使用 Cisco 路由器确定数据包泛洪的特征并加以跟踪

目录

简介

拒绝服务 (DoS) 攻击在互联网上十分常见。应付此类攻击的第一步是辨别该攻击究竟属于何种类型。许多常用的 DoS 攻击建立在高带宽数据包洪流或其他重复性数据包流的基础上。

可以通过将许多 DoS 攻击流中的数据包与 Cisco IOS® 软件的访问列表条目进行匹配，以隔离这些数据包。这对于过滤攻击十分有用。另外，在识别未知攻击以及跟踪“欺骗”数据包流以确定其真正源头时，这种方法也很有用。

某些时候，我们可将 Cisco 路由器的一些功能（如 debug 日志和 IP 记数）用于类似用途，尤其在遭遇新攻击或者非常规攻击的情况下。然而，随着 Cisco IOS 软件最新版本的发布，访问列表和访问列表日志记录已成为识别和跟踪常见攻击的首要功能。

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。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

最常见的 DoS 攻击

我们可能受到多种类型的 DOS 攻击。即使您忽略那些利用软件 Bug 使用较小的数据流量来关闭系统的攻击，但事实仍然是任何通过网络传送的 IP 数据包都可以用来实施泛洪 DoS 攻击。遭受攻击时，您必须时刻考虑到这种攻击可能是一种非常规的攻击。

虽然我们提出上述警告，然而您还应该记住一点：很多攻击是相似的。攻击者会选择利用常见的攻击方法，原因在于这些方法特别有效，并且难以跟踪，或者因为可用工具较多。许多 DoS 攻击者都缺乏自制工具的技能或动机，他们使用的都是 Internet 上已有的程序。这些工具中有些流行，有些则不流行。

在撰写本文时（ 1999 年 7 月），大部分客户向 Cisco 发出的帮助请求都和“smurf”攻击相关。这种攻击有两个受害者：“最终目标”和“反射器”。 攻击者将 ICMP 响应请求（ “ping” ）的激励流发送到反射器子网的广播地址。这些数据包的源地址被伪装为最终目标的地址。对于攻击者发送的每个数据包，反射器子网上的许多主机都会响应。这会导致最终目标泛洪并且同时浪费两个受害者的带宽。

另外一种类似的攻击称为“fraggle”，它通过相同的方法来利用定向广播，但它采用的是UDP回应请求，来代替ICMP回应请求。Fraggle 的放大系数通常低于 smurf，也没有 smurf 常用。

Smurf 攻击通常会被察觉，因为网络链路将会超载。有关这些攻击和相应防御措施的完整说明，请参阅拒绝服务攻击信息页 。

SYN 泛洪是另外一种常见攻击，该攻击使用 TCP 连接请求来泛洪目标机器。连接请求数据包的源地址和源 TCP 端口是随机的。这样是为了迫使目标主机维护许多从未完成的连接的状态信息。

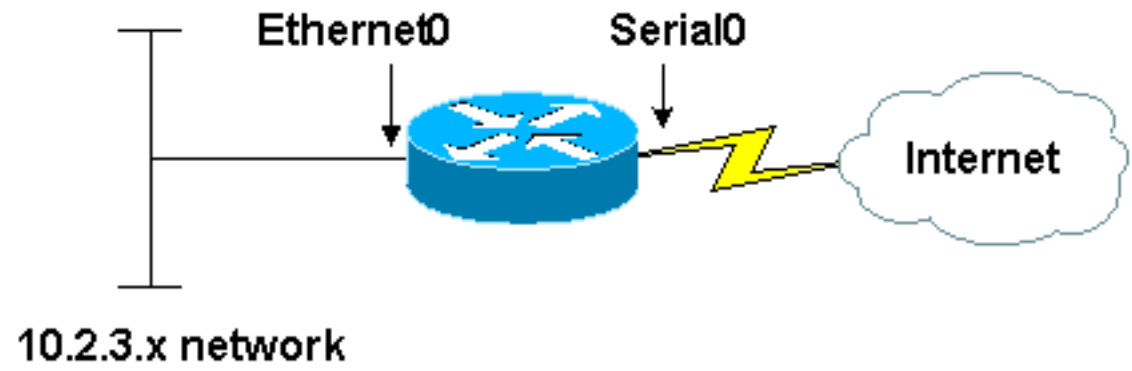
SYN 泛洪攻击通常会被察觉，因为目标主机（通常为 HTTP 和 SMTP 服务器）将发生速度变得极慢、崩溃或者死机的现象。从目标主机返回的数据流也可能会给路由器带来麻烦。这是因为该返回数据流会流向原始数据包的随机源地址，它缺乏“真实”IP 数据流的位置属性，可能会导致路由缓存溢出。在 Cisco 路由器上，发生此问题的迹象通常是路由器的内存容量耗尽。

在 Cisco 接到的报告中，smurf 和 SYN 泛洪攻击在泛洪 DoS 攻击中占据了绝大多数比例，因而迅速识别这两种攻击至关重要。使用 Cisco 访问列表可以轻而易举地识别上述两种攻击（ 以及某些“二级”攻击，例如 ping 泛洪）。

DOS 特性访问控制列表

想象一台带有二个接口的路由器。ethernet 0 连接到一个公司或小型 ISP 的内部局域网。Serial 0 提供通过上游 ISP 提供互联网连接。Serial 0 上的输入数据包速率被“固定”在全链路带宽值，LAN 上的主机运行缓慢、发生崩溃、死机或者表现出 DoS 攻击的其他迹象。路由器连接所在的小型站点没有网络分析器，且即使能够进行跟踪，该处的工作人员在读取分析器跟踪方面也缺乏经验或者根

本没有经验。



现在，假设您应用了一个访问列表，如以下输出所示：

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

该列表根本不会过滤任何数据流；所有条目均为许可。但由于该列表将数据包进行了有效分类，因此该列表可用于临时诊断所有三种类型的攻击：Smurf、SYN 泛洪和 Fraggle。

smurf 最终目标

如果您发出 **show access-list** 命令，则会看到类似于下面的输出：

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

到达串行接口的大部分数据流由 ICMP echo 应答数据包组成。这可能是 smurf 攻击的迹象，我们的站点是最终目标，而并非反射者。您可以在修改访问列表时收集有关攻击的更多信息，如以下输出所示：

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
```

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

此处所作的更改是向与可疑数据流相匹配的访问列表条目中添加了 **log-input 关键字。**（低于版本 11.2 的 Cisco IOS 软件缺少此关键字。请使用“log”关键字代替。）这样会使路由器记录有关与该列表条目相匹配的数据包的信息。假设配置了 **logging buffered，则可以使用 show log 命令查看产生的消息（由于速率限制，消息收集可能需要一段时间）。** 这些消息与以下输出类似：

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

回应应答数据包的源地址在地址前缀192.168.212.0/24、192.168.45.0/24和172.16.132.0/24中集群。(192.168.x.x和172.16.x.x网络中的私有地址不会在Internet上；这是实验室例证。）这正是 smurf 攻击的特征，源地址是 smurf 反射者的地址。如果在相应的 Internet“whois”数据库中查找这些地址块的所有者，可以找到这些网络的管理员，并请求他们协助对付攻击。

应该记住，在 smurf 攻击中，这些反射者同是受害者，并非攻击者，这一点非常重要。在任何 DoS 泛洪中，很少有攻击者在IP数据包上使用自己的源地址。在任何有效的 smurf 攻击中，他们都不可能这样做。应该假定泛洪数据包的所有地址都是完全伪装的，或者就是某种类型的受害者。对 smurf 攻击的最终目标而言，最有效的方法是与反射器联系，要求他们重新配置其网络以停止攻击或者要求他们帮助跟踪激发数据流。

由于 Smurf 攻击的最终目标遭受的损坏通常是由 Internet 传入链路的过载造成的，因此除了联系反射器之外，通常别无其他应对方法。当数据包到达受目标控制的任何计算机时，实际上已经造成了大多数损坏。

有一种权宜之计，就是要求上一级网络供应商过滤所有 ICMP 响应答复，或者过滤来自特定反射者的 ICMP 响应答复。我们不建议永久使用此类过滤器。即使对临时过滤器来说，也只应该过滤 echo replies，而并非过滤所有 ICMP 数据包。另一种可能是让上游提供商使用服务质量和速率限制功能限制 echo 应答的可用带宽。合理的带宽限制可以永久保持不变。上述两种方法都要求上游提供商的设备拥有所需的功能，而某些时候这些设备可能没有所需功能。

smurf 反射器

如果传入数据流由 echo 请求而不是由 echo 应答组成（换言之，如果第一个访问列表条目计算的匹配数量远高于合理预测的数量，而第二个条目没有发生这种情况），则应该怀疑我们的网络在 Smurf 攻击中被用作反射器，或者可能遭受了一次简单的 ping 泛洪攻击。在这两种情况下，如果攻击成功，串行线路的输出和输入端可能会被淹没。实际上，由于扩散因素的原因，输出端的过载比输入端可能会更加严重。

有以下几种方法可用于区别 Smurf 攻击和简单的 ping 泛洪：

- Smurf 刺激数据包会被发送到定向广播地址而非单播地址，而普通 ping 泛洪则几乎总是使用单播地址。您可以在相应访问列表条目上看到使用 log-input 关键字的地址。
- 如果您被用作 Smurf 反射者，则系统的以太网端的 **show interface 命令会显示数量不成比例的输出广播，且 show ip traffic 命令通常还会显示数量不成比例的已发送广播。**标准 ping 泛洪不会增加后台广播流量。
- 如果您被用作 Smurf 反射者，则发往 Internet 的流量将多于发自 Internet 的流量。一般而言，串行接口上的输出数据包多于输入数据包。即使刺激流完全充满输入接口，响应流也将大于刺激流，而且数据包丢弃将被计数。

与 smurf 攻击的最终目标相比，smurf 反射者的选择范围更广。如果反射器要终止攻击，则通常只需正确使用 no ip directed-broadcast 命令（或同等的非 IOS 命令）即可。即使没有主动攻击，每种配置中也会带有这些命令。有关如何防止 Cisco 设备被 Smurf 攻击利用的详细信息，请参阅改善 Cisco 路由器的安全性。有关常见 Smurf 攻击的更多一般信息以及有关保护非 Cisco 设备的信息，请参阅拒绝服务攻击信息页 。

与最终目标相比，smurf 反射者与攻击者的距离更近一步，因此它在跟踪攻击方面处于更加有利的位置。如果您要对攻击进行跟踪，需要与相关的 ISP 配合。如果您要在完成跟踪后采取任何行动，需要与相应的执法机构配合。如果您试图跟踪某个攻击，我们建议您尽早要求执法机构介入。请参阅跟踪部分以获得有关跟踪泛洪攻击的技术信息。

弗拉格尔

Fraggle 攻击与 smurf 攻击类似，不同之处是它使用 UDP ECHO 请求作为激励流，而没有使用 ICMP ECHO 请求。在访问控制列表地第三第四行定义了识别 fraggle 攻击。受害者的应对措施都相同，差别在于：在大多数网络中，UDP echo 服务的重要性要低于 ICMP echo 服务。因此您可以完全禁用它而不会造成较大地负面影响。

SYN 溢出

访问列表的第五行和第六行分别是：

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

第一行将任何 TCP 数据包与 ACK 位设置进行匹配。真正能够帮助我们识别攻击的是它能匹配任何不是 TCP SYN 的数据包。第二行仅与 TCP SYN 数据包相匹配。通过这些列表条目上的计数器可以很容易识别 SYN 泛洪。在正常数据流中，非 SYN TCP 数据包的数量至少超出 SYN 两倍，通常超出四倍或五倍。在SYN泛洪中，SYN 的数量通常超出非 SYN TCP 数据包若干倍。

如果没有遭受攻击，唯一能够产生此种现象的条件是：真正的连接请求大量超载。一般来说，这种超载现象不会出人意料地发生，也不会象真正的 SYN 泛洪那样发送尽可能多的 SYN 数据包。此外，SYN 泛洪通常包含带有完全无效的源地址的数据包；通过使用 **log-input 关键字，可以查看连接请求是否来自此类地址。**

有一种攻击被称为“进程表攻击”，它与 SYN 泛洪有些相似。在进程表攻击中，TCP 连接已完成，然后允许 TCP 连接在没有更多协议流量的情况下超时，而在 SYN 泛洪中，仅发送初始连接请求。由于进程表攻击要求完成 TCP 初始握手，因此通常要求攻击者利用其有权访问（通常通过窃取访问权限）的真实计算机的 IP 地址发动攻击。 因此可使用数据包日志记录很容易地将进程表攻击与 SYN 泛洪区分开来。进程表攻击中的所有 SYN 均来自同一个或几个地址，最多来自同一个或几个子网。

SYN 泛洪的受害者能够采取的应对措施非常有限。遭受攻击的系统通常是提供重要服务的系统，而封锁对这些系统的访问通常正是攻击者要达到的目的。许多路由器和防火墙产品（包括 Cisco 的产品）都具有可用于降低 SYN 泛洪影响的功能。但是，这些功能的效果因环境而异。有关详细信息，请参阅 Cisco IOS 防火墙功能集的文档、Cisco IOS TCP 拦截功能的文档以及改善 Cisco 路由器的安全性。

我们也可能跟踪 SYN 泛洪，但跟踪过程要求攻击者和受害者之间的路径上的每一个 ISP 的协助。如果您决心尝试追踪 SYN 泛洪，应尽早与执法部门联系，并与您自己的上一级服务供应商合作。有关使用 Cisco 设备进行跟踪的详细信息，请参阅本文档的跟踪部分。

其它攻击

如果您确信自己受到攻击，并且能够通过 IP 源地址和目的地址、协议号和端口号来识别该攻击，那么您可使用访问控制列表来验证您的假设。您可以创建一个与怀疑流量匹配的访问列表条目，将其用于相应接口，观察匹配计数器或记录流量。

日志记录和计数器警告

访问列表条目上的计数器会计算所有与该条目的匹配。如果您对两个接口应用同一个访问列表，那么您看到的计数将是总计数。

访问控制列表日志不会显示与条目匹配的每个数据包。日志受到速率限制，以防止 CPU 超载。日志显示的是适当的有代表性的例子，而并非完整的数据包追踪。请记住，有一些数据包是看不到的。

在一些软件版本中，访问控制列表日志只能在某些交换模式下工作。如果访问列表条目对大量匹配进行计数，但没有进行记录，则应尝试清除路由缓存以迫使数据包进行进程交换。在带有多个接口的高负载路由器上执行此项操作时要小心。重建缓存时可能会丢弃大量数据流。请尽可能使用

Cisco 快速转发。

访问控制列表和日志会影响性能，但影响不会很大。当路由器运行的 CPU 负载达到约 80% 以上时或在高速接口上应用访问列表时，请务必小心。

跟踪

DoS 数据包的源地址通常设置为与攻击者自身无关的值。因此，它们对于识别攻击者没有用。识别攻击来源的唯一可靠方法是通过网络逐跳进行跟踪。此过程包括对路由器进行重新配置以及检查日志信息。这需要攻击者与受害者之间的所有网络运营商的互相合作。要确保成功合作，通常需要执法机构介入，如果要对攻击者采取操作，也必须有执法机构介入。

DoS 泛洪的跟踪过程相对比较简单。从一台承载泛洪流量的已知路由器（称为 A）开始，我们可以识别A接收流量的来源路由器（称为 B）。然后登录 B，找到 B 接受流量的来源路由器（称为 C）。按照此过程继续查找，直至找到最终来源。

这种方法牵涉到下述几个问题：

- “最终来源”实际上可能是攻击者所攻陷的一台计算机，其拥有者和操作者可能是另外一位受害者。在此情况下，跟踪 DoS 泛洪只是第一步。
- 攻击者知道他们可能会被跟踪，因此通常只在有限时间内持续发动攻击。所以可能没有足够时间来对泛洪进行实际跟踪。
- 攻击可能来自多个来源，尤其在攻击者较为老练的情况下。应尽可能多地确认来源，这一点非常重要。
- 通信问题减缓了跟踪过程。通常，涉及到的一个或多个网络运营商可能没有精通相应技术的人员来应对攻击。
- 即使我们找到了攻击者，但法律和政治方面的原因却使我们很难对其采取行动。

跟踪 DoS 攻击的多数努力都无效。由于这个原因，很多网络运营商甚至不尝试对攻击进行跟踪，除非他们承受到某些压力。其他很多运营商只跟踪“严重”攻击，并且他们对“严重”的定义各不相同。有些运营商只有在执法机构介入时才会协助进行跟踪。

使用“log-input”进行跟踪

如果选择对穿过 Cisco 路由器的攻击进行跟踪，最有效的方法就是建立与攻击数据流匹配的访问列表条目，将 **log-input 关键字附加到该条目，然后将访问列表应用到相应接口（攻击流通过该接口向最终目标传送）的出站方向。**访问列表产生的日志条目会标识数据流经过的路由器接口，如果接口是多点连接，则会提供接收的数据流所来自的设备的第 2 层地址。第 2 层地址能够用于确认链中的下一台路由器，如通过使用 **show ip arp** ***mac-address*** 命令确认。

SYN 泛洪

要跟踪 SYN 泛洪，可以创建如下所示的访问列表：

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

该访问列表会记录所有发往目标主机的 SYN 数据包，包括合法 SYN。要确认通往攻击者的最可能的真实路径，请仔细检查日志条目。一般来说，从泛洪来源发出的匹配数据包的量最大。源 IP 地址本身并没有任何意义。应该寻找源接口和源 MAC 地址。有时可以将泛洪数据包与合法数据包相互

区分，因为泛洪数据包可能含有无效源地址。源地址无效的任何数据包都可能是泛洪的一部分。

泛洪可能来自多个源，但对于 SYN 泛洪而言通常不是如此。

smurf 刺激

要跟踪 Smurf 刺激流，请使用如下所示的访问列表：

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

注意，第一个条目并非只限于发送到反射者地址的数据包。原因是大多数 smurf 攻击会使用多个反射者的网络。如果您没有与最终目标保持联系，您可能无法知道所有的反射器地址。随着跟踪逐渐接近攻击来源，您可能会开始看到发往越来越多的目标的 echo 请求；这是好的迹象。

但如果您处理的 ICMP 流量很大，则可能会产生过多的日志记录信息，使您难以阅读。如果发生此种情况，您可以将目的地的地址限定为已知被使用的反射器之一。另外一种有效策略是使用一个条目，利用255.255.255.0的网络掩码在互联网上非常普遍这一事实。鉴于攻击者寻找 smurf 反射者的方法，实际用于 smurf 攻击的反射者地址更可能和这个掩码匹配。以 .0 或 .255 结尾的主机地址在 Internet 中非常少见。因此，您可以为 Smurf 刺激流建立一个相对比较具体的识别器，如以下输出所示：

```
access-list 169 permit icmp any host known-reflector echo log-input access-list 169 permit icmp
any 0.0.0.255 255.255.255.0 echo log-input access-list 169 permit icmp any 0.0.0.0 255.255.255.0
echo log-input access-list 169 permit ip any any
```

您可以通过该访问列表清除日志中的许多“噪声”数据包，同时，随着逐渐接近攻击者，您仍然有很大机会发现更多刺激流。

没有使用“log-input”的跟踪

log-input 关键词存在于 Cisco IOS 软件 11.2 版和更高版本,也存在于专门为服务提供商市场创建的基于特定 Cisco IOS 软件版本 11.1 的软件。旧版本的软件不支持该关键字。如果您使用的路由器运行的是较旧的软件版本，则有以下三种可行的选择：

- 建立访问列表，不进行记录，但条目必须匹配可疑流量。依次在每个接口的*输入端 采用访问控制列表，观察计数器*。寻找匹配率高的接口。这种方法的性能开销非常低，其有利于确认源接口。其最大的缺陷是无法提供链路层的源地址，因此它最适用于点到点线路。
- 使用 **log（而不是 log-input）关键词创建访问列表条目。** 再次将访问控制列表应用到每个接口的流入端上。此方法仍然不提供源 MAC 地址，但对于查看 IP 数据十分有用。例如，对于验证数据包流是否确实为攻击的一部分很有用。此方法对性能的影响可能适中，也可能较大，而且新版软件比旧版软件性能更强。
- 使用 **debug ip packet detail** 命令收集有关数据包的信息。这种方法可提供 MAC 地址，但对性能却产生了严重的影响。使用该方法易于出错，可能导致路由器无法使用。如果您使用此方法，应确保路由器以快速、自治或最佳模式交换攻击数据流。使用访问控制列表，将调试限定在您真正需要的信息的范围内。将 Debug 信息记录在本地日志缓冲区，但要关闭到 Telnet 会话和控制台的 Debug 信息的记录。如果可能，应安排人员守候路由器物理位置附近，确保必要时重新通电路由器。请记住，**debug ip packet** 命令不会显示有关快速交换数据包的信息。您需要发出 **clear ip cache 命令才能捕获相关信息。**每个 **clear 命令都会提供一两个 debug 输出的数据包。**

相关信息

- Kerberos
- 技术支持和文档 - Cisco Systems