

在IP输入进程的高CPU利用率故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[IP 输入](#)

[IP 数据包调试会话示例](#)

[相关信息](#)

简介

本文档介绍了如何对 IP 输入进程导致的 CPU 使用率过高进行故障排除。

注意： 本文档并未提供用于防止各类攻击的策略。

先决条件

要求

Cisco 建议您在继续阅读本文档之前首先阅读[对 Cisco 路由器上的 CPU 使用率过高进行故障排除](#)。

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创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

IP 输入

呼叫IP输入的Cisco IOS软件进程照料process-switching IP信息包。如果 IP 输入进程使用了过多的 CPU 资源，路由器将对许多 IP 数据流执行进程交换。请检查这些问题：

- 在具有许多数据流的接口上已禁用中断交换中断交换是指使用进程交换以外的交换算法。例如

，快速交换、最佳交换和 Cisco 快速转发交换等（有关详细信息，请参阅[性能调整基础知识](#)）。检查 `show interfaces switching` 命令的输出，查看哪个接口的数据流负担过重。通过检查 `show ip interface` 命令，可查看各个接口上使用的交换方法。在该接口上重新启用中断交换。请记住，输出接口上已配置常规快速交换：如果接口上已配置快速交换，则对从该接口发出的数据包执行快速交换。输入接口上已配置 Cisco 快速转发交换。要在特定接口上创建转发信息库 (FIB) 和邻接表条目，请对路由到该接口的所有接口配置 Cisco 快速转发交换。

- **在同一接口上已禁用快速交换**如果某个接口具有许多辅助地址或子接口，并且有许多数据流从该接口发出，其目标位置是同一接口上的某个地址，那么对所有这些数据流都执行进程交换。[在这种情况下，应启用接口上的 ip route-cache same-interface。](#)使用 Cisco 快速转发交换时，不需要在同一接口上单独启用 Cisco 快速转发交换。
- **在提供策略路由的接口上已禁用快速交换**如果接口上已配置路由映射，并且该路由映射已处理许多数据流，则路由器将对此数据流执行进程交换。[在这种情况下，应启用接口上的 ip route-cache policy。](#)检查在[配置基于策略的路由](#)的“启用快速交换基于策略的路由”部分提及的限制。
- **无法进行中断交换的数据流已到达**这可以是所列数据流类型中的任意一种。有关详细信息，请单击链接项。在交换缓存中尚无条目的数据包即使已配置快速、最佳或 Cisco 快速转发 (CEF) 交换，对于在快速交换缓存或 FIB 和邻接表中没有匹配的数据包，仍会加以处理。随后会在相应的缓存或表中创建条目，并且对匹配相同标准的所有后续数据包都执行快速、最佳或 CEF 交换。在正常情况下，这些已处理的数据包不会导致 CPU 使用率过高。但是，如果网络中存在具有以下特征的设备：1) 以极高的速率通过路由器为可达到的设备生成数据包，且 2) 使用不同的源或目标 IP 地址，这些数据包在交换缓存或表中没有匹配，因此，由 IP 输入进程处理这些数据包（如果已配置 NetFlow 交换，也会根据 NetFlow 缓存中的条目检查源和目标 TCP 端口）。该源设备可能是无法正常运行的设备，或者更有可能是尝试进行攻击的设备。（*）只针对收集邻接。关于 Cisco 快速转发邻接的更多信息参考的[Cisco 快速转发](#)。要发送到路由器的数据包以下示例为要发送到路由器的数据包：以极高的速率到达的路由更新。如果路由器收到必须处理的大量路由更新，则此任务可能导致 CPU 过载。通常，在稳定的网络中不会发生这种情况。收集更多信息的方式取决于您配置的路由协议。[但是，可以开始定期检查 show ip route summary 命令的输出。](#)如果值迅速更改，则表示网络不稳定。如果路由表频繁更改，则表示路由协议处理量在增加，这将导致 CPU 使用率提高。有关如何对此问题进行故障排除的详细信息，请参阅“互连网络故障排除指南”中的[TCP/IP 故障排除](#)部分。要发送到路由器的其他任何类型的数据流。检查登录到路由器的用户和用户操作。如果有用户已登录并发出可生成较长输出的命令，则在“IP 输入”进程导致较高的 CPU 使用率之后，[虚拟 Exec 进程](#)将导致更高的 CPU 使用率。欺骗攻击。[要识别此问题，请发出 show ip traffic 命令，以检查 IP 数据流量。](#)如果存在问题，则接收到的具有本地目标的数据包数量将非常之大。[然后，查看 show interfaces 和 show interfaces switching 命令的输出，检查数据包通过哪个接口传入。一旦您确定了接收接口，请在流出接口上打开 ip accounting，检验是否存在某种模式。](#)如果存在攻击，则源地址几乎始终不同，但目标地址是相同的。可配置访问列表暂时解决问题（最好是在距离数据包源最近的设备上），但真正的解决方案则是找到源设备并阻止攻击。广播数据流在 `show interfaces` 命令输出中检查广播数据包的数量。如果将广播数据包的量与接口上收到的数据包总量进行比较，则可知道是否存在广播开销。如果 LAN 包括多个连接到路由器的交换机，则表示生成树存在问题。带选项的 IP 数据包需要协议转换的数据包多链路点对点协议（Cisco 快速转发交换中支持此协议）压缩数据流如果路由器中不存在压缩服务适配器 (CSA)，则必须对压缩数据包执行进程交换。加密数据流如果路由器中不存在加密服务适配器 (ESA)，则必须对加密数据包执行进程交换。采用 X.25 封装经过串行接口的数据包在[X.25 协议簇](#)中，将在第二个开放系统互联 (OSI) 层上实施流控制。
- 以极高的速率到达的许多数据包，其目标位置在直接连接的子网中，这些数据包在地址解析协议 (ARP) 表中没有任何条目。由于窗口机制，TCP 数据流不应发生这种情况，但用户数据报协议 (UDP) 数据流会发生这种情况。要识别此问题，请重复建议的操作，以便找出欺骗攻击。
- 许多多播数据流经过路由器。遗憾的是，没有简便的方法可用于检查多播数据流量。[show ip](#)

[traffic](#) 命令仅显示概要信息。但是，如果在路由器上已配置多播路由，则可使用 [ip mroute-cache](#) 接口配置命令启用多播数据包的快速交换（默认情况下，多播数据包的快速交换处于关闭状态）。

- 路由器处于超额预订状态。如果路由器由于过度使用而无法处理这些数据流量，请尝试将负载分配到其他路由器上或购买高端路由器。
- 路由器上已配置 IP 网络地址转换 (NAT)，并且许多域名系统 (DNS) 数据包经过路由器。NAT 始终会将包含源或目标端口 53 (DNS) 的 UDP 或 TCP 数据包传送到进程级别。
- 还会传送其他类型的数据包，以便进行处理。
- 有 IP 数据包的分段。有在 CPU 和内存的一小增加在头顶上分段 IP 数据包。参考请[解决 IP 分段、MTU、MSS 和 PMTUD 问题与 GRE 和 IPSEC](#) 关于如何排除故障此问题的更多信息。

无论是何种原因导致 IP 输入进程中的 CPU 使用率过高，只要调试 IP 数据即可找到产生问题的原因。由于 CPU 使用率已经过高，因此必须非常小心地执行调试进程。[由于调试进程会生成许多消息，因此应该仅配置缓冲的日志记录。](#)

记入控制台会增加不必要的 CPU 干扰，并提高 CPU 使用率。记入主机（或监控程序日志记录）会在接口上生成其他数据流。

[可使用 debug ip packet detail exec 命令启动调试进程。](#)此会话持续时间不应超过三至五秒。调试消息将写入日志记录缓冲区。[示例 IP 调试会话](#)的捕获在本文的 IP 信息包调试会话示例部分提供。找到不需要的 IP 数据包源设备之后，可断开该设备与网络的连接，或者在路由器上创建访问列表，以丢弃从该目标发出的数据包。

IP 数据包调试会话示例

首先应使用 `show logging` 命令检查配置的日志记录目标：

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: level debugging, 52 messages logged Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 148 messages logged Trap logging: level informational, 64
message lines logged Logging to 192.168.100.100, 3 message lines logged Logging to
192.168.200.200, 3 message lines logged --More--
```

禁用除日志记录缓冲区以外的所有日志记录目标，并清空日志记录缓冲区：

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#no logging console router(config)#no logging monitor router(config)#no logging
192.168.100.100 router(config)#no logging 192.168.200.200 router(config)#^Z router#clear logging
Clear logging buffer [confirm] router#
```

为使调试输出具有较高的可读性，应启用日期时间和毫秒时间戳：

```
router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
router(config)#service timestamps log datetime msec router(config)#service timestamps debug
datetime msec router(config)#end router#
```

现在可以启动调试会话：

```
router#debug ip packet detail IP packet debugging is on (detailed)
```

调试的持续时间不应超过三至五秒。可使用 `undebug all exec` 命令停止会话：

```
router#undebug all All possible debugging has been turned off
```

可使用 `show logging exec` 命令检查结果：

```
router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: disabled Monitor logging: disabled Buffer logging: level debugging, 145 messages logged
Trap logging: level informational, 61 message lines logged Log Buffer (64000 bytes): *Mar 3
```

```
03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0), g=10.200.40.1, len 100, forward *Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205 (Ethernet0/0), g=10.200.40.1, len 100, forward *Mar 3 03:43:27.324: ICMP type=8, code=0 *Mar 3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206 (Ethernet0/0), g=10.200.40.1, len 100, forward *Mar 3 03:43:27.328: ICMP type=8, code=0 ...
```

日志将会显示以下内容：

- 每四毫秒接收到一个数据包
- 源 IP 地址为 192.168.40.53
- 数据包已通过接口 Ethernet0/1 进入
- 数据包具有不同的目标 IP 地址
- 数据包已通过接口 Ethernet0/0 发出
- 下一跳 IP 地址为 10.200.40.1
- 数据包为 ICMP 请求 (类型为 8) 在本示例中，您可以看到来自 IP 地址 192.168.40.53 的 ping 泛洪导致 IP 输入进程中的 CPU 使用率过高。由于在调试输出中显示了存在 SYN 标志，因此可使用此方法轻松检测到 SYN 泛滥：

```
*Mar 3 03:54:40.436: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204 (Ethernet0/0), g=10.200.40.1, len 44, forward *Mar 3 03:54:40.440: TCP src=11004, dst=53, seq=280872555, ack=0, win=4128 SYN
```

[相关信息](#)

- [对 Cisco 路由器上的 CPU 使用率过高进行故障排除](#)
- [show processes 命令](#)
- [Catalyst 2900XL/3500XL 交换机上的 CPU 使用率过高](#)
- [性能调整基础知识](#)
- [技术支持和文档 - Cisco Systems](#)