使用常见问题排除网络地址转换故障

目录

简介

本文档介绍网络地址转换(NAT)路由器进程的工作方式，并提供一些常见问题的答案。

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，通常是在您将两个网络连接到一起时，它会将内部网络中的私有（非全局唯一）地址转换为合法地址，然后再将数据包转发到另一个网络。

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。这可以有效地将整个内部网络隐藏在该地址后面，从而提供额外的安全性。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：基本上，NAT允许单个设备（如路由器）作为互联网（或公共网络）和本地网络（或专用网络）之间的代理，这意味着只需单个唯一IP地址即可代表整个计算机组到其网络外部的任何设备。

问：如何配置 NAT？

A.要配置传统NAT，您需要在路由器上至少建立一个接口（NAT外部）和路由器上的另一个接口（NAT内部），并为数据包报头中的IP地址制定一组转换规则（如果需要，还包括有效负载），并且这些转换规则需要配置。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其配置NAT虚拟接口部分。

问：Cisco IOS®软件和Cisco Adaptive Security Appliance(ASA)实施NAT的主要区别是什么？

A.基于Cisco IOS软件的NAT与Cisco ASA中的NAT功能没有本质上的区别。主要区别包括实施和设计要求中支持的不同流量类型。有关在Cisco ASA设备上配置NAT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 在哪些思科路由硬件上可用？如何订购硬件？

答：Cisco Feature Navigator工具允许客户识别功能(NAT)，并查找可用的Cisco IOS软件功能的版本和硬件版本。要使用此工具，请参阅Cisco功能导航器。

问：NAT 是发生在路由之前还是之后？

A.NAT处理事务的顺序取决于数据包是从内部网络传输到外部网络还是从外部网络传输到内部网络。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能否在公共无线局域网环境中部署？

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，并使这些用户能够在公共无线LAN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。使用NAT，您可以在内部网络上建立一个虚拟主机，以协调实际主机之间的负载均衡。

问：是否可以对 NAT 转换数量进行速率限制？

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。这样，用户可以更好地控制NAT地址的使用方式，速率限制NAT转换功能可用于限制病毒、蠕虫和拒绝服务攻击的影响。

问：NAT 使用的 IP 子网或地址如何获知或传播路由？

A.如果出现以下情况，则会获取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会安装IP别名和ARP条目，在这种情况下，路由器**canproxy-arp**会为这些地址分配地址。如果不需要此行为，请使用**theno-aliaskeyword**。

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 支持多少个并发 NAT 会话？

A.NAT会话限制受路由器中可用DRAM数量的限制。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。但是，也建议验证平台规格。

问：使用Cisco IOS NAT可以预期哪种路由性能？

A.Cisco IOS NAT支持Cisco快速转发(CEF)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？

是的。源和/或目标NAT转换可应用于具有IP地址（包括拨号程序接口）的任何接口或子接口。无法使用无线虚拟接口配置 NAT。无线虚拟接口在写入NVRAM时不存在。因此，重新启动后，路由器会丢失无线虚拟接口上的NAT配置。

问：Cisco IOS NAT 是否能够与热备份路由器协议 (HSRP) 配合使用以提供到 ISP 的冗余链路？

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：Cisco 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？

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，请参阅前一个问题：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？

是的。这可以通过使用访问列表而实现，该列表介绍了需要 NAT 的主机或网络集。同一主机上的所有会话可以转换，也可以通过路由器而不可以转换。

访问列表、扩展访问列表和路由映射可用于定义IP设备转换的依据。必须始终指定网络地址和适当的子网掩码。不能使用关键字来代替网络地址或子网掩码。使用静态NAT配置时，当数据包与任何STATIC规则配置都不匹配时，数据包无需任何转换即可通过。

问：配置PAT（过载）时，每个内部全局IP地址可创建的最大转换数是多少？

A.PAT（过载）将每个全局IP地址的可用端口分为三个范围：0-511、512-1023和1024-65535。PAT 为每个 UDP 或 TCP 会话分配唯一的源端口。它会尝试分配原始请求的相同端口值，但如果原始源端口已被使用，它会开始从特定端口范围的开始进行扫描，以查找第一个可用端口，并将其分配给会话。

问：PAT 的工作原理是什么？

A.PAT使用一个全局IP地址或多个地址。

使用一个IP地址表的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或端口”可以使用，则PAT会
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
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，则PAT从相关组的开头开始搜索（对于TCP或UDP应用程序，从1开始；对
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。

注意：对于传输控制协议(TCP)和用户数据报协议(UDP)，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。

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源端口。
9	如果请求的源端口可用，NAT将分配源端口，会话继续进行。
10	如果请求的源端口不可用，则NAT从相关组的开头开始搜索（TCP或UDP应用程序从1开始，ICMP从
11	如果端口可用，则分配该端口，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。

问：什么是 NAT IP 池？

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

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

示例 1

下一个示例将从网络192.168.1.0或192.168.2.0寻址的内部主机转换到全球唯一的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

在下一个示例中，目标是定义虚拟地址，连接分布在一组真实主机中。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：可配置的 NAT IP 池 (ip nat pool "name") 的最大数量是多少？

A.在实际使用中，可配置IP池的最大数量受特定路由器中可用DRAM数量的限制。（思科建议您将池大小配置为 255。）每个池的长度不得超过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。

问：与NAT池上的ACL相比，路由映射有何优点？

A.路由映射可保护不需要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。有关详细信息，请参阅对使用路由映射的多池的NAT支持。

问：NAT 环境中的 IP 地址“重叠”是什么？

A.IP地址重叠是指两个要互连的位置使用相同的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。

私有IP地址不可路由，需要NAT转换才能连接到外部世界。 该解决方案涉及从外部到内部的域名系统(DNS)名称查询响应的拦截、外部地址的转换设置，以及DNS响应在转发到内部主机之前需要修复。 NAT设备的两端均需要使用DNS服务器，才能解析要在两个网络之间建立连接的用户。

NAT能够检查并执行DNSA和PTR记录内容的地址转换，如在重叠网络中使用NAT所示。

问：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有一对一映射。用户还可以配置到端口级别的静态地址转换，并将IP地址的其余部分用于其他转换。当您执行端口地址转换(PAT)时，通常会发生这种情况。

下一个示例显示如何配置路由映射以允许静态NAT的外部到内部转换：

```
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 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

问：术语*NATOverloading*是什么意思；这是什么PAT?

是的。NAT过载是PAT，它涉及使用包含一个或多个地址范围的池，或者将接口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。这是一个包含IP地址和源/目标端口信息的转换表条目，通常称为PAT或过载。

PAT（或过载）是Cisco IOS NAT的一项功能，用于将*内部*（内部本地）私有地址转换为一个或多个*外部*（内部全局，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。

问：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。当您定义要转换的本地地址和要从中分配全局地址的地址池或接口IP地址时，以及当您关联这两个地址池时，即可完成动态映射。

问：什么是 ALG？

A.ALG是应用层网关(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)。

有关详细信息，请参阅将应用级网关与NAT配合使用。

问：是否可以同时使用静态和动态 NAT 转换来构建配置？

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，静态转换中使用的全局地址不会自动排除为包含这些相同全局地址的动态池。必须创建动态池才能排除静态条目分配的地址。有关详细信息，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必须显示NAT全局地址还是必须泄漏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：全范围和端口映射。

- 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。

有关详细信息，请参阅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。
- 对称端口允许NAT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 Don't Fragment (DF) 数据包的IP报头中未设置位，数据包可以分段。如果在数据包的IP报头中设置了DF位，则会丢弃该数据包，并且ICMP错误消息会指示返回发送方的下一跳MTU值。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。有关详细信息，请参阅解决GRE和IPsec的IP分段、MTU、MSS和PMTUD问题。

TCP分段在终端站上的应用程序发送数据时发生。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可以首先将数据分段为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可以添加IP报头以将数据包发送到远程终端主机。如果TCP数据段的IP数据包大于TCP主机之间路径上传出接口上的IP MTU，则IP可以对IP/TCP数据包进行分段以适应。这些IP数据包分段可以通过IP层在远程主机上重组，而完整的TCP数据段（最初发送的）可以交给TCP层。TCP 层不知道在传输过程中 IP 已对数据包进行了分段。

NAT 支持 IP 分段，但不支持 TCP 段。

问：NAT 是否支持无序的 IP 分段和 TCP 分段？

A.NAT仅支持无序的IP分段，因为**ofip virtual-reassembly**。

问：如何调试 IP 分段和 TCP 分段？

A.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：不需要。不支持的NAT MIB也不支持CISCO-IETF-NAT-MIB。

问：什么是*TCP超时*，它与NAT TCP计时器有何关系？

A.如果三次握手尚未完成，并且NAT看到TCP数据包，则NAT可以启动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转换的时间更改为超时？

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：当轻量级目录访问协议(LDAP)将额外的字节附加到每个LDAP应答数据包时，如何停止该协议？

A.LDAP设置为在处理Search-Res-Entry类型的消息时添加额外的字节（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。如果额外的10个字节的数据产生数据包，超过网络中的最大传输单位(MTU)，该数据包将被丢弃。在这种情况下，Cisco建议您使用**CLIno ip nat service append-ldap-search-rescommand**关闭此LDAP行为，以便发送和接收数据包。

问：对 NAT 设备上的内部全局/外部本地 IP 地址有何路由建议？

A.必须在NAT配置框中为诸如NAT-NVI等功能的内部全局IP地址指定路由。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，来自具有外部静态规则的in-to-out方向的任何数据包都需要这种路由。在这种情况下，当它为IG/OL提供路由时，还必须配置下一跳IP地址。如果未找到下一跳配置，则将其视为配置错误，会导致未定义的行为。

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?

A.当配置动态NAT转换的Cisco IOS NAT时，使用ACL识别可以转换的数据包。当前NAT架构不支持带有**log**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。

NAT 尚不支持 SCCP v17。在实施SCCP v17的NAT支持之前，必须将固件降级到版本8-3-5或更低版本，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？

A.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 的运营商 PAT 端口分配增强功能？

答：RTP和RTCP的服务提供商PAT端口分配增强功能可确保SIP、H.323和Skinny语音呼叫的端口分配。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。端口号将转换为指定范围内的一个符合RFC-1889的端口号。如果呼叫的端口号在该范围内，则可能导致PAT转换到此范围内的另一个端口号。同样，此范围外的端口号的PAT转换不能导致转换到给定范围内的号码。

问：什么是会话发起协议(SIP)，是否可以使用NAT路由SIP数据包？

A.会话发起协议(SIP)是基于ASCII的应用层控制协议，可用于建立、维护和终止两个或多个终端之间的呼叫。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：Cisco IOS Hosted NAT Traversal for SBC功能使Cisco IOS NAT SIP应用级网关(ALG)路由器能够充当Cisco多服务IP到IP网关上的SBC，这有助于确保IP语音(VoIP)服务的顺利交付。

有关详细信息，请参阅为会话边界控制器配置Cisco IOS托管的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？

A.NAT路由器处理的呼叫数取决于机箱上的可用内存量和CPU的处理能力。

问：NAT 路由器是否支持对 Skinny 数据包和 H323 数据包进行 TCP 分段？

A.Cisco IOS-NAT支持H323的TCP分段和SKINNY的TCP分段支持。

问：在语音部署中使用NAT过载配置时，是否有需要注意的注意事项？

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：在语音部署中使用clear ip nat trans *命令或clear ip nat trans forcedcommand时，是否引起任何已知问题？

A.在语音部署中，当您发出**clear ip nat trans ***命令或**acclear ip nat trans** forcedcommand并具有动态NAT时，您会清除针孔/关联，并且必须等待来自内部设备的下一个注册周期来重新建立此连接。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：不需要。目前不支持联合定位解决方案。下一个使用NAT的部署（在同一台设备上）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：不需要。请注意，UDP SIP ALG（用于大多数部署）不受影响。

NAT 与 VRF/MPLS

问：NAT路由器能否在VRF中的相同地址空间和全局地址空间中支持自身？目前，当我尝试配置以下项时，我收到此警告："%类似的静态条目(*10.1.1.1 —> 10.2.2.2)已经存在"：*

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

A.传统NAT支持不同VRF上的重叠地址配置。您必须使用**match-in-**vrfoption配置重叠规则并在同一VRF中为该特定VRF上的流量设置**upip nat inside/outside。**不支持全局路由表重叠。

您必须为不同VRF的重叠VRF静态NAT条目添加**match-in-vrfkeyword**。但是，无法重叠全局和 VRF NAT 地址。

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

问：传统NAT是否支持VRF-Lite（从VRF到不同VRF的路由）？

答：不需要。必须在不同VRF之间使用NVI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？

A.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。必须使用此解决方案代替单接口网络地址转换。

问：是否必须使用NAT NVI在全局接口和VRF中的接口之间进行路由？

A.Cisco建议您使用传统NAT进行VRF到全局NAT(ip nat inside/out)以及同一VRF中接口之间的转换。NVI 用于不同 VRF 之间的 NAT。

问：NAT NVI 是否支持 TCP 分段？

A.不支持NAT-NVI的TCP分段。

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

答：不需要。请注意，UDP SIP ALG（用于大多数部署）不受影响。

问：SNAT 是否支持 TCP 分段？

A.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)？

A.SNAT允许两个或多个网络地址转换程序用作转换组。转换组的一个成员处理需要转换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？

A.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是否支持非对称路由？

A. 非对称路由在启用NAT时支持NAT as-queuing .默认情况下，“排队时”处于启用状态。然而，从12.4(24)T开始， as-queuing 不再受支持。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？

A.NAT-PT是用于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，它允许纯IPv6设备与纯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？

A.CEF路径不支持NAT-PT。

问：NAT-PT 支持哪些 ALG？

A.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？

A.聚合服务路由器(ASR)使用NAT64。

依赖于平台的Cisco 7600/6k

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

A.SNAT在SX系列的Catalyst 6500上不可用。

问：6k 上的硬件是否支持 VRF 感知型 NAT？

A.此平台上的硬件不支持VRF感知NAT。

问：7600 和 Cat6000 是否支持 VRF 感知型 NAT？

A.在65xx/76xx平台上，不支持VRF感知NAT，且CLI被阻止。

注意：如果利用在虚拟环境透明模式下运行的FWSM，则可以实施设计。

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：不需要。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地址的专用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？

A.语音的NAT支持功能允许通过配置了网络地址转换(NAT)的路由器的SIP嵌入式消息转换回数据包。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？

A.NAT与MPLS VPN的集成功能允许在单个设备上配置多个MPLS VPN以协同工作。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。此增强功能使多个MPLS VPN客户能够共享服务，同时确保每个MPLS VPN彼此完全分离。

问：NAT 静态映射是否支持 HSRP 以实现高可用性？

A.当对配置了网络地址转换(NAT)静态映射并且路由器拥有的地址触发地址解析协议(ARP)查询时，NAT会以ARP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?

A.NAT虚拟接口(NVI)功能取消将接口配置为NAT内部或NAT外部的要求。

问：如何使用 NAT 实现负载均衡？

答：NAT有两种类型的负载均衡可以完成：您可以对一组服务器的入站负载均衡以分配服务器上的负载，也可以通过两个或多个ISP将用户流量负载均衡到Internet。

有关出站负载均衡的详细信息，请参阅两个ISP连接的Cisco IOS NAT负载均衡。

问：如何将NAT与IPSec结合实施？

A.支持 IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT 和IPSec NAT透明性。

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透明功能支持IPSec流量通过网络中的NAT或PAT点，因为它解决了NAT和IPSec之间的许多已知不兼容问题。

问：如何实施 NAT-PT？

A.NAT-PT（网络地址转换 — 协议转换）是IPv6-IPv4转换机制，如RFC 2765和RFC 2766中定义，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？

A.可以对组播流的源IP进行NAT。当组播动态NAT完成时，不能使用路由映射，因此仅支持访问列表。

有关详细信息，请参阅组播NAT如何在Cisco路由器上工作。目标组播组使用带有组播服务反射解决方案的NAT。

问：如何实施有状态 NAT (SNAT)？

A.SNAT为动态映射的NAT会话启用持续服务。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。只有在您与思科客户团队沟通后，才能执行未来部署，以验证与当前限制相关的设计。

建议在以下场景中使用SNAT:

- 主/备份不是推荐模式，因为与HSRP相比，有些功能缺失。
- 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架构在设计时并未考虑稳健性；因此，这些测试预计不会成功：

- 当有流量时清除NAT条目时。

- 当存在流量时，接口参数（如IP地址更改、关闭/不关闭等）发生更改时。
- SNAT specificclearorshowcommand预计不能正确执行，建议不要执行。一些SNAT相关的clearandshowcommand如下：

```
clear ip snat sessions *
clear ip snat sessions
```

```
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>
```

- 如果用户想要清除条目，clear ip nat trans forcedorclear ip nat trans *命令可用。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*配置了内部服务，则它还可以显示SNAT特定信息。
- 建议不要在备用路由器上清除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，请确保用于两个SNAT路由器的底层平台相同。

NAT 最佳做法

问：是否有 NAT 最佳做法？

是的。NAT 最佳做法如下所示：

1. 当您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. 如果将ACL用于permit ip any any的NAT，则可能会得到无法预测的结果。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可以转换这些数据包，也可以转换与NAT规则匹配的本地加密数据包。
3. 当NAT的网络重叠时，请使用match-in-vrfkeyword。您必须为不同VRF的重叠VRF静态NAT条目添加match-in-vrfkeyword，但无法重叠全局和vrf NAT地址。

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

4. 除非使用match-in-vrfkeyword，否则具有相同地址范围的NAT池不能用于不同VRF。例如：

```
ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
ip nat pool poolB 172.31.1.1 172.31.1.10 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：即使CLI配置有效，但如果不使用match-in-vrf关键字，则不支持配置。
5. 当您使用NAT接口过载部署ISP负载均衡时，最佳实践是使用路由映射，通过ACL匹配进行接口匹配。
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，当您在两个不同的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

- 技术支持和文档 - Cisco Systems

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）。