S12500由于IP/ARP攻击导致下一跳资源不足案例

以太网OAM SSH 程飞 2015-07-13 发表

现网S12500设备1框4号槽位单板下有很多用户反馈不能正常PING通网关，也不能通过三层访问其他网络业务。诊断日志中有如下的打印：
%@1493461564 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b2e, P2:ffffffff, P3:11.
%@1493461565 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b2f, P2:ffffffff, P3:11.

%@1493461564 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b2e, P2:ffffffff, P3:11.
%@1493461565 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b2f, P2:ffffffff, P3:11.

通过进一步查看诊断日志，发现在出现问题开始4号槽位单板打印类似如下信息， P1后面对应的是需要访问的IP地址（十六进制表示，如a8b1b3b转换成十进制为10.139.27.59）。从信息中，也可以看到这些访问的地址是递增的。当网络中存在连续的IP扫描或ARP攻击时才会出现地址递增的可能。

%@1493461564 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b2e, P2:ffffffff, P3:11.
%@1493461565 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b2f, P2:ffffffff, P3:11.
%@1493461566 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b30, P2:ffffffff, P3:11.
%@1493461567 Jun 18 10:26:25:508 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b31, P2:ffffffff, P3:11.
%@1493461568 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b32, P2:ffffffff, P3:11.
%@1493461569 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b33, P2:ffffffff, P3:11.
%@1493461570 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b34, P2:ffffffff, P3:11.
%@1493461571 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b35, P2:ffffffff, P3:11.
%@1493461572 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b36, P2:ffffffff, P3:11.
%@1493461573 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b37, P2:ffffffff, P3:11.
%@1493461574 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b38, P2:ffffffff, P3:11.
%@1493461575 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b39, P2:ffffffff, P3:11.
%@1493461576 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b3a, P2:ffffffff, P3:11.
%@1493461577 Jun 18 10:26:25:509 2012 ZJ-DS-S9512E Chassis=1-Slot=4; DRVL3/3/GET_PARA_INVALID:Get para invalid: 0xcc440000 [594]: P1:a8b1b3b, P2:ffffffff, P3:11.
2．软件实现上，当收到IP扫描或ARP攻击时，为了实现防攻击功能，会申请一个下一跳资源，如果此时IP扫描过多会导致下一跳资源占用过多，甚至出现资源不足的情况，影响正常用户的上网。
3．从目前的正常情况下，下一跳资源占用也是在一个比较高的数量上，而其中大部分为ARP占用的：
```
 Ipv4 route prefix       : 27332
 Ipv6 route prefix       : 15
 Allocated route entry   : 9195
 Ipv4Uc allocated nexthop: 9055  18    0    1    0    0    0    0    0    0    0
 Ipv6Uc allocated nexthop: 0    14    0    0    0    1    0    0    0    0    0
 Ipv4Mc allocated nexthop: 3
 Ipv6Mc allocated nexthop: 0
 Tunnel allocated nexthop: 0
 Ipv4Vn allocated nexthop: 25    0    0    0    0    0    0    0    0    0    0
 Max support vrf         : 1024
 Max support ipv4 prefix : 262144
 Max support ipv6 prefix : 65536
 Max support nexthop     : 13312
```
即此时已经占用9195个下一跳，而此单板只支持13312个下一跳资源。
纵上所述，此问题是由于当时网络中存在IP扫描和ARP攻击导致下一跳资源被异常占用，引发正常用户无法访问网络的情况。

1．可以在网络中部署ARP主动确认功能，以及关闭ARP黑洞路由功能，命令如下：
undo arp resolving-route enable
关闭ARP黑洞路由后当收到IP扫描的报文时不再下发黑洞路由，减少下一跳资源占用，这可能会导致CPU比正常情况下高的情况，但硬件中可以通过CPU-CODE机制限速这类上送CPU的报文。
arp anti-attack active-ack enable
启用ARP主动确认功能后，设备在新建或更新ARP表项前需进行主动确认，防止产生错误的ARP表项，异常占用下一跳资源。

2．可以在网络中部署源MAC地址固定的ARP攻击检测功能，命令入下：
arp anti-attack source-mac filter
在5秒内，如果收到同一源MAC地址的ARP报文超过一定的阈值（默认为150），则认为存在攻击，系统会将此MAC地址添加到攻击检测表项中。
一些重要的设备，可能会发送大量ARP报文，为了使这些ARP报文不被过滤掉，可以将这类设备的MAC地址配置成保护MAC地址，这样，即使该MAC地址存在攻击也不会被检测、过滤。 命令如下：
arp anti-attack source-mac exclude-mac mac-address &<1-n>

3．把部分设备的网关下移，把网关分散到不同网络设备上。

如果网络中存在IP扫描和ARP攻击会导致下一跳资源被异常占用，引发正常用户无法访问网络的情况。这个时候要根据日志信息，诊断信息，诊断文件以及现网情况共同分析。