



Configuring the DHCP Server On-Demand Address Pool Manager

Last Updated: December 20, 2011

The Cisco IOS Dynamic Host Configuration Protocol (DHCP) server on-demand address pool (ODAP) manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level. A DHCP pool configured in the router can also be used as an IP address pooling mechanism. The IP address pooling mechanism is configured in the router to specify the source of IP addresses for PPP peers.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Configuring the DHCP Server On-Demand Address Pool Manager, page 2](#)
- [Restrictions for Configuring the DHCP Server On-Demand Address Pool Manager, page 2](#)
- [Information About the DHCP Server On-Demand Address Pool Manager, page 2](#)
- [How to Configure the DHCP Server On-Demand Address Pool Manager, page 5](#)
- [Configuration Examples for DHCP Server On-Demand Address Pool Manager, page 28](#)
- [Additional References, page 35](#)
- [Feature Information for the DHCP Server On-Demand Address Pool Manager, page 37](#)
- [Glossary, page 38](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.



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

Prerequisites for Configuring the DHCP Server On-Demand Address Pool Manager

Before you configure the ODAP manager, you should understand the concepts documented in the “DHCP Overview” module.

You must configure standard Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) unless you intend to use non-MPLS VPNs.

In order for the IP address pooling mechanism to work correctly, the VPN routing and forwarding (VRF) instance 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 Authentication, Authorization, and Accounting (AAA) is used to authorize the PPP user, the command can be part of the user’s profile configuration.

Restrictions for Configuring the DHCP Server On-Demand Address Pool Manager

- The **ip dhcp excluded-address** command available in global configuration mode cannot be used to exclude addresses from VRF-associated pools.
- The **vrf** command available in DHCP pool configuration mode is currently not supported for host pools.
- Attribute inheritance is not supported on VRF pools.
- A router can be configured as a subnet allocation server and a DHCP server at the same time with one restriction: Separate pools must be created for subnet allocation and IP address assignment. An address pool cannot be used by DHCP for both subnet allocation and IP address assignment.

Information About the DHCP Server On-Demand Address Pool Manager

- [ODAP Manager Operation, page 2](#)
- [Subnet Allocation Server Operation, page 4](#)
- [Benefits of Using ODAPs, page 5](#)

ODAP Manager Operation

ODAPs enable pools of IP addresses to be dynamically increased or reduced in size depending on the address utilization level. 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.

ODAPs support address assignment using DHCP for customers using private addresses such as in MPLS VPNs. VPNs allow the possibility that two pools in separate networks can have the same address space, with private network addresses, served by the same DHCP server. These IP addresses can be distinguished by a VPN identifier to help select the VPN to which the client belongs.

Each ODAP is configured and associated with a particular MPLS VPN. Cisco IOS software also supports 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 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 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.

A PPP session belonging to a specific VPN is allocated an address only 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 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 considers 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 ODAP manager uses an 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.

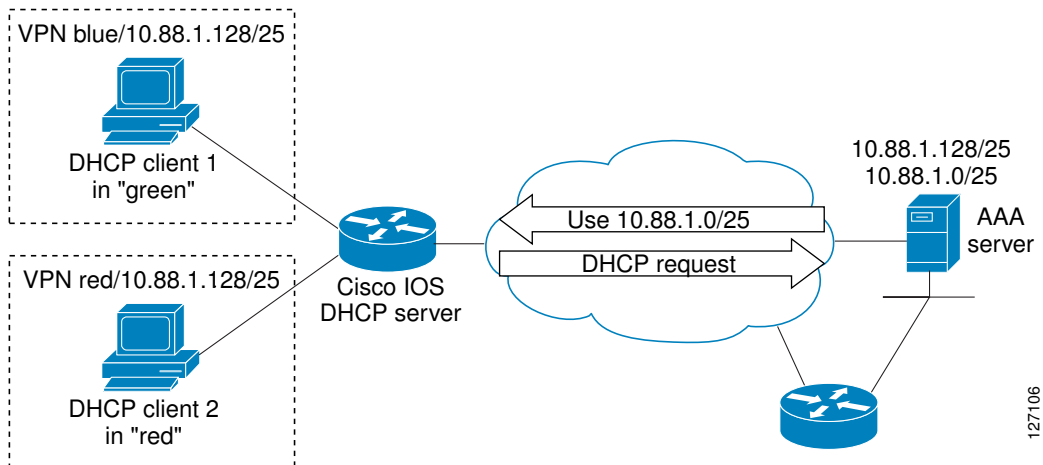
When a DHCP pool receives multiple subnets from an upstream DHCP server, an address from each subnet is automatically configured on the client connected interface so that the addresses within the subnets can be requested by DHCP clients.

The first address in the first subnet is automatically assigned to the primary address on the interface. The first address of each subsequent subnet is assigned to secondary addresses on the interface. In addition, as client addresses are reclaimed, the count of lease addresses for that subnet is decremented. Once a lease counter for a subnet reaches zero (that is, lease expiry), the subnet is returned to the pool. The previous address on the interface is removed and the first secondary address on the interface is promoted as the primary address of the interface.

The figure below shows an ODAP manager configured on the Cisco IOS DHCP server. The ODAP requests an initial pool from the AAA server. Clients make DHCP requests and the DHCP server fulfills requests from the pool. When the utilization rate meets 90 percent, the ODAP manager requests an

expansion and the AAA server allocates another subnet from which the ODAP manager can allocate addresses.

Figure 1 *ODAP Address Pool Management for MPLS VPNs*



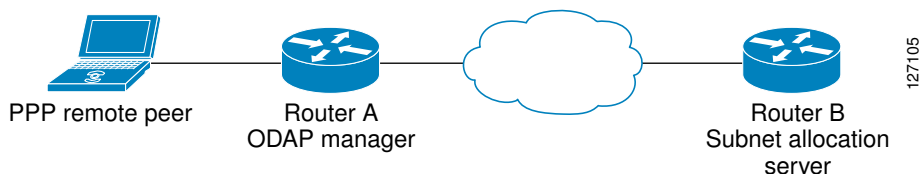
Subnet Allocation Server Operation

You can configure the ODAP manager to allocate subnets instead of individual IP addresses.

This capability allows the network operator to configure a Cisco IOS router as a subnet allocation server. The operation of a subnet allocation server is similar to the operation of a DHCP server, except that pools of subnets are created and assigned instead of pools of IP addresses. Subnet allocation pools are created and configured by using the **subnet prefix-length** command in DHCP pool configuration mode. The size of each assigned or allocated subnet is set by the *prefix-length* argument, using standard Common Interdomain Routing (CIDR) bit count notation to determine the number of addresses that are configured in each subnet lease.

When a DHCP server is configured as a subnet allocation server, it provides subnet allocation pools for ODAP manager allocation. In the figure below, Router B is the subnet allocation server and allocates subnets to the ODAP manager based on the demand for IP addresses and subnet availability. Router B is configured to allocate an initial amount of address space in the form of subnets to the ODAP manager. The size of the subnet allocated by the ODAP manager is determined by the subnet size that is configured on the subnet allocation server. The ODAP manager will then assign addresses to clients from these subnets and allocate more subnets as the need for address space increases.

Figure 2 *Subnet Allocation Server Topology*



When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP manager requires the address space. The binding is removed and the subnet is returned to the subnet pool only when the ODAP manager releases the subnet as address space utilization decreases.

The subnet allocation server can also be associated with a VRF. A VRF consists of an IP routing table, a derived Cisco Express Forwarding 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.

Benefits of Using ODAPs

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.

Multiple VRF and Independent Private Addressing Support

The ODAP manager automatically injects subnet routing information into the appropriate VRF.

How to Configure the DHCP Server On-Demand Address Pool Manager

- [Specifying DHCP ODAPs as the Global Default Mechanism, page 5](#)
- [Defining DHCP ODAPs on an Interface, page 6](#)
- [Configuring the DHCP Pool as an ODAP, page 7](#)
- [Configuring ODAPs to Obtain Subnets Through IPCP Negotiation, page 9](#)
- [Configuring AAA, page 11](#)
- [Configuring RADIUS, page 13](#)
- [Disabling ODAPs, page 15](#)
- [Verifying ODAP Operation, page 16](#)
- [Monitoring and Maintaining the ODAP, page 18](#)
- [Configuring DHCP ODAP Subnet Allocation Server Support, page 20](#)

Specifying DHCP ODAPs as the Global Default Mechanism

Perform this task to specify that the global default mechanism to use is on-demand address pooling.

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.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip address-pool dhcp-pool`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>ip address-pool dhcp-pool</code></p> <p>Example:</p> <pre>Router(config)# ip address-pool dhcp-pool</pre>	<p>Specifies on-demand address pooling as the global default IP address mechanism.</p> <ul style="list-style-type: none"> For remote access (PPP) sessions into MPLS VPNs, IP addresses are obtained from locally configured VRF-associated DHCP pools. <p>Note You must use two separate DHCP address pools for global configuration mode and VRF mode. If you change a global configuration pool to VRF mode, then all the IP addresses in the global pool will be lost. Hence make sure that you have a VRF pool for an interface in order to add an interface under a VRF.</p>

Defining DHCP ODAPs on an Interface

Perform this task to define on-demand address pools on an interface.

The interface on-demand address pooling configuration overrides the global default mechanism on that interface.

SUMMARY STEPS

- `enable`
- `configure terminal`
- `interface type number`
- `peer default ip address dhcp-pool [pool-name]`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>interface type number</code></p> <p>Example:</p> <pre>Router(config)# interface Virtual-Template 1</pre>	<p>Specifies the interface and enters interface configuration mode.</p>
<p>Step 4 <code>peer default ip address dhcp-pool [pool-name]</code></p> <p>Example:</p> <pre>Router(config)# peer default ip address dhcp-pool mypool</pre>	<p>Specifies an IP address from an on-demand address pool to be returned to a remote peer connecting to this interface.</p> <ul style="list-style-type: none"> The <i>pool-name</i> argument supports non-MPLS VPNs and is mandatory if the session is not associated with any VRF. Multiple pool names can be accepted but must be separated by blank spaces.

Configuring the DHCP Pool as an ODAP

Perform this task to configure a DHCP address pool as an ODAP pool.

SUMMARY STEPS

- `enable`
- `configure terminal`
- `ip dhcp pool pool-name`
- `vrf name`
- `origin {dhcp | aaa | ipcp} [subnet size initial size [autogrow size]]`
- `utilization mark low percentage-number`
- `utilization mark high percentage-number`
- `end`
- `show ip dhcp pool [pool-name]`

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>ip dhcp pool <i>pool-name</i></code></p> <p>Example:</p> <pre>Router(config)# ip dhcp pool pool1</pre>	<p>Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.</p>
<p>Step 4 <code>vrf <i>name</i></code></p> <p>Example:</p> <pre>Router(dhcp-config)# vrf vrf1</pre>	<p>(Optional) Associates the address pool with a VRF name.</p> <ul style="list-style-type: none"> Only use this command for MPLS VPNs.
<p>Step 5 <code>origin {dhcp aaa ipcp} [subnet size initial <i>size</i> [autogrow <i>size</i>]]</code></p> <p>Example:</p> <pre>Router(dhcp-config)# origin dhcp subnet size initial /16 autogrow /16</pre>	<p>Configures an address pool as an on-demand address pool.</p> <ul style="list-style-type: none"> 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. You can enter size as either the subnet mask (<i>nnnn.nnnn.nnnn.nnnn</i>) or prefix size (<i>/nn</i>). The valid values are /0 and /4 to /30. When a DHCP pool receives multiple subnets from an upstream DHCP server, an address from each subnet is automatically configured on the client connected interface so that the addresses within the subnets can be requested by DHCP clients. The first address in the first subnet is automatically assigned to the primary address on the interface. The first address of each subsequent subnet is assigned to secondary addresses on the interface. In addition, as client addresses are reclaimed, the count of lease addresses for that subnet is decremented. Once a lease counter for a subnet reaches zero (that is, lease expiry), the subnet is returned to the pool. The previous address on the interface is removed and the first secondary address on the interface is promoted as the primary address of the interface. If the origin aaa option is configured, AAA must be configured.

Command or Action	Purpose
<p>Step 6 <code>utilization mark low <i>percentage-number</i></code></p> <p>Example:</p> <pre>Router(dhcp-config)# utilization mark low 40</pre>	<p>Sets the low utilization mark of the pool size.</p> <ul style="list-style-type: none"> This command cannot be used unless the autogrow size option of the origin command is configured. The default value is 0 percent.
<p>Step 7 <code>utilization mark high <i>percentage-number</i></code></p> <p>Example:</p> <pre>Router(dhcp-config)# utilization mark high 60</pre>	<p>Sets the high utilization mark of the pool size.</p> <ul style="list-style-type: none"> This command cannot be used unless the autogrow size option of the origin command is configured. The default value is 100 percent.
<p>Step 8 <code>end</code></p> <p>Example:</p> <pre>Router(dhcp-config)# end</pre>	<p>Returns to privileged EXEC mode.</p>
<p>Step 9 <code>show ip dhcp pool [<i>pool-name</i>]</code></p> <p>Example:</p> <pre>Router# show ip dhcp pool</pre>	<p>(Optional) Displays information about DHCP address pools.</p> <ul style="list-style-type: none"> Information about the primary and secondary interface address assignment is also displayed.

Configuring ODAPs to Obtain Subnets Through IPCP Negotiation

Perform this task to configure ODAPs to use subnets obtained through IP Control Protocol (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 (IPCP) negotiation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **import all**
5. **origin ipcp**
6. **exit**
7. **interface** *type number*
8. **ip address pool** *pool-name*

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 ip dhcp pool <i>pool-name</i> Example: <pre>Router(config)# ip dhcp pool red-pool</pre>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 4 import all Example: <pre>Router(dhcp-config)# import all</pre>	Imports option parameters into the Cisco IOS DHCP server database.
Step 5 origin ipcp Example: <pre>Router(dhcp-config)# origin ipcp</pre>	Configures an address pool as an on-demand address pool using IPCP as the subnet allocation protocol.

Command or Action	Purpose
Step 6 <code>exit</code> Example: <code>Router(dhcp-config)# exit</code>	Exits DHCP pool configuration mode.
Step 7 <code>interface type number</code> Example: <code>Router(config)# interface ethernet 0</code>	Specifies the interface and enters interface configuration mode.
Step 8 <code>ip address pool pool-name</code> Example: <code>Router(config-if)# ip address pool red-pool</code>	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 AAA server, the AAA client must be configured on the VHG/PE router.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authorization configuration default group radius`
5. `aaa accounting network default start-stop group radius`
6. `aaa session-id common`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 <code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3 <code>aaa new-model</code> Example: <code>Router(config)# aaa new-model</code>	Enables AAA access control.
Step 4 <code>aaa authorization configuration default group radius</code> Example: <code>Router(config)# aaa authorization configuration default group radius</code>	Downloads static route configuration information from the AAA server using RADIUS.

Command or Action	Purpose
<p>Step 5 <code>aaa accounting network default start-stop group radius</code></p> <p>Example:</p> <p>or</p> <p>Example:</p> <p style="text-align: center;"><code>aaa accounting network default stop-only group radius</code></p> <p>Example:</p> <pre>Router(config)# aaa accounting network default start-stop group radius</pre> <p>Example:</p> <p>or</p> <p>Example:</p> <p>Example:</p> <pre>Router(config)# aaa accounting network default stop-only group radius</pre>	<p>Enables AAA accounting of requested services for billing or security purposes when you use RADIUS, and sends a “start” accounting notice at the beginning of a process.</p> <p>or</p> <p>Enables AAA accounting of requested services for billing or security purposes when you use RADIUS, and sends a “stop” accounting notice at the end of the requested user process.</p>
<p>Step 6 <code>aaa session-id common</code></p> <p>Example:</p> <pre>Router(config)# aaa session-id common</pre>	<p>Ensures that the same session ID will be used for each AAA accounting service type within a call.</p>

Configuring RADIUS

- [ODAP AAA Profile, page 13](#)

ODAP AAA Profile

The AAA server sends the RADIUS Cisco attribute value (AV) pair attributes “pool-addr” and “pool-mask” to the Cisco IOS DHCP server in the access request and access accept. The pool-addr attribute is the

IP address and the pool-mask attribute is the network mask (for example, pool-addr=192.168.1.0 and pool-mask=255.255.0.0). Together, these attributes comprise a network address (address/mask) that is allocated by the AAA server to the Cisco IOS DHCP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface *subinterface-name***
4. **radius-server host *ip-address* *auth-port* *port-number* *acct-port* *port-number***
5. **radius server attribute 32 include-in-access-req**
6. **radius server attribute 44 include-in-access-req**
7. **radius-server vsa send accounting**
8. **radius-server vsa send authentication**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 ip radius source-interface <i>subinterface-name</i></p> <p>Example:</p> <pre>Router(config)# ip radius source-interface Ethernet1/1</pre>	<p>Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.</p>
<p>Step 4 radius-server host <i>ip-address</i> <i>auth-port</i> <i>port-number</i> <i>acct-port</i> <i>port-number</i></p> <p>Example:</p> <pre>Router(config)# radius-server host 172.16.1.1 auth-port 1645 acct-port 1646</pre>	<p>Specifies a RADIUS server host.</p> <ul style="list-style-type: none"> • The <i>ip-address</i> argument specifies the IP address of the RADIUS server host.

Command or Action	Purpose
<p>Step 5 <code>radius server attribute 32 include-in-access-req</code></p> <p>Example:</p> <pre>Router(config)# radius server attribute 32 include-in-access-req</pre>	Sends RADIUS attribute 32 (NAS-Identifier) in an access request or accounting request.
<p>Step 6 <code>radius server attribute 44 include-in-access-req</code></p> <p>Example:</p> <pre>Router(config)# radius server attribute 44 include-in-access-req</pre>	Sends RADIUS attribute 44 (Accounting Session ID) in an access request or accounting request.
<p>Step 7 <code>radius-server vsa send accounting</code></p> <p>Example:</p> <pre>Router(config)# radius-server vsa send accounting</pre>	Configures the network access server (NAS) to recognize and use vendor-specific accounting attributes.
<p>Step 8 <code>radius-server vsa send authentication</code></p> <p>Example:</p> <pre>Router(config)# radius-server vsa send authentication</pre>	Configures the NAS to recognize and use vendor-specific authentication attributes.

Disabling ODAPs

This task shows how to disable an ODAP from a DHCP pool.

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.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip dhcp pool pool-name`
4. `no origin {dhcp | aaa | ipcp}`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>ip dhcp pool <i>pool-name</i></code> Example: <pre>Router(config)# ip dhcp pool pool1</pre>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 4 <code>no origin {dhcp aaa ipcp}</code> Example: <pre>Router(dhcp-config)# no origin dhcp</pre>	Disables the ODAP.

Verifying ODAP Operation**SUMMARY STEPS**

- enable**
- show ip dhcp binding** The following output 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. No bindings are shown under the Bindings from all pools not associated with VRF field because the Global pool has not allocated any addresses.

DETAILED STEPS

-
- Step 1** `enable`
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

show ip dhcp pool [pool-name] 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, and pool Global is configured to be in the global address space.

Example:

```
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

show ip dhcp binding The following output 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. No bindings are shown under the Bindings from all pools not associated with VRF field because the Global pool has not allocated any addresses.

Example:

```
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, page 18](#)

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 Internet Control Message Protocol (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 pool-name subnet *` command.

Monitoring and Maintaining the ODAP

This task shows how to monitor and maintain the ODAP. These commands need not be entered in any specific order.

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** *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** *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** *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** *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.

SUMMARY STEPS

1. **enable**
2. **clear ip dhcp [pool *pool-name*] binding {* | *address*}**
3. **clear ip dhcp [pool *pool-name*] conflict {* | *address*}**
4. **clear ip dhcp [pool *pool-name*] subnet {* | *address*}**
5. **debug dhcp details**
6. **debug ip dhcp server events**
7. **show ip dhcp import**
8. **show ip interface [*type number*]**
9. **show ip dhcp pool *pool-name***

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 clear ip dhcp [pool <i>pool-name</i>] binding {* <i>address</i>} Example: Router# clear ip dhcp binding *	Clears an automatic address binding or objects from a specific pool from the DHCP server database.
Step 3 clear ip dhcp [pool <i>pool-name</i>] conflict {* <i>address</i>} Example: Router# clear ip dhcp conflict *	Clears an address conflict or conflicts from a specific pool from the DHCP server database.

Command or Action	Purpose
<p>Step 4 <code>clear ip dhcp [pool <i>pool-name</i>] subnet {* <i>address</i>}</code></p> <p>Example:</p> <pre>Router# clear ip dhcp subnet *</pre>	Clears all currently leased subnets in the named DHCP pool or all DHCP pools if <i>pool-name</i> is not specified.
<p>Step 5 <code>debug dhcp details</code></p> <p>Example:</p> <pre>Router# debug dhcp details</pre>	Monitors the subnet allocation/releasing in the on-demand address pools.
<p>Step 6 <code>debug ip dhcp server events</code></p> <p>Example:</p> <pre>Router# debug ip dhcp server events</pre>	Reports DHCP server events, such as address assignments and database updates.
<p>Step 7 <code>show ip dhcp import</code></p> <p>Example:</p> <pre>Router# show ip dhcp import</pre>	Displays the option parameters that were imported into the DHCP server database.
<p>Step 8 <code>show ip interface [<i>type number</i>]</code></p> <p>Example:</p> <pre>Router# show ip interface</pre>	Displays the usability status of interfaces configured for IP.
<p>Step 9 <code>show ip dhcp pool <i>pool-name</i></code></p> <p>Example:</p> <pre>Router# show ip dhcp pool green</pre>	Displays DHCP address pool information.

Configuring DHCP ODAP Subnet Allocation Server Support

- [Configuring a Global Subnet Pool on a Subnet Allocation Server, page 21](#)
- [Configuring a VRF Subnet Pool on a Subnet Allocation Server, page 22](#)
- [Using a VPN ID to Configure a VRF Subnet Pool on a Subnet Allocation Server, page 23](#)
- [Verifying Subnet Allocation and DHCP Bindings, page 26](#)
- [Troubleshooting the DHCP ODAP Subnet Allocation Server, page 27](#)

Configuring a Global Subnet Pool on a Subnet Allocation Server

- [Global Subnet Pools, page 21](#)

Global Subnet Pools

Global subnet pools are created in a centralized network. The ODAP manager allocates subnets from the subnet allocation server based on subnet availability. When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP manager requires the address space. The binding is destroyed and the subnet is returned to the subnet pool only when the ODAP manager releases the subnet as address space utilization decreases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *network-number* [*mask* / *prefix-length*]
5. **subnet prefix-length** *prefix-length*

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip dhcp pool <i>pool-name</i> Example: Router(config)# ip dhcp pool GLOBAL-POOL	Enters DHCP pool configuration mode and specifies the subnet pool name.

Command or Action	Purpose
<p>Step 4 <code>network network-number [mask] / prefix-length</code></p> <p>Example:</p> <pre>Router(dhcp-config)# network 10.0.0.0 255.255.255.0</pre>	<p>Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.</p> <ul style="list-style-type: none"> The subnet mask or the prefix length can be configured in this step. The values that can be configured for the <i>prefix-length</i> argument follow CIDR bit count notation. The forward slash character must be used when configuring the <i>prefix-length</i> argument.
<p>Step 5 <code>subnet prefix-length prefix-length</code></p> <p>Example:</p> <pre>Router(dhcp-config)# subnet prefix- length 8</pre>	<p>Configures the subnet prefix length. The range of the <i>prefix-length</i> argument is from 1 to 31.</p> <ul style="list-style-type: none"> This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the <i>prefix-length</i> argument follow CIDR bit count notation format.

Configuring a VRF Subnet Pool on a Subnet Allocation Server

- [VRF Subnet Pools, page 22](#)

VRF Subnet Pools

A subnet allocation server can be configured to assign subnets from VRF subnet allocation pools for MPLS VPN clients. VPN routes between the ODAP manager and the subnet allocation server are configured based on the VRF name or VPN ID configuration. The VRF and VPN ID are configured to maintain routing information that defines customer VPN sites. The VPN customer site (or customer equipment [CE]) is attached to a PE router. The VRF is used to specify the VPN and consists of an IP routing table, a derived Cisco Express Forwarding 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.

The VRF name and VPN ID can be configured on the ODAP manager and subnet allocation server prior to the configuration of the subnet allocation pool.

SUMMARY STEPS

- enable**
- configure terminal**
- ip dhcp pool** *pool-name*
- vrf** *vrf-name*
- network** *network-number* [*mask* | / *prefix-length*]
- subnet prefix-length** *prefix-length*

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 <code>ip dhcp pool <i>pool-name</i></code></p> <p>Example:</p> <pre>Router(config)# ip dhcp pool VRF-POOL</pre>	<p>Enters DHCP pool configuration mode and specifies the subnet pool name.</p>
<p>Step 4 <code>vrf <i>vrf-name</i></code></p> <p>Example:</p> <pre>Router(dhcp-config)# vrf vrf1</pre>	<p>Associates the on-demand address pool with a VRF instance name (or tag).</p> <ul style="list-style-type: none"> The <code>vrf</code> command and <code>vrf-name</code> argument are used to specify the VPN for the VRF pool. The <code>vrf-name</code> argument must match the VRF name (or tag) that is configured for the client.
<p>Step 5 <code>network <i>network-number</i> [<i>mask</i> / <i>prefix-length</i>]</code></p> <p>Example:</p> <pre>Router(dhcp-config)# network 10.1.1.0 /24</pre>	<p>Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.</p> <ul style="list-style-type: none"> The subnet mask or the prefix length can be configured in this step. The values that can be configured for the <code>prefix-length</code> argument follow CIDR bit count notation. The forward slash character must be used when configuring the <code>prefix-length</code> argument.
<p>Step 6 <code>subnet prefix-length <i>prefix-length</i></code></p> <p>Example:</p> <pre>Router(dhcp-config)# subnet prefix-length 16</pre>	<p>Configures the subnet prefix length.</p> <ul style="list-style-type: none"> The range of the <code>prefix-length</code> argument is from 1 to 31. This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the <code>prefix-length</code> argument follow CIDR bit count notation format.

Using a VPN ID to Configure a VRF Subnet Pool on a Subnet Allocation Server

Perform this task to configure a VRF subnet pool, using a VPN ID, on a subnet allocation server.

- [VRF Pools and VPN IDs, page 24](#)

VRF Pools and VPN IDs

A subnet allocation server can be configured to assign subnets from VPN subnet allocation pools based on the VPN ID of a client. The VPN ID (or Organizational Unique Identifier [OUI]) is a unique identifier assigned by the IEEE.

The VRF name and VPN ID can be configured on the ODAP manager and subnet allocation server prior to the configuration of the subnet allocation pool.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target both** *route-target-number*
6. **vpn id** *vpn-id*
7. **exit**
8. **ip dhcp pool** *pool-name*
9. **vrf** *vrf-name*
10. **network** *network-number* [*mask*]/*prefix-length*]
11. **subnet prefix-length** *prefix-length*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip vrf <i>vrf-name</i> Example: Router(config)# ip vrf vrf1	Creates a VRF routing table and specifies the VRF name (or tag). <ul style="list-style-type: none"> • The <i>vrf-name</i> argument must match the VRF name that is configured for the client and VRF pool in Step 9.

	Command or Action	Purpose
Step 4	<p>rd <i>route-distinguisher</i></p> <p>Example:</p> <pre>Router(config-vrf)# rd 100:1</pre>	<p>Creates routing and forwarding tables for a VRF instance created in Step 3.</p> <ul style="list-style-type: none"> There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).
Step 5	<p>route-target both <i>route-target-number</i></p> <p>Example:</p> <pre>Router(config-vrf)# route-target both 100:1</pre>	<p>Creates a route-target extended community for the VRF instance that was created in Step 3.</p> <ul style="list-style-type: none"> The both keyword is used to specify which routes should be imported and exported to the target VPN extended community (or the ODAP manager in this configuration). The <i>route-target-number</i> argument follows the same format as the <i>route-distinguisher</i> argument in Step 4. These two arguments must match.
Step 6	<p>vpn id <i>vpn-id</i></p> <p>Example:</p> <pre>Router(config-vrf)# vpn id 1234:123456</pre>	<p>Configures the VPN ID.</p> <ul style="list-style-type: none"> This command is used only if the client (ODAP manager) is also configured with or assigned a VPN ID.
Step 7	<p>exit</p> <p>Example:</p> <pre>Router(config-vrf)# exit</pre>	<p>Exits VRF configuration mode and enters global configuration mode.</p>
Step 8	<p>ip dhcp pool <i>pool-name</i></p> <p>Example:</p> <pre>Router(config)# ip dhcp pool VPN-POOL</pre>	<p>Enters DHCP pool configuration mode and specifies the subnet pool name.</p> <ul style="list-style-type: none"> The vrf keyword and <i>vrf-name</i> argument are used to specify the VPN for the VRF pool. The <i>vrf-name</i> argument must match the VRF name (or tag) that is configured for the client.
Step 9	<p>vrf <i>vrf-name</i></p> <p>Example:</p> <pre>Router(dhcp-config)#vrf RED</pre>	<p>Associates the on-demand address pool with a VRF instance name.</p> <ul style="list-style-type: none"> The <i>vrf-name</i> argument must match the <i>vrf-name</i> argument that was configured in Step 3.

Command or Action	Purpose
<p>Step 10 <code>network network-number [mask]/prefix-length</code></p> <p>Example:</p> <pre>Router(dhcp-config)# network 192.168.0.0 /24</pre>	<p>Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.</p> <ul style="list-style-type: none"> The subnet mask or the prefix length can be configured in this step. The values that can be configured for the <i>prefix-length</i> argument follow CIDR bit count notation. The forward slash character must be used when configuring the <i>prefix-length</i> argument.
<p>Step 11 <code>subnet prefix-length prefix-length</code></p> <p>Example:</p> <pre>Router(dhcp-config)# subnet prefix-length 16</pre>	<p>Configures the subnet prefix length.</p> <ul style="list-style-type: none"> The range of the <i>prefix-length</i> argument is from 1 to 31. This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the <i>prefix-length</i> argument follow CIDR bit count notation format.

Verifying Subnet Allocation and DHCP Bindings

Perform this task to verify subnet allocation and DHCP bindings. The **show** commands need not be entered in any specific order.

The **show ip dhcp pool** and **show ip dhcp binding** commands need not be issued together or even in the same session because there are differences in the information that is provided. These commands, however, can be used to display and verify subnet allocation and DHCP bindings. The **show running-config | begin dhcp** command is used to display the local configuration of DHCP and the configuration of the **subnet prefix-length** command.

SUMMARY STEPS

1. **enable**
2. **show running-config | begin dhcp**
3. **show ip dhcp pool [pool-name]**
4. **show ip dhcp binding [ip-address]**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.

Command or Action	Purpose
<p>Step 2 <code>show running-config begin dhcp</code></p> <p>Example:</p> <pre>Router# show running-config begin dhcp</pre>	<p>Displays the local configuration of the router.</p> <ul style="list-style-type: none"> The configuration of the subnet prefix-length command will be displayed under the DHCP pools, for which subnet lease allocation has been configured. The subnet allocation size will be shown, following this command, in CIDR bit count notation. The sample output is filtered with the begin keyword to start displaying output at the DHCP section of the running configuration.
<p>Step 3 <code>show ip dhcp pool [pool-name]</code></p> <p>Example:</p> <pre>Router# show ip dhcp pool</pre>	<p>Displays information about DHCP pools.</p> <ul style="list-style-type: none"> This command can be used to verify subnet allocation pool configuration on both the subnet allocation server and the ODAP manager. The output of this command displays specific address pool information, including the name of the pool, utilization of address space, subnet size, number of total addresses, number of leased address, and pending events.
<p>Step 4 <code>show ip dhcp binding [ip-address]</code></p> <p>Example:</p> <pre>Router# show ip dhcp binding</pre>	<p>Displays information about DHCP bindings.</p> <ul style="list-style-type: none"> This command can be used to display subnet allocation to DHCP binding mapping information. The output from this command displays binding information for individual IP address assignment and allocated subnets. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address display only an IP address and are not followed by a subnet mask.

Troubleshooting the DHCP ODAP Subnet Allocation Server

SUMMARY STEPS

- enable
- debug dhcp [detail]
- debug ip dhcp server {events | packets | linkage}

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.

Command or Action	Purpose
<p>Step 2 <code>debug dhcp [detail]</code></p> <p>Example:</p> <pre>Router# debug dhcp detail</pre>	<p>Displays debugging information about DHCP client activities and monitors the status of DHCP packets.</p> <ul style="list-style-type: none"> This example is issued with the detail keyword on the ODAP manager. The detail keyword is used to display and monitor the lease entry structure of the client and the state transitions of lease entries. This command also displays the values of the <code>op</code>, <code>htype</code>, <code>hlen</code>, <code>hops</code>, server identifier option, <code>xid</code>, <code>secs</code>, <code>flags</code>, <code>ciaddr</code>, <code>yiaddr</code>, <code>siaddr</code>, and <code>giaddr</code> fields of the DHCP packet that are shown in addition to the length of the options field.
<p>Step 3 <code>debug ip dhcp server {events packets linkage}</code></p> <p>Example:</p> <pre>Router# debug ip dhcp server packets</pre>	<p>Enables DHCP server debugging.</p> <ul style="list-style-type: none"> This example is issued with the packets keyword on the subnet allocation server. The output displays lease transition, reception, and database information.

Configuration Examples for DHCP Server On-Demand Address Pool Manager

- [Specifying DHCP ODAPs as the Global Default Mechanism Example, page 28](#)
- [Defining DHCP ODAPs on an Interface Example, page 29](#)
- [Configuring the DHCP Pool as an ODAP Example, page 29](#)
- [Configuring the DHCP Pool as an ODAP for Non-MPLS VPNs Example, page 31](#)
- [IPCP Subnet Mask Delivery Example, page 32](#)
- [Configuring AAA and RADIUS Example, page 33](#)
- [Configuring a Global Pool on a Subnet Allocation Server Example, page 33](#)
- [Configuring a VRF Pool on a Subnet Allocation Server Example, page 34](#)
- [Using a VPN ID to Configure a VRF Pool on a Subnet Allocation Server Example, page 34](#)
- [Verifying Local Configuration on a Subnet Allocation Server Example, page 34](#)
- [Verifying Address Pool Allocation Information Example, page 35](#)
- [Verifying Subnet Allocation and DHCP Bindings Example, page 35](#)

Specifying DHCP ODAPs as the Global Default Mechanism Example

The following example shows how to configure the on-demand address pooling mechanism to 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-Template 1
 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 password
!
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 192.0.2.1 255.255.255.255
!
interface Loopback1
 ip vrf forwarding Green
 ip address 192.0.2.2 255.255.255.255
!
```

```

interface Loopback2
 ip vrf forwarding Red
 ip address 192.0.2.3 255.255.255.255
!
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 192.0.2.4 255.255.255.224
 duplex half
!
interface Ethernet4/1
 ip address 192.0.2.5 255.255.255.0
 duplex half
!
interface Ethernet4/2
 ip address 192.0.2.6 255.255.255.0
 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 209.165.200.225 255.255.255.224 area 0
 network 209.165.200.226 255.255.255.224 area 0
 network 209.165.200.227 255.255.255.224 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.0.2.1 remote-as 100
 neighbor 192.0.2.2 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 password
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
    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

```

Configuring a Global Pool on a Subnet Allocation Server Example

The following example shows how to configure a router to be a subnet allocation server and create a global subnet allocation pool named “GLOBAL-POOL” that allocates subnets from the 10.0.0.0/24 network. The use of the **subnet prefix-length** command in this example configures the size of each subnet that is allocated from the subnet pool to support 254 host IP addresses.

```

ip dhcp pool GLOBAL-POOL
  network 10.0.0.0 255.255.255.0

```

```

subnet prefix-length 24
!

```

Configuring a VRF Pool on a Subnet Allocation Server Example

The following example shows how to configure a router to be a subnet allocation server and create a VRF subnet allocation pool named “VRF-POOL” that allocates subnets from the 172.16.0.0/16 network and configures the VPN to match the VRF named “RED.” The use of the **subnet prefix-length** command in this example configures the size of each subnet that is allocated from the subnet pool to support 62 host IP addresses.

```

ip dhcp pool VRF-POOL
vrf RED
network 172.16.0.0 /16
subnet prefix-length 26
!

```

Using a VPN ID to Configure a VRF Pool on a Subnet Allocation Server Example

The following example shows how to configure a router to be a subnet allocation server and create a VRF subnet allocation pool named “VRF-POOL” that allocates subnets from the 192.168.0.0/24 network and configures the VRF named “RED.” The VPN ID must match the unique identifier that is assigned to the client site. The route target and route distinguisher are configured in the as-number:network-number format. The route target and route distinguisher must match. The configuration of the **subnet prefix-length** command in this example configures the size of each subnet that is allocated from the subnet pool to support 30 host IP addresses.

```

ip vrf RED
rd 100:1
route-target both 100:1
vpn id 1234:123456
exit
ip dhcp pool VPN-POOL
vrf RED
network 192.168.0.0 /24
subnet prefix-length /27
exit

```

Verifying Local Configuration on a Subnet Allocation Server Example

The following example is output from the **show running-config** command. This command can be used to verify the local configuration on a subnet allocation server. The output from this command displays the configuration of the **subnet prefix-length** command under the DHCP pool named “GLOBAL-POOL.” The total size of the subnet allocation pool is set to 254 addresses with the **network** command. The use of the **subnet prefix-length** command configures this pool to allocate a subnet that will support 254 host IP addresses. Because the total pool size supports only 254 addresses, only one subnet can be allocated from this pool.

```

Router# show running-config | begin dhcp
ip dhcp pool GLOBAL-POOL
  network 10.0.0.0 255.255.255.0
  subnet prefix-length 24
!

```

Verifying Address Pool Allocation Information Example

The following examples are output from the **show ip dhcp pool** command. This command can be used to verify subnet allocation pool configuration on the subnet allocation server and the ODAP manager. The output from this command displays information about the address pool name, utilization level, configured subnet size, total number of addresses (from subnet), pending events, and specific subnet lease information.

The following sample output shows that the configured subnet allocation size is /24 (254 IP addresses), that there is a pending subnet allocation request, and that no subnets are in the pool:

```
Router# show ip dhcp pool ISP-1
Pool ISP-1 :
  Utilization mark (high/low)      :100 / 0
  Subnet size (first/next)         :24 / 24 (autogrow)
  Total addresses                  :0
  Leased addresses                 :0
  Pending event                    :subnet request
  0 subnet is currently in the pool
```

The next example shows that the configured subnet allocation size is /24 (254 IP address), the configured VRF name is “RED” and a subnet containing 254 IP addresses has been allocated but no IP addresses have been leased from the subnet:

```
Router# show ip dhcp pool SUBNET-ALLOC
Pool SUBNET-ALLOC :
  Utilization mark (high/low)      :100 / 0
  Subnet size (first/next)         :24 / 24 (autogrow)
  VRF name                         :RED
  Total addresses                  :254
  Leased addresses                 :0
  Pending event                    :none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  10.0.0.1           10.0.0.1           - 10.0.0.254      0
```

Verifying Subnet Allocation and DHCP Bindings Example

The following example is from the **show ip dhcp binding** command. This command can be used to display subnet allocation to DHCP binding mapping information. The output of this command shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default). The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet) in CIDR bit count notation. Bindings for individual IP address display only an IP address and are not followed by a subnet mask.

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration      Type
                Hardware address/
                User name
10.0.0.0/26     0063.6973.636f.2d64.  Mar 29 2003 04:36 AM  Automatic
                656d.6574.6572.2d47.
                4c4f.4241.4c
```

Additional References

The following sections provide references related to configuring the DHCP ODAP manager.

Related Documents

Related Topic	Document Title
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Addressing Services Command Reference</i>
DHCP conceptual information	“DHCP Overview” module
DHCP server configuration	“Configuring the Cisco IOS DHCP Server” module
DHCP client configuration	“Configuring the Cisco IOS DHCP Client” module
DHCP relay agent configuration	“Configuring the Cisco IOS DHCP Relay Agent” module
DHCP advanced features	“Configuring DHCP Services for Accounting and Security” module
DHCP enhancements for edge-session management configuration	“Configuring DHCP Enhancements for Edge-Session Management” module
DHCP options	“DHCP Options” appendix in the <i>Network Registrar User’s Guide</i> , Release 6.1.1

Standards

Standards	Title
No new or modified standards are supported by this functionality.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 951	<i>Bootstrap Protocol (BOOTP)</i>
RFC 1542	<i>Clarifications and Extensions for the Bootstrap Protocol</i>
RFC 2131	<i>Dynamic Host Configuration Protocol</i>

RFCs	Title
RFC 2685	<i>Virtual Private Networks Identifier</i>
RFC 3046	<i>DHCP Relay Information Option</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for the DHCP Server On-Demand Address Pool Manager

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for the DHCP On-Demand Address Pool Manager

Feature Name	Releases	Feature Configuration Information
DHCP Server On-Demand Address Pool Manager for Non-MPLS VPNs	12.2(15)T 12.2(28)SB 12.2(33)SRC	<p>This feature was enhanced to provide ODAP support for non-MPLS VPNs.</p> <p>The following command was modified by this feature: peer default ip address.</p>

Feature Name	Releases	Feature Configuration Information
DHCP ODAP Server Support	12.2(15)T 12.2(28)SB 12.2(33)SRC	<p>This feature introduces the capability to configure a DHCP server (or router) as a subnet allocation server. This capability allows the Cisco IOS DHCP server to be configured with a pool of subnets for lease to ODAP clients.</p> <p>The following commands were introduced or modified by this feature: show ip dhcp binding, subnet prefix-length.</p>
DHCP Server On-Demand Address Pool Manager	12.2(8)T 12.28(SB) 12.2(33)SRC	<p>The ODAP manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level.</p> <p>The following commands were introduced or modified: aaa session-id, clear ip dhcp binding, clear ip dhcp conflict, clear ip dhcp subnet, ip address-pool, ip address pool, ip dhcp aaa default username, origin, peer default ip address, show ip dhcp pool, utilization mark high, utilization mark low, vrf.</p>

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 customer's 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 no single Cisco IOS feature is 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.

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.

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

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

© 2011 Cisco Systems, Inc. All rights reserved.