第 5 章　企业网络安全及网络管理

5.1　网络设备的安全

从广义上讲，网络安全可以分为网络设备安全和网络信息安全。网络管理员通常都能够对网络信息的安全给予足够的重视，却往往忽略了网络设备本身的安全。事实上，几乎所有的网络设备都存在着一些漏洞，掌握了这些漏洞的人可以控制设备，产生的后果很可能是毁灭性的。因此，没有网络设备的安全，网络的安全策略就没有任何意义。网络设备安全的重要性要求网络管理员必须十分清楚自己所管理的网络设备的安全程度并及时作出调整，确保设备安全，以避免受到攻击而造成不必要的损失。

网络设备安全包括了网络设备的物理安全和对网络设备的访问控制两个方面。网络设备最基本的安全性是要通过非网络技术手段来保证的。

5.1.1　网络设备的物理安全

网络设备的物理安全是指网络设备周围环境的安全及网络设备硬件的安全，是网络安全体系中最为重要的部分。通常可以从以下几个方面加以提高。

1. 提供正确的物理环境

正确的物理环境应该对场地的封闭、防火、防盗、防静电、适当的通风、温度的控制以及电源的安全等提供符合网络设备要求的安全保证。

基本的环境要求有：

（1）承重要求：根据设备及其附件（比如机柜、机箱、单板和电源等）的实际重量来评估地面承重要求，确保机房地面的承重能力满足要求。

（2）温度要求：机房内需维持温度在 0～40℃（长期工作）。

机房温度过高将会加速绝缘材料的老化过程，使设备的可靠性大大降低，严重影响设备的寿命。

（3）湿度要求：机房环境湿度需保持在 5%～95%（无冷凝）状态。

机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件锈蚀等现象。若机房内相对湿度过低，绝缘垫片会干缩而引起紧固螺钉松动，同时在干燥的气候环境下易产生静电，危害设备上的电路。

（4）洁净度要求：机房灰尘粒子≤3×10^4粒/m^3（3 天内桌面无可见灰尘）。

灰尘对设备的运行安全是一大危害。室内灰尘落在机体上，可以造成静电吸附，使金属接插件或金属接点接触不良。尤其是在室内相对湿度偏低的情况下，更易造成静电吸附，不但会影响设备寿命，而且容易造成通信故障。

（5）抗干扰要求：对供电系统要采取有效的防电网干扰措施。设备工作地最好不要与电力设备的接地装置或防雷接地装置合用，并尽可能距离远。远离强功率无线电发射台、雷达发射台和高频大电流设备。

（6）接地要求：为设备提供良好的接地系统，机箱与大地之间的电阻要小于 1Ω。良好的接地系统是设备稳定可靠运行的基础，是防雷击、抗干扰和防静电的重要保障。

（7）供电要求：按设备要求规划提供供电系统。表 5.1 列出了一些交换机交流电源模块规格的参数要求。

表 5.1　交流电源模块规格

项　　目	描　　述
额定电压范围	100～120V AC/ 200～240V AC;50/60Hz
最大电压范围	90～264V AC;47～63Hz
最大输入电流	13.3 A
输出功率	1200W(100～120V AC);2000W(200～240V AC)

（8）空间要求：为了便于散热和设备维护，建议设备前后与墙面或其他设备的距离不应小于 0.8m。如果安装于机柜，那么机房的净高不能小于 3m。

2. 控制到设备的直接访问

制定机房安全管理制度，严格管理机房的人员出入。

在可能的情况下为机架上锁，并且在控制台和辅助端口设置口令。如果不使用的话，建议关闭这类辅助端口，因为从理论上讲，只要能从物理上接近设备，就能通过改变设备上的一些硬件开关重置管理员口令或恢复出厂设置。

5.1.2　对网络设备的访问控制

对网络设备的访问控制的主要目的是防止非法用户进入网络设备并对其配置进行非法修改，避免网络瘫痪。对网络设备的访问进行控制包括为各种用户设置并加密口令，对远程访问用户（包括虚拟终端用户和 Web 用户）实施 ACL（访问控制列表），以及设置空闲会话超时、设置警示登录标语等技巧。

1. 通过设置并加密口令实现访问控制

网络设备提供的最基本的安全是在设备访问和配置过程中设置登录口令。如果对设备的访问和配置不加以审查，往往会引发安全问题。例如，通常设备出厂时没有设置登录口令或设置一些简单的默认口令，一些管理员就利用这些默认的口令进行管理，使攻击者很轻易就能找到一个入口登录设备。

口令设置包括 Console 口的登录口令、Telnet 远程登录口令和用户控制级别口令等的设置。

1）Console 口用户登录口令设置

Console 口用户登录认证方式有 None、Password 和 Scheme。默认情况下，Console 口登录用户具有最高权限，可以使用所有配置命令，并且不需要任何口令认证。因此，应对 Console 口用户登录进行适当的认证。

【例】 设置通过 Console 口登录交换机的用户进行 Password 认证，口令是明文 123456。

```
# 进入系统视图
<H3C> system-view
```

```
# 进入 AUX 用户界面视图
[H3C] user-interface aux 0
# 设置通过 Console 口登录交换机的用户进行 Password 认证
[H3C-ui-aux0] authentication-mode password
# 设置用户的认证口令为明文方式,口令为 123456
[H3C-ui-aux0] set authentication password simple 123456
[H3C-ui-aux0] quit
[H3C] quit
<H3C>  save
<H3C> reboot
```

重新启动交换机后,系统将提示登录用户输入访问口令,当输入刚才设置的口令123456(屏幕不显示)后,才能进入用户界面。

2) Telnet 远程登录口令设置

Telnet 登录也有 None、Password 和 Scheme 三种认证方式。

【例】 设置通过 Telnet 远程登录交换机的用户进行 Password 认证,口令是明文123456。

```
# 进入系统视图
<H3C>  system-view
# 进入 VTY0~VTY4 用户界面视图
[H3C] user-interface vty 0 4
# 设置通过 VTY0~VTY4 口登录交换机的用户进行 Password 认证
[H3C-ui-vty0-4] authentication-mode password
# 设置用户的认证口令为明文方式,口令为 123456
[H3C-ui-vty0-4] set authentication password simple 123456
[H3C-ui-vty0-4]quit
<H3C> save
<H3C> reboot
```

3) 用户控制级别口令的设置

登录用户的命令级别分为 4 个等级,不同的级别下只能使用等于或低于自己的级别的命令。使用 Console 口登录时系统默认值为最高级别 3,而从 VTY 用户界面登录时系统默认可以访问的命令级别为 0 级。登录用户的级别可以通过命令进行切换,高级别用户可以无条件切换为低级别用户,但是低级别用户从当前级别切换到高级别时,则必须通过相应的认证。为防止未授权用户的非法入侵,应设置用户从低级别切换到高级别时需要输入高级别用户的口令。

在进行用户级别切换时,为了保密,用户在屏幕上看不到所输入的密码。如果在系统允许的次数(3 次)内输入正确的认证信息,则切换到高级别用户,否则保持原用户级别不变。

【例】 设置通过 Console 口登录交换机的用户默认级别为 0,并设置切换各控制级别的口令。

```
# 进入系统视图
<H3C>system-view
# 进入 AUX 用户界面视图
```

```
[H3C] user-interface aux 0
# 设置默认用户登录级别为 0
[H3C-ui-aux0] user privilege level 0
[H3C-ui-aux0] quit
# 设置 1 级用户登录口令
[H3C]super password level 1 simple h3c1
# 设置 2 级用户登录口令
[H3C]super password level 2 simple h3c2
# 设置 3 级用户登录口令
[H3C]super password level 3 simple h3c3
[H3C]quit
<H3C>save
<H3C>reboot
```

交换机重启后，使用命令 super [*level*]来切换当前权限级别时将会提示输入验证口令。

2. 对虚拟终端的访问控制

虚拟端口相对于实端口而言，一般根据需要在交换机或路由器上虚拟出一些端口，称为虚拟终端或虚拟端口。每台设备一般有 5 个默认虚拟终端，在虚拟终端线路上实施 ACL（访问控制列表），可以控制谁能远程登录到该设备（访问控制列表内容详见 5.3 节，在此仅做简要介绍）。在虚拟终端线路上实施 ACL 具体有以下 3 种方式：

（1）通过基本 ACL 实现：通过源 IP 对 Telnet 用户进行控制。

（2）通过高级 ACL 实现：通过源 IP、目的 IP 对 Telnet 用户进行控制。

（3）通过二层 ACL 实现：通过源 MAC 对 Telnet 用户进行控制。

其中最常用的是通过源 IP 对 Telnet 用户进行控制，需要下面两个步骤：

（1）定义访问控制列表。

（2）引用访问控制列表，对 Telnet 用户进行控制。

【例】 在交换机上设置通过源 IP 地址对 Telnet 登录用户进行控制，仅允许源 IP 为 10.110.100.52 的 Telnet 用户访问本交换机。

```
# 定义基本访问控制列表
<H3C>system-view
[H3C] acl number 2000
# 仅允许源 IP 为 10.110.100.52 的用户访问交换机
[H3C-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[H3C-acl-basic-2000] quit
# 对虚拟终端引用访问控制列表
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] acl 2000 inbound
```

3. 对 Web 控制台的访问控制

通过 Web 远程管理网络设备具有友好的操作界面，使配置网络设备变得更加容易，但同时也容易引发一些安全问题，最好的解决办法是通过实施 ACL 控制哪些地址可以访问网络设备的 Web 服务（访问控制列表详见 5.3，在此仅做简要介绍）。

和对虚拟终端的访问控制类似，最常用的是通过源 IP 对 Web 用户进行控制，需要下面

两个步骤：

(1) 定义访问控制列表。

(2) 引用访问控制列表，对 Web 网管用户进行控制。

【例】 在交换机上设置通过源 IP 地址对 Web 网管用户进行控制，仅允许 IP 地址为 10.110.100.52 的 Web 网管用户访问交换机。

```
# 定义基本访问控制列表
<H3C>system-view
[H3C] acl number 2030
[H3C-acl-basic-2030] rule 1 permit source 10.110.100.52 0
[H3C-acl-basic-2030] quit
# 引用编号为 2030 的访问控制列表，仅允许来自 10.110.100.52 的 Web 用户访问交换机
[H3C] ip http acl 2030
```

必要时可通过命令 undo ip http enable 关闭 Web 服务，以减少安全隐患。

4. 控制会话超时及设置警示登录标语消息

如果控制台在用户控制级别为 level 3 下时没有人看管，那么任何人都可以乘机修改网络设备的配置。而对空闲会话的超时设置可以获得额外的安全保障。默认情况下，所有的用户界面的超时时间为 10 分钟，时间一到则断开会话。可以通过 idle-timeout 命令改变会话超时时间。

登录标语消息是当用户登录网络设备时，在界面上显示的内容。如果显示一些对非授权访问者的警告，如“非授权访问将被依法起诉”等，可以从心理上吓退一些非授权用户。

1) 设置用户界面的超时断开连接时间

idle-timeout *minutes* [*seconds*]
undo idle-timeout

【视图】 用户界面视图

【参数】 *minutes*：分钟数，取值范围为 0～35 791。

seconds：秒数，取值范围为 0～59。

默认情况下，用户超时断开连接的时间为 10 分钟。如果在所设定的时间内登录到当前用户界面上的用户没有对交换机执行任何操作，交换机将断开与该用户的连接。

设置 idle-timeout 0 即关闭超时中断连接功能。

【例】 控制用户界面超时时间为 6 分钟。

```
# 进入系统视图
<H3C>system-view
# 进入 AUX 用户界面视图
[H3C] user-interface aux 0
[H3C-ui-aux0] idle-timeout 6
[H3C-ui-aux0]quit
# 进入 VTY0~VTY4 用户界面视图
[H3C] user-interface vty 0 4
# 设置 VTY0 用户界面的超时时间为 6 分钟
```

```
[H3C-ui-vty0-4] idle-timeout 6
```

2）配置登录设备时的显示信息

header [**incoming** | **legal** | **login** | **shell**] *text*
undo header [**incoming** | **legal** | **login** | **shell**]

【视图】 系统视图

【参数】 incoming：配置 Modem 登录用户进入用户视图时的显示信息。

legal：配置登录用户进入用户视图前的授权信息。

login：配置登录验证时的显示信息。

shell：配置非 Modem 登录用户进入用户视图时的显示信息。

text：标题文本。当 login、shell、incoming 和 legal 没有配置时，默认为登录信息 login 的内容。系统支持两种输入方式：一种方式为所有内容在同一行输入，此时包括命令关键字及空格在内总共可以输入 254 个字符；另一种方式为通过按回车键分多行输入，此时不包括命令关键字在内最多可输入 2000 个字符（包括不可见字符，例如回车符等）。标题内容以第一个字符作为起始符和结束符，输入结束符后，按回车键退出交互过程。

【例】 配置登录验证时的显示信息。

```
[H3C] header login %
Input banner text, and quit with the character '%'.
Non-authorized,shall be sued at law! %
```

【拓展思考】

假设你是计算机网络实验室的管理员，请为本实验室拟定机房安全管理制度。

5.2　交换机端口安全

5.2.1　交换机端口地址绑定

5.2.1.1　交换机静态端口地址绑定——“MAC＋IP＋端口”绑定

【引入案例 1】

办公室主任的计算机配置在一个特定的地址段中，公司对该地址段开放了特殊的上网权限。有一天，主任的计算机上弹出了“IP 地址冲突”的对话框。有员工盗用了他的 IP 上网浏览。

【引入案例 2】

企业办公大楼网络中有一台计算机感染了病毒，引发了大量的广播数据包在网络上洪泛，网络管理员小王唯一的想法就是尽快地找到病源主机，并把它从网络中暂时隔离。

【案例分析】

当网络的布置很随意，并且没有任何安全设置的时候，用户只要插上网线，在任何地方都能够上网，这虽然使正常情况下的大多数用户很方便很满意，却很容易出现案例 1 中用户盗用 IP 的现象，而且一旦发生案例 2 中描述的网络问题，虽然网络管理员可以通过一些网

络监控软件查出感染病毒主机的 IP 地址或 MAC 地址信息，却很难快速、准确地定位主机，更谈不上将它隔离。

解决上述问题的一个较好的办法是将用户主机和接入交换机的端口进行绑定，也就是说，特定主机只有在某个特定端口下发出数据帧时，才能被交换机接收并转发，如果这台主机移动到其他位置，则无法实现正常访问网络。通过绑定技术，建立起“用户主机-交换机端口”的对应关系，在安全管理上起着非常重要的作用。

【基本原理】

网卡的 MAC 地址的唯一性确定了 MAC 地址在网络中代表着计算机身份证的作用。为了安全和方便管理，网络管理员将对用户计算机的 MAC 地址进行登记，并将 MAC 地址与接入交换机的端口进行绑定。MAC 地址与交换机端口绑定后，该 MAC 地址的数据流只能从绑定端口进入，而不能从其他端口进入，也就是说，特定主机只有在某个特定端口下发出数据帧时，才能被交换机接收并转发，如果这台主机移动到其他位置，则无法实现正常上网。

当一个 MAC 地址和交换机端口绑定后，该交换机端口仍然可以允许其他 MAC 地址的数据流通过。实际上，一些工具软件和病毒很容易伪造计算机的 MAC 地址，因此通常的做法是不要把网络安全信任关系单独建立在 IP 的基础上或 MAC 的基础上，理想的关系应该是建立在 IP＋MAC 的基础上。因此，通过“MAC＋IP＋端口”绑定，可以实现设备对转发报文的过滤控制，提高网络安全性。

实施“MAC＋IP＋端口”绑定后，会在交换机内部形成一个静态的“MAC-IP-端口”映射表，如图 5.1 所示。当端口接收到报文时，交换机将查看报文中的源 MAC、源 IP 地址与交换机所配置的静态表项是否一致。如果报文中的源 MAC、源 IP 地址与设定的 MAC、IP 相同，端口将转发该报文；如果报文中的源 MAC、源 IP 地址中任一个与所设定的 MAC、IP 不同，端口将丢弃该报文。

图 5.1 中，交换机查看来自 PC1 和 PC3 的报文，发现 PC1 和 PC3 的 MAC 地址与映射表中和端口 Ethernet1/0/1、Ethernet1/0/3 绑定的 MAC 地址并不匹配，于是交换机丢弃报文。因此 PC1 和 PC3 不能正常通信，只有 PC2 能正常工作。

一般来说，二层交换机主要技术特点是低交换延迟、支持不同的传输速率和工作模式和支持 VLAN。交换机最重要的一项工作是自学习 MAC 地址，即建立和维护“端口/MAC 地址映射表”，并没有对 IP 数据报进行处理的功能。因此要进行“MAC＋IP＋端口”绑定，可以采用二层智能型可网管交换机（又称 ACL 交换机或二层半交换机）。二层半交换机具有支持网络管理、广播风暴控制、支持流控、链路聚合功能、端口安全控制和静态地址绑定等功能，能满足宽带网对交换机在更大的带宽、更高的管理性能和更强的适应能力上的要求。

注意：在 H3C 接入层 S3100 系列的交换机中，二层半的 S3100-EI 系列以太网交换机支持“MAC＋IP＋端口”绑定。H3C 交换机中有些产品只支持“IP＋MAC＋端口”三者同时绑定，有些可以支持“IP＋端口”、“MAC＋端口”、“IP＋MAC”三种绑定方式中的任意两者。交换机是否支持端口绑定，支持哪一种方式的绑定要具体看其硬件及软件版本来确定。

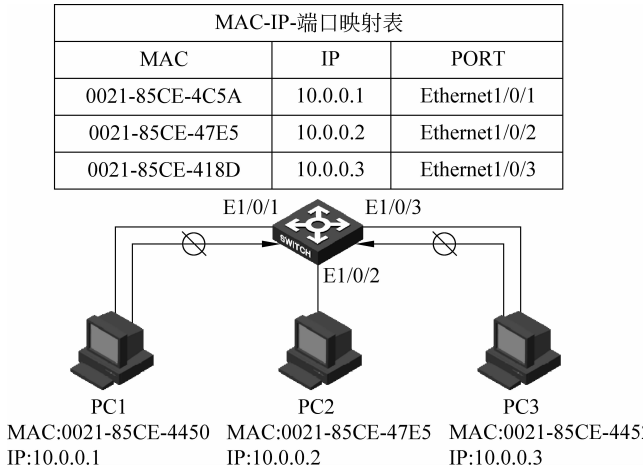

图 5.1　“MAC＋IP＋端口”绑定

“MAC＋IP＋端口”绑定技术适用于计算机位置固定、配置静态 IP 地址的办公室环境，对于有大量便携机的员工的园区网并不适用。

【命令介绍】

1. 将用户的 MAC 地址和 IP 地址绑定到指定端口上

1）在系统视图下

```
am user-bind mac-addr mac-address { ip-addr ip-address | ipv6 ipv6-address }
    [ interface interface-type interface-number ]
undo am user-bind mac-addr mac-address { ip-addr ip-address | ipv6 ipv6-address }
    [ interface interface-type interface-number ]
```

2）在以太网端口视图下

```
am user-bind { mac-addr mac-address [ip-addr ip-address | ipv6 ipv6-address] |
    ip-addr ip-address | ipv6 ipv6-address }
undo am user-bind { mac-addr mac-address [ip-addr ip-address | ipv6 ipv6-address]
    | ip-addr ip-address | ipv6 ipv6-address }
```

【视图】 系统视图/以太网端口视图

【参数】 interface *interface-type interface-number*：指定绑定的端口。其中 *interface-type interface-number* 表示端口类型和端口编号。

ip-addr *ip-address*：指定需要绑定的 IP 地址。其中 *ip-address* 表示绑定的 IP 地址。

mac-addr *mac-address*：指定需要绑定的 MAC 地址。其中 *mac-address* 表示绑定的 MAC 地址，格式为 H-H-H。

【例】 在系统视图下将 MAC 地址为 000f-e200-5101、IP 地址为 10.153.1.1 的合法用户与端口 Ethernet1/0/1 进行绑定。

```
[H3C] system-view
[H3C] am user-bind mac-addr 000f-e200-5101 ip-addr 10.153.1.1 interface
    Ethernet1/0/1
```

2. 显示端口绑定的配置信息

display am user-bind [**interface** *interface-type interface-number* | **ip-addr** *ip-addr* | **mac-addr** *mac-addr*]

【视图】 任意视图

【例】 显示当前所有端口绑定的配置信息。

```
<H3C>display am user-bind
Following User address bind have been configured:
Mac              IP          Port
000f-e200-5101   10.153.1.1  Ethernet1/0/1
000f-e200-5102   10.153.1.2  Ethernet1/0/2
Unit 1:Total 2 found, 2 listed.
Total: 2 found.
```

以上显示信息表示，设备 Unit 1 当前总共有两条端口绑定的配置：

(1) MAC 地址 000f-e200-5101、IP 地址 10.153.1.1 的用户已经与端口 Ethernet1/0/1 进行了绑定。

(2) MAC 地址 000f-e200-5102、IP 地址 10.153.1.2 的用户已经与端口 Ethernet1/0/2 进行了绑定。

【解决方案】

为解决案例 1，即避免 IP 地址随意配置甚至是恶意盗用 IP 的问题，在接入交换机上实施“MAC+IP+端口”绑定。实验拓扑如图 5.2 所示，接入交换机连接两台用户 PC，设置端口 Ethernet1/0/1 与 PC1 的 MAC 地址和 IP 地址绑定，并验证其效果。

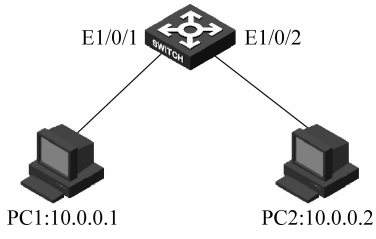

图 5.2 “MAC+IP+端口”绑定实验拓扑

【实验设备】

二层半交换机 1 台，PC 2 台，标准网线 2 根。

说明：本实验二层半交换机选择 H3C S3100-16TP-EI-H3-A。

【实施过程】

步骤 1：按照图 5.2 所示连接好设备，检查设备的软件版本，确保设备软件版本符合要求，配置交换机恢复出厂设置。

(1) 检查设备软件版本。

```
<H3C>display version
```

(2) 在用户模式下擦除设备配置文件，重启设备使系统恢复默认配置。

```
<H3C>reset saved-configuration
<H3C>reboot
```

步骤 2：配置 PC 的 IP 地址，并获取 PC 的 MAC 地址，使用命令行模式下的 ipconfig/

all 命令查看 PC 的 MAC 地址，结果如表 5.2 所示。

表 5.2　PC 的 IP 地址和 MAC 地址

设备名称	IP 地址	MAC 地址	连接交换机端口
PC1	10.0.0.1/24	0015-1785-50AE	Ethernet1/0/1
PC2	10.0.0.2/24	0015-1785-6550	Ethernet1/0/2

步骤 3：配置端口绑定。

(1) 配置 Switch。

```
# 进入系统视图
<H3C>system-view
# 进入 Ethernet1/0/1 端口视图
[H3C] interface ethernet1/0/1
# 将 PC1 的 MAC 地址和 IP 地址绑定到 Ethernet1/0/1 端口
[H3C-ethernet1/0/1] am user-bind mac-addr 0015-1785-50AE ip-addr 10.0.0.1
```

(2) 配置完毕，查看绑定信息：

```
[H3C-ethernet1/0/1]display am user-bind
Following User address bind have been configured:
  Mac              IP         Port
  0015-1785-50ae   10.0.0.1   Ethernet1/0/1
Unit 1:Total 1 found, 1 listed.
Total: 1 found.
```

步骤 4：端口绑定验证。

(1) 在 PC1 上用 ping 命令来测试到 PC2 的互通性，结果显示可达。

(2) 改变 PC1 的 IP 为 10.0.0.3，再次用 ping 命令来测试到 PC2 的互通性。结果显示超时，表示 PC1 改变 IP 地址后不能正常访问网络。

(3) 将 PC1 连接到 Ethernet1/0/2 端口，修改 IP 为 10.0.0.2，并将 PC2 连接到 Ethernet1/0/1 端口，修改 IP 为 10.0.0.1。用 ping 命令来测试 PC1 到 PC2 的互通性。结果显示超时，表示 MAC 地址不匹配 PC 也不能正常访问网络。

【实验总结】

“MAC＋IP＋端口”技术可以帮助网络管理员确保只有正确的 MAC 地址被配置了正确的 IP 并连接到正确的端口才能够接入网络。端口绑定技术可以帮助避免 IP 地址随意配置甚至是恶意盗用 IP 的问题。如果出现引入案例 2 中描述的情况时，如果已经实施了端口绑定，一旦网络管理员发现了感染病毒的 IP 或 MAC 地址信息，通过查找绑定记录，就能快速、准确地定位接入病源主机的交换机端口，并对该端口进行隔离，也可以直接使用 shutdown 命令关闭该端口。

MAC 地址、IP 地址与端口的绑定使用静态方式实现，对管理员来讲，必须手动输入 PC 的 IP 地址和 MAC 地址，工作量较大。