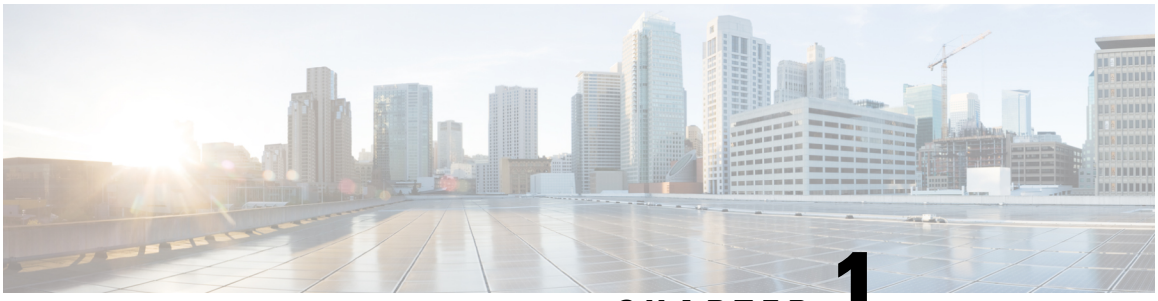
Access Node Control Protocol Configuration Guide, Cisco IOS XE Fuji 16.9.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

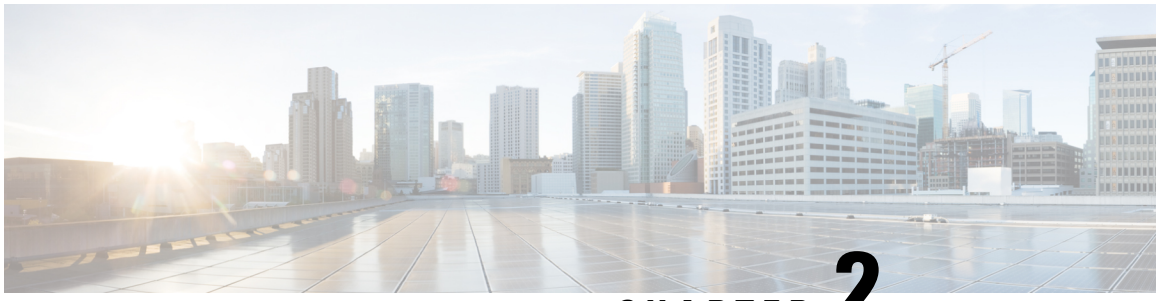
Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.



CHAPTER 2

Access Node Control Protocol

The Access Node Control Protocol (ANCP) feature enhances communication between Digital Subscriber Line Access Multiplexers (DSLAMs) and a broadband remote access server (BRAS), enabling the exchange of events, actions, and information requests between the multiplexer end and the server end. As a result, either end can implement appropriate actions.

Prerequisites for Access Node Control Protocol

To run ANCP over Transmission Control Protocol (TCP), IP must be enabled on broadband remote access servers (BRAS). Interactions from RADIUS to the BRAS are not required for ANCP and are dependent on the RADIUS server.

For information about release and platform support, see the Feature Information for Access Node Control Protocol, on page 15.

Restrictions for Access Node Control Protocol

Cisco IOS XE Release 2.4 supports interactions with the RADIUS server from the broadband remote access server (BRAS). Interactions from RADIUS to the BRAS are not required for ANCP and are dependent on the RADIUS server.

Information About Access Node Control Protocol

ANCP is used to aggregate traffic from multiple subscribers and deliver information for any application, while remaining independent from the application. ANCP is currently used in the application between DSLAMs and the broadband remote access server in a digital subscriber line (DSL) broadband environment.

The ANCP feature enables close communication between DSL aggregation multiplexers (DSLAMs) and network edge devices. Using ANCP between DSLAMs and a BRAS enables exchange of events, actions, and information requests so that the appropriate actions occur at the DSLAM and BRAS.

The ANCP architecture supports the following uses of ANCP:

Rate Adaptive Mode

Rate adaptive mode helps to maximize the line bit rate for a given line, and the rate is dependent on the quality of the signal achieved on the line. Rate adaptive mode conveys DSL modem line rate from a DSLAM to a broadband remote access server.

A BRAS running ANCP listens for TCP requests from its ANCP neighbors (DSLAMs).

- After a TCP session is established--ANCP begins exchanging messages to establish adjacency between the BRAS and its neighbors.
- After adjacency is established--ANCP event messages can be sent from the DSLAM to the BRAS.

Rate adaptive DSL uses signal quality to adjust line speeds. A BRAS typically sets the subscriber interfaces to the maximum bandwidth agreed to in the service license agreement (SLA).

When customer premises equipment (CPE) is synchronized to a data rate that is lower than the line speed, cell or packet loss occurs on the DSLAM. To prevent this, the DSLAM can use ANCP to notify the BRAS of newly adjusted circuit rates.

When a customer-facing port:

- Activates -- The DSLAM sends a Port Up message to the BRAS. The appropriate quality of service (QoS) takes effect in accordance with the ANCP-delivered information.
- Deactivates -- The DSLAM sends a Port Down message to the BRAS. ANCP reports the DSL state sent by the DSLAM, which is typically Silent or Idle. If the broadband remote access server receives another Port Up message, the subscriber sessions either time out or are renewed with a new shaping rate. The shaping rate on the interface does not change until the router receives a new Port Up message.

RADIUS Interaction

Interactions between the broadband remote access server and the RADIUS server are from the router to RADIUS.

The BRAS sends the following attributes and attribute-value pairs (AVPs) to the RADIUS server:

ANCP Line Rates	Upstream Data Rate	Downstream Data Rate	Output Policy Name
VSA 39	Attribute 197, Ascend-Data-Rate	Attribute 255, Ascend-Xmit-Rate	Attribute 77, Connect-Speed-Info
	Attribute Type 38, Rx Connect Speed AVP	Attribute Type 24, Tx Connect Speed AVP	

The BRAS uses Point-to-Point Protocol (PPPoE) to interact with the authentication, authorization, and accounting (AAA) module. RADIUS processes the information and then takes appropriate action.

Port Mapping

Port mapping associates customer premises equipment (CPE) clients of a DSLAM with VLAN subinterfaces on the BRAS. The VLANs include 802.1Q or queue-in-queue (Q-in-Q) hierarchical VLANs. Port mapping is configured in global configuration mode on the BRAS by grouping CPE client IDs with a specific DSLAM neighbor.

There are two methods you can use to map ports: configure all VLAN subinterfaces first, and the ANCP neighbor mappings next. Or, you can configure the mappings directly under the interface.

For example, the following commands configure port mapping for Q-in-Q VLAN subinterfaces:

```
ancp neighbor name
dslam-name
id
dslam-id
dot1q

outer-vlanid
 second-dot1q

inner-vlanid
 [interface

type number
] client-id
 "
client-id
"
```

or

```
ancp neighbor name
dslam-name
id
 dslam-id
dot1q

outer-vlanid
 client-id
 "
client-id
"
```

The *client-id*is a unique access-loop-circuit-id that the DSLAM sends to the BRAS for each unique port. The DSLAM sends this ID in the ANCP Port Up event message. The access-loop-circuit-id uses a defined format consisting of an access node identifier and digital subscriber line (DSL) information as mentioned below:

ATM/DSL

" *access-node-identifier* **atm** *slot/module/port* **.** *subinterface* **:** *vpi* **.** *vci* **"**

Ethernet/DSL

" *access-node-identifier* **ethernet** *slot* **/** *module* **/** *port* **.** *subinterface* [**:** *vlan-id*]**"**

The BRAS sets the default state as Down, on all ports of the router, until the DSLAM sends a Port Up message.

Noninteractive Operation Administration and Maintenance

ANCP provides an out-of-band control channel for performing noninteractive operation, administration, and maintenance (OAM) operations from the broadband remote access server. This channel enables router operators to view the ANCP port state of specific DSLAM ports. ANCP port state information is stored in the ANCP dynamic database on the BRAS.

Interactive OAM

The Interactive OAM and Scaling Improvements feature adds on-demand ping capability to ANCP for operations and troubleshooting.

Note This feature is enabled by default and requires no configuration.

General Switch Management Protocol and ANCP

ANCP is an extension of the General Switch Management Protocol (GSMP). GSMP defines a master-slave neighbor relationship in which the master initiates a connection to a slave. In ANCP, this master-slave relationship is reversed--the BRAS (master) listens and accepts incoming ANCP connections from the DSLAM (slave). The DSLAM uses event messages to communicate asynchronous events to the BRAS, such as topology changes and Port Down or Port Up events.

GSMP connectivity between the BRAS and the DSLAM occurs over TCP/IP (RFC 3293). The DSLAM initiates the connection to the router and the router accepts the connection if the appropriate interface is ANCP enabled.

The GSMP Adjacency Protocol establishes GSMP neighbor relationships.

1. During the adjacency-building:
    1. The DSLAM and router negotiate their capabilities and determine the synchronization state between the two ends.
    2. GSMP detects whether the router and the DSLAM have retained a local information database state in case of a transport failure, or whether both devices require a state update.
    3. If GSMP determines that it must resynchronize the adjacency, it restarts the adjacency synchronization process, which includes the capability negotiation defined in the ANCP extension draft available at:

http://tools.ietf.org/id/draft-wadhwa-gsmp-l2control-configuration-02.txt

1. In an ANCP, if a neighbor (neighbor1) contains capabilities that its neighbor (neighbor2) does not support, neighbor1 turns off the capabilities and recommunicates the packets to neighbor2 with the same set of capabilities as neighbor2.
2. After both the neighbors agree to the same set of capabilities, adjacency is established.

How to Configure Access Node Control Protocol

To configure ANCP, perform the following global or interface configuration tasks:

Enabling ANCP on an Ethernet Interface

Perform this task to enable ANCP on an Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface** *type number*
5. **ip address** *address mask*
6. **ancp enable**
7. **interface** *type number* **.** *subinterface*
8. **encapsulation dot1q** *vlanid* [**second-dot1q** *second-vlanid*]
9. **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	**ancp adjacency timer** *interval* **Example:** `Router(config)# ancp adjacency timer 100`	Sets the ANCP adjacency timer interval, which specifies the amount of time to wait before sending an ANCP hello packet to the DSLAM.
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet1/0/0`	Enters interface configuration mode to define an interface.
Step 5	**ip address** *address mask* **Example:** `Router(config-if)# ip address 10.16.1.2 255.255.0.0`	Assigns an IP address and subnet mask to the interface.
Step 6	**ancp enable** **Example:** `Router(config-if)# ancp enable`	Enables ANCP on the interface where IP is configured.

	Command or Action	Purpose
Step 7	**interface** *type number* **.** *subinterface* **Example:** `Router(config-if)# interface FastEthernet1/0/0.1`	Enters subinterface configuration mode to define a subinterface.
Step 8	**encapsulation dot1q** *vlanid* [**second-dot1q** *second-vlanid*] **Example:** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	Enables dot1q VLAN encapsulation on the subinterface for a single-queue 802.1Q VLAN or for Q-in-Q hierarchical VLANs.
Step 9	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.

Enabling ANCP on an ATM Interface

The **ancp enable** command should be configured only for the control VCs on which the ANCP message is sent from the DSLAM. Perform this task to enable ANCP on ATM interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface atm** *slot* **/** *subslot* **/** *port* **.** *subinterface*
5. **ip address** *ip-address mask*
6. **pvc** *vpi* **/** *vci*
7. **ancp enable**
8. **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.

	Command or Action	Purpose
Step 3	**ancp adjacency timer** *interval* **Example:** `Router(config)# ancp adjacency timer 100`	Sets the ANCP adjacency timer interval, which specifies the amount of time to wait before sending an ANCP hello packet to the DSLAM.
Step 4	**interface atm** *slot* **/** *subslot* **/** *port* **.** *subinterface* **Example:** `Router(config)# interface atm 2/0/1.1`	Enters subinterface configuration mode to define a subinterface.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-subif)# ip address 10.16.1.2 255.255.0.0`	Assigns an IP address and subnet mask to the subinterface.
Step 6	**pvc** *vpi* **/** *vci* **Example:** `Router(config-subif)# pvc 2/100`	Enters ATM virtual circuit configuration mode to enable an ANCP connection over ATM PVC.
Step 7	**ancp enable** **Example:** `Router(config-if-atm-vc)# ancp enable`	Enables ANCP on the interface where IP is configured.
Step 8	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode.

Mapping DSLAM Ports to VLAN Interfaces on Broadband Remote Access Servers

Perform this task to map DSLAM ports to VLAN interfaces on the BRAS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface** *type number.subinterface*
5. **encapsulation dot1q** *vlan-id*
6. **ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id*
7. **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	**ancp atm shaper percent-factor** *factor* **Example:** `Router(config)# ancp shaper percent-factor 95`	Enables ANCP cell tax accounting for ATM U-interface connections
Step 4	**interface** *type number.subinterface* **Example:** `Router(config)# interface FastEthernet0/0.1`	Enters interface configuration mode for the specified subinterface.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 411`	Enables IEEE 802.1Q encapsulation of traffic on a specified VLAN.
Step 6	**ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id* **Example:** `Router(config-subif)# ancp neighbor name dslam1 id 1.2.3.4 client-id "1.2.3.4. eth 0/0.1"`	Specifies the ANCP access DSLAM to which VLAN subinterfaces are mapped.
Step 7	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.

Mapping DSLAM Ports to PVC Interfaces on Broadband Remote Access Servers

The **ancp neighbor name** command is available under **pvc** and **pvc-in-range** command modes. This command creates a one-to-one mapping between a PVC and a DSLAM port. Perform this task to map DSLAM ports to PVC interfaces on the BRAS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface atm** *slot* / *subslot* / *port* **.** *subinterface*
5. Do one of the following:
   - **pvc** *vpi* / *vci*
   -
   - **range pvc** *start-vpi* / *start-vci* *end-vpi* / *end-vci*
6. **pvc-in-range** *vpi* / *vci*
7. **ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id*
8. **end**

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	**ancp atm shaper percent-factor** *factor* **Example:** `Router(config)# ancp shaper percent-factor 95`	Enables ANCP cell tax accounting for ATM U-interface connections.
Step 4	**interface atm** *slot* / *subslot* / *port* **.** *subinterface* **Example:** `Router(config)# interface atm 2/0/1.1`	Enters interface configuration mode for the specified ATM subinterface.
Step 5	Do one of the following: • **pvc** *vpi* / *vci* • • **range pvc** *start-vpi* / *start-vci* *end-vpi* / *end-vci* **Example:** `Router(config-subif)# pvc 1/101`	Creates a one-to-one mapping between a PVC and DSLAM port and enters ATM virtual circuit configuration mode. or Defines a range of ATM PVCs and enters PVC range configuration mode. • If a range of ATM PVCs are defined, use the **pvc-in-range** command to configure an individual PVC.

	Command or Action	Purpose
	Example: **Example:** `Router(config-subif)# range pvc 9/100 9/102`	
Step 6	**pvc-in-range** *vpi* / *vci* **Example:** `Router(config-if-atm-range-pvc)# pvc-in-range 9/100`	(Optional) Configures an individual PVC within a range in PVC range configuration mode.
Step 7	**ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id* **Example:** `Router(config-if-atm-range-pvc)# ancp neighbor name dslam1 id 1.2.3.4 client-id "1.2.3.4. atm0/0.1"`	Specifies the ANCP access DSLAM to which PVC subinterfaces are mapped. • This command is available under PVC range and ATM virtual circuit configuration modes.
Step 8	**end** **Example:** `Router(config-if-atm-range-pvc)# end`	Exits PVC range configuration mode.

Configuration Examples for Access Node Control Protocol

Enabling Access Node Control Protocol on Ethernet Interfaces Example

The following example shows how to enable ANCP on Ethernet subinterface 2/0/1.

```
interface GigabitEthernet 2/0/1
 ip address 192.168.64.16 255.255.255.0
 ancp enable
!
interface GigabitEthernet 2/0/1.1
 encapsulation dot1q 100 second-dot1q 200
!
ancp adjacency timer 100
```

Enabling Access Node Control Protocol on ATM Interfaces Example

The following example shows how to enable ANCP on ATM subinterface 2/0/1.1.

```
interface ATM2/0/0.1 point-to-point
 description ANCP Link to one DSLAM
 no ip mroute-cache
 ip address 192.168.0.2 255.255.255.252
```

```
 pvc 254/32
   protocol ip 192.168.0.1
   ancp enable
   no snmp trap link-status
```

Mapping DSLAM Ports to VLAN Interfaces on the BRAS Example

The following example shows how to map the CPE client ports of a DSLAM to Q-in-Q VLAN subinterfaces on the BRAS. In the example, the DSLAM neighbor named dslam1 with an IP address of 192.68.10.5 has a CPE client port mapped to Q-in-Q VLANs 100 and 200 configured on Ethernet interface 1/0/0.2. Another CPE client port is mapped to Q-in-Q VLANs 100 and 100 configured on Ethernet interface 1/0/0.1.

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
 ancp neighbor name dslam1 id 192.168.10.5 client-id "192.168.10.5 ethernet1/0/0.2"
!
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
 ancp neighbor name dslam1 id 192.168.10.5 client-id "192.168.10.5 ethernet1/0/0.1"
!
ancp atm shaper percent-factor 95
!
```

The example shown above maps the ports directly at the subinterface level. You can also configure all VLAN subinterfaces first, and perform the mappings under ANCP neighbor next, as shown in the following example:

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
!
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
!
ancp atm shaper percent-factor 95
!
ancp neighbor name dslam1 id 192.168.10.5
 dot1q 100 second-dot1q 100 interface GigabitEthernet1/0/0.1 client-id "192.168.10.5
ethernet1/0/0.2"
!
ancp neighbor name dslam1 id 192.168.10.5
 dot1q 100 second-dot1q 200 interface GigabitEthernet1/0/0.2 client-id "192.168.10.5
ethernet1/0/0.2"
```

Mapping DSLAM Ports to PVC Interfaces on the BRAS Example

The **ancp neighbor name** command maps the CPE client ports of a DSLAM to PVC interfaces on the BRAS. This command can be configured either globally or under PVC/PVC-in-Range mode.

In PVC or PVC-in-Range Configuration Mode

In this example, the router interfaces with one DSLAM which has two ports or clients.

```
interface ATM2/0/0.1 point-to-point
  description ANCP Link to one DSLAM
  no ip mroute-cache
  ip address 192.168.0.2 255.255.255.252
  pvc 254/32
     protocol ip 192.168.0.1 255.255.255.252
```

```
     ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-x-identifier"
       no snmp trap link-status
      !
interface ATM1/0/0.1 multipoint
  description TDSL clients - default TDSL 1024
  class-int speed:ubr:1184:160:10
  range pvc 10/41 10/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 10/103
      description TDSL client 16 Mbps with ANCP
      class-vc speed:ubr:17696:1184:05
      ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-x-identifier"
       !
  range pvc 11/41 11/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 11/108
      description TDSL client 16 Mbps with ANCP
      class-vc speed:ubr:17696:1184:05
      ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-y-identifier"
        !
```

In Global Configuration Mode

When the **ancp neighbor** command is configured globally, the PVC information for the ATM interface must also be specified, as shown in the following example:

```
interface ATM1/0/0.1 multipoint
 description TDSL clients - default TDSL 1024
 class-int speed:ubr:1184:160:10
 range pvc 10/41 10/160
   service-policy input SET-PRECEDENCE-0
   service-policy output premium-plus:l2c:25088
   pvc-in-range 10/103
     description TDSL client 16 Mbps with ANCP
     class-vc speed:ubr:17696:1184:05
!
 range pvc 11/41 11/160
   service-policy input SET-PRECEDENCE-0
   service-policy output premium-plus:l2c:25088
   pvc-in-range 11/108
     description TDSL client 16 Mbps with ANCP
     class-vc speed:ubr:17696:1184:05
!
ancp neighbor name dslam1 id 192.168.10.5
 atm 10/103 interface ATM1/0/0.1 client-id "dslam-port-x-identifier"
 atm 11/108 interface ATM1/0/0.1 client-id "dslam-port-y-identifier"
```

Additional References for Access Node Control Protocol

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ANCP Commands	*Cisco IOS Access Node Control Protocol Command Reference*

Related Topic	Document Title
IEEE 802.1Q VLAN	Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation
Queue-in-Queue VLAN Tags	IEEE 802.1Q-in-Q VLAN Tag Termination

RFCs

RFC	Title
ANCP extension draft	GSMP Extensions for Access Node Control Mechanism, Internet draft
RFC 3292	*General Switch Management Protocol (GSMP) V3*
RFC 3293	General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)

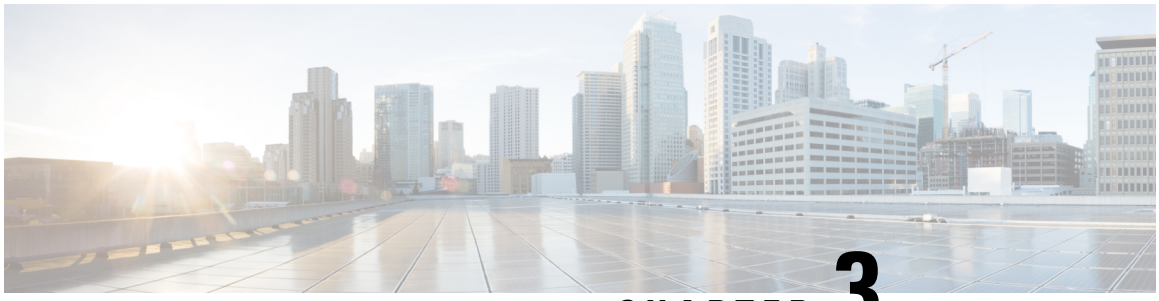
Feature Information for Access Node Control Protocol

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 Access Node Control Protocol

Feature Name	Releases	Feature Information
Access Node Control Protocol	Cisco IOS XE Release 2.4	In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000. The following command was introduced: **ancp vdsl ethernet shaper**.
Interactive OAM and Scaling Improvements	Cisco IOS XE Release 2.4	The Interactive OAM and Scaling Improvements feature adds on demand ping capability to ANCP for operations and troubleshooting. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000. The following commands were introduced or modified: **ping ancp**, **show ancp neighbor port**, **show ancp port**, **show ancp session**, **show ancp session adjacency**, **show ancp session event**, and **show ancp statistics**.



CHAPTER 3

Multiservice Activation in Access-Accept Message

The Multiservice Activation in Access-Accept Message feature is part of Access Node Control Protocol (ANCP) and allows multiple services to be included in a single RADIUS Access-Accept message.This feature is similar to the Multiservice Activation and Deactivation in a Change of Authorization (CoA) Message feature, but in this case all requested service activations are processed automatically. This means that if a service activation fails, no further service activations are processed, and any service that has already been activated by the Access-Accept message is deactivated.

Restrictions for Multiservice Activation in Access-Accept Message

- If one of the service activations fails, all unprocessed services from the Access-Accept message will be ignored, and any services from the Access-Accept message that have been activated will be deactivated.
- A two-stage application process exists when applying a quality of service (QoS) policy via a service in an Access-Accept message. The first stage involves parsing the policy and sending the policy value to the dataplane. The second stage involves the application of the QoS policy on the dataplane. In the instance where stage one is completed successfully, but stage two fails, the relevant service can indicate that the activation was successful.

Information About Multiservice Activation in Access-Accept Message

Multiservice Activation in Access-Accept Message Overview

An Access-Request message is sent by a RADIUS client to a RADIUS server to authenticate the user or subscriber profile included in the message. If the user or subscriber profile is:

- Acceptable--The RADIUS server may return an Access-Accept message
- Unacceptable--The RADIUS server may return an access-reject message

To enable multiservice activation, the Access-Accept message may include multiple Cisco generic VSA 250 (SSG_ACCOUNT_INFO) entries, with each VSA specifying a service name to be activated.

RSIM Format

```
vsa cisco generic 250 string "Aservice-name1"
vsa cisco generic 250 string "Aservice-name2"
vsa cisco generic 250 string "Aservice-name3"
```

RADIUS Format

```
07:06:23.234: RADIUS: Received from id 1645/36 11.12.13.2:1645, Access-Accept, len 112
07:06:23.238: RADIUS:  authenticator 92 C5 A2 F2 24 56 37 1E - 74 F4 C6 92 B0 E8 92 4C
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-1"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-2"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-3"
```

Upon receipt of the Access-Accept message, the specified services are extracted and each service is activated serially. If a service activation fails, all unprocessed services from the Access-Accept message are ignored, and any services from the Access-Accept message that have been activated are deactivated.

Note The RSIM format for Access-Accept multiple services requests for QoS services is not applicable for multiple service activation or deactivation requests in a CoA message. The format for CoA messages is VSA 252. For more information see Multiservice Activation and Deactivation in a CoA Message module

QoS Policy for VSA 250

You can use VSA 250 concatenated QoS syntax with the RADIUS Access-Accept message while establishing a session. The syntax parses the VSA concatenated string and activates the QoS and Intelligent Services Gateway (ISG) policy.

Note ISG manages multiple QoS services in one Access-Accept message and applies the message to activate static and parameterized QoS.

How to Configure Multiservice Activation in Access-Accept Message

Activating a Session Service Using Access-Accept

Configure Cisco VSA 250 in the service profile on RADIUS to dynamically activate a session service with Access-Accept. RADIUS uses VSA 250 in Access-Accept messages with the following syntax:

RSIM Format

```
vsa cisco generic 250 string
"Aservice-name-1"
```

Configuration Examples for Multiservice in Access-Accept Message

Activating QoS Services Using VSA 250 Example

To activate QoS Services, use the *qos:vc-qos-policy-out* syntax with the RADIUS Access-Accept message. The concatenated string is parsed and the QoS and ISG policy is activated.

The following example defines VSA 250 concatenated string parsing, and the activation of the ISG service and QoS policies:

qos:<qos-attribute-name>=<attribute value>[;qos:<qos-attribute-name>=<attribute value>...]

qos-attribute-name	Displays the QoS attribute name. The accepted attributes for the QoS attribute name in this special concatenated format are: vc-qos-policy-in vc-qos-policy-out vc-weight vc-watermark-min vc-watermark-max
attribute value	Displays the value to be assigned to the QoS attribute. The acceptable range of values are determined by the platform.

If the target session is an ATM VC, the vc-weight, vc-watermark-min, and vc-watermark-max attributes are interpreted.

The following example displays the concatenated QoS syntax for VSA 250:

vsa cisco generic 250 string "Aqos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in"

Additional References for Multiservice Activation in Access-Accept Message

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ANCP commands	Cisco IOS Access Node Control Protocol Command Reference
IEEE 802.1Q VLAN	Cisco IOS IEEE 802.1Q Support feature module
Access-Node Control Protocol	Metro Ethernet WAN Services and Architectures (white paper), Access Node Control Protocol
Queue-in-Queue VLAN Tags	IEEE 802.1Q-in-Q VLAN Tag Termination

RFCs

RFC	Title
ANCP extension draft	GSMP Extensions for Access Node Control Mechanism, Internet draft
RFC 3292	*General Switch Management Protocol (GSMP) V3*
RFC 3293	*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*

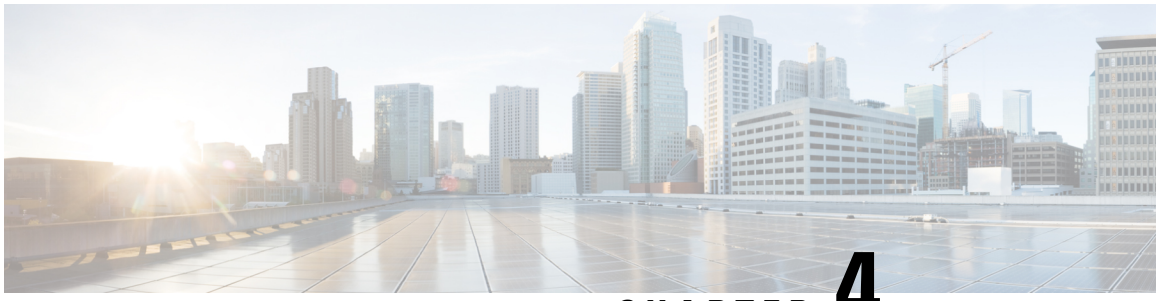
Feature Information for Multiservice Activation in Access-Accept Message

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 2: Feature Information for Multiservice Activation in Access-Accept Message

Feature Name	Releases	Feature Information
Multiservice Activation in Access-Accept Message	Cisco IOS XE Release 2.4	The Multiservice Activation in Access-Accept Message feature supports dynamic activation of multiple services using RADIUS Access-Accept messages. In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Routers. The following command was modified by this feature: **subscriber service multiple-accept**.



CHAPTER 4

Multiservice Activation and Deactivation in a CoA Message

This feature allows multiple services to be activated or deactivated by a single Change of Authorization (CoA) message sent from the policy server. This feature is similar to the Multiservice Activation in Access-Accept Message feature, but in this case it is assumed that the user session is already active.

Restrictions for Multiservice Activation and Deactivation in a CoA Message

- All service names included in the multiservice activation or deactivation message must be Intelligent Services Gateway (ISG) aware. For example, they must be of type class-map type service "service1."
- If one of the services activation or deactivation messages fails, the broadband remote access server (BRAS) rolls back only the previous successfully activated or deactivated services and those that were included in the same multiservice activation or deactivation CoA message.
- However, the current ISG implementation has limitations in the process of reestablishing the state of previously activated or deactivated services. For example, if a feature that can overlap is enabled in the same session, the new, successfully activated or deactivated feature parameters delete the old parameters of the same feature, which was already activated in that session. Attempts to reestablish old parameters of that feature fail.
- If a valid CLI-configured ISG service is forwarded through CoA to a new session and fails (ISG service is unable to find an accounting list):
  - BRAS does not wait for the hardware to be provisioned.
  - An ACK message is relayed.
  - ISG services are not applied.
  - Tracebacks are observed.

Information About Multiservice Activation and Deactivation in a CoA Message

Multiservice Activation and Deactivation in a CoA Message Overview

The CoA multiservice activation or deactivation message contains a list of services. Multiple services are listed in the form of multiple lines in a VSA 252.

For the case of multiservice deactivation within one CoA message, the RADIUS server sends the request to deactivate multiple services within one CoA multiservice deactivation message. For each service listed in the multiservice deactivation message, the BRAS deactivates the service. Successful deactivation of the service is followed by an accounting-stop message.

If a service cannot be successfully deactivated, the BRAS aborts the deactivation of all subsequent services contained in the multiservice activation message. The BRAS activates all the services within the same multiservice activation message that were successfully deactivated before the failed service activated.

An existing VSA 252 is used to form one multiservice activation or deactivation CoA message. To form one multiservice activate or deactivate CoA message, multiple lines of VSA 252 are included in the message. The following example shows mixed multiservice activation or deactivation in one CoA message:

RADIUS Format

```
ISG#
00:41:15: RADIUS: CoA  received from id 76 10.168.1.6:1700, CoA Request, len 67
00:41:15: CoA: 10.168.1.6 request queued
00:41:15: RADIUS:  authenticator C4 AC 5D 50 6A BE D7 00 - F9 1D FA 38 15 32 25 3A
00:41:15: RADIUS:  Vendor, Cisco       [26]  18
00:41:15: RADIUS:   ssg-account-info   [250] 12  "S151.1.1.2"
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 31           [Service-Log-On service1]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 32           [Service-Log-On service2]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0C 73 65 72 76 69 63 65 33        [Service-Log-Off service3]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 34           [Service-Log-On service4]
```

QoS Policy for VSA 252

You can use VSA 252 concatenated quality of service (QoS) syntax in a RADIUS CoA message. The syntax is used to activate or deactivate ISG service and the QoS policy by parsing the VSA 252 concatenated string.

Note ISG manages multiple QoS services in one CoA message and applies the message to activate static and parameterized QoS.

How to Configure Multiservice Activation and Deactivation in a CoA Message

Activating a Session Service Using CoA

Configure Cisco VSA 252 in the service profile on RADIUS to dynamically activate a session service with CoA. RADIUS uses VSA 252 in CoA messages with the following syntax:

```
vsa cisco generic 252 binary 0b suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

The CoA command in this example performs the following actions:

- Initiates an ISG service "qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;".
- Replaces the default QoS output child policy on virtual template IPOne_out and installs the IPOne_out policy if there is no default output child policy on the virtual template.
- Replaces the default QoS input child policy on virtual template IPOne_in and installs the IPOne_in policy if there is no default input child policy configured on the virtual template.

Deactivating a Session Service Using CoA

To dynamically activate a session service using CoA and default QoS policy on a virtual template, configure Cisco VSA 252 in the RADIUS service profile. RADIUS uses VSA 252 in CoA messages with the following syntax:

```
vsa cisco generic 252 binary 0c suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

The CoA command in this example performs the following actions:

- Terminates an ISG service "qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in".
- Replaces the QoS output child policy IPOne_out with the default child policy configured on the appropriate virtual template interface.
- Replaces the QoS input child policy IPOne_in with the default child policy configured on the appropriate virtual template interface.

Configuration Examples for Multiservice Activation and Deactivation in a CoA Message

Activating and Deactivating QoS Services Using VSA 252 Example

To activate QoS services, RADIUS adds one or more multiple QoS classes to the parent and child policy in one VSA 252 string and relays the following syntax:

```
CoA VSA 252 0b <new service>
```

In addition to the existing services, the new service should be installed and should not have overlapping classes with the current services.

The following example defines QoS activation and adds the QoS classes in the parameterized QoS service RADIUS form:

```
VSA252 0b q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
 ((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

To deactivate the second service, RADIUS relays the same VSA 252 string that was used for service activation, replacing "0b" with "0c".

The following example defines QoS deactivation and deletes the QoS classes in the parameterized QoS service RADIUS form:

```
VSA252 0c q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
 ((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

Additional References for Multiservice Activation and Deactivation in a CoA Message

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ANCP Commands	*Cisco IOS Access Node Control Protocol Command Reference*
IEEE 802.1Q VLAN	Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation
Queue-in-Queue VLAN Tags	IEEE 802.1Q-in-Q VLAN Tag Termination

RFCs

RFC	Title
ANCP extension draft	GSMP Extensions for Access Node Control Mechanism, Internet draft
RFC 3292	*General Switch Management Protocol (GSMP) V3*
RFC 3293	*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*

FeatureInformationforMultiserviceActivationandDeactivation in a CoA Message

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 Multiservice Activation and Deactivation in a CoA Message

Feature Name	Releases	Feature Information
Multiservice Activation and Deactivation in a CoA Message	Cisco IOS XE Release 2.4	The Multiservice Activation and Deactivation in a CoA Message feature supports dynamic activation and deactivation of multiple services using RADIUS CoA messages. In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Routers.