

网络地址转换(NAT)常见问题

目录

[简介](#)

[通用的NAT](#)

[语音NAT](#)

[与VRF/MPLS的NAT](#)

[NAT NVI](#)

[SNAT](#)

[NAT-PT \(对v4的v6\)](#)

[根据平台的思科7300/7600/6k](#)

[根据平台的思科850](#)

[NAT部署](#)

[NAT最佳实践](#)

[相关信息](#)

简介

本文提供回答关于网络地址转换(NAT)常见问题。

通用的NAT

Q. 什么是 NAT ?

A. 网络地址转换(NAT)为IP地址保存设计。这使得采用未注册 IP 地址的专用 IP 网络可以连接到 Internet。NAT 在路由器上运行，通常将两个网络连接在一起，并在数据包转发到另一个网络之前，将内部网络中的专用（非全局唯一）地址转换为合法地址。

作为此功能的一部分，NAT 可以配置为只向外界通告整个网络的一个地址。这样可以将整个内部网络有效地隐藏在该地址后面，使其更加安全。NAT在远程访问环境提供安全和地址保存的双重功能和典型地实现。

Q. NAT如何工作？

A. 基本上，NAT允许单个设备，例如路由器，作为在互联网之间的一个代理程序(或公共网络)和本地网络(或私有网络)，因此意味着仅单个唯一IP地址要求代表整个计算机组到任何东西他们的网络的外部。

Q. 如何配置NAT？

A. 为了配置传统NAT，您在路由器(从外部NAT需要做一个接口)和在路由器(里面NAT的另一个接口)和翻译的IP地址至少一一套规则在信息包报头(如果需要和有效载荷)需要配置。为了配置nat虚拟接

口(NVI) , 您需要至少一个接口配置与NAT enable (event)与同一套规则一起如上所述。

欲知更多信息 , 参考[寻址服务配置指南](#)或[配置NAT虚拟接口的Cisco IOS IP](#)。

Q. 主要区别NAT的Cisco IOS软件和思科PIX安全工具实施有何区别 ?

A. 基于Cisco IOS软件的NAT不是功能上不同的比在思科PIX安全工具的NAT功能。主要区别在实施包括支持的不同的流量类型。有关在 Cisco PIX 设备 (包括支持的数据流类型) 上配置 NAT 的详细信息 , 请参阅 [Cisco PIX 500 系列安全设备](#)和 [NAT 配置示例](#)。

Q. Cisco IOS NAT 在哪个 Cisco 路由硬件上可用 ? 如何订购硬件 ?

A. Cisco Feature Navigator工具在哪些允许客户识别功能(NAT)和查找版本和硬件版本此Cisco IOS软件特性是可用的。参考的[Cisco Feature Navigator](#)为了使用此工具。

Q. NAT 发生在路由之前还是之后 ?

A. 处理使用NAT的命令根据数据包是否去从网络内部外部网络或从外部网络网络内部。内部到外部的转换发生在路由之后 , 外部到内部的转换发生在路由之前。有关详细信息 , 请参阅 [NAT 运行顺序](#)。

Q. NAT能部署在公共无线局域网环境 ?

A. 可以。用户的Nat static IP支持功能提供支持用静态IP地址 , 启用那些用户建立IP会话在一个公共无线局域网环境。

Q. NAT是否执行服务器的TCP负载均衡在内部网络 ?

A. 可以。使用NAT , 您能设立在协调共享在实时主机中的负载的网络内部的一台虚拟主机。参考[避免服务器超载使用TCP负载均衡](#)欲知更多信息。

Q. 能速率限制NAT转换数量 ?

A. 可以。速率限制NAT转换功能提供能力限制并发NAT操作最大在路由器的。除给用户对如何的更多控制之外使用NAT地址 , 速率限制NAT转换功能可以用于限制病毒、蠕虫病毒和拒绝服务攻击的作用。

Q. 路由如何为由NAT使用的IP子网或地址了解或被传播 ?

A. 在下列情况下 , 可以察觉由 NAT 创建的 IP 地址的路由 :

- 内部全局地址池源自下一跳路由器的子网。
- 静态路由条目在下一跳路由器中配置 , 并在路由网络中重新分配。

当内部全局地址匹配与本地接口时 , NAT安装IP别名和ARP条目 , 在路由器为这些地址情况下 proxy-arp。如果此行为没有希望 , 请使用NO-别名关键字。

当NAT池配置时 , *add-route*选项可以用于自动路由射入。

Q. Cisco IOS NAT 中支持多少并发 NAT 会话 ?

A. NAT会话限制由相当数量在路由器的联机DRAM跳起。每个NAT转换消耗大约在DRAM的312个字节。结果，10,000个转换(更多比通常将被处理在单个路由器)消耗关于3 MB。所以，典型的路由硬件足够有支持的内存千位NAT转换。

Q. 使用 Cisco IOS NAT 时，可预期的路由性能如何？

A. Cisco IOS NAT 支持 Cisco 快速转发交换、快速交换以及进程交换。对于12.4T版本和以后，不再支持快速交换路径。对于Cat6k平台，交换顺序是Netflow (HW交换路径)，CEF，进程路径。

性能取决于以下几个因素：

- 应用类型及其数据流类型
- IP 地址是否为嵌入式
- 多条消息的交换与检查
- 要求的源端口
- 转换次数
- 当时运行的其他应用程序
- 硬件和处理器的类型

Q. Cisco IOS NAT 能否应用于子接口？

A. 可以。源 NAT 和/或目标 NAT 之间的转换可以应用于任何具有 IP 地址的接口或子接口（包括拨号器接口）。NAT不可能配置与无线虚拟接口。无线虚拟接口不在文字时存在对NVRAM。因此，在重新启动以后，路由器疏松在无线虚拟接口的NAT配置。

Q. Cisco IOS NAT 能否与热备用路由器协议 (HSRP) 配合使用，从而对 ISP 提供冗余链路？

A. 可以。NAT提供冗余的HSRP。然而，它是与SNAT (有状态的NAT)不同。与HSRP的NAT是一个无状态的系统。当失败发生时，当前会话没有保养。在静态NAT配置时(当数据包不匹配任何静态规则配置)时，数据包通过发送，不用任何转换。

Q. Cisco IOS NAT是否支持在帧中继接口的返程转换？是否支持在以太网端进行出站转换？

A. 可以。封装不为NAT重要。NAT可以执行有在接口的地方一个IP地址，并且接口从外部是内部的NAT或NAT。必须有里面和外部NAT的能作用。如果使用NVI，必须有至少一NAT启用接口。请参阅[我如何配置NAT？](#)了解更多信息。

Q. 单个支持NAT的路由器能否允许一些用户使用NAT和其他用户同一个以太网接口的继续使用他们自己的IP地址？

A. 可以。这可以是实现的通过描述需要NAT的套主机或网络的使用访问列表。同一台主机的所有会话将翻译或穿过路由器和不翻译。

访问列表、扩展访问列表和路由映射可以用于定义IP设备被转换的*规则*。应该始终指定网络地址和适当的子网掩码。不应该在网络地址或子网掩码位置使用关键字其中任一(请参阅[NAT FAQ](#)、[最佳实践和部署指南](#)关于更多详细信息)。使用静态NAT配置，当数据包没匹配与所有静态规则配置，数据包通过将发送，不用任何转换。

Q. 当配置为PAT (超载)时，什么是可以每个Inside Global IP地址创建转换的最大？

A. PAT (过载) 将每个全局 IP 地址的可用端口分成三个范围：0-511、512-1023 和 1024-65535。PAT 为每个 UDP 或 TCP 会话分配唯一的源端口。它尝试分配原始请求的相同端口值，但是，如果已经使用了初始源端口，开始扫描从最初特定的端口范围查找第一个可用端口并且分配它到会话。有12.2S代码基址的一例外。12.2S代码基址使用另外端口逻辑，并且没有端口预约。

Q. PAT 的工作原理是什么？

A. PAT与一个全局IP地址或多个地址一起使用。

PAT用一个IP地址

条件	说明
1	NAT/PAT 检查数据流并将其与转换规则进行匹配。
2	规则与 PAT 配置相匹配。
3	如果PAT知道关于流量类型，并且，如果该流量类型有“一套特定端口或端口它协商”该它将使用，PAT把他们放一边和不分配他们作为唯一标识符。
4	如果某个没有特殊端口要求的会话尝试连接到外部网络上，则 PAT 将转换 IP 源地址并检查初始源端口（例如433）的可用性。 注意： 对于传输控制协议 (TCP) 和用户数据报协议 (UDP)，范围为：1-511，512-1023，1024-65535。对于 Internet 控制消息协议 (ICMP)，第一组范围从 0 开始。
5	如果请求的源端口可用，则 PAT 将分配该源端口，然后会话继续。
6	如果请求的源端口不是可用的，PAT开始搜索从最初相关组(开始在1 TCP或UDP申请的和从0对ICMP)。
7	如果有端口可用，则分配该端口，然后会话继续。
8	如果没有端口可用，则丢弃数据包。

PAT用多个IP地址

条件	说明
1-7	前七个条件与处理单个 IP 地址的情况相同。
8	如果端口在第一个IP地址的相关组中不是可用的，NAT继续前进向在池的下个IP地址并且设法分配初始源端口请求的。
9	如果请求的源端口可用，则 NAT 将分配该源端口，然后会话继续。
10	如果请求的源端口不可用，则 NAT 将从相关组的起始处开始搜索（对于 TCP 或 UDP 应用程序，从 1 开始；对于 ICMP，从 0 开始）。

11	如果端口是可用的，分配，并且会话继续。
12	如果没有端口可用，除非池中的另一个 IP 地址可用，否则丢弃数据包。

Q. 什么是 NAT IP 池？

A. NAT IP 池是根据需要为 NAT 转换所分配的 IP 地址范围。要定义池，使用配置命令：

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

示例 1

以下示例翻译在从192.168.1.0或192.168.2.0网络寻址的内部主机之间对全局唯一10.69.233.208/28网络：

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

示例 2

在以下示例中，目标是定义虚拟地址的连接在一套实时主机中被分配。池定义了实时主机的地址。访问列表定义了虚拟地址。如果转换已经不存在，从serial interfaces 0 (外部接口)的TCP信息包目的地匹配访问列表翻译对从池的一个地址。

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

Q. 可配置 NAT IP 池 (ip nat pool "name") 的最大数量是多少？

A. 在实用的使用，可配置IP池最大由相当数量在特定路由器的联机DRAM限制。(思科建议您配置库容量255。)每个池应该是不大于16个位。在12.4(11)T中和以后，IOS介绍CCE (常见分类引擎)。这限制NAT只有最多255个池。在12.2S代码基址，没有最大数量池限制。

Q. 什么是使用route-map优点与在NAT池的ACL ？

A. route-map保护不必要的外部用户到达到内部的用户/服务器。它也有功能映射单个内部的IP地址到根据规则的不同的内部全局地址。参考[使用路由映射的多个池的NAT支持](#)欲知更多信息。

Q. 什么是 NAT 环境中的 IP 地址“重叠”？

A. IP 地址重叠是指两个要互联的位置使用相同的 IP 地址方案。这种情况很常见；在公司合并或收购时经常发生。如果没有特别的支持，这两个位置将无法彼此连接并建立会话。[重叠的 IP 地址可能是分配给其他公司的公用地址、分配给其他公司的专用地址，也可能是 RFC 1918 所定义的专用地址范围中的一个。](#)

专用 IP 地址不可路由，需要进行 NAT 转换才能与外界连接。解决方案包括拦截从外部到内部的域名系统 (DNS) 名称查询响应、设置外部地址转换，以及在将 DNS 响应转发到内部主机之前修复该响应。NAT 设备的两端都需要一个 DNS 服务器，以满足用户在两个网络之间进行连接的需求。

如[使用NAT所显示在重叠网络](#)，NAT能检查和进行在DNS A和PTR记录内容的地址转换。

Q. 什么是静态 NAT 转换？

A. 静态 NAT 转换在本地地址和全局地址之间具有一对一的映射关系。用户也可以将静态地址转换配置为端口级，并将剩余的 IP 地址用于其他转换。这通常发生在执行端口地址转换 (PAT) 的位置。

以下示例显示如何配置routemap允许外部到内部转换静态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
```

Q. 期限NAT超载是什么意思;此PAT？

A. 可以。NAT超载是PAT，介入使用池以范围一个或更多地址或使用接口IP地址与端口的组合。当您超载，您创建充分扩展转换。这是包含IP地址和来源/目的地端口信息的转换表条目，通常呼叫PAT或超载。

PAT (或超载)是使用转换对一个或更多的内部Cisco IOS NAT的功能(Inside local)专用地址外部(Inside Global，通常注册) IP地址。每次转换的唯一源端口号用于区分不同的会话。

Q. 什么是动态 NAT 转换？

A. 在动态 NAT 转换中，用户可以建立本地地址和全局地址之间的动态映射。动态映射通过定义分配全局地址和关联两个的本地地址将翻译的和地址池或接口IP地址完成。

Q. 什么是ALG？

A. ALG是应用层网关(ALG)。NAT进行在不运载来源和目的地IP地址在应用程序数据流的其中任一传输控制协议/用户数据报协议(TCP/UDP)流量的翻译服务。

这些协议包括FTP，HTTP，SKINNY，H232，DNS，RAS，SIP，TFTP，telnet，archie，finger，NTP，NFS，rlogin，rsh，rcp。嵌入在有效负载内的IP地址信息的特定协议要求应用级网关(ALG)的支持。

参考[使用有NAT的应用级网关](#)欲知更多信息。

Q. 能否建立一种同时包含静态和动态 NAT 转换的配置？

A. 可以。然而，同样IP地址不可能用于Nat static配置或在池NAT动态配置。所有公共IP地址需要是唯一。注意用于静态转换的全局地址没有自动地排除与包含那些同样全局地址的动态池。动态池必

须创建排除静态条目分配的地址。欲知更多信息，[同时参考配置静态和动态NAT](#)。

Q. 当traceroute通过NAT路由器时执行，traceroute应该应该显示Nat全局地址或它漏Nat本地地址？

A. Traceroute从外面应该总是返回全局地址。

Q. PAT如何分配端口？

A. NAT介绍额外端口功能：全方位和port-map。

- 不管其默认端口范围，全方位允许NAT使用所有端口。
- port-map允许NAT保留用户定义了特定应用程序的端口范围。

参考[PAT的用户定义的源端口范围](#)欲知更多信息。

在12.4(20)T2中向前，NAT引入L3/L4和对称波尔特的端口随机化。

- 端口随机化允许NAT随机地选择源端口请求的所有全局端口。
- 对称波尔特允许NAT支持独立的终端。

参考的[解剖学：查看网络内部网络地址译码器](#)欲知更多信息。

Q. IP分段和TCP分段有何区别？

A. IP分段发生在第3层(IP);TCP分段发生在Layer4 (TCP)。IP分段发生，当大于接口的最大传输单元(MTU)被发送在此接口外面的数据包。当他们被派出接口，这些数据包将必须被分段或丢弃。如果不要分段(DF)位在数据包的IP报头没有设置，数据包将被分段。如果DF位在数据包的IP报头设置，数据包丢弃，并且指示下一跳MTU vlaue的ICMP错误信息将返回到发送方。IP数据包的所有片段运载在IP报头的同样Ident，允许最终接收方重新组装片段到原始IP数据包。参考请[解决IP分段，MTU、MSS和PMTUD问题与GRE和IPsec](#)欲知更多信息。

当在终端站的一应用程序发送数据，TCP分段发生。应用程序数据分成什么TCP考虑最大的大块发送。从TCP通过的数据此单元到IP呼叫分段。TCP分段在IP数据包发送。当他们穿过网络和遭遇更小的MTU链路比他们能通过，适合这些IP数据包能然后变为IP段。

TCP首先将分段此数据到TCP分段(根据TCP MSS值)，并且添加TCP报头并且通过此TCP数据段对IP。然后IP将添加一IP报头发送数据包到远程终端主机。如果与TCP数据段的IP数据包大于在一流出接口的IP MTU在TCP主机IP之间的路径然后将分段IP/TCP数据包为了适合。这些IP数据包片段在远程主机将被重新组装由IP层，并且(最初发送)的完整TCP数据段将被递交到TCP层。TCP层不知道在传输期间，IP分段数据包。

NAT支持IP段，但是不支持TCP分段。

Q. NAT支持故障中为IP分段和TCP分段？

A. NAT支持仅故障中IP段由于ip虚拟重组。

Q. 如何对debug ip分段和TCP分段？

A. NAT使用同样调试CLI IP分段和TCP分段：`debug ip nat frag`。

Q. 有没有支持的NAT MIB ?

A. 不能。那里在没有支持的NAT MIB , 包括CISCO-IETF-NAT-MIB。

Q. 什么如何是TCP超时和它与NAT TCP计时器关连 ?

A. 如果三方握手没有完成, 并且NAT看到TCP数据包, 则NAT将启动60秒钟计时器。当三方握手完成时, 默认情况下NAT使用24小时计时器NAT条目。如果终端主机发送RESET, NAT更换从24个小时的默认计时器到60秒。一旦FIN, 当接收FIN和FIN-ACK时, NAT更换从24个小时的默认计时器到60秒。

Q. 能否更改它采取为了NAT translation能从NAT translation表计时的时间 ?

A. 可以。您能更改NAT超时值所有条目的或不同种类的NAT translations (例如UDP超时、dns超时、TCP超时、finrst超时、ICMP超时、PPTP超时、SYN超时、波尔特超时和ARP PING超时)。

Q. 如何从附加额外的字节终止轻量级目录访问协议(LDAP)到每LDAP应答数据包 ?

A. LDAP设置添加额外的字节(LDAP搜索发生), 当处理类型搜索RES条目时消息。LDAP附加10字节的搜索结果对其中每一LDAP应答数据包。在此10额外的字节的数据导致超出在网络情况下的数据包最大传输单元(MTU), 数据包丢弃。在这种情况下, 思科建议您关闭此LDAP行为使用CLI `no ip nat service ldap search RES`命令为了数据包能发送和接收。

Q. 什么是Inside Global/外部本地IP地址的路由建议在NAT方框 ?

A. 路由在Inside Global IP地址的NAT配置的方框必须指定功能的例如NAT-NVI。同样地, 在外部本地IP地址的NAT方框应该也指定路由。在这种情况下, 从的所有数据包在对方向使用外部静态规则将要求这种路由。在这样方案中, 当提供路由为IG/OL, 应该也配置时下一跳IP地址。如果下一跳配置未命中, 这认为配置错误, 并且导致未确定行为。

NVI-NAT是存在仅输出功能路径。如果直接地有与NAT-NVI的连接子网或在方框配置的外部NAT转换规则, 则在那些方案, 您需要为下一跳提供一个假的下一跳IP地址并且相关的ARP。这是需要的为了基础结构能递交数据包到转换的NAT。

Q. Cisco IOS NAT是否支持与“日志”关键字的ACL ?

A. 为动态 NAT 转换配置 Cisco IOS NAT 时, 将使用 ACL 标识可转换的数据包。当前 NAT 体系结构不支持包含“log”关键字的 ACL。

语音NAT

Q. 装备Cisco Unified Communications Manager的NAT支持小型客户机控制协议(SCCP) v17 (CUCM) V7 ?

A. 默认电话负载的CUCM 7和全部CUCM 7支持的SCCPv17。当电话注册时, 使用的SCCP版本取决于在CUCM和电话之间的最高的普通的版本。

NAT不支持SCCP v17。直到SCCP的v17 NAT支持实现, 必须降级固件到版本8-3-5或以下, 以便SCCP v16协商。只要使用SCCP v16, CUCM6不会遇到与任何电话负载的NAT问题。Cisco

IOS当前不支持SCCP版本17。

Q. NAT支持哪些CUCM /SCCP/firmware负载版本？

A. NAT支持CUCM版本6.x和以下版本。支持SCCP v15的这些CUCM版本发布与默认8.3.x (或及早)电话固件加载(或及早)。

NAT不支持CUCM版本7.x或以上版本。这些CUCM版本发布与支持SCCP v17的默认8.4.x电话固件加载(或以上)。

如果或以后使用CUCM 7.x，在CUCM TFTP server必须安装，以便电话以SCCP v15使用一固件加载或为了由NAT及早支持一更旧的固件加载。

下面的链路确认固件加载8.3.x包含SCCP v15或及早和与NAT一起使用和固件加载8.4.x包含SCCP v17，并且不会与NAT一起使用。

<http://third-gen-phones.gforce.cisco.com/twiki/prod/bin/view/Thirdgenphones/CCMLoadNumberAndCodeNameDecoderRing>

Q. 什么是 RTP 和 RTCP 的服务提供商 PAT 端口分配增强？

A. RTP和RTCP功能的服务提供商PAT波尔特分配增强保证该SIP、H.323和skinny语音呼叫的。用于RTP数据流的端口号是偶数端口号，并且RTCP数据流是下随后的奇端口号。端口号翻译到在范围内的一个编号指定符合RFC-1889。一个具有该范围内端口号的呼叫将导致 PAT 转换为此范围内的另一个端口号。同样，范围之外端口号的 PAT 转换将不会导致转换为给定范围内的编号。

有关详细信息，请参阅 [RTP 和 RTCP 的服务提供商 PAT 端口分配增强](#)。

Q. 什么是会话初始化协议(SIP)，并且可以SIP数据包是NATted？

A. 会话初始协议 (SIP) 是基于 ASCII 的应用层控制协议，可用于建立、维持和终止两个或多个端点之间的呼叫。SIP 是 Internet 工程任务组 (IETF) 为在 IP 上实现多媒体会议而开发的备选协议。Cisco SIP 的实施使支持的 Cisco 平台能够通过 IP 网络用信号通知设置语音和多媒体呼叫。

SIP数据包可以是NATted。

Q. 什么是会话博德控制器的(SBC)托管的NAT横越支持？

A. Cisco IOS托管SBC功能的NAT横越使Cisco IOS NAT SIP应用层网关(ALG)路由器作为在Cisco多服务IP到IP网关的SBC，帮助保证VoIP服务平稳的发送。

参考[配置Cisco IOS托管会话博德控制器的NAT横越](#)，并且[SP托管SIP呼叫的NAT横越使用Cisco IOS会话博德控制器](#)欲知更多信息。

Q. 路由器内存能和CPU处理多少SIP， skinny和H323呼叫与NAT？

A. 已处理呼叫编号由NAT路由器的是偶发的内存数量在方框和CPU的处理功率的联机。

Q. NAT路由器是否支持skinny和H323数据包的TCP分段？

A. IOS-NAT H323的支持TCP分段12.4主线和TCP SKINNY的分段支持从向前12.4(6)T。

Q. 有没有密切注意的任何警告，当曾经NAT超载配置在语音部署时？

A. 可以。当您有NAT超载配置，并且时语音部署，您需要注册消息通过NAT和创建out->in的一个关联能到达此内部设备。内部设备在一个定期方式发送此注册，并且NAT更新此针孔/关联从信息正如在信令消息。

Q. 有没有发出引起的任何已知的问题清楚ip nat trans *发出命令或清楚ip nat trans被强制的in命令语音部署？

A. 在语音部署，当您issue清楚ip nat trans *请发出命令或一清楚ip nat trans被强制的命令并且有动态NAT，您将消除针孔/关联，并且必须等待从内部设备的下个注册周期到再establish这。Cisco建议您不使用这些清楚in命令语音部署。

Q. NAT支持语音代管的解决方案？

A. 不能。当前不支持并行定位解决方案。与NAT的下列的部署(在同一个方框)认为一并行定位解决方案：CME/DSP-Farm/SCCP/H323.

Q. NVI是否支持skinny ALG、H323 ALG和TCP SIP ALG？

A. 不能。注意UDP SIP ALG (使用由多数部署)没有被影响。

与VRF/MPLS的NAT

Q. NAT路由器支持是否NATting在VRF的同一个地址空间象在全局地址的NATted将间隔？目前，我收到此警告：“%相似的静态条目(1.1.1.1---当我尝试配置以下时，> 22.2.2.2)已经存在”：

```
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
```

A. overlapping地址的传统NAT支持在不同的VRF配置。您会必须配置重叠在与匹配在VRF选项和设置ip nat inside/规则从外部的在流量的同样VRF在该特定VRF。重叠支持不包括全球路由表。

您必须添加交迭的VRF静态NAT条目的匹配在VRF关键字不同的VRF的。然而，交迭全局和VRF NAT地址是不可能的。

```
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
```

Q. 传统NAT支持VRF-Lite (从VRF的NATting到不同的VRF)？

A. 不能。您必须使用NVI区别VRF之间的NATting。您能使用传统NAT执行从VRF的在同样VRF内的NAT到全局或NAT。

NAT NVI

Q. 什么是NAT NVI ?

A. NVI代表NAT虚拟接口。它允许NAT翻译两区别VRF之间。应该使用此解决方案代替[单接口网络地址转换](#)。

Q. 应该使用NAT NVI，当在接口在全局和接口之间的NATting在VRF ?

A. 思科建议您使用传统NAT VRF对全局NAT (ip nat inside/)和在接口之间在同样VRF。NVI使用区别VRF之间的NAT。

Q. 支持NAT-NVI的TCP分段 ?

A. 没有TCP分段的支持NAT-NVI的。

Q. NVI是否支持skinny ALG、H323 ALG和TCP SIP ALG ?

A. 不能。注意UDP SIP ALG (使用由多数部署)没有被影响。

Q. TCP分段支持与SNAT ?

A. SNAT不支持任何TCP ALGs (例如，SIP，SKINNY，H323或者DNS)。所以，不支持TCP分段。然而，支持UDP SIP和DNS。

SNAT

Q. 什么是有状态的NAT (SNAT) ?

A. SNAT允许两个或多个网络地址转换器功能作为转换组。处理流量要求IP地址信息的转换的转换组的一个成员。另外，当他们发生，它通知备份译码器活动流。备份译码器能然后使用从活动译码器的信息准备重复的转换表条目。所以，如果活动译码器由致命故障妨害，流量可能迅速地交换到备份。通信流继续，因为使用同样网络地址转换，并且那些转换的状态以前定义。[使用思科有状态的NAT](#)欲知更多信息，参考[增强的IP RTP优先策略弹性](#)。

Q. TCP分段支持与SNAT ?

A. SNAT不支持任何TCP ALGs (例如，SIP，SKINNY，H323或者DNS)。所以，不支持TCP分段。然而，支持UDP SIP和DNS。

Q. SNAT支持为asymmetric路由 ?

A. Asymmetric路由支持NAT通过启用作为队列。默认情况下，和队列是enable (event)。然而，从向前12.4(24)T，不再支持和队列。客户必须确保数据包适当地路由，并且适当的延迟被添加为了不对称路由能正确地运作。

NAT-PT (对v4的v6)

Q. 什么是NAT-PT ?

A. NAT-PT是v4对v6 NAT的转换。协议转换(NAT-PT)是IPv6-IPv4转换机制，如对[RFC 2765](#) 和 [RFC 2766定义](#)，允许IPv6-only设备用IPv4-only设备通信反之亦然。参考[实现IPv6的NAT-PT](#)关于此功能的更多信息

Q. 思科快速转发(CEF)路径支持NAT-PT ？

A. CEF路径不支持NAT-PT。

Q. NAT-PT支持什么ALGs ？

A. NAT-PT支持TFTP/FTP和DNS。没有语音和SNAT的支持在NAT-PT。

Q. ASR是否1004支持NAT-PT ？

A. 聚合服务路由器(ASR)使用NAT64。关于配置NAT64的更多信息，参考[配置无状态的NAT64的路由网络](#)。

根据平台的思科7300/7600/6k

Q. 在Catalyst 6500的有状态的NAT (SNAT)联机在SX系列 ？

A. SNAT不是可用的在SX系列的Catalyst 6500。

Q. 在6k的硬件方面支持VRF感知NAT ？

A. 在此平台的硬件方面不支持VRF感知NAT。

Q. 7600是否和Cat6000支持VRF感知NAT ？

A. 在65xx/76xx平台上，不支持VRF感知NAT，并且CLIs阻塞。

注意：您能通过虚拟上下文透明模式运行的有效利用FWSM实现设计。

根据平台的思科850

Q. 思科是否850支持在版本12.4T的skinny NAT ALG ？

A. 不能。没有skinny NAT ALG的支持在850系列的12.4T。

NAT部署

Q. 如何实现NAT ？

A. NAT启用使用未注册的IP地址连接到互联网的私有IP互连网络。NAT转换在内部网络的私有(RFC1918)地址成法律可路由地址，在数据包转发在另一网络上前。

关于实现NAT的更多信息，参考[配置IP地址保存的NAT](#)。

Q. 如何实现与语音的NAT ?

A. 语音功能的NAT支持允许SIP通过通过路由器的被嵌入的消息配置与将翻译的网络地址转换(NAT)回到数据包。应用层网关(ALG)与NAT一起使用转换语音数据包。

关于实现与语音的NAT的更多信息，参考[ALGs的NAT支持](#)。

Q. 与MPLS VPN的集成NAT ?

A. 与MPLS VPN功能的NAT集成允许在单个装置将配置的多个MPLS VPN。NAT能从哪MPLS VPN区分收到IP数据流，即使MPLS VPN全部使用同样IP编址方案。此增强使广泛MPLS VPN客户共享服务，当保证时每MPLS VPN是完全从其他中分离出。

Q. Nat static映射是否支持高可用性的HSRP ?

A. 当地址解析服务(ARP)查询为配置与网络地址转换(NAT)静态映射并且由路由器拥有的地址时被触发，NAT回应应在ARP指向的接口的BIA MAC地址。两路由器作为暂挂的HSRP活动和。必须启用和配置他们的NAT内部接口属于组。

Q. I implemet NAT NVI ?

A. NAT虚拟接口(NVI)功能去除需求从外部配置接口作为内部的NAT或NAT。关于NAT NVI的更多信息，参考[配置NAT虚拟接口](#)。

Q. 如何实现与NAT的负载均衡 ?

A. 有可以完成与NAT:的两负载均衡您能装载平衡入站对一套服务器分配在服务器的负载，并且您能装载平衡您的用户数据流到在两个或多个ISP的互联网。

关于入站负载均衡的更多信息，参考[避免服务器超载使用TCP负载均衡](#)。

关于平衡的出站负载的更多信息，参考[两ISP连接的IOS NAT负载均衡](#)。

Q. 如何实现在conjunction的NAT与IPSec ?

A. 有IP安全封装安全有效载荷(ESP)的支持通过NAT和IPSec NAT透明度。

IPSec ESP通过NAT功能提供能力通过在超载或端口地址转换(PAT)模式的一Cisco IOS NAT已配置设备支持多个并发IPSec ESP通道或连接。

IPSec NAT透明度功能引入IPSec数据流的支持能游遍在网络的NAT或PAT点通过寻址许多已知不相容在NAT和IPSec之间。

Q. 如何实现NAT-PT ?

A. NAT-PT (网络地址转换-协议转换)是IPv6-IPv4转换机制，如对[RFC 2765](#) 和[RFC 2766定义](#)，允许IPv6-only设备与IPv4-only设备联络反之亦然。

关于实现和配置NAT-PT的更多信息，参考[实现IPv6的NAT-PT](#)。

Q. 如何实现组播NAT？

A. 它是可能的NAT组播流的来源IP。route-map不可能使用，当执行动态NAT组播时，只有访问列表为此支持。

欲知更多信息，参考[如何组播在Cisco路由器的NAT工作](#)。使用[多点传送服务器反射](#)解决方案，目的地组播组是NATted。

Q. 如何实现有状态的NAT (SNAT)？

A. SNAT启用动态地被映射的NAT会话的持续服务。没有对SNAT的需要是静态定义的接收冗余的好处的塞申斯。在没有SNAT时，使用的会话动态NAT映射会被切断在致命故障情形下，并且必须被重建。支持仅最小SNAT配置。应该进行将来部署，在谈与您的思科客户团队为了验证设计相对当前限制之后。

SNAT为以下方案推荐：

- 正如SNAT白皮书所描述的HSRP模式：[增强的IP RTP优先策略弹性使用思科有状态的NAT](#)。
- 因为有一些功能与HSRP比较，主要的/备份不是一个推荐的模式。
- 故障切换方案和2路由器设置的。即，如果一个路由器失败，另一个路由器接管无缝地。(SNAT体系结构没有设计处理接口飘荡。)
- 支持非不对称路由方案。不对称路由可以被处理，只有当在应答数据包的延迟高于那在2 SNAT路由器之间交换SNAT消息。

目前SNAT体系结构没有设计处理稳健性;因此，这些测验没有预计成功：

- 清除NAT条目，当有流量时。
- 更改接口参数(类似IP地址更改，shut/no-shut等等)，当有流量时。
- **清楚SNAT**的特定或**显示命令**没有预计适当地执行和没推荐。某些SNAT涉及的**结算和显示命令**如下：

```
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>
```

- 如果用户要清除条目，**清楚ip nat trans**强制了或**结算ip nat trans ***命令可以使用。如果用户要查看条目，**show ip nat translation**，**show ip nat translations verbose**，并且**显示ip nat**可以使用**stats**命令。如果**service internal**配置，将显示SNAT特定信息。
- NAT转换在备用路由器没有推荐清除。总是清楚在主要的SNAT路由器的NAT条目。
- SNAT不是HA;因此，在两路由器的配置应该是相同的。两路由器应该有同一镜像运行。并且请确保用于两SNAT路由器的基础平台是相同的。

NAT最佳实践

Q. 有没有任何NAT最佳实践？

A. 可以。这些是NAT最佳实践：

1. 当设置动态NAT的时规则的曾经动态和静态NAT，ACL应该如此屏蔽静态本地主机没有重叠。
2. 当心使用ACL NAT与**permit ip any any**，您能取得不可预知的结果。在12.4(20)T NAT将转换本地生成的HSRP和路由协议信息包后，如果被派出外部接口，以及本地加密的信息包匹配NAT规则的他们。
3. 当您有NAT的时重叠网络，请使用匹配在**VRF**关键字。您必须添加交迭的VRF静态NAT条目的匹配在**VRF**关键字不同的VRF的，但是交迭全局和VRF NAT地址是不可能的。

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

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

4. 除非使用，有同样地址范围的NAT池不可能用于不同的VRF匹配在**VRF**关键字。例如：

```
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
```

注意：虽然CLI配置有效，没有匹配在**VRF**关键字配置不支持Wven。

5. 当部署与NAT接口超载时的ISP负载均衡，最佳实践是使用route-map以在ACL匹配的接口匹配。
6. 当曾经池映射时，您不应该使用两不同的映射(ACL或route-map)共享同一个NAT池地址。
7. 当部署同样NAT在故障切换方案的时两不同路由器规定，您应该使用HSRP冗余。
8. 请勿定义在静态NAT和动态池的同一个内部全局地址。此操作可能导致负面的结果。

相关信息

- [IP路由技术支持](#)
- [技术支持和文档 - Cisco Systems](#)