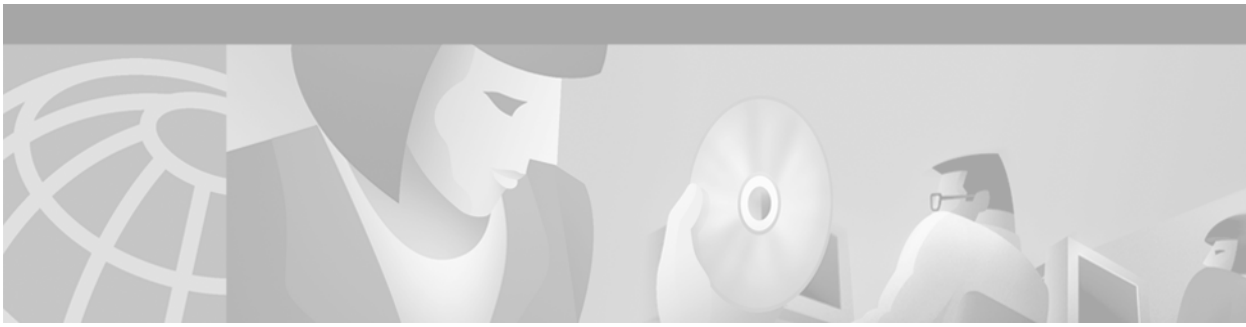


Release Notes for NRP-2SV Card for Cisco 6400 Carrier-Class Broadband Aggregator

November 26, 2001

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback.

Overview

This document describes the NRP-2SV node route processor card for the Cisco 6400 carrier-class broadband aggregator. The NRP-2SV supports Cisco IOS Release 12.2(2)B1. This document describes basic installation of the NRP-2SV and describes some parameters to optimize the performance of the new card.

This release note contains these sections:

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

Installing the NRP-2SV Card

NRP-2SV cards can be installed in slots 1 through 8 in the Cisco 6400 chassis. This section describes the procedure for removing the existing NRP-1 or NRP-2 card in a Cisco 6400 chassis and then installing the new NRP-2SV card.

All cards, modules, and components support online insertion and removal (often referred to as hot swapping). Hot swapping allows you to remove, replace, and rearrange the cards without turning off the system power. When the system detects that a card or module has been added or removed, it automatically runs diagnostic and discovery routines, acknowledges the presence or absence of the card or module, and resumes system operation without any operator intervention.

Removing an NRP Card

To remove an installed NRP-1 or NRP-2 card from the chassis:

Step 1 Attach an ESD-preventive wrist strap.

Step 2 Disconnect any cables connected to the NRP card that you are about to remove.

Step 3 Unfasten the upper and lower retaining screws.

Step 4 Grasp the upper and lower extraction levers. Pull up on the upper lever while pushing down on the lower lever. This action disengages the NRP carrier from the connectors on the backplane.

Step 5 Slide the NRP card out of the slot.

Step 6 Place the NRP card on an antistatic surface or put it in a static-shielding bag or in a box lined with antistatic material.

Installing an NRP-2SV Card

Step 1 Hold the NRP-2SV module vertically, with the NRP-2SV faceplate toward you and the backplane connectors away from you. Ensure that the module is right side up by noting the lettering on the faceplate.

Step 2 Carefully align the upper and lower edges of the NRP-2SV carrier with the upper and lower guides in the chassis. See Figure 1 for an example of inserting an NRP-2SV module in the chassis.

⚠ **Caution** To ensure that the NRP-2SV card mates properly with all backplane connector pins, the card length and card slots have been designed with very close tolerances. To slide the module into the slot requires gentle pressure with each hand, at the top and bottom of the faceplate.

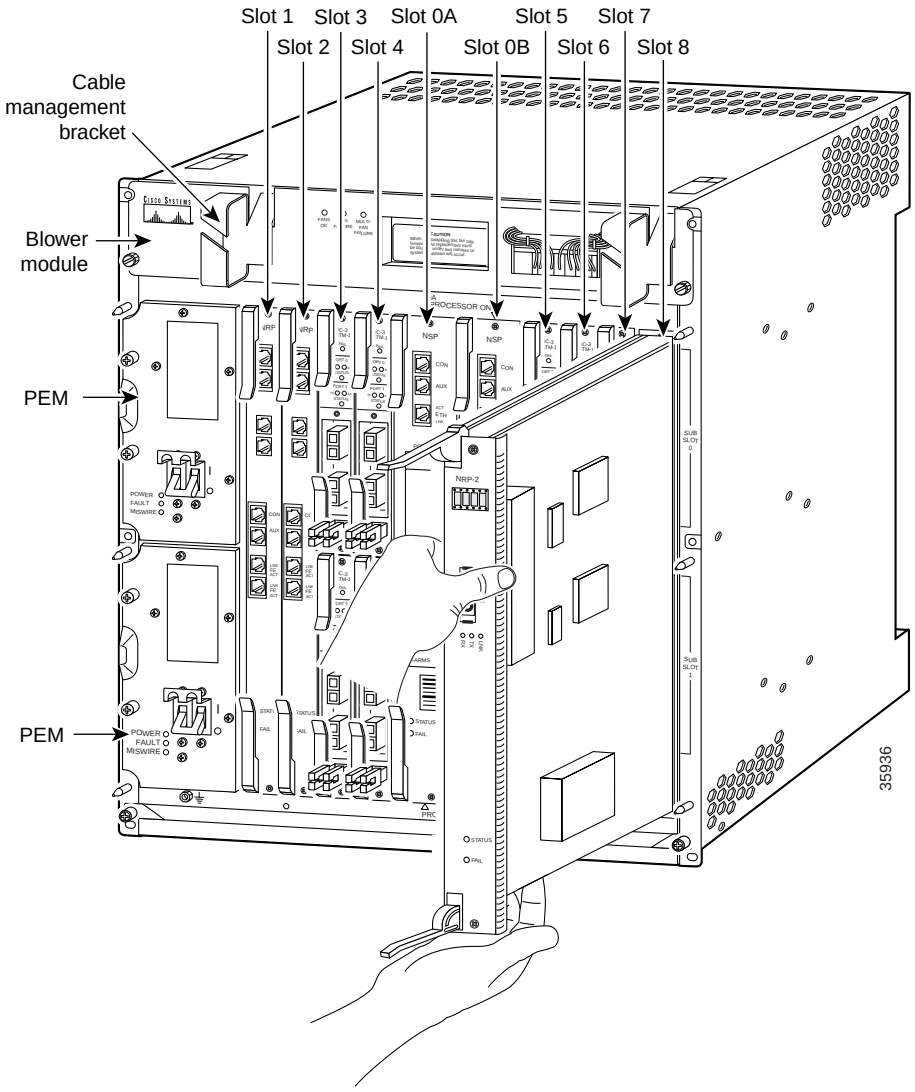
Step 3 Gently slide the NRP-2SV card into the slot until it makes contact with the backplane.

Step 4 Press the upper lever down and the lower lever up at the same time.

Step 5 Secure the carrier by tightening the upper and lower retaining screws.

Step 6 Connect the cables.

Figure 1 Inserting an NRP-2SV into the Chassis



Warning Statements

The following warnings apply to the NRP-2SV module.

Warning **Class 1 laser product. To see translations of this warning, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Warning **Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures. To see translations of this warning, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Warning **Invisible laser radiation present. To see translations of this warning, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Warning Statement for Sweden

Varning! **Osynlig laserstrålning när denna del är öppen och förregleringen är urkopplad. Rikta inte blicken in mot strålen.**

Warning Statement for Finland

Varoitus **Alleviates ja suojalukitus ohitettaessa olet alttiina näkymättömälle lasersäteilylle. Äjä katso säteeseen.**

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they reduce electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place. To see translations of this warning, refer to the *Regulatory Compliance and Safety Information* document that accompanied the Cisco 6400 chassis.**

Session and Tunnel Scalability

The NRP-2SV card supports Cisco IOS Release 12.2(2)B1. This software supports the number of sessions and tunnels shown in Table 1. While using NRP-SSG, Cisco IOS Release 12.2(2)B1 supports the number of sessions and tunnels shown in Table 2.

Table 1 Session and Tunnel Scalability in Cisco IOS Release 12.2(2)B1

	NRP-2SV	
Protocol	**Number of Supported Sessions**	**Number of Supported Tunnels**
L2TP PPPoA	up to 8000	up to 2000
L2TP PPPoE	up to 8000	up to 2000
PPPoA	up to 8000	—
PPPoE	up to 8000	—
PPP Autosense	up to 4000	—
RBE	up to 8000	—
RFC 1483 IP Routed	up to 8000	—
RFC1483 MPLS VPN	up to 4000	up to 500
RBE MPLS VPN	up to 4000	up to 500

Table 2 NRP-SSG Session and Tunnel Scalability in Cisco IOS Release 12.2(2)B1

	NRP-2SV	
Protocol with NRP-SSG	**Number of Supported Sessions**	**Number of Supported Tunnels**
L2TP PPPoA	up to 4000	up to 2000
L2TP PPPoE	up to 4000	up to 2000
PPPoA	up to 8000	—
PPPoE	up to 8000	—
RBE	up to 8000	—
RFC 1483 IP Routed	up to 8000	—
GRE PPPoA	up to 8000	up to 2000

Note In most NRP-2 configurations, 256 MB DRAM is adequate for up to 6500 (PPPoE) sessions. More sessions require 512 MB DRAM.

Scalability Parameters

This section provides scalability tuning parameter values used during testing for 8000 PPPoA sessions and 2000 L2TP tunnels. These parameters prevent known issue CSCdu86416 from happening. During development testing of these parameters, all sessions come up in about 20 minutes.

```
interface Virtual-Template1
keepalive 200
ppp timeout retry 25
ppp timeout authentication 20

vpdn-group 1
l2tp tunnel hello 150
l2tp tunnel receive-window 500
l2tp tunnel nosession-timeout 20
l2tp tunnel retransmit retries 12
l2tp tunnel retransmit timeout min 4
l2tp tunnel retransmit timeout max 6
```

Following is the hold-queue CLI used during testing.

```
interface ATM0/0/0
 no ip address
 load-interval 30
 atm vc-per-vp 2048
 no atm ilmi-keepalive
 hold-queue 4096 in
 hold-queue 4096 out
end
```

IP QoS—Policing and Marking

Cisco IOS QoS offers two kinds of traffic regulation mechanisms—policing and shaping.

The rate-limiting features of committed access rate (CAR) and the Class-Based Policing features provide the functionality for policing traffic.

The features of Generic Traffic Shaping (GTS), Class-Based Shaping, Distributed Traffic Shaping (DTS), and Frame Relay Traffic Shaping (FRTS) provide the functionality for shaping traffic.

Release 12.2(2)B1 supports the Committed Access Rate (CAR) feature on NRP, which allows policing upstream/downstream subscriber traffic to specific rates. Additionally, traffic can be marked with specific IP Precedence. You can also use an access list (ACL) to classify traffic to be policed (and optionally marked).

For more details on CAR, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/car.pdf

Configurations

CAR can be configured on an interface or subinterface that has an IP address (or IP unnumbered Loopback). When configured on a virtual-template, it is applied to all the virtual-access interfaces derived from the template. Modifying the CAR parameters on the virtual-template propagates the modification to the virtual-access interfaces.

To rate-limit or mark traffic from/to subscribers, you can configure upstream and/or downstream policing/marking as shown in the following examples (for more details, refer to the website mentioned earlier).

PPPoE/PPPoA Termination—Configure CAR in the Virtual-Template

```
rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop
```

This restricts downstream traffic of each PPPoE (PPPoA) session to 256000 bits/sec. The burst size and excess burst size are 16000 bytes and 32000 bytes, respectively. Traffic exceeding the policing rate and burst are dropped.

```
rate-limit input 256000 16000 32000 conform-action set-prec-transmit 5 exceed-action set-prec-transmit 0
```

This sets the IP precedence bits in the IP header to 5 for packets that meet the policing rate. Exceeding packets are transmitted with IP precedence set to 0.

RBE Interface—Configure CAR on the RBE Subinterface

```
interface ATM0/0/0.1001 point-to-point
  ip address 174.128.240.1 255.255.255.252
  rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop
  atm route-bridged ip
  pvc 31/1001
    encapsulation aal5snap
```

1483 Routing—Configure CAR on the 1483 Routed Subinterface

```
interface ATM0/0/0.1005 point-to-point
  ip address 174.128.240.1 255.255.255.252
  rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop
  pvc 31/1005
    encapsulation aal5snap
```

On the trunk side, you can configure upstream and/or downstream policing/marking by configuring CAR on an ATM subinterface, Fast-Ethernet/Gigabit-Ethernet interface, or subinterface.

CAR is not supported on PPP/L2TP LAC at present, or on GRE tunnels.

Configuring Policing/Marking in RADIUS User Profile

For PPPoE/PPPoA sessions that terminate on NRP, instead of configuring CAR on the virtual template, you can configure CAR on the RADIUS user profile. This allows separate policing/marking on different PPPoE (PPPoA) sessions even though the sessions share the same virtual template. When the policing/marking parameters are defined on the AAA profile of a user, Cisco IOS software applies these policing/marking parameters to any PPPoE (PPPoA) session established by the user.

The following AAA user profile for john defines a policing rate of 120,000 bps. You can use any AAA server that supports Cisco AV pair (the following AAA configurations are for a Merit AAA Server).

john Password = “xyz”

Service-Type = Framed-User,

Framed-Protocol = PPP,

av-pair = “ip:addr-pool=pool4”,

av-pair = “lcp:interface-config#1=rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop”

av-pair = “lcp:interface-config#2=rate-limit input 64000 16000 32000 conform-action transmit exceed-action drop”

Note The ' #1', '#2' need not be specified if there is only one “lcp:interface-config” AV-pair in the RADIUS user profile.

The “lcp:interface-config=” AV-pair takes the rest of the AV-pair string as a Cisco IOS command and applies it to the virtual-access interface when the user initiates the PPP session. For john, it therefore applies this command to the virtual-access interface:

rate-limit output 120000 16000 32000 conform-action transmit exceed-action drop

For AAA-based policing to work, you must configure the following in global configuration mode:

virtual-profile aaa

Verifying Policing/Marking

You can use the following command to verify CAR policing/marking:

show interface <int> rate-limit

Where <int> is any interface including virtual-access interface.

This command displays the CAR configuration on the interface and policing statistics.

```
NRP-2SV# sh int Virtual-access 4 rate-limit
Virtual-Access4
  Output
    matches: all traffic
      params: 256000 bps, 16000 limit, 32000 extended limit
      conformed 335 packets, 459710 bytes; action: transmit
      exceeded 46 packets, 65851 bytes; action: drop
      last packet: 182368ms ago, current burst: 10017 bytes
      last cleared 00:05:22 ago, conformed 11000 bps, exceeded 1000 bps
```

Important Notes and Recommendations

1. Performance impact—CAR policing algorithm impacts performance due to its additional use of processor resource. Typical performance impact may be about 20 to 30%, although it would vary depending on the traffic mix and the configured protocol:
   - Packet Marking will additionally impact performance by about 2%
   - Using an ACL with CAR will affect performance depending on the type of ACL used

   Burst Size—The recommended configuration for burst size and excess burst size is as follows:

   Burst size = amount of traffic at the policed rate that can flow in one second interval (expressed in bytes)

   Excess burst = 2 x burst size

For example, for a policing rate of 256,000 bps, you can choose burst = 32,000 (bytes), and excess burst = 64,000 (bytes). This will allow bursty traffic while maintaining an average policing rate of 256,000 bps. Smaller burst sizes will drop more packets for bursty traffic—larger burst sizes will better accommodate traffic bursts.

For example, CAR configuration for 256 Kbps policing rate should be:

rate-limit output 256000 32000 64000 conform-action transmit exceed-action drop

However, if the traffic is not very bursty, then lower values of burst and excess-burst may work, but typically burst-size should not be less than 16,000 bytes for TCP traffic. You may need to experiment to find burst and excess bursts that best fit the traffic characteristics.

2. For PPPoE and PPPoA subscribers, you can configure the above rate-limit command in the virtual-template. If PPPoE is used, it is possible to use only one policing rate for all subscribers on an NRP (since only one virtual-template is used in PPPoE). If PPPoA is used, it is possible to use multiple virtual templates with different policing rates on the same NRP. For 1483-routed and RBE cases, configure CAR on the ATM subinterface for the subscriber. Ensure that the subinterface has an IP address (either directly, or IP unnumbered interface).
3. CAR support with SSG is not available. Do not turn on SSG.
4. IP Policing is not applicable in PPP/L2TP case (on LAC) or on tunnel interfaces.
5. CAR works with CEF-switched packets, so do not configure fast or process switching for traffic to be policed. CAR doesn't officially support policing of packets locally generated by the router or any packets that aren't CEF-switched including multicast packets.
6. Unlike shaping that buffers packets exceeding the shaping rate (until its buffer is full) and transmits them later, policing drops packets that exceed the configured rate. So depending on the traffic volume and burstiness, policing may lead to a larger amount of packet drops compared to shaping.
7. Some applications, such as VoIP and streaming video, are sensitive to packet drops. CAR should not be configured so that it can drop traffic of such applications. However, CAR can be used if the application completely downloads a voice/audio file before playing it.
8. AAA download of policing parameters—If you download policing parameters from a AAA server, the downloaded command string is parsed during PPP session establishment, which reduces the number of PPP sessions that can be established per second. The maximum number of PPP calls per second will be less than 10, depending on the PPP parameters configured in the virtual-template (ppp keepalive, authentication/retry timeouts), the number of configured sessions, and the traffic volume.
9. For scaling to a large number of PPPoE/PPPoA sessions, you should tune the ppp keepalive and authentication/retry timeouts according to scalability guidelines by appropriate configuration of ppp keepalive, ppp timeout retry, and ppp timeout authentication statements in the virtual-template. This is particularly important if you configure CAR policing parameters in AAA user profile.
10. The rate-limit command in a RADIUS user profile must not exceed 240 characters (which is sufficient for configuring any kind of policing and marking). If it does, the router may give errors or crash.

For more information on this feature, see the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2*, “Policing and Shaping” chapter.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com. To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the *Cisco 6400 Hardware Installation and Maintenance Guide*..