DHCP Server RADIUS Proxy

The Dynamic Host Configuration Protocol (DHCP) Server RADIUS Proxy is a RADIUS-based address assignment mechanism in which a DHCP server authorizes remote clients and allocates addresses based on replies from a RADIUS server.

Prerequisites for DHCP Server RADIUS Proxy

Before you can configure the DHCP Server RADIUS Proxy, you must be running DHCPv4 or a later version. For information about release and platform support, see "Feature Information for DHCP Server RADIUS Proxy".

Restrictions for DHCP Server RADIUS Proxy

The DHCP Server RADIUS Proxy supports only one address authorization pool on the router.

Information About DHCP Server RADIUS Proxy

DHCP Server RADIUS Proxy Overview

The DHCP Server RADIUS Proxy feature is an address allocation mechanism for RADIUS-based authorization of DHCP leases. This feature supports DHCP options 60 and 121.

1. The DHCP server passes client information to a RADIUS server.

2. The RADIUS server returns all required information to the DHCP server as RADIUS attributes.
3. The DHCP server translates the RADIUS attributes into DHCP options, and sends this information back to RADIUS in a DHCP OFFER message.
4. DHCP binding is synchronized after the RADIUS server authorizes the client session.

If a local pool and an authorization pool are configured on the router, the DHCP server can assign addresses from both pools for different client interfaces.

DHCP Server RADIUS Proxy Architecture

The allocation of addresses in a DHCP and RADIUS solution occurs as follows:

1. The client accesses the network from a residential gateway and sends a DHCP DISCOVER broadcast message to the relay agent. The DHCP DISCOVER message contains the client IP address, hostname, vendor class identifier, and client identifier.
2. The relay agent sends a DHCP DISCOVER unicast message containing the following information to the router:
   - Relay agent information (option 82) with the remote ID suboption containing the inner and outer VLAN IDs
   - Client information in the DHCP DISCOVER packet

The router determines the address of the DHCP server from the IP helper address on the interface that receives the DHCP packet.

1. RADIUS receives an access-request message to translate the DHCP options to RADIUS attributes.
2. RADIUS responds with an access-accept message, and delivers the following attributes to the DHCP server:
   - Framed-IP-Address
   - Framed-IP-Netmask
   - Session-Timeout
   - Session-Duration
3. The DHCP server sends an OFFER unicast message containing the following translations from the RADIUS server access-accept message to the client:
   - Framed-IP-Address inserted into the DHCP header.
   - Framed-IP-Netmask inserted into DHCP option 1 (subnet mask).
   - Session-Timeout inserted into DHCP option 51 (IP address lease time).
   - Framed-Route that is translated from the standard Cisco Framed-Route format into DHCP option 121 or the DHCP default gateway option (if the network and netmask are appropriate for a default route).
   - A copy of relay agent information (option 82). Before the DHCP client receives the packet, the relay removes option 82.
   - T1 time set to the Session-Timeout and T2 time set to the Session-Duration.
4. The client returns a formal request for the offered IP address to the DHCP server in a DHCP REQUEST broadcast message.

5. The DHCP confirms that the IP address is allocated to the client by returning a DHCP ACK unicast message containing lease information and the DHCP options to the client.
6. A RADIUS server accounting request starts, followed by a RADIUS server accounting response that is used by the AAA subsystem.

When a RADIUS server attribute is not present in an access-accept message, the corresponding DHCP option is not sent to the DHCP client. If the required information to produce a particular RADIUS server attribute is not available to the DHCP server, the DHCP server does not include information in the RADIUS packet. Non-inclusion can be in the form of not sending an attribute (if there is no information at all), or omitting information from the attribute (in the case of CLI-based format strings).

If a DHCP option is provided to the DHCP server but is invalid, the DHCP server may not transmit the corresponding RADIUS attribute in the access-request, or may transmit an invalid RADIUS server attribute.

DHCP Server and RADIUS Translations

The table below lists the translations of DHCP options in a DHCP DISCOVER message to attributes in a RADIUS server access-request message.

Table 1: DCHP DISCOVER to RADIUS Access-Request Translations

DHCP DISCOVER	RADIUS Access-Request
Virtual MAC address of the residential gateway	User-Name
Not Applicable	User-Password as configured on the DHCP server
Gateway address of the relay agent (giaddr field of a DHCP packet)	NAS-identifier
Hostname	Cisco AV pair client-hostname that equals the value of DHCP option 12
Vendor class	Cisco AV pair dhcp-vendor-class that equals a hexadecimal-encoded value of DHCP option 60
Client identifier	Cisco AV pair dhcp-client-id that equals the hexadecimal-encoded value of DHCP option 61
DHCP relay information option that can contain VLAN parameter on the D-router	Cisco AV pair dhcp-relay-info that equals the hexadecimal-encoded value of DHCP option 82

The table below lists the translations of attributes in a RADIUS server access-accept message to DHCP options in a DHCP OFFER message.

Table 2: RADIUS Access-Accept to DHCP OFFER Translations

RADIUS Access-Accept	DHCP OFFER
Framed-IP-Address	IP address of the residential gateway
Framed-IP-Netmask	Subnet mask (option 1)

RADIUS Access-Accept	DHCP OFFER
Session-Timeout	IP address lease time (option 51)
Cisco AV pair session-duration in seconds, where seconds is greater than or equal to the number of seconds in the Session-Timeout attribute.	Provides session control on the DHCP server. This attribute is not transmitted to the DHCP client.
Framed-Route (RADIUS attribute 22). One route for each DHCP option is allowed with a maximum of 16 Framed-Route options for a RADIUS packet.	Contains up to 16 classless routes in one option (option 121)

RADIUS Profiles for DHCP Server RADIUS Proxy

When you configure RADIUS server user profiles for DHCP server RADIUS proxy, use the following guidelines:

- The Session-Timeout attribute must contain a value, in seconds. If this attribute is not present, the DHCP OFFER is not sent to the client.
- A RADIUS user profile must contain the following attributes:
  - Framed-IP-Address
  - Framed-IP-Netmask
  - Framed-Route
  - Session-Timeout
  - Session-Duration--Session-Duration is the Cisco AV pair session-duration = seconds, where seconds is the maximum time for the duration of a lease including all renewals. The value for Session-Duration must be greater than or equal to the Session-Timeout attribute value, and it cannot be zero.
- Additional RADIUS server attributes are allowed but are not required. The DHCP server ignores additional attributes that it does not understand. If a RADIUS server user profile contains a required attribute that is empty, the DHCP server does not generate the DHCP options.

How to Configure DHCP Server RADIUS Proxy

Configuring the DHCP Server for RADIUS-based Authorization

Perform this task on the DHCP server to configure address allocation for RADIUS-based authorization of DHCP leases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service dhcp**
4. aaa new-model
5. **aaa group server radius** *group-name*

6. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
7. **exit**
8. **aaa authorization network** *method-list-name* **group** *group-name*
9. **aaa accounting network** *method-list-name* **start-stop group** *group-name*
10. **ip dhcp pool** name
11. **accounting** *method-list-name*
12. **authorization method** *method-list-name*
13. **authorization shared-password** password
14. **authorization username** string
15. exit
16. **interface** *type slot* / *subslot* / *port* [**.** *subinterface*]
17. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*[**,** *vlan-id*[- *vlan-id*]]}
18. **ip address** *address mask*
19. no shutdown
20. **radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
21. **radius-server key** {*0 string* | *7 string* | *string*}
22. **exit**

DETAILED STEPS

	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	**service dhcp** **Example:** `Router(config)# service dhcp`	Enables DHCP server and relay agent features on the router. By default, these features are enabled on the router.
Step 4	aaa new-model **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control system.
Step 5	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius group1`	Specifies the name of the server host list to group RADIUS server hosts. Enters server-group configuration mode. *group-name* --Character string to name the server group. The following words cannot be used as group name: • auth-guest

	Command or Action	Purpose
		• enable • guest • if-authenticated • if-needed • krb5 • krb-instance • krb-telnet • line • local • none • radius • rcmd • tacacs • tacacsplus
Step 6	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config-sg)# server 10.1.1.1 auth-port 1700 acct-port 1701`	*Specifies the IP address of the RADIUS server host for the defined server group. Repeat this command for each RADIUS server host to associate with the server group.* • *ip-address*-- IP address of the RADIUS server host. • **auth-port** *port-number*-- (Optional) Specifies the UDP destination port for authentication requests. Default value is 1645. • **acct-port** *port-number*-- (Optional) Specifies the UDP destination port for accounting requests. Default value is 1646.
Step 7	**exit** **Example:** `Router(config-sg)# exit`	Exits server-group configuration mode.
Step 8	**aaa authorization network** *method-list-name* **group** *group-name* **Example:** `Router(config)# aaa authorization network auth1 group group1`	Specifies the methods list and server group for DHCP authorization. • *method-list-name* --Character string to name the authorization methods list. • **group** --Specifies a server group.

	Command or Action	Purpose
		• *group-name* --Name of the server group to apply to DHCP authorization.
Step 9	**aaa accounting network** *method-list-name* **start-stop group** *group-name* **Example:** `Router(config)# aaa accounting network acct1 start-stop group group1`	Specifies that AAA accounting runs for all network service requests. • *method-list-name* --Character string to name the accounting methods list. • **start-stop** --Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice is received by the accounting server. • **group** --Specifies a server group. • *group-name* --Name of the server group to apply to DHCP accounting.
Step 10	**ip dhcp pool** name **Example:** `Router(config)# ip dhcp pool pool1`	Specifies a name for the DHCP server address pool. Enters DHCP pool configuration mode. • *name* --Name of the pool.
Step 11	**accounting** *method-list-name* **Example:** `Router(config-dhcp)# accounting acct1`	Enables DHCP accounting. • *method-list-name* --Name of the accounting methods list.
Step 12	**authorization method** *method-list-name* **Example:** `Router(config-dhcp)# authorization method auth1`	Enables DHCP authorization. • *method-list-name* --Name of the authorization methods list.
Step 13	**authorization shared-password** password **Example:** `Router(config-dhcp)# authorization shared-password cisco`	Specifies the password that is configured in the RADIUS user profile.

	Command or Action	Purpose
Step 14	**authorization username** string **Example:** `Router(config-dhcp)# authorization username %%c-user1`	Specifies the parameters that RADIUS sends to a DHCP server when downloading configuration information for a DHCP client. The *string* command argument contains the following formatting characters to insert DHCP client information: • **%c-** --Ethernet address of the DHCP client (chaddr field) • **%i-** --Inner VLAN ID from the DHCP relay information (option 82) • %o---Outer VLAN ID from the DHCP relay information (option 82) • **%p** --Port number from the DHCP relay information (option 82) • **%g** --Gateway address of the DHCP relay agent (giaddr field) • **%%** --Transmits the percent sign (%) character in the string sent to the RADIUS server **Note** The percent (%) is a marker to insert the DHCP client information associated with the specified character. The % is not sent to the RADIUS server unless you specify the %% character.
Step 15	exit **Example:** `Router(config-dhcp)# exit`	Exits DHCP pool configuration mode.
Step 16	**interface** *type slot* / *subslot* / *port* [**.** *subinterface*] **Example:** `Router(config)# interface ethernet 1/10.0`	Configures an interface or subinterface that allows the DHCP client to obtain an IP address from the DHCP server. Enters interface or subinterface configuration mode.
Step 17	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*[**,** *vlan-id*[- *vlan-id*]]} **Example:** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	(Optional) Enables IEEE 802.1Q encapsulation of traffic on a subinterface in a virtual LAN (VLAN). • *vlan-id* --VLAN ID, integer in the range 1 to 4094. To separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs, enter a hyphen. (Optional) To separate each VLAN ID range from the next range, enter a comma.

	Command or Action	Purpose
		• second-dot1q--Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature to configure an inner VLAN ID. • **any** --Any second tag in the range 1 to 4094.
Step 18	**ip address** *address mask* **Example:** `Router(config-if)# ip address 192.168.1.1 255.255.255.0`	Specifies an IP address for an interface or subinterface. • *address* is the IP address of the interface or subinterface. • *mask* is the subnet address for the IP address.
Step 19	no shutdown **Example:** `Router(config-if)# no shutdown`	Enables the interface or subinterface.
Step 20	**radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 10.1.1.1`	Specifies a RADIUS server host. • *ip-address* is the IP address of the RADIUS server host. • **auth-port** *port-number*-- (Optional) Specifies the UDP destination port for authentication requests. Default value is 1645. • **acct-port** *port-number*-- (Optional) Specifies the UDP destination port for accounting requests. Default value is 1646.
Step 21	**radius-server key** {*0 string* | *7 string* | *string*} **Example:** `Router(config)# radius-server key cisco`	Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon. • **0** *string*-- Specifies an unencrypted (cleartext) shared key • **7** *string* -- Specifies a hidden shared key. **Note** Any key you enter must match the key on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 22	**exit**	Exits global configuration mode.

Monitoring and Maintaining the DHCP Server

Perform this task to verify and monitor DHCP server information:

SUMMARY STEPS

1. **enable**
2. **debug ip dhcp server packet**
3. **debug ip dhcp server events**
4. **show ip dhcp binding** [*address*]
5. **show ip dhcp server statistics**
6. **show ip dhcp pool** [*name*]
7. **show ip route dhcp** [*address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip dhcp server packet** **Example:** `Router# debug ip dhcp server packet`	(Optional) Enables DHCP server debugging.
Step 3	**debug ip dhcp server events** **Example:** `Router# debug ip dhcp server events`	(Optional) Reports DHCP server events, such as address assignments and database updates.
Step 4	**show ip dhcp binding** [*address*] **Example:** `Router# show ip dhcp binding`	(Optional) Displays a list of all bindings created on a specific DHCP server. • Use the **show ip dhcp binding** command to display the IP addresses that have already been assigned. Verify that the address pool has not been exhausted. If necessary, re-create the pool to create a larger pool of addresses. • Use the **show ip dhcp binding** command to display the lease expiration date and time of the IP address of the host.
Step 5	**show ip dhcp server statistics** **Example:** `Router# show ip dhcp server statistics`	(Optional) Displays count information about server statistics and messages sent and received.

	Command or Action	Purpose
Step 6	**show ip dhcp pool** [*name*] **Example:** `Router# show ip dhcp pool`	(Optional) Displays the routes added to the routing table by the DHCP server and relay agent.
Step 7	**show ip route dhcp** [*address*] **Example:** `Router# show ip route dhcp [address]`	(Optional) Displays information about DHCP address pools.

Configuration Examples for DHCP Server Radius Proxy

Configuring the DHCP Server Example

The following example shows how to configure a DHCP server for RADIUS-based authorization of DHCP leases. In this example, DHCP clients can attach to Ethernet interface 4/0/1 and Ethernet subinterface 4/0/3.10. The username string (%c-user1) specifies that the RADIUS server sends the Ethernet address of DHCP client named user1 to the DHCP server.

```
Router> enable
Router# configure terminal
Router(config)# service dhcp
Router(config)# aaa new-model
Router(config)# aaa group server radius rad1
Router(config-sg)# server 10.1.1.1
Router(config-sg)# server 10.1.5.10
Router(config-sg)# exit
Router(config)# aaa authorization network auth1 group group1
Router(config)# aaa accounting network acct1 start-stop group group1
Router(config)# aaa session-id common
Router(config)# ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100 timeout 5
!
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# accounting acct1
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
Router(config-dhcp)# authorization username %c-user1
Router(config-dhcp)# exit
!
Router(config)# interface ethernet4/0/1
Router(config-if)# ip address 15.0.0.1 255.255.255.0
Router(config-if)# exit
Router(config-if)# interface ethernet4/0/3.10

Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# radius-server host 10.1.3.2
Router(config)# radius-server key cisco
Router(config)# exit
```

Configuring RADIUS Profiles Example

The following example shows how to configure a typical RADIUS user profile to send attributes in an access-accept message to the DHCP server:

```
DHCP-00059A3C7800 Password = “metta”
Service-Type = Framed,
Framed-Ip-Address = 10.3.4.5,
Framed-Netmask = 255.255.255.0,
Framed-Route = "0.0.0.0 0.0.0.0 10.3.4.1",
Session-Timeout = 3600,
Cisco:Cisco-Avpair = "session-duration=7200”
```

Additional References

The following sections provide references related to the DHCP Server RADIUS Proxy feature.

Related Documents

Related Topic	Document Title
DHCP relay configuration	*Configuring the Cisco IOS XE DHCP Relay Agent*
DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*

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, and support for existing MIBs has not been modified 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
No new or modified RFCs are supported by this feature, and support for existing RFCs was not modified by this feature.	--

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/techsupport

Feature Information for DHCP Server RADIUS Proxy

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 3: Feature Information for the Cisco IOS XE DHCP Relay Agent

Feature Name	Releases	Feature Configuration Information
DHCP Server RADIUS Proxy	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.9S	DHCP Server RADIUS Proxy enables a server to authorize remote clients and allocate addresses based on replies from the server. In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were modified by this feature: **authorization method (dhcp)**, **authorization shared-password, authorization username (dhcp)**.

Glossary

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

DHCP --Dynamic Host Configuration Protocol.

giaddr --Gateway IP address. The giaddr field of the DHCP message provides the DHCP server with information about the IP address subnet on which the client is to reside. It also provides the DHCP server with an IP address where the response messages are to be sent.

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

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

server --DHCP or BOOTP server.

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.