# Broadband Scalability and Performance

The infrastructure of a service provider must be capable of supporting the services that an enterprise customer or Internet service provider (ISP) wants to offer its subscribers. The service provider must also be able to scale up to an expanding subscriber base. You can configure the Cisco ASR1000 Series Routers for high broadband scalability.


- Finding Feature Information in This Module, on page 1
- Contents, on page 1
- PPP Sessions and L2TP Tunnel Scaling, on page 1
- Configuring the Cisco ASR 1000 Series Router for High Scalability, on page 2
- Using the cisco avpair lcp interface config RADIUS Attribute, on page 5
- Additional References, on page 7
- Feature Information for Broadband Scalability and Performance, on page 8


## Finding Feature Information in This Module

Your software release might not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information for Broadband Scalability and Performance, on page 8.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

## Contents

This guide provides information about the following topics:

## PPP Sessions and L2TP Tunnel Scaling

The ASR 1000 Series Routers are deployed in a variety of broadband deployment models for terminating Point-to-Point Protocol (PPP) Sessions and initiating or terminating Layer 2 Tunneling Protocol (L2TP) tunnels. The maximum number of PPP sessions and L2TP tunnels is dependent on the hardware combination.

# Restrictions for PPP Sessions and L2TP Tunnel Scaling

This section lists the restrictions for the PPP sessions and L2TP tunnel scalability.

- To achieve maximum scaling for the 1001, 1002, and 1004 chassis, we recommend software redundancy be disabled for broadband applications, and only hardware redundancy be configured.
- Restrictions on 48000 session scaling with RP2 and ESP-40G include:
  - Intelligent Services Gateway (ISG) Services are not supported
  - Point-to-Point Protocol over ATM (PPPoA) and Point-to-Point Protocol over Ethernet (PPPoEoA) sessions are not supported
  - RP2 requires 16 GB DRAM to support 48000 sessions

**Note** If any of the listed restrictions is not met, the router scales to a maximum of 32000 sessions only.

- Restrictions on the 64000 session scaling with RP2 and ESP-40G:
  - ISG services are not supported
  - PPPoA and PPPoEoA sessions are not supported
  - Per-session QoS with queuing actions (for example, shaping) is not supported
  - RP2 requires 16 GB DRAM to support 64000 sessions

**Note** If any of the listed restrictions is not met, the router scales to a maximum of 32000 sessions or 48000 sessions only.

- Restrictions on 64000 L2TP tunnel scaling with RP2 and ESP-40G:
  - ISG services are not supported
  - Per-session QoS is not supported
  - RP2 requires 16 GB DRAM
  - High Availability (SSO) is not supported

**Note** If any of the listed restrictions is not met, the router scales to a maximum of 16000 L2TP tunnels.

- The RP2 and ESP10 hardware combination is not supported for broadband.
- RP1 with 2GB of DRAM is not recommended for broadband deployment.

# Configuring the Cisco ASR 1000 Series Router for High Scalability

The Cisco ASR 1000 Series Routers provide powerful performance and scalability for embedded services.

To achieve maximum scaling on the 1001, 1002, and 1004 chassis, IOS software redundancy must be disabled.

To ensure high scalability on the Cisco ASR 1000 Series Aggregation Services Router, perform the following configuration tasks:

# Configuring Call Admission Control

The Call Admission Control (CAC) feature is configured to protect the ASR 1000 processing resources that must be configured. CAC can restrict the media bandwidth dedicated to active calls when CPU utilization exceeds the configured threshold.

This section provides the following examples for configuring CAC:

**Configuring a PPPoE Session**

```
router(config)# call admission new-model
router(config)# call admission limit 1000
router(config)# call admission cpu-limit 80
router(config)# call admission pppoe 10 1
```

**Configuring a PPPoA Session**

```
router(config)# call admission new-model
router(config)# call admission limit 1000
router(config)# call admission cpu-limit 80
router(config)# call admission pppoa 10 1
```

**Configuring a VPDN Session**

```
router(config)# call admission new-model
router(config)# call admission limit 1000
router(config)# call admission cpu-limit 80
router(config)# call admission vpdn 10 1
```

# Control Plane Policing

The Control Plane Policing feature allows you to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS XE routers and switches against reconnaissance and denial-of-service (DoS) attacks. The control plane thus helps maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

For examples about configuring the Control Plane Policing feature, see the “Control Plane Policing” section in the *Quality of Service Solutions Configuration Guide* located at:

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-ctrl-pln-plc.html

# VPDN Group Session Limiting

Using the Virtual Private Dialup Network (VPDN) Group Session Limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. VPDN session limits can increase performance and reduce latency for routers that are otherwise forced to operate at high capacity.

For more information about VPDN Group Session Limiting, see the feature documentation at:

http://www.cisco.com/en/US/docs/ios-xml/ios/vpdn/configuration/xe-3s/vpd-tunnel-mgmt.html

# PPPoE Session Limiting

The PPPoE Session Limit Support feature prevents the router from using too much memory for virtual access by limiting the number of PPPoE sessions that can be created on a router or on all Ethernet interfaces and subinterfaces as well as ATM interfaces and subinterfaces.

For more information about PPPoE session limiting, see the feature documentation at:

http://www.cisco.com/en/US/docs/ios-xml/ios/bbdsl/configuration/xe-3s/bba-limit-legcfg-xe.html

# Monitoring PPP Sessions Using the SNMP Management Tools

To prevent the virtual access subinterfaces from being registered with the Simple Network Management Protocol (SNMP) functionality of the router and using up the memory, do not use the SNMP management tools of the router to monitor PPP sessions. Use SNMP views to isolate the bulk queries and accidental requests.

Use the **no virtual-template snmp** command to disable the SNMP management tools:

```
Router(config)# no virtual-template snmp
```

# Configuring the Access Interface Input and Output Hold Queue

The default value of Gigabit Ethernet and 10 Gigabit Ethernet interfaces is 375 packets for the input and output hold queues. If the interfaces are required to handle a high rate of control packets, such as LCP, IPCP, PPP, L2TP, and DHCP, the default value may not be sufficient. To ensure high scalability, set the access interface input and output hold queue to 4096:

```
Router(config)# interface gig1/0/0
Router(config-if)# hold-queue 4096 in
```

# Configuring the keepalive Command

For PPP sessions, the **keepalive** command sets the keepalive timer for a specific interface. To ensure proper scaling and to minimize CPU utilization, set the timer for 60 seconds or longer. The default value is 10 seconds:

```
interface Virtual-Template1
 ip unnumbered Loopback1
 keepalive 60
 no peer default ip address
 ppp authentication pap
```

**Note** For IP sessions, the keepalives are not enabled by default. Enabling keepalives for IP sessions provides the same capability as PPP keepalives except that ICMP or ARP is used to test the presence of subscribers. For more information about Using ARP for Keepalive Messages and Using ICMP for Keepalive Messages, see the feature documentation at:
http://www.cisco.com/en/US/docs/ios-xml/ios/isg/configuration/xe-3s/Configuring_ISG_Policies_for_Session_Maintenance.html

## Scaling the L2TP Tunnel Configurations

To prevent head-of-the-line blocking of the IP input process and save system resources, configure the vpdn ip udp ignore checksum command:

```
Router(config)# vpdn ip udp ignore checksum
```

When you configure this command, the router directly queues the L2TP Hello packets and Hello acknowledgements to the L2TP control process. We recommend that you configure this command in all the scaled LAC and LNS L2TP tunnel configurations.

If you do not configure the vpdn ip udp ignore checksum command, the L2TP software sends the packets to UDP to validate the checksum. When too many packets are queued to the IP input process, the router starts Selective Packet Discard (SPD) mechanism that causes IP packets to be dropped.

**Note** Head-of-the-line blocking of the IP input process might occur in other nonL2TP configurations. A flush occurring on an input interface indicates that the SPD mechanism is discarding packets.

# Using the cisco avpair lcp interface config RADIUS Attribute

When you use the lcp:interface-config RADIUS attribute to reconfigure the virtual access subscriber interface, call setup rate could be reduced on the Cisco ASR 1000 Series Aggregation Services Routers because the lcp:interface-config command syntax includes an IOS interface configuration command. This command is any valid IOS command that can be applied to an interface. When the lcp:interface-config attribute is downloaded from the RADIUS server to the Cisco ASR 1000 Series Aggregation Services Routers, the command parser is activated to configure the interface according to AV-pair, determining if the option is valid and then applying the configuration to the virtual access interface (VAI).

The subscriber session scaling on the Cisco ASR 1000 Series Aggregation Services Routers is not impacted by using the lcp:interface-config RADIUS attribute any more than if the equivalent IOS interface command was applied directly onto the virtual-template configuration and was cloned onto the VAI using that method. Using either the lcp:interface-config RADIUS attribute or the virtual-template to apply configuration onto the VAI it is the type of configuration being applied which may in a few cases affect the maximum subscriber session scale of the Cisco ASR 1000 Series Aggregation Services Routers.

## Enhancing the Scalability of Per-User Configurations

To enhance scalability of per-user configurations without changing the router configuration, use the ip:vrf-id and ip:ip-unnumbered RADIUS attributes. These per-user vendor-specific attributes (VSAs) are used to map sessions to VRFs and IP unnumbered interfaces. The VSAs are applied to virtual access subinterfaces and are processed during PPP authorization.

The ip:vrf-id attribute is used to map sessions to VRFs. Any profile that uses the ip:vrf-id VSA must also use the ip:ip-unnumbered VSA to install IP configurations on the VAI that is to be created. The PPP that is used on a VAI to be created requires the ip:ip-unnumbered VSA. An Internet Protocol Control Protocol (IPCP) session is not established if IP is not configured on the interface. You must configure either the ip address command or the ip unnumbered command on the interface so that these configurations are present on the VAI that is to be created. However, specifying the ip address and ip unnumbered commands on a virtual template interface is not required because pre-existing IP configurations, if any, are removed when the ip:ip-vrf VSA

is installed on the VAI. Therefore, any profile that uses the ip:vrf-id VSA must also use the ip:ip-unnumbered VSA to install IP configurations on the VAI that is to be created.

These per-user VSAs can be applied to VAIs. Therefore, the per-user authorization process does not require the creation of full VAIs, which improves scalability.

## Setting the VRF and IP Unnumbered Interface Configurations in User Profiles

Although the Cisco ASR 1000 Series Aggregation Services Router continues to support the lcp:interface-config VSA, the ip:vrf-id and ip:ip-unnumbered VSAs provide another way to set the VRF and IP unnumbered interface configurations in user profiles. The ip:vrf-id and ip:ip-unnumbered VSAs have the following syntax:

```
Cisco:Cisco-AVpair = "ip:vrf-id=vrf-name"
Cisco:Cisco-AVpair = "ip:ip-unnumbered=interface-name"
```

You should specify only one ip:vrf-id and one ip:ip-unnumbered value in a user profile. However, if the profile configuration includes multiple values, the Cisco ASR 1000 Series Aggregation Services Router applies the value of the last VSA received, and creates a virtual access subinterface. If the profile includes the lcp:interface-config VSA, the router always applies the value of the lcp:interface-config VSA.

## Setting the VRF and IP Unnumbered Interface Configurations in Virtual Interface Templates

You can specify one VSA value in a user profile on RADIUS and another value locally in the virtual template interface. The Cisco ASR 1000 Series Aggregation Services Router clones the template and then applies the values configured in the profiles it receives from RADIUS, resulting in the removal of any IP configurations when the router applies the profile values.

## Redefining User Profiles to Use the ip:vrf-id and ip:ip-unnumbered VSAs

The requirement of a full virtual access interface when using the lcp:interface-config VSA in user profiles can result in scalability issues, such as increased memory consumption. This situation is especially true when the Cisco ASR 1000 Series Aggregation Services Router attempts to apply a large number of per-user profiles that include the lcp:interface-config VSA. Therefore, when updating your user profiles, we recommend that you redefine the lcp:interface-config VSA to the scalable ip:vrf-id and ip:ip-unnumbered VSAs.

The following example shows how to redefine a VRF named newyork using the ip:vrf-id VSA:

```
Change:
Cisco:Cisco-Avpair = "lcp:interface-config=ip vrf forwarding newyork"
To:
Cisco:Cisco-Avpair = "ip:vrf-id=newyork"
```

The following example shows how to redefine the Loopback 0 interface using the ip:ip-unnumbered VSA.

```
Change:
Cisco:Cisco-Avpair = "lcp:interface-config=ip unnumbered Loopback 0"
To:
```

Cisco:Cisco-Avpair = “ip:ip-unnumbered=Loopback 0”

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Control Plane Policing | *Quality of Service Solutions Configuration Guide* |
| VPDN Group Session Limiting | *VPDN Configuration Guide, Cisco IOS XE Release 3S* |
| PPPoE session limiting | Configuring PPP over Ethernet Session Limit Support Feature Guide |
| Using ARP for Keepalive Messages and Using ICMP for Keepalive Messages | Intelligent Services Gateway Configuration Guide Cisco IOS XE Release 3S |

### Standards

| Standard | Title |
|---|---|
| None | — |

### MIBs

| MIB | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at this URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| None | — |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Broadband Scalability and Performance

The table below lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

**Note** The below table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

***Table 1: Feature Information for Broadband Scalability and Performance***

| Feature Name | Releases | Feature Information |
|---|---|---|
| High Availability Overview | Cisco IOS XE 2.1S | In Cisco IOS XE Release 2.1S, this feature was introduced on the Cisco ASR 1000 Series Router. |
| Walk-by User Support for PWLAN in ISG | Cisco IOS XE 3.7S | In Cisco IOS XE Release 3.7S, this feature was introduced on the Cisco ASR 1000 Series Router. |