

Service Provider PAT Port Allocation Enhancement for RTP and RTCP

Problem Overview

With the increase in the use of multimedia and real-time traffic over the Internet, private network administrators face the unique challenge of defending their networks from both internal and external threats, while allowing voice, multimedia, and gaming traffic to flow through transparently.

Private residential user networks and small-office/home-office (SOHO) networks connect into the service provider network region using a simple home gateway. Home gateways can perform basic Network Address Translation (NAT), but are not sophisticated enough to perform Port Address Translation (PAT). They must rely on the service provider's session border controller for this capability.

One particular challenge is enabling PAT to work in conjunction with Routing Table Protocol (RTP) and Real-Time Control Protocol (RTCP), which have well-defined working port ranges. The home gateway needs to be replaced with an application-level gateway, or the service provider session border controller needs to modify the PAT headers for packets before they reach the private networks.

The Cisco IOS[®] Session Border Controller can help in resolving this problem with a new feature: Service Provider PAT Port Allocation Enhancement for RTP and RTCP. This product bulletin outlines this new software feature.

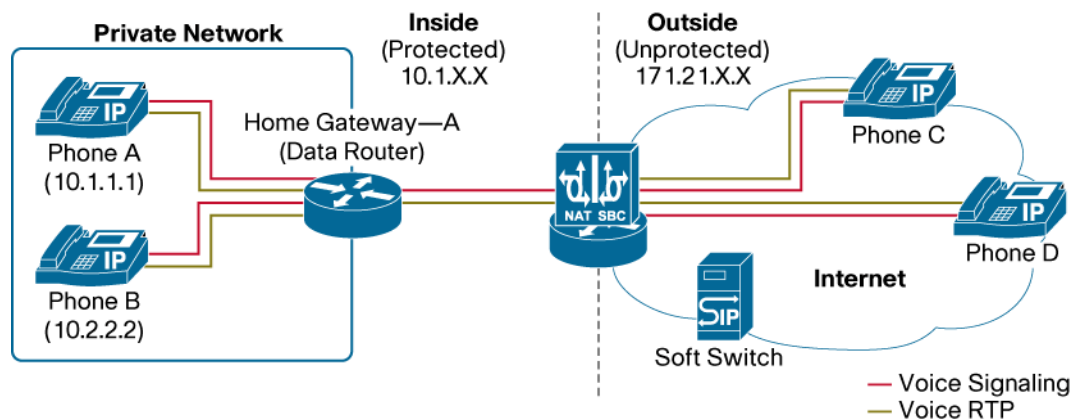
Session Border Controller Definition and PAT Traversal Solution for SIP Calls

A session border controller works with a variety of multimedia-capable network devices. It is a "toolkit" of functions, including:

- H.323 and Session Initiation Protocol (SIP) signaling interworking
- Codec translation
- NAT and PAT
- Billing and call-detail-record (CDR) normalization for authentication, authorization, and accounting (AAA)
- Quality of service (QoS) and bandwidth management

Figure 1 depicts a network scenario in which the private networks connect to the service provider's session border controller.

Figure 1. Voice Call with PAT Enhancement Network Scenario



Consider a scenario in which subscriber A in the private network makes a call to subscriber C, and that call traverses the Internet. The PAT function at the session border controller will translate the RTP port number for the call to 16384 and the RTCP port number to 16385. Subsequently, subscriber B tries to make a call to subscriber D. The PAT function tries to use the same port number 16384 that is already in use. This port is not selected and the next viable port that is picked for the call is 1024. This creates a problem since 1024 is not within the RTP port range based on RFC-1889.

The RTP RFC-1889 stipulates that an even port number be used for the RTP stream and the next subsequent odd port number be used for the corresponding RTCP stream.

Both the above issues are resolved with the new Service Provider PAT Port Allocation Enhancement for RTP and RTCP feature of the Cisco IOS Session Border Controller. This feature ensures that for SIP, H.323, and Skinny voice calls using Cisco IOS Session Border Controller, the port numbers used for RTP streams are even port numbers and the RTCP streams are the next subsequent odd port number.

With this feature, the Cisco IOS Session Border Controller gives the administrator the control to ensure that PAT-enabled voice calls will be guaranteed to get the port number translated to a number within the range specified by the RFC, thereby conforming to RFC-1889. A call with a port number within the range will result in a PAT translation to another port number within this range. Likewise, a PAT translation for a port number outside this range will not result in a translation to a number within the given range. The feature adds a CLI to provide a range that can be used to pick a port for the RTP and RTCP streams comprising a voice call using session protocols H.323, SIP, and Skinny.

The following CLI defines a portmap:

```
ip nat portmap A
  appl skinny-rtcp startport 16384 size 128
```

The port map is applied using the following CLI:

```
ip nat inside source list 1 pool inside_pool overload portmap A
```

The NAT filtering is enabled using the following CLI:

```
access-list 1 permit 192.168.100.0 0.0.0.255
```

The feature also provides a mechanism for permitting a User Datagram Protocol (UDP) packet stream using the following configuration, irrespective of the voice protocol being used:

```
ip nat portmap A
```

```
appl udp-hdr startport 16384 size 128
```

The feature ensures that for SIP, H.323, and Skinny voice calls using Cisco IOS Session Border Controller, the port numbers used for RTP streams are even port numbers and the RTCP streams are the next subsequent odd port number. This function can be disabled by using the following CLIs:

For SIP calls:

```
no ip nat service allow-sip-even-rtp-port
```

For Skinny calls:

```
no ip nat service allow-skinny-even-rtp-port
```

For H.323 calls

```
no ip nat service allow-h323-even-rtp-port
```

Feature Working on NAT Session Border Controller

Consider a private network with two IP phones, IP Phone A (10.1.1.1) and IP Phone B (10.2.2.2). The network has only one public IP address: 171.21.10.1. The network will therefore have to rely on PAT for supporting the two IP phones.

Suppose the first caller uses IP Phone A to make a voice call to Phone C. The state information, including the IP address and the port number, are used to create a pinhole with the address and port number that will be used for the RTP stream and the RTCP stream for the voice call. The information is obtained from the embedded protocol headers in the signaling packets. The PAT translation will be performed on all the RTP and RTCP packets that arrive subsequently at the session border controller.

The private address for IP Phone A is 10.1.1.1 and the port number is 16384. The configuration has the port map starting at 16500 with a range of 128. For the first call that is established, the internal address and port combination is 10.1.1.1 and 16384. The external mapping for the above combination will be 171.21.10.1 and 16500.

Now, the next caller uses IP Phone B to place a call to Phone D. The private address and port combination is 10.2.2.2 and 16384. This combination will be mapped to the external address and port combination 171.20.10.1 and 16502. Note that NAT uses the same IP address since the global IP address pool has just one IP address available.

We can observe that the two calls can use the same port number internally with the PAT feature. Table 1 shows the details of these call scenarios.

Table 1. PAT Translation Details

Call Scenario	Original		Translated	
	Private IP Address	Private Port Number	Public IP Address	Public Port Number
IP Phone A calling Phone C	10.1.1.1	16384	171.21.10.1	16500
IP Phone B calling Phone D	10.2.2.2	16384	171.21.10.1	16502

Availability

The Service Provider PAT Port Allocation Enhancement for RTP and RTCP feature is available starting with Cisco IOS Software Release 12.4(11)T.

Platforms Supported

The Cisco® products that support this feature include the Cisco AS5400XM and AS5350XM Universal Gateways, Cisco 2800 and 3800 Series Integrated Services Routers, Cisco 3700 Series Multiservice Access Routers, Cisco 7200VXR Series Routers, and the Cisco 7301 Router.

Restrictions

No known restrictions have been identified at this time.

For More Information

For information about configuring Cisco IOS Hosted NAT Traversal using Cisco IOS Session Border Controller, visit

http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a008071c4ba.html

Marketing Contacts

- Dax Choksi, product manager, Security Technology Group

**Americas Headquarters**

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

www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912

www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)