# show access-list template through vpn service

# show access-list template

To display information about access control lists (ACLs), use the **show access-list template** command in privileged EXEC mode.

**show access-list template** {**summary***aclname* | **exceed** *number* | **tree**}

## Syntax Description

| | |
|---|---|
| **summary** | Displays summary information about ACLs. |
| *aclname* | Displays information about the specified ACL. |
| **exceed** *number* | Limits the results to template ACLs that replace more than the specified *number* of individual ACLs. |
| **tree** | Provides an easily readable summary of the frequency of use of each of the ACL types that the template ACL function sees. |

## Command Modes

Privileged EXEC#

## Command History

| Cisco IOS Release | Description |
|---|---|
| 12.2(27)SBKA | This command was introduced on the Cisco 10000 series router. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Examples

This section provides examples of the different forms of the **show access-list template** command.

### show access-list template summary

The following example shows output from the **show access-list template summary** command:

```
Router# show access-list template summary

Maximum rules per template ACL = 100
Templates active = 1
Number of ACLs those templates represent = 50
Number of tree elements = 1
```

Output from this command includes:

- Maximum number of rules per template ACL
- Number of discovered active templates
- Number of ACLs replaced by those templates

### show access-list template aclname

The following example shows output from the **show access-list template** *aclname* command:

```
Router# show access-list template 4Temp_1073741891108
 Showing data for 4Temp_1073741891108
 4Temp_1073741891108 peer_ip used is 172.17.2.62,
 is a parent, attached acl count = 98
 currentCRC = 59DAB725
Router# show access-list template 4Temp_1342177340101
 Showing data for 4Temp_1342177340101
 4Temp_1342177340101 idb’s ip peer = 172.17.2.55,
 parent is 4Temp_1073741891108, user account attached to parent = 98
 currentCRC = 59DAB725
```

Output from this display includes:

- Peer IP of the interface associated with the named template ACL
- Name of the ACL serving as the primary user of the named template ACL
- Number of ACLs matching the template of the named template ACL
- Current cyclic redundancy check 32-bit (CRC32) value

### show access-list template exceed number

The following example shows output from the **show access-list template exceed** *number* command:

```
Router# show access-list template exceed 49
ACL name                          OrigCRC    Count     CalcCRC
4Temp_#120795960097               104FB543   50      104FB543
```

The table below describes the significant fields shown in the display.

***Table 1: show access-list template exceed Field Descriptions***

| Field | Description |
|---|---|
| ACL Name | Name of the template ACL. Only template ACLs that contain more than the specified number (**exceed** *number*) of child ACLs are listed. |
| OrigCRC | Original CRC32 value |
| Count | Count of ACLs that match the template ACL |
| CalcCRC | Calculated CRC32 value |

### show access-list template tree

The following example shows output from the **show access-list template tree** command:

```
Router# show access-list template tree
```

```
ACL name      OrigCRC   Count  CalcCRC
4Temp_1073741891108      59DAB725   98  59DAB725
```

The table below describes the significant fields shown in the display.

*Table 2: show access-list template tree Field Descriptions*

| Field | Description |
|---|---|
| ACL name | Name of an ACL on the Red-Black tree |
| OrigCRC | Original CRC32 value |
| Count | Number of users of the ACL |
| CalcCRC | Calculated CRC32 value |

# show atm svc ppp

To display information about each switched virtual circuit (SVC) configured for PPP over ATM, use the **show atm svc ppp** command in privileged EXEC mode.

**show atm svc ppp**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |

## Examples

The following is sample output from the **show atm svc ppp** command:

```
Router# show atm svc ppp
ATM Int.       VCD/Name      VPI   VCI  Type   VCSt  VA  VASt
2/0.1          10             0    60   SVC     UP   1   UP
```

The table below describes the fields shown in the display.

*Table 3: show atm svc ppp Field Descriptions*

| Field | Description |
|---|---|
| ATM Int. | Interface on which the SVC is configured. |
| VCD/Name | Virtual circuit descriptor (VCD) or name associated with the SVC. |
| VPI | Virtual path identifier. |
| VCI | Virtual channel identifier. |
| Type | Type of virtual circuit. |
| VCSt | Virtual circuit state. |
| VA | Virtual access interface number. |
| VASt | Virtual access interface state. |

# show call admission statistics

To monitor the global Call Admission Control (CAC) configuration parameters and the behavior of CAC, use the **show call admission statistics**command in user EXEC or privileged EXEC mode.

**show call admission statistics** [**detailed** ]

## Syntax Description

| **detailed** | Displays detailed statistics pertaining to the CAC. |
|---|---|

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 3.12S | The **detailed** keyword was added. |

## Examples

The following is sample output from the **show call admission statistics** command:

```
Router# show call admission statistics

Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

The table below describes the significant fields shown in the display.

*Table 4: show call admission statistics Field Descriptions*

| Field | Description |
|---|---|
| Total call admission charges | Percentage of system resources being charged to the system. If you configured a resource limit, security association (SA) requests are dropped when this field is equal to that limit. |
| limit | Maximum allowed number of total call admission charges. Valid values are 0 to 100000. |
| Total calls rejected | Number of SA requests that were not accepted. |
| accepted | Number of SA requests that were accepted. |
| unscaled | Not related to Internet Key Exchange (IKE). This value always is 0. |

## Examples

The following is sample output from the **show call admission statistics** [**detailed** ] command:

```
Router# show call admission statistics detailed

CAC New Model (SRSM) is ACTIVE
CAC statistics duration:  1873(seconds)
Total calls rejected 29, accepted 1749
Current hardware CAC status is: Not Dropping

Total call Session charges: 0, limit 0

CPU utilization: Five Sec Average CPU Load, Current actual CPU: 1%, Limit: 2%
Total count of session 1659, Limit: 128000

CAC Events:
        Reject reason          Times of activation   Duration of activation(secs)
Rejected calls
        CPU-limit:                        9                      42
 9
        SessionCharges:                   18                     42
 18
        LowPlatformResource:              8                      832
 1
        Session Limit:                    1                      47
 1

Total dropped FSOL packets at data plane: 4581
  IOSD_CPU_OVERLIMIT_DROPS:               2381
  CPS_OVERLIMIT_DROPS:                    1892
  TOTAL_SESSION_OVERLIMIT_DROPS:          189
  CPU_RP_OVERLIMIT_DROPS:                 20
  CPU_FP_OVERLIMIT_DROPS:                 20
  MEM_RP_OVERLIMIT_DROPS:                 20
  MEM_FP_OVERLIMIT_DROPS:                 20
  MEM_QFP_OVERLIMIT_DROPS:                20
  MEM_CC_OVERLIMIT_DROPS:                 19

platform resource low: FALSE
platform resource polling interval: 5 seconds
    BQS_QUEUE       : current:  0%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 0
    MEM_RP          : current: 67%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 251
    MEM_FP          : current:  8%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 494
    MEM_CC          : current: 52%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 829
    MEM_QFP         : current: 11%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 778
    CPU_RP          : current:  7%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 383
    CPU_FP          : current: 11%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 697
```

The table below describes the significant fields shown in the display.

***Table 5: show call admission statistics detailed Field Descriptions***

| Field | Description |
|---|---|
| Total dropped FSOL packets at data plane: 4581 | Total packets dropped at Data Plane level by the ESP is 4581. |
| IOSD_CPU_OVERLIMIT_DROPS: 2381 | 2381 packets dropped because the IOS CPU utilization threshold is reached. |
| CPS_OVERLIMIT_DROPS: 1892 | 1892 packets dropped due to calls per second (CPS) over threshold limit. |

| Field | Description |
|---|---|
| TOTAL_SESSION_OVERLIMIT_DROPS:189 | 189 packets dropped due to total session limit. |
| CPU_RP_OVERLIMIT_DROPS: 20 | 20 packets dropped due to Route Processor (RP) CPU over threshold limit. |
| CPU_FP_OVERLIMIT_DROPS: 20 | 20 packets dropped due to Forwarding Processor (FP) CPU over threshold limit. |
| MEM_RP_OVERLIMIT_DROPS: 20 | 20 packets dropped due to RP memory over threshold limit. |
| MEM_FP_OVERLIMIT_DROPS: 20 | 20 packets dropped due to FP memory over threshold limit. |
| MEM_QFP_OVERLIMIT_DROPS: 20 | 20 packets dropped due to Quantum Flow Processor (QFP) memory over threshold limit. |
| MEM_CC_OVERLIMIT_DROPS: 19 | 19 packets dropped due to CC memory over threshold limit. |

## Related Commands

| Command | Description |
|---|---|
| **call admission limit** | Specifies the maximum total concurrent session charges allowed in the system. |
| **clear call admission statistics** | Clears call admission control (CAC) statistics. |
| **debug call-admission trace** | Prints the different events that occurred, which are related to CAC. |
| **elog Event logging** | Specifies all the events that are triggered when CAC is enabled. |

# show ccm clients

To display information about cluster control manager (CCM) clients on high availability (HA) dual Route Processor systems, use the **show ccm clients** command in privileged EXEC mode.

**show ccm clients**[**id** *ccm-group-id*]

## Syntax Description

| | |
|---|---|
| **id** *ccm-group-id* | (Optional) Displays information about the specified CCM group. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 3.5S | This command was modified. The output was enhanced to include information about periodic session updates. |

## Usage Guidelines

The CCM manages the capability to synchronize session initiation on the standby processor of a dual Route Processor HA system. Use the **show ccm clients** command to display information about CCM clients.

## Examples

The following is sample output from the **show ccm clients** command on a Cisco ASR 1000 Series Router's active processor:

```
Router# show ccm clients

CCM bundles sent since peer up:
                                        Sent            Queued for flow control
    Sync Session                        3               0
    Update Session                      1               0
    Active Bulk Sync End                1               0
    Session Down                        3               0
    ISSU client msgs                    178             0
    Dynamic Session Sync                0               0
    Periodic Update Session             3               0
    Unknown msgs                        0               0
Client events sent since peer up:
    PPP                                 15              3
    PPPoE                               8               3
    PPPoA                               0               0
    VPDN FSP                            0               0
    AAA                                 15              3
    PPP SIP                             2               0
    LTERM                               3               0
    AC                                  0               0
    VPDN LNS                            0               0
    ATOM SUB                            0               0
    Ether-Infra CCM                     0               0
```

The following is sample output from the **show ccm clients** command on a router's active processor:

```
Router# show ccm clients

CCM bundles sent since peer up:
                                        Sent            Queued for flow control
    Sync Session                        10              1
    Update Session                      6               1
    Active Bulk Sync End                1               0
    Session Down                        10              0
    ISSU client msgs                    115             0
    Dynamic Session Sync                0               0
    Unknown msgs                        0               0
Client events sent since peer up:
    PPP                                 66
    PPPoE                               0
    PPPoA                               0
    AAA                                 44
    PPP SIP                             11
    LTERM                               11
    AC                                  0
    SSS FM                              0
    IP SIP                              0
    IP IF                               0
    DPM                                 0
    COA                                 0
```

The following is sample output from the **show ccm clients** command on a router's standby processor:

```
Router# show ccm clients

CCM bundles rcvd since last boot:
    Sync Session                8
    Update Session              0
    Active Bulk Sync            1
    Session Down                8
    ISSU client msgs            59
    Dynamic Session Sync        0
    Unknown msgs                0
Client events extracted since last boot:
    PPP                         72
    PPPoE                       50
    PPPoA                       0
    AAA                         32
    PPP SIP                     0
    LTERM                       8
    AC                          0
    SSS FM                      0
    IP SIP                      0
    IP IF                       0
    DPM                         0
    COA                         0
    Auto Svc                    0
```

The table below describes the significant fields shown in the display. Any data not described in the table below is used for Cisco internal debugging purposes.

*Table 6: show ccm clients Field Descriptions*

| Field | Description |
|---|---|
| Sent | Number of CCM bundles sent by the active processor since initiation on the standby processor. |

| Field | Description |
|---|---|
| Queued for flow control | Number of the following types of CCM bundles queued on the active processor when flow control is OFF since initiation on the standby processor:<br>• Sync Session—Synchronization session bundles.<br>• Update Session—Individual client update to session bundles.<br>• Active Bulk Sync—Active processor bulk synchronization bundles.<br>• Session Down—Session down bundles.<br>• ISSU client msgs—In service software upgrade (ISSU) bundles.<br>• Dynamic Session Sync—Dynamic cluster update to session bundles.<br>• Unknown msgs—Unknown message bundles.<br>The queued bundles will be sent when flow control is ON again. |
| Periodic Update Session | Cumulative number of periodic updates sent on active processor, or received on standby processor. |
| Client events sent since peer up | Number of client events sent since initiation on the standby processor. |
| CCM bundles rcvd since last boot | Number of the following types of CCM bundles received by the standby processor since initiation:<br>• Sync Session—Synchronization session bundles.<br>• Update Session—Individual client update to session bundles.<br>• Active Bulk Sync—Active processor bulk synchronization bundles.<br>• Session Down—Session down bundles.<br>• ISSU client msgs—ISSU bundles.<br>• Dynamic Session Sync—Dynamic cluster update to session bundles.<br>• Unknown msgs—Unknown message bundles. |
| Client events extracted since last boot | Number of client events extracted since initiation on the standby processor. |

## Related Commands

| Command | Description |
|---|---|
| **show ccm queues** | Displays CCM queue statistics. |
| **show ccm sessions** | Displays CCM session information. |

# show ccm queues

To display cluster control manager (CCM) queue statistics for high availability (HA) dual Route Processor systems, use the **show ccm queues** command in privileged EXEC mode.

**show ccm queues**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 3.5S | This command was modified. The output was enhanced to include information about periodic session updates. |

## Usage Guidelines

The CCM manages the capability to synchronize session initiation on the standby processor of a redundant processor HA system. Use the **show ccm queues** command to display queue statistics for CCM sessions on active and standby processors. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

## Examples

The following is sample output from the **show ccm queues** command on a Cisco ASR 1000 Series Router. No field descriptions are provided because command output is used for Cisco internal debugging purposes only.

```
Router# show ccm queues

10 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 3 CCM              0    20        196        197        1          0         20
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1  3 Sync Session            3        0        2        0       333      1000
 2  3 Sync Client             0        0        0        0         0         0
 3  3 Update                  2        0        1        0         0         0
 4  3 Session Down            3        0        2        0       333      1000
 5  3 Bulk Sync Begi          1        0        1        0         0         0
 6  3 Bulk Sync Cont          2        0        2        0         0         0
 7  3 Bulk Sync End           1        0        1        0         0         0
 8  3 Rcv Bulk End            0        0        0        0         0         0
 9  3 Dynamic Sync C          2        0        1        0         0         0
10  3 Going Active            0        0        0        0         0         0
11  3 Going Standby           0        0        0        0         0         0
12  3 Standby Presen          1        0        1        0         0         0
13  3 Standby Gone            0        0        0        0         0         0
15  3 CP Message            335        0       20        0         8      1000
16  3 Recr Session            0        0        0        0         0         0
17  3 Recr Update             0        0        0        0         0         0
```

```
18  3 Recr Sess Down            0        0        0        0         0         0
19  3 ISSU Session N            1        0        1        0         0         0
20  3 ISSU Peer Comm            0        0        0        0         0         0
21  3 Free Session            101        0        2        0         0         0
22  3 Sync Dyn Sessi            0        0        0        0         0         0
23  3 Recr Dyn Sessi            0        0        0        0         0         0
24  3 Session Ready             0        0        0        0         0         0
25  3 Pending Update            0        0        0        0         0         0
26  3 Cleanup All Se            0        0        0        0         0         0
27  3 Periodic Update           3        0        2        0       333      1000
28  3 Recreate Periodic Update  0        0        0        0         0         0
29  3 Enable Periodic Update    1        0        0        0         0         0
30  3 Disable Periodic Update   0        0        0        0         0         0
31  3 Modify Periodic Update    0        0        0        0         0         0

FSM Event Names           Events
 0    Invalid                   0
 1    All Ready                 3
 2    Required Not Re           1
 3    Update                    2
 4    Down                    101
 5    Error                     0
 6    Ready                     0
 7    Not Syncable              0
 8    Recreate Down             0
 9    Periodic Update           3
```

The following is sample output from the **show ccm queues** command. No field descriptions are provided because command output is used for Cisco internal debugging purposes only.

```
Router# show ccm queues

8 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 4 CCM              0     7      16167      16168        1          0         20
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1  4 Sync Session              0        0        0        0         0         0
 2  4 Sync Client               0        0        0        0         0         0
 3  4 Update                    0        0        0        0         0         0
 4  4 Session Down              0        0        0        0         0         0
 5  4 Bulk Sync Begi            1        0        1        0         0         0
 6  4 Bulk Sync Cont            2        0        2        0         0         0
 7  4 Bulk Sync End             1        0        1        0         0         0
 8  4 Rcv Bulk End              0        0        0        0         0         0
 9  4 Dynamic Sync C            0        0        0        0         0         0
10  4 Going Active              0        0        0        0         0         0
11  4 Going Standby             0        0        0        0         0         0
12  4 Standby Presen            1        0        1        0         0         0
13  4 Standby Gone              0        0        0        0         0         0
15  4 CP Message              188        0        7        0         0         0
16  4 Recr Session              0        0        0        0         0         0
17  4 Recr Update               0        0        0        0         0         0
18  4 Recr Sess Down            0        0        0        0         0         0
19  4 ISSU Session N            1        0        1        0         0         0
20  4 ISSU Peer Comm            0        0        0        0         0         0
21  4 Free Session          16103        0        1        0         0         0
22  4 Sync Dyn Sessi            0        0        0        0         0         0
23  4 Recr Dyn Sessi            0        0        0        0         0         0
24  4 Session Ready             0        0        0        0         0         0
FSM Event Names           Events
 0    Invalid                   0
 1    All Ready                 0
```

```
2    Required Not Re           0
3    Update                    0
4    Down                  16103
5    Error                     0
6    Ready                     0
7    Not Syncable              0
8    Recreate Down             0
```

## Related Commands

| Command | Description |
|---|---|
| **show ccm clients** | Displays CCM client information. |
| **show ccm sessions** | Displays CCM session information. |

# show ccm sessions

To display information about cluster control manager (CCM) sessions on high availability (HA) dual Route Processor systems, use the **show ccm sessions** command in privileged EXEC mode.

**show ccm sessions**[**id** *ccm-group-id*]

## Syntax Description

| | |
|---|---|
| **id** *ccm-group-id* | (Optional) Displays information about the specified CCM group. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 3.5S | This command was modified. The output was enhanced to include information about periodic session updates. |

## Usage Guidelines

The CCM manages the capability to synchronize session initiation on the standby processor of a redundant processor HA system. Use the **show ccm sessions** command to display information on CCM sessions on active and standby processors, and also to display information on subscriber redundancy policies configured using the **subscriber redundancy** command.

## Examples

The following is sample output from the **show ccm sessions** command on a Cisco ASR 1000 Series Router active processor. To display information about periodic session updates, the **subscriber redundancy dynamic periodic-update interval** command must be configured.

```
Router# show ccm sessions

Global CCM state:                        CCM HA Active - Dynamic Sync
Global ISSU state:                       Compatible, Clients Cap 0x9EFFE

                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready    0           1           0
Number of sessions in state Ready:       0           0           0
Number of sessions in state Dyn Sync:    3           0           0

Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         2           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:01 -         8           -         -
         RGF Bulk Tim 00:05:00 -         0           -         -

Periodic Update:
    Number of sessions Interested in Periodic Update:  1
    Configured Periodic Update Interval(In Minutes):   10
```

The following is sample output from the **show ccm sessions** command on a Cisco 10000 series router active processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Active - Dynamic Sync
Global ISSU state:                       Compatible, Clients Cap 0x0
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0
Number of sessions in state Not Ready:0
Number of sessions in state Ready:       0
Number of sessions in state Dyn Sync:    0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         2           -         -
         Dynamic CPU  00:00:10 -         0           90        0
```

The following is sample output from the **show ccm sessions** command on a Cisco 10000 series router standby processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Standby - Collecting
Global ISSU state:                       Compatible, Clients Cap 0xFFE
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready:   0           0           0
Number of sessions in state Ready:       0           0           0
Number of sessions in state Dyn Sync:    0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:20 -         0           -         -
```

The following is sample output from the **show ccm sessions** command on a Cisco 7600 series router active processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Active - Dynamic Sync
Global ISSU state:                       Compatible, Clients Cap 0xFFFE
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready:   7424        0           0
Number of sessions in state Ready:       0           0           0
Number of sessions in state Dyn Sync:    20002       28001       0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         924         -         -
         Dynamic CPU  00:00:10 -         0           90        2
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:20 -         18          -         -
```

The following is sample output from the **show ccm sessions** command on a Cisco 7600 series router standby processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Standby - Collecting
Global ISSU state:                       Compatible, Clients Cap 0xFFE
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready:   8038        0           0
Number of sessions in state Ready:       20002       0           28001
Number of sessions in state Dyn Sync:    0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         1           -         -
         RF Notif Ext 00:00:20 -         0           -         -
```

The table below describes the significant fields shown in the output, in the order in which they display. Any data not described in the table is used for Cisco internal debugging.

*Table 7: show ccm sessions Field Descriptions*

| Field | Description |
|---|---|
| Global CCM state | Displays the processor’s active or standby status and its CCM state. For example:<br>• CCM HA Active—Dynamic Sync means that this is the active processor, standby is in STANDBY_HOT state, and CCM is ready to synchronize sessions.<br>• CCM HA Active—Collecting means that this is the active processor and there is no standby processor. CCM can collect sessions but cannot synchronize them to a standby processor.<br>• CCM HA Active—Bulk Sync means that this is the active processor and a standby processor is booting up. CCM is doing a bulk synchronization of sessions.<br>• CCM HA Standby—Collecting means that this is the standby processor and is in STANDBY_HOT state. CCM is collecting sessions for synchronizing if a switchover happens. |
| Global ISSU state | Compatible, Clients Cap 0xFFFE0 indicates that CCM is compatible for in-service software upgrade (ISSU) clients--that is, ISSU-compatible Cisco IOS versions are running on both processors. It also means that CCM has the client capability for the clients in the bitmask 0xFFFE. |
| Current | CCM sessions currently ready for synchronization. |
| Bulk Sent | CCM sessions sent during bulk synchronization. |
| Bulk Rcvd | CCM sessions received during bulk synchronization. |

| Field | Description |
|---|---|
| Number of sessions in state Down | Sessions in the down state. |
| Number of sessions in state Not Ready | Sessions in the not ready state. |
| Number of sessions in state Ready | Sessions in the ready state. |
| Number of sessions in state Dyn Sync | Sessions in the dynamic synchronization state. |
| Timeout | Displays statistics for the following timers:<br>• Rate—Monitors the number of sessions to be synchronized per configured time period.<br>• Dynamic CPU—Monitors CPU limit, number of sessions, delay, and allowed calls configured for dynamic synchronization parameters.<br>• Bulk Time Li—Monitors the time limit configured for bulk synchronization.<br>• RF Notif Ext—Monitors redundancy facility (RF) active and standby state progressions and events.<br>Use the subscriber redundancy command to modify parameters that these timers monitor. |
| Delay | Timer delay (in hh:mm:ss) for bulk and dynamic synchronization for subscriber sessions. |
| Remaining | Indicates remaining time in seconds before the timer expires. |
| Starts | Indicates the number of times the timer started. |
| CPU Limit | CPU usage percentage, a configurable value; default is 90 percent. |
| CPU Last | Indicates the last time that the CPU limit timer was running. |
| Number of sessions Interested in Periodic Update | Number of sessions that have registered their interest in using the periodic update feature. |
| Configured Periodic Update Interval (In Minutes) | Periodic update interval, in minutes, that was configured with the **subscriber redundancy dynamic periodic-update interval** command. |

## Related Commands

| Command | Description |
|---|---|
| **show ccm clients** | Displays CCM client information. |
| **show ccm queues** | Displays CCM queue information. |

| Command | Description |
|---|---|
| **subscriber redundancy** | Configures subscriber session redundancy policies. |

# show checkpoint

To display a list of checkpoint clients, entitities, or statistics, use the **show checkpoint**command in privileged EXEC mode.

**show checkpoint** {**clients** | **entities** | **statistics**}

## Syntax Description

| | |
|---|---|
| **clients** | Displays detailed information about checkpoint clients. |
| **entities** | (Optional) Displays detailed information about checkpoint entities. |
| **statistics** | (Optional) Displays detailed information about checkpoint statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| 15.(0)1S | This command was modified. The output of this command was modified to include the Buffers Held Peak statistic. |

## Examples

The following is sample output from the **show checkpoint clients** command:

```
Router# show checkpoint clients
                         Check Point List of Clients
 CHKPT on ACTIVE server.
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Network RF Client          3          5        On
  Total API Messages Sent:                     26
  Total Transport Messages Sent:               --
  Length of Sent Messages:                  13480
  Total Blocked Messages Sent:                 26
  Length of Sent Blocked Messages:          13480
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Messages Received:                     14
  Total Rcv Message Len:                      360
  Total Bytes Allocated:                    73800
  Buffers Held:                                 0
  Buffers Held Peak:                            3
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:            T
############ Checked that logs were clean
No tracebacks or errmsgs in log.
######## No IPC Buffer Leaks
```

The table below describes the significant fields shown in the display.

*Table 8: show checkpoint clients Field Descriptions*

| Field | Description |
|---|---|
| Client ID | The identification number number assigned to the client. |
| Entity ID | The identification number used by In-Service Software Upgrade (ISSU) for each entity within this client. |
| Buffers Held Peak | Displays the highest number of buffers held for a client. |
| Transport Frag Count | Reports the number of fragmentation buffers used. |
| Transport Frag Peak | Reports the high water mark of fragmentation buffers requested. |

The following is sample output from the **show checkpoint statistics** command:

```
Router# show checkpoint statistics

Check Point Status
 CHKPT on ACTIVE server.
Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:            17896
TP MAX Message Size:               17992
CHKPT Pending Msg Timer:             100 ms
  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:          3781
  Total Messages Sent:              2771
  Total Sent Message Len:         382032
  Total Bytes Allocated:         2399648
  Rcv  Msg Q Peak:                    67
  Hold Msg Q Peak:                     0
  Buffers Held Peak:                 118
  Current Buffers Held:                0
  Huge Buffers Requested:              0
```

The following is sample output from the **show checkpoint entities**command:

```
Router# show checkpoint entities

Check Point List of Entities
 CHKPT on ACTIVE server.
--------------------------------------------------------------------------------
Entity ID         Entity Name
--------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            13
  Member(s) of entity 0 are:
    Client ID          Client Name
------------------------------------------
          168          DHCP Snooping
           41          Spanning-tree
          167          IGMP Snooping
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           36          LAN-Switch PAgP/LACP
           35          LAN-Switch Port Mana
           38          LAN-Switch Port Secu
          158          Inline Power Checkpo
          156          Cat4k Chassis
          172          Cat4K EbmHostMan
          157          Cat4K Link State
```

## Related Commands

| Command | Description |
|---|---|
| **show xconnect** | Displays information about xconnect attachment circuits and pseudowires. |

# show controllers shdsl

To display the status of the controller configured for single-pair high-bit-rate digital subscriber line (SHDSL) mode, use the **show controllers shdsl**command in privileged EXEC mode.

**Cisco HWIC-4SHDSL and HWIC-2SHDSL**
**show controllers shdsl** *slot number/ subslot number/*{**brief** | **detailed**}

**Cisco IAD2420**
**show controller shdsl number**

## Syntax Description

| | |
|---|---|
| **brief** | Provides a summary of the controller's status. |
| **detailed** | Provides a detailed report of the controller's status. |
| *number* | SHDSL controller number. The valid controller number for SHDSL mode is 0. |
| *slot number* | Identifies the slot on the router in which the HWIC is installed. |
| *subslot number* | Identifies the subslot on the router in which the HWIC is installed. |
| *port number* | Identifies the port on the router in which the HWIC is installed. By default, the Cisco HWIC-4SHDSL and HWIC-2SHDSL use port number 0. |

## Command Default

Controller number

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was updated for the Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router and on the Cisco 2800 and 3800 series access routers. |
| 12.2(8)T | This command was introduced on Cisco IAD2420 series. |

## Usage Guidelines

This command is used to display the controller mode, the controller number, and associated statistics.

## Examples

### Cisco HWIC-4SHDSL and HWIC-2SHDSL

The following example displays the status of a Cisco HWIC-4SHDSL controller in slot 0, subslot 2, port 0 on a Cisco access router:

```
Router# show controllers shdsl 0/2/0 brief
Controller SHDSL 0/2/0 is UP
  Hardware is HWIC-4SHDSL, rev 2 on slot 0, hwic slot 2
  Capabilities: IMA, M-pair, 2/4 wire, Annex A, B, F & G, CPE termination
  cdb=0x43EB384C, plugin=0x43DE9410, ds=0x43E9A1C4 base=0xB8000000
  FPGA Version is REL.3.4.0, NIOSII FW:Ver 2.6, status Running
  SDC-16i HW:Rev 1.2, status UP, FW:Ver 1.2-1.1.3__57, status Running
  SDFE-4 HW:Rev 1.2, status UP, FW:Ver 1.1-1.5.2__001  , status Running
  NIOSII Firmware image: System
  SDC16i Firmware image: System
  SDFE4  Firmware image: System
  Number of pairs 4, number of groups configured 1
  Ignored CLI cmds(0), Event buffer: in use(0), failed(0)
  Group (0) is Not configured.
  Group (1) info:
        Type: M-pair over g.shdsl, status: Configure Firmware
        Interface: ATM0/2/1, hwidb: 0x43F04EA0, UTOPIA phy 1
        Configured/active num links: 2/0, bit map: 0x3/0x0
        Line termination: CPE, line mode: M-pair, Annex-B, PMMS disabled
        Line coding: 16-TCPAM, configured/actual rate: 4608/0 kbps
        SHDSL wire-pair (0) is in DSL DOWN state
        SHDSL wire-pair (1) is in DSL config state
Router#
```

### Cisco IAD2420 Series

The following example displays the status of the controller that is configured for SHDSL mode on a Cisco IAD2420 series IAD:

```
Router# show controller shdsl
 0
 SHDSL 0 controller UP
 SLOT 3: Globespan xDSL controller chipset
 Frame mode: Serial ATM
 Configured Line rate: 1160Kbps
 Line Re-activated 0 times after system bootup
 LOSW Defect alarm: None
 CRC per second alarm: None
 Line termination: CPE
 FPGA Revision: 9
```

## Related Commands

| Command | Description |
|---|---|
| **controller shdsl 0** | Configures the controller status and the controller number. |

# show cwmp map

To display the Cisco WAN Management Protocol (CWMP) map information, use the **show cwmp map** command in privileged EXEC mode.

**show cwmp map** {**hosttable** | **landevice** | **lanethernetinterface** | **routetable** | **wanconnectiondevice** | **wandevice**}

## Syntax Description

| | |
|---|---|
| **hosttable** | Displays host table information. |
| landevice | Displays LAN device profile information. |
| lanethernetinterface | Displays LAN Ethernet interface profile information. |
| **routetable** | Displays map forwarding table information. |
| wanconnectiondevice | Displays WAN connection device profile information. |
| wandevice | Displays WAN device profile information. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Examples

The following is sample output from the **show cwmp map hosttable** command, which shows the object parameter values:

```
Device# show cwmp map hosttable
Host ID IP Address      Source  MAC Address          LeaseTimeRemaining  HostName
1       172.17.0.2       DHCP   0063.6973.636f.2d61. 86255               iou132
                                6162.622e.6363.3030.
                                2e38.3430.312d.4574.
                                312f.30
```

The following is sample output from the **show cwmp map landevice** command, which shows the mapping between the interfaces available in the customer premises equipment (CPE) and the instance number of the object InternetGatewayDevice.LANDevice:

**Note** All the L3 Ethernet interfaces that are not configured with the **cwmp wan default** command and the logical interface (VLAN) of the switch port in the CPE are considered as a landevice.

```
Device# show cwmp map landevice
CWMP LAN Id     Interface
2               Ethernet0/1
3               Ethernet0/2
```

```
4               Ethernet0/3
5               Ethernet1/0
6               Ethernet1/1
7               Ethernet1/2
8               Ethernet1/3
```

The following is example output from the **show cwmp map lanethernetinterface** command, which shows the mapping between the instance of the object, InternetGatewayDevice.LANDevice. and InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig. This display shows all the Layer 2 switch ports grouped under a Layer 3 interface (a VLAN interface).

```
Device# show cwmp map lanethernetinterface

CWMP LAN Id     CWMP LAN Ether Id       Interface
```

The following is example output from the **show cwmp map routetable** command, which shows the static IP routes configured in the CPE. This display provides the values of the parameters of the object, InternetGatewayDevice.Layer3Forwarding.Forwarding.

```
Device# show cwmp map routetable
CWMP Id Enable  Dest Address    Dest Mask       Gateway Address Met     Interface
1       TRUE    0.0.0.0         0.0.0.0         172.16.0.2      1
```

The following is example output from the **show cwmp map wandevice** command, which shows the mapping between the interface in CPE and the instance number of the interface specified in the TR-069 Agent. This is equivalent to the CWMP object instances, InternetGatewayDevice.WANDevice.

**Note** By default, the ATM interface is considered a wandevice even when the **wmp wan** command is not configured. L3 Ethernet interfaces are considered as wandevice only when the **cwmp wan default**command is configured.

```
Device# show cwmp map wandevice
CWMP WAN Id     Interface
1               Ethernet0/0
```

The following is example output from the **show cwmp map wanconnectiondevice** command, which shows the instance numbers of the object InternetGatewayDevice.WANDevice.i. and InternetGatewayDevice.WANDevice.i.WANConnectionDevice.j. This command also shows the associated interface in the CPE and connection type used. The connection type value is one of the following:

- IPoE--If TR-069 Agent communicates with ACS via Ethernet Interface
- IPoA--IPoA configuration
- PPPoA--PPPoA configuration
- PPPoE--PPPoE configuration
- CIP--CIP configuration
- EoA--EoA configuration

This command also shows the VPI and VCI values of the ATM interface represented by the object, InternetGatewayDevice.WANDevice.i.WANConnectionDevice.j.

```
Device# show cwmp map wanconnectiondevice

CWMP WAN Id     CWMP WAN Conn Id        Interface              VPI     VCI     Type
1               1                       Ethernet0/0                            IPoE
```

# show cwmp methods

To display the TR-069 Agent supported remote procedure call (RPC) methods and vendor profile methods, use the **show cwmp methods** command in privileged EXEC mode.

**show cwmp methods**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Examples

The following is sample output from the **show cwmp methods** command:

```
Device# show cwmp methods
CWMP RPC Methods Supported:
GetRPCMethods
SetParameterValues
GetParameterValues
GetParameterNames
SetParameterAttributes
GetParameterAttributes
AddObject
DeleteObject
Reboot
Download
Upload
X_00000C_SetConfiguration
X_00000C_ShowStatus
```

# show cwmp parameter

To display the TR-069 Agent (also called the Cisco WAN Management Protocol [CWMP]) parameter information, use the **show cwmp parameter** command in privileged EXEC mode.

**show cwmp parameter** {*parameter-name* | **all** | **notify** {**active** | **all** | **forceactive** | **passive**}}

## Syntax Description

| | |
|---|---|
| *parameter-name* | A CWMP (TR-069 Agent) parameter. |
| **all** | Displays all CWMP (TR-069 Agent) parameters. |
| **notify** | Displays a CWMP parameter notification attribute. |
| **active** | Displays the CWMP parameters with an active notification attribute. |
| **all** | Displays all of the CWMP parameters with a notification attribute. |
| **forceactive** | Displays all of the forceactive CWMP parameters. |
| **passive** | Displays all of the CWMP parameters with a passive notification attribute. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Examples

The following is sample output from the **show cwmp parameter** *parameter-name* command, which displays the value for the specified parameter:

```
Device# show cwmp parameter InternetGatewayDevice.ManagementServer.URL

Parameter = InternetGatewayDevice.ManagementServer.URL
Value = http://iou131.cisco.com/cwmp-1-0/testacs
```

The following is sample output from the **show cwmp parameter all**command, which displays all of the parameter names supported by the TR-069 Agent:

```
Device# show cwmp parameter all
InternetGatewayDevice
LANDeviceNumberOfEntries
WANDeviceNumberOfEntries
WANDevice
WANConnectionNumberOfEntries
WANCommonInterfaceConfig
WANAccessType
Layer1UpstreamMaxBitRate
Layer1DownstreamMaxBitRate
PhysicalLinkStatus
TotalBytesSent
TotalBytesReceived
```

```
TotalPacketsSent
TotalPacketsReceived
WANConnectionDevice
WANIPConnectionNumberOfEntries
WANPPPConnectionNumberOfEntries
WANIPConnection
Enable
ConnectionStatus
PossibleConnectionTypes
ConnectionType
Name
Uptime
LastConnectionError
AddressingType
ExternalIPAddress
SubnetMask
DefaultGateway
DNSEnabled
DNSServers
MACAddress
ConnectionTrigger
WANPPPConnection
Enable
ConnectionStatus
Name
Uptime
LastConnectionError
Username
Password
ExternalIPAddress
X_00000C_SubnetMask
DNSEnabled
DNSServers
MACAddress
TransportType
PPPoEACName
PPPoEServiceName
WANDSLLinkConfig
Enable
LinkStatus
LinkType
AutoConfig
DestinationAddress
ATMTransmittedBlocks
ATMReceivedBlocks
AAL5CRCErrors
ATMCRCErrors
WANEthernetInterfaceConfig
Enable
Status
MACAddress
MaxBitRate
DuplexMode
Stats
BytesSent
BytesReceived
PacketsSent
PacketsReceived
WANDSLInterfaceConfig
Enable
Status
UpstreamCurrRate
DownstreamCurrRate
UpstreamMaxRate
```

```
DownstreamMaxRate
UpstreamNoiseMargin
DownstreamNoiseMargin
UpstreamAttenuation
DownstreamAttenuation
UpstreamPower
DownstreamPower
ATURVendor
ATURCountry
ATUCVendor
ATUCCountry
TotalStart
ShowtimeStart
Stats
Total
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
Showtime
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
WANDSLConnectionManagement
ConnectionServiceNumberOfEntries
ConnectionService
WANConnectionDevice
WANConnectionService
DestinationAddress
LinkType
Name
LANDevice
LANEthernetInterfaceNumberOfEntries
LANUSBInterfaceNumberOfEntries
LANWLANConfigurationNumberOfEntries
LANHostConfigManagement
DHCPServerConfigurable
DHCPServerEnable
DHCPRelay
MinAddress
MaxAddress
ReservedAddresses
SubnetMask
DNSServers
DomainName
```

```
IPRouters
IPInterfaceNumberOfEntries
IPInterface
Enable
IPInterfaceIPAddress
IPInterfaceSubnetMask
IPInterfaceAddressingType
Hosts
HostNumberOfEntries
Host
IPAddress
AddressSource
LeaseTimeRemaining
MACAddress
HostName
LANEthernetInterfaceConfig
Enable
Status
MACAddress
MaxBitRate
DuplexMode
Stats
BytesSent
BytesReceived
PacketsSent
PacketsReceived
DeviceInfo
Manufacturer
ManufacturerOUI
ModelName
Description
SerialNumber
HardwareVersion
SoftwareVersion
SpecVersion
ProvisioningCode
UpTime
DeviceLog
ManagementServer
URL
Username
Password
PeriodicInformEnable
PeriodicInformInterval
PeriodicInformTime
ParameterKey
ConnectionRequestURL
ConnectionRequestUsername
ConnectionRequestPassword
UpgradesManaged
LANConfigSecurity
ConfigPassword
Layer3Forwarding
DefaultConnectionService
ForwardNumberOfEntries
Forwarding
Enable
Status
DestIPAddress
DestSubnetMask
SourceIPAddress
SourceSubnetMask
GatewayIPAddress
Interface
```

```
ForwardingMetric
IPPingDiagnostics
DiagnosticsState
Interface
Host
NumberOfRepetitions
Timeout
DataBlockSize
SuccessCount
FailureCount
AverageResponseTime
MinimumResponseTime
MaximumResponseTime
Time
NTPServer1
NTPServer2
NTPServer3
NTPServer4
NTPServer5
CurrentLocalTime
LocalTimeZone
LocalTimeZoneName
DaylightSavingsUsed
DaylightSavingsStart
DaylightSavingsEnd
TraceRouteDiagnostics
DiagnosticsState
Host
Timeout
MaxHopCount
ResponseTime
NumberOfRouteHops
RouteHops
HopHost
```

The following is sample output from the **show cwmp parameter notify active**command, which displays all of the parameters in which the notification attribute is set to active:

```
Device# show cwmp parameter notify active

Active Notification:
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceSubnetMask
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceAddressingType
```

The following is sample output from the **show cwmp parameter notify all**command, which displays all of the parameters in which the notification attribute is set:

```
Device# show cwmp parameter notify all
Active Notification:
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceSubnetMask
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceAddressingType
```

```
Passive Notification:
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.Enable
```

The following is sample output from the **show cwmp parameter notify forceactive**command, which displays all of the forceactive parameters in the TR-069 Agent:

```
Device# show cwmp parameter notify forceactive

Forced Active Notification:
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress
```

The following is sample output from the **show cwmp parameter notify passive**command, which displays all of the parameters in which the notification attribute is set to passive:

```
Device# show cwmp parameter notify passive

Passive Notification:
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.Enable
```

# show cwmp persistent

To display all of the persistent Cisco WAN Management Protocol (CWMP) parameters stored in the NVRAM by the TR-069 Agent, use the **show cwmp persistent** command in privileged EXEC mode.

**show cwmp persistent data**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Examples

The following is sample output from the **show cwmp persistent data**command:

```
Device# show cwmp persistent data
InternetGatewayDevice.ManagementServer.URL
 InternetGatewayDevice.ManagementServer.Username
 InternetGatewayDevice.ManagementServer.Password
 InternetGatewayDevice.ManagementServer.PeriodicInformEnable
 InternetGatewayDevice.ManagementServer.PeriodicInformInterval
 InternetGatewayDevice.ManagementServer.PeriodicInformTime
 InternetGatewayDevice.ManagementServer.ParameterKey
 InternetGatewayDevice.ManagementServer.ConnectionRequestURL
 InternetGatewayDevice.ManagementServer.ConnectionRequestUsername
 InternetGatewayDevice.ManagementServer.ConnectionRequestPassword
 InternetGatewayDevice.ManagementServer.UpgradesManaged
```

# show cwmp session

To display the TR-069 Agent session information, use the **show cwmp session** command in privileged EXEC mode.

**show cwmp session**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Examples

The following is sample output from the **show cwmp session** command when a successful session is established between the TR-069 Agent and the auto-configuration server (ACS):

```
Device# show cwmp session

CWMP Agent status: Enabled
No CWMP Session currently running
Management Server: http://iou131.cisco.com/cwmp-1-0/testacs
Connection Request URL: http://172.16.0.1/00000C/388280450/cwmp
Last successful connection request at time: 10:46:47 PST Tue Jun 17 2008
Last successful session at time: 10:46:48 PST Tue Jun 17 2008
Last failed session at time: 10:42:48 PST Tue Jun 17 2008
```

The following is sample output from the **show show cwmp session** command when a session is unable to connect between the TR-069 Agent and the ACS:

```
Device# show cwmp session

CWMP Agent status: Enabled
CWMP Session currently running
Management Server for this session: http://iou131.cisco.com/cwmp-1-0/testacs
Hold Requests for this session: 0
Max-Envelopes from ACS for this session: 1
Number of outstanding requests: 1
Requests outstanding over the session:
Inform
Inform
Requests to be sent over the session: 0
Management Server: http://iou131.cisco.com/cwmp-1-0/testacs
Connection Request URL: http://172.16.0.1/00000C/388280450/cwmp
Last successful connection request at time:
Last successful session at time: 10:39:05 PST Tue Jun 17 2008
Last failed session at time: 10:42:03 PST Tue Jun 17 2008
Session retry count: 1
```

# show dsl interface atm

To display information specific to the asymmetric digital subscriber line (ADSL) for a specified ATM interface, use the **show dsl interface atm** command in user EXEC or privileged EXEC mode.

**show dsl interface atm** *interface-number*

## Syntax Description

| | |
|---|---|
| *interface-number* | (Optional) ATM interface number. |

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XJ | The command was introduced on Cisco 1700 series routers. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.1(5)YB | Support for this command was added to Cisco 2600 series and Cisco 3600 series routers. |
| 12.1(5)XR1 | Support for this command was added to the Cisco IAD2420 series. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |

## Usage Guidelines

Use this command to display the status or results of a line test and to get information on port status, alarms, configured and actual transmission rates, and transmission errors. The **atm** word in this command is not a keyword but it is part of the command and optional. The output of this command is not affected by the **atm** keyword.

The output from this command appears the same as the output from the **show controller atm**command on Cisco 1400 series routers.

## Examples

### ADSL: Example

The following is sample output from the **show dsl interface atm** command for a CPE device that is configured for ADSL:

```
Router# show dsl interface atm 0/0
Alcatel 20150 chipset information
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.1 (G.DMT)
ITU STD NUM:     0x01                            0x1
Vendor ID:       'ALCB'                          'ALCB'
Vendor Specific: 0x0000                          0x0000
Vendor Country:  0x00                            0x0F
Capacity Used:   85%                             98%
Noise Margin:    13.5 dB                          7.0 dB
Output Power:     9.5 dBm                        12.0 dBm
```

```
Attenuation:      1.5 dB                          3.5 dB
Defect Status:   None                            None
Last Fail Code:  None
Selftest Result: 0x00
Subfunction:     0x15
Interrupts:      5940 (0 spurious)
PHY Access Err:  0
Activations:     1
SW Version:      3.670
FW Version:      0x1A04
                 Interleave             Fast    Interleave              Fast
Speed (kbps):             0             8128             0               864
Reed-Solomon EC:          0                0             0                 0
CRC Errors:               0                0             0                 7
Header Errors:            0                0             0                 2
Bit Errors:               0                0
BER Valid sec:            0                0
BER Invalid sec:          0                0
DMT Bits Per Bin
00: 0 0 0 0 0 0 0 7 6 7 9 A B C C C
10: C C C C C C B B B B A 9 A 9 0 0
20: 0 0 0 0 0 0 2 2 3 4 4 5 6 6 7 7
30: 7 8 8 8 9 9 9 A A A A A A B B B
40: B B B B B B B B B B B A B B B B
50: B B B B B B B B B B B B 2 B B B
60: B B B B B B B B B B B B B B B B
70: B B B B B B B B B B B B B B B B
80: B B B B B B B B B B B B B B B B
90: B B B B B B B B B B B B B B B B
A0: B B B B B B B B B B B B B B B B
B0: B B B B B B B B B B B B A B A A
C0: A A A A A A A A A A A A A A A A
D0: A A A A A A A A A A A 9 9 9 9 9
E0: 9 9 9 9 9 9 9 9 9 9 9 9 8 8 8 8
F0: 8 8 8 8 8 8 7 7 7 7 6 6 5 5 4 4
```

The table below describes the significant fields shown in the display.

*Table 9: show dsl interface atm Field Descriptions*

| Field | Description |
|---|---|
| Modem Status | Status of the modem. Possible states include the following:<br>DMTDSL_INVALID--Error state.<br>DMTDSL_STOP--Administrative down state.<br>DMTDSL_INIT--Restarting line.<br>DMTDSL_CHK_HW--Confirming that required HW exists.<br>DMTDSL_DLOAD_1--Downloading the init.bin file.<br>DMTDSL_DLOAD_2--Downloading operational firmware.<br>DMTDSL_MODE_CHK--Verifying that download was successful.<br>DMTDSL_DO_OPEN--Issue ADSL_OPEN command.<br>DMTDSL_RE_OPEN--Cycle the link. Retry open.<br>DMTDSL_ACTIVATING--Waiting for activation to succeed.<br>DMTDSL_LOOPBACK--Activation done.<br>DMTDSL_SHOWTIME--Activation succeeded. |
| DSL Mode | DSL operating mode. |
| ITU STD NUM | ITU standard number for the operating mode. |
| Vendor ID | Vendor identification code. |
| Vendor Specific | Indicates if this router is specified for a vendor. |
| Vendor Country | Code for the country where the vendor is located. |
| Capacity Used | Percentage of the capacity that is being used. |
| Noise Margin | Noise margin, in decibels. |
| Output Power | Power output, in decibels. |
| Attenuation | Attenuation of the signal, in decibels. |
| Defect Status | Status of defects. |
| Last Fail Code | Last failure code that was logged. |
| Selftest Result | Results of the self-test. |
| Subfunction | Code for the subfunction running. |
| Interrupts | Code for interrupts used. |
| PHY Access Err | Number of physical access errors. |
| Activations | Number of activations of the router. |

| Field | Description |
|---|---|
| SW Version | Software version number. |
| FW Version | Firmware version number. |
| Speed | The train speed for upstream and downstream. It shows both the interleave and the fast mode. |
| Reed-Solomon EC | Reed-Solomon error-correction statistics. |
| CRC Errors | Cyclic redundancy check statistics. |
| Header Errors | ATM header error reports. |
| Bit Errors | Total number of bit errors. |
| BER Valid sec | Bit error rate valid seconds. |
| BER Invalid sec | Bit error rate invalid seconds. |

### G.SHDSL: Example

The following is sample output from the **show dsl interface atm** command for a CPE device that is configured for G.SHDSL:

```
Router# show dsl interface atm 0/0
Globespan G.SHDSL Chipset Information
Equipment Type: Customer Premise
Operating Mode: G.SHDSL
Clock Rate Mode: Auto rate selection Mode
Reset Count: 1
Actual rate: 2320 Kbps
Modem Status: Data
Noise Margin: 42 dB
Loop Attenuation: 0.0 dB
Transmit Power: 13.5 dB
Receiver Gain: 204.8000 dB
Last Activation Status:No Failure
CRC Errors: 0
Chipset Version: 1
Firmware Version: R1.0
```

The table below describes the significant fields shown in the display.

***Table 10: show dsl interface atm Field Descriptions***

| Field | Description |
|---|---|
| Equipment Type | Terminal type, which can be one of the following:<br>• Customer Premise (CPE)--This value indicates that the device is connected to a DSLAM. This is the default.<br>• Central Office (CO)--If the devices are connected back-to-back, one of the routers can act as a CO. |

| Field | Description |
|---|---|
| Operating Mode | G.SHDSL annex configuration, which can be one of the following values:<br>• A--Operating parameters for North America. This value is the default.<br>• B--Operating parameters for Europe. |
| Clock Rate Mode | Upstream and downstream bit rate configuration, in kb/s. If the upstream and downstream rates have different values, the device will train to lowest of the rates. If the value indicates "Auto Rate Selection Mode," the CO and CPE devices will negotiate the speed and train. |
| Reset Count | Number of times the G.SHDSL chip has been reset since powering up. |
| Actual rate | The actual bit rate that the transceiver is using. This rate could be different from the requested (configured) rate. |
| Modem Status | One of the following values:<br>• Handshake--local transceiver is trying to reach the far-end transceiver.<br>• Training--startup training is in progress.<br>• Data--training was successful. |
| Received SNR | The received signal-to-noise ratio (SNR), in decibels (dB). |
| SNR Threshold | SNR threshold below which the router will retrain. The default is 23 dB. |
| Loop Attenuation | The difference in decibels between the power received at the near-end device and the power transmitted from the far-end device. |
| Transmit Power | Local STU transmit power, in decibels per milliwatt (dBm). |
| Receiver Gain | Total receiver gain. |
| Last Activation Status | Defines the last failure state of the G.SHDSL chip. |
| CRC Errors | Number of cyclic redundancy check (CRC) errors observed after bootup or resetting of the interface. |
| Chipset Version | Vendor's chipset version. |
| Firmware Version | Version of the vendor's chipset firmware. |

## Related Commands

| Command | Description |
|---|---|
| **dsl operating-mode** | Modifies the operating mode of the digital subscriber line for an ATM interface. |
| show controller atm | Displays information about about an inverse multiplexing over ATM (IMA) group. |

# show ip http client cookie

To display the HTTP client cookies, use the **show ip http client cookie** command in privileged EXEC mode.

**show ip http client cookie** {**brief**|**summary**} [{**domain** *cookie-domain*|**name** *cookie-name*|**session** *session-name*}]

## Syntax Description

| **brief** | Displays a brief summary of client cookies. |
|---|---|
| summary | Displays a detailed summary of client cookies. |
| domain | (Optional) Displays all cookies in a domain |
| *cookie-domain* | (Optional) Client cookie domain or host name. |
| name | (Optional) Displays cookies matching a specific name. |
| *cookie-name* | (Optional) Client cookie name. |
| session | (Optional) Displays cookies specific to a client session. |
| *session-name* | (Optional) Client session name. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |

## Examples

The following is example output from the **show ip http client cookie brief**command:

```
Device# show ip http client cookie brief
HTTP client cookies of session HTTP CFS :
HTTP client cookies of session CWMP_CLIENT :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie8          8                              1       172.17.0.2
/cwmp-1-0/
cookie7          7                              1       172.17.0.2
/cwmp-1-0/
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
HTTP client cookies of session cwmp_test_client :
```

The following is example output from the **show ip http client cookie brief domain**command:

```
Device# show ip http client cookie brief domain 172.16.0.2
```

```
HTTP client cookies of domain 172.16.0.2 :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie brief name**command:

```
Device# show ip http client cookie brief name cookie3
HTTP client cookies of name cookie3 :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie brief session**command:

```
Device# show ip http client cookie brief session CWMP_CLIENT
HTTP client cookies of session CWMP_CLIENT :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie8          8                              1       172.17.0.2
/cwmp-1-0/
cookie7          7                              1       172.17.0.2
/cwmp-1-0/
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie summary**command:

```
Device# show ip http client cookie summary
HTTP client cookies of session HTTP CFS :
HTTP client cookies of session CWMP_CLIENT :
Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
```

```
CommentURL    :

Name          : cookie3
Value         :  3
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie2
Value         :  2
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie1
Value         :  1
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
HTTP client cookies of session cwmp_test_client :
```

The following is example output from the **show ip http client cookie summary domain**command:

```
Device# show ip http client cookie summary domain 172.17.0.2
HTTP client cookies of domain 172.17.0.2 :
Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

The following is example output from the **show ip http client cookie summary name**command:

```
Device# show ip http client cookie summary name cookie7
HTTP client cookies of name cookie7 :
```

```
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

The following is example output from the **show ip http client cookie summary session**command:

```
Device# show ip http client cookie summary session CWMP_CLIENT
HTTP client cookies of session CWMP_CLIENT :
Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie3
Value         :  3
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie2
Value         :  2
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie1
Value         :  1
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
```

```
Comment        :
CommentURL     :
```

# show mpf cpu

To display the average CPU utilization over a duration of the last 5 seconds, the last 1 minute, and the last 5 minutes when Multi-Processor Forwarding (MPF) is enabled on the second CPU, use the **show mpf cpu**command in user EXEC or privileged EXEC mode.

**show** **mpf** **cpu** [**history**]

## Syntax Description

| | |
|---|---|
| history | (Optional) Displays graphical output of the second CPU utilization over the last 60 seconds, the last 60 minutes, and the last 72 hours. |

## Command Default

No default behavior or values.

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)YM2 | This command was introduced in Cisco IOS Release 12.3(14)YM2 and supported on the Cisco 7200 VXR and Cisco 7301 routers. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T. |

## Examples

The following example shows that the average utilization of the second CPU is 33 percent for the last 5 seconds, 25 percent for the last minute, and 30 percent for the last 5 minutes:

```
Router# show mpf cpu
CPU utilization for five seconds: 33%; one minute: 25%; five minutes: 30%
```

The following example shows graphical output of utilization of the second CPU for the last 60 seconds (percentage of CPU use per second), the last 60 minutes (percentage of CPU use per minute), and the last 72 hours (percentage of CPU use per hour).

```
Router# show mpf cpu history
slns 12:12:40 AM Saturday Nov 18 2000 UTC
3333333333333333333333333333333333333333333333333333333333
3333333333333333333333333333333333333333333333333333333333
100
90
80
70
60
50
40
30 ***************************
20 ***************************
10 ***************************
0....5....1....1....2....2....3....3....4....4....5....5....
     0     5     0    5     0     5    0    5    0    5
    CPU% per second (last 60 seconds)
3333333333333333333333333333333333333333333333333333333333
```

```
3333333333333333333333333333333333333333333333333333333333
100
90
80
70
60
50
40
30 #################
20 #################
10 #################
0....5....1....1....2....2....3....3....4....4....5....5....
    0     5    0     5     0     5    0     5    0     5
     CPU% per minute (last 60 minutes)
     * = maximum CPU% # = average CPU%
1
60
80
100 *
90 *
80 *
70 **
60 **
50 **
40 ##
30 ##
20 ##
10 ##
0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
    0         5     0    5    0    5    0    5    0    5    0    5    0
     CPU% per hour (last 72 hours)
     * = maximum CPU% # = average CPU%
```

## Related Commands

| Command | Description |
|---|---|
| **clear mpf interface** | Clears MPF packet counts on all physical interfaces. |
| **clear mpf punt** | Clears MPF per-box punt reason and count. |
| **ip mpf** | Enable MPF on the second CPU of Cisco 7200 VXR and Cisco 7301 routers. |
| **show ip cef exact-route** | Displays the exact route for a source-destination IP address pair in CEF. |
| **show mpf interface** | Displays MPF packet count information on each physical interface. |
| show mpf ip exact-route | Displays the exact route for a source-destination IP address pair in an MPF system. |
| **show mpf punt** | Displays the MPF punt reason and punt packet count for the chassis. |
| **sw-module heap fp** | Fine-tunes the MPF heap memory allocation. |

# show mpf interface

To display Multi-Processor Forwarding (MPF) packet counter information on each physical interface, use the **show mpf interface**command in user EXEC or privileged EXEC mode.

**show mpf interface** [**interface-name-and-number**] [**dot1q-vlan-num**]

## Syntax Description

| | |
|---|---|
| *interface-name-and-number* | (Optional) Displays punt counts for a specified Gigabit Ethernet interface and its slot number and port number. |
| *dotlq-vlan-num* | (Optional) Displays punt counts on a specific subinterface by specifying the 802.1Q VLAN number. |

## Command Default

No default behavior or values.

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)YM2 | This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T. |

## Usage Guidelines

This command is supported for physical interfaces and subinterfaces. There is no support for the virtual access interface (VAI).

You can display the interface count information for a specific Gigabit Ethernet interface by specifying the interface name and number. To display interface information for a specified subinterface only, you must use the 802.1Q VLAN number for the subinterface because the MPF software does not recognize the subinterface number.

Using the show mpf interface command without arguments displays the interface information for all Gigabit Ethernet interfaces and subinterfaces.

Using the **clear mpf interface** command resets the interface packet counters shown in the **show mpf interface** command output.

## Examples

The following example using the show mpf interface command without arguments displays interface information about up or down state, type of counter (receiving or transmitting packet or bytes), and count number for packets or bytes for all Gigabit Ethernet interfaces (only GigabitEthernet0/1 in this example) and subinterfaces:

```
Router# show mpf interface
Name           Index   State       Counter              Count
Gi0/1          0       up          RX packets           1004
                                   RX bytes             158632
                                   TX packets           5004
```

```
Name           Index  State        Counter             Count
                                   TX bytes            790632
                                   RX punts            32961
                                   TX punts            85972
Gi0/1          1      up
Gi0/1.100      100    up           RX packets          1004
                                   RX bytes            158632
                                   TX packets          5004
                                   TX bytes            790632
                                   RX punts            25
Gi0/1.101      101    up
Gi0/1.102      102    up
Gi0/1.105      105    up
Gi0/1.106      106    up
Gi0/1.107      107    up
Gi0/1.200      200    up
Gi0/1.201      201    up           RX punts            29
Gi0/1.202      202    up
Gi0/1.206      206    up
Gi0/1.2002     602    up           RX punts            26114
Gi0/1.2004     604    up
```

The following example specifies interface information for Gigabit Ethernet interface 0/1 subinterface 100. However, all Gigabit Ethernet interface and subinterface information is displayed because MPF does not recognize the subinterface number, unless it is a VLAN number.

```
Router# show mpf interface
GigabitEthernet0/1.100
Name          Index   State     Counter               Count
Gi0/1         0       up        RX packets            1004
                                RX bytes              158632
                                TX packets            5004
                                TX bytes              790632
                                RX punts              32996
                                TX punts              86062
Gi0/1         1       up
Gi0/1.100     100     up        RX packets            1004
                                RX bytes              158632
                                TX packets            5004
                                TX bytes              790632
                                RX punts              25
Gi0/1.101     101     up
Gi0/1.102     102     up
Gi0/1.105     105     up
Gi0/1.106     106     up
Gi0/1.107     107     up
Gi0/1.200     200     up
Gi0/1.201     201     up       RX punts               29
Gi0/1.202     202     up
Gi0/1.206     206     up
Gi0/1.2002    602     up       RX punts               26142
Gi0/1.2004    604     up
```

The following example displays the interface information for VLAN number 100 on Gigabit Ethernet interface 0/1, including up state, receiving packet count, receiving bytes count, transmitting packet count, transmitting byte count, and receiving punt count:

```
Router# show mpf interface GigabitEthernet0/1 100
Name          Index   State     Counter               Count
Gi0/1.100     100     up        RX packets            1004
                                RX bytes              158632
                                TX packets            5004
```

```
                                   TX bytes              790632
                                   RX punts              25
```

The table below describes the fields shown in the output examples.

*Table 11: show mpf interface Field Descriptions*

| Field | Description |
|---|---|
| Name | Gigabit Ethernet interface name and number. |
| Index | This is for internal use and can be ignored. |
| State | Up or down state of interface. |
| Counter | Type of counter. |
| Count | Number of packets or bytes. |
| RX packets | Packets received through the Gigabit Ethernet interface and processed by the second CPU, CPU1. These packets are MPF accelerated. |
| RX bytes | Bytes received and processed by the second CPU, CPU1. |
| RX punts | Packets received through the Gigabit Ethernet interface and punted by the second CPU, CPU1, to CPU0 for Cisco IOS processing. |
| RX drop | Packets received through the Gigabit Ethernet interface but dropped by the second CPU, CPU1. |
| TX packets | MPF accelerated packets transmitted from the Gigabit Ethernet interface using the second CPU, CPU1. |
| TX bytes | Bytes transmitted by the second CPU, CPU1. |
| TX punts | Packets transmitted from the second CPU, CPU1. Packets that have been punted to CPU0 and processed by Cisco IOS software are redirected to CPU1 for transmitting from the relevant Gigabit Ethernet interface. |
| TX drop | Packets that were dropped by the second CPU, CPU1, while in the process of being transmitted from the Gigabit Ethernet interface. |

## Related Commands

| Command | Description |
|---|---|
| **clear mpf interface** | Clears MPF packet counts on all physical interfaces. |
| **clear mpf punt** | Clears MPF per-box punt reason and count. |
| **ip mpf** | Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router. |
| **show ip cef exact-route** | Displays the exact route for a source-destination IP address pair in CEF. |
| **show mpf cpu** | Displays the average CPU utilization when MPF is enabled on the second CPU. |
| show mpf ip exact-route | Displays the exact route for a source-destination IP address pair in an MPF system. |

| Command | Description |
|---|---|
| **show mpf punt** | Displays the MPF punt reason and punt packet count for the chassis. |
| **sw-module heap fp** | Fine-tunes the MPF heap memory allocation. |

# show mpf ip exact-route

To display the exact route for a source-destination address IP pair in a Multi-Processor Forwarding (MPF) system, use the **show mpf ip exact-route**command in user EXEC or privileged EXEC mode.

**show mpf ip exact-route** [**vrf** **vrf-name**] **src-ip-addr** **dst-ip-addr**

## Syntax Description

| | |
|---|---|
| vrf | (Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance. |
| vrf-name | (Optional) Name assigned to the VRF. |
| src-ip-addr | Specifies the network source address. |
| dst-ip-addr | Specifies the network destination address. |

## Command Default

No default behavior or values.

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)YM2 | This command was introduced in Cisco IOS Release 12.3(14)YM2 and supported on the Cisco 7200 VXR and Cisco 7301 routers. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T. |

## Usage Guidelines

When you are load balancing per destination, this command shows the exact next hop that is used for a given IP source-destination pair.

## Examples

The following sample output displays the exact next hop (10.1.104.1) for the specified source IP address (10.1.1.1) and destination IP address (172.17.249.252):

```
Router# show mpf ip exact-route 10.1.1.1 172.17.249.252
10.1.1.1         -> 172.17.249.252 :GigabitEthernet2/0 (next hop 10.1.104.1)
```

The table below describes the significant fields shown in the output example.

*Table 12: show mpf ip exact-route Field Descriptions*

| Field | Description |
|---|---|
| 10.1.1.1 -> 172.17.249.252 | From source 10.1.1.1 IP address to destination IP address 172.17.249.252. |
| GigabitEthernet2/0 (next hop 10.1.104.1) | Next hop is 10.1.104.1 on GigabitEthernet interface 2/0. |

## Related Commands

| Command | Description |
|---|---|
| **clear mpf interface** | Clears MPF packet counts on all physical interfaces. |
| **clear mpf punt** | Clears MPF per-box punt reason and count. |
| **ip mpf** | Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router. |
| **show ip cef exact-route** | Displays the exact route for a source-destination IP address pair in CEF. |
| **show mpf cpu** | Displays the average CPU utilization when MPF is enabled on the second CPU. |
| **show mpf interface** | Displays MPF packet count information on each physical interface. |
| **show mpf punt** | Displays the MPF punt reason and punt packet count for the chassis. |
| **sw-module heap fp** | Fine-tunes the MPF heap memory allocation. |

# show mpf punt

To display the Multi-Processor Forwarding (MPF) punt reason and punt packet count for the chassis, use the **show mpf punt**command in user EXEC or privileged EXEC mode.

**show mpf punt**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)YM2 | This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T. |

## Usage Guidelines

The punt reason and punt packet count are collected for each box or chassis, not for each interface. Packets that are punted are directed for Cisco IOS processing and are not accelerated by MPF.

## Examples

The following example displays the types of packet, the reasons for the punt, and the punt packet counts for the router chassis.

```
Router# show mpf punt
  Type     Message         Count
  l2tp     unknown session errors          7
  l2tp     L2TP control          6
  ipv4/verify     adjacency punt          1
  ethernet     unknown ethernet type             542
  ppp     punts due to unknown protocol    333
  arp     ARP request          6
```

The table below describes the fields in the **show mpf punt** output display.

*Table 13: show mpf punt Field Descriptions*

| Field | Description |
|---|---|
| Type | Packet type or encapsulation, such as ARPA, Ethernet, or L2TP. |
| Message | Reason for punting the packet to Cisco IOS processing. |
| Count | Punt packet count. |

## Related Commands

| Command | Description |
|---|---|
| **clear mpf interface** | Clears MPF packet counts on all physical interfaces. |

| Command | Description |
|---|---|
| **clear mpf punt** | Clears MPF per-box punt reason and count. |
| **ip mpf** | Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router. |
| **show ip cef exact-route** | Displays the exact route for a source-destination IP address pair in CEF. |
| **show mpf cpu** | Displays the average CPU utilization when MPF is enabled on the second CPU. |
| **show mpf interface** | Displays MPF packet count information on each physical interface. |
| show mpf ip exact-route | Displays the exact route for a source-destination IP address pair in an MPF system. |
| **sw-module heap fp** | Fine-tunes the MPF heap memory allocation. |

# show ppp interface

To display the IP Control Protocol (IPCP) and Link Control Protocol (LCP) information for all the sessions on an ATM or Gigabit Ethernet interface, use the **show ppp interface** command in user EXEC or privileged EXEC mode.

**show ppp interface** *interface number*

## Syntax Description

| | |
|---|---|
| *interface number* | Specifies a particular ATM or Gigabit Ethernet interface and the interface number. |

## Command Modes

User EXEC (>)
Privileged EXEC (#))

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.4 | This command was introduced. |
| Cisco IOS Release 15.0(1)M | This command was integrated into Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

The **show ppp interface**command is used to display IPCP and LCP information for all the sessions on an ATM or Gigabit Ethernet interface.

## Examples

The following example displays the IPCP and LCP information on the Gigabit Ethernet interface. The output is self-explanatory.

```
Device# show ppp interface GigabitEthernet 0/1/0.101

Gi0/1/0.101 No PPP serial context
PPP Session Info
----------------
Interface        : Vi2.1
PPP ID           : 0x26000001
Phase            : UP
Stage            : Local Termination
Peer Name        : user_01@domain_3
Peer Address     : 12.0.0.1
Control Protocols: LCP[Open] CHAP+ IPCP[Open]
Session ID       : 1
AAA Unique ID    : 12
SSS Manager ID   : 0x25000003
SIP ID           : 0x7B000002
PPP_IN_USE       : 0x15

Vi2.1 LCP: [Open]
Our Negotiated Options
Vi2.1 LCP:    MRU 1492 (0x010405D4)
Vi2.1 LCP:    AuthProto CHAP (0x0305C22305)
Vi2.1 LCP:    MagicNumber 0x21F4CD31 (0x050621F4CD31)
Peer's Negotiated Options
Vi2.1 LCP:    MRU 1492 (0x010405D4)
Vi2.1 LCP:    MagicNumber 0x4A51A20E (0x05064A51A20E)
```

```
Vi2.1 IPCP: [Open]
Our Negotiated Options
Vi2.1 IPCP:    Address 10.0.0.1 (0x03060A000001)
Peer's Negotiated Options
Vi2.1 IPCP:    Address 12.0.0.1 (0x03060C000001)
```

```
Device# show ppp interface atm 3/0.2

 AT3/0.2 No PPP serial context
 PPP Session Info
 ----------------
 Interface        : Vi2.1
 PPP ID           : 0x3A000001
 Phase            : UP
 Stage            : Local Termination
 Peer Name        : joe@pepsi.com
 Peer Address     : 20.21.22.23
 Control Protocols: LCP[Open] PAP+ IPCP[Open]
 Session ID       : 1
 AAA Unique ID    : 12
 SSS Manager ID   : 0x40000003
 SIP ID           : 0x86000002
 PPP_IN_USE       : 0x15

 Vi2.1 LCP: [Open]
 Our Negotiated Options
 Vi2.1 LCP:    MRU 1492 (0x010405D4)
 Vi2.1 LCP:    AuthProto PAP (0x0304C023)
 Vi2.1 LCP:    MagicNumber 0x06545BB4 (0x050606545BB4)
 Peer's Negotiated Options
 Vi2.1 LCP:    MRU 1492 (0x010405D4)
 Vi2.1 LCP:    MagicNumber 0x01CB46A9 (0x050601CB46A9)

 Vi2.1 IPCP: [Open]
 Our Negotiated Options
   NONE
 Our Rejected options
   Address
 Peer's Negotiated Options
 Vi2.1 IPCP:    Address 20.21.22.23 (0x030614151617)
```

## Related Commands

| Command | Description |
|---|---|
| **ppp bap** | Displays the BAP configuration settings and run-time status for a multilink bundle. |
| **ppp queues** | Monitors the number of requests processed by each AAA background process. |

# show ppp subscriber statistics

To display PPP subscriber statistics, use the **show ppp subscriber statistics** command in privileged EXEC mode.

**show ppp subscriber statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

This command is useful for obtaining events and statistics for PPP subscribers. Use the show ppp subscriber statistics command to display a cumulative count of PPP subscriber events and statistics, and to display an incremental count since the clear ppp subscriber statistics command was last issued.

## Examples

The following is sample output from the show ppp subscriber statistics command:

```
Router# show ppp subscriber statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          32011         32011
DeEncap                        16002         16002
CstateUp                       173           173
CstateDown                     36            36
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       173           173
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        167           167
PPPBindResp                    173           173
PPPReneg                       3             3
RestartTimeout                 169           169
>
PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  16008         16008
IDB CSTATE DOWN                40            40
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 10            10
```

The table below describes the significant fields shown in the display. Any data not described in the table below is used for internal debugging purposes.

*Table 14: show ppp subscriber statistics Field Descriptions*

| Field | Description |
|---|---|
| PPP Subscriber Events | PPP subscriber event counts. |
| Encap | Number of times PPP encapsulation occurred. |
| DeEncap | Number of times PPP deencapsulation occurred. |
| CstateUp | Number of times PPP interfaces were initialized. |
| CstateDown | Number of times PPP interfaces were shut down. |
| FastStart | Number of PPP sessions started by link control protocol (LCP) packets before the interface state was up. |
| LocalTerm | Number of locally terminated PPP sessions. |
| LocalTermVP | Number of locally terminated PPP sessions running on virtual profiles. |
| MoreKeys | Number of PPP sessions in the intermediate state--that is, processing service keys--before a session is forwarded or terminated locally. |
| Forwarding | Number of PPP sessions in forwarding state. |
| Forwarded | Number of PPP sessions that have been forwarded. |
| SSSDisc | Number of PPP sessions disconnected from the subscriber service switch after receiving a disconnect notification. |
| SSMDisc | Number of PPP sessions disconnected from the dataplane after receiving a disconnect notification. |
| PPP BindResp | Number of PPP responses where the interface has been bound to the session. |
| PPP Reneg | Number of PPP renegotiation events. |
| RestartTimeout | Occurrences of the restart timer beginning on PPP encapsulated interfaces in the down state. |
| PPP Subscriber Statistics | PPP subscriber statistic counts. |
| IDB CSTATE UP | Occurrences of the IDB making the transition to the up state. |
| IDB CSTATE DOWN | Occurrences of the IDB making the transition to the down state. |
| APS UP | Occurrences of PPP sessions receiving automatic protection switching (APS) selected events. |
| APS UP IGNORE | Occurrences of PPP sessions receiving APS selected events when the IDB state was down. |
| APS DOWN | Occurrences of PPP sessions receiving APS deselected events. |
| READY FOR SYNC | Number of PPP sessions ready for synchronization. |

## Related Commands

| Command | Description |
|---|---|
| **clear ppp subscriber statistics** | Clears PPP subscriber statistics. |

# show pppatm redundancy

To display PPP over ATM (PPPoA) statistics, use the **show pppatm** redundancy command in privileged EXEC mode.

**show pppatm redundancy**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 2.1 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

This command is useful for obtaining statistics for PPPoA sessions. This command gives a total count of PPPoA events since the clear pppatm statistics command was last issued.

## Examples

The following is sample output from the **show pppatm redundancy** command:

```
Router# show pppatm redundancy
 4000 : Context Allocated events
 3999 : SSS Request events
 7998 : SSS Msg events
 3999 : PPP Msg events
 3998 : Up Pending events
 3998 : Up Dequeued events
 3998 : Processing Up events
 3999 : Vaccess Up events
 3999 : AAA unique id allocated events
 3999 : No AAA method list set events
 3999 : AAA gets nas port details events
 3999 : AAA gets retrived attrs events
 68202 : AAA gets dynamic attrs events
 3999 : Access IE allocated events
```

The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

*Table 15: show pppatm redundancy Field Descriptions*

| Field | Description |
|---|---|
| SSS request events | Subscriber service switch (SSS) requests. |
| SSS Msg events | SSS responses |
| PPP Msg events | PPP responses. |

| Field | Description |
|---|---|
| Up Pending events | ATM VC notification of events in queue. |
| Up dequeued events | ATM VC notification of events removed from queue. |
| Processing Up events | PPPoA events processed. |
| Vaccess Up events | Number of events for which the virtual access interface state changed to up. |
| AAA unique id allocated events | Number of events for which a unique AAA ID was allocated. |
| No AAA method list set events | Number of events for which no AAA accounting list was configured. |
| AAA get NAS port details events | Number of NAS port events. |
| AAA gets retrieved attrs events | Number of AAA retrieved attributes events for incoming and outgoing packets. |
| AAA gets dynamic attrs events | Number of AAA dynamic attributes events for start/stop packets. |
| Access IE allocated events | Number of IE (internal ID) allocated events. |

## Related Commands

| Command | Description |
|---|---|
| **show pppatm statistics** | Displays PPP ATM statistics. |
| **show pppoe redundancy** | Displays PPPoE events and statistics. |

# show pppatm session

To display information on PPP over ATM (PPPoA) sessions, use the **show pppatm session** command in privileged EXEC mode.

**show pppatm session**[{**interface atm** *interface-number.sub-interface number*}]

## Syntax Description

| | |
|---|---|
| **interface atm** | (Optional) Configures an ATM interface. |
| *interface-number.subinterface-number* | Interface number and possibly a subinterface number. A period (.) must precede the optional subinterface number. |

## Command Default

If no keywords or arguments are provided, information for all PPPoA sessions is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

This command is used for obtaining detailed information on PPPoA sessions, and the interfaces on which they are running.

If a subinterface number is given in the command, the output is a report of the PPPoA sessions in the subinterface. If a main interface number is given, the output has the report for each individual subinterface of that main interface. If no interface is given, the output contains the report for each ATM interface on the router.

## Examples

The following example shows how to display information for PPPoA sessions on ATM interface 8/0/0.12345678:

```
Router# show pppatm session atm8/0/0.12345678
     1 session  in LCP_NEGOTIATION (LCP) State
     1 session  total
Uniq ID  ATM-Intf       VPI/VCI   Encap   VT  VA         VA-st  State
```

8001 8/0/0.12345678 0/32035 SNAP 10 N/A N/A LCP

The table below describes the significant fields shown in the display.

***Table 16: show pppatm session Field Descriptions***

| Field | Description |
|---|---|
| Uniq ID | Unique identifier for the PPPoA session. |
| ATM-Intf | The ATM interface port number. |

| Field | Description |
|---|---|
| VPI | Virtual path identifier of the permanent virtual circuit (PVC). |
| VCI | Virtual channel identifier of the PVC. |
| Encap | Number of times PPP encapsulation occurred. |
| VT | Virtual template number used by the session. |
| VA | Virtual access interface number. |
| VA-st | Virtual access interface state. |
| State | PPPoA state of the session. |

## Related Commands

| Command | Description |
|---|---|
| **show pppatm summary** | Displays PPPoA session counts |

# show pppatm statistics

To display PPP over ATM (PPPoA) statistics, use the **show pppatm statistics** command in privileged EXEC mode.

**show pppatm statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |

## Usage Guidelines

Use the **show pppatm statistics**command to display statistics for PPPoA sessions. This command gives a total count of PPPoA events since the **clear pppatm statistics** command was last issued.

## Examples

The following is sample output from the **show pppatm statistics** command:

```
Router# show pppatm statistics
 4000 : Context Allocated events
 3999 : SSS Request events
 7998 : SSS Msg events
 3999 : PPP Msg events
 3998 : Up Pending events
 3998 : Up Dequeued events
 3998 : Processing Up events
 3999 : Vaccess Up events
 3999 : AAA unique id allocated events
 3999 : No AAA method list set events
 3999 : AAA gets nas port details events
 3999 : AAA gets retrived attrs events
 68202 : AAA gets dynamic attrs events
 3999 : Access IE allocated events
```

The table below describes the significant fields shown in the display.

*Table 17: show pppatm statistics Field Descriptions*

| Field | Description |
|---|---|
| Context Allocated events | Number of PPPoA events for which a context has been allocated. |
| SSS Request events | Subscriber service switch (SSS) requests. |
| SSS Msg events | SSS responses. |
| PPP Msg events | PPP responses. |

| Field | Description |
|---|---|
| Up Pending events | ATM VC notification of events in queue. |
| Up Dequeued events | ATM VC notification of events removed from queue. |
| Processing Up events | PPPoA events processed. |
| Vaccess Up events | Number of events for which the virtual access interface state changed to up. |
| AAA unique id allocated events | Number of events for which a unique authentication, authorization, and accounting (AAA) ID was allocated. |
| No AAA method list set events | Number of events for which no AAA accounting list was configured. |
| AAA get nas port details events | Number of network accesss server (NAS) port events. |
| AAA gets retrieved attrs events | Number of AAA retrieved attributes events for incoming and outgoing packets. |
| AAA gets dynamic attrs events | Number of AAA dynamic attributes events for start/stop packets. |
| Access IE allocated events | Number of IE (internal ID) allocated events. |

## Related Commands

| Command | Description |
|---|---|
| **clear pppatm statistics** | Clears PPP ATM statistics. |

# show pppatm summary

To display PPP over ATM (PPPoA) session counts, use the **show pppatm summary** command in privileged EXEC mode.

**show pppatm summary** [**interface atm** *interface-number* [. *subinterface-number*]]

## Syntax Description

| | |
|---|---|
| **interface atm** *interface-number* **.** *subinterface-number* | (Optional) Specifies a particular ATM interface by interface number and possibly a subinterface number. A period (**.**) must precede the optional subinterface number. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

This command is useful for obtaining session counts, the state of the PPPoA sessions, and the interfaces on which they are running.

This command gives a summary of the number of PPPoA sessions in each state and the session information of each individual session. If a subinterface number is given in the command, the output is a summary report of the PPPoA sessions in the subinterface. If a main interface number is given, the output will have the summary reports for each individual subinterface of that main interface as shown in the Examples section. If no interface is given, the output will contain the summary reports for each ATM interface on the router.

## Examples

The following example displays PPPoA session counts and states for ATM interface 5/0:

```
Router# show pppatm summary interface atm 5/0
ATM5/0.3:
       0 sessions total
ATM5/0.6:
       1 in PTA (PTA) State
       1 sessions total
VPI     VCI     Conn ID         PPPoA ID        SSS ID          PPP ID        AAA ID   VT
     VA/SID  State
  6     101       11            DA000009       BB000013       E5000017        C        1
     1.1     PTA
```

Most of the fields displayed by the **show pppatm summary** command are self-explanatory. The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

*Table 18: show pppatm summary Field Descriptions*

| Field | Description |
|---|---|
| VPI | Virtual path identifier of the permanent virtual circuit (PVC). |

| Field | Description |
|---|---|
| VCI | Virtual channel identifier of the PVC. |
| Conn ID | Unique connection identifier for the PPPoA session. This ID can be correlated with the unique ID in the **show vpdn session** command output for the forwarded sessions. |
| PPPoA ID | Internal identifier for the PPPoA session. |
| SSS ID | Internal identifier in the Subscriber Service Switch. |
| PPP ID | Internal identifier in PPP. |
| AAA ID | Authentication, authorization, and accounting (AAA) unique identifier for accounting records. |
| VT | Virtual template number used by the session. |
| VA/SID | PPPoA virtual access number for PPP Termination Aggregation (PTA) sessions, and switch identifier for forwarded sessions. |
| State | PPPoA state of the session. |

## Related Commands

| Command | Description |
|---|---|
| **clear pppatm interface atm** | Clears PPP ATM sessions on an ATM interface. |
| **debug pppatm** | Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC. |
| **show pppatm trace** | Displays a sequence of PPPoA events, errors, and state changes when the **debug pppatm** command is enabled. |

# show pppoe intermediate-agent info

To display PPPoE Intermediate Agent configuration, use the **show pppoe intermediate-agent info** command in user EXEC or privileged EXEC mode.

**show ppoe intermediate-agent info interface** *interface*

## Syntax Description

| | |
|---|---|
| **interface** *interface* | Interface for which information is displayed. |

## Command Default

This command has no default settings.

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| IOS XE 3.12 | This command was implemented on Cisco ME 2600X switches. |

## Examples

The following is sample output from the **show pppoe intermediate-agent info** command:

```
Router# show pppoe intermediate-agent info
PPPoE Intermediate-Agent is enabled
Global access-node-id is default
Global generic error msg is not set
Global identifier-string and delimiter are not set
PPPoE Intermediate-Agent trust/rate is configured on the following
Interfaces:
Interface IA Trusted Vsa Strip Rate limit (pps)
----------------------- -------- ------- --------- ----------------
GigabitEthernet0/33 yes no no unlimited
PPPoE Intermediate-Agent is configured on following bridge domains:
40,50
```

The following is sample output from the **show pppoe intermediate-agent information interface** *interface* command:

```
Router# show pppoe intermediate-agent info interface GigabitEthernet 0/10
Interface IA Trusted Vsa Strip Rate limit (pps)
----------------------- -------- ------- --------- ----------------
Gi 0/33 yes no no unlimited
PPPoE Intermediate-Agent is configured on following bridge domains:
40,50
```

## Related Commands

| Command | Description |
|---|---|
| **show pppoe intermediate-agent statistics** | Displays the number of packet received for all PPPoE discovery packets (PADI,PADO,PADR,PADS,PADT) on all interfaces (per-port and per-port-per-EFP). |

| Command | Description |
|---|---|
| **clear pppoe intermediate-agent statistics** | Clears packet counters for all PPPoE discovery packets (PADI,PADO,PADR,PADS,PADT) on all interfaces (per-port and per-port-per-EFP). |

# show pppoe intermediate-agent statistics

To display PPPoE Intermediate Agent statistics (packet counters), use the **show pppoe intermediate-agent statistics** command in user EXEC or privileged EXEC mode.

**show ppoe intermediate-agent statistics interface** *interface*

## Syntax Description

| | |
|---|---|
| **interface** *interface* | Interface for which statistics is displayed. |

## Command Default

This command has no default settings.

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| IOS XE 3.12 | This command was implemented on Cisco ME 2600X switches. |

## Examples

The following is sample output from the **show pppoe intermediate-agent statistics** command:

```
Router# show pppoe intermediate-agent statistics
PPPOE IA Per-Port Statistics
---- -----------------
Interface : GigabitEthernet0/33
Packets received
All = 53
PADI = 17 PADO = 0
PADR = 17 PADS = 0
PADT = 19
Packets dropped:
Rate-limit exceeded = 0
Server responses from untrusted ports = 0
Client requests towards untrusted ports = 0
Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 8 PADO = 0 PADR = 8 PADS = 0 PADT = 9
BD 50: Packets received PADI = 9 PADO = 0 PADR = 9 PADS = 0 PADT = 10
```

The following is sample output from the **show pppoe intermediate-agent statistics interface** *interface* command:

```
Router# show pppoe intermediate-agent statistics interface GigabitEthernet 0/10
Interface : Gi 0/10
Packets received
All = 3
PADI = 0 PADO = 0
PADR = 0 PADS = 0
PADT = 3
Packets dropped:
Rate-limit exceeded = 0
Server responses from untrusted ports = 0
Client requests towards untrusted ports = 0
Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 6 PADO = 0 PADR = 6 PADS = 0 PADT = 6
```

## Related Commands

| Command | Description |
|---|---|
| **show pppoe intermediate-agent info** | Displays all the interfaces and VLANs on which PPPoE is configured. |

# show ppp atm trace

To display a sequence of PPP over ATM (PPPoA) events, errors, and state changes when the **debug pppatm** command is enabled, use the **show pppatm trace** command in privileged EXEC mode.

**show pppatm trace** [{**error** | **event** | **state**}] **interface atm** *interface-number* [{[.*subinterface-number*]}] **vc** {[*vpi*]/ *vci* | **virtual-circuit-name**}

## Syntax Description

| | |
|---|---|
| **error** | (Optional) PPPoA events. |
| **event** | (Optional) PPPoA errors. |
| **state** | (Optional) PPPoA state. |
| **interface atm** *interface-number* | Specifies a particular ATM interface by interface number. |
| **.** *subinterface-number* | (Optional) Specifies a subinterface number preceded by a period. |
| **show pppatm trace** [{**error** \| **event** \| **state**}] **interface atm** *interface-number* [{[.*subinterface-number*]}] **vc** {[*vpi*]/ *vci* \| **virtual-circuit-name**}<br>**vc** *vpi* / *vci* | Virtual circuit (VC) keyword followed by a virtual path identifier (VPI) and virtual channel identifier (VCI). The absence of the "/" and a *vpi* causes the *vpi* value to default to 0. |
| *virtual-circuit-name* | Name of the VC. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

When the **debug pppatm** command has been enabled, this command displays messages from the specified permanent virtual circuit (PVC). If only one **debug pppatm** command keyword is supplied in the command, the report will display only the sequence of events for that particular debug type.

## Examples

The following example traces the debugging messages supplied by the **debug pppatm** command on PVC 101. The report is used by Cisco technical personnel for diagnosing system problems.

```
Router# debug pppatm trace interface atm 1/0.10 vc 101
Router# debug pppatm state interface atm 1/0.10 vc 101
Router# debug pppatm event interface atm 1/0.10 vc 101
Router# show pppatm trace interface atm 1/0.10 vc 101
Event = Disconnecting
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = SSS Cleanup
State = DOWN
Event = Up Pending
Event = Up Dequeued
Event = Processing Up
Event = Access IE allocated
Event = Set Pkts to SSS
Event = AAA gets retrieved attrs
Event = AAA gets nas port details
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = AAA unique id allocated
Event = No AAA method list set
Event = SSS Request
State = NAS_PORT_POLICY_INQUIRY
Event = SSS Msg
State = PPP_START
Event = PPP Msg
State = LCP_NEGOTIATION
Event = PPP Msg
Event = Access IE get nas port
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = PPP Msg
Event = Set Pkts to SSS
State = FORWARDED
```

## Related Commands

| Command | Description |
|---|---|
| **clear pppatm interface atm** | Clears PPP ATM sessions on an ATM interface. |
| **debug pppatm** | Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC. |
| **show pppatm summary** | Displays PPPoA session counts. |

# show pppoe debug conditions

To display PPP over Ethernet (PPPoE) debug information, use the **show pppoe debug conditions** command in user EXEC or privileged EXEC mode.

**show pppoe debug conditions**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Examples

The following is sample output from the **show pppoe debug conditions** command. The fields in the display are self-explanatory.

```
Router# show pppoe debug conditions
PPPoE global debugs: packet
AT6/0 debugs: event, error
AT6/0, VC 1/100 debugs: data
```

## Related Commands

| Command | Description |
|---|---|
| **clear pppoe** | Clears PPPoE sessions. |
| **debug pppoe** | Displays debugging information for PPPoE sessions. |
| **show pppoe session** | Displays information about currently active PPPoE sessions. |

# show pppoe derived

To display the cached PPP over Ethernet (PPPoE) configuration that is derived from the subscriber profile for a specified PPPoE profile, use the **show pppoe derived** command in privileged EXEC mode.

**show pppoe derived group** *group-name*

## Syntax Description

| | |
|---|---|
| **group** *group-name* | PPPoE profile for which the cached PPPoE configuration will be displayed. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |

## Usage Guidelines

A subscriber profile can be configured locally on the router or remotely on a AAA server. The PPPoE configuration that is derived from a subscriber profile is cached locally under the PPPoE profile. Use the **show pppoe derived**command to display the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.

A subscriber profile contains a list of PPPoE service names. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. A subscriber profile is assigned to a PPPoE profile by using the **service profile** command in BBA group configuration mode.

## Examples

The following example shows the PPPoE configuration for PPPoE profile "sp_group_a" that is derived from subscriber profile "abc". The services "isp_xyz", "isp_aaa", and "isp_bbb" will be advertised to each PPPoE client connection that uses PPPoE profile "sp_group_a".

```
Router# show pppoe derived group sp_group_a
Derived configuration from subscriber profile 'abc':
Service names:
   isp_xyz, isp_aaa, isp_bbb
```

## Related Commands

| Command | Description |
|---|---|
| **clear pppoe derived** | Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile. |
| **pppoe service** | Adds a PPPoE service name to a local subscriber profile. |
| **service profile** | Assigns a subscriber profile to a PPPoE profile. |
| **subscriber profile** | Defines Subscriber Service Switch policy for searches of a subscriber profile database. |

# show pppoe redundancy

To display PPP over Ethernet (PPPoE) redundancy events and statistics, use the **show pppoe redundancy** command in privileged EXEC mode.

**show pppoe redundancy**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |

## Usage Guidelines

This command is useful for obtaining statistics and redundancy events for PPPoE sessions such as recreating UP and DOWN states, and number of sessions waiting for an ATM virtual circuit to turn active. This command gives a cumulative count of PPPoE redundancy queue events and statistics, and an incremental count of PPPoE redundancy queue events and statistics since the last time the clear pppoe redundancy command was issued.

The **show pppoe redundancy** command does not show any output on an active Route Processor but shows output only on a standby Route Processor.

## Examples

The following is sample output for the show pppoe redundancy command:

### On Active Route Processor

```
Router# show pppoe redundancy

11 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
Router#
```

### On Standby Route Processor

```
Router-stby# show pppoe redundancy
13 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 9 PPPoE CCM EV     0   36        1524      1525        1          0        20
 Event Names
                           Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1* 9 Recreate UP           32000        0       36        0        93      2000
 2* 9 Recreate DOWN             0        0        0        0         0         0
 3* 9 VC Wait UP                0        0        0        0         0         0
 4* 9 VC Wait Encap             0        0        0        0         0         0
Sessions waiting for Base Vaccess: 0
Sessions waiting for ATM VC UP:    0
Sessions waiting for Auto VC Encap 0
```

The table below describes the significant fields in the sample output.

*Table 19: show pppoe redundancy Field Descriptions*

| Field | Description |
|---|---|
| size | |
| max | |
| kicks | |
| starts | |
| false | |
| suspends | |
| ticks | |
| Events | |
| Queued | |
| MaxQueued | |
| Suspends | |
| usec/evt | |
| max/evt | |

## Related Commands

| Command | Description |
|---|---|
| **show pppoe statistics** | Displays PPPoE statistics. |

# show pppoe relay context all

To display PPP over Ethernet (PPPoE) relay contexts created for relaying PPPoE Active Discovery (PAD) messages, use the **show pppoe relay context all** command in privileged EXEC mode.

**show pppoe relay context all**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

Use this command to display relay contexts created for relaying PAD messages.

## Examples

The following is sample output from the **show pppoe relay context all** command:

```
Router# show pppoe relay context all
Total PPPoE relay contexts 1
UID    ID     Subscriber-profile      State
25     18     Profile-1               RELAYED
```

The table below describes the significant fields shown in the show pppoe relay context all command output.

*Table 20: show pppoe relay context all Field Descriptions*

| Field | Description |
|---|---|
| Total PPPoE relay contexts | PPPoE relay contexts created for relaying PAD messages. |
| UID | Unique identifier for the relay context. |
| ID | PPPoE session identifier for the relay context. |
| Subscriber-profile | Name of the subscriber profile that is used by the PPPoE group associated with the relay context. |
| State | Shows the state of the relay context, which will be one of the following:<br>• INVALID--Not valid.<br>• RELFWD--PPPoE relay context was forwarded.<br>• REQ_RELAY--Relay has been requested. |

### Related Commands

| Command | Description |
|---|---|
| **clear pppoe relay context** | Clears PPPoE relay contexts created by PAD messages. |
| **show pppoe session** | Displays information about currently active PPPoE sessions. |

# show pppoe session

To display information about currently active PPP over Ethernet (PPPoE) sessions, use the **show pppoe session** in privileged EXEC mode.

**show pppoe session** [{**all** | **interface** *type number* | **packets** [{**all** | **interface** *type number* | **ipv6** }]}]

## Syntax Description

| | |
|---|---|
| *all* | (Optional) Displays detailed information about the PPPoE session. |
| **interface** *type number* | (Optional) Displays information about the interface on which the PPPoE session is active. |
| **packets** | (Optional) Displays packet statistics for the PPPoE session. |
| **ipv6** | (Optional) Displays PPPoE session packet statistics for IPv6 traffic |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)YG | This command was introduced on the Cisco SOHO 76, 77, and 77H routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for the Cisco 7200, 7301, 7600, and 10000 series platforms. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 and the output following the use of the **all** keyword was modified to indicate if a session is Interworking Functionality (IWF)-specific or if the **tag ppp-max-payload** tag is in the discovery frame and accepted. |
| 12.4(15)XF | The output was modified to display Virtual Multipoint Interface (VMI) and PPPoE process-level values. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Ad Hoc Router-to-Radio Networks (MANETs). |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 2.5 | This command was implemented on Cisco ASR 1000 series routers. |
| Cisco IOS XE Release 3.5S | This command was modified. The **ipv6** keyword was added. |

### Single Session: Example

The following is sample output from the show pppoe session command:

```
Router# show pppoe session
     1 session  in FORWARDED (FWDED) State
     1 session  total
```

| Uniq ID | PPPoE SID | RemMAC | Port | VT | VA | State | LocMAC | VA-st |
|---|---|---|---|---|---|---|---|---|
| 26 | 19 | 0001.96da.a2c0 | Et0/0.1 | 5 | N/A | RELFWD | 000c.8670.1006 | VLAN:3434 |

## PPPoE Session with IWF and ppp-max-payload Tag Example

The following is sample output from the **show pppoe session** command when there is an IWF session and the ppp-max-payload tag is accepted in the discovery frame (available in Cisco IOS Release 12.2(31)SB2):

```
Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total.  1 session of it is IWF type
```

| Uniq ID | PPPoE SID | RemMAC | Port | VT | VA | State | LocMAC | VA-st | Type |
|---|---|---|---|---|---|---|---|---|---|
| 26 | 21 | 0001.c9f2.a81e | Et1/2 | 1 | Vi2.1 | PTA | 0006.52a4.901e | UP | IWF |

The table below describes the significant fields shown in the displays.

*Table 21: show pppoe session Field Descriptions*

| Field | Description |
|---|---|
| Uniq ID | Unique identifier for the PPPoE session. |
| PPPoE SID | PPPoE session identifier. |
| RemMAC | Remote MAC address. |
| Port | Port type and number. |
| VT | Virtual-template interface. |
| VA | Virtual access interface. |

| Field | Description |
|---|---|
| State | Displays the state of the session, which will be one of the following:<br>• FORWARDED<br>• FORWARDING<br>• LCP_NEGOTIATION<br>• LOCALLY_TERMINATED<br>• PPP_START<br>• PTA<br>• RELFWD (a PPPoE session was forwarded for which the Active discovery messages were relayed)<br>• SHUTTING_DOWN<br>• VACCESS_REQUESTED |
| LocMAC | Local MAC address. |

### show pppoe session all: Example

The following example shows information per session for the **show pppoe session all** command.

```
Router# show pppoe session all

Total PPPoE sessions 1
session id: 21
local MAC address: 0006.52a4.901e, remote MAC address: 0001.c9f2.a81e
virtual access interface: Vi2.1, outgoing interface: Et1/2, IWF
PPP-Max-Payload tag: 1500
    15942 packets sent, 15924 received
    224561 bytes sent, 222948 received
```

### PPPoE Session Including Credit Flow Statistics: Example

The following example shows the output from the **show pppoe session all** command. This version of the display includes PPPoE credit flow statistics for the session.

```
Router# show pppoe session all
Total PPPoE sessions 1
session id: 1
local MAC address: aabb.cc00.0100, remote MAC address: aabb.cc00.0200
virtual access interface: Vi2, outgoing interface: Et0/0
17 packets sent, 24 received
1459 bytes sent, 2561 received
PPPoE Flow Control Stats
Local Credits: 65504 Peer Credits: 65478
Credit Grant Threshold: 28000 Max Credits per grant: 65534
PADG Seq Num: 7 PADG Timer index: 0
PADG last rcvd Seq Num: 7
PADG last nonzero Seq Num: 0
PADG last nonzero rcvd amount: 0
PADG Timers: [0]-1000 [1]-2000 [2]-3000 [3]-4000
PADG xmit: 7 rcvd: 7
PADC xmit: 7 rcvd: 7
PADQ xmit: 0 rcvd: 0
```

### show pppoe session packet ipv6: Example

The following is sample output form the **show pppoe session packet ipv6** command. The output field descriptions are self-explanatory.

```
Device# show pppoe session packet ipv6

SID     Pkts -In         Pkts-Out        Bytes-In        Bytes-Out
1       2800            9               2721600         770
```

## Related Commands

| Command | Description |
|---|---|
| **clear pppoe relay context** | Clears PPPoE relay contexts created for relaying PAD messages. |
| **show pppoe relay context all** | Displays PPPoE relay contexts created for relaying PAD messages. |

# show pppoe statistics

To display PPP over Ethernet (PPPoE) events and statistics, use the **show pppoe statistics** command in privileged EXEC mode.

**show pppoe statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

This command is useful for obtaining statistics and events for PPPoE sessions. Use the show pppoe statistics command to display a cumulative count of PPPoE events and statistics, and to display an incremental count since the last time the clear pppoe statistics command was issued.

## Examples

The following is sample output from the show pppoe statistics command:

```
Router# show pppoe statistics
PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              16002         16002
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  16002         16002
SSS DISCONNECT                 0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           16002         16002
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                16002         16002
SSM UPDATED                    16002         16002
SSM DISCONNECT                 0             0
>
PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    16002         16002
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        16002         16002
PPPoE Handles Freed            0             0
Dynamic Bind Request           16002         16002
Static Bind Request            16002         16002
```

The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

*Table 22: show pppoe statistics Field Descriptions*

| Field | Description |
|---|---|
| INVALID | Errors in the segment handling state machine; this field typically displays a zero. |
| PRE-SERVICE FOUND | Number of occurrences of PPPoE service policy having been located and configuration data having been read from the external server to the bba-group profile. |
| PRE-SERVICE NONE | Number of failures of PPPoE service policy profile configuration read from the external server. |
| SSS CONNECT LOCAL | Subscriber service switch (SSS) connections that received loca l termination directives. |
| SSS FORWARDING | SSS connections that received forwarding notification. |
| SSS FORWARDED | SSS connections that received forwarded notification. |
| SSS MORE KEYS | PPPoE sessions that are in the intermediate state, processing service keys, before a session is forwarded or terminated locally. |
| SSS DISCONNECT | PPPoE sessions disconnected after receiving a disconnect notification from the subscriber service switch. |
| CONFIG UPDATE | PPPoE sessions receiving serving policy configuration updates. |
| STATIC BIND RESPONSE | Number of responses that the interface is bound to the PPP session. |
| PPP FORWARDING | Number of PPPoE sessions in the forwarding state. |
| PPP FORWARDED | Number of forwarded PPPoE sessions. |
| PPP DISCONNECT | PPPoE sessions disconnected after receiving a disconnect message from the state machine. |
| PPP RENEGOTIATION | PPPoE sessions renegotiated after receiving a renegotiation message from the state machine. |
| SSM PROVISIONED | Segment switching manager (SSM) response that the dataplane has been initialized. |
| SSM UPDATED | SSM response that the dataplane has been successfully updated. |
| SSM DISCONNECT | Dataplane disconnects from PPPoE sessions. |
| SSS Request | SSS requests to determine if a call is to be forwarded or locally terminated. |
| SSS Response Stale | SSS responses received for sessions that are already freed. |
| SSS Disconnect | SSS disconnect messages to PPPoE sessions. |

| Field | Description |
|---|---|
| PPPoE Handles Allocated | Handles assigned for PPPoE sessions. |
| PPPoE Handles Freed | Handles freed for PPPoE sessions. |
| Dynamic Bind Request | PPPoE requests to start PPP sessions. |
| Static Bind Request | PPPoE requests to bind interfaces to PPP sessions. |

## Related Commands

| Command | Description |
|---|---|
| **clear pppoe statistics** | Clears PPPoE statistics. |

# show pppoe summary

To display a summary of the currently active PPP over Ethernet (PPPoE) sessions per interface, use the **show pppoe summary** command in user EXEC or privileged EXEC mode.

**show pppoe summary** [**per subinterface**]

## Syntax Description

| | |
|---|---|
| **per subinterface** | (Optional) Displays the PPPoE sessions per subinterface. |

## Command Default

If no argument is specified, information for all PPPoE sessions is displayed.

## Command Modes

User EXEC (>)
Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Examples

The following is sample output from the **show pppoe summary** command:

```
Router# show pppoe summary
PTA   Locally terminated sessions
    FWDED Forwarded sessions
    TRANS All other sessions (in transient state)
                    TOTAL     PTA   FWDED   TRANS
TOTAL                1762    1749      11       2
ATM2/0               1453    1443       8       2
ATM4/0                309     306       3       0
```

The table below describes the significant fields shown in the display.

*Table 23: show pppoe summary Field Descriptions*

| Field | Description |
|---|---|
| TOTAL | Total number of sessions. |
| PTA | Total number of PPP Terminated Aggregation (PTA) sessions. |
| FWDED | Total number of sessions that are forwarded. |
| TRANS | Total number of sessions transmitted. |

## Related Commands

| Command | Description |
|---|---|
| **clear pppoe** | Clears PPPoE sessions. |
| **debug pppoe** | Displays debugging information for PPPoE sessions. |
| **show pppoe session** | Displays information about currently active PPPoE sessions. |

# show pppoe throttled mac

To display information about MAC addresses from which PPP over Ethernet (PPPoE) sessions are throttled, that is, not currently accepted**, use the show pppoe throttled mac command**in privileged EXEC mode**.**

**show pppoe throttled mac**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB4A | This command was introduced. |
| 12.2(28)SB6 | This command was integrated into Cisco IOS Release 12.2(28)SB6. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |

## Usage Guidelines

PPPoE connection throttling limits the number of PPPoE session requests that can be made from a MAC address within a specified period of time. Use the show pppoe throttled mac command to display MAC addresses and ingress ports of users that exceed connection throttling limits configured using the sessions throttle command.

## Examples

The following is sample output from the show pppoe throttled mac command:

```
Router# show pppoe throttled mac
MAC(s) throttled
MAC              Ingress Port
00c1.00aa.006c          ATM1/0/0.101
007c.009e.0070          ATM1/0/0.101
0097.009d.007a          ATM1/0/0.101
008c.0077.0082          ATM1/0/0.101
00b5.00a8.009f          ATM1/0/0.101
00a4.0088.00b5          ATM1/0/0.101
```

The table below describes the significant fields shown in the display.

*Table 24: show pppoe throttled mac Field Descriptions*

| Field | Description |
|---|---|
| MAC | MAC address whose PPPoE session requests are limited. |
| Ingress Port | Interface port to which the MAC address attempted to set up a connection. |

## Related Commands

| Command | Description |
|---|---|
| **sessions throttle** | Configures PPPoE connection throttling in BBA-group configuration mode. |

# show sss circuits

**Note** Effective with Cisco IOS Release 15.0(1)S, the show sss circuits command is replaced by the **show subscriber circuits** command. See the **show subscriber circuits** command for more information.

To display Subscriber Service Switch (SSS) circuits information, use the **show sss circuits** command in privileged EXEC mode.

**show sss circuits**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(27)SBA | This command was integrated into Cisco IOS Release 12.2(27)SBA. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |
| 15.0(1)S | This command was replaced by the **show subscriber circuits** command. |

## Usage Guidelines

You can use the **show sss circuits** command to display detailed information about the subscriber switch circuits on the router. This command also displays encapsulation information that can be used for debugging.

## Examples

The following is sample output from the **show sss circuits** command:

```
Router# show sss circuits
Current Subscriber Circuit Information: Total number of circuits 1
Common Circuit ID 0            Serial Num 2          Switch ID 1671285332
---------------------------------------------------------------------------
   Status  Encapsulation
   UP flg  len dump
   Y  AES  18  00605C47 AF880060 2FBB3E88 8100000A 0800
   Y  AES  0
```

The table below describes the significant fields shown in the display.

*Table 25: show sss circuits Field Descriptions*

| Field | Description |
|---|---|
| Total number of circuits | Total number of SSS circuits. |
| Common Circuit ID | Common circuit ID for two or more SSS circuits. |
| Serial Num | Serial number of the SSS circuit. |
| Switch ID | SSS ID. |
| Status | Status of the flag. |
| Encapsulation | Type of the encapsulation used or configured. |
| AES | The Advanced Encryption Standard (AES). |

## Related Commands

| Command | Description |
|---|---|
| **show sss session** | Displays SSS session status. |

# show sss session

**Note** Effective with Cisco IOS Release 15.0(1)S, the **show sss session** command is replaced by the **show subscriber session** command. See the **show subscriber session** command for more information.

To display Subscriber Service Switch (SSS) session status, use the **show sss session** command in privileged EXEC mode.

**show sss session** [**all**]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Provides an extensive report about the SSS sessions. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 15.0(1)S | This command was replaced by the **show subscriber session** command. |

## Usage Guidelines

Use this command to verify the correct operation of PPP connections in the SSS environment.

The **show sss session** command reports only the current active SSS sessions. For example, an interface that is configured as an IP subscriber interface has an Intelligent Services Gateway (ISG) session running all the time. If the session cannot become active due to AAA failure(s), it is not listed in the report.

## Examples

The following sample output from the **show sss session** command provides a basic report of SSS session activity:

```
Router# show sss session
Current SSS Information: Total sessions 9
Uniq ID Type       State         Service      Identifier                        Last Chg
9       PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:02:36
10      PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:01:52
11      PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:01:52
3       PPPoE/PPP  connected     VPDN         user3@cisco.com          2d21h
6       PPPoE/PPP  connected     Local Term   user1                    00:03:35
7       PPPoE/PPP  connected     Local Term   user2                    00:03:35
8       PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:02:36
2       PPP        connected     Local Term   user5                    00:05:06
4       PPP        connected     VPDN         nobody2@cisco.com        00:06:52
```

The following sample output from the **show sss session all**command provides a more extensive report of SSS session activity:

```
Router# show sss session
```

```
 all
Current SSS Information: Total sessions 9
SSS session handle is 40000013, state is connected, service is VPDN
Unique ID is 9
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:49
Root SIP Handle is DF000010, PID is 49
AAA unique ID is 10
Current SIP options are Req Fwding/Req Fwded
SSS session handle is B0000017, state is connected, service is VPDN
Unique ID is 10
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:05
Root SIP Handle is B9000015, PID is 49
AAA unique ID is 11
Current SIP options are Req Fwding/Req Fwded
SSS session handle is D6000019, state is connected, service is VPDN
Unique ID is 11
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:13
Root SIP Handle is D0000016, PID is 49
AAA unique ID is 12
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 8C000003, state is connected, service is VPDN
Unique ID is 3
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user3@cisco.com
Last Changed 2d21h
Root SIP Handle is D3000002, PID is 49
AAA unique ID is 3
Current SIP options are Req Fwding/Req Fwded
SSS session handle is BE00000B, state is connected, service is Local Term
Unique ID is 6
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user1
Last Changed 00:03:56
Root SIP Handle is A9000009, PID is 49
AAA unique ID is 7
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DC00000D, state is connected, service is Local Term
Unique ID is 7
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user2
Last Changed 00:03:57
Root SIP Handle is 2C00000A, PID is 49
AAA unique ID is 8
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DB000011, state is connected, service is VPDN
Unique ID is 8
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:58
Root SIP Handle is 1000000F, PID is 49
AAA unique ID is 9
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 3F000007, state is connected, service is Local Term
Unique ID is 2
SIP subscriber access type(s) are PPP
Identifier is user5
Last Changed 00:05:30
Root SIP Handle is 8A000009, PID is 92
```

```
AAA unique ID is 1
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 97000005, state is connected, service is VPDN
Unique ID is 4
SIP subscriber access type(s) are PPP
Identifier is nobody2@cisco.com
Last Changed 00:07:16
Root SIP Handle is 32000000, PID is 92
AAA unique ID is 5
Current SIP options are Req Fwding/Req Fwded
```

Most of the fields displayed by the **show sss session** and **show sss session all**commands are self-explanatory. The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

*Table 26: show sss session Field Descriptions*

| Field | Description |
|---|---|
| Uniq ID | The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces. |
| Type | Access protocols relevant to this session. |
| State | Status of the connection, which can be one of the following states:<br>• connected--The session has been established.<br>• wait-for-req--Waiting for request.<br>• wait-for-auth--Waiting for authorization.<br>• wait-for-fwd--Waiting to be forwarded; for example, waiting for virtual private dialup network (VPDN) service. |
| Service | Type of service given to the user. |
| Identifier | A string identifying the user. This identifier may either be the username, or the name used to authorize the session. When **show sss session**command is used on the LNS, this identifier is optional and may not display the username, or the name used to authorize the session on LNS. |
| Last Chg | Time interval in hh:mm:ss format since the service for this session was last changed. |

## Related Commands

| Command | Description |
|---|---|
| **show vpdn session** | Displays session information about the L2TP and L2F protocols, and PPPoE tunnels in a VPDN. |

# show vpdn session

To display session information about active Layer 2 sessions for a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

**show vpdn session** [{**l2f** | **l2tp** | **pptp**}] [{**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]}]

## Syntax Description

| | |
|---|---|
| **l2f** | (Optional) Displays information about Layer 2 Forwarding (L2F) calls only. |
| **l2tp** | (Optional) Displays information about Layer 2 Tunneling Protocol (L2TP) calls only. |
| **pptp** | (Optional) Displays information about Point-to-Point Tunnel Protocol (PPTP) calls only. |
| **all** | (Optional) Displays extensive reports about active sessions. |
| **packets** | (Optional) Displays information about packet and byte counts for sessions. |
| **ipv6** | (Optional) Displays IPv6 packet and byte-count statistics. |
| **sequence** | (Optional) Displays sequence information for sessions. |
| **state** | (Optional) Displays state information for sessions. |
| *filter* | (Optional) One of the filter parameters defined in the table below. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.1(1)T | This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) session information. The **packets** and **all** keywords were added. |
| 12.1(2)T | This command was enhanced to display PPPoE session information on actual Ethernet interfaces. |
| 12.2(13)T | Reports from this command were enhanced with a unique identifier that can be used to correlate a particular session with the session information retrieved from other **show** commands or **debug** command traces. |
| 12.3(2)T | The **l2f**, **l2tp**, and the **pptp** keywords were added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.4(11)T | The **l2f** keyword was removed. |
| Cisco IOS XE Release 2.5 | This command was implemented on Cisco ASR 1000 series routers. |
| Cisco IOS XE Release 2.6 | The **ipv6** keyword was added. The **show vpdn session** command with the **all** and the **l2tp all** keywords was modified to display IPv6 counter information. |

## Usage Guidelines

Use the **show vpdn session** command to display information about all active sessions using L2TP, L2F, and PPTP.

The output of the **show vpdn session** command displays PPPoE session information as well. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Reports and options for this command depend upon the configuration in which it is used. Use the command-line question mark (?) help function to display options available with the **show vpdn session** command.

The table below defines the filter parameters available to refine the output of the **show vpdn session** command. You can use any one of the filter parameters in place of the *filter* argument.

*Table 27: Filter Parameters for the show vpdn session Command*

| Syntax | Description |
|---|---|
| **interface serial** *number* | Filters the output to display only information for sessions associated with the specified serial interface.<br>• *number* --The serial interface number. |
| **interface virtual-template** *number* | Filters the output to display only information for sessions associated with the specified virtual template.<br>• *number* --The virtual template number. |
| **tunnel id** *tunnel-id session-id* | Filters the output to display only information for sessions associated with the specified tunnel ID and session ID.<br>• *tunnel-id* --The local tunnel ID. The range is 1 to 65535.<br>• *session-id* --The local session ID. The range is 1 to 65535. |
| **tunnel remote-name** *remote-name local-name* | Filters the output to display only information for sessions associated with the tunnel with the specified names.<br>• *remote-name* --The remote tunnel name.<br>• *local-name* --The local tunnel name. |
| **username** *username* | Filters the output to display only information for sessions associated with the specified username.<br>• *username* --The username. |

The **show vpdn session** command provides reports on call activity for all active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session
L2TP Session Information Total tunnels 1 sessions 4
LocID RemID TunID Intf          Username             State    Last Chg Uniq ID
4     691   13695 Se0/0         nobody2@cisco.com        est    00:06:00  4
5     692   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  8
6     693   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  9
3     690   13695 SSS Circuit   nobody3@cisco.com        est    2d21h     3
```

```
L2F Session Information Total tunnels 1 sessions 2
 CLID   MID    Username                   Intf          State   Uniq ID
 1      2      nobody@cisco.com              SSS Circuit   open    10
 1      3      nobody@cisco.com              SSS Circuit   open    11
%No active PPTP tunnels
PPPoE Session Information Total tunnels 1 sessions 7
PPPoE Session Information
UID    SID    RemMAC         OIntf           Intf      Session
              LocMAC                         VASt      state
3      1      0030.949b.b4a0 Fa2/0           N/A       CNCT_FWDED
              0010.7b90.0840
6      2      0030.949b.b4a0 Fa2/0           Vi1.1     CNCT_PTA
              0010.7b90.0840                UP
7      3      0030.949b.b4a0 Fa2/0           Vi1.2     CNCT_PTA
              0010.7b90.0840                UP
8      4      0030.949b.b4a0 Fa2/0           N/A       CNCT_FWDED
              0010.7b90.0840
9      5      0030.949b.b4a0 Fa2/0           N/A       CNCT_FWDED
              0010.7b90.0840
10     6      0030.949b.b4a0 Fa2/0           N/A       CNCT_FWDED
              0010.7b90.0840
11     7      0030.949b.b4a0 Fa2/0           N/A       CNCT_FWDED
              0010.7b90.0840
```

The table below describes the significant fields shown in the **show vpdn session** display.

***Table 28: show vpdn session Field Descriptions***

| Field | Description |
|---|---|
| LocID | Local identifier. |
| RemID | Remote identifier. |
| TunID | Tunnel identifier. |
| Intf | Interface associated with the session. |
| Username | User domain name. |
| State | Status for the individual user in the tunnel; can be one of the following states:<br>• est<br>• opening<br>• open<br>• closing<br>• closed<br>• waiting_for_tunnel<br>The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state. |
| Last Chg | Time interval (in hh:mm:ss) since the last change occurred. |
| Uniq ID | The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces. |

| Field | Description |
|---|---|
| CLID | Number uniquely identifying the session. |
| MID | Number uniquely identifying this user in this tunnel. |
| UID | PPPoE user ID. |
| SID | PPPoE session ID. |
| RemMAC | Remote MAC address of the host. |
| LocMAC | Local MAC address of the router. It is the default MAC address of the router. |
| OIntf | Outgoing interface. |
| Intf VASt | Virtual access interface number and state. |
| Session state | PPPoE session state. |

The **show vpdn session packets** command provides reports on call activity for all the currently active sessions. The following output is from a device carrying an active PPPoE session:

```
Router# show vpdn session packets

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       202333          202337          2832652         2832716
```

The table below describes the significant fields shown in the **show vpdn session packets** command display.

*Table 29: show vpdn session packets Field Descriptions*

| Field | Description |
|---|---|
| SID | Session ID for the PPPoE session. |
| Pkts-In | Number of packets coming into this session. |
| Pkts-Out | Number of packets going out of this session. |
| Bytes-In | Number of bytes coming into this session. |
| Bytes-Out | Number of bytes going out of this session. |

The **show vpdn session all** command provides extensive reports on call activity for all the currently active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session all
L2TP Session Information Total tunnels 1 sessions 4
Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
```

```
    Internet address is 10.0.0.63
    Session state is established, time since change 00:03:53
      52 Packets sent, 52 received
      2080 Bytes sent, 1316 received
    Last clearing of "show vpdn" counters never
    Session MTU is 1464 bytes
    Session username is nobody@cisco.com
      Interface
      Remote session id is 692, remote tunnel id 58582
    UDP checksums are disabled
    SSS switching enabled
    No FS cached header information available
    Sequencing is off
    Unique ID is 8
  Session id 6 is up, tunnel id 13695
  Call serial number is 3355500003
  Remote tunnel name is User03
    Internet address is 10.0.0.63
    Session state is established, time since change 00:04:22
      52 Packets sent, 52 received
      2080 Bytes sent, 1316 received
    Last clearing of "show vpdn" counters never
    Session MTU is 1464 bytes
    Session username is nobody@cisco.com
      Interface
      Remote session id is 693, remote tunnel id 58582
    UDP checksums are disabled
    SSS switching enabled
    No FS cached header information available
    Sequencing is off
    Unique ID is 9
  Session id 3 is up, tunnel id 13695
  Call serial number is 3355500000
  Remote tunnel name is User03
    Internet address is 10.0.0.63
    Session state is established, time since change 2d21h
      48693 Packets sent, 48692 received
      1947720 Bytes sent, 1314568 received
    Last clearing of "show vpdn" counters never
    Session MTU is 1464 bytes
    Session username is nobody2@cisco.com
      Interface
      Remote session id is 690, remote tunnel id 58582
    UDP checksums are disabled
    SSS switching enabled
    No FS cached header information available
    Sequencing is off
    Unique ID is 3
  Session id 4 is up, tunnel id 13695
  Call serial number is 3355500001
  Remote tunnel name is User03
    Internet address is 10.0.0.63
    Session state is established, time since change 00:08:40
      109 Packets sent, 3 received
      1756 Bytes sent, 54 received
    Last clearing of "show vpdn" counters never
    Session MTU is 1464 bytes
    Session username is nobody@cisco.com
      Interface Se0/0
      Remote session id is 691, remote tunnel id 58582
    UDP checksums are disabled
    IDB switching enabled
    FS cached header information:
      encap size = 36 bytes
      4500001C BDDC0000 FF11E977 0A00003E
      0A00003F 06A506A5 00080000 0202E4D6
      02B30000
    Sequencing is off
    Unique ID is 4
  L2F Session Information Total tunnels 1 sessions 2
  MID: 2
  User:  nobody@cisco.com
  Interface:
  State:  open
  Packets out: 53
  Bytes out: 2264
  Packets in: 51
  Bytes in: 1274
  Unique ID: 10
    Last clearing of "show vpdn" counters never
  MID: 3
  User:  nobody@cisco.com
  Interface:
  State:  open
  Packets out: 53
  Bytes out: 2264
  Packets in: 51
  Bytes in: 1274
  Unique ID: 11

  Last clearing of "show vpdn" counters never
  %No active PPTP tunnels
  PPPoE Session Information Total tunnels 1 sessions 7
  PPPoE Session Information
  SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
  1       48696           48696           681765          1314657
  2       71              73              1019            1043
  3       71              73              1019            1043
  4       61              62              879             1567
  5       61              62              879             1567
  6       55              55              791             1363
  7       55              55              795             1363
```

The significant fields shown in the **show vpdn session all** command display are similar to those defined in the show vpdn session packets Field Descriptions and the show vpdn session Field Descriptions tables above.

## Related Commands

| Command | Description |
|---|---|
| **show sss session** | Displays Subscriber Service Switch session status. |
| **show vpdn** | Displays basic information about all active VPDN tunnels. |
| **show vpdn domain** | Displays all VPDN domains and DNIS groups configured on the NAS. |
| **show vpdn group** | Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information. |
| **show vpdn history failure** | Displays the content of the failure history table. |
| **show vpdn multilink** | Displays the multilink sessions authorized for all VPDN groups. |
| **show vpdn redirect** | Displays statistics for L2TP redirects and forwards. |

| Command | Description |
|---|---|
| **show vpdn tunnel** | Displays information about active Layer 2 tunnels for a VPDN. |

# shutdown (PVC range)

To deactivate a permanent virtual circuit (PVC) range, use the **shutdown** command in PVC range configuration mode. To reactivate a PVC range, use the **no** form of this command.

**shutdown**
**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Command Default

PVC range is active.

## Command Modes

PVC range configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Examples

In the following example, a PVC range called "range1" is deactivated:

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  shutdown
```

## Related Commands

| Command | Description |
|---|---|
| **range pvc** | Defines a range of ATM PVCs. |
| **show pppatm summary** | Deactivates an individual PVC within a PVC range. |

# shutdown (PVC-in-range)

To deactivate an individual permanent virtual circuit (PVC) within a PVC range, use the **shutdown** command in PVC-in-range configuration mode. To reactivate an individual PVC within PVC range, use the **no** form of this command.

**shutdown**
**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The PVC is active.

## Command Modes

PVC-in-range configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Examples

In the following example, "pvc1" within the PVC range called "range1" is deactivated:

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  pvc-in-range pvc1 7/104
   shutdown
```

## Related Commands

| Command | Description |
|---|---|
| **pvc-in-range** | Configures an individual PVC within a PVC range. |
| **shutdown (PVC range)** | Deactivates a PVC range. |

# subscriber access

To configure a network access server (NAS) to enable the Subscriber Service Switch (SSS) to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name, or to add the circuit-id key received in the point-to point protocol (PPP) over Ethernet (PPPoE) control message as a unique key to the database, use the **subscriber access**command in global configuration mode. To disable SSS preauthorization, use the **no** form of this command.

**subscriber access** {**pppoe** | **pppoa**} {**pre-authorize nas-port-id** [{**default***list-name*}] [**send username**] | **unique-key circuit-id** *circuit-id-key*}
**no subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id**

## Syntax Description

| | |
|---|---|
| **pppoe** | Specifies PPPoE. |
| **pppoa** | Specifies PPP over ATM (PPPoATM). |
| **pre-authorize nas-port-id** | Signals the SSS to preauthorize the NAS-Port-ID string before authorizing the domain name. |
| **default** | (Optional) Uses the default method list name instead of the named *list-name*argument. |
| *list-name* | (Optional) Authentication, authorization, and accounting (AAA) authorization configured on the Layer 2 Tunnel Protocol (L2TP) Access Concentrator (LAC). |
| **send username** | (Optional) Specifies to send the authentication username of the session in the Change_Info attribute (attribute 77). |
| **unique-key** | Sets up the unique key for the PPPoE subscriber. |
| **circuit-id** *circuit-id-key* | Specifies a unique subscriber circuit-id key. |

## Command Default

Preauthorization is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)B | This command was introduced on the Cisco 6400 series, the Cisco 7200 series, and the Cisco 7401 Application Specific Router (ASR). |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T, and the **pppoe**and **pppoa**keywords were added. |
| 12.4(2)T | The **send username** keywords were added. |
| 12.3(14)YM2 | This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers. |

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

The NAS-Port-ID string is used to locate the first service record, which may contain one of three attributes, as follows:

- A restricted set of values for the domain substring of the unauthenticated PPP name.

This filtered service key then locates the final service. See the **vpdn authorize domain**command for more information.

- PPPoE session limit.
- The logical line ID (LLID).

Once NAS port authorization has taken place, normal authorization, which is usually the domain authorization, continues.

### Logical Line ID

The LLID is an alphanumeric string of 1 to 253 characters that serves as the logical identification of a subscriber line. The LLID is maintained in a RADIUS server customer profile database and enables users to track their customers on the basis of the physical lines on which customer calls originate. Downloading the LLID is also referred to as "*preauthorization"* because it occurs before normal virtual private dialup network (VPDN) authorization downloads layer L2TP information.

The **subscriber access**command enables LLID and SSS querying only for PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN or Dot1Q) calls; all other calls, such as ISDN, are not supported.

### Per-NAS-Port Session Limits for PPPoE

Use the **subscriber access**command to configure the SSS preauthorization on the LAC so that the PPPoE per-NAS-port session limit can be downloaded from the customer profile database. To use PPPoE per-NAS-port session limits, you must also configure the PPPoE Session-Limit per NAS-Port Cisco attribute-value pair in the user profile.

## Examples

The following example signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to sessions that have a PPPoE access type.

```
aaa new-model
aaa group server radius sg-llid
 server 172.20.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg-group
 server 172.20.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg-group
aaa authorization network mlist_llid group sg-llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg-group password 0 lab
```

```
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol 12tp
 domain example.com
 initiate-to ip 10.1.1.1
 local name s7200-2
!
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist-llid
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.2.2.2 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
 pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.20.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.20.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

The following example is identical to the previous example except that it also adds support for sending the PPP authenticating username with the preauthorization in the Connect-Info attribute. This example also includes command-line interface (CLI) suppression on the LLID if the username that is used to authenticate has a domain that includes #184.

```
aaa new-model
aaa group server radius sg-llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg-group
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg-group
aaa authorization network mlist-llid group sg-llid
aaa session-id common
!
```

```
username s7200-2 password 0 lab
username s5300 password 0 lab
username sg-group password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example1.com
 domain example1.com#184
 initiate-to ip 10.1.1.1
 local name s7200-2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
 protocol pppoe
 virtual-template 1
!
subscriber access pppoe pre-authorize nas-port-id mlist-llid send username
!
```

## Related Commands

| Command | Description |
|---|---|
| **ip radius source-interface** | Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets. |
| **l2tp attribute clid mask-method** | Configures a NAS to provide L2TP calling line ID suppression for calls belonging to a VPDN group. |
| **subscriber authorization enable** | Enables SSS type authorization. |
| **vpdn authorize domain** | Enables domain preauthorization on a NAS. |
| **vpdn l2tp attribute clid mask-method** | Configures a NAS to provide L2TP calling line ID suppression globally on the router. |

# subscriber authorization enable

To enable Subscriber Service Switch type authorization, use the **subscriber authorization enable**command in global configuration mode. To disable the Subscriber Service Switch authorization, use the **no** form of this command.

**subscriber authorization enable**
**no subscriber authorization enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Authorization is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This feature was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

The **subscriber authorization enable** command triggers Subscriber Service Switch type authorization for local termination, even if virtual private dialup network (VPDN) and Stack Group Bidding Protocol (SGBP) are disabled.

## Examples

The following example enables Subscriber Service Switch type authorization:

```
subscriber authorization enable
```

## Related Commands

| Command | Description |
|---|---|
| **subscriber access** | Enables Subscriber Service Switch preauthorizationof a NAS port identifier (NAS-Port-ID) string before authorizing the domain name. |
| **vpdn authorize domain** | Enables domain preauthorization on a NAS. |

# subscriber profile

To define a Subscriber Service Switch (SSS) policy for searches of a subscriber profile database, use the **subscriber profile**command in global configuration mode. To change or disable the SSS policy, use the **no** form of this command.

**subscriber profile** *profile-name*
**no subscriber profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | A unique string, which can represent (but is not limited to) keys such as a domain, dialed number identification service (DNIS), port name, or PPP over Ethernet (PPPoE) service name. |

## Command Default

No default profile name

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This feature was introduced. |

## Usage Guidelines

This command is used to locally search the subscriber profile database for authorization data when an authentication, authorization, and accounting (AAA) network authorization method list is configured. Make sure that the **aaa authorization network default local** global configuration command is included in the configuration--do *not* use the **aaa authorization network default** command without the **local**keyword.

## Examples

The following example provides virtual private dialup network (VPDN) service to users in the domain cisco.com, and uses VPDN group group 1 to obtain VPDN configuration information:

```
!
subscriber profile cisco.com
 service vpdn group 1
```

The following example provides VPDN service to DNIS 1234567, and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile dnis:1234567
 service vpdn group 1
```

The following example provides VPDN service using a remote tunnel (used on the multihop node), and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile host:lac
 service vpdn group 1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization** | Sets parameters that restrict user access to a network. |
| **service deny** | Denies service for the SSS policy. |
| **service local** | Enables local termination service for the SSS policy. |
| **service relay** | Enables relay of PAD messages over an L2TP tunnel. |
| **service vpdn group** | Provides VPDN service for the SSS policy. |

# subscriber redundancy

To configure the broadband subscriber session redundancy policy for synchronization between High Availability (HA) active and standby processors, use the **subscriber redundancy** command in global configuration mode. To delete the policy, use the **no** form of this command.

**subscriber redundancy** {**bulk limit** {**cpu** *percent* **delay** *seconds* [**allow** *sessions*] | **time** *seconds*} | **dynamic limit** {**cpu** *percent* **delay** *seconds* | [**allow** *sessions*] | **periodic-update interval** [*minutes*]} | **delay** *seconds* | **rate** *sessions seconds* | **disable**}
**no subscriber redundancy** {**bulk limit** {**cpu** | **time**} | **dynamic limit** {**cpu** | **periodic-update interval** [*minutes*]} | **delay** | **rate** | **disable**}

## Syntax Description

| | |
|---|---|
| **bulk** | Configures a bulk synchronization redundancy policy. |
| **limit** | Specifies the synchronization limit. |
| **dynamic** | Configures a dynamic synchronization redundancy policy. |
| **cpu** *percent* | Specifies, in percent, the CPU busy threshold value. Range: 1 to 100. Default: 90. |
| **delay** *seconds* | Specifies the minimum time, in seconds, for a session to be ready before bulk or dynamic synchronization occurs. Range: 1 to 33550. |
| **allow** *sessions* | (Optional) Specifies the minimum number of sessions to synchronize when the CPU busy threshold is exceeded and the specified delay is met. Range: 1 to 2147483637. Default: 25. |
| **time** *seconds* | Specifies the maximum time, in seconds, for bulk synchronization to finish. Range: 1 to 3000. |
| **periodic-update interval** | Enables the periodic update of accounting statistics for subscriber sessions. |
| *minutes* | (Optional) Interval, in minutes, for the periodic update. Range: 10 to 1044. Default: 15. |
| **rate** *sessions seconds* | Specifies the number of sessions per time period for bulk and dynamic synchronization.<br>• *sessions*—Range: 1 to 32000. Default: 250.<br>• *seconds*—Range: 1 to 33550. Default: 1. |
| **disable** | Disables stateful switchover (SSO) for all subscriber sessions. |

## Command Default

The default subscriber redundancy policy is applied.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |
| Cisco IOS XE Release 3.5S | This command was modified. The **periodic-update interval** keyword and *minutes* argument were added. |
| 15.2(1)S | This command was modified. The **disable** keyword was added. |

## Usage Guidelines

Cisco IOS HA functionality for broadband protocols and applications allows for SSO and In-Service Software Upgrade (ISSU) features that minimize planned and unplanned downtime and failures. HA uses the cluster control manager (CCM) to manage the capability to synchronize subscriber session initiation on the standby processor of a redundant processor system.

- Use the **bulk** keyword to create and modify the redundancy policy used during bulk (startup) synchronization.
- Use the **dynamic** keyword with the **limit** keyword to tune subscriber redundancy policies that throttle dynamic synchronization by monitoring CPU usage and synchronization rates.
- Use the **delay** keyword to establish the minimum session duration for synchronization and to manage dynamic synchronization of short-duration calls.
- Use the **rate** keyword to throttle the number of sessions to be synchronized per period.
- Use the **dynamic** keyword with the **periodic-update interval** keyword to enable subscriber sessions to periodically synchronize their dynamic accounting statistics (counters) on the standby processor. The periodic update applies to new and existing subscriber sessions. All subscriber sessions do not synchronize their data at exactly the same time. Session synchronization is spread out based on the session creation time and other factors. This command is rejected if a previous instance of the command has not finished processing.
- Use the **disable** keyword to disable SSO for all subscriber sessions.

## Examples

The following example shows how to configure a 10-second delay when CPU usage exceeds 90 percent during bulk synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy bulk limit cpu 90 delay 10 allow 25
```

The following example shows how to configure a maximum time of 90 seconds for bulk synchronization to be completed:

```
Router(config)# subscriber redundancy bulk limit time 90
```

The following example shows how to configure a 15-second delay when CPU usage exceeds 90 percent during dynamic synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy dynamic limit cpu 90 delay 15 allow 25
```

The following example shows how to configure 2000 sessions to be synchronized per second during bulk and dynamic synchronization:

```
Router(config)# subscriber redundancy rate 2000 1
```

The following example shows how to configure a periodic update so that subscriber sessions synchronize their accounting statistics every 30 minutes:

```
Router(config)# subscriber redundancy dynamic periodic-update interval 30
```

The following example shows how to disable SSO for all subscriber sessions:

```
Router(config)# subscriber redundancy disable
```

## Related Commands

| Command | Description |
|---|---|
| **show ccm sessions** | Displays CCM session information. |
| **show pppatm statistics** | Displays PPPoA statistics. |
| **show pppoe statistics** | Displays PPPoE statistics. |
| **show ppp subscriber statistics** | Displays PPP subscriber statistics. |

# sw-module heap fp

To fine-tune the Multi-Processor Forwarding (MPF) heap memory allocation required for specific session scaling and application needs, use the **sw-module heap fp**command in global configuration mode. To return the setting to the default (32 MB), use the **no** form of the command.

**sw-module heap fp** [*megabytes*]
**no sw-module heap fp**

## Syntax Description

| | |
|---|---|
| *megabytes* | (Optional) The heap size in megabytes (MB) for the MPF processor. The default size is 32 MB. |

## Command Default

The default heap memory allocation size is 32 MB.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)YM2 | This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T. |

## Usage Guidelines

The default heap size is 32 MB if you do not specify otherwise. Once you have changed and saved the MPF heap memory configuration, reboot the router for the MPF memory size adjustment to take effect.

The following table lists the recommended heap memory size by type of deployment and number of sessions configured:

*Table 30: Recommended Heap Memory Sizes*

| Type of Deployment | Number of Sessions | Recommended Heap Size |
|---|---|---|
| PTA/LAC/LNS | 8000 and over | 80 MB |

## Examples

The following example sets or changes the MPF heap memory size in a router to 80 MB:

```
Router(config)# sw-module heap fp 80
```

## Related Commands

| Command | Description |
|---|---|
| **clear mpf interface** | Clears MPF packet counts on all physical interfaces. |
| **clear mpf punt** | Clears MPF per-box punt reason and count. |
| **ip mpf** | Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router. |
| **show ip cef exact-route** | Displays the exact route for a source-destination IP address pair in CEF. |

| Command | Description |
|---|---|
| **show mpf cpu** | Displays the average CPU utilization when MPF is enabled on the second CPU. |
| **show mpf interface** | Displays MPF packet count information on each physical interface. |
| show mpf ip exact-route | Displays the exact route for a source-destination IP address pair in an MPF system. |
| **show mpf punt** | Displays the MPF punt reason and punt packet count for the chassis. |

# tag ppp-max-payload

To establish a range for the PPP maximum payload to be accepted by the Broadband Remote Access Server (BRAS), use the **tag ppp-max-payload** command under a virtual template in BBA group configuration mode. To disable the effect of this command, use the **tag p pp-max-payload deny**command.

**tag ppp-max-payload** [**minimum** *octets* **maximum** *octets*] [**deny**]

## Syntax Description

| | |
|---|---|
| **minimum** | (Optional) Specifies a minimum number of octets. The default minimum value is 1492. |
| **maximum** | (Optional) Specifies a maximum number of octets. The default maximum value is 1500. |
| *octets* | (Optional) The minimum and maximum number (depending on which keyword precedes the value in the command syntax) of octets that can be accepted by the BRAS. |
| **deny** | (Optional) Disables the effect of any values previously entered with the **tag ppp-max-payload** command. |

## Command Default

The physical interface default maximum transmission unit (MTU) value is used.

## Command Modes

BBA group configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

The value of the ppp-max-payload tag accepted from a client cannot exceed the physical interface MTU minus 8 bytes (PPP over Ethernet [PPPoE] encapsulation plus PPP encapsulation). That is, the maximum accepted value of this tag from any client is limited to the minimum of physical interface MTU minus 8 and the maximum value configured by the **tag ppp-max-payload maximum** *value*.

This maximum value cap set under the BBA group can be critical to network operation because the physical interface default MTU can be extremely high (for example, 4470 octets for an ATM interface) and the BRAS administrator may not want to negotiate such a high maximum receive unit (MRU) for a session. The minimum value limitation is required to protect the BRAS against excessive fragmentation loads due to PPPoE clients negotiating too low a value for the MRU.

## Examples

The following example shows the PPP-Max-Payload and IWF PPPoE Tag Support feature enabled to accept ppp-max-payload tag values from 1492 to 1892, limits the number of sessions per MAC address to 2000 when the IWF is present, and verifies that the PPP session can accept 1500-byte packets in both directions:

```
bba-group pppoe global
 virtual-template 1
 sessions per-mac limit 1
 sessions per-mac iwf limit 2000
 tag ppp-max-payload minimum 1492 maximum 1892
```

```
interface Virtual-Template1
ppp lcp echo mru verify minimum 1500
```

## Related Commands

| Command | Description |
|---|---|
| **bba-group pppoe** | Enters BBA group configuration mode and defines a PPPoE profile. |

# test virtual-template subinterface

To determine if a virtual template can support the creation of subinterfaces, use the test virtual-template subinterface command in privileged EXEC mode.

**test virtual-template** *template* **subinterface**

## Syntax Description

| | |
|---|---|
| *template* | The identifying string of the virtual template to be tested. |

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(15)B | This command was integrated into Cisco IOS Release 12.2(15)B. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |

## Usage Guidelines

This command tests the specified virtual template to determine if it can support the creation of virtual access subinterfaces. If the virtual template cannot support subinterfaces, this command lists the commands that are configured on the virtual template and that are incompatible with subinterfaces.

## Examples

The following example tests virtual template 1 to determine if it can support subinterfaces. The output shows that the **traffic-shape rate** 50000 8000 8000 1000 command that is configured on virtual template 1 prevents the virtual template from being able to support subinterfaces.

```
Router# test virtual-template 1 subinterface
Subinterfaces cannot be created using Virtual-Template1
Interface specific commands:
traffic-shape rate 50000 8000 8000 1000
```

## Related Commands

| Command | Description |
|---|---|
| **debug vtemplate subinterface** | Displays debug messages relating to virtual access subinterfaces. |
| **virtual-template subinterface** | Enables the creation of virtual access subinterfaces. |

# vendor-tag circuit-id service

To enable processing of the PPPoE Vendor-Specific tag in a PPPoE Active Discovery Request (PADR) packet, which extracts the Circuit-Id part of the tag and sends it to a AAA server as the NAS-Port-Id attribute in RADIUS access requests, use the **vendor-tag circuit-id service**command in BBA group configuration mode. To disable the command function (default), use the **no** form of this command.

**vendor-tag circuit-id service**
**no vendor-tag circuit-id service**

## Syntax Description

This command has no argument or keywords.

## Command Default

This command is disabled.

## Command Modes

BBA group configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

When this command is not enabled and the Broadband Remote Access Server (BRAS) receives a packet with the Vendor-Specific tag attached, the tag is ignored and the session is allowed to come up. The Vendor-Specific tag is extracted and processed for its Circuit-Id part when the **vendor-tag circuit-id service** command is enabled in BBA group configuration mode. Once the command is configured, the BRAS processes incoming PADR packets and sends the Circuit-Id tag to the AAA server as a NAS-Port-Id RADIUS attribute.

## Examples

In the following example, outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Session-confirmation (PADS) packets are configured to retain the incoming Vendor-Specific Line-Id tag:

```
bba-group pppoe pppoe-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service

interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-tag
```

## Related Commands

| Command | Description |
|---|---|
| **vendor-tag circuit-id strip** | Removes an incoming Vendor-Specific Line-Id tag from outgoing PADO and PADR packets. |

# vendor-tag circuit-id strip

**Note** Effective with Cisco IOS Release 12.2(31)SB2, the **vendor-tag circuit-id strip** command is replaced by the **vendor-tag strip** command. See the **vendor-tag strip** command for more information.

To remove the incoming Vendor-Specific Line-ID tag from outgoing PPPoE Active Discovery Offer and Request (PADO and PADR) packets, use the **vendor-tag circuit-id strip**command in BBA group configuration mode. To disable the command function, use the **no** form of this command.

**vendor-tag circuit-id strip**
**no vendor-tag circuit-id strip**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command's functionality is disabled. In the default condition, outgoing packets from the Broadband Remote Access Server (BRAS) have a digital subscriber line access multiplexer (DSLAM) inserted Remote-ID tag when the **vendor-tag remote-id service** command is configured.

## Command Modes

BBA group configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(31)SB2 | This command was replaced by the **vendor-tag strip** command. |

## Usage Guidelines

Outgoing packets from the BRAS will have a digital subscriber line access multiplexer (DSLAM)-inserted Line-ID tag when the **vendor-tag circuit-id service** command is configured. The DSLAM must remove the tag from the PADO packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending out the packets. When the **vendor-tag circuit-id strip** command is configured, the BRAS removes the incoming Vendor-Specific Line-ID tag from the outgoing packets.

Outgoing PADO and PADS packets from the BRAS will have the DSLAM-inserted Circuit-ID tag. The DSLAM must remove the tag from PADO and PADS packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending the packets out, and this is accomplished using the **vendor-tag circuit-id strip** command.

## Examples

In the following example, the BRAS removes incoming Vendor-Specific Line-ID tags from outgoing PADO and PADS packets:

```
bba-group pppoe pppoe-rm-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service
 vendor-tag circuit-id strip
```

```
interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-tag
```

## Related Commands

| Command | Description |
|---|---|
| **vendor-tag circuit-id service** | Enables processing of the PPPoE Vendor-Specific tag in a PADR packet so the Circuit-ID part can be sent to a AAA server as the NAS-Port-ID attribute in RADIUS access requests. |

# vendor-tag remote-id service

To enable processing of the PPPoE Vendor-Specific tag in a PPPoE Active Discovery Request (PADR) packet, which extracts the Remote-ID part of the tag and sends it to an AAA server as the NAS-Port-ID attribute in RADIUS access requests, use the **vendor-tag remote-id service**command in BBA group configuration mode. To disable the command function, use the **no** form of this command.

**vendor-tag remote-id service**
**no vendor-tag remote-id service**

## Syntax Description

This command has no argument or keywords.

## Command Default

This command’s functionality is disabled. In this default condition, when the Broadband Remote Access Server (BRAS) receives a packet with the vendor-specific tag attached, the tag is ignored and the session is allowed to come up.

## Command Modes

BBA group configuration (config-bba-group)#

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. |
| Cisco IOS XE 2.3.0 | This command was integrated. This command is supported on ASR 1000 series. |

## Usage Guidelines

When this command is not enabled and the BRAS receives a packet with the Vendor-Specific tag attached, the tag is ignored and the session is allowed to come up. The Vendor-Specific tag is extracted and processed for its Remote-ID part when the **vendor-tag remote-id service** command is enabled in BBA group configuration mode. When the command is configured, the BRAS processes incoming PADR packets and sends the Remote-ID tag to the AAA server as a NAS-Port-ID RADIUS attribute.

## Examples

In the following example, outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Session-Confirmation (PADS) packets are configured to retain the incoming Vendor-Specific Line-ID tag:

```
Router(config-bba-group)# bba-group pppoe pppoe-tag
Router(config-bba-group)# sessions per-mac limit 50
Router(config-bba-group)# vendor-tag remote-id service

Router(config-bba-group)# interface FastEthernet0/0.1
Router(config-bba-group)# encapsulation dot1Q 120
Router(config-bba-group)# pppoe enable group pppoe-tag
```

## Related Commands

| Command | Description |
|---|---|
| **vendor-tag strip** | Removes an incoming Vendor-Specific Line-ID tag from outgoing PADO and PADR packets. |

# vendor-tag strip

To remove the incoming Vendor-Specific Line-ID tag from outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Request (PADR) packets, use the **vendor-tag strip**command in BBA group configuration mode. To disable the command function, use the **no** form of this command.

**vendor-tag strip**
**no vendor-tag strip**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command’s functionality is disabled. In the default condition, outgoing packets from the Broadband Remote Access Server (BRAS) have a digital subscriber line access multiplexer (DSLAM)-inserted Remote-ID tag when the **vendor-tag remote-id service** command is configured.

## Command Modes

BBA group configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. This command replaces the **vendor-tag circuit-id strip** command. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Outgoing packets from the BRAS will have a DSLAM-inserted Remote-ID tag when the **vendor-tag remote-id service** command is configured. The DSLAM must remove the tag from the PPPoE Active Discovery (PAD) outgoing packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending out the packets. When the **vendor-tag strip** command is configured, the BRAS removes the incoming Vendor-Specific Line-ID tag from the outgoing packets.

Outgoing PADO and PPPoE Active Discovery Session-Confirmation (PADS) packets from the BRAS will have the DSLAM-inserted Circuit-ID tag. The DSLAM must remove the tag from PADO and PADS packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending the packets out, and this is accomplished using the **vendor-tag strip** command.

The **vendor-tag circuit-id strip** command may continue to perform its normal function in prior releases, but it is no longer being updated. Support for the **vendor-tag circuit-id strip**command will cease in a future release.

## Examples

In the following example, the BRAS removes incoming Vendor-Specific Remote-ID tags from outgoing PADO and PADS packets:

```
bba-group pppoe pppoe-rm-tag
 sessions per-mac limit 50
 vendor-tag remote-ID service
 vendor-tag strip

interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-tag
```

## Related Commands

| Command | Description |
|---|---|
| **vendor-tag circuit-id strip** | Removes the incoming Vendor-Specific Line-ID tag from outgoing PADO and PADR packets. |
| **vendor-tag remote-id service** | Enables processing of the PPPoE Vendor-Specific tag in a PADR packet so the Remote-ID part can be sent to a AAA server as the NAS-Port-ID attribute in RADIUS access requests. |

# virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

**virtual-profile virtual-template** *number*
**no virtual-profile virtual-template** *number*

## Syntax Description

| | |
|---|---|
| *number* | Number of the virtual template to apply, ranging from 1 to 30. |

## Command Default

Disabled. No virtual template is defined, and no default virtual template number is used.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 F | This command was introduced. |

## Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

## Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

## Related Commands

| Command | Description |
|---|---|
| **interface virtual-template** | Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces. |

# virtual-template (BBA group)

To configure a PPPoE profile with a virtual template to be used for cloning virtual access interfaces, use the **virtual-template**command in BBA group configuration mode. To remove the virtual template from a PPPoE profile, use the **no** form of this command.

**virtual-template** *template-number*
**no virtual-template** *template-number*

## Syntax Description

| | |
|---|---|
| *template-number* | Identifying number of the virtual template that will be used to clone virtual-access interfaces. |

## Command Default

A virtual template is not specified.

## Command Modes

BBA group configuration (config-bba-group)#

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.3(7)XI3 | This command was integrated into Cisco IOS Release 12.3(7)XI3. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| Cisco IOS XE 2.3.0 | This command was integrated. This command is supported on ASR 1000 series. |

## Usage Guidelines

Each PPPoE profile can clone virtual-access interfaces using only one virtual template. If you enter a second **virtual-template** command in a PPPoE profile, it will replace the first **virtual-template** command.

You can configure different PPPoE profiles to use different virtual templates. You can also configure multiple PPPoE profiles to use the same virtual template.

## Examples

The following example shows the configuration of two PPPoE profiles:

```
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
bba-group pppoe vpn2
 virtual-template 2
 sessions per-vc limit 2
 sessions per-mac limit 1
!
```

## Related Commands

| Command | Description |
|---|---|
| **bba-group pppoe** | Creates a PPPoE profile. |

# virtual-template pre-clone

To specify the number of virtual-access interfaces to be created and cloned from a specific virtual template, use the **virtual-template pre-clone** command in global configuration mode. To disable precloning, use the **no** form of this command.

**virtual-template** *template-number* **pre-clone** *number*
**no virtual-template** *template-number* **pre-clone** *number*

## Syntax Description

| | |
|---|---|
| *template-number* | The number of the virtual template interfaces from which the new virtual-access interfaces are created. |
| *number* | The number of virtual-access interfaces to be created. |

## Command Default

Precloning is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)DC | This command was introduced on the Cisco 6400 node route processor. |
| 12.2(4)T | This command was integrated into Cisco IOS Release 12.2(4)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

The number of precloned virtual-access interfaces should be set to the number of expected PPPoA and PPPoE sessions.

The precloned virtual-access interfaces will be attached to the PVC upon receipt of the first PPP packet from the client on the PVC. The virtual-access interface will be detached from the PVC upon termination of the PPP session.

When a PPP session is terminated, the virtual-access interface will remain in the router and will be reused. When precloning is disabled, any virtual-access interfaces that were already precloned but have not yet been used will remain in the router for future use.

## Examples

The following example shows how to create 1200 precloned virtual-access interfaces on virtual template 1:

```
virtual-template 1 pre-clone 1200
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation (ATM)** | Configures the AAL and encapsulation type for an ATM VC, VC class, VC, bundle, or PVC range. |
| **show vtemplate** | Displays a list of all configured virtual templates. |

# virtual-template snmp

To allow virtual access registration with Simple Network Management Protocol (SNMP), use the **virtual-template snmp**command in global configuration mode. To disable virtual access with SNMP, use the **no**form of this command.

**virtual-template snmp**
**no virtual-template snmp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Virtual access registration is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SB | This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SB. |
| 12.2(33)SB | The default configuration of this command was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4, as described in the Usage Guidelines. |

## Usage Guidelines

### Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command is disabled by default. This default setting enhances scaling and prevents a large number of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

With the **virtual-template snmp** command disabled, a router no longer accepts the **snmp trap link-status**command under a virtual-template interface. Instead, the router displays a configuration error message as shown in the following example:

```
Router(config)# interface
 virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual-template interface is already registered in the interfaces MIB.

## Examples

The following example shows how to enable virtual access registration with SNMP:

```
Router> enable
Router# configure terminal
Router(config)# virtual-template snmp
```

Router(config)#

## Related Commands

| Command | Description |
|---|---|
| **snmp trap link-status** | Enables the generation of SNMP link traps. |

# vlan-id dot1q

To enable IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface, use the **vlan-id dot1q** command in interface configuration mode. To disable 802.1Q encapsulation for a specific VLAN, use the **no** form of this command.

**vlan-id dot1q** *vlan-id*
**no vlan-id dot1q** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN identifier. Valid values range from 1 to 4095. |

## Command Default

IEEE 802.1Q VLAN encapsulation is not enabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB |
| Cisco IOS XE Release 2.5 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

This command allows you to enable IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface without associating the VLAN with a subinterface. Configuring 802.1Q VLANs on the main interface without using up subinterfaces increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.

You can configure a VLAN on a main interface and at the same time configure VLANs on subinterfaces of the same interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time. To configure PPPoE over 802.1Q VLAN support on a subinterface, use the **encapsulation dot1q** and **pppoe enable** commands in interface configuration mode.

It is not possible to shut down traffic for individual VLANs that are configured on the main interface.

## Examples

The following example shows how to configure PPPoE over an 802.1Q VLAN on Fast Ethernet interface 0/0:

```
interface fastethernet 0/0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-id dot1q 20
  pppoe enable group PPPOE
  exit-vlan-config
```

The following example configures Ethernet interface 0 to bridge packets using VLAN ID 100 and assigns the interface to bridge group 1:

```
interface ethernet 0
 vlan-id dot1q 100
  description bridged vlan 100
  bridge-group 1
 bridge-group 1
```

## Related Commands

| Command | Description |
|---|---|
| **debug pppoe** | Displays debugging information for PPPoE sessions. |
| **pppoe enable** | Enables PPPoE sessions on an Ethernet interface or subinterface. |
| **vlan-range dot1q** | Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface. |
| **encapsulation dot1q** | Enables PPPoE over 802.1Q VLAN support on a subinterface. |

# vlan-range dot1q

To enable IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface, use the **vlan-range dot1q** command in interface configuration mode. To disable 802.1Q encapsulation for a range of VLANs, use the **no** form of this command.

**vlan-range dot1q** *start-vlan-id end-vlan-id* [**native**]
**no vlan-range dot1q** *start-vlan-id end-vlan-id*

## Syntax Description

| | |
|---|---|
| *start-vlan-id* | VLAN identifier of the first VLAN in the range. Valid values range from 1 to 4095. |
| *end-vlan-id* | VLAN identifier of the last VLAN in the range. Valid values range from 1 to 4095. |
| **native** | (Optional) Instructs the interface to bridge untagged (native) packets. |

## Command Default

IEEE 802.1Q VLAN encapsulation is not enabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |
| Cisco IOS XE Release 2.5 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

This command allows you to enable IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface without associating each VLAN with a subinterface. Configuring an 802.1Q VLAN range on the main interface without using up subinterfaces increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.

You can configure a VLAN range on a main interface and at the same time configure VLANs outside the range on subinterfaces of the same interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time. To configure PPPoE over 802.1Q VLAN support on a subinterface, use the **encapsulation dot1q** and **pppoe enable** commands in interface configuration mode.

It is not possible to shut down traffic for individual VLANs that are configured on the main interface.

To bridge both tagged and untagged packets, regardless of their VLAN ID, you do not need to create a VLAN ID range.

## Examples

The following example shows how to configure PPPoE over a range of 802.1Q VLANs on Fast Ethernet interface 0/0:

```
interface fastethernet 0/0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-range dot1q 20 30
  pppoe enable group PPPOE
  exit-vlan-config
```

The following example configures Ethernet interface 0 to bridge untagged (native) packets using a range of VLAN IDs from 1 to 500 and assigns the interface to bridge group 1:

```
interface ethernet 0
 vlan-range dot1q 1 500 native
  description 1 to 500
  bridge-group 1
 bridge-group 1
```

## Related Commands

| Command | Description |
|---|---|
| **debug pppoe** | Displays debugging information for PPPoE sessions. |
| **pppoe enable** | Enables PPPoE sessions on an Ethernet interface or subinterface. |
| **vlan-id dot1q** | Enables IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface. |
| **encapsulation dot1q** | Enables PPPoE over 802.1Q VLAN support on a subinterface. |

# vpdn authorize domain

To enable domain preauthorization on a network access server (NAS), use the **vpdn authorize domain** command in global configuration mode. To disable domain preauthorization, use the **no** form of this command.

**vpdn authorize domain**
**no vpdn authorize domain**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Domain preauthorization is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)DC1 | This command was introduced on the Cisco 6400 NRP. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

A domain preauthorization RADIUS user profile must also be created. See the Examples section and refer to the *Cisco IOS Security Configuration Guide* for information on how to create these profiles.

## Examples

### Domain Preauthorization Configuration on the LAC Example

The following example shows the configuration necessary for an L2TP access concentrator (LAC) to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

### Domain Preauthorization RADIUS User Profile Example

The following example shows a domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33{
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
```

```
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:vpn-domain-list=net1.com,net2.com"
6=5
}
}
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

# vpn service

To configure a static domain name, use the **vpn service** command in ATM VC, ATM VC class or VC class configuration mode or in PVC range configuration mode. To remove a static domain name, use the **no** form of this command.

**vpn service** *domain-name* [**replace-authen-domain**]
**no vpn service** *domain-name* [**replace-authen-domain**]

## Syntax Description

| | |
|---|---|
| *domain-name* | Static domain name. |
| **replace-authen-domain** | (Optional) Specifies that when a static name is configured and VPDN preauthentication is configured, the domain name specified for VPN service replaces the domain field in the username for authentication. |

## Command Default

No default behavior or values

## Command Modes

ATM VC configuration
ATM VC class configuration
PVC range configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(1)DC1 | This command was introduced on the Cisco 6400 NRP. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.3(7)XI7 | The **replace-authen-domain** keyword was added and this command was integrated into Cisco IOS Release 12.2(7)XI7. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

Use the **vpn service** command in a permanent virtual circuit (PVC), VC class configuration, or PVC range configuration so that PPP over ATM (PPPoA) or PPP over Ethernet over ATM (PPPoEoA) sessions in those PVCs will be forwarded according to the domain name supplied, without starting PPP.

To replace the VPN service domain name with the domain name from the username during preauthentication, use this command with the **replace-authen-domain** keyword, in conjunction with the **vpdn authen-before-forward** command.

## Examples

In the following partial example, VPDN group 1 is selected for PPPoA session forwarding based on the domain name example.com:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.com
 initiate-to ip 10.1.1.1 priority 1
.
```

```
.
.
interface ATM1/0.1 multipoint
 pvc 101
  encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net
```

In the following partial example using the **replace-authen-domain** keyword, the domain field is replaced by the domain name during preauthentication:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.net
 authen-before-forward
 initiate-to ip 10.1.1.1 priority 1
.
.
.
interface atm 4/0
 ip address 3.0.0.2 255.255.0.0
 pvc 1/20
encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net replace-authen-domain
```

## Related Commands

| Command | Description |
|---|---|
| **vpdn authen-before-forward** | Enables authentication of all dial-in L2TP sessions before the sessions are forwarded to the tunnel server (global preauthentication). |