

实验二十八 DI-602LB+配置访问控制列表(ACL)

一、产品简介:

DI-602LB+ / DI-604LB+是专门为网吧和中小型企业事业单位推出的一款性价比极高的智能型宽带路由器。拥有强大的数据处理能力,支持多种主流宽带接入技术,并且内置丰富的防火墙功能,能够有效防止病毒攻击及非法入侵。它采用了 MARVELL 专用高速交换芯片,配合专门针对宽带接入优化操作系统,可以满足 200 个用户并发同时上网而不会出现掉线,延迟大的现象。

二、实验目的:

- 1、了解 DI-602LB+/DI-604LB+访问控制列表的配置方法。
- 2、通过 ACL 封锁 QQ 应用

三、实验设备:

- 1、DI-602LB+/604LB+ 一台
- 2、PC 两台

四、实验环境:



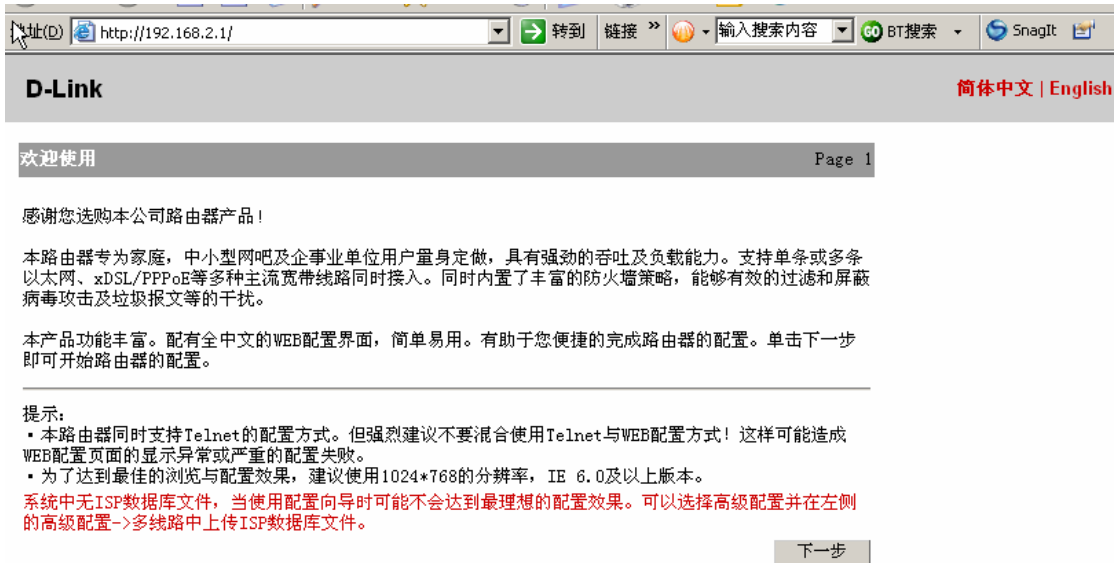
五、实验步骤:

1. DI-602LB+/604LB+缺省情况下是通过 TP2 端口来进行配置。TP2 端口的默认 IP 地址是 192.168.2.1/24。

2.把 PC1 的网卡和 TP2 端口相连 并把 PC1 的 IP 地址配置成 192.168.2.40/24 , 然后打开浏览器，输入 192.168.2.1，出现下面画面：



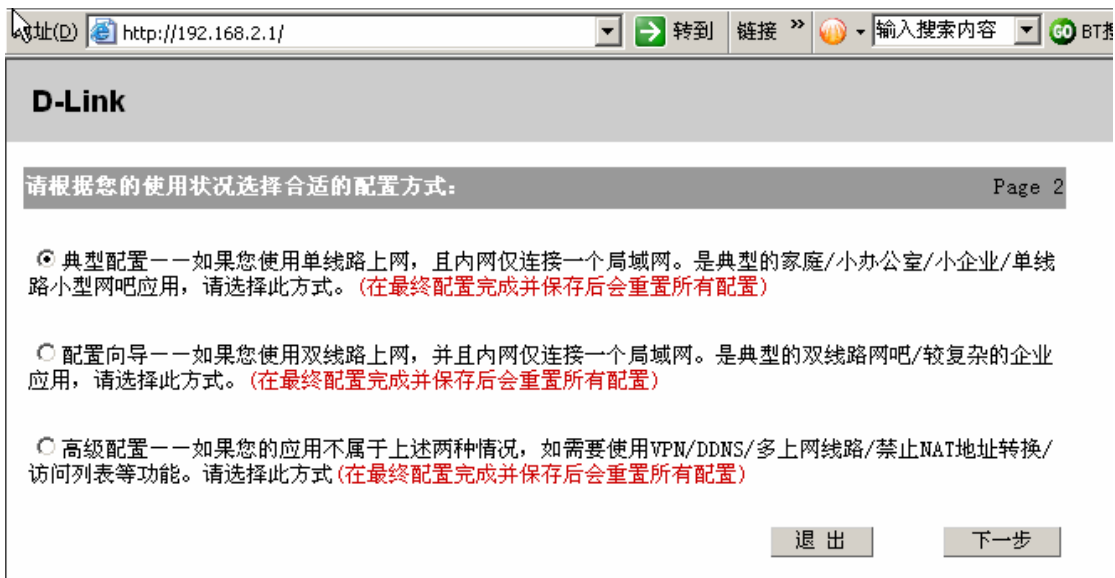
输入用户名和密码，均为 admin，单击确定，出现下面画面：



端口	类型	PPPoE	IP地址	MAC地址	协议	接收	发送	注意
TP0	WAN	No	---	00e0.0f7d.0880	down	0 packets	0 packets	
TP1	WAN	No	---	00e0.0f7d.0881	down	0 packets	0 packets	
TD2	LAN	No	192.168.2.1/24	00e0.0f7d.0882	up	408 packets	468 packets	

正在打开网页 http://192.168.2.1/?module=25...

单击下一步, 出现下面画面:



单击下一步, 出现下面画面:

D-Link

选择广域网口配置类型

广域网口 (TP0): 典型配置二: 广域网口使用PPPOE (大部分的宽带网或xDSL)

用户名: 100000595850 使用ADSL线路时的配置参数, 需要填入运营商给提供的用户名和密码信息

密码: ●●●●●●●●

局域网口设置

IP 地址: 192 . 168 . 1 . 1 (范围: 1-40)

子网掩码: 255. 255. 255. 0

DNS服务器IP: 202. 96. 209. 133 (当勾选开启DHCP服务器功能时必须填入此项。)

开启DHCP服务器功能

退出

3. 广域网口选择 PPPOE 方式连接, 并填写 ADSL 账户的用户名和密码, 单击下一步, 出现下面画面:

D-Link

配置参数汇总 Page 6

广域网口配置

TP0:	典型配置二: 广域网口使用PPPOE (大部分的宽带网或xDSL)
用户名:	100000595850

局域网口配置

TP1 - TP2 可作为局域网口	
IP 地址:	192. 168. 0. 1
子网掩码:	255. 255. 255. 0
DNS服务器IP:	202. 96. 209. 133
开启DHCP服务器功能:	启用
IP可分配的地址范围:	192. 168. 0. 50 - 192. 168. 0. 250

提示: 所有配置将在点击保存并重启后生效。

退出 上一步 保存并重启

确认配置无误后, 单击保存并重启, 出现下面画面:



提交处理中 ...

请稍候！请在本次配置完成后再进行其他的配置，以免配置失败！

**设备正在重启，本次配置的连接已经断开！
大约2-3分钟之后可重新登陆。**

15秒后会自动关闭浏览器。

4. 当设备重新启动完毕，可以再次进入其配置界面进行其他相关参数的设置工作，在进入初始界面后点击“下一步”，然后在下面的页面中单击“返回配置界面”。

本路由器已经被配置过，配置为 Page 8

典型配置(一个端口连接广域网，一个端口连接局域网，启用DHCP服务器)

广域网口配置

TP0:	典型配置二：广域网口使用PPPOE（大部分的宽带网或xDSL）
用户名:	100000595850

局域网口配置

TP1 - TP2 可作为局域网口	
IP地址 & 子网掩码:	192.168.0.1 & 255.255.255.0
DNS服务器IP:	202.96.209.133
开启DHCP服务器功能:	启用
IP可分配的地址范围:	192.168.0.50 - 192.168.0.250

退出

返回配置页面

端口状态实时显示	端口	类型	PPPoE	IP地址	MAC地址	协议	收包	发包
(行48列11页)	TP0	WAN	Yes	221.221.14.91	00e0.0f7d.0880	up	128 packets	168 packets

5. 出现下图画面，单击高级配置，并在高级配置中点选防火墙，如下图：

退出高级配置

- 基本配置
- 高级配置**
 - 多线路
 - 端口映射
 - 特殊地址映射
 - >> 防火墙
 - 默认路由

防火墙

端口	过滤方向	过滤列表	启用	操作
TP0	IN	FW_TP0_IN	<input type="checkbox"/>	应用
	OUT	FW_TP0_OUT	<input type="checkbox"/>	应用
TP1	IN	FW_TP1_IN	<input checked="" type="checkbox"/>	应用
	OUT	FW_TP1_OUT	<input type="checkbox"/>	应用

提示：如果过滤列表为红色标明列表为空，为蓝色标明列表非空。

再单击 TP1 端口的 FW_TP1_IN 过滤列表，会出现设置过滤规则的画面，

6. 在过滤列表中添加如下规则：

deny	udp	IP: any	IP: any Port: eq 8000	Always
deny	ip	IP: any	IP: 219. 133. 38. 230	Always
deny	ip	IP: any	IP: 219. 133. 38. 5	Always
deny	ip	IP: any	IP: 219. 133. 48. 103	Always
deny	ip	IP: any	IP: 219. 133. 49. 5	Always
deny	ip	IP: any	IP: 219. 133. 49. 6	Always
permit	ip	IP: any	IP: any	Always

说明：(1) 添加规则的时候，时间列表，源端口等不需要设定的部分请留为空；(2) 注意，在规则设定中添加任何一条规则之后，在最后面就会产生一条隐含的规则（拒绝任何来源到任何目的），而规则的执行顺序是由上至下，所以，要在最后加上一条允许通过的规则，否则数据包就全部会被丢弃。

7. 规则设置完成后，单击返回，回到下图界面：

端口	过滤方向	过滤列表	启用	操作
TP0	IN	FW_TP0_IN	<input type="checkbox"/>	应用
	OUT	FW_TP0_OUT	<input type="checkbox"/>	应用
TP1	IN	FW_TP1_IN	<input checked="" type="checkbox"/>	应用
	OUT	FW_TP1_OUT	<input type="checkbox"/>	应用

提示：如果过滤列表为红色标明列表为空，为蓝色标明列表非空。

单击 TP1 接口 IN 方向上的“应用”按钮，使配置生效。

8 把 PC2 的 IP 地址设成自动获得 IP 方式,PC2 可以正常使用各种网络应用,但此时 QQ 不能再使用。

六、实验总结

1. 设置了任何一条规则以后 ,在最后面就隐含了一条禁止 Any 到 Any 的命令 ;
2. 规则执行顺序为自上而下 ;
3. 规则配置完成后 ,要在防火墙界面上单击 “ 应用 ” 按钮 ,使配置生效。

七、实验完毕