



OVERVIEW

APPLICATION LAYER GATEWAY AND TRANSLATION TYPE SUPPORT

Cisco IOS® Network Address Translation (NAT) performs translation service on any TCP/UDP traffic that does not carry source and/or destination IP addresses in the application data stream (ie: http, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh, rcp).

Specific protocols that do embed IP address information within the payload require support of an application level gateway (ALG). Table 1 details ALG support within Cisco IOS Software.

WHAT IS NEW

- Distributed Defect Tracking System (DDTS) CSCed93887: 64K IPsec NAT-T UDP sessions per Port Address Translation (PAT) IP Address
- Available in Cisco IOS Software Releases 12.3(08)XW, 12.3(08)T01, 12.3(09.10), and 12.3(09.10)T

Table 1. NAT for IPv4: ALG Support

Protocols and Applications Supported	Comments
Internet Control Message Protocol (ICMP)	<p>ICMP and PAT/Overloading Inside Address Scheme</p> <p>While conducting Port Address Translation (PAT) for ICMP traffic, the sequential numbers are associated to ports. Following is an example of the transition table, assuming continuous the ping traffic from source to destination:</p> <pre>icmp w:0 x:0 y:0 z:0 icmp w:1 x:1 y:1 z:1 icmp w:65535 x:65535 y:65535 x:65535</pre> <p>If the traffic still sustains, then the ICMP sequential numbers will rollover and start from 0. Thus, NAT would not create any new translation for this source to destination traffic).</p>
FTP PORT and PASV commands	
NetBIOS over TCP/IP (datagram, name, and session services)	
Progressive Networks' RealAudio ⁴	
White Pines' CuSeeMe	
Xing Technologies' StreamWorks	
DNS "A" and "PTR" queries	

Protocols and Applications Supported	Comments
NetMeeting 2.1, 2.11 (4.3.2519) and 3.01 (4.4.3385)	<ul style="list-style-type: none"> • H.323v2 for NetMeeting v.2.x and v3.x • H.323v1 for NetMeeting v2.x—Cisco IOS Software Releases 12.0(1) and 12.0(1)T • H.323v2 for NetMeeting v3.x—Cisco IOS Software Release 12.0(7)T
NetMeeting Directory (Internet Locator Server)	<ul style="list-style-type: none"> • Release 12.1(5)T • Set of messages using enhanced LDAPv2 implementation that enables NM users to register with and find other users through a centralized NM directory
H.323v2 —H.225/245 message types, except RAS	<ul style="list-style-type: none"> • Release 12.1(5)T • Includes FastConnect, Setup, Alerting, Facility, Progress, OpenLogicalChannel, OpenLogicalChannelAck, MCLocationIndication, CommunicationModeCommand, CommunicationModeResponse
H.323v2 RAS	<ul style="list-style-type: none"> • Release 12.2(2)T
H.323v3 and v4 in v2 Compatibility Mode	<p>Release 12.3(2)T</p> <ul style="list-style-type: none"> • Enables v3 and v4 capable devices to work properly in v2 mode • Does not support new H.323 messages introduced with either v3 or v4 • Ability to deal with: <ul style="list-style-type: none"> – Multiple messages in a single IP packet – Cases when the TPKT header and TPKT data are in different IP packets – Cases when the packet length changes after H323-ALG processing
Session Initiation Protocol (SIP)	<ul style="list-style-type: none"> • Release 12.2(8)T
Cisco's Skinny Client Control Protocol (SCCP)	<ul style="list-style-type: none"> • Release 12.1(5)T • Cisco IP Phone to Cisco Call Manager protocol • To specify a port other than the default port, on which the CCM is listening for skinny messages use the following command in global configuration mode: Router(config)# ip nat service skinny tcp port number • SCCP client to CCM typically flows from “inside” to “outside”, where the Cisco Call Manager (CCM) is on the “inside” (behind the NAT device) DNS should be used to resolve the CCM IP address to connect to. • Cisco IOS NAT supports translation of DNS A and PRT records
Real Time Streaming Protocol (RTSP)	<p>Release 12.3(7)T</p> <ul style="list-style-type: none"> • First ALG to make use of the new Common Name Based Application Recognition (CNBAR) support • Enables support for the following applications: “QuickTime, Real Audio G2, Microsoft Windows Media Technology (WMT), and Cisco IPTV”, which all make use of RTSP
VDOLive	<ul style="list-style-type: none"> • Releases 11.3(4) and 11.3(4)T
Vxtreme	<ul style="list-style-type: none"> • Releases 11.3(4) and 11.3(4)T
IP Multicast	<ul style="list-style-type: none"> • Release 12.0(1)T

Protocols and Applications Supported	Comments
PPTP support	<ul style="list-style-type: none"> • Source address translation only • Release 12.1(2)T³ • Adds support for PAT configurations <ul style="list-style-type: none"> – 1-1 NAT translation already supported • The Call Id field within the PPTP headers are included in the NAT Translation entry, in order to uniquely identify each PPTP session using the same PAT IP Address
MPLS VPN (VRF aware NAT)—Phase 1	<ul style="list-style-type: none"> • Release 12.2(13)T • NAT configured with MPLS on the MPLS Peripheral Edge (PE) device includes the VRF Table Id as part of the NAT Translation entry • The VRF Table Id allows NAT to differentiate between overlapped IP Addresses, which are common with an MPLS VPN design • NAT performs translation as it normally does • Phase 1 does not support VRF to VRF in the same PE in this initial release. • VRF to VRF in the same PE is targeted for Release 12.3(6th)T
Stateful NAT Fail-over—Phase 1	<ul style="list-style-type: none"> • Release 12.2(13)T • Phase 1 implementation <ul style="list-style-type: none"> – Two NAT routers, Primary—Backup role – Backup NAT router does not perform any NAT translations, but automatically takes over if the primary fails – Failover of external translation only – Dynamic translations are updated on the backup NAT router as they are created or deleted on the primary NAT router – No support for asymmetric routing. Must prefer active path. – Simple translations only (header translation), no ALG translations supported in this phase
Stateful NAT Fail-over—Phase 2	<p>Release 12.3(7)T</p> <ul style="list-style-type: none"> • Phase 2 implementation—new additions to Phase 1 capability <ul style="list-style-type: none"> – All translation types are supported – Asymmetric Out-to-In • Includes ALG support for FTP, H225, H245, PPTP/GRE, NetMeeting Directory (ILS), RAS, SIP (both TCP & UDP based), Skinny, TFTP, ...
Single IPsec ESP Mode tunnels in a Port Address Translation (PAT) configuration	<ul style="list-style-type: none"> • Release 12.2(1.4)Mainline • DDTS CSCdu28439 • Single IPsec ESP mode tunnel at a time, first step prior to adding support for multiple concurrent IPsec tunnels in a PAT configuration in Release 12.2(13)T • A new extended entry derived from this translation

Protocols and Applications Supported	Comments
	<ul style="list-style-type: none"> Traffic must be generated from the “inside” New CLI <pre>[no]ip nat inside source static esp <IL address> interface <Interface name></pre>
Multiple IPsec ESP Mode tunnels in a (PAT) configuration	<ul style="list-style-type: none"> Release 12.2(13)T Ability to support multiple IPsec ESP mode tunnels in a PAT/Overload configuration For IPsec peers that do not support NAT-T (UDP wrapping)
SPI Matching—Multiple IPsec ESP Mode tunnels	<p>Release 12.2(15)T</p> <ul style="list-style-type: none"> SPIs are generated by either one of end-points and box-in-middle (like NATs). They are not supposed to modify the SPIs, otherwise the other-end-point will be rejecting the session. SPIs generated at different end-points are not the same, and the box-in-the-middle has no way of co-relating them. Due to this, if multiple clients are trying to go out through NAT, it has to serialize the flow. This way, only when the response for the 1st is received the 2nd is let through. Then a SPI match is achieved.
64K IPsec NAT-T session per PAT IP Address—New FIX	<p>CSCed93887</p> <ul style="list-style-type: none"> Releases 12.3(08)XW, 12.3(08)T01, 12.3(09.10), and 12.3(09.10)T New configuration option: ‘ip nat service fullrange udp port 500’ Prior to this fix Cisco IOS PAT configuration only allowed a max of 511 concurrent IPsec VPN sessions with the NAT-T UDP Wrapper With this fix all 64K ports per IP Address are available

Table 2. NetMeeting

<p>1 NetMeeting 2.10 (4.3.2206) is supported as of 12.0(1)/12.0(1)T and in 12.1/12.1T as of DDTS CSCdr01843.</p> <p>NetMeeting 2.11 (4.3.2519) is supported as of 12.0/12.0T as of DDTS CSCdr36191 and 12.1/12.1T as of DDTS CSCdr01843</p> <p>NetMeeting 3.01 (4.4.3385) is supported in 12.1/12.1T as of DDTS CSCdr36191.</p> <p>NetMeeting 3.00 is not supported, and it’s recommend that users upgrade to the latest version of NetMeeting (currently 3.01—4.4.3385)</p> <p>2 Following capability in NetMeeting is not supported:</p> <p>NetMeeting support for Security on Data Calls</p> <p>For all hardware, NAT with support for Microsoft’s NetMeeting application requires either a ‘J’ or an ‘O’ image, enterprise feature set or Cisco IOS Firewall feature set respectively.</p> <p>3 Only payload encryption with PPTP sessions is supported with NAT. The GRE Control flows must not be encrypted in order for an Overload (Port Address Translation) configuration to work successfully</p> <p>4 Support for Progressive Networks’ RealAudio is through support for their PNA (Progressive Networks Audio) client/server protocol. It does not include support for RTSP “Real Time Streaming Protocol” at this time.</p>

Table 3. Network Address Translation (NAT) for IPv4 Translation Types and General Functionality

1-1 Static	<ul style="list-style-type: none"> IP address pools can be contiguous or non-contiguous Can configure at the source address level, and source address and port level, ex.
------------	---

	<pre>ip nat inside source static 192.168.10.1 171.69.232.209</pre> <pre>ip nat inside source static tcp 192.168.10.1 25 171.69.232.209 25</pre> <ul style="list-style-type: none"> • Network Static maps the same “host” address <pre>ip nat inside source {static {network local-network global-network mask}</pre> <pre>[extendable] [no-alias] [no-payload]</pre>
1-1 Dynamic	<ul style="list-style-type: none"> • Can be applied to “inside” or “outside” traffic • Once a session matches the NAT configuration, an address translation will select an address dynamically from the appropriate pool • IP address pools can be contiguous or non-contiguous
Port Address Translation (PAT)	<ul style="list-style-type: none"> • PAT capability is available in all NAT images • Multiplexes users and IP sessions over 1 or more IP Addresses • One or more IP Addresses can be used as input to overload on to • Applies a unique source port to uniquely identify and differentiate between inside users • Theoretically, 65535 source ports are available; however, specific and known ports for applications and protocols understood by Cisco IOS Nat are set aside • IP Address can be statically configured in the case of a pool used by PAT, however the majority of customers use a dynamically configured IP Address from PPP or DHCP, in this case NAT is configured to use the interfaces name
Bi-Directional (Overlapping) NAT	<ul style="list-style-type: none"> • Requires DNS on either one of sides • Enables networks that both use the same addressing scheme to inter-connect • Cisco IOS NAT supports translation of DNS A and PTR record types
Destination Based NAT'ing using Route Maps	<ul style="list-style-type: none"> • The dynamic translation command can now specify a route-map to be processed instead of an access-list. A route-map allows the user to match any combination of access-list, next-hop IP address, and output interface to determine which pool to use: http://www.cisco.com/warp/public/105/nat_routemap.html
Route-maps with 1-1 Static NAT Translations	<ul style="list-style-type: none"> • Release 12.2(4)T • DDTS CSCdr52161 • Adds the ability to have NAT multi-homing capability with Static address translations • Previously Cisco IOS NAT supported multi-homing through route-maps and dynamic address pool configuration • Static NAT statements could not accept configurations, such as the following one: <pre>ip nat inside source static route-map XXX <ip-address></pre>
Inside Destination NAT'ing	<ul style="list-style-type: none"> • Load balancing TCP sessions to multiple “inside” servers • Only applicable when configured in a PAT (Overload) scenario
Autoaliasing of Pool Address	<p>Many customers want to configure Cisco IOS NAT to translate their local addresses to global addresses allocated from unused addresses from an attached subnet. This requires that the router answer ARP requests for those addresses so that packets destined for the global addresses are accepted by the router and translated. (Routing takes care of this packet delivery when the global addresses are allocated from a virtual network which isn't connected to anything.)</p> <p>When a NAT pool used as an inside global or outside local, then the pool consists of addresses on an attached</p>

	<p>subnet, and the software will generate an alias for that address so that the router will answer ARPs for those addresses.</p> <p>This automatic aliasing also occurs for inside global or outside local addresses in static entries. It can be disabled for static entries with the “no-alias” keyword:</p> <pre>ip nat inside source static <local-ip-address> <global-ip-address> no-alias</pre>
NAT MIB	<p>Release 12.2(13)T</p> <ul style="list-style-type: none"> • Cisco co-authored draft • Provides information on: <ul style="list-style-type: none"> – NAT configuration – NAT Timer settings – Pool configuration – Translation Table details • Definitions of Managed Objects for Network Address Translators (NAT): http://www.ietf.org/internet-drafts/draft-ietf-nat-natmib-09.txt
Host Number Preservation	<p>For ease of network management, some sites prefer to translate prefixes, rather than addresses. In other words, they wish the translated address to have the same host number as the original address. Of course, the two prefixes must be of the same length. This feature can be enabled by configuring dynamic translation as usual, but configuring the address pool to be of type “match-host:”</p> <pre>ip nat pool fred <start> <end> prefix-length <len> type match-host</pre>
Translation Entry Limit	<ul style="list-style-type: none"> • Can specify a maximum number of NAT translation entries allowed • Global to NAT within the router
Rate limiting NAT Translation	<ul style="list-style-type: none"> • Release 12.3(4)T • Note: ‘All-hosts’ component of this enhancement will be available with CSCec16330 in Release 12.3T • The enhancement allows customers to configure a NAT Rate Limiting hierarchy within each NAT router: <ul style="list-style-type: none"> – Maximum number of concurrent translations for the router – Maximum number of concurrent translations applied to each MPLS VPNs (assumed that router is a part of MPLS network) – Maximum number of concurrent translations for an individual MPLS VPNs (assumed that router is a part of MPLS network) – Maximum number of concurrent translations applied to an ACL <ul style="list-style-type: none"> • ACL might be used to describe a specific subnet to apply this maximum to, a specific prefix list, or prefix lists • Rate limiting can be applied to multiple ACLs with the router – Maximum number of concurrent translations applied to all IP Hosts (All-hosts) transiting the router

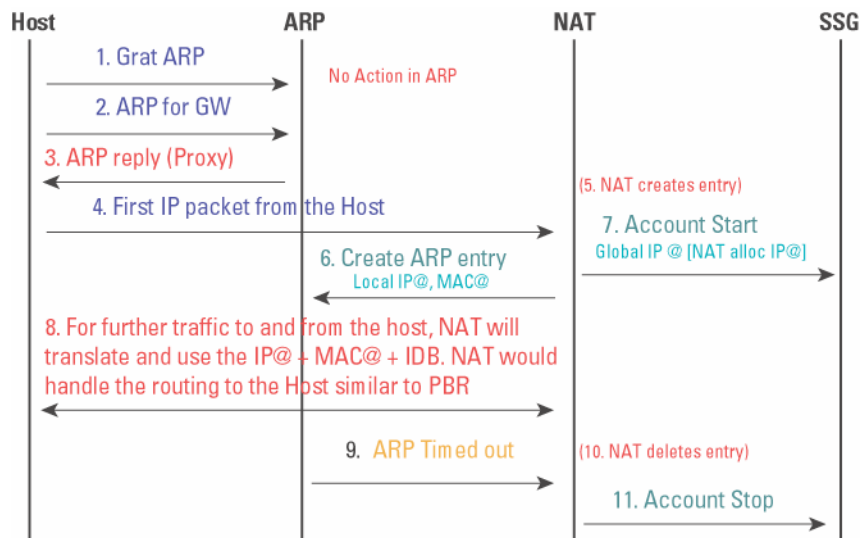
	<ul style="list-style-type: none"> – Maximum number of concurrent translations for an individual IP Host. This value will override the ‘All-hosts’ maximum if configured for the specific IP host
NAT Timers	<ul style="list-style-type: none"> • When port translation is configured, there is finer control over translation entry timeouts, because each entry contains more context about the traffic using it. • Non-DNS UDP translations time-out after five minutes • DNS times out in one minute • TCP translations time out after twenty-four hours, unless a RST or FIN is seen on the stream, in which case it times out in one minute • ICMP flows default is one minute (available with extended translation entries) • Synchronous (SYN) default is one minute (available with extended translations) <pre>ip nat translation udp-timeout seconds</pre> <pre>ip nat translation dns-timeout seconds</pre> <pre>ip nat translation tcp-timeout seconds</pre> <pre>ip nat translation finrst-timeout seconds</pre> <pre>ip nat translation icmp-timeout seconds</pre> <pre>ip nat translation syn-timeout seconds</pre>
Writing NAT Translations to the Syslog	<ul style="list-style-type: none"> • Release 12.2(1.4) • DDTS CSCdp81712 • New NAT CLI command to enable or disable logging of all NAT translations created and removed to the Syslog <pre>[no] ip nat log translations syslog</pre> <p>Specify the necessary syslog commands (ie: server’s IP address). If you do not want to see messages on the console, configure “no logging console”. This will enable only the syslog server to log information.</p> <p>The format of NAT information logged will be (for example, for ICMP Ping via NAT Overload configs) :</p> <pre>Apr 25 11:51:29 [10.0.19.182.204.28] 1: 00:01:13: NAT:Created icmp 135.135.5.2:7 171 12.106.151.30:7171 54.45.54.45:7171 54.45.54.45:7171</pre> <pre>Apr 25 11:52:31 [10.0.19.182.204.28] 8: 00:02:15: NAT:Deleted icmp 135.135.5.2:7 172 12.106.151.30:7172 54.45.54.45:7172 54.45.54.45:7172</pre> <p>There is no functionality change via the feature. The logging of NAT translations can be enabled/disabled via syslog.</p>
Static NAT support with HSRP	<ul style="list-style-type: none"> • Release 12.2(2)T • DDTS CSCdt23430 • When “triggering” an ARP entry for a NAT’d address, NAT should use the HSRP Virtual MAC address if HSRP is configured on the interface to which the ARP will point. This will ensure that the upstream devices will point to the new HSRP Active router during a failure of the Active HSRP router when a cut-over occurs. The ARP entry will not point to the original Active router, which may no longer be available. <ul style="list-style-type: none"> – Assumes NAT is mirrored on these 2 or more HSRP routers

	<ul style="list-style-type: none"> – No NAT State will be exchanged between these routers running NAT in an HSRP group
Header-only translation with NAT	<ul style="list-style-type: none"> • Release 12.2(4)T • DDTS CSCds57685 • Configure Cisco IOS NAT to only apply translation rules to the external IP Address and Ports, and ignore all IP addresses and ports embedded in the payload and negotiated by the protocol • Global to NAT in the router, cannot be configured per ALG
Cisco Express Forwarding and Outside translations	<p>If there is no adjacency for the destination address, Cisco Express Forwarding punts it to process switching for ARP. Since the “outside” mapping is a translatable address for packets going from inside to outside, ARP for the destination address and hence the adjacency never gets populated.</p> <p>This causes Cisco Express Forwarding to drop few packets and whatever they punt to process switching. The workarounds for this are:</p> <ul style="list-style-type: none"> • To have the “add_route” configured with outside source static • To have next-hop instead of interface for the static route/default-network <p>Note: The “add_route” command is strongly discouraged for overlapping network scenario</p>
Performance enhancements	<ul style="list-style-type: none"> • Release 12.3(4)T • Collection of enhancements aimed at improving overall performance of the NAT feature within Cisco IOS Software <ul style="list-style-type: none"> – Optimized CPU utilization—taking longer to ramp to higher CPU percentages <ul style="list-style-type: none"> Will vary based on the IP type of traffic inspected by NAT Specific hardware is in question Other features active within the router – Improved throughput when using NAT • The specific enhancements are: <ul style="list-style-type: none"> – Support for Cisco Express Forwarding <ul style="list-style-type: none"> TCP Flags—SYN, FIN, and RST now handled in Cisco Express Forwarding Translation entry creation in the Cisco Express Forwarding path under – Support for Cisco Express Forwarding – Translation table optimization <ul style="list-style-type: none"> Improved creation and searching of translations Pool and Port List optimization – Support of Fragmented Packets

Static IP configured users

- Release 12.3(7)T:
[NAT—Static IP Support](#)
- Enables Static IP users to be mapped automatically to an IP Address from the NAT pool without requiring them to re-configure their device
- This enhancement is primarily for markets involved in IP Mobility (IP roaming). Those markets might have users who are not using DHCP for dynamic IP addressing
- Allows users that have been configured with Static IP Addresses to “roam” into a Public WLAN “hot spot”, to connect to the network, and to use it
- No requirement to configure each individual Static IP user
- NAT Dynamic IP Address pools can be used to allocate a routable IP address
- Duplicate (or overlapped) Static IP users connecting to the same router are not supported
- When enabled, NAT is triggered by the sequence of events from the Static IP user and works with ARP to ensure that Static IP user is able to connect
- NAT will provide a Global/Routable IP Address to the Static IP user, ensuring reach-ability to the client from the outside
 - NAT will create a translation entry for each Static IP user
 - NAT works with ARP to write the ARP entry for this user
 - This ARP entry is “locked” and will not be modified with the exception of removal by NAT, when the associated NAT translation entry is removed

Figure 1
Static IP: NAT with ARP



**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.

©2007 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, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, 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. (0705R)

© 2007 Cisco Systems, Inc. All rights reserved.

Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com