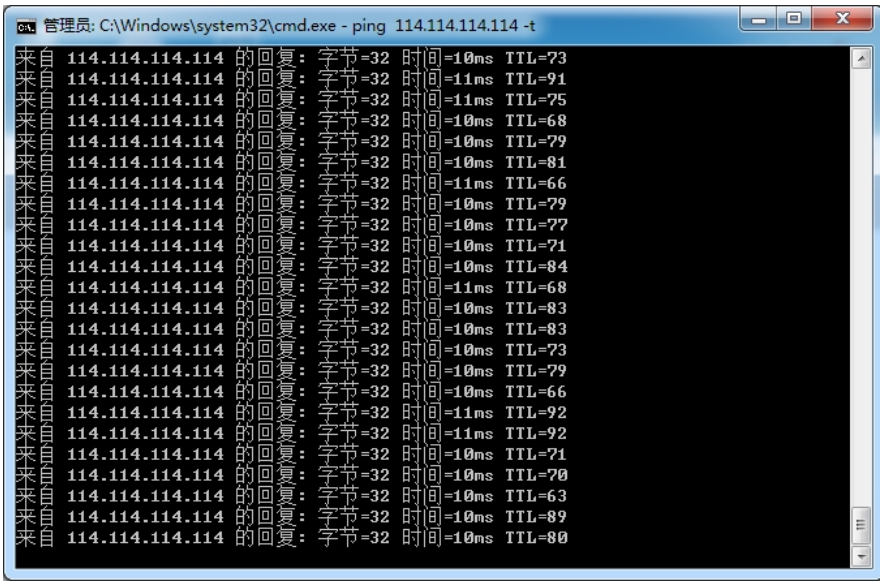
某局点SecPath F1000-AK120(V7) 配置每ip限速后业务流量丢包问题处理经验案例

关萌 2018-03-28 发表

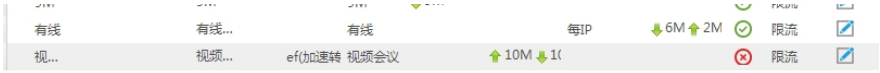
某局点客户使用我司SecPath F1000-AK120防火墙设备，使用PPPoE加固定IP方式两个出口，做为互联网出口设备，在使用过程中用户发现用户上网慢，用户怀疑使用了等价路由导致流量负载问题，使用户流量上网慢。用户将两个出口修改为主备模式。修改后仍然大量用户反馈上网慢，于是求助我们，经过我们初步分析发现有部分用户流量特别大，互联网出口已经达到用户购买的最大带宽，建议用户配置每IP限速，在用户配置每IP限速后发现用户上网速度仍然很慢。并出现了ping外网丢包的情况。

不启用限速策略的情况下配置

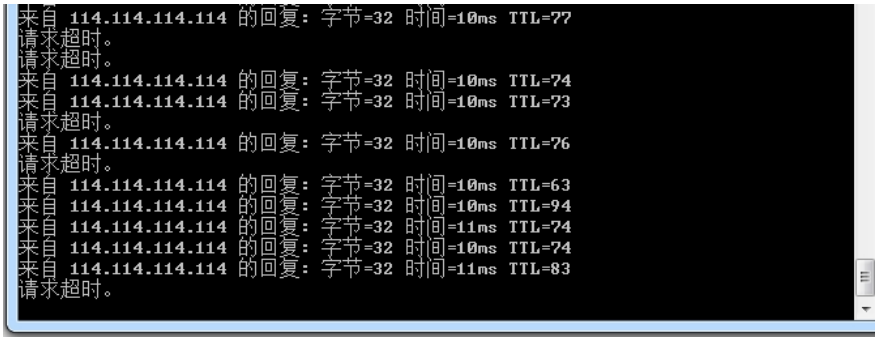
不记用限速策略的情况下ping外网不丢包



启用限速策略情况下配置如下



启用限速后ping外网出现丢包情况如下



客户关键配置信息如下

```
<Core-F1000-AK>dis cu
#
interface Dialer1
 ppp chap password cipher $c$3$YZMBxNOLEf3Sh430kFDG5QixJKQPGHw9PbXf
 ppp chap user 7800000*
 ppp pap local-user 7800000* password cipher $c$3$5BttXX4VFGC1a4OGqwvubv/PB/5CLYhAJBl/
 dialer bundle enable
 dialer-group 1
 dialer timer idle 0
 dialer timer autodial 5
```

```
 ip address ppp-negotiate
 tcp mss 1024
 nat outbound 3000
#
interface Vlan-interface10
 description TO_电信
 ip address *.119.131.118 255.255.255.248
 nat outbound 3000
 nat static enable
#
interface GigabitEthernet1/0/4
 port link-mode route
 description TO_联通
 pppoe-client dial-bundle-number 1
#
interface GigabitEthernet1/0/7
 port link-mode route
 description TO_Phone
 ip address *.110.108.242 255.255.255.248
 nat static enable
#
interface GigabitEthernet1/0/10
 port link-mode route
 description TO_cisco
 ip address 10.1.0.253 255.255.255.0
 ip policy-based-route wx
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 description TO_电信
 port access vlan 10
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 bandwidth 10000
 port access vlan 10
#
interface GigabitEthernet1/0/11
 port link-mode bridge
 description TO_hillstone
 port access vlan 10
#
 ip route-static 0.0.0.0 0 Dialer1
 ip route-static 0.0.0.0 0 *.119.131.113 preference 70
 ip route-static 10.1.0.0 16 10.1.0.254
 ip route-static 10.10.0.0 16 10.1.0.244
 ip route-static 172.16.10.0 24 10.1.0.254
#
traffic-policy
 rule name 访客
  action qos profile 访客
  source-address address-set 访客
 rule name 租客
  action qos profile 租客
  source-address address-set 租客
 rule name 1
  action qos profile 1
  source-address address-set 2M
 rule name 1M
  action qos profile 1M
  source-address address-set 1M
 rule name 0.5M
  action qos profile 0.5M
  source-address address-set 0.5M
```

```
 rule name 7M
  action qos profile 7M
  source-address address-set 7M
 rule name 9M
  action qos profile 9M
  source-address address-set 9M
 rule name 有线
  disable
  action qos profile 有线
  source-address address-set 有线租客
 rule name 视频会议
  disable
  action qos profile 视频会议
  source-address address-set 视频会议
  dscp ef
 profile name 0.5M
  bandwidth downstream maximum 500
 profile name 1
  bandwidth downstream maximum 2000
 profile name 1M
  bandwidth downstream maximum 1000
 profile name 7M
  bandwidth downstream maximum 7000
 profile name 9M
  bandwidth downstream maximum 9000
 profile name 访客
  bandwidth downstream maximum 2000
 profile name 视频会议
  bandwidth downstream guaranteed 10000
  bandwidth upstream guaranteed 10000
  traffic-priority 7
  remark dscp ef
 profile name 有线
  bandwidth upstream maximum per-ip 2000
  bandwidth downstream maximum per-ip 6000
 profile name 租客
  bandwidth downstream maximum per-ip 5000
#
return
```

从配置可以看出，用户当前所有流量都从dialer1口出去，而用户没有对dialer1口进行带宽配置，而dialer口默认带宽为64Kbps,在用户做策略后。策略会参考接口的带宽，也就是64Kbps去做QoS限速和保障。这样用户的流量就被丢弃了。导致了ping外网丢包。

```
[FW1-Dialer1]dis interface Dialer 1
Dialer1
Current state: UP
Line protocol state: UP(spoofing)
Description: Dialer1 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet protocol processing: disabled
Link layer protocol: PPP
LCP: initial
Physical: Dialer, baudrate: 64000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

在接口下配置bandwidth 100000后问题解决。每ip限速生效，并且ping外网不再有丢包的情况。

在配置QoS流量监管时需要注意配置接口带宽与实际情况相符，同时注意接口带宽配置命令的单位是kbps。