

不同部门间单向隔离

在路由器的实际应用中，我们经常利用“访问控制”对各用户进行访问限制，这里我们以一个例子讲述如何设置“访问控制”达到部门间的单向隔离。

要求将公司内部的财务部与销售部单向隔离，使财务部只能访问网易与广东地税局的网站和销售部的所有 PC 主机，销售部可以访问任意网站，但是不能访问财务部 PC 主机。具体设置如下：

一、点击基本设置→内网设置→内网设置，添加一个多子网段，如下图，



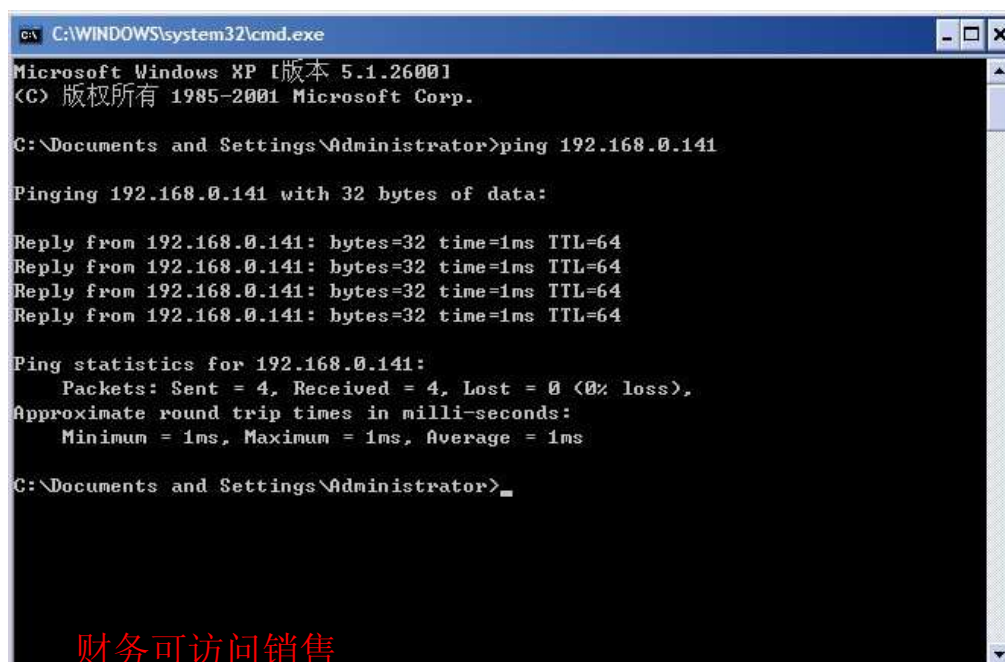
The image shows a router configuration interface with three tabs: "路由名称" (Route Name), "内网设置" (Internal Network Settings), and "DHCP服务" (DHCP Service). The "内网设置" tab is active. The configuration includes:

- 路由IP地址: 192.168.0.1
- 子网掩码: 255.255.255.0
- DNS 缓存服务器: 启用
- 老化时间: 300 秒
- 多子网段: 开关

	IP地址	子网掩码
1、	192.168.1.1	255.255.255.0
2、	0.0.0.0	0.0.0.0
3、	0.0.0.0	0.0.0.0
4、	0.0.0.0	0.0.0.0
5、	0.0.0.0	0.0.0.0

Buttons: 提交设置 (Submit Settings), 取消设置 (Cancel Settings)

为财务部分配 192.168.1.1 网段 IP，手动设置 IP 地址；销售分配 192.168.0.1 网段，可由路由器 DHCP 服务器分配。此时两个 IP 地址段内的主机可以互相访问，如下图所示：



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.0.141

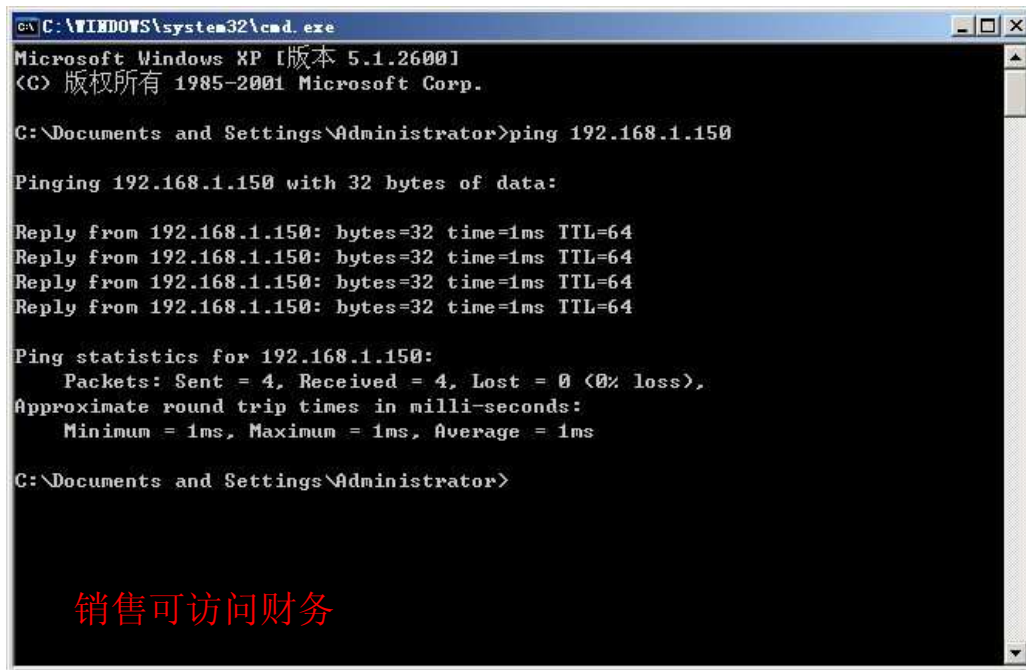
Pinging 192.168.0.141 with 32 bytes of data:

Reply from 192.168.0.141: bytes=32 time=1ms TTL=64
Reply from 192.168.0.141: bytes=32 time=1ms TTL=64
Reply from 192.168.0.141: bytes=32 time=1ms TTL=64
Reply from 192.168.0.141: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.141:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

财务可访问销售



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:

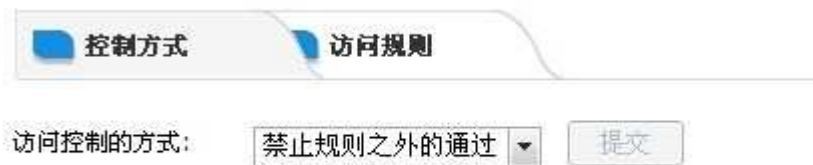
Reply from 192.168.1.150: bytes=32 time=1ms TTL=64
Reply from 192.168.1.150: bytes=32 time=1ms TTL=64
Reply from 192.168.1.150: bytes=32 time=1ms TTL=64
Reply from 192.168.1.150: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

销售可访问财务

二、点击防火墙设置→访问控制设置→访问控制→访问控制的方式：选择禁止规则之外的通过→提交，如下图：



1、点击防火墙设置→访问控制设置→访问规则，添加一条规则允许财务部访问指定的网站和销售部的主机，这里我们以网易及地税局网站为例

1.1 描述：财务允许

1.2 状态 打钩激活；

1.3 控制方式选择允许通过，执行顺序为 2；

1.4 主机 IP 地址范围填入财务部的 IP 地址范围，点击→添加→完成；

1.5 单击远端地址范围（基于域名），添加允许财务部访问的域名，及在远端地址范围中填入销售部的 IP 地址，点击完成并添加后即可。规则如下图所示：

控制方式 | **访问规则**

状态: 激活 日志

描述: 财务访问指定网站

控制方式: 允许通过

执行顺序: 1 (1-65535)值越小越先被执行。

主机IP地址范围: 192.168.1.2-192.168.1.254, (为空: 表示对该规定所有内部IP有效)

远端地址范围(基于IP): 192.168.0.2-192.168.0.254, (可以为空)

远端地址范围(基于域名): 163.com, gdltax.gov.cn (可以为空)

协议: (为空: 表示对该规定所有协议和端口)

基于时间控制: 启用

2、再做一条规则允许销售部访问任何网站但无法访问财务部

2.1 禁止访问财务部

- 1) 描述: 销售禁止访问
- 2) 状态 打钩激活 ;
- 3) 控制方式选择允许通过。执行顺序为 2;
- 4) 在主机 IP 地址范围是输入销售部地址范围,
- 5) 在远端地址 IP 中输入财务部地址网段, 点击—>添加—>完成
如下图所示:

控制方式 | **访问规则**

状态: 激活 日志

描述: 销售禁止访问财务

控制方式: 禁止通过

执行顺序: 2 (1-65535)值越小越先被执行。

主机IP地址范围: 192.168.0.2-192.168.0.254, (为空: 表示对该规定所有内部IP有效)

远端地址范围(基于IP): 192.168.1.2-192.168.1.254, (可以为空)

远端地址范围(基于域名): (可以为空)

协议: (为空: 表示对该规定所有协议和端口)

基于时间控制: 启用

2.2 允许访问任何网站

- 1) 描述: 销售允许外网
- 2) 状态 打钩激活 ;
- 3) 控制方式选择允许通过。执行顺序为 3;
- 4) 在主机 IP 地址范围是输入销售部地址范围, 点击—>添加—>完成

如下图所示：

控制方式

访问规则

状态： 激活 日志

描述：

控制方式：

执行顺序： (1-65535) 值越小越先被执行。

主机IP地址范围： (为空：表示对该规定所有内部IP有效)

远端地址范围 (基于IP)： (可以为空)

远端地址范围 (基于域名)： (可以为空)

协议： (为空：表示对该规定所有协议和端口)

基于时间控制： 启用

三、IP-MAC 地址绑定

在做完以上访问规则后，用户需要对内网 IP 地址进行物理地址绑定，点击“认证服务器->IP/MAC 绑定”，只需填写描述、IP 地址、绑定类型为唯一，点击查询 MAC 地址，添加，即可完成对 IP/MAC 地址绑定。如下图所示：

MAC地址绑定

描述：

IP地址：

MAC地址：

类型：

接口：

描述信息	IP地址	MAC地址	类型	接口	操作
销售部01	192.168.0.141	00:0d:60:d0:73:25	唯一	局域网	
财务部01	192.168.1.150	00:e0:4c:08:a9:a3	唯一	局域网	

四、做完以上规则后，需要“保存设置”，并对以上所做规则进行测试，以免设置后无法达到预定效果，影响工作效率。

1. 财务部测试效果：

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.0.141

Pinging 192.168.0.141 with 32 bytes of data:

Reply from 192.168.0.141: bytes=32 time=1ms TTL=64
Reply from 192.168.0.141: bytes=32 time=1ms TTL=64
Reply from 192.168.0.141: bytes=32 time=1ms TTL=64
Reply from 192.168.0.141: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.141:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

财务可访问销售

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping news.163.com

Pinging news.163.com [119.147.105.189] with 32 bytes of data:

Reply from 119.147.105.189: bytes=32 time=11ms TTL=57
Reply from 119.147.105.189: bytes=32 time=10ms TTL=57
Reply from 119.147.105.189: bytes=32 time=10ms TTL=57
Reply from 119.147.105.189: bytes=32 time=10ms TTL=57

Ping statistics for 119.147.105.189:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 11ms, Average = 10ms

C:\Documents and Settings\Administrator>ping www.baidu.com

Pinging www.baidu.com [61.135.169.125] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 61.135.169.125:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

只可访问指定网站

2、销售部测试效果:


```
ca C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

销售部无法访问财务部

```
ca C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping www.qq.com

Pinging www.qq.com [123.129.194.144] with 32 bytes of data:

Reply from 123.129.194.144: bytes=32 time=62ms TTL=57
Reply from 123.129.194.144: bytes=32 time=61ms TTL=57
Reply from 123.129.194.144: bytes=32 time=62ms TTL=57
Reply from 123.129.194.144: bytes=32 time=62ms TTL=57

Ping statistics for 123.129.194.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 62ms, Average = 61ms

C:\Documents and Settings\Administrator>ping www.sohu.com

Pinging www.sohu.com [121.14.0.103] with 32 bytes of data:

Reply from 121.14.0.103: bytes=32 time=8ms TTL=57
Reply from 121.14.0.103: bytes=32 time=8ms TTL=57
Reply from 121.14.0.103: bytes=32 time=7ms TTL=57

Ping statistics for 121.14.0.103:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 8ms, Average = 7ms
```

允许访问任何网站