

设置交换机的侦听口以监视网络会话

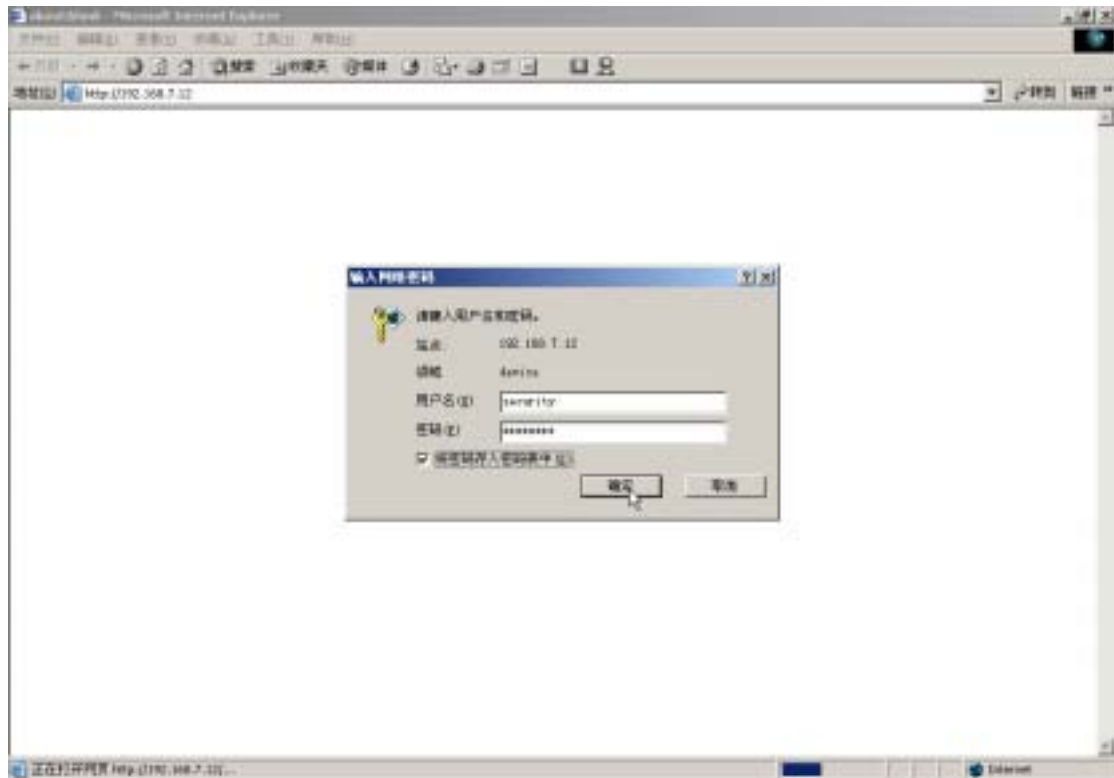
作者：SQL (SQL@263.net)

网站：www.isfocus.com

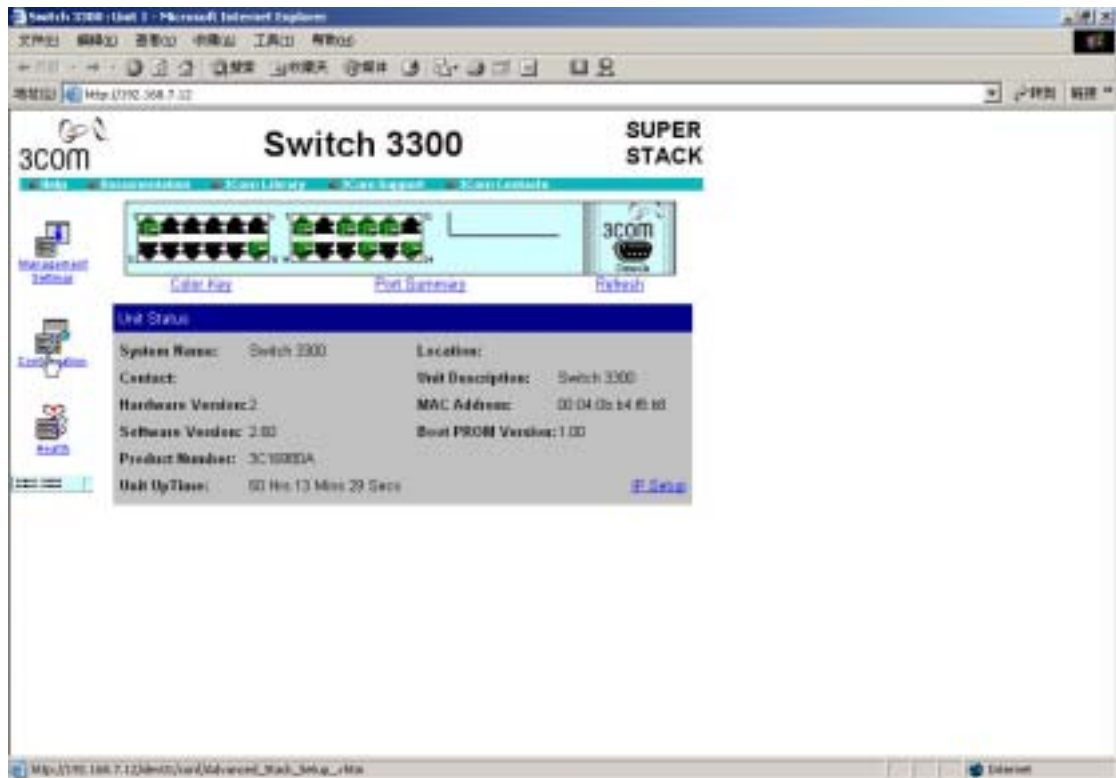
以前公司里用 HUB 的时候，可是非常幸福哦，我随便开一个 IRIS 就能监视整个公司里的网络数据包，能很方便和清楚的看到大家都在做什么，简直就是没有秘密可言了。后来玩 IDS 测试 SESSIONWALL 的时候我用 URL 的预先阻断功能，就能做到想黑那里就黑那里的假像，后来很多人纷纷效仿把公司网络简直搞的是一团糟糕。总结一下就是基于 HUB 的网络安全性能实在是非常低，而且几乎没有什么可管理性。如果您正在筹划一个新的网络结构，我强烈建议采用交换机代替 HUB 来实现（当然费用的差距也必须考虑）。

采用交换机的网络基本上就没有可被监听的危险了，但是前提就是交换机也必须好好配置和管理，否则把买来的设备用默认状态摆在那里也是很危险的。还是以我们公司为例好了。我们用的是 3COM 的 3300 的交换机 24 口的那种，我简单的把我的网络接口配置成了一个侦听接口，还是可以轻松的监听整个网络的数据包，下面简单的介绍下步骤。说明下就是现在的网络监视软件如 IDS 和信息审计系统等等都是需要把自己的网络接口在交换机上设置为侦听口的，否则是没有办法正常监视网络流量的。

首先是用串口从后面接上交换机给设备设置一个 IP 地址，这个可以随便设置当然和我们在一个网段是最方便的了。然后默认情况下 3COM 的 WEB 服务就是打开的我们可以用 IE 登陆上去。



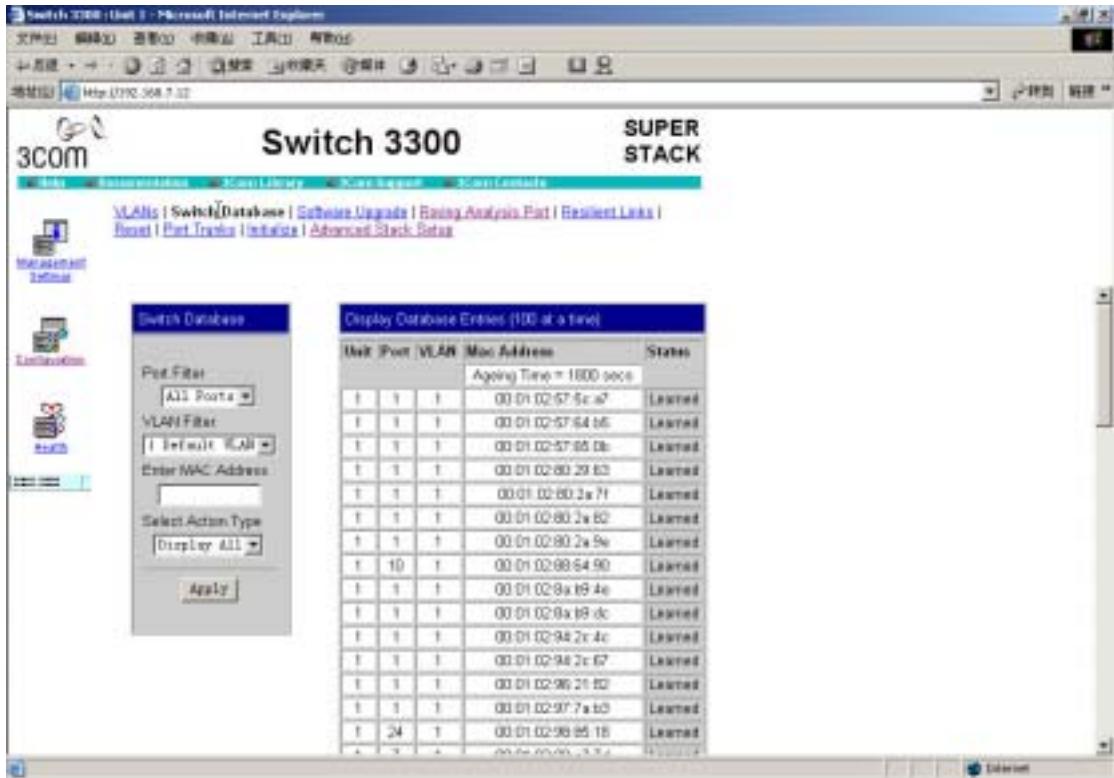
默认的口令和用户名我们可以用 :security 登陆这是 3COM 设备的一个默认管理帐号，很多人没有改有意思的是我在互联网上用 SNMP 扫描找到的 3COM 交换机 99%用这个帐号都可以进去。



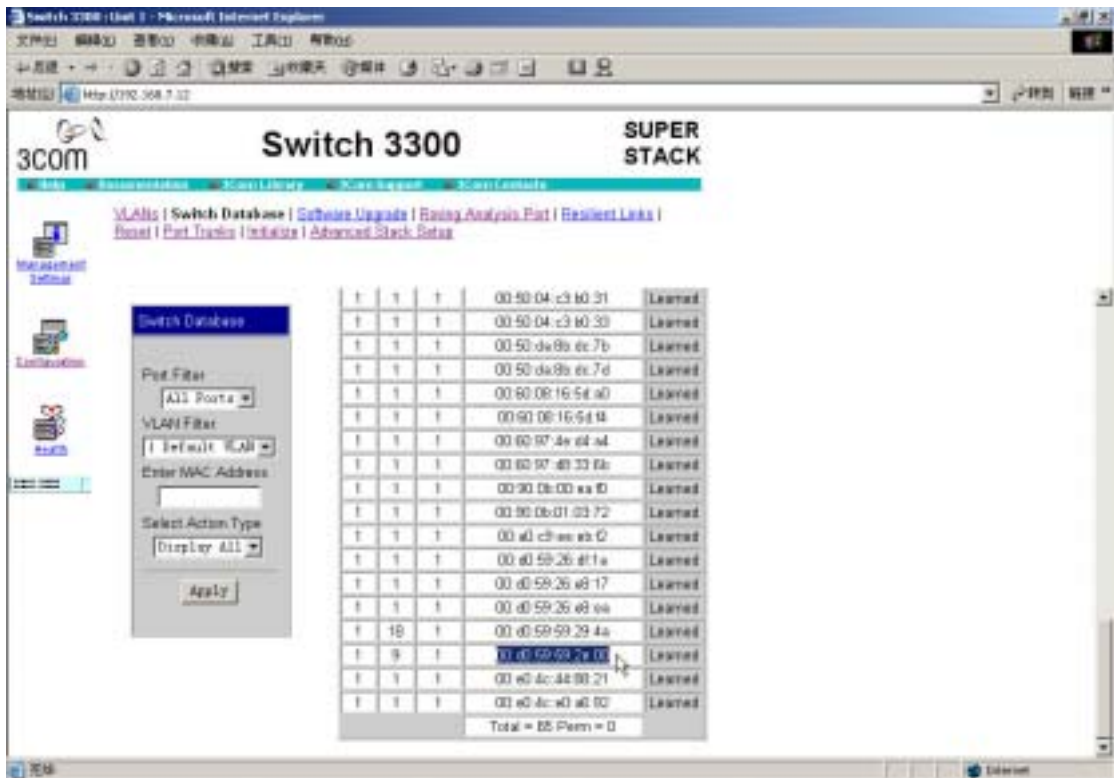
成功通过验证后我们就可以看到如上的管理界面了,感觉 3300 的管理界面做的还是不错的。简单易用,功能还很强大,听说 4400 更厉害可惜还没有用过。



我们点击左面的 **configuration** 选项,再从右边出来界面中选择 **Roving AnalysisPort**。这个界面就是配置交换机侦听口的地方了。当然你如果实现知道自己的网络接口接在交换机那个口上就比较方便可以直接配置了,如果你不知道的话可以点击 **Advanced Stack Setup** 这里来查看当前 IP 地址和交换机端口的对应关系。

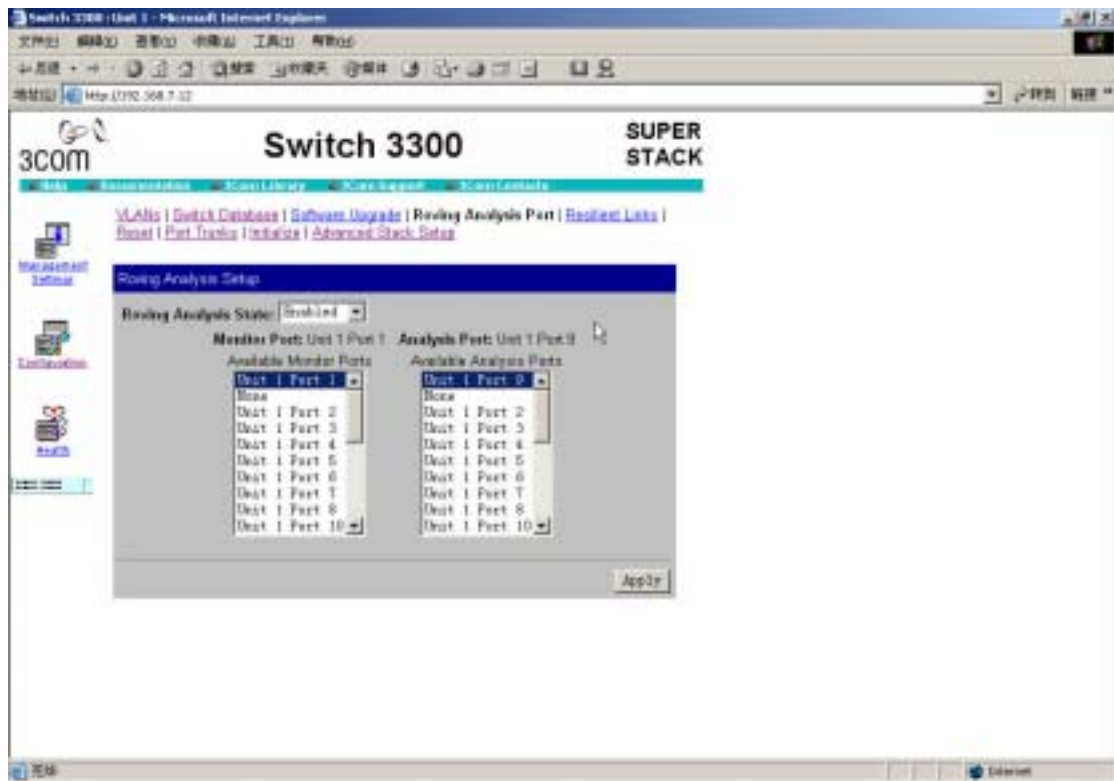


从上面界面中，很方便的可以查看这个交换机一共有多少个接口 VLAN 以及对应的 MAC 地址都是什么。

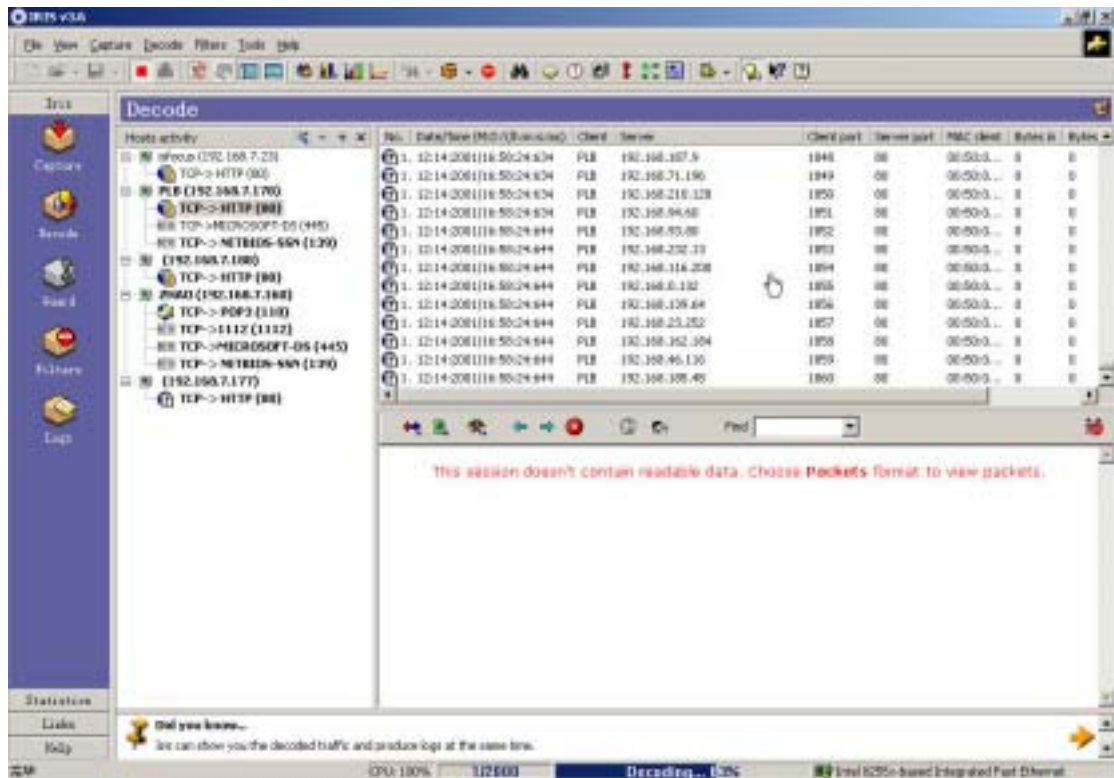


看到没有上面 00:00:59:59:2e:00 对应的第 9 个口就是接的我的计算机上面的地址是我的网

卡的 MAC 地址，记住这个下面就可以把交换机上第 9 口设置为整个交换机的侦听口了。



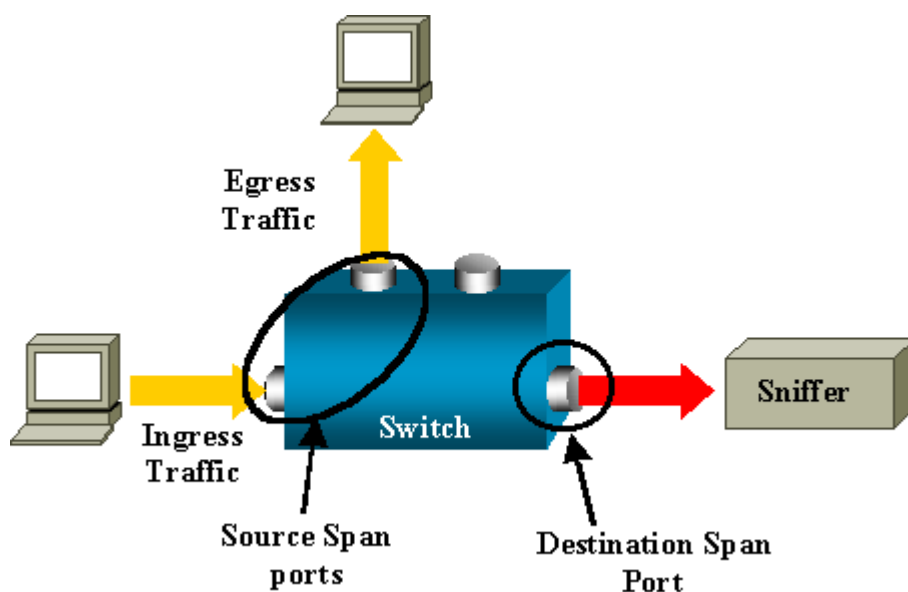
回到刚才的 Roving Anaysis Port 设置地方，在左面的 Available Monitor Ports 里面选择 Unit 1 Port 1 代表选择整个交换机的所有端口，并不是我一开始理解的只是 PORT1 上的流量内容而是交换机上所有的流量报文。右边的 Available Analysis Ports 选择我们刚才看到自己的 Port 9 然后在 STATE 里面选择 Enabled 就可以了。



打开 IRIS 又可以监视整个网络中的报文了，正好看到一个同事的计算机在疯狂的发送 445 和 80 的数据包，一看目的 IP 都是随机的肯定又是中了 NIMUDA 了，赶快通知他杀毒避免了部门里其他同事的受害，是不是很有成就感。

这是 3COM 的交换机下面的简单的把 CISCO 的设置办法也帖出来，国内目前这两种设备用的算是比较多的了。

所谓侦听端口是指这样一个端口，所有通过被侦听端口的流量都会被自动复制一份传至该端口，缺省的情况下交换机上的这种功能是被屏蔽(Disable)的。如果需要可以手工设置。见下图。



Egress Traffic: 离开交换机的流量

Ingress Traffic: 进入交换机的流量

Source Span ports: 被侦听端口

Destination Span Port: 侦听端口

Administrative Source: 所有配置为被侦听口或被侦听 vlan 的列表

一、 Cisco Catalyst 4000, 5000, and 6000 Series 系列交换机，有关设置侦听端口的命令由一系列 set span 命令组成。

```
switch (enable) set span
```

```
Usage: set span disable [dest_mod/dest_port|all]
```

```
set span <src_mod/src_ports...|src_vlans...|sc0>
```

```
<dest_mod/dest_port> [rx|tx|both]
```

```
[inpkts <enable|disable>]
```

注：src_mod 是指被侦听的端口号；src_ports 是指被侦听端口所在的模块号；dest_mod,是指侦听端口号；dest_port 是指侦听端口所在的模块号；src_vlan 是 vlan 名，表示属于该 vlan 的端口都是被侦听端口；rx 是指只侦听接收的包；tx 是指只侦听发送的包；both 是指侦听收、发双方向的包。

配置过程如下：

1、使用基于端口的侦听方式：

```
switch (enable) set span enable
switch (enable) set span 6/1 , 6/3 6/2
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1,6/3
Oper Source : Port 6/1,6/3
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

这条命令执行后，端口 6/2 设置为侦听口，端口 6/1，6/3 设置为被侦听口。接在端口 6/2 上的机器将能接收到通过端口 6/1，6/3 的所有流量。

2、使用基于 vlan 的侦听方式：

```
switch (enable) set span enable
switch (enable) set span 2,3 6/2
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

这条命令执行后，端口 6/2 设置为侦听口，属于 vlan 2，3 的所有端口设置为被侦听口。接在端口 6/2 上的机器将能接收到通过属于 vlan 2，3 的端口的所有流量。

3、可以使用命令 Switch(enable) show span 来查看设置的结果：

```
switch (enable) show span
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
```

Filter : -
Status : active

注：侦听口与被侦听口可以不属于同一个 vlan。

二、Cisco Catalyst 2900XL/3500XL/2950 系列交换机，配置命令为：

```
Switch(config-if)#port monitor interface
```

注：interface 是指侦听端口。

举例：我们要将接口 Fa0/1 设置为侦听口，Fa0/2 及 Fa0/5 设置为被侦听口，基本过程如下：

1、在配置模式下，首先选择接口 Fa0/1:

```
Switch(config)#int fa0/1
```

输入被侦听端口：

```
Switch(config-if)#port monitor fastEthernet 0/2
```

```
Switch(config-if)#port monitor fastEthernet 0/5
```

指定管理端口：

```
Switch(config-if)#port monitor VLAN 1
```

这条命令并不意味着接口 Fa0/1 将侦听 vlan 1 的所有端口，它只是用来指定管理接口。

退出保存后，接口 Fa0/1 设置为侦听口，接口 Fa0/2, Fa0/5 设置为被侦听口。连接在接口 Fa0/1 上的机器将能接收到通过接口 Fa0/2, Fa0/5 的流量。

可以用命令 Switch# show port monitor 来查看设置的结果：

```
Switch#show port monitor
```

```
Monitor Port Port Being Monitored
```

```
-----  
FastEthernet0/1 VLAN1
```

```
FastEthernet0/1 FastEthernet0/2
```

```
FastEthernet0/1 FastEthernet0/5
```

注：侦听口与被侦听口必须属于同一个 vlan。

说了这么多的废话，只是的简单的介绍了下交换机侦听口这个东西和它的强大应用。以及如果被入侵者利用的一个危害。所以建议对于网络中设备的安全也不应该忽视，尤其是默认的口令和 SNMP 的关键字的问题都是需要注意，另外像 WEB 这种服务最好也不好开。CISCO 的设备很多都可以利用 WEB 服务的越权访问漏洞进去的（在我其他的文章里有详细介绍）。总之保证网络中的每一个接点的安全才可以最终构建出一个真正安全的网络工作环境。

ISFOCUS 小组是由一群可爱的年轻人组成的，处于对网络安全的钻研热情使大家彼此成为朋友，我们欢迎你的加入。