



合肥鼎杰教育 CCNP+RHCE 就业班、不就业退学费 www.dingjie365.com

合肥鼎杰 IT 教育安徽首家专业 Cisco、Linux 双国际授权机构，

CCIE、RHCA 全程授课，

CCNP+RHCE 金牌网络工程师就业班、不就业退学费

鼎杰论坛-安徽 IT 第一人气社区 <http://bbs.dingjie365.com>

千 G 视频资料等你来下载!!!

咨询地址：合肥市长江中路 365 号三孝口 CBD 广场公寓楼 16 楼 1607 室

咨询电话：0551-2836661、13866792964、18956016413

咨询 QQ：334134561、376438308

鼎杰超级群：57647952

鼎杰至尊群：65687124

使用 simware 做 QOS 实验

IP QOS 一直是学习网络的同学比较难于理解的问题，包括令牌桶，CAR，PQ，CQ，CBQ 都是比较晦涩的概念，而且市面上也没有讲的特别明白的教材。为什么 QOS 问题会比较麻烦呢？据我了解的情况：

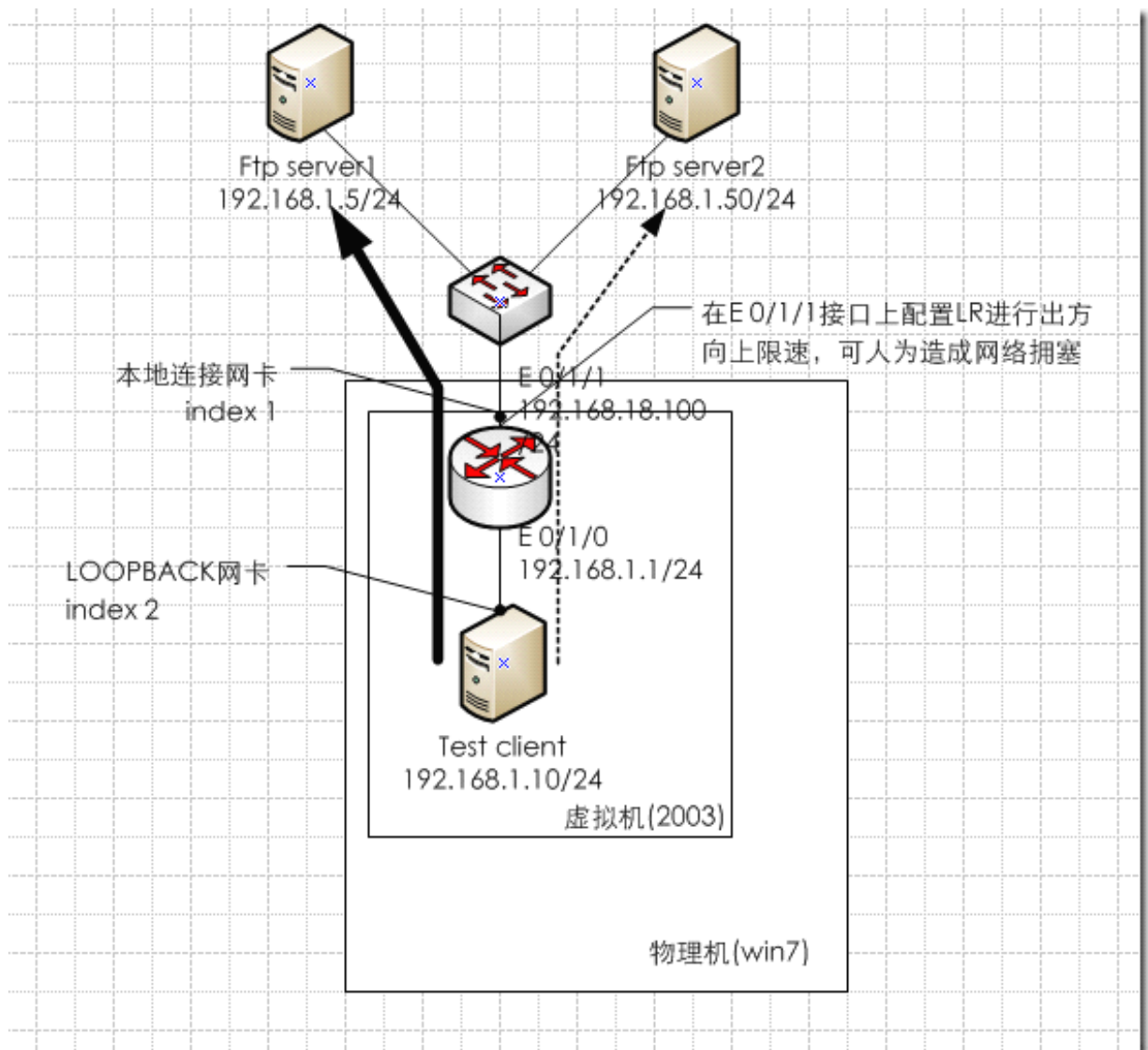
- 1、首先 QOS 并不是经常被使用，企业网通常带宽较宽，网络瓶颈不容易出现。
- 2、一直以来 QOS 技术是逐渐成熟的技术，由于缺乏正确的测试手段和错误的理解，经常会出现配置完成后没有效果的情况。

下面我就将近期在这方面的经验共享给大家

一、实验环境搭建

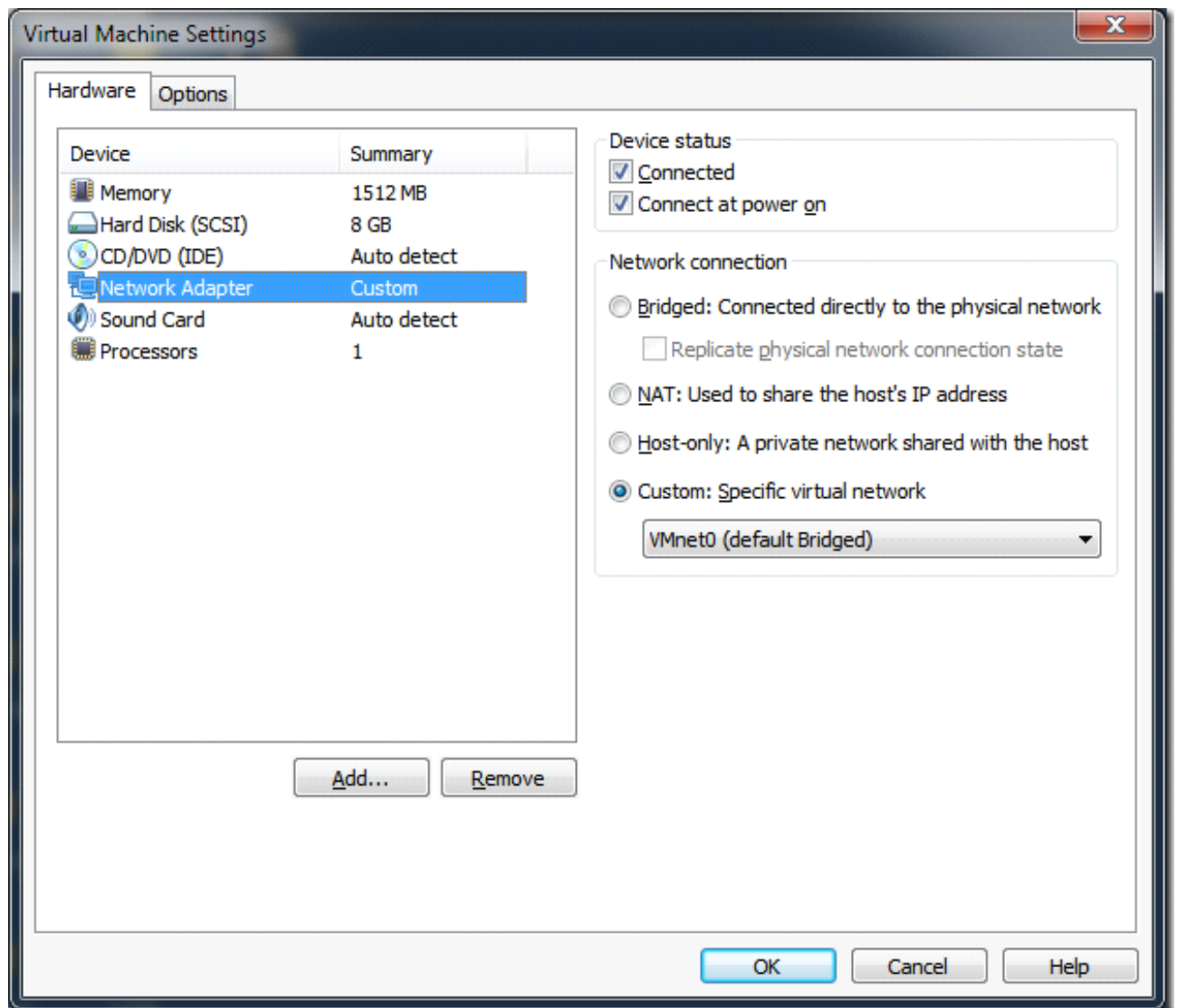


地址：合肥市长江中路 365 号 CBD 中央广场公寓楼 1607 室
电话：0551-2836661 论坛：[Http://bbs.dingjie365.com](http://bbs.dingjie365.com)



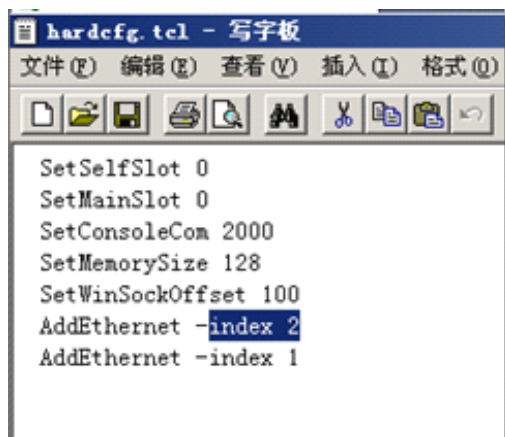
先介绍一下实验环境，需要一台测试机，我的是图中的 WIN7 机器，内装 VMWARE workstation，建立一个 2003 server 的虚拟机，2003 虚拟机要建立 h3c.com.cn 的 AD。虚拟机本地连接网卡与物理机有线网卡桥接：





在 2003 虚拟机中添加一块 loopback 网卡，配置地址为 192.168.1.10/24，缺省网关为 192.168.1.1。
添加一个 SIMWARE 路由器，配置文件如下：





这样路由启动后，E 0/1/1 连接的是虚拟机里的本地连接网卡与物理机有线网卡桥接，可以实现联通 192.168.18.0/24 网段；e 0/1/0 连接 2003 虚拟机的 loopback 网卡，可以联通 192.168.1.0/24 网段。在所有设备上正确配置路由，这里不再详细描述。

```
interface Ethernet0/1/0
port link-mode route
ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/1/1
port link-mode route
ip address 192.168.18.100 255.255.255.0
qos lr outbound cir 256 cbs 16000 ebs 0
#
```

正确配置完成后，在 2003 虚拟机上就可以 ping 通 192.168.18.5 和 18.50。

二、LR 限速

在 e 0/1/1 口下作 LR 限速使得网络拥塞更容易出现。在 2003 上向 192.168.1.5 FTP 上传文件测试速度，实际速度为 40KB/s，限速成功。

三、制造拥塞

网络环境基本就绪了，下面一个非常重要的任务就是制造网络拥塞，很多人在 qos 方面测试不成功可能都会跟这里有关系，有人说 FTP 下载不就可以了？FTP 是可以占掉大部分的带宽，但是由于 FTP 是滑动窗口机制使得其很难耗尽网络带宽，有人说 FTP 单线程不行可以多线程，实际上如果单纯的 FTP 应用不论多少线程都不可能造成我下面要讲到的网络拥塞，还有人使用网络测速工具来试图制造网络拥塞，但是所有的测速工具都是双向，发出的数据包必须确认到达，有去也有回后才算成功，实际上网络真正拥塞时，这种确认机制很难实现，测速工具的流泪也就很难全部打上了。





说了这么多，我的制造网络拥塞的手段是利用 SNIFFER 的数据包发送工具来实现类似攻击的大数据流，针对本次的网络结构，可以采用在 192.168.1.10 上 ftp 上载文件到 192.168.1.5 时，利用 sniffer 进行抓包，找到一个大的 TCP 数据包，然后将这个包重复的发出：

No.	Status	Source Address	Dest Address	Summary
61		[192.168.1.10]	[61.182.207.135]	DNS: C ID=15396 OP=QUERY NAME=_ldap._
62		[192.168.18.50]	[192.168.1.10]	FTP: R PORT=1223 150 Opening BINARY
63		[192.168.18.5]	[192.168.1.10]	TCP: D=1227 S=20 SYN SEQ=1418229396 I
64		[192.168.1.10]	[192.168.18.5]	TCP: D=20 S=1227 SYN ACK=1418229397 S
65		[192.168.18.5]	[192.168.1.10]	TCP: D=1227 S=20 ACK=4220805104 W
66	#	[192.168.1.10]	[192.168.18.5]	Expert: FTP Slow First Response
67		[192.168.1.10]	[192.168.1.10]	MZ<9000030000000040
68		[192.168.1.10]	[192.168.1.10]	<08F6C102>t<03>G<B
69		[192.168.18.5]	[192.168.1.10]	ACK=310474165 WI
70		[192.168.1.10]	[192.168.1.10]	ACK=4220808024 W
71		[192.168.1.10]	[192.168.1.10]	<00008D>M<08>QVh<C
72		[192.168.1.10]	[192.168.1.10]	<C1>Pj<EB>S<E8>W<C
73		[192.168.18.5]	[192.168.1.10]	<00008BD8>j<CDE8BF
74		[192.168.1.10]	[192.168.1.10]	ACK=4220810944 W
75		[192.168.1.10]	[192.168.1.10]	<80>N<09018B>E<E48
76		[192.168.1.10]	[192.168.1.10]	<F4>;E<F80F85AC00C
77		[192.168.18.5]	[192.168.1.10]	<83CE0281>8NCRcu<C

Find Frame... ALT+F3
Find Next Frame F3
Go to Frame...
Go to First Frame
Go to Last Frame
Mark Current Frame
Go to Marked Frame
Save Selected...
Select Range...
Define Filter...
Select Filter...
Display Setup...
Send Current Frame...
Send Current Buffer...
Add Frame to Plot Lib

IP: Destination address =
IP: No options
IP:
TCP: ----- TCP header -----
00000000: 00 00 5e 01 0a 00 02 00
00000010: 05 dc 54 8a 40 00 80 06
00000020: 12 05 04 cb 00 14 fb 94
00000030: fa f0 fd bd 00 00 4d 5a

Send current frame

Configuration

Send
☒ Continuously
☐ 1 time(s)

Send Type
☐ Delay 1 Millisecond
☒ 100 % of network

Packet
Data Size: 1514

0000: 00 00 5e 01 0a 00 02 00 4c 4f 4f 50 08 00 45 00 | ..^.....LOOP..E.
0010: 05 dc 54 8a 40 00 80 06 0c 32 c0 a8 01 0a c0 a8 | ..T.@....2.....
0020: 12 05 04 cb 00 14 fb 94 5f f0 54 88 76 95 50 10 |_.T.v.P.
0030: fa f0 fd bd 00 00 4d 5a 90 00 03 00 00 00 04 00 |MZ.....
0040: 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 |@.
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
0070: 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 |!
0080: 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d | .L.!This program

确定 取消



[illegible]

地址：合肥市长江中路 365 号 CBD 中央广场公寓楼 1607 室
电话：0551-2836661 论坛：[Http://bbs.dingjie365.com](http://bbs.dingjie365.com)



```
Description: Ethernet0/1/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Link delay is 0(sec)
Internet Address is 192.168.18.100/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-5e01-0a01
IPv6 Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-5e01-0a01
Output queue : (Urgent queuing : Size/Length/Discards) 1/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards) 69/75/323005
  Last 300 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
  Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
  Input: 0 packets, 0 bytes, 0 buffers
  Output: 0 packets, 0 bytes

[H3C-Ethernet0/1/1]dis inter e 0/1/1
Ethernet0/1/1 current state: UP
Line protocol current state: UP
Description: Ethernet0/1/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Link delay is 0(sec)
Internet Address is 192.168.18.100/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-5e01-0a01
IPv6 Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-5e01-0a01
Output queue : (Urgent queuing : Size/Length/Discards) 1/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards) 69/75/324575
  Last 300 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
  Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
  Input: 0 packets, 0 bytes, 0 buffers
  Output: 0 packets, 0 bytes

[H3C-Ethernet0/1/1]
```

可以多次连续多次参看该接口的状态，**FIFO 队列长度 75，SIZE 会很接近这个数值并保持稳定**，这说明网络拥塞真正发生了。

四、PQ

加上 SNIFFER 攻击数据流（目的地址 18.5），FTP 192.168.18.50,连接过程和上载都非常慢，几乎不能使用。

针对目的地址 192.168.18.50 配置 PQ，将其置于 TOP 队列。

```
#
qos pql 1 protocol ip acl 3000 queue top
acl number 3000
rule 0 permit ip destination 192.168.18.50 0
#
interface Ethernet0/1/1
port link-mode route
ip address 192.168.18.100 255.255.255.0
```





```
qos lr outbound cir 256 cbs 16000 ebs 0
```

配置完成后,重新上传文件,连接速度和上传速度明显提高,与没打攻击流前相差不大。

注意观察 PQ 队列中，TOP 队列和 NORMAL 队列中都有数值，TOP 队列中 DISCARD 数值基本不变，而 NORMAL 队列中 DISCARD 数值快速增长。





五、CBQ

注意 CBQ 利用 SIMWARE 来实验要使用 AF 流（不要用 EF 流，不知什么原因 EF 流无法使用，表现为 ACL 显示命中，DIS INTERFACE 时，EF 队列使用没有数值，这是 SIMWARE 的问题，真实路由器上没有问题）。

```
traffic classifier 50 operator and
if-match acl 3000
#
traffic behavior 50
queue af bandwidth 100 cbs 2500
#
qos policy 50
classifier 50 behavior 50
#
acl number 3000
rule 0 permit ip destination 192.168.18.50 0
#

interface Ethernet0/1/1
port link-mode route
qos max-bandwidth 256
ip address 192.168.18.100 255.255.255.0
qos apply policy 50 outbound
qos lr outbound cir 256 cbs 16000 ebs 0
#
```





正确配置 CBQ 后，在从 2003 向 192.168.18.50 上传数据，实测 FTP 速度为 15KB/s,与保证带宽差不多。

```
[H3C-behavior-50]dis inter e 0/1/1
Ethernet0/1/1 current state: UP
Line protocol current state: UP
Description: Ethernet0/1/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Link delay is 0(sec)
Internet Address is 192.168.18.100/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-5e01-0a01
IPv6 Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0000-5e01-0a01
Output queue : (Urgent queuing : Size/Length/Discards) 1/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (Class Based Queuing : Size/Discards) 102/181753
  Queue Size: 0/44/58 (EF/AF/BE)
  BE queues: 1/2/256 (Active/Max active/Total)
  AF queues: 1 (Allocated)
  Bandwidth(Kbps): 104/204 (Available/Max reserve)
  Last 300 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
  Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
  Input: 0 packets, 0 bytes, 0 buffers
  Output: 0 packets, 0 bytes
```

注意观察 EF/AF/BE 队列大小。

关于 CBQ 想多说几句，CBQ 中 EF 队列是 LLQ，绝对优先转发，需要设置最大占有带宽，以防止饿死其他队列。AF 确保转发，每个队列要设置最小保证带宽值，BE 是尽力转发，缺省队列，虽然是缺省队列但也是 WFQ 机制的，也会对缺省的数据流再细分成多个队列，加权公平传输。EF+所有 AF 流带宽不能大于接口带宽，而且接口上默认会保留一部分带宽，上图中 EF+所有 AF 带宽不能大于 204。表面上 AF 队列要比 BE 队列高级的多，但是如果在满足了 AF 最小带宽要求之后，在剩余带宽的使用上 BE 队列可能会比 AF 队列更具有优势。

还有就是 CBQ 好像默认对 PING 进行了优化，只要端口上开启了 CBQ，PING 的时延和丢包率都会大大的改善，这是实验结果，在真实设备上也一样，并没有得到 H3C 官方的任何这方面的说明。

