文章编号:1003-5850(2009)09-0063-04

交换机安全技术

Switch Board Security Technology

古乐声 陈 俊 李艳翠

(河南科技学院计科系 河南新乡 453003)

【摘 要】交换机是网络中重要的硬件设备,与网络的整体安全性有着直接的密切的联系。在概述交换机安全技术的基础上给出了一些典型的安全方案,并以一个实例介绍了基本的安全配置。

【关键词】端口,密码,虚拟局域网,访问控制列表

中图分类号:TP393 文献标识码:A

ABSTRACT As an important hardware in the network, the switch board has direct close connections with the whole security of the network. This paper provides some typical security plans on the basis of summing up the switch security technology, and gives an example with the basic security configure.

KEYWORDS port, password, virtual LAN, access control list

随着计算机网络的日益普及,网络的安全性越来越受到人们的关注。交换机是一个网络中主要的硬件设备,安全性与网络的整体安全性有着直接的密切的联系。通过应用一些交换机的安全技术和策略,进行合理的组合搭配,可以最大限度地防范网络上日益泛滥的攻击和侵害,有效的减少网络发生故障的几率,增强网络的安全性,利于网络的维护和管理。

1 安全技术概述

1.1 更新IOS

确保在每一台交换机上安装最新版本的IOS,防止因IOS漏洞引起的安全问题。

1.2 设置"enable secret"密码

enable secret这条命令是设置进入特权模式的密码,等同于enable password,但是不同的是enable password是明文显示的,enable secret是密文显示的,而且当你同时设置了enable password和enable secret时,enable secret生效,enable password无效。

1.3 基于端口的MAC地址绑定

基于网络管理的需要,很多时候需要限制交换机每个端口上接入的机器数量,这就需要用到交换机端口的MAC地址绑定功能。对于交换机的每一个以太网端口,采用MAC地址表(MAC-address-table)的方式对端口进行锁定。只有网络管理员在MAC地址表中指定的网卡的MAC地址才能通过该端口与网络连接,其他的网卡地址不能通过该端口访问网络。

1.4 适当地使用访问控制列表

访问控制列表(ACL)是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪能些数据包可以收、哪能数据包需要拒绝。至于数据包是被接收还是拒绝,可以由类似于源地址、目的地址、端口号等的特定指示条件来决定。

1.4.1 标准IP访问控制列表

一个标准IP访问控制列表匹配IP包中的源地址或源地址中的一部分,可对匹配的包采取拒绝或允许两个操作。编号范围是从1到99的访问控制列表是标准IP访问控制列表。

1.4.2 扩展IP访问控制列表

扩展IP访问控制列表比标准IP访问控制列表具有更多的匹配项,包括协议类型、源地址、目的地址、源端口、目的端口、建立连接的和IP优先级等。编号范围是从100到199的访问控制列表是扩展IP访问控制列表。

1.5 基于端口的VLAN划分

这是最常应用的一种VLAN划分方法,应用也最为广泛、最有效,目前绝大多数VLAN协议的交换机都提供这种VLAN配置方法。这种划分VLAN的方法是根据以太网交换机的交换端口来划分的,是将VLAN交换机上的物理端口和VLAN交换机内部的PVC(永久虚电路)端口分成若干个组,每个组构成一个虚拟网,相当于一个独立的VLAN交换机。

VLAN就是一个单独的广播域,VLAN之间相互隔离,这大大提高了网络的利用率,确保了网络的安全保密性。人们在LAN上经常传送一些保密的、关键性的数据。保密的数据应提供访问控制等安全手段。一个有效和容易实现的方法是将网络分段成几个不同的

* 2009-06-05收到,2009-07-18改回

** 古乐声,男,1973年生,硕士,讲师,研究方向:网络安全技术。

广播组，网络管理员限制了 VLAN 中用户的数量，禁止未经允许而访问 VLAN 中的应用。交换端口可以基于应用类型和访问特权来进行分组，被限制的应用程序和资源一般置于安全性 VLAN 中。

2 典型安全方案介绍

2.1 安全方案之一：层过滤

现在的新型交换机大都可以通过建立规则的方式来实现各种过滤需求。规则设置有两种模式，一种是 MAC 模式，可根据用户需要依据源 MAC 或目的 MAC 有效实现数据的隔离，另一种是 IP 模式，可以通过源 IP、目的 IP、协议、源应用端口及目的应用端口过滤数据封包；建立好的规则必须附加到相应的接收或传送端口上，则当交换机此端口接收或转发数据时，根据过滤规则来过滤封包，决定是转发还是丢弃。

2.2 安全方案之二：802.1X 基于端口的访问控制

为了阻止非法用户对局域网的接入，保障网络的安全性，基于端口的访问控制协议 802.1X 无论在有线 LAN 或 WLAN 中都得到了广泛应用。例如华硕最新的 GigaX2024/2048 等新一代交换机产品不仅仅支持 802.1X 的 Local、RADIUS 验证方式，而且支持 802.1X 的 Dynamic VLAN 的接入，即在 VLAN 和 802.1X 的基础上，持有某用户账号的用户无论在网络内的何处接入，都会超越原有 802.1Q 下基于端口 VLAN 的限制，始终接入与此账号指定的 VLAN 组内，这一功能不仅为网络内的移动用户对资源的应用提供了灵活便利，同时又保障了网络资源应用的安全性；另外，GigaX2024/2048 交换机还支持 802.1X 的 Guest VLAN 功能，即在 802.1X 的应用中，如果端口指定了 Guest VLAN 项，此端口下的接入用户如果认证失败或根本无用户账号的话，会成为 Guest VLAN 组的成员，可以享用此组内的相应网络资源，这一种功能同样可为网络应用的某一些群体开放最低限度的资源，并为整个网络提供了一个最外围的接入安全。

2.3 安全方案之三：流量控制（traffic control）

交换机的流量控制可以预防因为广播数据包、组播数据包及因目的地址错误的单播数据包数据流量过大造成交换机带宽的异常负荷，并可提高系统的整体效能，保持网络安全稳定的运行。

2.4 安全方案之四：SNMP v3 及 SSH

安全网管 SNMP v3 提出全新的体系结构，将各版本的 SNMP 标准集中到一起，进而加强网管安全性。SNMP v3 建议的安全模型是基于用户的安全模型，即 USM。USM 对网管消息进行加密和认证是基于用户进行的，具体地说就是用什么协议和密钥进行加密和认证均由用户名称（userNmae）权威引擎标识符（EngineID）来决定（推荐加密协议 CBCDES，认证协议 HMAC-MD5-96 和 HMAC-SHA-96），通过认证、加密和时限提供数据完整性、数据源认证、数据保密和消息时限服务，从而有效防止非授权用户对管理信息的修改、伪装和窃听。至于通过 Telnet 的远程网络管理，由于 Telnet 服务有一个致命的弱点——以明文的方式传输用户名及口令，所以，很容易被别有用心的人窃取口令，受到攻击，但采用 SSH 进行通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听，便于网管人员进行远程的安全网络管理。

2.5 安全方案之五：Syslog 和 Watchdog

交换机的 Syslog 日志功能可以将系统错误、系统配置、状态变化、状态定期报告、系统退出等用户设定的期望信息传送给日志服务器，网管人员依据这些信息掌握设备的运行状况，及早发现问题，及时进行配置设定和排障，保障网络安全稳定地运行。Watchdog 通过设定一个计时器，如果设定的时间间隔内计时器没有重启，则生成一个内在 CPU 重启指令，使设备重新启动，这一功能可使交换机在紧急故障或意外情况下时可智能自动重启，保障网络的运行。

2.6 安全方案之六：双映像文件

一些新型号的交换机（如 ASUS GigaX2024/2048）具备双映像文件，这一功能保护设备在异常情况下（固件升级失败等）仍然可正常启动运行。文件系统分 major 和 mirror 两部分进行保存，如果一个文件系统损害或中断，另外一个文件系统会将其重写，如果两个文件系统都损害，则设备会清除两个文件系统并重写为出厂时默认设置，确保系统安全启动运行。

3 个案规划及详细配置

某公司网络有 20 台左右计算机，主干部分包括 2 台 Catalyst 2950 交换机（分别命名为：Sw0、Sw1）和一台 Cisco 2620 路由器，整个网络都通过路由器 Cisco 2620 与外部互联网进行连接。所连的用户主要分布于四个部分，即：生产部、财务部、信息中心和人事部，如图 1 所示。要求完成以下功能配置：

① 所有交换机和路由器都使用加密密码，防止非管理人员修改配置；

② 为了公司相应部分网络资源的安全性需要，特别是对于像财务部、人事部这样的敏感部门，其网络上的信息不允许外单位人员随便访问；

③ 从外网不能 PING 公司内的任何一台主机；

④ 不允许财务部的主机上互联网，其他的部门都可以。

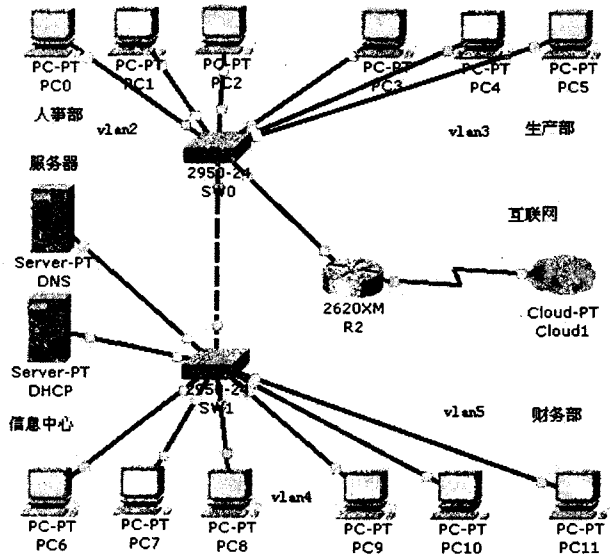

图 1 网络拓扑图

3.1 VLAN 规划

把公司网络划分为生产部、财务部、人事部和信息中心四个主要部分，对应的 VLAN 组名为：Prod、Fina、Huma、Info，如表 1 所示。

表 1 VLAN 规划

Vlan 号	Vlan 名	端口号
2	Huma	Fa0/1—fa0/3
3	Prod	Fa0/4—fa0/6
4	Info	Fa0/1—fa0/3 fa0/7，fa0/8
5	Fina	Fa0/4—fa0/6

3.2 IP 地址规划

如表 2 所示。

表 2 IP 地址规划

部门	PC 号	IP 地址	网关
人事部	PC0—PC2	192.168.1.2—192.168.1.4	192.168.1.1
生产部	PC3—PC5	192.168.2.2—192.168.2.4	192.168.2.1
信息中心	PC6—PC8	192.168.3.2—192.168.3.4	192.168.3.1
	DHCP 服务器	192.168.3.5	
	DNS 服务器	192.168.3.6	
财务部	PC9—PC11	192.168.4.2—192.168.4.4	192.168.4.

3.3 主要的配置

3.3.1 设置加密密码

（以交换机 0 配置为例，交换机 1、路由器 R2 的配置与此类似）：

```
Switch#conf t
Switch(config)#hostname SW0
SW0(config)#enable secret cisco
```

3.3.2 vlan 划分

交换机 0

① 创建 VLAN，并将相应的端口划分入 VLAN，如

```
SW0(vlan)#vlan 2 name huma
SW0(config)#int fa0/1
SW0(config-if)#switchport acc vlan 2
```

② 使用 VTP，并设置为服务器模式

```
SW0(vlan)#vtp domain cisco
SW0(vlan)#vtp password cisco
SW0(vlan)#vtp server
```

③ 设置中继端口

```
SW0(config)#int fa0/24
SW0(config-if)#switchport mode trunk
SW0(config)#int fa0/23
SW0(config-if)#switchport mode trunk
```

交换机 1

① 创建 VLAN，并将相应的端口划分入 VLAN

② 使用 VTP，并设置为客户模式

```
SW1(vlan)#vtp domain cisco
SW1(vlan)#vtp password cisco
SW1(vlan)#vtp client
```

③ 设置中继端口

```
SW1(config)#int fa0/24
SW1(config-if)#switchport mode trunk
```

3.3.3 ALC 配置

① 设置子接口，封装协议

```
R2(config)#int fa0/0
R2(config-if)#no ip add
R2(config-if)#no sh
R2(config)#int fa0/0.1
R2(config-subif)#encapsulation dot1q 2
R2(config-subif)#ip add 192.168.1.1 255.255.255.0
R2(config-subif)#no sh
R2(config-subif)#int fa0/0.2
R2(config-subif)#encapsulation dot1q 3
R2(config-subif)#ip add 192.168.2.1 255.255.255.0
R2(config-subif)#no sh
R2(config-subif)#int fa0/0.3
R2(config-subif)#encapsulation dot1q 4
R2(config-subif)#ip add 192.168.2.1 255.255.255.0
R2(config-subif)#no sh
R2(config-subif)#int fa0/0.4
R2(config-subif)#encapsulation dot1q 5
R2(config-subif)#ip add 192.168.4.1 255.255.255.0
```

（下转第 68 页）

结合 UNCON 模型的形式化描述，TUCON 模型的形式化描述为：

Platform _ Verify（PCRs，ATT（O））∧ Authorization _ check（ATT（S），ATT（O），R）∧ Obligation _ verify（ATT（S），ATT（O），R）∧ Condition _ verify(ATT(S),ATT(O),R)→Object _ Unseal（Object）→ Object _ Access（Object）→ Threshold _ Check(ATT(S)→ATT _ update(ATT(S),ATT(O))。

TUCON 模型的访问流程如图 3 所示。

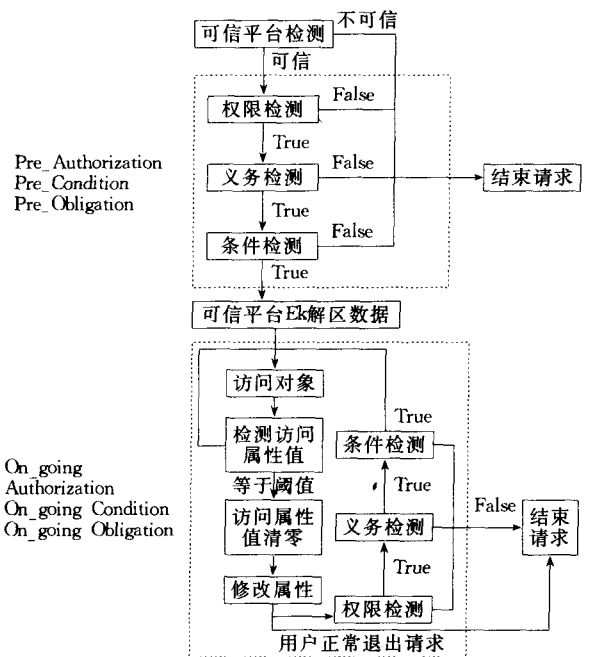

图 2 UCON模型控制流程

3 结束语

安全的数据共享是访问控制中的主要研究内容，本文将可信平台的安全性和 UCON 模型的访问控制结合起来，建立了 TUCON 模型，解决了 UCON 模型存在的问题，实现了数据的安全共享。根据此方案研究数据访问控制的应用是进一步研究的内容。

参 考 文 献

[1] Padayachee K，Eloff J H P，Adapting Usage Control as a Deterrent to Address the Inadequacies of Access Controls[J]. Comput. Secur，doi：10. 1016/j. cose. 2009. 03. 003，2009.

[2] Wang H，Zhang Y C，Cao J L. Access Control Management for Ubiquitous Computing[J]. Future Generation Computer Systems，2008(24)：870-878.

[3] Fu S，Xu C. Coordinated Access Control with Temporal and Spatial Constraints on Mobile Execution in Coalition Environments[J]. Future Generation Computer Systems，2007，23(6)：804-815.

[4] 丁 霞，徐开勇，李立新等. 基于 UCONABC 模型的电子文档安全系统[J]. 计算机工程，2008，34(2)：127-143.

[5] 胡兆玮，于万钧，杨 博. 使用控制授权模型的安全性研究[J]. 计算机应用研究，2008，25(1)：226-229.

[6] 陆建新，杨树堂，陆松年等. 可信计算中一种基于属性的封装存储方案[J]. 信息技术，2008(1)：1-4.

[7] 刘宏伟，高万鹏. 可信计算平台数据维护技术的研究与实现[J]. 信息安全，2006，22(9)：65-67.

（上接第 65 页）

R2(config-subif)#no sh

② 创建访问控制列表，并应用于相应的端口上

R2（config）# access-list 100 deny tcp 192.168.4.0 255.255.255.0 any eq www

R2(config)#access-list 100 permit ip any any

R2(config)#int fa0/0

R2(config-if)#ip access-group 100 out

R2(config)#access-list 101 deny icmp any any

R2(config)#access-list 101 permit ip any any

R2(config)#int s0/0

R2(config-if)#ip access-group 101 in

说明：本案中 2950 没有 ACL 配置功能，使用了 2620 路由器来代替。

4 结 论

交换机是网络中的重要设备，安全性配置对整个网络有着至关重要的意义。设置加密密码是最基本的安全措施；VLAN 技术具有控制网络广播风暴、增强网络安全性、便于网络维护和管理等优点，得到了越来越广泛的应用；随着多层交换机的不断使用，ACL 技术的应用也将越来越普遍。

参 考 文 献

[1] Cisco Systems. 思科网络技术学院教程[M]. 北京：人民邮电出版社，2004.

[2] 陆魁军. 计算机网络工程实践教程[M]. 浙江：浙江大学出版社，2006.

[3] 汪松鹤，汪永益. 网络交换机的安全威胁与防范[J]. 网络安全，2009，28(1)：16-17.

[4] 赵海涛. 交换机安全性研究[J]. 科学技术与工程，2007，7(6)：21-23.

[5] 赵晓峰. 网络骨干节点路由器、交换机安全问题及对策[J]. 网络安全，2006，25(11)：24-26.

[6] 陈广山. IP 层的安全机制研究[J]. 电脑开发与应用，2008，21(9)：52-54.