

Configuring the DHCP Server On-Demand Address Pool Manager

The Cisco IOS XE 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 XE 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.

- Prerequisites for Configuring the DHCP Server On-Demand Address Pool Manager, on page 1
- Restrictions for Configuring the DHCP Server On-Demand Address Pool Manager, on page 2
- Information About the DHCP Server On-Demand Address Pool Manager, on page 2
- How to Configure the DHCP Server On-Demand Address Pool Manager, on page 5
- How to Configure DHCP ODAP Subnet Allocation Server Support, on page 18
- Configuration Examples for DHCP Server On-Demand Address Pool Manager, on page 26
- Additional References, on page 32
- Feature Information for the DHCP Server On-Demand Address Pool Manager, on page 34
- Glossary, on page 35

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 instance (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.

Note For a default session, you can apply access interface VRF and VRF service simultaneously.

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

- From Cisco IOS Release 17.6.1, you can use the **ip dhcp excluded-address** *vrf-name* global configuration command to exclude addresses from the VRF associated pools.
- The **vrf** DHCP pool configuration command 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

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 XE 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 (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.

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 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 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.

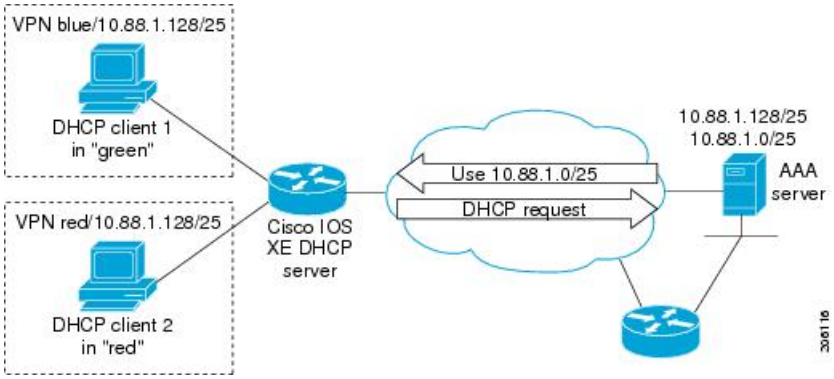
Subnet release from an ODAP follows a Last Leased subnet First (LLF) policy, which prefers the last leased subnet to be released first. This LLF policy searches for a releasable subnet (a subnet with no addresses currently being leased) starting with the last leased subnet. If a releasable subnet is 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 XE 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 also configure the ODAP manager to allocate subnets instead of individual IP addresses.

This capability allows the network operator to configure a Cisco IOS XE 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 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.

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

Defining 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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip address-pool dhcp-pool** **Example:** `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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **peer default ip address dhcp-pool** [*pool-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Virtual-Template1`	Specifies the interface and enters interface configuration mode.
Step 4	**peer default ip address dhcp-pool** [*pool-name*] **Example:** `Router(config-if)# peer default ip address dhcp-pool mypool`	Specifies an IP address from an on-demand address pool to be returned to a remote peer connecting to this interface. • The *pool-name* 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 space.

Configuring the DHCP Pool as an ODAP

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **vrf** *name*
5. **origin** {**dhcp** | **aaa**| **ipcp**} [**subnet size initial** *size* [**autogrow** *size*]]
6. **utilization mark low** *percentage-number*

7. **utilization mark high** *percentage-number*
8. **end**
9. **show ip dhcp pool** [*pool-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool red-pool`	Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode.
Step 4	**vrf** *name* **Example:** `Router(dhcp-config)# vrf red`	(Optional) Associates the address pool with a VRF name. • Only use this command for MPLS VPNs.
Step 5	**origin** {**dhcp** | **aaa**| **ipcp**} [**subnet size initial** *size* [**autogrow** *size*]] **Example:** `Router(dhcp-config)# origin dhcp subnet size initial /16 autogrow /16`	Configures an address pool as an on-demand address pool. • 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 (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). 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

	Command or Action	Purpose
		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.
Step 6	**utilization mark low** *percentage-number* **Example:** `Router(dhcp-config)# utilization mark low 40`	Sets the low utilization mark of the pool size. • This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured. • The default value is 0 percent.
Step 7	**utilization mark high** *percentage-number* **Example:** `Router(dhcp-config)# utilization mark high 60`	Sets the high utilization mark of the pool size. • This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured. • The default value is 100 percent.
Step 8	**end** **Example:** `Router(dhcp-config)# end`	Returns to global configuration mode.
Step 9	**show ip dhcp pool** [*pool-name*] **Example:** `Router# show ip dhcp pool`	(Optional) Displays information about DHCP address pools. • 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 your router 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 XE 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** | **interface** *interface_name*
5. **origin ipcp**
6. **exit**
7. **interface** *type number*
8. **ip address pool** *pool-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool red-pool`	Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode.

Step 4	**import** {**all** | **interface** *interface_name*
	Example:
	`Device(dhcp-config)# import all`
	`Device(dhcp-config) # import interface Ethernet0/0`
		Imports DHCP option parameters into the DHCP server database.

Step 5	**origin ipcp** **Example:** `Router(dhcp-config)# origin ipcp`	Configures an address pool as an on-demand address pool using IPCP as the subnet allocation protocol.
Step 6	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP pool configuration mode.
Step 7	**interface** *type number* **Example:**	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface GigabitEthernet 0/0/0`	
Step 8	**ip address pool** *pool-name* **Example:** `Router(config-if)# ip address pool red-pool`	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

Perform this task to configure 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. Do one of the following:
   - **aaa accounting network default start-stop group radius**
   - or
   - **aaa accounting network default stop-only group radius**
6. **aaa session-id common**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:**	Enables AAA access control.

	Command or Action	Purpose
	`Router(config)# aaa new-model`	
Step 4	**aaa authorization configuration default group radius** **Example:** `Router(config)# aaa authorization configuration default group radius`	Downloads static route configuration information from the AAA server using RADIUS.

Step 5	Do one of the following:
	• **aaa accounting network default start-stop group radius**
	• or
	• **aaa accounting network default stop-only group radius**
	Example:
	`Router(config)# aaa accounting network default start-stop group radius`
	Example:
	Example:
	`Router(config)# aaa accounting network default stop-only group 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
		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 6	**aaa session-id common** **Example:** `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

ODAP AAA Profile

The AAA server sends the RADIUS Cisco AV pair attributes "pool-addr" and "pool-mask" to the Cisco IOS XE 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 make up a network address (address/mask) that is allocated by the AAA server to the Cisco IOS XE 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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**ip radius source-interface** *subinterface-name*
	Example:
	`Router(config)#`
	`ip radius source-interface GigabitEthernet0/0/0`
		Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

Step 4	**radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number*
	Example:
	`Router(config)#`
	`radius-server host 172.16.1.1 auth-port 1645 acct-port 1646`
		Specifies a RADIUS server host.
		• The *ip-address* argument specifies the IP address of the RADIUS server host.

Step 5	**radius server attribute 32 include-in-access-req**
	Example:
	`Router(config)#`
	`radius server attribute 32 include-in-access-req`
		Sends RADIUS attribute 32 (NAS-Identifier) in an access request or accounting request.

Step 6	**radius server attribute 44 include-in-access-req** **Example:** `Router(config)#`	Sends RADIUS attribute 44 (Accounting Session ID) in an access request or accounting request.

	Command or Action	Purpose
	`radius server attribute 44 include-in-access-req`	

Step 7	**radius-server vsa send accounting**
	Example:
	`Router(config)#`
	`radius-server vsa send accounting`
		Configures the network access server (NAS) to recognize and use vendor-specific accounting attributes.

Step 8	**radius-server vsa send authentication**
	Example:
	`Router(config)#`
	`radius-server vsa send authentication`
		Configures the NAS to recognize and use vendor-specific authentication attributes.

What to do next

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool red-pool`	Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode.
Step 4	**no origin** {**dhcp**| **aaa**| **ipcp**} **Example:** `Router(dhcp-config)# no origin dhcp`	Disables the ODAP.

Verifying ODAP Operation

Perform this task to verify ODAP operation.

SUMMARY STEPS

1. **enable**
2. **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, while pool Global is configured to be in the global address space.
3. **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. 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.

DETAILED STEPS

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **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, while 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 3 **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. 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.

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.    Infinite                On-demand
                 2d38.3930.39
172.16.0.2       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3839.31
172.16.0.3       5674.312d.7465.7374.    Infinite                On-demand
                 2d36.3432.34
172.16.0.4       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3236.34
172.16.0.5       5674.312d.7465.7374.    Infinite                On-demand
                 2d34.3331.37
172.16.0.6       5674.312d.7465.7374.    Infinite                On-demand
                 2d37.3237.39
172.16.0.9       5674.312d.7465.7374.    Infinite                On-demand
                 2d39.3732.36
172.16.0.10      5674.312d.7465.7374.    Infinite                On-demand
                 2d31.3637
172.16.0.11      5674.312d.7465.7374.    Infinite                On-demand
                 2d39.3137.36
172.16.0.12      5674.312d.7465.7374.    Infinite                On-demand
                 2d37.3838.30
172.16.0.13      5674.312d.7465.7374.    Infinite                On-demand
                 2d32.3339.37
172.16.0.14      5674.312d.7465.7374.    Infinite                On-demand
                 2d31.3038.31
172.16.0.17      5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3832.38
172.16.0.18      5674.312d.7465.7374.    Infinite                On-demand
                 2d32.3735.31
```

Troubleshooting Tips

You can determine the client identifier by using the **debug ip dhcp server packet** command. In the following sample output, the client is identified by the value 0b07.1134.a029:

```
Device# debug ip dhcp server packet

DHCPD:DHCPDISCOVER received from client 0b07.1134.a029 through relay 10.1.0.253.
DHCPD:assigned IP address 10.1.0.3 to client 0b07.1134.a029.
.
.
.
```

Monitoring and Maintaining the ODAP

This task shows how to monitor and maintain the ODAP.

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip dhcp** [**pool** *pool-name*] **binding** {*****	*address*} **Example:** `Router# clear ip dhcp binding *`	Deletes an automatic address binding or objects from a specific pool from the DHCP server database.
Step 3	**clear ip dhcp** [**pool** *pool-name*] **conflict** {*****	*address*} **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
Step 4	**clear ip dhcp** [**pool** *pool-name*] **subnet**{*****| *address*} **Example:** `Router# clear ip dhcp subnet *`	Clears all currently leased subnets in the named DHCP pool or all DHCP pools if *name* is not specified.
Step 5	**debug dhcp details** **Example:** `Router# debug dhcp details`	Monitors the subnet allocation/releasing in the on-demand address pools.
Step 6	**debug ip dhcp server events** **Example:** `Router# debug ip dhcp server events`	Reports DHCP server events, like address assignments and database updates.
Step 7	**show ip dhcp import** **Example:** `Router# show ip dhcp import`	Displays the option parameters that were imported into the DHCP server database.
Step 8	**show ip interface** [*type number*] **Example:** `Router# show ip interface`	Displays the usability status of interfaces configured for IP.
Step 9	**show ip dhcp pool** *pool-name* **Example:** `Router# show ip dhcp pool green`	Displays DHCP address pool information.

How to Configure DHCP ODAP Subnet Allocation Server Support

Configuring a Global Pool on a Subnet Allocation Server

Perform this task to configure a global subnet pool on a subnet allocation server.

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool GLOBAL-POOL`	Enters DHCP pool configuration mode and specifies the subnet pool name.
Step 4	**network** *network-number* [*mask*| / *prefix-length*] **Example:** `Router(dhcp-config)# network 10.0.0.0 255.255.255.0`	Configures the subnet number and mask for a DHCP address pool on a DHCP server. • The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument.
Step 5	**subnet prefix-length** *prefix-length* **Example:** `Router(dhcp-config)# subnet prefix-length 8`	Configures the subnet prefix length. The range of the *prefix-length* 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 *prefix-length* argument follow CIDR bit count notation format.

Configuring a VRF Subnet Pool on a Subnet Allocation Server

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 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 provider edge (PE) router. The VRF is used to specify the VPN and 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.

Before you begin

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 dhcp pool** *pool-name*
4. **vrf** vrf-name
5. **network** *network-number* [*mask* |*/prefix-length*]
6. **subnet prefix-length** *prefix-length*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool VRF-POOL`	Enters DHCP pool configuration mode and specifies the subnet pool name.
Step 4	**vrf** vrf-name **Example:**	Associates the on-demand address pool with a VPN routing and forwarding (VRF) instance name (or tag).

	Command or Action	Purpose
	`Router(dhcp-config)# vrf RED`	• The **vrf**keyword and *vrf-name* argument are used to specify the VPN for the VRF pool. The *vrf-name* argument must match the VRF name (or tag) that is configured for the client.
Step 5	**network** *network-number* [*mask* |*/prefix-length*] **Example:** `Router(dhcp-config)# network 10.1.1.0 /24`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS XE DHCP server. • The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument.
Step 6	**subnet prefix-length** *prefix-length* **Example:** `Router(dhcp-config)# subnet prefix-length 16`	Configures the subnet prefix length. The range of the *prefix-length* 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 *prefix-length*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

A subnet allocation server can also 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.

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf vrf-name** **Example:** `Router(config)#ip vrf RED`	Creates a VRF routing table and specifies the VRF name (or tag). • The *vrf-name* argument must match the VRF name that is configured for the client and VRF pool in Step 9.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF instance created in Step 3. • 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	**route-target both** route-target-number **Example:** `Router(config-vrf)# route-target both 100:1`	Creates a route-target extended community for the VRF instance that was created in Step 3. • 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 *route-target-number*argument follows the same format as the *route-distinguisher* argument in Step 4. These two arguments must match.
Step 6	**vpn id** vpn-id **Example:**	Configures the VPN ID.

	Command or Action	Purpose
	`Router(config-vrf)# vpn id 1234:123456`	• This command is only used if the client (ODAP manager) is also configured with or assigned a VPN ID.
Step 7	**exit** **Example:** `Router(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 8	**ip dhcp pool** pool-name **Example:** `Router(config)# ip dhcp pool VPN-POOL`	Enters DHCP pool configuration mode and specifies the subnet pool name. • The **VRF**keyword and *vrf-name* argument are used to specify the VPN for the VRF pool. The *vrf-name* argument must match the VRF name (or tag) that is configured for the client.
Step 9	**vrf** vrf-name **Example:** `Router(dhcp-config)#vrf RED`	Associates the on-demand address pool with a VRF instance name. • The *vrf-name* argument must match the *vrf-name* argument that was configured in Step 3.
Step 10	**network** *network-number* [*mask* |*/prefix-length*] **Example:** `Router(dhcp-config)# network 192.168.0.0 /24`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS XE DHCP server. • The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument.
Step 11	**subnet prefix-length** *prefix-length* **Example:** `Router(dhcp-config)# subnet prefix-length 16`	Configures the subnet prefix length. • The range of the *prefix-length* 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 *prefix-length* argument follow CIDR bit count notation format.

Verifying the Subnet Allocation and DHCP Bindings

Perform this task to verify subnet allocation and DHCP bindings.

The **show ip dhcp pool** and **show ip dhcp binding**commands do not need to be issued together or even in the same session as 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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config**	begin dhcp **Example:** `Router# show running-config | begin dhcp`	Used to display the local configuration of the router. • 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.
Step 3	**show ip dhcp pool [pool-name]** **Example:** `Router# show ip dhcp pool`	Displays information about DHCP pools. • 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.
Step 4	**show ip dhcp binding [ip-address]** **Example:** `Router# show ip dhcp binding`	Displays information about DHCP bindings. • 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

	Command or Action	Purpose
		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 only display an IP address and are not followed by a subnet mask.

Troubleshooting the DHCP ODAP Subnet Allocation Server

Perform this task to troubleshoot the DHCP ODAP subnet allocation server.

SUMMARY STEPS

1. **enable**
2. **debug dhcp** [**detail**]
3. **debug ip dhcp server** {**events** | **packets** | **linkage**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug dhcp** [**detail**] **Example:** `Router# debug dhcp detail`	Displays debugging information about DHCP client activities and monitors the status of DHCP packets. • 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 op, htype, hlen, hops, server identifier option, xid, secs, flags, ciaddr, yiaddr, siaddr, and giaddr fields of the DHCP packet that are shown in addition to the length of the options field.
Step 3	**debug ip dhcp server** {**events**	**packets**	**linkage**} **Example:** `Router# debug ip dhcp server packets` **Example:**	Enables DHCP server debugging. • This example is issued with the **packets** and events keywords on the subnet allocation server. The output displays lease transition and reception, as well as database information.

	Command or Action	Purpose
	`Router# debug ip dhcp server events`	

Configuration Examples for DHCP Server On-Demand Address Pool Manager

Defining 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-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 run
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 ATM2/0/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM3/0/0
 no ip address
 no atm ilmi-keepalive
!
interface GigabitEthernet0/0/0
 ip address 10.0.105.12 255.255.255.224
 duplex half
!
interface GigabitEthernet0/0/1
 ip address 150.10.10.1 255.255.255.0
 duplex half
!
interface GigabitEthernet0/0/2
 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
```

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 GigabitEthernet0/1/1
 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 GigabitEthernet0/1/1
!
!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 for 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 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 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 for 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 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 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 configuration 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 there are no subnets 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 only display 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 2009 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	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual information	“DHCP Overview” module
DHCP server configuration	“Configuring the Cisco IOS XE DHCP Server” module

Related Topic	Document Title
DHCP client configuration	"Configuring the Cisco IOS XE DHCP Client" module
DHCP relay agent configuration	"Configuring the Cisco IOS XE DHCP Relay Agent" module
DHCP advanced features	"Configuring DHCP Services for Accounting and Security" module

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 IOS XE 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	*Bootstrap Protocol (BOOTP)*
RFC 1542	*Clarifications and Extensions for the Bootstrap Protocol*
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2685	*Virtual Private Networks Identifier*
RFC 3046	*DHCP Relay Information Option*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/public/support/tac/home.shtml

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	Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.9S	This feature was enhanced to provide ODAP support for non-MPLS VPNs. The following command was modified by this feature: **peer default ip address**
DHCP ODAP Server Support	Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.9S	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. The following commands were introduced or modified by this feature: **subnet prefix-length** and **show ip dhcp binding**

Feature Name	Releases	Feature Configuration Information
DHCP Server On-Demand Address Pool Manager	Cisco IOS XE Release 2.3	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. The following commands were introduced by this feature: **aaa session-id**, **clear ip dhcp subnet**, **ip address pool**, **ip dhcp aaa default username**, **origin**, **show ip dhcp pool**, **utilization mark high**, **utilization mark low**, **vrf**. The following commands were modified by this feature: **clear ip dhcp binding**, **clear ip dhcp conflict**, **ip address-pool**, **peer default ip address**.

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.