Contents

- 1 Welcome to the "Network Address Translation (NAT)" Wiki Page
  - 1.1 NAT Deployment Guide
  - 1.2 NAT Best Practices
  - 1.3 NAT FAQ
    - 1.3.1 Generic NAT
    - 1.3.2 Voice-NAT
    - 1.3.3 NAT with VRF/MPLS
    - 1.3.4 NAT NVI
    - 1.3.5 SNAT
    - 1.3.6 NAT-PT (v6<->v4)
    - 1.3.7 Platform Dependent

Welcome to the "Network Address Translation (NAT)" Wiki Page

NAT Deployment Guide

Implementing NAT
NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT translates the private (RFC1918) address in the internal network into legal routable addresses before packets are forwarded onto another network.

For more information about implementing NAT, please see Configuring NAT for IP Address Conservation

Implementing NAT and Voice

The NAT Support for Voice feature allows SIP embedded messages passing through a router configured with Network Address Translation (NAT) to be translated back to the packet. An application layer gateway (ALG) is used with NAT to translate the Voice packets. For more information about implementing NAT with Voice. please see NAT Support for ALGs

NAT Integration with MPLS VPN's
The NAT Integration with MPLS VPNs feature allows multiple MPLS VPNs to be configured on a single device to work together. NAT can differentiate which MPLS VPN it receives IP traffic from even if the MPLS VPNS are all using the same IP addressing scheme. This enhancement enables multiple MPLS VPN customers to share services while ensuring that each MPLS VPN is completely separate from the other. For more information please see NAT Integration with MPLS VPNs and Integrating NAT with MPLS VPNs.

NAT - Static Mapping Support with HSRP for High Availability

When an Address Resolution Protocol (ARP) query is triggered for an address that is configured with Network Address Translation (NAT) static mapping and owned by the router, NAT responds with the BIA MAC address on the interface to which the ARP is pointing. Two routers are acting as HSRP active and standby. Their NAT inside interfaces must be enabled and configured to belong to a group.For more information, please see NAT - Static Mapping Support with HSRP for High Availability .

Implemeting NAT NVI

The NAT Virtual Interface (NVI) feature removes the requirement to configure an interface as either Network Address Translation (NAT) inside or NAT outside.

For more information about NAT NVI, please see Configuring the NAT Virtual Interface

Implementing Load-balancing with NAT

There are two kinds of load-balancing that can be done with NAT. You can load balance inbound to a set of Servers to distribute the load on the servers and you can load balance your user traffic to the Internet over 2 or more ISP's.

For more information about inbound load balancing please see Avoiding Server Overload Using TCP Load Balancing

For more information about outbound load balancing, please see IOS NAT Load-Balancing for Two ISP Connections

Implementing NAT in conjucntion with IPSEC

There is support for IPSec ESP through NAT and IPSec NAT Transparency.

The IPSec ESP through NAT feature provides the ability to support multiple concurrent IP Security (IPSec) Encapsulating Security Payload (ESP) tunnels or connections through a Cisco IOS Network Address Translation (NAT) device configured in Overload or Port Address Translation (PAT) mode. Please see Support for IPSec ESP Through NAT and NAT Support for IPSec ESP - Phase II for more information about this feature.

The IPSec NAT Transparency feature introduces support for IP Security (IPSec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network by addressing many known incompatabilites between NAT and IPSec. Please see IPSec NAT Transparency for more information about this feature.

Implementing NAT-PT

Network Address Translation?Protocol Translation (NAT-PT) is an IPv6-IPv4 translation mechanism, as defined in RFC 2765 and RFC 2766, allowing IPv6-only devices to communicate with IPv4-only devices and vice versa. Please see Implementing NAT-PT for IPv6 for more information about implementing and configuring NAT-PT.

Implementing Multicast NAT

It is possible to NAT the source ip for a multicast stream. A route-map can not be used when doing dynamic NAT for Multicast, only an access list is supported for this. For more information, please see How Does Multicast NAT Work on Cisco Routers?. The destination multicast group is natted using a Multicast Service Reflection solution.

Implementing Stateful NAT (SNAT)

SNAT enables continuous service for dynamically mapped NAT sessions. Sessions that are statically defined receive the benefit of redundancy without the need for SNAT. In the absence of SNAT, sessions that use dynamic NAT mappings would be severed in the event of a critical failure and would have to be reestablished. Only the minimal SNAT configuration is supported. Future deployments should only be done after talking to your Cisco Account Team to validate the design relative to current restrictions.

For more information about implementing SNAT, please see Configuring NAT for High Availability

SNAT is recommended for the following :
? HSRP mode as described in the SNAT white-paper: Enhanced IP Resiliency Using Cisco Stateful NAT
? Primary / Backup is not a recommended mode since there are some features missing compared to HSRP.
? For fail-over scenarios and for 2 router setup. Meaning if one router crashes, the other router takes over seamlessly. (Interface-flaps aren't something which SNAT architecture is designed to handle).
? Non-asymmetric routing scenario is supported. Asymmetric routing can be handled only if the latency in the reply packet is higher than that between 2 SNAT routers to exchange the SNAT messages.
Currently SNAT architecture is not designed to handle robustness and so below tests are not expected to succeed:
? Clearing NAT entries while traffic is going on.
? Changing interface parameters (like ip-address change, shut / no-shut, etc) while traffic is going on .
? SNAT specific clear or show CLIs aren't expected to execute properly and not recommended.
? Some of the SNAT related clear and show commands are as follows :
clear ip snat sessions *
clear ip snat sessions <ip address of the peer >
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>

? If the user wishes to clear entries the standard "clear ip nat trans forced" or "clear ip nat trans *" can be used or if the user wishes to see entries, commands like "show ip nat translation", "show ip nat translations verbose" & "show ip nat stats", can be used. If "service internal" is configured, it will show SNAT specific information as well.
? Clearing NAT translations at the back up router is not recommended. Always clear the NAT entries on the primary SNAT router.
? SNAT is not HA , so configs on both routers should be the same. Both routers should have the same image running and also make sure that underlying platform used for both the SNAT routers are the same.

NAT Best Practices

1. When doing both dynamic and static NAT, the ACL that sets the rule for dynamic NAT should exclude the static local hosts so there is no overlap.

2. Beware of using ACL for NAT with "permit ip any any" as you can get unpredictable results. After 12.4(20)T NAT will translate locally generated hsrp and routing protocol packets if they are sent out the "ouside" interface, as well as locally encrypted packets matching the NAT rule.

3. When you have overlapping networks for NAT, use "Match-in-vrf".

You must add "match-in-vrf" keyword for the overlapping vrf static NAT entries for different vrfs but it is not possible to overlap global and vrf NAT addresses.

72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf

72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf

4. NAT pools with same address range can?t be used in different VRFs unless MATCH-IN-VRF keywords is used.

For example:

```
ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24
ip nat pool poolB 171.1.1.1 171.1.1.10 prefix-length 24
ip nat inside source list 1 poolA vrf A match-in-vrf
ip nat inside source list 2 poolB vrf B match-in-vrf
```

NOTE: without MATCH-IN-VRF keyword and even though CLI configuration is valid, it?s unsupported configuration.

5. When deploying ISPs load balancing with NAT interface overload, it?s best practice to use route-map with interface match over ACL matching.

6. When using pool mapping, it?s not recommended to use 2 different mapping (ACL or route-map) to share the same NAT pool address.

7. When deploying the same NAT rules on 2 different routers in the failover scenario, it?s recommend to use HSRP redundancy.

NAT FAQ

Generic NAT

Q1. What is NAT?

A1. Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network. As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation, and is typically implemented in remote-access environments.

Q2. How does NAT work?

A2. Basically, Network Address Translation allows a single device, such as a router, to act as agent between the Internet (or "public network") and a local (or "private") network. This means that only a single unique IP address is required to represent an entire group of computers to anything outside their network. Please read How NAT Works for more information.

Q3: How do I configure NAT?

A3: To configure traditional NAT, you need to make at least one interface on a router "NAT Outside" and another interface on the router "NAT Inside" and a set of rules for translating the IP addresses in the packet headers (and payloads as well if desirable) need to be configured. To configure Nat Virtual Interface (NVI), you need at least one interface configured with "NAT enable" along with the same set of rules as mentioned above.

For more information, please see the NAT Configuration Guide or the Configuring the NAT Virtual Interface .

Q4. What are the main differences between the Cisco IOS® Software and Cisco® PIX® Security Appliance implementations of NAT?

A4. Cisco IOS Software-based NAT is not fundamentally different from the NAT function in the Cisco PIX Security Appliance. The main differences involve the different traffic types supported in the implementations. Refer to Cisco PIX 500 Series Security Appliances and NAT Configuration Examples for more information on the configuration of NAT on Cisco PIX devices (includes the traffic types supported).

Q5. On which Cisco routing hardware is Cisco IOS NAT available? How can the hardware be ordered?

A5. The Cisco Feature Navigator tool allows customers to identify a feature (NAT) and find which release and hardware this Cisco IOS Software feature is available on. To use this tool, please go to Cisco Feature Navigator.

Q6. Does NAT occur before or after routing?
A6. The order in which the transactions are processed using NAT is based on whether a packet is going from the inside network to the outside network, or from the outside network to the inside network. Inside to outside translation occurs after routing, and outside to inside translation occurs before routing.
For more information, visit NAT Order of Operation.

Q7. Can NAT be deployed in a Public Wireless LAN environment?

A7. Yes, the NAT - Static IP Support feature provides support for users with static IP addresses, enabling those users to establish an IP session in a Public Wireless LAN environment. Please see NAT - Static IP Support for more information about this feature.

Q8. Does NAT do TCP load-balancing for Servers on the internal Network?

A8. Yes, using NAT, you can establish a virtual host on the inside network that coordinates load sharing among real hosts. Please see TCP Load Distribution for NAT for more information.

Q9. Can I rate-limit the number of NAT translations?
A9. Yes, the Rate Limiting NAT Translation feature provides the ability to limit the maximum number of concurrent network address translation (NAT) operations on a router. In addition to giving users more control over how NAT addresses are used, the Rate Limiting NAT Translation feature can be used to limit the effects of viruses, worms, and denial-of-service attacks. For more information, please see Rate Limiting NAT Translation.

Q10. How is routing learned or propagated for IP subets or addresses that are used by NAT?
A10. Routing for IP addresses created by NAT is learned if:

? The inside global address pool is derived from the subnet of a next-hop router

? Static route entry is configured in the next-hop router and redistributed within the routing network

When Inside Global address is matched with the local interface, NAT will install an IP Alias and an ARP entry, in which case trhe router will proxy-arp for thise addresses.
If this behavior is not wanted, use the "no-alias" keyword.

When a NAT pool is configured, the ?add-route? option can be used for automatic route injection.

Q11. How many concurrent NAT sessions are supported in Cisco IOS NAT?
A11. The NAT session limit is bounded by the amount of available DRAM in the router. Each NAT translation consumes about 312 bytes in DRAM. As a result, 10,000 translations (more than would generally be handled on a single router) would consume about 3 MB. Therefore, typical routing hardware has more than enough memory to support thousands of NAT translations.

Q12. What kind of routing performance can be expected when using Cisco IOS NAT?
A12. Cisco IOS NAT supports Cisco Express Forwarding switching, fast switching, and process switching. For 12.4T release and later, fast switching-path is no longer supported.
For Cat6k platform, the switching order is Netflow (HW switching path), CEF, Process Path.

Performance depends on several factors:
? The type of application and its type of traffic

? Whether IP addresses are embedded

? Exchange and inspection of multiple messages

? Source port required

? The number of translations

? Other applications running at the time

? The type of hardware and processor

Q13. Can Cisco IOS NAT be applied to subinterfaces?
A13. Yes. Source and/or destination NAT translations can be applied to any interface or subinterfaces having an IP address (including dialer interfaces). NAT cannot be configured with Wireless Virtual Interface. Wireless Virtual Interface doesnot exist at the time of writing to NVRAM. Thus, after reboot, the router will loose NAT configuration on the Wireless Virtual Interface.

Q14. Can Cisco IOS NAT be used with Hot Standby Router Protocol (HSRP) to provide redundant links to an ISP?
A14.) Yes, NAT does provide HSRP redundant. However, this is different from SNAT (Stateful NAT). NAT with HSRP is a stateless system. The current session is not maintained when failure taken place. Static NAT configuration, when packet doesn?t matched with any STATIC rule configuration, packet will be sent through without any translation. Please see NAT - Static Mapping Support with HSRP for High Availability

for more information about this feature.

Q15. Does Cisco IOS NAT support inbound translations on a Frame Relay interface? Does it support outbound translations on the Ethernet side?
A15. Yes, encapsulation does not matter for NAT. NAT can be done where there is an IP address on an interface and the interface is NAT inside or NAT outside. There must be an inside and an outside for NAT to function. If you are using NVI, there most be at least one NAT enabled interface. Please see **Q3** for more details.

Q16. Can a single NAT-enabled router allow some users to use NAT and other users on the same Ethernet interface to continue with their own IP addresses?
A16. Yes. This can be accomplished through the use of an access list describing the set of hosts or networks that require NAT. All sessions on the same host will either be translated or will pass through the router and not be translated. Access lists, extended access lists, and route maps can be used to define "rules" by which IP devices get translated. The network address and appropriate subnet mask should always be specified. The keyword "any" should not be used in place of the network address or subnet mask (see NAT Best Practices for more detail). With Static NAT configuration, when packet doesn?t matched with any STATIC rule configuration, packet will be sent through without any translation.

Q17. When configuring for PAT (overloading), what is the maximum number of translations that can be created per inside global IP address?
A17. PAT (overloading) divides the available ports per global IP address into three ranges: 0-511, 512-1023, and 1024-65535. PAT assigns a unique source port for each UDP or TCP session. It will attempt to assign the same port value of the original request, but if the original source port has already been used, it will start scanning from the beginning of the particular port range to find the first available port and will assign it to the conversation. There is an exception for 12.2S code base. 12.2S code base uses different port logic and there is no port reservation.

Q18. How does PAT work?
A18. PAT works with either one global IP address or multiple addresses.

- **PAT with one IP address:**

1. NAT/PAT inspects traffic and matches it to a translation rule.

2. Rule matches to a PAT configuration.

3.If PAT knows about the traffic type, and that traffic type has "a set of specific ports or ports it negotiates" that it will use, PAT sets them aside and does not allocate them as unique identifiers.

4.If a session with no special port requirements attempts to connect out, PAT translates the IP source address and checks availability of the originated source port (433, for example).

Note: For Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), the ranges are: 1-511, 512-1023, 1024-65535. For Internet Control Message Protocol (ICMP), the first group starts at 0.

5. If the requested source port is available, PAT assigns the source port, and the session continues.

6. If the requested source port is not available, PAT starts searching from the beginning of the relevant group (starting at 1 for TCP or UDP applications, and from 0 for ICMP).

7. If a port is available it is assigned, and the session continues.

8. If no ports are available, the packet is dropped.

- **PAT with multiple IP addresses**:

1-7. The first seven conditions are the same as with a single IP address.

8. If no ports are available in the relevant group on the first IP address, NAT moves on to the next IP address in the pool and tries to allocate the original source port requested.

9. If the requested source port is available, NAT assigns the source port and the session continues.

10. If the requested source port is not available, NAT starts searching from the beginning of the relevant group (starting at 1 for TCP or UDP applications, and from 0 for ICMP).

11. If a port is available, it is assigned and the session continues

12. If no ports are available, the packet is dropped, unless another IP address is available in the pool.

Q19. What are NAT IP pools?
A19. NAT IP pools are a range of IP addresses that are allocated for NAT translation as needed. To define a pool, the configuration command is used:

ip nat pool <name> <start-ip> <end-ip> { netmask <netmask> | prefix-length <prefix-length> } [type { rotary }]

Example 1.

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Example 2.

In the following example, the goal is to define a virtual address, connections to which are distributed among a set of real hosts. The pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial interface 0 (the outside interface) whose

destination matches the access list are translated to an address from the pool.

ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1

Q20. What is the maximum number of configurable NAT IP pools (ip nat pool "name")?
A20. In practical use, the maximum number of configurable IP pools is limited by the amount of available DRAM in the particular router. It is highly recommended that a pool of size 255 is configured.) It?s recommended that each pool to be no more than 16 bits. In 12.4(11)T and later, IOS introduce CCE (Common Classification Engine). This has limited NAT to only have maximum 255 pools. In 12.2S code base, there is no maximum pools restriction

Q21. What is the advantage of using route-map vs ACL on a NAT pool?
A21. *A r*oute-map is protecting unwanted outside users to reach to the inside users/servers. It also has the capability to map a single inside IP address to different Inside Global addresses based on the rule. Please see NAT Support for Multiple Pools Using Route Maps for more information.

Q22. What is IP address "overlapping" within the context of NAT?
A22. IP address overlapping refers to a situation where two locations that want to interconnect are both using the same IP address scheme. This is not an unusual occurrence; it often happens when companies merge or are acquired. Without special support, the two locations will not be able to connect and establish sessions. The overlapped IP address can be a public address assigned to another company, a private address assigned to another company, or can come from the range of private addresses as defined in RFC 1918. Private IP addresses are unroutable and require NAT translations to allow connections to the outside world. The solution involves intercepting Domain Name System (DNS) name-query responses from the outside to the inside, setting up a translation for the outside address, and fixing up the DNS response before forwarding it to the inside host. A DNS server is required to be involved on both sides of the NAT device to resolve users wanting to have connection between both networks.

NAT is able to inspect and perform address translation on the contents of DNS "A" and "PTR" records, as shown in Using NAT in Overlapping Networks.

Q23. What are static NAT translations?
A23. Static NAT translations have one-to-one mapping between local and global addresses. Users can also configure static address translations to the port level, and use the remainder of the IP address for other translations. This typically occurs where you are performing Port Address Translation (PAT).

The following example shows how to configure routemap to allow outside-to-inside translation for static NAT:

ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A

Q24. What is meant by the term NAT "overloading", is this PAT?

A24. Yes, NAT "overloading" is PAT. This involves using a pool with a range of one or more addresses or using an interface IP address in combination with the port. When you overload, you create a fully extended translation, this is a translation table entry containing IP address and source/destination port information. This is commonly called PAT or overloading, this is a feature of Cisco IOS NAT that is used to translate "internal" (inside local) private addresses to one or more "outside" (inside global, usually registered) IP addresses. Unique source port numbers on each translation are used to distinguish between the conversations.

Q25. What are dynamic NAT translations?
A25. In dynamic NAT translations, the users can establish dynamic mapping between local and global addresses. This is done by defining the local addresses to be translated and the pool of addresses or interface IP address from which to allocate global addresses, and associating the two.

Q26. What is ALG?

A26. ALG is an Application Layer Gateway (ALG). Network Address Translation (NAT) performs translation service on any Transmission Control Protocol/User Datagram Protocol (TCP/UDP) traffic that does not carry source and/or destination IP addresses in the application data stream.

These protocols include FTP, HTTP, SKINNY, H232, DNS, RAS, SIP ,TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh, rcp. Specific protocols that do imbed IP address information within the payload require support of an Application Level Gateway (ALG).

Please see Using Application Level Gateways with NAT for more information.

Q27. Is it possible to build a configuration with both static and dynamic NAT translations?
A27. Yes, but the same IP address cannot be used for the NAT static configuration and In the pool for NAT dynamic configuration. All the Public IP address needs to be unique. Note that the global addresses used in static translations are not automatically excluded with dynamic pools containing those same global addresses. Dynamic pools have to be created to exclude addresses assigned by static entries. For more information, please see Configuring Static and Dynamic NAT Simultaneously .

Q28. When a Traceroute is done through a NAT router, should traceroute show the NAT-Global address or should it leak the NAT-Local address?

'*A28.*' *Traceroute from outside should always give the Global address.*
'**Q29.***How does PAT allocate port?*

A29.*NAT also introduces additional port features, full-range and port-map.*
- Full-range allows NAT to use all ports regarless of its default port range.
- Port-map allows NAT to reserve a user define port range for specific application User Defined Source Port Ranges for PAT

In 12.4(20)T2 onward, NAT introduces port randomization for L3/L4 and symmetric-port.
- Port Randomization allows NAT to randomly select any global port for the source port request.
- Symmetric-port allows NAT to support for "endpoint independent", please see Anatomy: A Look Inside Network Address Translators for more information.

Q30. What is the different between IP Fragmentation and TCP Segmentation?

A30. IP fragmentation occurs at Layer 3 (IP) and that TCP segmentation occurs at Layer 4 (TCP). IP Fragmentation takes place when packets that are larger than the Maximum Transmission Unit (MTU) of an interface are sent out this interface. These packets will have to be either fragmented, or discarded when they are sent out the interface. If the Don't Fragment (DF) bit is not set in the IP header of the packet, the packet will be fragmented. If the DF bit is set in the IP header of the packet, the packet is dropped and an ICMP error message indicating the next-hop MTU vlaue will be returned to the sender. All the fragments of an IP packet carry the same Ident in the IP header, this allows the final receiver to reassemble the fragments into the original IP packet. Please see Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC for more information.

TCP Segmentation takes place when when an application on an end station is sending data. The application data is broken into what TCP considers the best-sized chunks to send. This unit of data passed from TCP to IP is called a segment. TCP segments are sent in IP datagrams. These IP datagrams can then become IP Fragments as they pass through the network and encounter lower MTU links than they can fit through.

TCP will first segment this data into TCP segments (based on TCP MSS value) and will add the TCP header and pass this TCP segment to IP. Then IP will add an IP header to send the packet to the remote end host. If the IP packet with the TCP segment is larger than the IP mtu on an outgoing interface on the path between the TCP hosts then IP will fragment the the IP/TCP packet in order to fit. These IP packet fragments will be reassembled on the remote host by the IP layer and the complete TCP segment (that was originally sent) will be handed to the TCP layer. The TCP layer has no idea that IP had fragmented the packet during transit.

NAT can deal with IP fragments but it does not deal with TCP Segments.

Q31. Does NAT support Out-of-Order for IP Fragmentation and TCP Segmentation?

A31. NAT can only deal with out-of-order IP Fragments and this is because of " ip virtual-reassembly".

Q32. How to debug IP Fragmentation and TCP Segmentation?
A32. NAT uses the same debug CLI for both IP Fragmentation and TCP Segmentation: ?debug ip nat frag?

Q33. Is there a supported NAT MIB?
A33. No, there in no supported NAT MIB.

Q34. What is 'TCP Timeout' and how does it relate to the NAT TCP Timer?
A34. If the three way handshake is not completed, and NAT sees a TCP packet, then NAT will start 60

second timer. When the three way handshake is completed, NAT by default uses a 24 hour timer for a NAT entry. If end-host sends a RESET then NAT will change the default timer from 24 hours to 60 seconds. In the case of FIN, only when NAT will receive FIN and FIN-ACK, it will change the default timer from 24 hours to 60 seconds.

Q35. Can I change the amount of time it takes for a NAT tranlation to time out from the NAT tranlation table?
A35. Yes, you can change the NAT timeout values for all entries or for different types of NAT tranlations ;like udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout and arp-ping-timeout. For more information about changing the default values for these timeout settings, please see ip nat translation (timeout).

Q36. How do I stop Lightweight Directory Access Protocol (LDAP) from attaching extra bytes to each LDAP reply packet?
A36. The LDAP settings are such that they will add the extra bytes (LDAP search results) while processing messages of type Search-Res-Entry. LDAP attaches 10 bytes of search results to each of LDAP reply packet. In the event that this 10 extra bytes of data result in the packet exceeding the Maximum Transmission Unit (MTU) in a network and getting dropped. In this case, it is recommended to turn off this LDAP behavior using the CLI "no ip nat service append-ldap-search-res" in order for the packets to be sent and received.

Voice-NAT

Q37. Does NAT support Skinny Client Control Protocol (SCCP) v17 which is shipped with Cisco Unified Communications Manager (CUCM) V7?

A37. CUCM 7 and all of the default phone loads for CUCM 7 support SCCPv17. The SCCP version used is determined by the highest common version between CUCM and the phone when the phone registers. NAT does not yet support SCCP v17. Until NAT support for SCCP v17 is implemented, the firmware must be downgraded to version 8-3-5 or below so that SCCP v16 is negotiated. CUCM6 will not encounter the NAT problem with any phone load as long as it uses SCCP v16. IOS does not currently support SCCP version 17.

Q38. Which CUCM /SCCP/Firmware load versions are supported by NAT?

A38. CUCM version 6.x and early CUCM releases come with default 8.3.x or early phone firmware load supports SCCP v15 or below, hence is supported by NAT.

CUCM version 7.x or after come with default 8.4.x phone firmware load supports SCCP v17, hence not supported by NAT. If CUCM 7.x or above is used, an older firmware load will have to put on the CUCM TFTP server so phones use a firmware load with SCCP v15 or below in order to be supported by NAT.

The link below confirms that firmware load 8.3.x contains SCCP v15 or below and will work with NAT and that Firmware load 8.4.x contains SCCP v17 and will NOT work with NAT.
http://third-gen-phones.gforge.cisco.com/twiki/prod/bin/view/Thirdgenphones/CCMLoadNumberAndCodeNameDecoderI

For more information about NAT and SCCP, please see NAT-Support of IP Phone to Cisco CallManager.

Q39. What is Service Provider PAT Port Allocation Enhancement for RTP and RTCP?
A39. The Service Provider PAT Port Allocation Enhancement for RTP and RTCP feature ensures that for SIP, H.323, and Skinny voice calls. The port numbers used for RTP streams are even port numbers and the RTCP streams are the next subsequent odd port number. The port number is translated to a number within the range specified 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.

Refer to Service Provider PAT Port Allocation Enhancement for RTP and RTCP for more information.

Q40. What is Session Initiation Protocol (SIP) and can SIP packets be NATTed?
A40. Session Initiation Protocol (SIP) is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. SIP is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. The Cisco SIP implementation enables supported Cisco platforms to signal the setup of voice and multimedia calls over IP networks. For more information, visit
Overview of SIP. SIP packets can be NATTed, for more information please see NAT Support for SIP and NAT Support of H.323 v2 RAS.

Q41. What is Hosted NAT Traversal support for Session Border Controller (SBC)?
A41. The Cisco IOS Hosted NAT Traversal for SBC feature enables a Cisco IOS NAT SIP Application-Level Gateway (ALG) router to act as a SBC on a Cisco Multiservice IP-to-IP Gateway, helping to ensure smooth delivery of voice over IP (VoIP) services.

Refer to Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller and SP Hosted NAT Traversal for SIP Calls Using Cisco IOS Session Border Controller for more information.

Q42. How many SIP, Skinny and H323 calls can a routers memory and CPU handle with NAT?
A42. The number of calls handled by a NAT router is contingent on the amount of memory available on the box and the processing power of the CPU.

Q44. Does a NAT router suppport TCP segmentation of Skinny and H323 packets?

A44. IOS-NAT support TCP segmentation for H323 in 12.4 Mainline and TCP segmentation support for SKINNY from 12.4(6)T onward.

Q45. Are there any caveats to watch out for when using a NAT Overload configuration in a voice deployment?
A45. Yes. When you have NAT overload configs and a voice deployment, you need the registration message to go through NAT and create an association for out->in to reach this inside device. The inside device sends this registration in a periodic fashion and NAT updates this pin-hole / association from the information as in the Signalling message.

Q46. Are there any known problems caused by doing a "clear ip nat trans *" or "clear ip nat trans forced" in a voice deployment?

A46. In voice deployments when you do a "clear ip nat trans *" or "clear ip nat trans forced" and have dynamic NAT, you will wipe out the pin-hole / association and need to wait till the next registration cycle from the inside device to re-estabilish this. It is not recommended to do these clear commands in a voice deployment.

Q47. Does NAT support Voice co-located solution?

A47. No. Co-located solution is currently not supported. The following deployment with NAT, on the same box, are considered as co-located solution: CME/DSP-Farm/SCCP/H323.

Q48. Does NVI support Skinny ALG, H323 ALG & TCP SIP ALG?

A48. No. Note that UDP SIP ALG (used by most deployments) isn't impacted by this.

NAT with VRF/MPLS

Q49. Will a NAT router ever support natting the same address space in a VRF as is being NATTed in Global address space?
Currently, we get a warning
"% similar static entry (1.1.1.1 ---> 22.2.2.2) already exists"
when we try to configure the following:
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED
A49. Legacy NAT supports overloapping address config over different vrfs. You would have to configure overlapping at rule with "match-in-vrf" option and set up "ip nat inside/outside" in the same vrf for traffic over that specific vrf. The overlapping support does not include the global routing table. There is DDTS for this - CSCsx73334.

You must add "match-in-vrf" keyword for the overlapping vrf static NAT entries for different vrfs but it is not possible to overlap global and vrf NAT addresses.

72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf

72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf

Q50. Does legacy NAT support VRF-Lite (Natting from a VRF to a different VRF)?

A50. No, you have to use NVI for Natting between different VRF's . Please see NAT Virtual Interface for more information and examples. You can use legacy NAT to do NAT from vrf to global or NAT withing the same VRF.

NAT NVI

Q51. What is NAT NVI?

A51. NVI stands for NAT Virtual Interface. It allows NAT to translate between two different VRF's. This should be used in lieu of "NAT on a Stick" . Please see NAT NVI for more details.

Q52. Should NAT NVI be used when NATTing between an interface in Global and an interface in a VRF?

A52. It is recommended to use legacy nat for vrf to global NAT(ip nat inside/out) and between interfaces in the same VRF. NVI is used for NAT between different vrfs.

Q53. Is TCP segmentation for NAT-NVI supported?
A53. There is no support for TCP segmentation for NAT-NVI.

Q54. Does NVI support Skinny ALG, H323 ALG & TCP SIP ALG?

A54. No. Note that UDP SIP ALG (used by most deployments) isn't impacted by this.

Q55. Does TCP Segmentation supported with SNAT?

A55. SNAT doesn?t support any TCP ALGs based, such as, SIP/SKINNY/H323/DNS. Thus, TCP Segmentation is not supported. However, UDP SIP/DNS are supported.

SNAT

Q56. What is Stateful NAT (SNAT) ?
A56. SNAT allows two or more network address translators to function as a translation group. One member of the translation group handles traffic requiring translation of IP address information. Additionally, it informs the backup translator of active flows as they occur. The backup translator can then use information from the active translator to prepare duplicate translation table entries; therefore, if the active translator is hindered by a critical failure, the traffic can rapidly be switched to the backup. The traffic flow continues since the same network address translations are used, and the state of those translations has been previously defined.Please see Enhanced IP Resiliency Using Cisco Stateful NATfor more information.

Q57. Is TCP Segmentation supported with SNAT?
A57. SNAT doesn?t support any TCP ALGs based, such as, SIP/SKINNY/H323/DNS. Thus, TCP Segmentation is not supported. However, UDP SIP/DNS are supported.

Q58. Is SNAT support for Asymetric-routing?

A58. Asymetric-routing supports by enabling as-queuing. By default, as-queueing is enable. However, from 12.4(24)T onward, as-queuing is no longer supported. It?s customer responsibility to make sure packets are route properly and proper delay added to get asymmetric-routing work correctly.

NAT-PT (v6<->v4)

Q59. What is NAT-PT?
A59. NAT-PT is V4 to V6 translation for NAT. Protocol Translation (NAT-PT) is an IPv6-IPv4 translation mechanism, as defined in RFC 2765 and RFC 2766,
allowing IPv6-only devices to communicate with IPv4-only devices and vice versa. Please see Implementing NAT-PT for IPv6 and Cisco IOS NAT for IPV6
for more information about this feature

Q60. Is NAT-PT supported in the CEF path?

A60. NAT-PT is not supported in the CEF path.

Q61. What ALGs are supported in NAT-PT?

A61. NAT-PT supports TFTP/FTP and DNS. There are no Voice and SNAT support in NAT-PT.

Platform Dependent

Cisco 7300/7600/6k

Q62. Is Stateful NAT also known as S-NAT and available on Catalyst 6500 on the SX train?
A62. Stateful NAT, also known as S-NAT, is not available on Catalyst 6500 on the SX train.

Q63. Is VRF Aware NAT Supported in hardware on the 6k?

A63. VRF Aware NAT is not supported in hardware on this platform.

Q64. Do the 7600 and Cat6000 support "VRF Aware NAT"?

A64. In the 65xx/76xx platform section VRF aware NAT is not supported and the CLI's are being blocked via:

Note: It is possible to implement a design by leveraging a FWSM running in virtual context transparent mode to accomplish it.

Cisco 850

Q65: Does the Cisco 850 support Skinny NAT ALG in 12.4T?

A65: There is no support for Skinny NAT ALG in 12.4T on the 850 series.