Define Interface Policy-Map AV Pairs AAA

Last Updated: January 17, 2012

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco RADIUS vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level.

The Define Interface Policy-Map AV Pairs AAA has the following benefits:

- The ability to apply QoS policies transparently as required without the disruption of session reauthentication provides a high degree of flexibility, smaller configuration files, and more efficient usage of queuing resources. This ability eliminated the need to pre-provision subscribers.
- The ability to modify the applied policy map as needed without session disruption (session dropped and reauthenticated) is an advantage to service providers.
- Nondisruptive support for special event triggers is essential to support new dynamic bandwidth services such as pre-paid and turbo button services.

The QoS policy map is used to define the subscriber user experience for broadband service and can facilitate delivery of higher value services such as VoIP and video.

Finding Feature Information

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

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

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.

Prerequisites for Define Interface Policy-Map AV Pairs AAA

- Authentication, Authorization, and Accounting (AAA) must be enabled and already set up to use RADIUS.
- Configuring a service policy on the ATM subinterface requires enabling Dynamic Bandwidth Selection (DBS) on the VC.

Restrictions for Define Interface Policy-Map AV Pairs AAA

For the Cisco 7000 series routers:

- Only the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters are supported for this feature.

For the Cisco 10000 series routers:

- You cannot configure a service policy on a VC and on a session at the same time.
- All ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, are supported for this feature.

Information About Define Interface Policy-Map AV Pairs AAA

Dynamically Applying and Modifying a Policy Map

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco VSAs that allow you to dynamically apply a policy map and modify a policy map applied to a session, without session reauthentication, at the ATM VC level using RADIUS. The purpose of the Cisco VSA (attribute 26) is to communicate vendor-specific information between the network access server (NAS) and the RADIUS server. The Cisco VSA encapsulates vendor-specific attributes that allow vendors such as Cisco to support their own extended attributes.

The Define Interface Policy-Map AV Pairs AAA feature allows the two new Cisco VSAs to be installed on an ATM VC after a PPPoA or PPPoEoA session establishment. Using RADIUS, this feature allows a policy map to be applied (“pulled”) and then modified by specific events (“pushed” by the policy server) while that session remains active.

Previously, a policy map could only be configured on a VC or ATM point-to-point subinterface by using the modular QoS CLI (MQC) or manually with the virtual template. Also previously, a service policy on a VC could be modified in the session but that session was dropped and reauthenticated. Currently for a PPPoA or PPPoEoA session, the pull part of the feature uses RADIUS to dynamically apply policy maps on an ATM VC and eliminates the need to statically configure a policy map on each VC. After a policy map is applied directly on the interface, certain events can signal the policy server to push a policy map onto a specific VC without the need for session reauthentication.

Note Configuring a service policy on the ATM subinterface still requires MQC configuration.

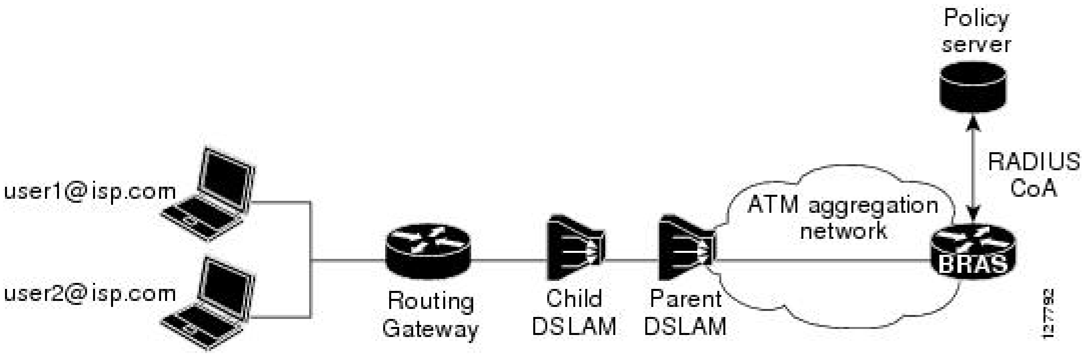
Two new Cisco AV pairs for service policy are set up in the user file on the RADIUS server. When the router requests the policy map name, the policy map name in the user file is pulled to the VC on the router when the PPPoA or PPPoEoA session is established. The Cisco AV pairs identify a "service policy-output" and "service policy-input" to identify QoS policies configured on the router from a RADIUS server. The Cisco AV pairs apply the appropriate policy map directly on the interface. Service policies are only applied at this time when the subscriber first authenticates the VC.

The "push" functionality of the feature allows you to modify an existing QoS profile (a policy map) applied to a session while that session remains active, thus allowing QoS policies to be applied as required without session reauthentication disruption. Specific events, including time-of-day, byte count, and user request, can signal the policy server to push a policy map onto a specific VC.

The policy server has the ability to send a Change of Authorization (CoA), which is the ability to change authorization of active sessions on the fly. The push functionality requires that CoA is enabled on the AAA server. One of the session attributes CoA pushes is the policy map, in an input and output direction.

The figure below shows that a CoA request is sent from the policy server to a broadband rate access server (BRAS), which causes a policy map change on PPPoA sessions set up between the BRAS and the routing gateway (RG).

Figure 1 *Change of Authorization--Policy Map Change on PPPoA Sessions*



For clarification, a policy map defines QoS actions and rules and associates these to a class map. In a policy map, you can define QoS actions for such things as policing and class-based weighted fair queuing (CBWFQ). After a policy map is configured on the router with the **policy-map** command, using the **service-policy** command attaches the configured policy map to a VC interface and specifies the direction (inbound or outbound) that the policy should be applied.

When a service policy is configured on the VC (or ATM point-to-point subinterface), the service policy is applied to all sessions that use that VC.

Note For the Cisco 7200 series routers, you can configure a service policy on a VC and on a session at the same time. On the Cisco 10000 series routers, you must either configure a service policy on a VC or on a session, but not both at the same time.

Note The Cisco 7200 series routers and Cisco 7301 router only support the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters for this feature. The Cisco 10000 series routers support all ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, for this feature.

- New Cisco VSAs, page 4
- Policy Map Troubleshooting Scenarios, page 4

New Cisco VSAs

To support the Define Interface Policy-Map AV Pairs AAA feature, the following two new Cisco AV pairs for policy map are defined at the ATM VC level:

- Cisco VSA attribute is vc-qos-policy-in
- Cisco VSA attribute is vc-qos-policy-out

They are formatted as:

- cisco-avpair = “atm:vc-qos-policy-in=<*in policy name*>”
- cisco-avpair = “atm:vc-qos-policy-out=<*out policy name*>”

To further support the Define Interface Policy-Map AV Pairs AAA feature, two existing Cisco Generic RADIUS VSAs will replace and deprecate two others that do not correctly follow the Cisco VSA naming guidelines.

The two replacement VSAs are:

- cisco-avpair = “ip:sub-qos-policy-in=<*in policy name*>”
- cisco-avpair = “ip:sub-qos-policy-out=<*out policy name*>”

The replacement VSAs replace the following existing VSAs:

- cisco-avpair = “ip:sub-policy-In=<*in policy name*>”
- cisco-avpair = “ip:sub-policy-Out=<*out policy name*>”

We recommend using the new VSAs. However, the replaced attributes are currently still supported.

Policy Map Troubleshooting Scenarios

- If a policy map is already configured on the ATM VC, the policy map pulled from the RADIUS server has higher precedence. This means that a **show policy-map** command shows the policy map pulled from the RADIUS server.
- After a policy map is successfully pulled on the VC, any configuration or unconfiguration after that using the **[no] service-policy input/output** *name* command does not affect the policy map used by the VC. Issuing a **show policy-map**command displays the pulled policy map. Issuing a **show run** command displays the current user configuration on the router.

- To remove the dynamic policy that is pulled from the RADIUS server, use the **no dbs enable** command or clear the PPPoA or PPPoEoA session associated with the VC.
- You should push both the input and output policy map together on the VC. If you push only one policy in one direction (for example, the input direction), then the output direction by default is a null policy push. The result is that on the VC, the input policy map is the policy pushed by the CoA. The output policy map is whatever policy was configured locally on the VC. If no output policy map was configured on the VC, there is no output policy map.

How to Configure Define Interface Policy-Map AV Pairs AAA

Configuring AV Pairs Dynamic Authorization and the Policy Map on the RADIUS Server

To configure the Define Interface Policy-Map AV Pairs AAA feature, follow the steps on the RADIUS server.

Prerequisites

AAA must be enabled and already set up to use RADIUS.

A PPPoEoA or PPPoA session is established.

The CoA functionality is enabled--required for the push functionality.

The **dbs enable** CLI is configured on the VC.

The policy map is configured on the router.

SUMMARY STEPS

1. atm:vc-qos-policy-in=<in policy name>

DETAILED STEPS

	Command or Action	Purpose

Step 1	atm:vc-qos-policy-in=<in policy name>
	Example:
	`atm:vc-qos-policy-out=<out policy name>`
	Example:
	`userid    Password ="cisco"`
	Example:
	`   Service-Type = Framed,`
	Example:
	`   Framed-Protocol = PPP,`
	Example:
	`   cisco-avpair = "atm:vc-qos-policy-out=dyn_out",`
	Example:
	`   cisco-avpair = "atm:vc-qos-policy-in=test_vc"`
		Enters the two new Cisco AV pairs for service policy on the RADIUS server in the user file. When the router requests the policy name, this information in the user file is “pulled.”
		A RADIUS user file contains an entry for each user that the RADIUS server will authenticate. Each entry, which is also referred to as a *user profile*, establishes an attribute the user can access.
		When looking at a user file, the data to the left of the equal sign (=) is an attribute defined in the dictionary file, and the data to the right of the equal sign is the configuration data.
		In this example, you have configured a service policy that attaches a policy map to the ATM VC interface and specifies the direction (inbound for data packets traveling into the interface or outbound for data packets leaving the interface).
		The policy map applied in the outbound direction is dyn_out and the inbound policy map is test_vc.

Configuring AV Pairs Dynamic Authorization and the Policy Map on the AAA Server

On the local AAA server, configure dynamic authorization that supports CoA in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. Configure the **client** command and **server-key** keyword or the **client** command and **server-key** command.

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	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Sets up the local AAA server for dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction and enters dynamic authorization local server configuration mode. In this mode, the RADIUS application commands are configured.

	Command or Action	Purpose
Step 5	Configure the **client** command and **server-key** keyword or the **client** command and **server-key** command. **Example:** **aaa server radius dynamic-author** **Example:** **auth-type** {**any** | **all** | **session-key**} **Example:** **domain** {**delimiter** *character* | **stripping [right-to-left]**} **Example:** **client** {*ip_addr* | *hostname*} [**server-key** [**0** | **7**] *string*] [**vrf** *vrfname* [**server-key** [**0** | **7**] *string*]] **Example:** **ignore** {**session-key** | **server-key**} **Example:** **port** {*port-num*} **Example:** **server-key** [**0** | **7**] *string* **Example:** `Router(config)aaa server radius dynamic-author`	You can use the **client**command and **server-key** keyword and *string* argument to configure the server key at the "client" level, or use the **server-key** command and *string* argument to configure the server key at the "global" level, which allows all the clients configured with the **client** command to use the global server key. **Note** Configuring the server key at the client level overrides the server key configured at the global level. For security purposes, we recommend configuring each client and configuring different server-keys for each client. The example configuration enables change of authorization and configures two client routers with different server-keys (cisco1 and cisco2). The **auth-type**, **domain**, **ignore session-key**, **ignore server-key**, and **port** commands are optional. **Note** When using the **auth-type** command and **session-key** keyword, the session-key attribute must match for authorization to be successful. The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid. The **domain** command configures username domain options for the RADIUS application. • The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, **/**, **$**, **%**, \, **#** or **-** • The **stripping** keyword compares the incoming username with the names oriented to the left of the **@** domain delimiter. • The **right-to-left** keyword terminates the string at the first delimiter going from right to left.

Command or Action	Purpose

Example:
`Router(config-locsvr-da-radius)#client 192.168.0.5 vrf coa server-key cisco1`
Example:
`Router(config-locsvr-da-radius)#client 192.168.1.5 vrf coa server-key cisco2`	

Configuring AV Pairs Dynamic Authorization and the Policy Map on the Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** [*module*/*slot*/*port.subinterface*] **point-to-point**
4. **pvc vpi/vci**
5. **dbs enable**
6. **exit**
7. **policy-map** *policy-map-name*
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.

	Command or Action	Purpose
Step 3	**interface atm** [*module*/*slot*/ *port*.*subinterface*] **point-to-point** **Example:** `Router(config)# interface ATM 4/0/1 point-to-point`	Specifies the interface, for example ATM4/0, and the encapsulation type on an ATM PVC. Enters subinterface mode.
Step 4	**pvc vpi/vci** **Example:** `Router(config-if)# pvc 1/101`	Creates or assigns a name to an ATM permanent virtual circuit (PVC) in subinterface configuration mode. The **pvc** command creates a PVC and attaches it to the virtual path identifier (VPI) and virtual channel identifier (VCI) specified. Enters ATM virtual circuit configuration mode. The example specifies VPI 1 and VCI 101 for this PVC.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Enables Dynamic Bandwidth Selection (DBS) in ATM VC configuration mode. Enabling this command allows the ATM shaping parameters to be retrieved from the RADIUS user profile. **Note** The **no dbs enable** command re-creates the VC and removes the dynamic policy that is pulled from the RADIUS server. Consequently, any configured modular QoS CLI (MQC) policy map on the PVC will be installed on the VC. Do not issue the **no dbs enable** command when the VC is active.
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM VC configuration mode and returns to subinterface configuration mode. Repeat this step one more time to exit subinterface configuration mode and return to global configuration mode.
Step 7	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map voice` **Example:**	Creates a policy map on the router. In the example, a policy map named voice is created.

Step 8	**end**
	Example:
	`Router(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Verifying Define Interface Policy-Map AV Pairs AAA

Perform this optional task to verify the configuration of the Define Interface Policy-Map AV Pairs AAA feature.

SUMMARY STEPS

1. **show policy-map interface**
2. **show running-config**
3. **show running-config**

DETAILED STEPS

Step 1 **show policy-map interface**

The **show policy-map interface**command shows the policy map voice attached to the ATM VC:

Example:

```
Router# show policy-map interface atm 4/0
ATM4/0: VC 1/101 -
 Service-policy input: voice
   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Step 2 **show running-config**

The following example displays the running configuration on the router showing the AAA setup; policy map configuration; ATM VC, PPPoA, and DBS-enabled CLI configuration; Virtual-Template configuration; and RADIUS server configuration:

Example:

```
Router# show running-config
.
.
.
aaa new-model
!
aaa user profile TEST
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
aaa session-id common
ip subnet-zero
.
.
.
policy-map voice
class Class-Default
fair-queue
.
.
.
!
interface ATM4/0.1 point-to-point
 pvc 1/101
```

```
  dbs enable
  encapsulation aal5mux ppp Virtual-Template1
 !
.
.
.
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp authentication chap
!
.
.
.
!
radius-server host 172.19.197.225 auth-port 1890 acct-port 1891
radius-server timeout 15
radius-server key 7 060506324F41
radius-server vsa send accounting
radius-server vsa send authentication
!
.
.
.
!
!
end
```

Step 3 **show running-config**

The following example displays the PPPoA client configuration:

Example:

```
.
.
.
!
interface ATM4/0.1 point-to-point
 pvc 1/101
  encapsulation aal5mux ppp Virtual-Template1
 !
!
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp chap hostname userid
 ppp chap password 7 030752180500
!
.
.
.
```

Configuration Examples for Define Interface Policy-Map AV Pairs AAA

Service-Policy Map Already Configured Example

The following example shows the existing MQC used to attach policy maps voice and outname under PVC 4/103. Using the **show policy-map interface**command shows that MQC-configured policy maps voice and outname are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
  service-policy input voice
  service-policy output outname
 !
Router# show policy-map interface atm 4/0.3
 ATM4/0.3: VC 4/103 -
  Service-policy input: voice
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
  Service-policy output: outname
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
Router#
```

The following example shows MQC used to establish a PPPoEoA session, which causes the policy maps (test_vc and dyn_out) set up on the RADIUS server to be downloaded or “pulled” to the VC. The policy maps downloaded from the RADIUS server have higher precedence than the MQC service-policy maps (voice and outname) configured on the PVC. Using the **show policy-map interface**command shows that the pulled policy maps are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
  dbs enable
  encapsulation aal5autoppp Virtual-Template1
  service-policy input voice
  service-policy output outname
 !
end
Router# show policy-map interface atm 4/0.3
 ATM4/0.3: VC 4/103 -
  Service-policy input: test_vc
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
  Service-policy output: dyn_out
    Class-map: class-default (match-any)
      5 packets, 370 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        5 packets, 370 bytes
        5 minute rate 0 bps
Router#
PPPoE Session Information
Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st
      2      2  0010.1436.bc70  ATM4/0.3                 1  Vi3.1      PTA
```

```
                0010.1436.b070  VC:  4/103                  UP
Router#
```

Service-Policy Map Pulled Example

The following example shows a policy named voice configured for input service policy on the RADIUS server. The router is already configured for PPPoA and AAA. The PPPoA session pulls the service policy name from the RADIUS server.

The **show policy-map interface**command displays the input service policy named voice attached to the ATM interface:

```
Router# show policy-map interface atm 4/0.1
ATM4/0: VC 1/101 -
 Service-policy input: voice
   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Using the **show run interface**command displays the currently running configuration, but not the pulled service policy:

```
Router# show run interface atm 4/0.1
Building configuration...
Current configuration : 107 bytes
!
interface ATM 4/0.1
    pvc 1/101
         dbs enable
         encapsulation aal5mux ppp Virtual-Template 1
    !
!
end
```

Service-Policy Map Pushed Example

This configuration example has five parts that show that PPPoA sessions are established between a broadband remote access server (BRAS) and a routing gateway (RG), the change of authorization (CoA push request) that passes between a policy server and the BRAS, and how the pulled policy maps are replaced by pushed policy maps after the CoA request.

The five parts are: BRAS PPPoA configuration, RG PPPoA configuration, session information on BRAS prior to a push, debug on BRAS after receiving the CoA request, and session information on BRAS after a CoA push request has taken place.

The following example shows the current PPPoA configuration on BRAS:

```
aaa new-model
 !
 aaa authentication ppp default group radius
 aaa authorization network default group radius
 !
 aaa server radius dynamic-author
  client <address> server-key <key>
 !
 aaa session-id common
 !
 ip routing
 !
 policy-map DefaultIn
   class class-default
   set ip precedence 0
 policy-map DefaultOut
```

```
  class class-default
  set ip precedence 0
!
policy-map PullMapIn
  class class-default
  set ip precedence 0
policy-map PullMapOut
  class class-default
  set ip precedence 0
!
policy-map 7up
  class class-default
    fair-queue
policy-map Sprite
  class class-default
    bandwidth 1000
!
policy-map PushMapIn
  class class-default
  set ip precedence 0
policy-map PushMapOut
  class class-default
  set ip precedence 0
!
!
vc-class atm xyz
  protocol ppp Virtual-Template1
  encapsulation aal5snap
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 no clns route-cache
 no shutdown
!
interface ATM4/0.1 point-to-point
 no atm enable-ilmi-trap
 pvc 0/101
  class-vc xyz
  vbr-nrt 400 300 50
  dbs enable
  service-policy in DefaultIn
  service-policy out DefaultOut
 !
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ppp authentication chap
!
radius-server host <address> auth-port <port> acct-port <port>
radius-server key <key>
radius-server vsa send authentication
```

The following example shows the PPPoA configuration set up on the RG:

```
aaa new-model
 !
 aaa session-id common
 !
 ip routing
 !
 interface Loopback0
  ip address 10.1.1.1 255.255.255.0
 !
 interface ATM2/0/0
  no ip address
  no atm ilmi-keepalive
  no atm enable-ilmi-trap
  no clns route-cache
  no shutdown
 !
 interface ATM2/0/0.1 point-to-point
  pvc 0/101
   protocol ppp Virtual-Template1
  !
 !
 interface Virtual-Template1
  ip unnumbered Loopback0
  no peer default ip address
  ppp chap hostname InOut
  ppp chap password 0 <password>
```

The following example uses the **show subscriber session all** command to display session information on BRAS prior to policy maps being pushed. PullMapIn and PullMapOut are the profiles pulled from the AAA server. The CoA request pushes the BRAS to change its input policy map (PullMapIn) and output policy map (PullMapOut) to PushMapIn and PushMapOut respectively.

```
Router# show subscriber session all
Current Subscriber Information:Total sessions 1
--------------------------------------------------
Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:32, Last Changed:00:00:12
AAA unique ID:55
Interface:Virtual-Access1.1
Policy information:
  Context 6531F6AC:Handle C700008A
  Authentication status:authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    service-type         2 [Framed]
    ssg-account-info     "S10.1.1.1"
    vc-qos-policy-in     "PullMapIn"
    vc-qos-policy-out    "PullMapOut"
  Prepaid context:not present
Configuration sources associated with this session:
Interface:Virtual-Template1, Active Time = 00:00:32
```

The following example displays the output of the **debug aaa coa** and **debug pppatm event**commands to show that the input policy map, PushMapIn, and output policy map, PushMapOut, have been applied or pushed on the BRAS after the BRAS received the CoA push request from the policy server:

```
2d20h:RADIUS:COA  received from id 41 10.0.56.145:1700, CoA Request, len 122
2d20h:COA:10.0.56.145 request queued
2d20h: ++++++ CoA Attribute List ++++++
2d20h:6523AE20 0 00000001 service-type(276) 4 Framed
2d20h:6523AF4C 0 00000009 ssg-account-info(392) 9 S10.1.1.1
2d20h:6523AF5C 0 00000009 ssg-command-code(394) 1 17
2d20h:6523AF6C 0 00000009 vc-qos-policy-in(342) 7 PushMapIn
2d20h:6523AF7C 0 00000009 vc-qos-policy-out(343) 4 PushMapOut
2d20h:
2d20h: PPPATM:Received VALID vc policy PushMapIn
2d20h: PPPATM:Received VALID vc policy PushMapOut
2d20h:PPPATM:ATM4/0.1 0/101 [54], Event = SSS Msg Received = 5
2d20h:Service policy input PushMapIn policy output PushMapOut applied on 0/101
2d20h: PPPATM:Applied VALID vc policy PushMapIn and PushMapOut
2d20h:RADIUS(00000000):sending
2d20h:RADIUS(00000000):Send CoA Ack Response to 10.0.56.145:1700 id 41, len 20
2d20h:RADIUS: authenticator 04 D5 05 E2 FE A3 A6 E5 - B2 07 C0 A1 53 89 E0 FF
```

The following example uses the **show subscriber session all** command to display session information on the BRAS after the BRAS received the CoA push request from the policy server. The policy information shows that PushMapIn and PushMapOut are the current policy maps on the BRAS that were pushed by the CoA request:

```
Router# show subscriber session all
Current Subscriber Information:Total sessions 1
--------------------------------------------------
Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:44, Last Changed:00:00:22
AAA unique ID:55
Interface:Virtual-Access1.1
Policy information:
  Context 6531F6AC:Handle C700008A
  Authentication status:authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    service-type         2 [Framed]
    ssg-account-info     "S10.1.1.1"
    vc-qos-policy-in     "PushMapIn"
    vc-qos-policy-out    "PushMapOut"
  Prepaid context:not present
Configuration sources associated with this session:
Interface:Virtual-Template1, Active Time = 00:00:44
```

Additional References

The following sections provide references related to the Define Interface Policy-Map AV Pairs AAA feature.

Related Documents

Related Topic	Document Title
WAN commands: complete command syntax, command mode, defaults, usage guidelines, and examples.	*Cisco IOS Wide-Area Networking Command Reference*
Quality of Service commands, such as **show policy-map**.	*Cisco IOS Quality of Service Solutions Command Reference*

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 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 has not been 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 Define Interface Policy-Map AV Pairs AAA

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 Define Interface Policy-Map AV Pairs AAA

Feature Name	Releases	Feature Information
Define Interface Policy-Map AV Pairs AAA	12.3(7)XI2 12.2(28)SB 12.2(33)SRC12.4(20)T 15.1(2)T	The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco Remote Authentication Dial-In User Service (RADIUS) vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level. This feature was integrated into Cisco IOS Release 12.3(7)XI2 and introduced for the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The “pull” functionality was implemented. This feature was integrated into Cisco IOS Release 12.2(28)SB. Support for the “push” functionality was added on the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The name for this functionality is RADIUS Push for MOD CLI Policies, which was integrated into the Define Interface Policy-Map AV Pairs AAA feature module. This feature was integrated into Cisco IOS Release 12.2(33)SRC. This feature was integrated into Cisco IOS Release 12.4(20)T. The **right-to-left** keyword was added to the **domain** command in Cisco IOS Release 15.1(2)T.

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