验证 NAT 的运行和基本的 NAT 故障排除

目录

简介

NAT 环境中发生 IP 连通性问题时，经常难以确定问题的原因。事实上在存在潜在问题的时候，常常错误地归咎于 NAT。本文说明如何使用 Cisco 路由器上现有的工具来验证 NAT 的运行。我们还将向您说明如何执行基本的 NAT 故障排除以及如何避免 NAT 故障排除中的常见错误。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

如何排除 NAT

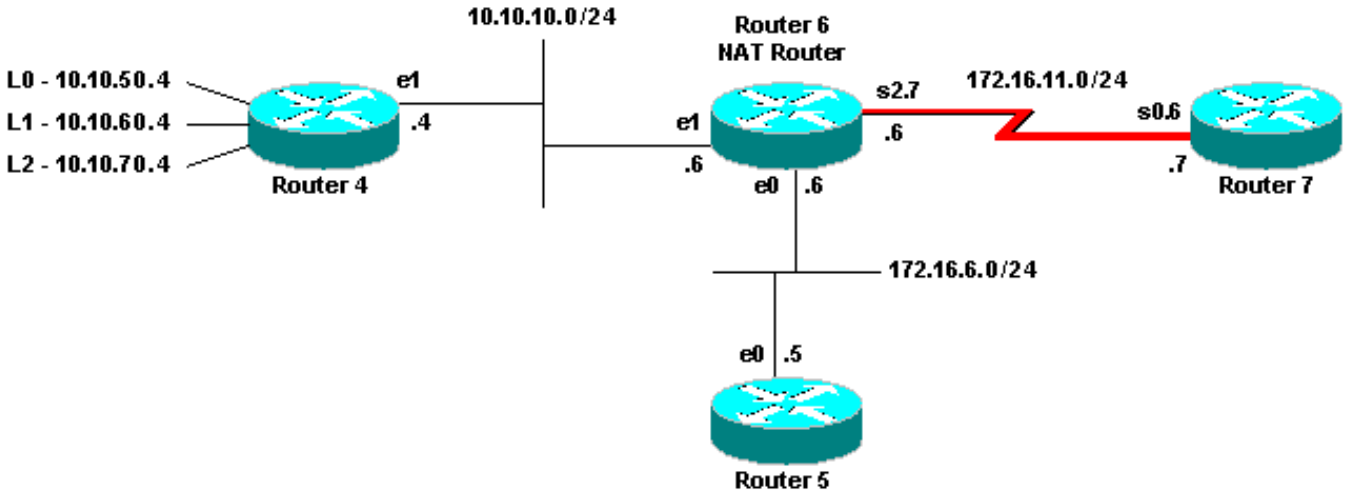
当您尝试确定 IP 连接问题的原因时，它有助于排除 NAT。请执行下列步骤来检验 NAT 是否如预期一样工作：

1. 根据配置，清楚地确定应该实现什么样的 NAT。这时您可以确定该配置是否有问题。有关配置 NAT 的帮助，请参阅配置网络地址转换：部分。
2. 检验转换表中是否有正确转换。
3. 使用 **show** 和 debug 命令验证是否正在进行转换。
4. 详细观察数据包的处理过程，并检验路由器是否有传输数据包所需要的正确路由信息。

以下是一些问题实例，在这里，我们使用上述步骤来帮助确定问题的原因。

问题示例：能 Ping 一个路由器，但不能 Ping 另一个

在下面的网络图中，路由器 4 可以 ping 路由器 5（172.16.6.5），但却不能 ping 路由器 7（172.16.11.7）：



所有路由器都没有运行路由协议，而且 Router 4 将 Router 6 当作自己的默认网关。按以下方式对 NAT 配置路由器 6：

路由器 6

```
interface Ethernet0
 ip address 172.16.6.6 255.255.255.0
 ip directed-broadcast
 ip nat outside
 media-type 10BaseT
```

```
 !
interface Ethernet1
 ip address 10.10.10.6 255.255.255.0
 ip nat inside
 media-type 10BaseT
 !
interface Serial2.7 point-to-point
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
 frame-relay interface-dlci 101
 !
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length
24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
 !
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4
```

首先让我们确定 NAT 是否正常运行。我们从配置中可以知道，路由器 4 的 IP 地址（10.10.10.4）假定为以静态方式转换到 172.16.6.14。通过在路由器 6 上使用 **show ip nat translation** 命令，您可以检验转换表中是否存在该转换：

```
router-6# show ip nat translation Pro Inside global Inside local Outside local Outside global --
- 172.16.6.14 10.10.10.4 --- ---
```

现在，确保路由器 4 发出 IP 数据流时进行这一转换。您可以通过 Router 6 使用两种方式执行此操作：通过运行 NAT **debug** 或通过使用 show ip nat statistics 命令监控 NAT 统计数据。由于 **debug** 命令应始终用作最后手段，因此请先使用 show 命令。

此处的目的是监控成功次数计数器，查看在从路由器发送数据流时它是否增加。每次使用转换表中的转换进行地址转换时，成功次数计数器都会增加。首先清除统计数据，然后显示统计数据，试着从路由器 4 上 ping 路由器 7，然后再显示统计数据。

```
router-6# clear ip nat statistics router-6# router-6# show ip nat statistics Total active
translations: 1 (1 static, 0 dynamic; 0 extended) Outside interfaces: Ethernet0, Serial2.7
Inside interfaces: Ethernet1 Hits: 0 Misses: 0 Expired translations: 0 Dynamic mappings: --
Inside Source access-list 7 pool test refcount 0 pool test: netmask 255.255.255.0 start
172.16.11.70 end 172.16.11.71 type generic, total addresses 2, allocated 0 (0%), misses 0
router-6#
```

在路由器 4 上使用 **ping 172.16.11.7** 命令后，路由器 6 上的 NAT 统计数据显示如下：

```
router-6# show ip nat statistics Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces: Ethernet0, Serial2.7 Inside interfaces: Ethernet1 Hits: 5 Misses: 0 Expired
translations: 0 Dynamic mappings: -- Inside Source access-list 7 pool test refcount 0 pool test:
netmask 255.255.255.0 start 172.16.11.70 end 172.16.11.71 type generic, total addresses 2,
allocated 0 (0%), misses 0
```

我们可以从 **show** 命令中发现命中数增加 5。每次从 Cisco 路由器成功完成一次 ping 操作时，成功次数应该增加 10。源路由器（Router 4）发送的5个互联网控制消息协议（ICMP）ECHO应该被转换，而且来自目的地路由器（Router 7）的5个ECHO回复数据包也应该被转换，总共有10个Hit。5 个丢失的 hit 很可能是由 ECHO 回复未被转换或者路由器 7 未发送 ECHO 回复造成的。

检查是否存在可导致路由器 7 不向路由器 4 发达 Echo 回复数据包的任何原因。首先查看 NAT 对数据包执行的操作。Router 4 正在发送 ICMP 回应数据包，其源地址为 10.10.10.4，目的地地址为 172.16.11.7。完成 NAT 之后，Router 7 接收到的包的源地址为 172.16.6.14,目的地地址为 172.16.11.7。Router 7 需要对 172.16.6.14 作出应答，而由于 172.16.6.14 没有直接连接到 Router 7，因此，它需要网络的一个路由以便作出响应。让我们检查 Router 7 的路由表，以便检验是否存在该路由。

```
router-7# show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.12.0 is directly connected, Serial0.8 C
172.16.9.0 is directly connected, Serial0.5 C 172.16.11.0 is directly connected, Serial0.6 C
172.16.5.0 is directly connected, Ethernet0
```

我们发现路由器 7 的路由表没有 172.16.6.14 的路由。只要我们添加该路由，ping 操作就可以正常进行。

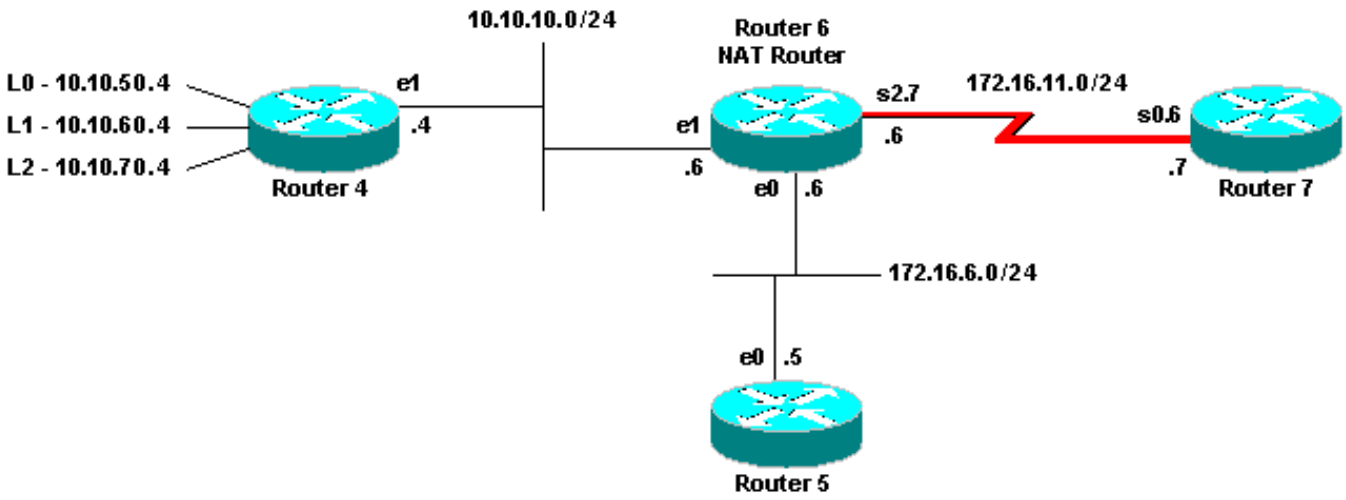
问题汇总

我们首先定义 NAT 要完成的任务。接下来，我们检验转换表中有静态NAT条目而且是正确的。我们通过监控 NAT 的统计信息来检验是否真正在进行转换。我们在那里发现一个问题，使得我们检查 Router 7 上的路由信息。我们发现 Router 7 需要一个到 Router 4 内部全局地址的路由。

请注意，在这种简单的试验室环境中，用 **show ip nat statistics** 命令来监控 NAT 的统计数据很有用。但是，在执行多个转换的更复杂的 NAT 环境中，这个 **show** 命令将不再有用。在这种情况下，可能需要在路由器上运行 **debugs** 命令。下一个问题场景演示了 **debug** 命令的使用。

问题示例：外部网络设备不能与内部路由器通信

在这种情况下，路由器 4 能 **ping** 通路由器 5 和路由器 7，但是 10.10.50.0 网络上的设备却不能与路由器 5 或路由器 7 通信（我们在测试实验室中通过从 IP 地址 10.10.50.4 的环回接口发出 ping 信号来模拟这种情况）。让我们查看其网络图：



路由器 6

```
interface Ethernet0
 ip address 172.16.6.6 255.255.255.0
 ip directed-broadcast
 ip nat outside
 media-type 10BaseT
 !
interface Ethernet1
 ip address 10.10.10.6 255.255.255.0
 ip nat inside
 media-type 10BaseT
 !
```

```
interface Serial2.7 point-to-point
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
 frame-relay interface-dlci 101
 !
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length
24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
 !
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4
```

首先，清楚地说明预期的 NAT 行为。从路由器 6 的配置可以知道，NAT 要以动态方式将 10.10.50.4 转换为 NAT 池“test”中的第一个可用地址。该池包括地址 172.16.11.70 和 172.16.11.71。根据您在上一个问题中所学到的知识，您可以推导出路由器 5 和路由器 7 收到的数据包的源地址将为 172.16.11.70 或 172.16.11.71。这些地址与路由器 7 位于同一个子网中，因此路由器 7 应该具有一个直接连接的路由，但路由器 5 需要路由到该子网（如果该路由器还没有子网）。

您可以使用 **show ip route** 命令查看路由器 5 的路由表是否列出 172.16.11.0：

```
router-5# show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.9.0 is directly connected, Serial1 S
172.16.11.0 [1/0] via 172.16.6.6 C 172.16.6.0 is directly connected, Ethernet0 C 172.16.2.0 is
directly connected, Serial0
```

您可以使用 **show ip route** 命令查看路由器 7 的路由表是否将 172.16.11.0 列为直接连接的子网：

```
router-7# show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.12.0 is directly connected, Serial0.8 C
172.16.9.0 is directly connected, Serial0.5 C 172.16.11.0 is directly connected, Serial0.6 C
172.16.5.0 is directly connected, Ethernet0 S 172.16.6.0 [1/0] via 172.16.11.6
```

我们现在已经清楚地说明了 NAT 要做的内容，我们需要检验它是否正常运行。我们以检查 NAT 转换表并检验预期的转换是否在正在开始。因为我们所关心的转换将被动态创建，因此，我们首先必须从相应地址发送 IP 数据流。在发送来源为 10.10.50.4，目标为 172.16.11.7 的 **ping** 后，路由器 6 中的转换表将显示：

```
router-6# show ip nat translation Pro Inside global Inside local Outside local Outside global --
- 172.16.6.14 10.10.10.4 --- --- --- 172.16.11.70 10.10.50.4 --- ---
```

由于转换表中存在预期的转换，因此，我们知道 ICMP 回应数据包正在得到适当转换，但是回送应答数据包又如何呢？如上所述，您可以监控 NAT 的统计数据，但是在复杂环境中不是很有帮助。另一个选项是在 NAT 路由器（路由器 6）上运行 NAT 调试。在这种情况下，当您发送来源为 10.10.50.4，目标为 172.16.11.7 的 ping 时，应该对路由器 6 执行 **debug ip nat**。**debug** 结果如下：

注意： 在对路由器执行 **debug** 命令时，可能会使路由器过载，从而导致路由器无法运行。在没有 Cisco 技术支持工程师的监督下，尽量不要对重要的生产路由器运行 **debug**，如果必需运行，请务必谨慎。

```
router-6# show log Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: level debugging, 39 messages logged Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 39 messages logged Trap logging: level informational, 33
message lines logged Log Buffer (4096 bytes): 05:32:23: NAT: s=10.10.50.4->172.16.11.70,
d=172.16.11.7 [70] 05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70] 05:32:25:
NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71] 05:32:25: NAT*: s=172.16.11.7,
d=172.16.11.70->10.10.50.4 [71] 05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72]
05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72] 05:32:29: NAT*: s=10.10.50.4-
>172.16.11.70, d=172.16.11.7 [73] 05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73]
05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74] 05:32:31: NAT*: s=172.16.11.7,
d=172.16.11.70->10.10.50.4 [74]
```

正如我们从以上 **debug** 命令输出所见，第一行显示源地址 10.10.50.4 正在转换为 172.16.11.70。第二行显示目的地地址 172.16.11.70 正在被转换回 10.10.50.4。整个 **debug** 命令执行过程的其余部分会重复这一情况。这告诉我们路由器 6 正在两个方向上转换数据包。

我们现在更加详细准确地观察正在发生的情况。Router 4 发送一个从 10.10.50.4 到 172.16.11.7 的包。Router 6 对该包进行 NAT 并转发一个源地址为 172.16.11.70、目标地址为 172.16.11.7 的包。Router 7 发送一个源为 172.16.11.7、目标为 172.16.11.70 的应答。路由器 6 对该数据包进行 NAT，产生一个源地址为 172.16.11.7 且目标地址为 10.10.50.4 的数据包。在这时，Router 6 应该根据其路由表中的信息将此包路由到 10.10.50.4。您需要使用 **show ip route** 命令来确认路由器 6 在路由表中有必需的路由。

```
router-6# show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.8.0 is directly connected, Serial1 C
172.16.10.0 is directly connected, Serial2.8 C 172.16.11.0 is directly connected, Serial2.7 C
172.16.6.0 is directly connected, Ethernet0 C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets C 10.10.10.0 is directly connected, Ethernet1
```

问题汇总

首先，我们清楚地定义了 NAT 要完成的任务。然后，我们检验转换表中是否有必要转换。第三，我们使用 **debug** 或 show 命令验证了是否确实执行了转换。最后，我们更加详细地观察了包的处理情况以及路由器需要什么条件以便转发或应答包。

故障排除列表

您现在掌握了一个基本程序，可找到导致连接问题的原因。以下是排除常见问题的检验表。

转换表里没有安装转换

如果您发现转换表中未安装适当的转换，请检验：

- 配置是否正确。让 NAT 完成您希望的目标有时很困难。有关配置帮助，请参阅配置网络地址转换：部分。
- 没有任何入站访问列表拒绝数据包进入 NAT 路由器。
- 如果包从内部传输到外部，NAT 路由器是否在路由表中有适当的路由。有关详细信息，请参阅 NAT 运行顺序。
- NAT 命令引用的访问列表支持所有必需的网络。
- NAT 池有足够的地址。这是只在 NAT 没有配置处理过载时才应出现的问题。
- 路由器接口正确地定义为 NAT 内部接口或 NAT 外部接口。

- 如果正在转换域名系统（DNS）包的有效负载，请确定此包的IP头中在对地址进行转换。如果未进行转换，NAT 则不会查看该包的有效载荷。

未使用正确的转换条目

如果转换表中安装了正确的转换条目，但却没有使用，请进行以下检查：

- 检验是否没有任何入站访问列表拒绝数据包进入 NAT 路由器。
- 对于从内部传输到外部的数据包，检验是否有到目的地的路由，该检验在转换之前进行。有关详细信息，请参阅 NAT 运行顺序。

NAT 运行正常，但是仍有连接问题

如果 NAT 运行正常，采用以下步骤排除连接问题：

- 检验第 2 层连接。
- 检验第 3 层路由信息。
- 搜索可能导致问题的数据包过滤器。

端口 80 的 NAT 转换不能正常运行

端口 80 的 NAT 转换不能正常运行，但是其他端口的转换可以正常运行。

要解决此问题，请完成以下步骤：

1. 运行 **debug ip nat translations** 和 debug ip packet 命令，以查看转换是否正确并且是否在转换表中安装了正确的转换条目。
2. 验证服务器是否响应。
3. 禁用 HTTP 服务器。
4. 清除 NAT 和 ARP 表。

%NAT ：系统繁忙。稍后尝试

%NAT：当执行与 NAT 相关的 **show** 命令或执行 show running-config 或 write memory 命令时，将显示 Try later 错误消息。出现此问题是由于 NAT 表大小的增加。当 NAT 表大小增加时，路由器的内存将会用光。

请重新加载路由器以解决此问题。如果配置 HSRP SNAT 时出现此错误消息，请配置以下命令以解决该问题：

```
Router(config)#standby delay minimum 20 reload 20
Router(config)#standby 2 preempt delay minimum 20 reload 20 sync 10
```

大转换表增加 CPU 使用量

主机可能发送数以百计的转换，因而会导致高的 CPU 使用量。换句话说，它可能会使表变得很大，以至于 CPU 达到 100% 使用率。**ip nat translation max-entries 300** 命令对每个主机设置 300 个条目的限制，或对路由器设置总转换数量限制。解决方法是使用 **ip nat translation max-entries all-hosts 300** 命令。

% 已经映射公共 IP 地址（内部 IP 地址 -> 公共 IP 地址）

当您尝试为一个公共 IP 地址配置两个内部 IP 地址帧听相同端口时，将出现此消息。

```
% X.X.X.X already mapped (172.30.62.101 -> X.X.X.X)
```

要通过 NAT 将公共 IP 地址转换为两个内部 IP 地址，请在 DNS 中使用两个公共 IP 地址。

ARP 表中没有条目

这是对 NAT 条目使用 *no-alias* 选项的结果。no-alias 选项意味着路由器不响应地址且不安装 ARP 条目。如果另一个路由器使用一个NAT池作为包括在附加的子网的地址的Inside Global池，别名为该地址生成，以便路由器能答复地址解析服务(ARP)要求那些地址。这会使路由器为虚假地址创建 ARP 条目。

结论

以上问题说明 NAT 并不总是 IP 连通性问题的原因。在很多情况下是 NAT 之外的其他原因，因而需要进一步的调查。我们解释了故障排除和检验 NAT 运行时要采取的基本步骤。这些步骤包括：

- 清楚地定义 NAT 要完成的任务。
- 检验转换表中是否有正确的转换。
- 使用 **show** 和 debug 命令验证是否正在执行转换。
- 详细观察数据包的处理过程，并检验路由器是否有传输数据包所需要的正确路由信息。

令牌 0 错误，需要的令牌为 TOK_NUMBER|TOK_PUNCT

此错误消息只是参考性消息，对设备的正常行为没有任何影响。

```
Bad token 0, wanted TOK_NUMBER|TOK_PUNCT
```

此错误表示 NAT 尝试对 FTP 打开的地址进行第 4 层修复，但在数据包中找不到转换所需的 IP 地址。

消息中之所以包含令牌，是因为数据包中的 IP 地址是通过在 IP 数据包中搜索令牌或搜索一组符号以便找到所需转换的详细信息而找到的。

当启动 FTP 会话时，它将协商命令信道和数据信道这两条信道。它们是具有不同端口号的两个 IP 地址。FTP 客户端和服务器协商第二条数据信道来传输文件。通过控制信道交换的数据包的格式为“PORT,i,i,i,i,p,p”，其中 i,i,i,i 是四字节的 IP 地址，p,p 指定端口。NAT 将会尝试匹配此模式，并在必要时转换地址/端口。NAT 必须转换两条信道的编址方案。NAT 会扫描命令流中的数字，直到认为找到需要转换的端口命令。它会尝试解析转换，对于这一转换，它将使用前面所述的模式进行计算。

如果数据包损坏或 FTP 服务器或客户端的命令格式错误，NAT 将无法正确计算转换，因而会生成该错误。建议将 FTP 客户端设置为“被动”，以便启动两条信道。这有时会帮助 FTP 通过 NAT。

相关信息

- NAT 支持页
- 技术支持 - Cisco Systems