查看网络地址转换 (NAT) 常见问题解答

目录

简介

本文档介绍有关网络地址转换 (NAT) 的常见问题解答。

通用 NAT

问：什么是 NAT？

答：网络地址转换 (NAT) 是为保护 IP 地址而设计的。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 具有确保安全和保护地址的双重功能，通常在远程访问环境中实施。

问： NAT 的工作原理是什么？

答：基本而言，NAT 允许单个设备（例如路由器）充当互联网（或公用网络）与本地网络（或专用网络）之间的代理，这意味着只需要一个唯一的 IP 地址即可向其网络之外的任何对象表示整个计算机组。

问： 如何配置 NAT？

答：要配置传统 NAT，至少需要在某台路由器上设置一个（NAT 外部）接口，并在该路由器上设置另一个（NAT 内部）接口，另外还需要配置一组用于转换数据包报信头（以及负载，如果需要）中 IP 地址的规则。要配置 NAT 虚拟接口 (NVI)，至少需要配置一个启用了 NAT 的接口以及上面提到的一组相同的规则。

有关详细信息，请参阅Cisco IOS® IP编址服务配置指南或配置NAT虚拟接口。

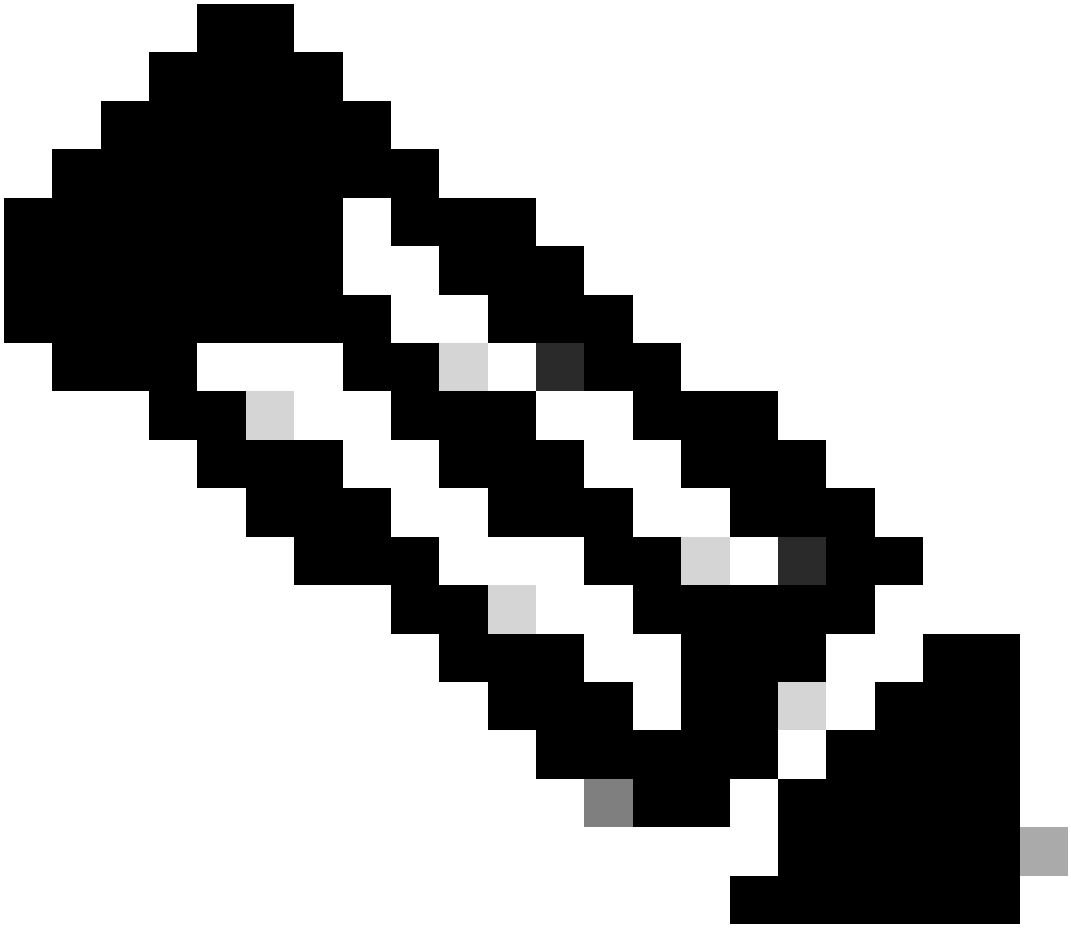
问： Cisco IOS软件和Cisco PIX安全设备实施NAT的主要区别是什么？

答：思科基于软件的 IOS NAT 与思科 PIX 安全设备中的 NAT 功能没有本质区别。主要区别包括实

施中支持的流量类型不同。有关 Cisco PIX 设备上 NAT 配置的详细信息（包括支持的流量类型），请参阅 NAT 配置示例。

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

答：Cisco Feature Navigator工具允许客户识别功能(NAT)，并查看此Cisco IOS软件功能的可用版本和硬件版本。要使用此工具，请参阅思科功能导航器。



注意：只有思科注册用户才能访问思科内部工具和信息。

问： NAT 发生在路由之前还是之后？

答：使用 NAT 处理事务的顺序基于数据包是从内部网络传递到外部网络，还是从外部网络传递到内部网络。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。

问： NAT 是否可以部署在公共无线局域网环境中？

答：是的。NAT 静态 IP 支持功能为具有静态 IP 地址的用户提供支持，使这些用户能够在公共无线局域网环境中建立 IP 会话。

问： NAT 是否会对内部网络上的服务器执行 TCP 负载均衡？

答：是的。使用 NAT，可以在内部网络上建立一个虚拟主机，用以协调真实主机之间的负载共享。

问： 是否可以对 NAT 转换数量进行速率限制？

答：是的。使用“NAT 转换的速率限制”功能可以限制路由器上并发 NAT 操作的最大数量。除了支持用户更好地控制 NAT 地址的使用外，“NAT 转换的速率限制”功能还可用于限制病毒、蠕虫和拒绝服务攻击所产生的影响。

问： NAT 使用的 IP 子网或地址如何学习或传播路由？

答：以下情况将获知 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。

当内部全局地址与本地接口匹配时，NAT会设置一个IP别名和一个ARP条目，在这种情况下，路由器可以代理ARP获取这些地址。如果不需要此行为，请使用 no-alias 关键字。

配置 NAT 池时，可以使用 add-route 选项进行自动路由注入。

问： Cisco IOS NAT 中支持多少并发 NAT 会话？

答：NAT 会话限制取决于路由器中可用 DRAM 的数量。每次 NAT 转换大约都会使用 DRAM 中的 312 个字节。因此，转换 10,000 次（超过该次数通常会在单个路由器上处理）大约使用 3 MB。因此，典型的路由硬件具有足够多的内存来支持成千上万次 NAT 转换。

问： 使用 Cisco IOS NAT 时，可预期的路由性能如何？

答：Cisco IOS NAT 支持思科快速转发交换、快速交换和进程交换。12.4T 版和更高版本不再支持快速切换交换路径。对于 Cat6k 平台，切换交换顺序为 Netflow（硬件切换交换路径）、CEF、过程路径。

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

问： Cisco IOS NAT 能否应用于子接口？

答：是的。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）。无法使用无线虚拟接口配置 NAT。在写入 NVRAM 时，不存在无线虚拟接口。因此，在重新启动后，路由器会失去无线虚拟接口上的 NAT 配置。

问： 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？

答：是的。NAT 确实会提供 HSRP 冗余。但是，它与 SNAT（有状态 NAT）不同。使用 HSRP 的 NAT 是一个无状态系统。发生故障时不保留当前会话。在静态 NAT 配置期间（数据包与任何静态规则配置都不匹配），系统直接发送数据包，而不进行任何转换。

问： 思科 IOS NAT 是否支持在帧中继接口上进行入站转换？是否支持在以太网端进行出站转换？

答：是的。封装对 NAT 并不重要。只要接口上有 IP 地址并且接口是 NAT 内部或 NAT 外部接口，即可执行 NAT。必须有一个内部和外部接口才能让 NAT 正常工作。如果您使用 NVI，必须至少有一个启用了 NAT 的接口。有关详细信息，请参阅如何配置NAT？。

问： 启用了 NAT 的单个路由器是否允许一些用户使用 NAT，而同一以太网接口上的其他用户可以继续使用自己的 IP 地址？

答：是的。这可通过使用一个访问列表来完成，该访问列表描述需要 NAT 的一组主机或网络。

访问列表、扩展访问列表和路由图映射均可用于定义 IP 设备的转换规则。必须始终指定网络地址和相应的子网掩码。不能使用关键字 any 代替网络地址或子网掩码。使用静态NAT时，当数据包与任何静态规则配置都不匹配时，数据包会通过而不进行任何转换。

问： 配置 PAT（过载）时，可以为每个内部全局 IP 地址创建的最大转换次数是多少？

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，但如果原始的源端口已经使用，它将从特定端口范围的开始端口进行扫描，以查找第一个可用端口并将其分配给对话。但 12.2S 代码库例外。12.2S 代码库使用不同的端口逻辑，并且不预留端口。

问： PAT 的工作原理是什么？

答：PAT 使用一个全局 IP 地址或多个地址。

使用一个 IP 地址的 PAT

条件	描述
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知道流量类型，并且如果该流量类型具有“它协商的一组特定端口”，则PAT会保留这些端口，并且不将它们分配为唯一标识符。
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：传输控制协议(TCP)和用户数据报协议(UDP)的范围是：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可用，PAT 将从相关组的开始处开始搜索（对于 TCP 或 UDP 应用，从 1 开始；对于 ICMP，从 0 开始）。
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。

使用多个 IP 地址的 PAT

条件	描述
1-7	前七个条件与处理单个 IP 地址的情况相同。
8	如果第一个 IP 地址的相关组中没有可用的端口，NAT 将移动到池中的下一个 IP 地址并尝试分配所请求的原始源端口。
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	如果端口可用，则系统会分配该端口，并继续会话。
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。

问： 什么是 NAT IP 池？

答：NAT IP 池是根据需要分配用于 NAT 转换的 IP 地址范围。要定义池，请使用配置命令：

<#root>

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

示例 1

下一个示例在寻址的内部主机之间转换，从192.168.1.0或192.168.2.0网络到全球唯一的10.69.233.208/28网络：

```
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
```

示例 2

在本例中，目标是定义虚拟地址，其连接在一组实际主机之间分配。池定义真实主机的地址。访问列表定义虚拟地址。如果不存在转换，则从目标与访问列表匹配的串行接口 0（外部接口）发送的 TCP 数据包将转换为池中的地址。

```
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
```

问： 可配置NAT IP池(ip nat pool <name>)的最大数量是多少？

答：在实际应用中，可配置的 IP 池的最大数量取决于特定路由器中可用 DRAM 的数量。（思科建议您将池大小配置为 255。）每个池的位数不能超过16位。在12.4(11)T及更高版本中，Cisco IOS引入了CCE（通用分类引擎）。这将 NAT 限制为最多只能有 255 个池。在 12.2S 代码库中，没有最大池数限制。

问： 相较于在 NAT 池中使用 ACL，使用路由图映射有什么优势？

答：路由图映射可以防止不受欢迎的外部用户访问内部用户/服务器。此外，它还可以根据规则将单个内部 IP 地址映射到不同的内部全局地址。有关更多信息，请参阅使用路由图映射对多个池提供 NAT 支持。

问： NAT环境中的IP地址重叠是什么？

答：IP 地址重叠是指要互连的两个位置均使用相同的 IP 地址方案。这种情况并不少见，通常发生在公司合并或被收购时。如果没有特殊支持，两个位置将无法连接和建立会话。重叠的IP地址可以是分配给其他公司的公有地址、分配给其他公司的私有地址，也可以来自RFC 1918中定义的私有地址范围

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。

NAT 能够对 DNS A 和 PTR 记录的内容进行检查并执行地址转换，如在重叠网络中使用 NAT 中所述。

问： 什么是静态 NAT 转换？

答：静态 NAT 转换是本地地址与全局地址之间的一对一映射。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。

下一个示例显示如何配置routemap以允许静态NAT的外部到内部转换：

<#root>

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 10.1.10.128 0.0.0.127'

route-map R1 permit 10
match ip address ACL-A
```

问： 术语NAT过载是什么意思；这是PAT吗？

答：是的。NAT 过载即 PAT，涉及使用由一个或多个地址组成的地址范围的池或将接口 IP 地址与端口结合使用。过载时，将可以创建完全扩展的转换。这是一个转换表条目，其中包含 IP 地址和源/目标端口信息，通常称为 PAT 或过载。

PAT（或过载）是思科 IOS NAT 的一项功能，用于将内部（内部本地）专用地址转换为一个或多个外部（内部全局，通常已注册）IP 地址。每次转换的唯一源端口号用于区分不同的会话。

问： 什么是动态 NAT 转换？

答：在动态 NAT 转换中，用户可以在本地地址与全局地址之间建立动态映射。动态映射通过以下操作来完成：定义要转换的本地地址以及要从中分配全局地址的地址池或接口 IP 地址池，并将两者关联起来。

问： ALG 是什么？

答：ALG 即应用层网关 (ALG)。NAT 对应用数据流中未携带源和/或目标 IP 地址的所有传输控制协

议/用户数据报协议 (TCP/UDP) 流量执行转换服务。

这些协议包括 FTP、HTTP、SKINNY、H232、DNS、RAS、SIP、TFTP、telnet、archie、finger、NTP、NFS、rlogin、rsh 和 rcp。在负载中嵌入 IP 地址信息的特定协议需要支持应用层网关 (ALG)。

有关更多信息，请参阅将应用层网关与 NAT 结合使用。

问： 能否建立一种同时包含静态和动态 NAT 转换的配置？

答：是的。但是，同一 IP 地址不能用于 NAT 静态配置，如果在 IP 地址位于池中，则不能用于 NAT 动态配置。所有公共 IP 地址都必须唯一。请注意，如果动态池中包含静态转换中使用的全局地址，则系统不会自动排除这些相同的全局地址。必须创建动态池才能排除静态条目分配的地址。有关更多信息，请参阅同时配置静态和动态 NAT。

问： 当通过NAT路由器执行traceroute时，traceroute是显示NAT全局地址还是泄漏NAT本地地址？

A.来自外部的Traceroute必须始终返回全局地址。

问： PAT 如何分配端口？

A. NAT引入了额外的端口功能：full-range和port-map。

- 全范围允许 NAT 使用所有端口，而不考虑其默认端口范围。
- 端口映射允许 NAT 为特定应用保留用户定义的端口范围。

有关更多信息，请参阅用于 PAT 的用户定义的源端口范围。

从 12.4(20)T2 开始，NAT 引入了 L3/L4 端口随机化和对称端口。

- 使用端口随机化，NAT 可以针对源端口请求随机选择任意全局端口。
- 使用对称端口，NAT可以支持点独立。

问： IP 分段与 TCP 分段的区别是什么？

A.IP分段发生在第3层(IP)；TCP分段发生在第4层(TCP)。如果将大于接口最大传输单位 (MTU) 的数据包从该接口发送出去，将会发生 IP 分段。这些数据包在从接口发送出去时必须进行分段或丢弃。如果数据包的IP报头中未设置Do not Fragment (DF)位，则会对数据包进行分段。如果数据包的IP报头中设置了DF位，则会丢弃该数据包，并向发送方返回指示下一跳MTU值的ICMP错误消息。IP 数据包的所有分段在 IP 报信头中都具有相同的标识，这样，最终接收者才能将这些分段重组为原始 IP 数据包。有关更多信息，请参阅解决 GRE 和 Ipsec 中的 IP 分段、MTU、MSS 和 PMTUD 问题。

当终端站上的应用发送数据时，将会发生 TCP 分段。应用数据将分解为 TCP 认为大小最适合发送的块。从 TCP 传递到 IP 的这一数据单位称为段。TCP 段以 IP 数据报的形式发送。之后，这些 IP

数据报在通过网络时会变成 IP 分段，并且遇到的 MTU 链路比适合它们通过的链路要小。

TCP首先将数据分段为TCP数据段（基于TCP MSS值），然后添加TCP报头并将此TCP数据段传递到IP。然后，IP协议添加一个IP报头，以将数据包发送到远程终端主机。如果带有TCP分段的IP数据包大于TCP主机之间路径上传出接口上的IP MTU，则IP会对IP/TCP数据包进行分段以便适合。这些IP数据包分段由IP层在远程主机上重组，而完整的TCP数据段（最初发送的）将交给TCP层。TCP层不知道IP在传输期间对数据包进行了分段。NAT支持IP分段，但不支持TCP分段。

问： NAT 是否支持无序的 IP 分段和 TCP 分段？

答：由于存在 ip virtual-reassembly，NAT 仅支持无序的 IP 分段。

问： 如何调试 IP 分段和 TCP 分段？

答：NAT对IP分段和TCP分段使用相同的调试CLI：debug ip nat frag。

问： 是否有受支持的 NAT MIB？

答：没有受支持的 NAT MIB（包括 CISCO-IETF-NAT-MIB 在内）。

问： TCP 超时是什么？它与 NAT TCP 计时器的关系有如何关系？

A.如果三次握手尚未完成，并且NAT看到一个TCP数据包，则NAT会启动60秒计时器。三方握手完成后，NAT 会默认对 NAT 条目使用 24 小时计时器。如果终端主机发送 RESET，NAT 会将默认计时器从 24 小时更改为 60 秒。对于 FIN，NAT 在收到 FIN 和 FIN-ACK 时会将默认计时器从 24 小时更改为 60 秒。

问： 是否可以从NAT转换表中将NAT转换所需的时间更改为超时？

答：是的。您可以更改所有条目或不同类型NAT转换的NAT超时值（例如，udp-timeout、dns-timeout、tcp-timeout、finrst-timeout、icmp-timeout、pptp-timeout、syn-timeout、port-timeout和arp-ping-timeout）。

问： 如何阻止轻量级目录访问协议 (LDAP) 将额外字节附加到每个 LDAP 应答数据包？

答：LDAP 设置在处理 Search-Res-Entry 类型的消息时会添加额外字节（LDAP 搜索结果）。LDAP 会将搜索结果的 10 个字节附加到每个 LDAP 应答数据包。如果这额外的 10 字节数据导致数据包超过网络中的最大传输单位 (MTU)，则该数据包将被丢弃。在这种情况下，思科建议您使用 CLI 命令 no ip nat service append-ldap-search-res 禁用此 LDAP 行为，以便正常发送和接收数据包。

问： 对 NAT 设备上的内部全局/外部本地 IP 地址有何路由建议？

答：必须在配置了 NAT 的设备上指定内部全局 IP 地址的路由，以便实现 NAT-NVI 等功能。同样，还必须在NAT框中为外部本地IP地址指定路由。在这种情况下，任何使用外部静态规则从in到out方向的数据包都需要这种路由。在这种情况下，在为IG/OL提供路由的同时，还必须配置下一跳

IP地址。如果缺少下一跳配置，则会被视为配置错误，并导致不确定的行为。

NVI-NAT 仅出现在输出功能路径中。如果子网与 NAT-NVI 直接连接，或者在设备上配置了外部 NAT 转换规则，则在这些情况下，您需要提供一个虚拟的下一跳 IP 地址以及下一跳的关联 ARP。底层基础设施必须使用它们才能将数据包交给 NAT 进行转换。

问： Cisco IOS NAT是否支持带有log关键字的ACL？

答：当您为动态 NAT 转换配置 Cisco IOS NAT 时，ACL 用于识别可转换的数据包。当前NAT体系结构不支持带有log（日志）关键字的ACL。

语音 NAT

问：NAT 是否支持思科统一通信管理器 (CUCM) V7 随附的瘦客户端控制协议 (SCCP) v17？

A. CUCM 7和CUCM 7的所有默认电话负载都支持SCCPv17。使用的 SCCP 版本取决于电话注册时 CUCM 和电话之间最高的通用版本。

创建本文档时，NAT尚不支持SCCP v17。在实现对SCCP v17的NAT支持之前，必须将固件降级到版本8-3-5或更早版本，以便协商SCCP v16。只要使用SCCP v16，CUCM6就不会遇到任何电话负载的NAT问题。思科 IOS 目前不支持 SCCP v17。

问： NAT 支持哪些 CUCM/SCCP/固件负载版本？

答：NAT 支持 CUCM 6.x 版和更早版本。这些 CUCM 版本在发布时具有支持 SCCP v15（或更早版本）的默认 8.3.x 版（或更早版本）电话固件负载。

NAT 不支持 CUCM 7.x 版或更高版本。这些 CUCM 版本在发布时具有支持 SCCP v17（或更高版本）的默认 8.4.x 版电话固件负载。

如果使用 CUCM 7.x 或更高版本，则必须在 CUCM TFTP 服务器上安装较早的固件负载，以便电话使用包含 SCCP v15 或更早版本的固件负载，从而得到 NAT 的支持。

问： 什么是 RTP 和 RTCP 的服务提供商 PAT 端口分配增强？

答：RTP 和 RTCP 的运营商 PAT 端口分配增强功能确保对 SIP、H.323 和 Skinny 语音呼叫进行增强。用于 RTP 流的端口号为偶数端口号，而 RTCP 流是随后的下一个奇数端口号。端口号将转换为符合 RFC-1889 的指定范围内的数字。如果呼叫的端口号在此范围内，则会将PAT转换到此范围内的另一个端口号。同样，此范围之外的端口号的PAT转换不会导致到给定范围之内的号码的转换。

问： 什么是会话初始协议 (SIP)？SIP 数据包是否可以进行 NAT？

答：会话发起协议 (SIP) 是一种基于 ASCII 的应用层控制协议，可用于在两个或多个终端之间建立、维护和终止呼叫。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 数据包可以进行 NAT。

问： 什么是对会话边界控制器 (SBC) 的托管 NAT 遍历支持？

答：通过适用于 SBC 的 Cisco IOS 托管 NAT 遍历功能，Cisco IOS NAT SIP 应用层网关 (ALG) 路由器可以充当思科多业务 IP 到 IP 网关上的 SBC，这有助于确保顺利提供 IP 网络语音 (VoIP) 服务。

有关详细信息，请参阅配置会话边界控制器的 Cisco IOS 托管 NAT 遍历。

问： 路由器内存和 CPU 可以使用 NAT 处理多少 SIP 呼叫、Skinny 呼叫和 H323 呼叫？

答：NAT 路由器处理的呼叫数取决于设备上可用的内存量和 CPU 处理能力。

问： NAT路由器是否支持Skinny和H323数据包的TCP分段？

答：Cisco IOS-NAT支持12.4 Mainline中的H323的TCP分段，并且从12.4(6)T开始支持SKINNY的TCP分段。

问：在语音部署中使用 NAT 过载配置时，是否有任何需要注意的警告？

答：是的。使用 NAT 过载配置和语音部署时，注册消息需要通过 NAT，并且您需要创建一个关联，以便从外部向内部发送的数据到达该内部设备。内部设备定期发送此注册，NAT 根据信令消息中的信息更新此针孔/关联。

问：在语音部署中发出 clear ip nat trans * 命令或 clear ip nat trans forced 命令是否会导致已知问题？

A.在语音部署中，如果发出clear ip nat trans *命令或clear ip nat trans forced命令并且使用动态NAT，则会清除针孔/关联，必须等待来自内部设备的下一个注册周期才能重新建立针孔/关联。思科建议您不要在语音部署中使用这些清除命令。

问： NAT 是否支持语音联合定位解决方案？

答：目前不支持联合定位解决方案。使用NAT的下一个部署（在同一机箱上）被视为一个共置解决方案：CME/DSP-Farm/SCCP/H323。

问： NVI 是否支持 Skinny ALG、H323 ALG 和 TCP SIP ALG？

答：请注意，UDP SIP ALG（为大多数部署所用）不受影响。

NAT 与 VRF/MPLS

问：NAT路由器在全局地址空间进行NAT的同时，是否也支持NAT在VRF中对同一地址空间进行NAT？目前，我在尝试配置以下内容时收到以下警告：“%类似的静态条目

(10.1.1.1 —> 10.210.2.2)已存在”：

<#root>

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED

A.传统NAT支持不同VRF上的重叠地址配置。对于特定 VRF 上的流量，您必须使用 match-in-vrf 选项在规则中配置重叠，并在同一 VRF 中设置 ip nat inside/outside。不支持全局路由表重叠。

对于不同的 VRF，必须为重叠 VRF 静态 NAT 条目添加 match-in-vrf 关键字。但是，无法重叠全局和 VRF NAT 地址。

<#root>

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf

72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf

问： 传统 NAT 是否支持 VRF-Lite（在两个 VRF 之间进行 NAT）？

答：您必须使用 NVI 才能在两个不同的 VRF 之间进行 NAT。您可以使用传统NAT执行从VRF到全局的NAT或同一VRF内的NAT。

NAT NVI

问：什么是 NAT NVI？

答：NVI 代表 NAT 虚拟接口。它允许 NAT 在两个不同的 VRF 之间进行转换。此解决方案必须代替单接口网络地址转换。

问：在全局接口和VRF中的接口之间执行NAT时，是否必须使用NAT NVI？

答：思科建议您使用传统 NAT 将 VRF 转换为全局 NAT (ip nat inside/out) 以及在同一 VRF 中的两个接口之间转换。NVI 用于不同 VRF 之间的 NAT。

问： NAT NVI 是否支持 TCP 分段？

答：NAT NVI 不支持 TCP 分段。

问： NVI 是否支持 Skinny ALG、H323 ALG 和 TCP SIP ALG？

答：请注意，UDP SIP ALG（为大多数部署所用）不受影响。

问： SNAT 是否支持 TCP 分段？

答：SNAT 不支持任何 TCP ALG（例如 SIP、SKINNY、H323 或 DNS）。因此，不支持 TCP 分段。但是，支持 UDP SIP 和 DNS。

SNAT

问：什么是有状态 NAT (SNAT)？

答：SNAT 允许两个或多个网络地址转换器充当转换组。转换组中的一个成员负责处理需要转换 IP 地址信息的流量。此外，它还会在出现活动流时通知备份转换器。然后，备份转换器可以使用活动转换器中的信息来准备重复的转换表条目。因此，如果活动转换器受到严重故障的阻碍，流量可以快速切换到备份转换器。由于使用相同的网络地址转换并且之前已对这些转换的状态进行了定义，因此，流量可以继续流动。

问： SNAT 是否支持 TCP 分段？

答：SNAT 不支持任何 TCP ALG（例如 SIP、SKINNY、H323 或 DNS）。因此，不支持 TCP 分段。但是，支持 UDP SIP 和 DNS。

问： SNAT是否支持不对称路由？

A.非对称路由通过启用为队列来支持NAT。默认情况下，“排队时”处于启用状态。不过，从 12.4(24)T 开始，不再支持“排队时”。客户必须确保正确路由数据包，并增加适当的延迟，以使非对称路由正常工作。

NAT-PT（v6 到 v4）

问：NAT-PT 是什么？

答：NAT-PT 是 NAT 的 v4 到 v6 转换。协议转换(NAT-PT)是IPv6-IPv4转换机制(如RFC 2765 和 RFC 2766 中所定义)，它允许仅IPv6设备与仅IPv4设备通信，反之亦然。

问： 思科快速转发 (CEF) 路径是否支持 NAT-PT？

答：CEF 路径不支持 NAT-PT。

问： NAT-PT 支持哪些 ALG？

答：NAT-PT 支持 TFTP/FTP 和 DNS。NAT-PT 不支持语音和 SNAT。

问： ASR 1004 是否支持 NAT-PT？

答：汇聚多业务路由器 (ASR) 使用 NAT64。

与平台相关的思科 7300/7600/6k

问：有状态 NAT (SNAT) 是否可用于 SX 系列的 Catalyst 6500？

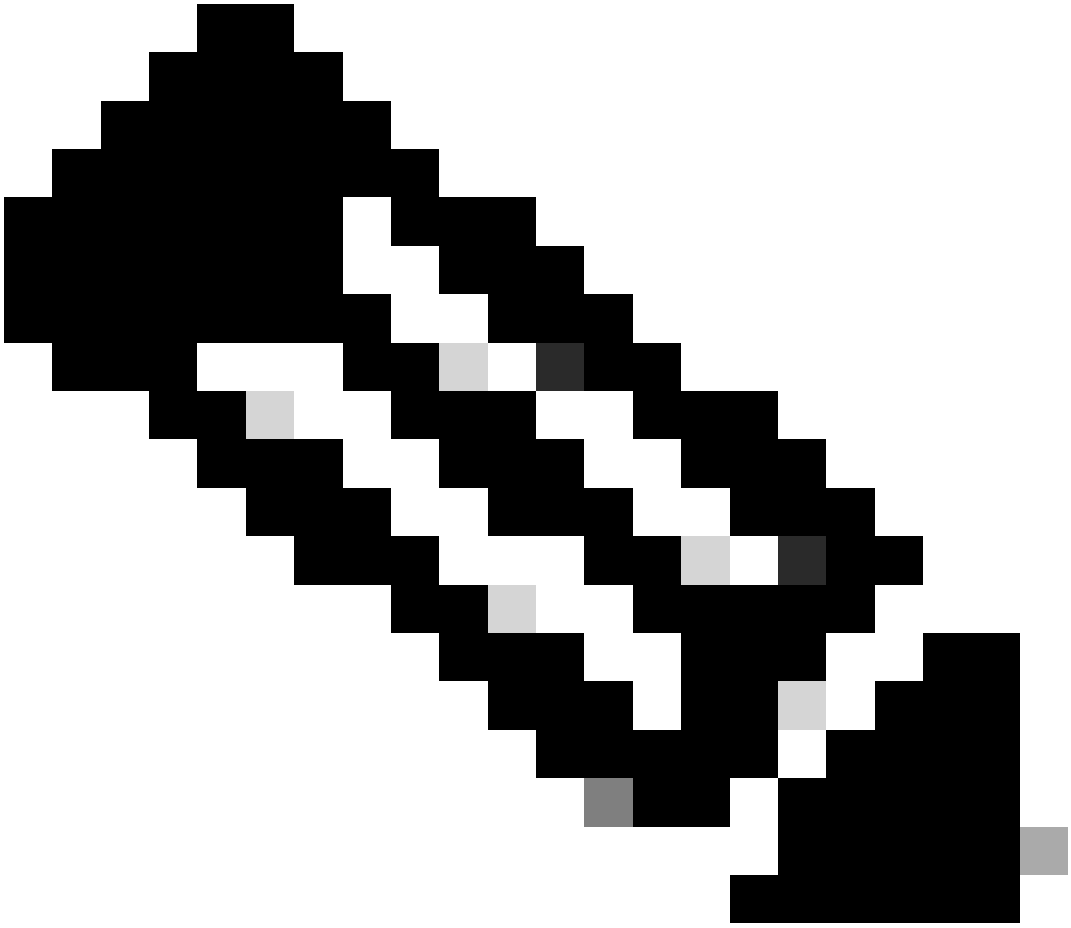
答：SNAT 不可用于 SX 系列的 Catalyst 6500。

问： 6k 上的硬件是否支持 VRF 感知型 NAT？

答：此平台上的硬件不支持 VRF 感知型 NAT。

问： 7600 和 Cat6000 是否支持 VRF 感知型 NAT？

答：65xx/76xx 平台不支持 VRF 感知型 NAT，并且会阻止 CLI。



注意：可以利用在虚拟上下文透明模式下运行的 FWSM 来实施设计。

与平台相关的思科 850

问：思科 850 是否支持 12.4T 版本中的 Skinny NAT ALG？

答：否。850 系列不支持 12.4T 中的 Skinny NAT ALG。

NAT 部署

问：如何实施 NAT？

A. NAT允许使用未注册IP地址的私有IP网际网络连接到Internet。在将数据包转发到另一个网络之前，NAT 将内部网络中的私有 (RFC1918) 地址转换为合法的可路由地址。

问： 如何使用语音实施 NAT？

答：使用 NAT 语音支持功能，通过配置有网络地址转换 (NAT) 的路由器传递的 SIP 嵌入消息可以转换回数据包。将应用层网关 (ALG) 与 NAT 结合使用可转换语音数据包。

问： 如何将 NAT 与 MPLS VPN 相集成？

答：使用 NAT 与 MPLS VPN 的集成功能，可以在单个设备上配置多个 MPLS VPN，从而实现协同工作。NAT 可以区分其接收的 IP 流量来自哪个 MPLS VPN，即使多个 MPLS VPN 都使用相同的 IP 寻址方案也是如此。利用这一增强功能，多个 MPLS VPN 客户可以在共享服务的同时确保每个 MPLS VPN 彼此完全独立。

问： NAT 静态映射是否支持 HSRP 以实现高可用性？

答：如果某个地址配置了网络地址转换 (NAT) 静态映射并且由路由器所有，则针对该地址触发地址解析协议 (ARP) 查询时，NAT 将使用 ARP 所指向的接口上的 BIA MAC 地址做出响应。两个路由器分别充当 HSRP 活动路由器和备用路由器。必须启用并配置它们的 NAT 内部接口才能属于某个组。

问： 如何实施NAT NVI？

答：使用 NAT 虚拟接口 (NVI) 功能时，无需将接口配置为 NAT 内部或 NAT 外部接口。

问： 如何使用 NAT 实现负载均衡？

A.使用NAT可以完成两种负载均衡：可以对一组服务器的入站负载进行负载均衡，以便将负载分配到服务器上，也可以通过两个或多个ISP将用户流量负载均衡到互联网。

有关出站负载均衡的更多信息，请参阅两个ISP连接的Cisco IOS NAT负载均衡。

问： 如何将NAT与IPSec结合使用？

答：我们支持通过 NAT 和 IPSec NAT 透明功能实现的 IP 安全 (IPSec) 封装安全负载 (ESP)。

利用“通过 NAT 的 IPSec ESP”功能，可以借助在过载或端口地址转换 (PAT) 模式下配置的思科 IOS NAT 设备支持多个并发 IPSec ESP 隧道或连接。

IPSec NAT 透明功能解决了 NAT 与 IPSec 之间的许多已知不兼容问题，可以支持 IPSec 流量通过网络中的 NAT 或 PAT 点。

问： 如何实施 NAT-PT？

答：NAT-PT（网络地址转换-协议转换）是一种IPv6-IPv4转换机制，如RFC 2765和RFC 2766 中所定义，它允许仅IPv6设备与仅IPv4设备通信，反之亦然。

问： 如何实施组播 NAT？

答：可以对组播流的源 IP 进行 NAT。在对组播执行动态 NAT 时不能使用路由图映射，因此，仅支持访问列表。

有关更多信息，请参阅组播 NAT 在思科路由器上如何工作。目标组播组使用组播服务反射解决方案进行 NAT。

问： 如何实施有状态 NAT (SNAT)？

答：SNAT 可以为动态映射的 NAT 会话提供连续服务。静态定义的会话无需 SNAT 即可获得冗余带来的益处。如果缺少 SNAT，则使用动态 NAT 映射的会话将在发生严重故障时中断，并且必须重新建立。系统仅支持最低的 SNAT 配置。只有在与您的思科客户团队沟通后，才能执行未来的部署，以便验证设计是否符合当前的限制。

建议在以下情况下使用SNAT：

- 由于与 HSRP 相比，主/备份模式缺少一些功能，因此不建议此模式。
- 故障切换场景以及使用 2 个路由器的设置。也就是说，如果一个路由器崩溃，另一个路由器可以无缝接管。（SNAT 架构无法用来处理接口震荡问题。）
- 支持对称路由场景。只有在应答数据包中的延迟大于 2 个 SNAT 路由器之间交换 SNAT 消息的延迟时，才能处理非对称路由。

目前SNAT架构的设计目的不是处理稳健性；因此，这些测试预计不会成功：

- 有流量时，清除 NAT 条目。
- 在有流量时更改接口参数（如IP地址更改、关闭/不关闭等）。
- SNAT 特定的 clear 或 show 命令应当不会正常执行，也不推荐使用。

  与SNAT相关的部分clear< /strong>和show命令如下所示：

  <#root>

  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，可以使用clear ip nat trans forced< /strong>或clear ip nat trans *命令。
- 如果用户要查看条目，可以使用< show ip nat translation 、show ip nat translations verbose 和show ip nat stats 命令。如果已配置内部服务，它也会显示SNAT特定的信息。

- 建议不要清除备份路由器上的 NAT 转换。始终清除主 SNAT 路由器上的 NAT 条目。
- SNAT不是HA；因此，两台路由器上的配置必须相同。两台路由器必须运行相同的映像。此外，还要确保两个 SNAT 路由器使用相同的基础平台。

NAT 最佳做法

问：是否有 NAT 最佳做法？

答：是的。NAT 最佳做法如下所示：

1. 同时使用动态和静态NAT时，为动态NAT设置规则的ACL必须排除静态本地主机，这样就不会发生重叠。
2. 将 NAT 的 ACL 与 permit ip any any 配合使用时要谨慎，因为您会获得不可预知的结果。在12.4(20)T之后，如果本地生成的HSRP和路由协议数据包是从外部接口发送出去的，NAT会对其进行转换，也会转换与NAT规则匹配的本地加密数据包。
3. 如果将重叠网络用于 NAT，请使用 match-in-vrf 关键字。

   对于不同的 VRF，必须为重叠 VRF 静态 NAT 条目添加 match-in-vrf 关键字，但不能重叠全局和 VRF NAT 地址。

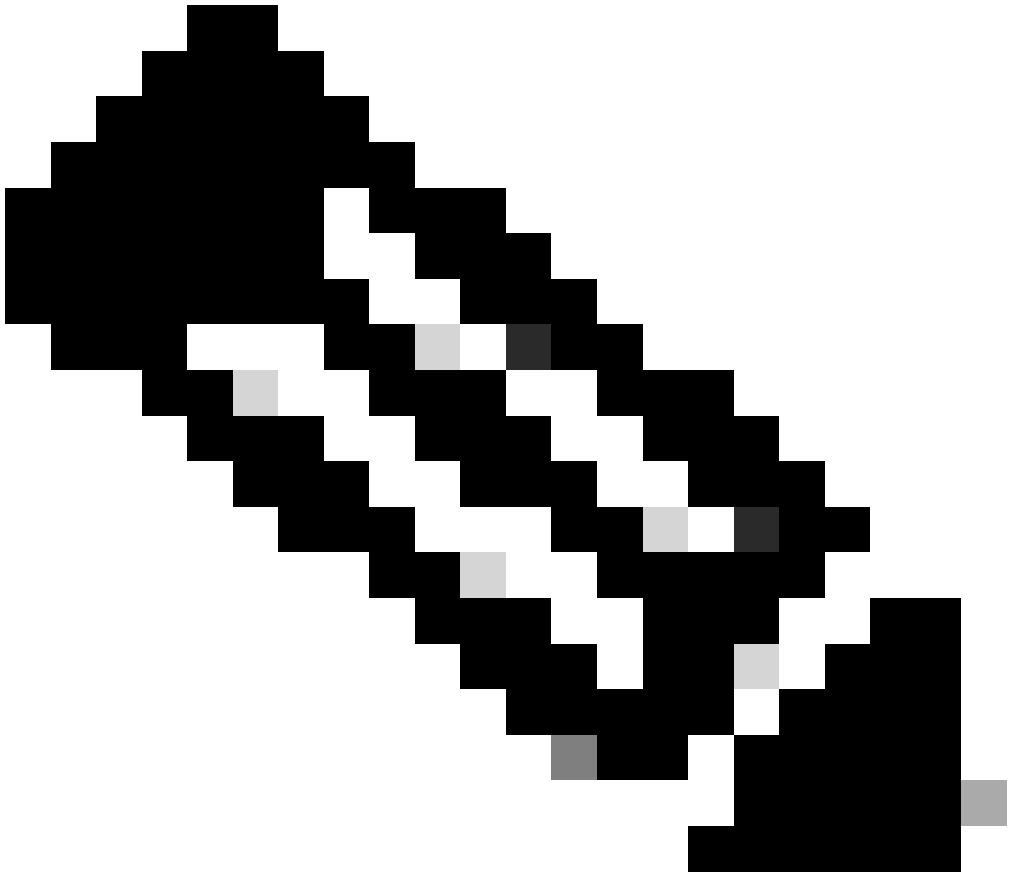
   ```
   <#root>
   Router(config)#
   ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
   ```

   ```
   <#root>
   Router(config)#
   ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
   ```

4. 除非使用 match-in-vrf 关键字，否则不能在不同的 VRF 中使用地址范围相同的 NAT 池。

   例如：

   ```
   <#root>
     ip nat pool poolA 1710.1.1.1 1710.1.1.10 prefix-length 24
     ip nat pool poolB 1710.1.1.1 1710.1.1.10 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：即使CLI配置有效，但不支持没有match-in-vrf关键字的配置。

5. 使用 NAT 接口过载部署 ISP 负载均衡时，最佳做法是通过 ACL 匹配将路由图映射用于接口匹配。
6. 使用池映射时，不能使用两个不同的映射（ACL或路由映射）来共享同一个NAT池地址。
7. 在故障切换场景中，当在两个不同路由器上部署相同的NAT规则时，必须使用HSRP冗余。
8. 不要在静态 NAT 和动态池中定义相同的内部全局地址。否则，将会导致意外的结果。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。