an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces, use the **ip address-pool** command in global configuration mode. To disable IP address pooling globally on all interfaces with the default configuration, use the **no** form of this command.

ip address-pool [**dhcp-pool** | **dhcp-proxy-client** | **local**]

no ip address-pool

Syntax Description

dhcp-pool	(Optional) Uses on-demand address pooling as the global default address mechanism. This option supports only remote access (PPP) sessions into MPLS VPNs. IP addresses are obtained from locally configured VRF-associated Dynamic Host Configuration Protocol (DHCP) pools.
dhcp-proxy-client	(Optional) Uses the router as the proxy-client between a third-party (DHCP) server and peers connecting to the router.
local	(Optional) Uses the local address pool named <i>default</i> .

Defaults

IP address pooling is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(8)T	The dhcp-pool keyword was added.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The global default mechanism applies to all interfaces that have been left in the default setting of the **peer default ip address pool** command.

If any **peer default ip address** command other than **peer default ip address pool** (the default) is configured, the interface uses that mechanism and not the global default mechanism. Thus all interfaces can be independently configured or left unconfigured so that the global default mechanism setting applies. This flexibility minimizes the configuration effort on the part of the administrator.

The **ip address-pool dhcp-pool** command supports only remote access (PPP) sessions into Multiprotocol Label Switching Virtual Private Networks (MPLS VPNs). IP addresses are obtained from locally configured virtual routing and forwarding (VRF)-associated DHCP pools. A VRF VPN instance is a per-VPN routing information repository that defines the VPN membership of a customer site.

Examples

The following example specifies the DHCP on-demand address pooling mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-pool
```

The following example specifies the DHCP proxy client mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-proxy-client
```

The following example specifies a local IP address pool named “default” as the global default mechanism for all interfaces that have been left in their default setting:

```
ip address-pool local
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
exec	Allows an EXEC process on a line.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
ppp	Starts an asynchronous connection using PPP.
show cot dsp	Displays information about the COT DSP configuration or current status.
show ip local pool	Displays statistics for any defined IP address pools.
slip	Starts a serial connection to a remote host using SLIP.

ip address pool (DHCP)

To enable the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IP Control Protocol (IPCP) negotiation, use the **ip address pool** command in interface configuration mode. To disable autoconfiguring of the IP address of the interface, use the **no** form of this command.

ip address pool *name*

no ip address pool

Syntax Description

<i>name</i>	Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in <i>name</i> .
-------------	---

Defaults

IP address pooling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Use this command to automatically configure the IP address of a LAN interface when there are DHCP clients on the attached LAN that should be serviced by the DHCP pool on the router. The DHCP pool obtains its subnet dynamically through IPCP subnet negotiation.

Examples

The following example specifies that the IP address of Ethernet interface 2 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface Ethernet 2
  ip address pool abc
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip dhcp aaa default username

To specify the default user name for non-VRF address pools that have been configured to obtain subnets through AAA, use the **ip dhcp aaa default username** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip dhcp aaa default username *name*

no ip dhcp aaa default username *name*

Syntax Description

<i>name</i>	Name of the address pool.
-------------	---------------------------

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The behavior for when the USERNAME attribute is sent in the AAA request was changed.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Address pools that are configured with the **vrf** and **origin aaa** DHCP pool configuration commands will set the USERNAME attribute in the AAA request to the specified VRF name. If the VPN ID as specified in RFC 2685 is configured for the VRF, the VPN ID will be sent instead.

Address pools that are not configured with the **vrf** command but are configured with the **origin aaa** command, will set the USERNAME attribute in the AAA request to the specified *name* in the **ip dhcp aaa default username** command.

Use the **debug aaa attribute** command to verify the value of the USERNAME attribute in the subnet request to the AAA server.

In Cisco IOS Release 12.2(8)T, if this command is not configured, no AAA subnet request from non-VRF ODAPs will be sent.


In Cisco IOS Release 12.2(15)T, if the DHCP pool is not configured with VRF and the **ip dhcp aaa default username** command is not configured, the AAA request will still be sent with the USERNAME attribute set to the DHCP pool name.

This command is not needed if all ODAPs on the VHG/PE are VRF-associated.

Examples

The following example sets the USERNAME attribute in the AAA request to green:

```
ip dhcp aaa default username green
```

 ip dhcp aaa default username

Related Commands	Command	Description
	debug aaa attribute	Verifies the value of the AAA attributes.
	origin	Configures an address pool as an on-demand address pool.
	vrf	Associates the on-demand address pool with a VPN routing and forwarding instance.

origin

To configure an address pool as an on-demand address pool (ODAP) or static mapping pool, use the **origin** command in DHCP pool configuration mode. To disable the ODAP, use the **no** form of this command.

origin { **dhcp** | **aaa** | **ipcp** | **file** *url* } [**subnet size** **initial** *size* [**autogrow** *size*]]

no origin { **dhcp** | **aaa** | **ipcp** | **file** *url* } [**subnet size** **initial** *size* [**autogrow** *size*]]

Syntax Description		
dhcp		Specifies the Dynamic Host Configuration Protocol (DHCP) as the subnet allocation protocol.
aaa		Specifies authentication, authorization, and accounting (AAA) as the subnet allocation protocol.
ipcp		Specifies the IP Control Protocol (IPCP) as the subnet allocation protocol.
file <i>url</i>		Specifies the external database file that contains the static bindings assigned by the DHCP server. The <i>url</i> argument specifies the location of the external database file.
subnet size initial <i>size</i>	(Optional)	Specifies the initial size of the first requested subnet. You can enter <i>size</i> as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.
autogrow <i>size</i>	(Optional)	Specifies that the pool can grow incrementally. The <i>size</i> argument is the size of the requested subnets when the pool requests additional subnets (upon detection of high utilization). You can enter <i>size</i> as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.

Defaults The default size value is /0.

Command Modes DHCP pool configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.3(11)T	The file keyword was added.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines If you do not configure the pool as an autogrow pool, the pool will not request additional subnets if one subnet is already in the pool.

Use the **dhcp** keyword to obtain subnets from DHCP, the **aaa** keyword to obtain subnets from the AAA server, and the **ipcp** keyword to obtain subnets from IPCP negotiation. If you expect that the utilization of the pool may grow over time, use the **autogrow** *size* option. If a pool has been configured with the

autogrow *size* option, ensure that the source server is capable of providing more than one subnet to the same pool. Even though the Cisco IOS software specifies the requested subnet size, it can accept any offered subnet size from the source server.

Examples

The following example shows how to configure an address pool named green to use DHCP as the subnet allocation protocol with an initial subnet size of 24 and an autogrow subnet size of 24:

```
ip dhcp pool green
  vrf green
  origin dhcp subnet size initial /24 autogrow /24
  utilization mark high 80
  utilization mark low 20
```

The following example shows how to configure the location of the external text file:

```
ip dhcp pool abcpool
  origin file tftp://10.1.0.1/staticbindingfile
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

peer default ip address

To specify an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface, use the **peer default ip address** command in interface configuration mode. To disable a prior peer IP address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ip address {*ip-address* | **dhcp-pool** | **dhcp** | **pool** [*pool-name*]}

no peer default ip address

Syntax Description		
<i>ip-address</i>		Specific IP address to be assigned to a remote peer dialing in to the interface. To prevent duplicate IP addresses from being assigned on more than one interface, this argument cannot be applied to a dialer rotary group nor to an ISDN interface.
dhcp-pool		Retrieves an IP address from an on-demand address pool. This option only supports remote access (PPP) sessions into MPLS VPNs.
dhcp		Retrieves an IP address from the DHCP server.
pool		Uses the global default mechanism as defined by the ip address-pool command unless the optional <i>pool-name</i> argument is supplied. This is the default.
<i>pool-name</i>		(Optional) Name of a local address pool created using the ip local pool command. DHCP retrieves an address from this pool regardless of the global default mechanism setting.

Defaults The default is **pool**.

Command Modes Interface configuration

Command History	Release	Modification
	11.0	This command was introduced.
	12.2(8)T	The dhcp-pool keyword was added.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines This command applies to point-to-point interfaces that support the PPP or Serial Line Internet Protocol (SLIP) encapsulation. This command sets the address used on the remote (PC) side.



Note

This command replaces the **async default ip address** command.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.

The **peer default ip address** command can override the global default mechanism defined by the **ip address-pool** command on an interface-by-interface basis, as follows:

- For all interfaces not configured with a peer default IP address mechanism (equivalent to selecting the **peer default ip address pool** command), the router uses the global default mechanism that is defined by the **ip address-pool** command.
- If you select the **peer default ip address pool *pool-name*** form of this command, then the router uses the locally configured pool on this interface and does not follow the global default mechanism.
- If you select the **peer default ip address *ip-address*** form of this command, the specified IP address is assigned to any peer connecting to this interface and any global default mechanism is overridden for this interface.
- If you select the **peer default ip address dhcp** form of this command, the DHCP proxy-client mechanism is used by default on this interface and any global default mechanism is overridden for this interface.
- If you select the **peer default ip address dhcp-pool** form of this command, the DHCP on-demand address pooling mechanism is used by default on this interface and any global default mechanism is overridden for this interface.

Examples

The following command specifies that this interface will use a local IP address pool named pool3:

```
peer default ip address pool pool3
```

The following command specifies that this interface will use the IP address 172.19.34.21:

```
peer default ip address 172.19.34.21
```

The following command reenables the global default mechanism to be used on this interface:

```
peer default ip address pool
```

The following example specifies address 192.168.7.51 for asynchronous interface 6:

```
line 20
 speed 115200
 interface async 6
 peer default ip address 192.168.7.51
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.
encapsulation slip	Enables SLIP encapsulation.
exec	Allows an EXEC process on a line.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
ppp	Starts an asynchronous connection using PPP.

Command	Description
show cot dsp	Displays information about the COT DSP configuration or current status.
slip	Starts a serial connection to a remote host using SLIP.

show ip dhcp pool

To display information about the Dynamic Host Configuration Protocol (DHCP) address pools, use the **show ip dhcp pool** command in privileged EXEC configuration mode.

```
show ip dhcp pool [name]
```

Syntax Description	<i>name</i> (Optional) Displays information about a specific address pool. If not specified, displays information about all address pools.
--------------------	--

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines	Use this command to determine the subnets allocated and to examine the current utilization level for the pool or all the pools if the <i>name</i> argument is not used.
------------------	---

Examples	The following example shows DHCP address pool information for pool 1. Table 1 lists descriptions for each field in the example.
----------	---

```
Router# show ip dhcp pool 1

Pool 1:
  Utilization mark (high/low)      : 85 / 15
  Subnet size (first/next)          : 24 / 24 (autogrow)
  VRF name                          : RED
  Total addresses                   : 28
  Leased addresses                  : 11
  Pending event                     : none
  2 subnets are currently in the pool :
  Current index   IP address range   Leased addresses
  10.1.1.12       10.1.1.1 - 10.1.1.14 11
  10.1.1.17       10.1.1.17 - 10.1.1.30 0
```

Table 1 show ip dhcp pool Field Descriptions

Field	Description
Pool 1	The name of the pool.
Utilization mark (high/low)	The configured high and low utilization level for the pool.
Subnet size (first/next)	The size of the requested subnets.
VRF name	The VRF name to which the pool is associated.

Table 1 *show ip dhcp pool Field Descriptions (continued)*

Field	Description
Total addresses	The total number of addresses in the pool.
Leased addresses	The number of leased addresses in the pool.
Pending event	Displays any pending events.
2 subnets are currently in the pool	The number of subnets allocated to the address pool.
Current index	Displays the current index.
IP address range	The IP address range of the subnets.
Leased addresses	The number of leased addresses from each subnet.

utilization mark high

To configure the high utilization mark of the current address pool size, use the **utilization mark high** command in DHCP pool configuration mode. To remove the high utilization mark, use the **no** form of this command.

utilization mark high *percentage-number*

no utilization mark high *percentage-number*

Syntax Description

<i>percentage-number</i>	Percentage of the current pool size.
--------------------------	--------------------------------------

Defaults

The default high utilization mark is 100 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level exceeds the configured high utilization mark, the pool will schedule a subnet request.

This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured.

Examples

The following example sets the high utilization mark to 80 percent of the current pool size:

```
utilization mark high 80
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark low	Configures the low utilization mark of the current address pool size.

utilization mark low

To configure the low utilization mark of the current address pool size, use the **utilization mark low** command in DHCP pool configuration mode. To remove the low utilization mark, use the **no** form of this command.

utilization mark low *percentage-number*

no utilization mark low *percentage-number*

Syntax Description

<i>percentage-number</i>	Percentage of the current pool size.
--------------------------	--------------------------------------

Defaults

The default low utilization mark is 0 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level drops below the configured low utilization mark, a subnet release is scheduled from the address pool. This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured.

Examples

The following example sets the low utilization mark to 20 percent of the current pool size:

```
utilization mark low 20
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark high	Configures the high utilization mark of the current address pool size.

vrf

To associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name, use the **vrf** command in DHCP pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

<i>name</i>	Name of the VRF to which the address pool is associated.
-------------	--

Defaults

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Associating a pool with a VRF allows overlapping addresses with other pools that are not on the same VRF. Only one pool can be associated with each VRF. If the pool is configured with the **origin dhcp** command or **origin aaa** command, the VRF information is sent in the subnet request. If the VRF is configured with an RFC 2685 VPN ID, the VPN ID will be sent instead of the VRF name.

Examples

The following example associates the on-demand address pool with a VRF named red:

```
ip dhcp pool red_pool
  origin dhcp subnet size initial 24 autogrow 24
  utilization mark high 85
  utilization mark low 15
  vrf red
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

Cisco Access Registrar—A RADIUS server that supports service provider deployment of access services by centralizing AAA information and simplifying provisioning and management.

client—A host trying to configure its interface (obtain an IP address) using DHCP or BOOTP protocols.

DHCP—Dynamic Host Configuration Protocol.

incremental subnet size—The desired size of the second and subsequent subnets requested for an on-demand pool.

initial subnet size—The desired size of the first subnet requested for an on-demand pool.

IPCP—IP Control Protocol. Protocol that establishes and configures IP over PPP.

MPLS—Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

ODAP—on-demand address pool.

PE router—provider edge router.

PPP—Point-to-Point Protocol.

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

relay agent—A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

releasable subnet—A leased subnet that has no address leased from it.

server—DHCP or BOOTP server.

VHG—Virtual Home Gateway. A Cisco IOS software component that terminates PPP sessions. It is owned and managed by the service provider on behalf of its customer to provide access to remote users of that customers network. A single service provider device (router) can host multiple VHGs of different customers. A VHG can be dynamically brought up and down based on the access pattern of the remote users. Note that there is no single IOS feature called the VHG; it is a collection of function and features.

VHG/PE router—A device that terminates PPP sessions and maps the remote users to the corresponding MPLS VPNs.

VPN—Virtual Private Network. Enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

VPN information—In this document, VPN information refers to VRF name or VPN ID.

VRF—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Copyright © 2001–2005 Cisco Systems, Inc. All rights reserved.