思科交换机4500系列交换机完整配置手册

目　录

Cisco Catalyst 4500 系列交换机功能应用与安全解决方案

一、Cisco Catalyst 4500 系列交换机概述

1、功能概述

Cisco® Catalyst® 4500 系列交换机(图 1)将无阻塞第二到四层交换与最优控制相集成，有助于为部署关键业务应用的大型企业、中小型企业（SMB）和城域以太网客户提供业务永续性。Cisco Catalyst 4500 系列凭借众多智能服务将控制扩展到网络边缘，其中包括先进的服务质量 (QoS)、可预测性能、高级安全性和全面的管理。它提供带集成永续性的出色控制，将永续性集成到硬件和软件中，缩短了网络停运时间，有助于确保员工的效率、公司利润和客户成功。Cisco Catalyst 4500 系列的模块化架构、介质灵活性和可扩展性减少了重复运营开支，提高了投资回报（ROI），从而在延长部署寿命的同时降低了拥有成本。

图 1 Cisco Catalyst 4500 系列交换机

图 1

2、技术融合

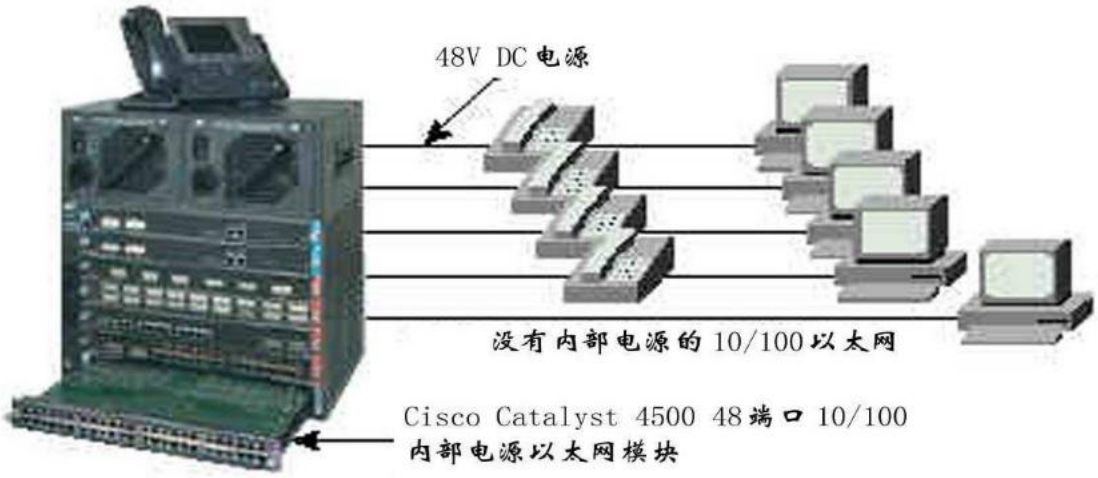
在当今竞争高度激烈的业务环境中，融合网络在帮助机构通过提高生产效率、组织灵活性和降低运营成本，从而获得竞争优势方面起着重要作用。将数据、话音和视频集成在单一（基于 IP 的）网络上，需要一个能区分各种流量类型并根据其独特需求加以管理的交换基础设施。Cisco Catalyst 4500 系列与 Cisco IOS 相结合，提供了一种可实现先进功能和控制的基础设施。

3、最优控制

Cisco Catalyst 4500 系列为所有将集成以解决业务问题的应用提供了网络基础设施。通过集成永续性扩展智能网络服务，可控制所有流量类型并实现最短停运时间。Cisco Catalyst 4500 系列凭借以下特性提供了这种控制能力。

4、集成永续性

通过 Cisco Catalyst 4500 系列的冗余交换管理引擎（不到一秒内实现故障转换）功能(Cisco Catalyst 4507R 和 Catalyst 4510R 交换机)、基于软件的故障容许、冗余风扇和 1+1 电源冗余，最大限度地缩短了网络停运时间。所有 Cisco Catalyst 4500 系列机箱中都具备以太网电源(PoE)，简化了网络设计，并限制了 IP 电话实施中的故障点数目。



5、高级 QoS

集成的基于第二到四层的 QoS 和流量管理功能，在 32000 个 QoS 策略条目的基础上，对关键任务和时间敏感型流量进行了分类和优先排序。Cisco Catalyst 4500 系列可以利用基于主机、网络和应用信息的入口和出口策略控制器机制，对高带宽流量进行整形和速率限制。

6、可预测性能

Cisco Catalyst 4500 系列在硬件中为第二到四层流量提供了高达 102Mpps 的线速转发速率。交换性能与支持的路由或第三层高级服务数量无关。

7、高级安全性能

对荣获专利的思科第二层安全特性的支持，可防止恶意服务器的安全违规，以及可能截获密码及数据的“中间人”攻击。此外，它还支持第二到四层过滤和监督，以防来自恶意网络攻击者的流量进入网络。

8、全面的管理

Cisco Catalyst 4500 系列为所有端口的配置和控制提供了基于 Web 的管理功能，因而可以集中管理重要网络特性，如可用性和响应能力等。

9、可扩展架构

融合通过消除分立的话音、视频和数据基础设施，降低了网络整体拥有成本，简化了管理和维护。Cisco Catalyst 4500 系列的模块化架构具有可扩展性和灵活性，无需多平台部署，最大限度地降低了维护开支。为进一步延长客户网络设备的使用寿命，Cisco Catalyst 4500 系列提供了以下特性：

线卡的向后兼容性

客户可灵活地在已有机箱中将线卡升级到更高速度的接口，不必更换整个机箱，为未来特性提供更大发展空间。

10、延长了增加投资的时间。

Cisco Catalyst 4500 系列架构的设计配备了大量的硬件资源，可支持针对您网络需求的未来特性。您只需进行简单的 Cisco IOS 软件升级，就可获得多种硬件支持的特性，无需全面的机箱升级。

11、Cisco Catalyst 4500 系列产品线

Cisco Catalyst 4500 系列包括四种机箱选择：Cisco Catalyst 4510R (10 插槽)、Catalyst 4507R (7 插槽)、 Catalyst 4506 (6 插槽)和 Catalyst 4503 (3 插槽)。

机箱	引擎插槽	线卡插槽	最高端口数
Catalyst 4503	1	2	116
Catalyst 4506	1	5	242
Catalyst 4507R	2	5	244
Catalyst 4510R	2	8	388

12、设备通用架构

Cisco Catalyst 4500 系列具有一个通用架构，采用了现有 Cisco Catalyst 4000 系列的线卡，可扩展到 384 个 10/100 或 100BASE-FX 快速以太网端口，或 384 个 10/100/1000BASE-T 或 1000BASE-LX 千兆位以太网端口。Cisco Catalyst 4500 系列与现有 Cisco Catalyst 4000 系列线卡和交换管理引擎兼容，延长了它在融合网络中的部署寿命。

13、Cisco Catalyst 4500 系列交换机的特点

Cisco Catalyst 4500 系列为企业 LAN 接入、小型骨干网、第三层分布点和集成化 SMB 及分支机构部署提供了先进的高性能解决方案 。其优势包括：

（1）性能

Cisco Catalyst 4500 系列提供了带宽可随端口的添加而扩展的高级交换解决方案，采用了领先的特定应用集成电路(ASIC) 技术，提供线速第二到三层 10/100 或千兆位交换。第二层交换以全面的线卡兼容性提供了模块化交换管理引擎灵活性，可扩展到 136 Gbps、 102 mpps。第三到四层交换基于思科快速转发，也可扩展到 136 Gbps、 102 mpps。

（2）端口密度

Cisco Catalyst 4500 系列可达到一个机箱中 384 个铜或光纤以太网端口的网络组件连接要求。Catalyst 4500 系列支持业界最高密度的 10/100/1000 自动检测，自动协商从网络边缘直接到桌面计算机的千兆位以太网连接。可选万兆位以太网上行链路端口有助于实施高密度千兆位以太网到桌面部署和交换机间应用。

（3）交换管理引擎冗余性

Cisco Catalyst 4507R 和 Catalyst 4510R 交换机支持 1+1 交换管理引擎冗余，实现集成永续性。冗余交换管理引擎可缩短网络停运时间，实现业务连续性和提高员工效率。在状态化切换（SSO）的支持下，第二个交换管理引擎作为备用，可在主交换管理引擎发生故障时，在不到一秒的时间内接管一切。此外，也支持 Cisco IOS 软件中的不间断转发（NSF）感知特性，可与支持 NSF 的设备互操作，在因交换管理引擎切换而更新路由信息时，可继续转发分组。

A、 Supervisor Engine II-Plus——以入门级价格提供增强的第二层特性，适用于小型第二层配线间以及简单的第三层 QoS 和安全性。

B、 Supervisor Engine II-Plus-TS ——在 Supervisor Engine II-Plus 的基础上增加了 20 个线速千兆以太网（GE）端口（12 个千兆以太网 PoE 铜线端口、8 个千兆以太网 SFP 光端口）。只在 Catalyst 4503 机箱中支持。

C、 Supervisor Engine IV ——中等配线间和第三层网络，提供增强的安全特性和第三层路由（EIGRP，OSPF，IS-IS 协议，BGP）。

D、 Supervisor Engine V ——高级性能和先进特性，在 Catalyst 4510R 机箱中支持 242 个端口。

E、 Supervisor Engine V-10GE ——在 Supervisor Engine V 的基础上添

加了两条万兆以太网上行链路和 NetFlow。在 Catalyst 4510R 机箱中最多支持 384 个端口。

（4）以太网电源 (PoE)

Cisco Catalyst 4500 系列支持 802.3af 标准和思科预标准电源，以便在 10/100 或 10/100/1000 端口上提供 PoE，使客户可支持电话、无线基站、摄像机和其他设备。此外， PoE 允许企业在单一电源系统上隔离关键设备—所以整个系统可由备用的不间断电源（UPS）支持。所有新 Cisco Catalyst PoE 线卡可同时在每个端口上支持 15.4 W。这些卡与所有 Cisco Catalyst 4500 系列机箱和交换管理引擎兼容。

（5）高级安全特性

Cisco Catalyst 4500 系列上支持 802.1x、访问控制列表(ACL)、Secure Shell(SSH)协议、动态 ARP 检测(DAI)、源 IP 防护和专用虚拟 LAN(PVLAN)等安全特性，可增强网络中的控制能力和灵活性。通过有选择地或全部实施上述特性，网络管理员可防止对于服务器或应用的未授权访问，允许不同的人能以不同的许可权来使用同一 PC。

（6）Cisco IOS 软件网络服务

Cisco Catalyst 4500 系列交换机提供能增强公司网络的成熟的第二到三层特性。这些特性可满足大中型企业的先进的联网要求，因为它们已根据多年来客户的反馈意见进行了改进。

（7）投资保护

Cisco Catalyst 4500 系列灵活的模块化架构为 LAN 接入层或分支机构网络提供了经济有效的接口升级。已部署了采用较早交换管理引擎版本的 Cisco Catalyst 4503 和 Catalyst 4506 交换机、现在需要更高性能和增强特性的客户，可方便地升级到 Cisco Catalyst 4500 系列 Supervisor Engine II-Plus、Catalyst 4500 系列 Supervisor Engine V-10GE、Catalyst 4500 Supervisor Engine IV 或 Catalyst 4500 Supervisor Engine V。Catalyst 4500 系列各成员间的备件可兼容，Catalyst 4003 和 Catalyst 4006 机箱提供了电源和交换线卡通用性，降低了整体部署、移植和支持成本。

（8）功能透明的线卡

Cisco Catalyst 4500 系列系统只需添加一个新的交换管理引擎，如 Cisco Catalyst 4500 系列 supervisor engines II-Plus、IV、V 或 V-10GE，即可轻松地将所有系统端口升级到更高层的交换功能。无需更换现有线卡和布线，就可以实现更高层的功能增强。

（a）交换管理引擎

A、 Supervisor Engine II-Plus——以入门级价格提供增强的第二层特性，适用于小型第二层配线间以及简单的第三层 QoS 和安全性。

B、Supervisor Engine II-Plus-TS ——在 Supervisor Engine II-Plus 的基
础上增加了 20 个线速千兆以太网（GE）端口（12 个千兆以太网 PoE 铜线端口、8 个千兆以太网 SFP 光端口）。只在 Catalyst 4503 机箱中支持。

C、Supervisor Engine IV ——中等配线间和第三层网络，提供增强的安全特性和第三层路由（EIGRP，OSPF，IS-IS 协议，BGP）。

D、Supervisor Engine V ——高级性能和先进特性，在 Catalyst 4510R

机箱中支持 242 个端口。

E、Supervisor Engine V-10GE ——在 Supervisor Engine V 的基础上添加了两条万兆以太网上行链路和 NetFlow。在 Catalyst 4510R 机箱中最多支持 384 个端口。

（b）线卡

A、百兆以太网铜线——百兆以太网线卡包括 24 端口和 48 端口连接类型，都带可任选 PoE。

B、百兆以太网光纤——支持多模光纤和单模光纤，以及 FX、LX 和 BX 收发器。

C、千兆以太网铜线——提供 24 端口或 48 端口，带或不带 PoE。

D、千兆以太网光纤——千兆以太网光纤卡提供高性能千兆以太网上行链路和服务器群连接。提供多种端口数和光接口类型（千兆位接口转换器[GBIC]和 SFP 光接口

（9）到桌面的千兆位连接

Cisco Catalyst 4500 系列已提供众多的 1000-Mbps 桌面和服务器交换解决方案。其千兆位解决方案的范围可通过用于 Catalyst 4500 系列的 48 和 24 端口三速自动检测和自动协商 10/100/1000BASE-T 线卡，方便地扩展到桌面。采用自动检测技术的三速 48 和 24 端口模块，无需更换线卡即可将快速以太网桌面在将来移植到千兆位以太网，提供了 LAN 投资保护。Catalyst 4500 系列 Supervisor Engine V-10GE 提供了两条为 10/100/1000BASE-T 到桌面汇聚而优化的线速万兆位以太网上行链路。

（10）基于硬件的组播

协议独立型组播(PIM)、密集和疏松模式、互联网小组管理协议(IGMP)和思科群组管理协议支持基于标准和经思科技术增强的高效多媒体联网，且对性能无影响。

（11）Cisco NetFlow 服务

用于 Supervisor Engine IV 和 V 的 Cisco NetFlow 服务卡支持硬件中的统计数据获取，用于基于流量和基于 VLAN 的统计监控。

针对关键任务应用的带宽保护

当部署 Cisco Catalyst 4500 系列 Supervisor Engines II-Plus、IV、V 或 V-10GE 时，在实施 QoS 或安全特性时不会降低转发性能；Catalyst 4500 系列平台继续以全线速转发分组。

（12）到桌面的光纤连接

Cisco Catalyst 4500 系列 24 和 48 端口 100BASE-FX 线卡提供了光纤电缆设施的安全性和永续性，使之极适于有距离限制、入侵漏洞或 RF 干扰的网络。处理保密信息或提供电子商务的企业客户或政府机构将受益于这些线卡的安全优势。

14、Cisco Catalyst 4500 系列的主要特性

特性	功能和说明	优势
箱		
模块化 3、6、7 和 10 插槽 Cisco Catalyst 4500 系列机箱	支持交换管理引擎(Cisco Catalyst 4507R 和 Catalyst 4510R 上可支持 2 个)，带集成 PoE 的电源。	提供了具备高级集成永续性的通用架构，可以根据园区内联网的要求标准化。

状态化切换(SSO)和不间断转发(NSF)感知	提供双交换管理引擎，故障转换可在不到一秒内完成。保持第二层会话。路由事件期间，继续第三层转发。	大幅度缩短了网络停机时间，有助于确保业务的持续性和提高生产效率。
灵活的交换模块—基于标准、自动检测和自动协商	提供众多接口选择：10/100Mbps 以太网和10/100/1000、1000Mbps 千兆位以太网或 10000Mbps 万兆位以太网。	支持IP园区的LAN带宽扩展，可在扩展网络时提供方便的移植。
64Gbps 容量背板(Cisco Catalyst 4503)	每秒转发超过 4800 万 64 字节以太网分组。	可以满足一个系统所有接口以线速全面运行的吞吐量要求。
100Gbps 容量背板(Cisco Catalyst 4506 和 Catalyst 4507R)	为线速、无阻塞 75 mpps 转发提供了充足的容量。	可以满足一个系统所有接口以线速全面运行的最糟糕情况下的吞吐量要求（无阻塞矩阵要求配备 Supervisor Engine II-Plus、IV 或 V 或 V-10GE)。
136Gbps 容量背板(Cisco Catalyst 4510R)	为线速、无阻塞 102 mpps 转发提供了充足的容量，支持多达 8 个接口模块。	无阻塞、高密度应用。
集成 Cisco IOS 软件增强了第三层交换(Cisco Catalyst 4000/4500 supervisor engines IV 和 V)	以千兆位速度提供基于 ASIC 的 IP 路由。	提供了网络流量的第三层子网控制功能；成熟的路由协议。
多层 QoS	为第二层 CoS 和第三层 ToS、流量整形、共享、监督和带动态缓冲限制（DBL）的拥塞避免机制，提供了 QoS 功能。在每个端口上提供了多个队列。	为网络流量优先排序提供了集中控制功能；可方便地创建和管理策略，以保护关键任务应用。
入口和出口监督(Cisco Catalyst supervisor engines II-Plus、IIPlus-TS、IV、V 和 V-10GE)	在每个端口基础上，在入口识别分组，在出口重新分类和重新标记分组。	根据用户定义的流量分类方法，提供了精确的流量控制功能，确保了 QoS 策略的实施。
集成 PoE	为连接到支持 PoE 的 Cisco Catalyst 4500 系列交换机端口的设备提供电源。设备包括 IP 电话、接入点、摄像机和其	为桌面提供了单一线路；无需办公间不间断电源（UPS）。

	他符合思科或 IEEE 802.3af 标准的设施。	
全面的安全性		
802.1x，用于基于身份的网络服务	使用经过思科增强的 802.1x 协议，无论用户位于何处或使用什么设备，网络都可根据用户登陆信息来授予许可权。	允许不同的人员使用相同 PC，但拥有不同功能，以便用户无论采用何种方式登陆网络，都只能获得他们指定的权利—防止了未授权访问。
ACL	仅限用户访问网络的指定区域，防止对于所有其他应用和信息的未授权访问。	防止针对服务器和应用的未授权访问；只允许指定用户访问特定服务器。
专用 VLAN	防止用户看到其他人在同一交换机上生成的流量。	有助于确保同一交换机上用户的保密性。
受密码保护的管理界面	需密码来通过 Telnet 或 SSH 进行本地或远程访问。	提供针对未授权配置修改的保护。

15、Cisco Catalyst 4500 系列交换机的优点

（1） 安全、强大——通过冗余组件提供高可靠性

（2）服务中升级——热插拔和删除组件

（3）千兆以太网的价格——比可堆叠设备更为经济有效（大于 48 个端口）

（4）自适应性——不需要大规模升级就能提供万兆以太网上行链路

（5）极高的安全性——利用 Cisco Catalyst 集成式安全特性，能够提供思科最全面的局域网接入保护

（6）战略性思科平台——已安装了 400,000 多个机箱

（7）集中式体系结构——简洁、扩展能力强、性能高

（8）支持 IP 语音

（9）投资保护

（10）是目前部署最广泛的模块化交换机

16、Cisco Catalyst 4500 系列的应用

（1）采用以太网骨干的多层交换企业网络

当前的领先网络设计在 LAN 中使用了第二层和第三层服务的结合(Cisco Catalyst 4500 系列)，在分布层和核心网络层使用了第三层路由(Catalyst 4500 或Catalyst 6500 系列)。Catalyst 4500 系列通过Catalyst 4500 系列Supervisor Engine IV、V 或 V-10GE 系列，在硬件中支持纯 IP 路由(在软件中支持互联网分组交换[IPX]协议和 AppleTalk)，可部署在企业网络中的低密度分布点。

分布层 Cisco Catalyst 4500 系列交换机使用思科快速转发路由引擎，能扩展到 136 Gbps、102 mpps (在 Catalyst 4500 系列 Supervisor Engine V-10GE 上)。这有助于在硬件中实现数百万分组/秒的第三层交换吞吐率，且不会影响报头前缀长度。

（2）中型企业和企业分支机构应用

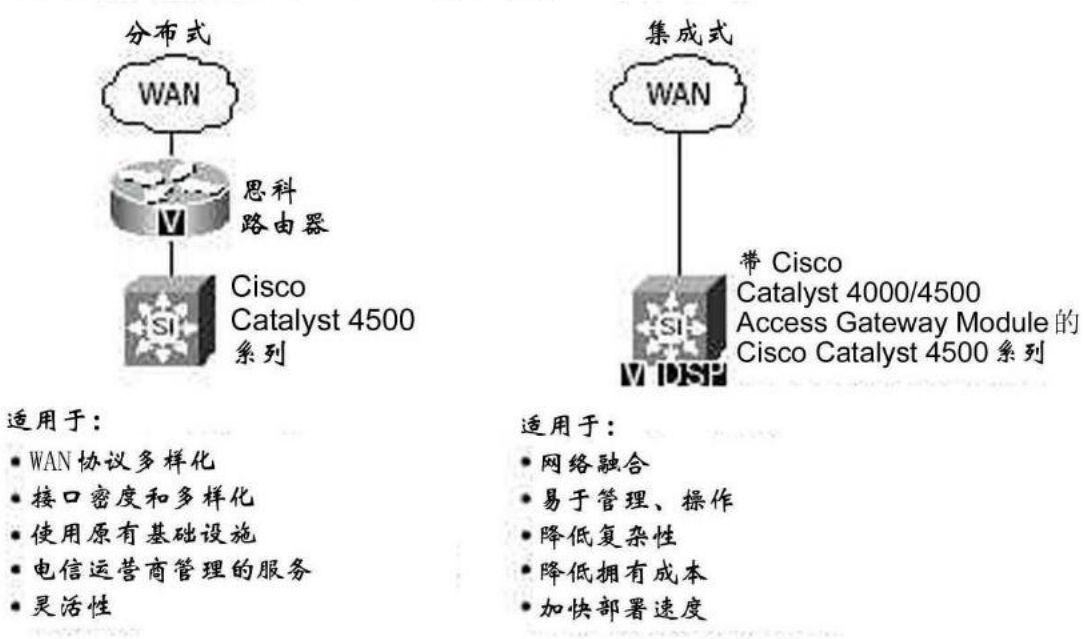
思科系统公司现推出了 Cisco Catalyst 4500 Supervisor IV、V 和 V-10GE，提

供了一种中型企业设计选择，满足了重视价值、正寻找一个灵活、可扩展 LAN 解决方案的客户的需求。这些交换管理引擎专门针对中型企业或教育界客户的 LAN 接入而进行了优化，提供了当前和未来用以管理网络应用的性能和特性。它们提供无阻塞第二到四层服务，来支持适用于数据、话音和视频融合网络的、永续、智能的多层交换解决方案。

（3）中小型企业和分支机构应用

Cisco Catalyst 4500 系列提供了一个理想的分支机构解决方案，能满足各种运营机构以及小型企业应用的需要。Cisco Catalyst 4500 Supervisor Engine IV 添加了增强第三层交换功能和千兆位线速性能，可部署在分支机构骨干网络之中。Cisco IOS 软件在其他交换机和 WAN 路由器之间提供了稳定的网络连接。

下图为分支机构设计的 LAN/WAN 体系结构



二、Cisco Catalyst 4500 系列交换机的解决方案

1、DHCP 的解决方案：

（1）不用交换机的 DHCP 功能而是利用 PC 的 DHCP 功能

1.1.在交换机上配置 DHCP 服务器：

使用命令：ip dhcp-server 192.168.0.69

1.2.在交换机中为每个 VLAN 设置同样的 DHCP 服务器的 IP 地址：

```
Catalyst4507(Config)#interface Vlan11
Catalyst4507(Config-vlan)#ip address 192.168.1.254 255.255.255.0
Catalyst4507(Config-vlan)#ip helper-address 192.168.0.69
Catalyst4507(Config)# interface Vlan12
Catalyst4507(Config-vlan)#ip address 192.168.2.254 255.255.255.0
Catalyst4507(Config-vlan)# ip helper-address 192.168.0.69
```

1.3.在 DHCP 服务器上设置网络地址分别为 192.168.1.0、192.168.2.0 的作用域，并将这些作用域的“路由器“选项设置为对应 VLAN 的接口 IP 地址。

1.4、在 DHCP 服务器上设置各作用域的主 DNS 和辅助 DNS

（2） 利用三层交换机自带的 DHCP 功能实现多 VLAN 的 IP 地址自动分配

配置说明：
2.1.同时为多个 VLAN 的客户机分配地址
2.2.VLAN 内有部分地址采用手工分配的方式
2.3.为客户指定网关、Wins 服务器等
2.4.VLAN 2 的地址租用有效期限为 1 天，其它为 3 天
2.5.按 MAC 地址为特定用户分配指定的 IP 地址
三层交换机上最终配置如下：
ip dhcp excluded-address 10.1.1.1 10.1.1.19 //不用于动态地址分配的地址
ip dhcp excluded-address 10.1.1.240 10.1.1.254
ip dhcp excluded-address 10.1.2.1 10.1.2.19
ip dhcp pool global //global 是 pool name， 由用户指定
network 10.1.0.0 255.255.0.0 //动态分配的地址段
domain-name client.com //为客户机配置域后缀
dns-server 10.1.1.1 10.1.1.2 // 为客户机配置 dns 服务器
netbios-name-server 10.1.1.5 10.1.1.6 //为客户机配置 wins 服务器
netbios-node-type h-node //为客户机配置节点模式（影响名称解释的顺利，如 h-node=先通过 wins 服务器解释...）
lease 3 //地址租用期限：3 天
ip dhcp pool vlan1 //本 pool 是 global 的子 pool，将从 global pool 继承 domain-name 等
network 10.1.1.0 255.255.255.0
option default-router 10.1.1.100 10.1.1.101 //为客户机配置默认网关
ip dhcp pool vlan2 //为另一 VLAN 配置的地址池名称
pool network 10.1.2.0 255.255.255.0
default-router 10.1.2.100 10.1.2.101
lease 1
ip dhcp pool vlan1_chengyong //总是为 MAC 地址为...的机器分配...地址
host 10.1.1.21 255.255.255.0 client-identifier 010050.bade.6384
//client-identifier=01 加上客户机网卡地址
ip dhcp pool vlan1_tom host 10.1.1.50 255.255.255.0 client-identifier 010010.3ab1.eac8
（3）三层交换机上实现跨 VLAN 的 DHCP 配置（路由器+三层交换机）
三层交换机交换机上的配置：
vlan database(划分 VLAN)
vlan 2
vlan 3
interface FastEthernet0/2（将端口 f0/2 划分入 vlan2）
switchport access vlan 2
switchport mode access
no ip address
interface FastEthernet0/3（将端口 f0/3 划分入 vlan3）
switchport access vlan 3
switchport mode access
no ip address

```
    ......
interface Vlan1
ip address 192.168.1.2 255.255.255.0
ip helper-address 192.168.1.1 (将 DHCP 请求的广播数据包转化为单播请    求
路由器才会响应)

interface Vlan2
ip address 192.168.2.1 255.255.255.0
ip helper-address 192.168.1.1
!
interface Vlan3
ip address 192.168.3.1 255.255.255.0
ip helper-address 192.168.1.1
```

路由器上的配置:

```
ip dhcp pool tyl-01（配置第一个 VLAN 的地址池）
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1 (配置 PC 网关)
dns-server 61.134.1.4（配置 DNS 服务器）

ip dhcp pool tyl-02（配置第二个 VLAN 的地址池）
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 61.134.1.4

ip dhcp pool tyl-03（配置第三个 VLAN 的地址池）
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
dns-server 61.134.1.4
ip route 192.168.2.0 255.255.255.0 192.168.1.2（配置静态路由）
ip route 192.168.3.0 255.255.255.0 192.168.1.2
ip dhcp excluded-address 192.168.1.1 192.168.1.2 (将路由器 F0/0 和 C4507R
VLAN1 的 IP 地址排除)
ip dhcp excluded-address 192.168.2.1 (C4507R VLAN1 的 IP 地址排除)
ip dhcp excluded-address 192.168.3.1 (C4507R VLAN1 的 IP 地址排除)
```

（4）相关的 DHCP 调试命令：

```
1、 no service dhcp //停止 DHCP 服务[默认为启用 DHCP 服务]
2、sh ip dhcp binding //显示地址分配情况
3、 show ip dhcp conflict //显示地址冲突情况
4、debug ip dhcp server {events | packets | linkage} //观察 DHCP 服务器
工作情况
```

（5）DHCP 故障排错

如果 DHCP 客户机分配不到 IP 地址，常见的原因有两个。第一种情况是没有把连接客户机的端口设置为

Portfast 方式。linux 客户机开机后检查网卡连接正常，Link 是 UP 的，就开始发送 DHCPDISCOVER 请求，而此时

交换机端口正在经历生成树计算，一般需要 30-50 秒才能进入转发状态。linux 客户机没有收到 DHCP SERVER 的

响应就会给网卡设置一个 169.169.X.X 的 IP 地址。解决的方法是把交换机端口设置为 Portfast 方式：

```
Catalyst4507R(config)#interface mod_num/port_num
 Catalyst4507R(config-if)#spanning-tree portfast
```

2、ARP 防护的解决方案

（1）基于端口的 MAC 地址绑定

1.1 利用交换机的 Port-Security 功能实现

以下是一个配置实例：

```
switch#config t
switch (config) #int f0/1
switch (config-if) #switchport mode access
//设置交换机的端口模式为 access 模式，注意缺省是 dynamic
//dynamic 模式下是不能配置 port-securty 命令的
switch (config-if) #switchport port-security
//打开 port-security 功能
switch (config-if) #switchport port-security mac-address xxxx.xxxx.xxxx
//xxxx.xxxx.xxxx 就是你要关联的 mac 地址
switch (config-if) #switchport port-security maximum 1
//其实缺省就是 1
switch (config-if) #switchport port-security violation shutdown
//如果违反规则，就 shutdown 端口
//这个时候你 show int f0/1 的时候就会看到接口是 err-disable 的
```

附：

```
switchport port-security 命令语法
Switch (config-if) #switchport port-security ?
aging         Port-security aging commands
mac-address   Secure mac address  //设置安全 MAC 地址
maximum       Max secure addresses
//设置最大的安全 MAC 地址的数量，缺省是 1
violation     Security violation mode
//设置违反端口安全规则后的工作，缺省是 shutdown
```

（2）基于 MAC 地址的扩展访问列表

```
Switch(config)Mac access-list extended MAC10
#定义一个 MAC 地址访问控制列表并且命名该列表名为 MAC10
Switch(config)permit host 0009.6bc4.d4bf any
#定义 MAC 地址为 0009.6bc4.d4bf 的主机可以访问任意主机
Switch(config)permit any host 0009.6bc4.d4bf
#定义所有主机可以访问 MAC 地址为 0009.6bc4.d4bf 的主机
Switch(config-if )interface Fa0/20
```

#进入配置具体端口的模式
Switch(config-if)mac access-group MAC10 in
＃在该端口上应用名为 MAC10 的访问列表（即前面我们定义的访问策略）
Switch(config)no mac access-list extended MAC10
＃清除名为 MAC10 的访问列表
（3）基于 IP 地址的 MAC 地址绑定
只能将应用 1 或 2 与基于 IP 的访问控制列表组合来使用才能达到 IP-MAC 绑定功能。
Switch(config)Mac access-list extended MAC10
＃定义一个 MAC 地址访问控制列表并且命名该列表名为 MAC10
Switch(config)permit host 0009.6bc4.d4bf any
＃定义 MAC 地址为 0009.6bc4.d4bf 的主机可以访问任意主机
Switch(config)permit any host 0009.6bc4.d4bf
＃定义所有主机可以访问 MAC 地址为 0009.6bc4.d4bf 的主机
Switch(config)Ip access-list extended IP10
＃定义一个 IP 地址访问控制列表并且命名该列表名为 IP10
Switch(config)Permit 192.168.0.1 0.0.0.0 any
＃定义 IP 地址为 192.168.0.1 的主机可以访问任意主机
Permit any 192.168.0.1 0.0.0.0
＃定义所有主机可以访问 IP 地址为 192.168.0.1 的主机
Switch(config-if)interface Fa0/20
#进入配置具体端口的模式
Switch(config-if)mac access-group MAC10 in
＃在该端口上应用名为 MAC10 的访问列表（即前面我们定义的访问策略）
Switch(config-if)Ip access-group IP10 in
＃在该端口上应用名为 IP10 的访问列表（即前面我们定义的访问策略）
Switch(config)no mac access-list extended MAC10
＃清除名为 MAC10 的访问列表
Switch(config)no Ip access-group IP10 in
＃清除名为 IP10 的访问列表
（4）cisco 的 DAI 技术
通过 DHCP snooping 和 ARP inspection 技术对 ARP 的防护
4.1、arp 防护的原理
因为经常看到网上有看到求助 ARP 病毒防范办法，其实 ARP 欺骗原理简单，利用的是 ARP 协议的一个“缺陷”，通过 ARP 来达到欺骗主机上面的网关的 ARP 表项。其实 ARP 当时设计出来是为了 2 个作用的：
(a)，IP 地址冲突检测
(b)，ARP 条目自动更新，更新网关。
ARP 欺骗就是利用这里面的第二条，攻击的主机发送一个 ARP 更新，条目的 ip 地址是网关，但是 MAC 地址一项，却不是网关，当其他主机接受到，会根据 ARP 协议的规则，越新的越可靠的原则，达到欺骗的目的。
虽然 ARP 不是 tcp/ip 协议簇中的一员，但是鉴于以太网的大行其道，所以放弃动态 ARP 协议，使用手动方式的来来做 ARP 映射，好像不大现实（个别情况除外）。

4.2、深入 ARP 协议特征

其实这里面使用到了 2 个技术：DHCP snooping 和 ARP inspection

(a)、DHCP snooping

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

当交换机开启了 DHCP-Snooping 后，会对 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。另外，DHCP-Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址。

(i).作用：

DHCP-snooping 的主要作用就是隔绝非法的 DHCP server，通过配置非信任端口。建立和维护一张 DHCP-snooping 的绑定表，这张表一是通过 DHCP ack 包中的 ip 和 MAC 地址生成的，二是可以手工指定。这张表是后续 DAI(dynamic ARP inspect)和 IP Source Guard 基础。这两种类似的技术，是通过这张表来判定 ip 或者 MAC 地址是否合法，来限制用户连接到网络的。

(ii).配置:

```
switch (config) #ip DHCP snooping
switch (config) #ip DHCP snooping vlan 10
switch (config-if) #ip DHCP snooping limit rate 10
/*DHCP 包的转发速率，超过就接口就 shutdown，默认不限制
switch (config-if) #ip DHCP snooping trust
/*这样这个端口就变成了信任端口，信任端口可以正常接收并转发 DHCP Offer 报文，不记录 ip 和 MAC 地址的绑定，默认是非信任端口
switch#ip DHCP snooping binding 0009.3452.3ea4 vlan 7 192.168.10.5 interface gi1/0/10
/*这样可以静态 ip 和 MAC 一个绑定
switch (config) #ip DHCP snooping database tftp:// 10.1.1.1/DHCP_table
/*因为掉电后，这张绑定表就消失了，所以要选择一个保存的地方，ftp，tftp，flash 皆可。本例中的 DHCP_table 是文件名，而不是文件夹，同时文件名要手工创建一个
```

(b). ARP inspection

(i).介绍

DAI 是以 DHCP-snooping 的绑定表为基础来检查 MAC 地址和 ip 地址的合法性。

(ii).配置

```
switch (config) #ip DHCP snooping vlan 7
switch (config) #ip DHCP snooping information option
/*默认
switch (config) #ip DHCP snooping
switch (config) #ip ARP inspection vlan 7
/* 定义对哪些 VLAN 进行 ARP 报文检测
```

switch（config）#ip ARP inspection validate src-MAC dst-MAC ip
/*对源，目 MAC 和 ip 地址进行检查
switch（config-if）#ip DHCP snooping limit rate 10
switch（config-if）#ip ARP inspection limit rate 15
/* 定义接口每秒 ARP 报文数量
switch（config-if）#ip ARP inspection trust
/*信任的接口不检查 ARP 报文，默认是检测
4.3、交换机会错认受 DoS 攻击

对于前面 DHCP-snooping 的绑定表中关于端口部分，是不做检测的；同时对于已存在于绑定表中的 MAC 和 ip 对于关系的主机，不管是 DHCP 获得，还是静态指定，只要符合这个表就可以了。如果表中没有就阻塞相应流量。

在开始应用 Dynamic ARP Inspection 时，交换机会记录大量的数据包，当端口通过的数据包过多时，交换机会认为遭受 DoS 攻击，从而将端口自动 errdisable，造成通信中断。为了解决这个问题，我们需要加入命令 errdisable recovery cause ARP-inspection

在 Cisco 网络环境下，boot request 在经过了启用 DHCP SNOOPING 特性的设备上时，会在 DHCP 数据包中插入 option 82 的选项（具体见 RFC3046）

这个时候，boot request 中数据包中的 gateway ip address:为全 0，所以一旦 DHCP relay 设备检测到这样的数据包，就会丢弃。

如果 DHCP 服务器使用了中继服务，那需要在网关交换机上键入如下命令:
方法一：
inter vlan7
ip DHCP relay information trusted
方法二：
switch（config）# ip DHCP relay information trust-all
4.4.防止非法的 ARP 请求

虽然 DHCP snooping 是用来防止非法的 DHCP server 接入的，但是它一个重要作用是一旦客户端获得一个合法的 DHCP offer。启用 DHCP snooping 设备会在相应的接口下面记录所获得 IP 地址和客户端的 MAC 地址。这个是后面另外一个技术 ARP inspection 检测的一个依据。ARP inspection 是用来检测 ARP 请求的，防止非法的 ARP 请求。

认为是否合法的标准的是前面 DHCP snooping 时建立的那张表。因为那种表是 DHCP server 正常回应时建立起来的，里面包括是正确的 ARP 信息。如果这个时候有 ARP 攻击信息，利用 ARP inspection 技术就可以拦截到这个非法的 ARP 数据包。

3、vlan 技术的解决方案

（1）、虚拟局域网络(Virtual LANs)简介

所谓「虚拟网络」(Virtual LAN, 简称VLAN) 就是「逻辑网络」 (Logical LAN)，是指利用特定的技术将实际上并不一定连结在一起的工作站以逻辑的方式连结起来，使得这些工作站彼此之间通讯的行为和将它们实际连结在一起时一样。所谓「虚拟桥接网络」(Virtual Bridged LAN, 简称VBLAN) 就是指在桥接网络上提供虚拟网络的服务。

（2）虚拟网络的特性如下：

（a）工作站之群组具弹性。工作站可以动态的加入或退出某一个虚拟网络。也

就是说，虚拟网络的组成成员可以机动调整，增加了组网的弹性。
（b）虚拟网络具防火墙效果。
这是指属于不同虚拟网络间的工作站彼此之间不可以直接通讯。如有必要通讯，必须通过路由器来转送。由于虚拟网络是一个独立的广播网域，因此其运作的模式与传统的IP 子网络（IP Subnet）相同。IP 子网络也是一个独立的广播网域，而且IP 子网络彼此之间不能直接通讯，必须透过路由器的转送。路由器事实上就是扮演防火墙的角色。
（3）发展虚拟网络技术的主要动能有四个:
a、支持虚拟组织的需求,
b、简化网络管理的程序,
c、提升网络资源的使用效率,
d、加强网络安全
（4）vlan划分的6中策略：
4.1、 基于端口划分的VLAN
这种划分VLAN的方法是根据以太网交换机的端口来划分,这些属于同一VLAN的端口可以不连续，如何配置，由管理员决定，如果有多个交换机，例如，可以指定交换机 1 的1~6端口和交换机 2 的1~4端口为同一VLAN，即同一VLAN可以跨越数个以太网交换机，根据端口划分是目前定义VLAN的最广泛的方法，IEEE 802.1Q规定了依据以太网交换机的端口来划分VLAN的国际标准。
这种划分的方法的优点是定义VLAN成员时非常简单，只要将所有的端口都指定义一下就可以了。它的缺点是如果VLAN A的用户离开了原来的端口，到了一个新的交换机的某个端口，那么就必须重新定义。
4.2、基于MAC地址划分VLAN
这种划分VLAN的方法是根据每个主机的MAC地址来划分，即对每个MAC地址的主机都配置他属于哪个组。这种划分VLAN的方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN不用重新配置，所以，可以认为这种根据MAC地址的划分方法是基于用户的VLAN，这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个VLAN组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样，VLAN就必须不停的配置。
4.3、基于网络层划分VLAN
这种划分VLAN的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的，虽然这种划分方法是根据网络地址，比如IP地址，但它不是路由，与网络层的路由毫无关系。它虽然查看每个数据包的IP地址，但由于不是路由，所以，没有RIP，OSPF等路由协议，而是根据生成树算法进行桥交换，
这种方法的优点是用户的物理位置改变了，不需要重新配置所属的VLAN，而且可以根据协议类型来划分VLAN，这对网络管理者来说很重要，还有，这种方法不需要附加的帧标签来识别VLAN，这样可以减少网络的通信量。
这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法)，一般的交换机芯片都可以自动检查网络上数据包的以太网祯头，但要让芯片能检查IP帧头，需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。
4.4、根据IP组播划分VLAN

IP 组播实际上也是一种VLAN的定义，即认为一个组播组就是一个VLAN，这种划分的方法将VLAN扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要是效率不高。

4.5. 按策略划分的 VLAN

基于策略组成的 VLAN 能实现多种分配方法，包括 VLAN 交换机端口、MAC 地址、IP 地址、 网络层协议等。网络管理人员可根据自己的管理模式和本单位的需求来决定选择哪种类型 的 VLAN 。

4.6. 按用户定义、非用户授权划分的 VLAN

基于用户定义、非用户授权来划分 VLAN，是指为了适应特别的 VLAN 网络，根据具体的 网络用户的特别要求来定义和设计 VLAN，而且可以让非 VLAN 群体用户访问 VLAN，但是需要 提供用户密码，在得到 VLAN 管理的认证后才可以加入一个 VLAN。

(5)使用 VLAN 具有以下优点：

5. 1、控制广播风暴

一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。

5. 2、提高网络整体安全性

通过路由访问列表和 MAC 地址分配等 VLAN 划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同 VLAN，从而提高交换式网络的整体性能和安全性。

5.3、网络管理简单、直观

（6）Catalyst 4500系列交换机虚拟子网vlan的配置：

1).Catalyst 4500交换机上VLAN及VTP的配置 经超级终端进入控制台

a). 设置VLAN管理域 进入"SET VTP AND・・・・ ",选"VTP ADMINISTRATION CONFIGURATION" 设置VALN管理域名"GIETNET"; VTP方式为"SERVER"。

b). 设置VLAN及TRUNK： 将所有子网的交换机、HUB上连至Catalyst 3200的10MB或100MB口，并按上述原则分配VLAN，将这些端口进行虚网划分如下：

本项设置是从控制台的CONFIGURATION选定"LOCAL VLAN PROT CONFIGURATION"，进行VLAN及TRUNK口的指定，并把所有的3个VLAN填入TRUNK口的配置单中， 最后显示如下

2). Cisco 4500路由器的设置

把Cisco 4500的f0口按子网数"分割"成相应的"子口"， 根据其设置的ISL（InterSwitch Link)号,与相应子网进行逻辑连接。在本例中，f0被分割为f0.1、f0.2、f0.3与VLAN1、VLAN2、VLAN3连接，其配置命令如下：

```
router#config t
router(config)#int f0.1
router(config-subif)#Description VLAN1_GIET
router(config-subif)#ip address 192.168.111.1 255.255.255.192
router(config-subif)#encapsulation isl 2
. .
router(config)#int f0.2
router(config-subif)#Description VLAN2_gzbnic
router(config-subif)#ip addess 192.168.111.65 255.255.255.192
router(config-subif)#encapsulation isl 3
```

. .
Ctl Z
wr
设置完毕,把边界路由器中有关子网路由项全部指向Cisco 4500,用户的网关按其子网路由器地址设定。

（7）CATALYST 4500 交换机动态 VLAN 与 VMPS 的配置

7.1.VMPS 的介绍:

VMPS 的是 VLAN Membership Policy Server 的简称.它是一种基于端口 MAC 地址动态选择 VLAN 的集中化管理服务器.当某个端口的主机移动到另一个端口后,VMPS 动态的为其指定 VLAN.不过基于 CISCO IOS 的 CATALYST 4500 系列交换不支持 VMPS 的功能,它只能做为 VLAN 查询协议(VLAN Query Protocol)的客户机,通过 VQP 的客户机,可以和 VMPS 通信.如果要让 CATALYST 4500 系列交换机支持 VMPS 的功能,那你应当使用 CatOS(或选择 CATALYST 6500 系列交换机 hoho).

VMPS 使用 UDP 端口监听来自 VQP 客户机的请求,因此,VPMS 客户机也没必要知道 VMPS 到底是位于本地网络还是远程网络.当 VMPS 服务器收到来自 VMPS 客户机的请求后,它将在本地数据库里查找 MAC 地址到 VLAN 的映射条目信息.

VMPS 将对请求进行响应.如果被指定的 VLAN 局限于一组端口,VMPS 将验证对发出请求的端口进行验证:

1.如果请求端口的 VLAN 被许可,VMPS 向客户发送 VLAN 做为响应.

2.如果请求端口的 VLAN 不被许可,并且 VMPS 不是处于安全模式(secure mode),VMPS 将发送"access-denied"(访问被拒绝)的信息做为响应.

3.如果请求端口的 VLAN 不被许可,但 VMPS 处于安全模式,VMPS 将发送"port-shutdown"(端口关闭)的信息做为响应.

但如果数据库里的 VLAN 信息和端口的当前 VLAN 信息不匹配,并且该端口连接的有活动主机,VMPS 将发送"access-denied","fallback VLAN name"(后退 VLAN 名),"port-shutdown"或"new VLAN name"(新 VLAN 名)信息.至于发送何种信息取决于 VMPS 模式的设置.

如果交换机从 VMPS 那里收到"access-denied"的信息,交换机将堵塞来自该 MAC 地址,前往或从该端口返回的流量.交换机将继续监视去往该端口的数据包,并且当交换机识别到一个新的地址后,它会向 VMPS 发出查询信息.如果交换机从 VMPS 那里收到"port-shutdown"信息,交换机将禁用该端口,该端口必须通过命令行或 SNMP 重新启用.

VMPS 有三种模式(但 User Registration Tool,即 URT,只支持 open 模式):

1.open 模式.

2.secure 模式.

3.multiple 模式.

open 模式:

当端口未指定 VLAN:

1.如果该端口的 MAC 地址与之相关联的 VLAN 信息被许可,VMPS 将向客户返回 VLAN 名.

2.如果该端口的 MAC 地址与之相关联的 VLAN 信息不被许可,VMPS 将向客户返回"access-denied"信息.

当端口已经指定 VLAN:

1.如果数据库里的 VLAN 与 MAC 地址相关联的信息和端口的当前 VLAN 关联信

息不匹配,并配置的有 fallback VLAN 名,那么 VMPS 将返回 fallback VLAN 名给客户机.

2.如果数据库里的 VLAN 与 MAC 地址相关联的信息和端口的当前 VLAN 关联信息不匹配,并没有配置 fallback VLAN 名,那么 VMPS 将返回"access-denied"信息给客户机.

secure 模式:

当端口未指定 VLAN:

1.如果该端口的 MAC 地址与之相关联的 VLAN 信息被许可,VMPS 将向客户返回 VLAN 名.

2.如果该端口的 MAC 地址与之相关联的 VLAN 信息不被许可,端口将被关闭.

当端口已经指定 VLAN:

如果数据库里的 VLAN 与 MAC 地址相关联的信息和端口的当前 VLAN 关联信息不匹配,即使有配置 fallback VLAN 名,端口仍将被关闭.

multiple 模式:

当多个 MAC 地址(主机)处于同一 VLAN 的时候,多个 MAC 地址可以对应一个动态端口.如果动态端口的链路 down 掉,端口将被还原成未指定状态,并且在指定 VLAN 之前,VMPS 将对这些地址重新检查;如果这些主机位于不同的 VLAN,VMPS 将向客户返回最新的 MAC 地址到 VLAN 映射的信息.

当然,你也可以在 VMPS 上指定 fallback VLAN 名.如果该端口未指定任何 VLAN,VMPS 将把端口和发起请求的 MAC 地址进行比较:

1.如果主机的 MAC 地址在数据库中不存在,并且 VMPS 上指定的有 fallback VLAN 名,那么将向客户机返回 fallback VLAN 名信息.

2.如果主机的 MAC 地址在数据库中不存在,但 VMPS 上未指定 fallback VLAN 名,那么将向客户机返回"access-denied"信息.

如果该端口已经指定任何 VLAN,VMPS 将把端口和发起请求的 MAC 地址进行比较:

不管 VMPS 上有没有配置 fallback VLAN 名,只要 VMPS 处于 secure 模式,那么它就将反馈"port-shutdown"信息给客户机.

有的时候我们也可能看到非法的 VMPS 客户机请求,如下两种:

1.当 VMPS 上未配置 fallback VLAN 名,并且数据库里没有相应的 MAC 地址到 VLAN 的映射信息.

2.当端口已经被指定了 VLAN,并且 VMPS 不处于 multiple 模式,但是 VMPS 收到了第二个不同 MAC 地址的 VMPS 客户机请求信息.

7.2.VMPS 客户机的介绍:

当端口被配置为动态(dynamic)的时候,它基于 MAC 地址的接收 VLAN 信息.这些 VLAN 信息是基于端口 MAC 地址,从 VMPS 那里动态获得的.动态端口一次只能属于一个 VLAN.当链路 up 后,端口不会立即转发流量,直到该端口获得了 VLAN 信息.当动态端口所连的主机发起第一个数据包的时候,数据包中的源 MAC 地址就做为 VQP 的请求信息中的一个关键部分,它尝试去匹配 VMPS 数据库里的 MAC 地址.如果匹配成功,那么 VMPS 向客户机发送 VLAN 信息(VLAN ID);如果匹配不成功,那么 VMPS 要么拒绝该请求,要么把端口关闭(这取决于 VMPS 所处的模式).当多个 MAC 地址(主机)处于同一 VLAN 的时候,多个 MAC 地址可以对应一个动态端口.如果动态端口的链路 down 掉,端口将被还原成未指定状态,并且在指定 VLAN 之前,VMPS 将对这些地址重新检查;如果这些主机位于不同的 VLAN,VMPS 将向客户

返回最新的 MAC 地址到 VLAN 映射的信息.

7.3.VMPS 客户机的配置:

VMPS 客户机的配置:

!

vmps server 172.20.128.179 primary /------指定主 VMPS 的地址,也可用主机名代替 IP 地址------/

vmps server 172.20.128.178 /------指定备用 VMPS 的地址,也可用主机名代替 IP 地址,最多可以配置 4 个 VMPS------/

!

验证 VMPS 信息:

```
Switch#show vmps
VQP Client Status:
--------------------
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.179 (primary, current)
172.20.128.178
Reconfirmation status
---------------------
VMPS Action: No Dynamic Port
```

如上还显示了 VMPS 客户机的默认信息.

在 VMPS 客户机上配置动态端口:

```
!
interface fa1/1
switchport mode access
switchport access vlan dynamic
!
```

验证信息:

```
Switch# show interface fa1/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: dynamic auto
Operational Mode: dynamic access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
```

如果在动态端口上配置了语音 VLAN ID(VVID),那么该端口可以既属于接入 VLAN,也可属于语音 VLAN.因此,一个连接的有 IP 电话的端口可以有单独的 VLAN 信息:

1.数据流量走接入 VLAN.

2.语音流量走语音 VLAN.

确认动态 VLAN 的成员关系:

```
Switch#vmps reconfirm
```

设置 VMPS 客户机从 VMPS 周期性的重新确认动态 VLAN 的成员关系,设置等待确认的时间(单位:分钟);设置 VMPS 客户机与 VMPS 通信的尝试次数:

```
!
vmps reconfirm 120 /------默认 60 分钟------/
vmps retry 5 /------默认 3 次------/
```

7.4.VMPS 数据库配置文件模板:

```
!
vmps domain /------VMPS 域名必须指定------/
vmps mode {open|secure} /------默认为 open 模式------/
vmps fallback
vmps no-domain-req {allow|deny}
!
vmps-mac-addrs
!
address vlan-name /------定义 MAC 地址到 VLAN 的映射------/
!
vmps-port-group /------定义端口组------/
device {port |all-ports}
!
vmps-vlan-group /------定义 VLAN 口组------/
vlan-name
!
vmps-port-policies {vlan-name |vlan-group }
port-group
device port
!
```

把它上载到交换机可以访问的 TFTP 服务器上即可,如下:

```
!
vmps domain NUAIKO
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
vmps-mac-addrs
!
address 1111.1111.1111 vlan-name BLAKKBLOOD
address 2222.2222.2222 vlan-name BLAKKBLOOD
address 3333.3333.3333 vlan-name 91Lab
address 4444.4444.4444 vlan-name 91Lab
address 5555.5555.5555 vlan-name --NONE--
```

```
address 6666.6666.6666 vlan-name A502
!
vmps-port-group CCIE
device 198.92.30.32 port Fa1/3
device 172.20.26.141 port Fa1/4
vmps-port-group JNCIE
device 198.4.254.222 port Fa0/1
device 198.4.254.222 port Fa0/2
device 198.4.254.223 all-ports
!
vmps-vlan-group 15101
vlan-name BLAKKBLOOD
vlan-name A502
!
vmps-port-policies vlan-group 15101
port-group CCIE
vmps-port-policies vlan-name 91Lab
device 198.92.30.32 port Fa0/9
vmps-port-policies vlan-name A502
device 198.4.254.22 port Fa0/10
port-group JNCIE
!
```

4、Catalyst 4500 系列交换机 NAT 配置：

4.1 4500 系列交换机 NAT 的支持

sup3/4 的 Catalys4000/4500 系列机从 12.1(13)EW 开始支持 AGW 模块，在 AGW 模块运行 12.2(13)T 及以上版本 IOS 时，可以通过 AGM 模块支持 NAT，此时 NAT 以软件方式实现。

4.2、NAT 概述

NAT（Network Address Translation）网络地址转换，其功能是将企业内部自行定义的非法 IP 地址转换为 Internet 公网上可识别的合法 IP 地址。

由于现行 IP 地址标准——IPv4 的限制，Internet 面临着 IP 地址空间短缺的问题，从 ISP 申请并给企业的每位员工分配一个合法 IP 地址是不现实的。NAT 技术能较好解决现阶段 IPV4 地址短缺的问题。

4.3、NAT 原理及配置

NAT 设备维护一个状态表，用来把非法的 IP 地址映射到合法的 IP 地址上去。

```
Router(config)#show ip nat translation
```

显示应为：

Inside local，即内部局部地址——在内部网络上一个主机分配到的 IP 地址，通常是网管人员自己定义的私有地址。

Inside global，即内部全局地址——一个合法的 IP 地址，向外部网络描述一个或多个本地合法 IP 地址。

Outside local，即外部局部地址——出现在内部网络的一个外部主机的 IP 地址。不一定是合法地址，它可以在内部网络中，从可路由的地址空间进行分配。

Outside global，即外部全局地址——主机的拥有者在外部网络上分配给主机的 IP 地址。该地址可以从全局可路由地址或网络空间进行分配。

路由器目前支持内部地址翻译、外部地址翻译和双向地址翻译功能。

内部地址翻译包括：源地址的静态单一地址翻译、源地址的静态子网翻译、源地址静态 tcp 翻译、源地址静态 udp 翻译、源地址访问列表＋地址池翻译、源地址访问列表＋设备接口翻译、目的地址访问列表＋地址池翻译。

外部地址翻译包括：源地址的静态单一地址翻译、源地址的静态子网翻译、源地址静态 tcp 翻译、源地址静态 udp 翻译、源地址访问列表＋地址池翻译。

NAT 分为三种类型：静态 NAT（staticNAT）、NAT 池（pooledNAT）和端口 NAT（PAT）。

静态 NAT

内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。例如路由器的配置：

```
ip nat inside source static 192.168.1.5 211.168.79.75
```

将局域网中的 192.168.1.5 永久映射为全局合法 IP211.168.79.75。此功能可应用到内部网的 WWW 发布、Ftp Server 及 Mail Server。

NAT 池

NAT 池指用户向 ISP 申请了一组合法 IP，在路由器中，将这一组 IP 定义成 NAT 池，通过动态分配的办法，共享很少的几个外部合法 IP 地址。如果 NAT 池中动态分配的外部 IP 地址全部被占用后，后续的 NAT 翻译申请将会失败。用地址超载功能，通过端口号区分不同的连接，可解决这个问题。

路由器的配置：

```
ip access-list standard 1

permit 192.168.1.0 255.255.255.0//局域网中内部局部地址的配置

ip nat pool DCR 211.1.1.1 211.1.1.2 255.255.255.252//局域网中 NAT 池的配置
ip nat inside source list 1 pool DCR overload //地址超载的配置
```

如果局域网中有 20 台 PC，但向 ISP 只申请到 211.1.1.1 和 211.1.1.2 两个合法 IP，通过如上配置，可实现所有的 PC 同时访问 Internet。推荐用户使用地址超载功能。

PAT

```
 nat static add port tcp 80 200.1.1.61
```

PAT，即端口地址转换。通过 PAT 技术，用户只需向 ISP 申请一个合法 IP，就可以满足所有的用户访问 Internet。PAT 可以支持同时连接 64500 个 TCP / IP、UDP / IP，但实际可以支持的工作站个数会少一些。

```
ip access-list standard 1
permit 192.168.1.0 255.255.255.0
ip nat inside source
 list 1 interface Serial0/0 overload//指定访问列表 LIST 1 访问外网时转换成 Serial0/0 口的 IP 地址。
```

5、三层交换机的访问控制列表

在通常的网络管理中，我们都希望允许一些连接的访问，而禁止另一些连接的访问，但许多安全工具缺乏网络管理所需的基本通信流量过滤的灵活性和特定的控制手段。三层交换机功能强大，有多种管理网络的手段，它有内置的 ACL(访问控制列表)，因此我们可利用 ACL(访问控制列表)控制 Internet 的通信流量。

5.1 利用标准 ACL 控制网络访问

当我们要想阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者想要拒绝某一协议簇的所有通信流量时，可以使用标准访问控制列表来实现这一目标。标准访问控制列表检查数据包的源地址，从而允许或拒绝基于网络、子网或主机 IP 地址的所有通信流量通过交换机的出口。

标准 ACL 的配置语句为：

Switch#access-list access-list-number (1’99)
{permit|deny}{anyA|source[source-wildcard-mask]}{any|destination[destination-mask]}

例 1：允许 192.168.3.0 网络上的主机进行访问：

Switch#access-list 1 permit 192.168.3.0 0.0.0.255

例 2：禁止 172.10.0.0 网络上的主机访问：

Switch#access-list 2 deny 172.10.0.0 0.0.255.255

例 3：允许所有 IP 的访问：

Switch#access-list 1 permit 0.0.0.0 255.255.255.255

例 4：禁止 192.168.1.33 主机的通信：

Switch#access-list 3 deny 192.168.1.33 0.0.0.0

上面的0.0.0.255和0.0.255.255等为32位的反掩码，0表示“检查相应的位”，1 表示“不检查相应的位”。如表示 33.0.0.0 这个网段，使用通配符掩码应为 0.255.255.255。

5.2 利用扩展 ACL 控制网络访问

扩展访问控制列表既检查数据包的源地址，也检查数据包的目的地址，还检查数据包的特定协议类型、端口号等。扩展访问控制列表更具有灵活性和可扩充性，即可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其它协议的流量通过，可灵活多变的设计 ACL 的测试条件。

扩展 ACL 的完全命令格式如下：

Switch#access-list access-list-number(100’199) {permit|deny}
protocol{any|source[source-mask]}{any|destination[destination-mask]}[port-number]

例 1：拒绝交换机所连的子网 192.168.3.0 ping 通另一子网 192.168.4.0：

Switch#access-list 100 deny icmp 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255

例 2：阻止子网 192.168.5.0 访问 Internet（www 服务）而允许其它子网访问：

Switch#access-list 101 deny tcp 192.168.5.0 0.0.0.255 any www

或写为：Switch#access-list 101 deny tcp 192.168.5.0 0.0.0.255 any 80

例 3：允许从 192.168.6.0 通过交换机发送 E-mail，而拒绝所有其它来源的通信：
Switch#access-list 101 permit tcp 192.168.6.0 0.0.0.255 any smtp

5.3 基于端口和 VLAN 的 ACL 访问控制

标准访问控制列表和扩展访问控制列表的访问控制规则都是基于交换机的，如果仅对交换机的某一端口进行控制，则可把这个端口加入到上述规则中。
配置语句为：
Switch# acess-list port <port-id><groupid>
例:对交换机的端口 4，拒绝来自 192.168.3.0 网段上的信息，配置如下：
Switch# acess-list 1 deny 192.168.3.0 0.0.0.255
Switch# acess-list port 4 1 // 把端口 4 加入到规则 1 中。
基于 VLAN 的访问控制列表是基于 VLAN 设置简单的访问规则，也设置流量控制，来允许（permit)或拒绝(deny)交换机转发一个 VLAN 的数据包。
配置语句：
Switch#acess-list vlan <vlan-id> [deny|permit]
例：拒绝转发 vlan2 中的数据：
Switch# access-list vlan2 deny
另外，我们也可通过显示命令来检查已建立的访问控制列表,即
Switch# show access-list
例：
Switch# show access-list //显示 ACL 列表；
ACL Status：Enable // ACL 状态 允许；
Standard IP access list: //IP 访问列表；
GroupId 1 deny srcIp 192.168.3.0 any Active //禁止 192.168.3.0 的网络访问；
GroupId 2 permit any any Active //允许其它网络访问。
若要取消已建立的访问控制列表，可用如下命令格式：
Switch# no access-list access-list-number
例：取消访问列表 1：
Switch# no access-list 1
基于以上的 ACL 多种不同的设置方法，我们实现了对网络安全的一般控制方法，使三层交换机作为网络通信出入口的重要控制点，发挥其应有的作用。而正确地配置 ACL 访问控制列表实质将部分起到防火墙的作用，特别对于来自内部网络的攻击防范上有着外部专用防火墙所无法实现的功能，可大大提升局域网的安全性能。

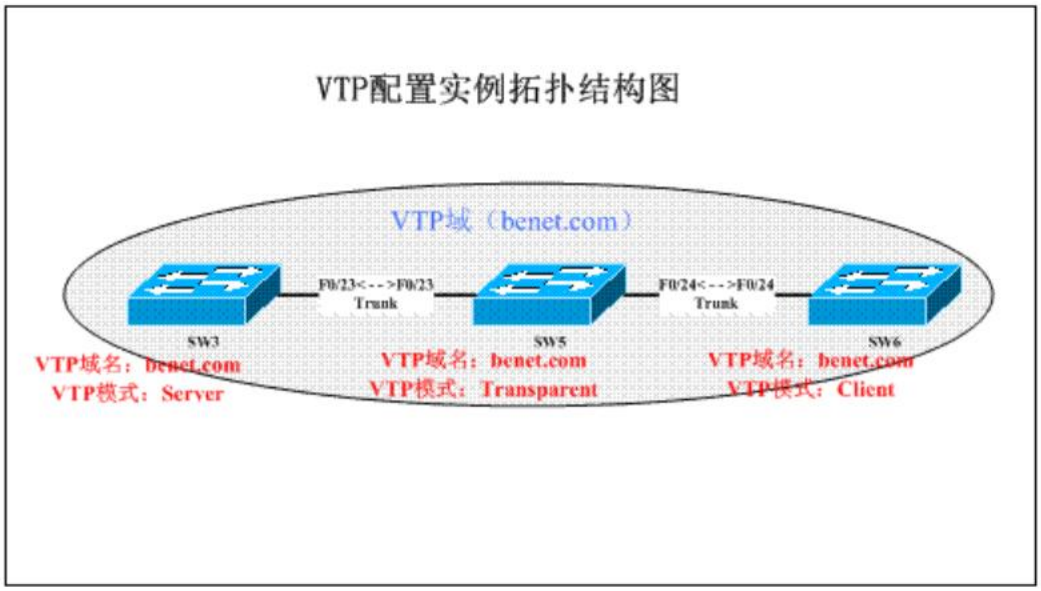
6. VTP 技术

6.1，VLANTrunkProtocol（VTP）：用 VTP 设置和管理整个域内的 VLAN，在管理域内 VTP 自动发布配置信息，其范围包括所有 TRUNK 连接，如交换互连（ISL）、802.10 和 ATMLAN（LANE）

当交换机加电时，它会周期性地送出 VTP 配置请求，直至接到近邻的配置（summary）广播信息，从而进行结构配置必要的更新。
交换机的 VTP 配置有三种模式：服务器、客户和透明模式。

6.2，试验原理：VTP 是一种消息协议，它使用第二层帧，在全网的基础上管理 VLAN 的添加、删除和重命名，以实现 VLAN 配置的一致性。有了 VTP，就可以在一台交换机上集中修改 VLAN 的配置，所做的修改会被自动传播到网络中的所有其它计算机上。

6.3 试验拓扑图：



6.4 试验步骤：

配置 SW3 为服务器（server）模式，SW5 和 SW6 为客户端（client）模式。验证 SW5 和 SW6 是否能够学习到 SW3 的 VLAN 信息。

6.4.1、配置 SW3 的 F0/23,SW5 的 F0/23、F0/24 以及 SW6 的 F0/24 号端口为 trunk 模式。（在所以的交换机之间必须启用中继模式）具体配置以 SW5 为例如下图

```
SW5>en
SW5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW5(config)#interface range f0/23 -24
SW5(config-if-range)#switchport mode trunk
SW5(config-if-range)#end
```

6.4.2、设置 SW3 的 VTP 域名为 benet.com，并设置其模式为服务器（server）模式，启用版本 1（缺省值），启用 VTP 修剪功能（能够减少中继端口上不必要的广播信息量）。

```
sw3(config)#
sw3(config)#vtp domain benet.com
Changing VTP domain name from wang to benet.com
sw3(config)#vtp mode server
Setting device to VTP SERVER mode
sw3(config)#vtp version 1
sw3(config)#vtp prunning
                  ^
% Invalid input detected at '^' marker.

sw3(config)#vtp pruning
Pruning already switched on
sw3(config)#
```

6.4.3、配置 SW3 的 VLAN1 的 IP 地址（交换机的管理 IP 地址标示了 VTP 通告的具体位置）

```
sw3(config)#interface vlan 1
sw3(config-if)#ip address 172.16.18.18 255.255.0.0
sw3(config-if)#no shutdown
sw3(config-if)#
01:31:18: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
```

6.4.4、在 SW3 上配置 vlan10，vlan20，vlan30 用以说明 SW5 和 SW6 所学习的 VLAN 信息。

```
sw3#vlan database
sw3(vlan)#vlan 10 name caiwu
VLAN 10 added:
    Name: caiwu
sw3(vlan)#vlan 20 name xiaoshou
VLAN 20 added:
    Name: xiaoshou
sw3(vlan)#vlan 30 name gongcheng
VLAN 30 added:
    Name: gongcheng
sw3(vlan)#exit
APPLY completed.
Exiting....
```

6.4.5、配置 SW5 和 SW6 的 VTP 域名为 benet.com，并启用 V1 版本（缺省值）以 SW5 为例，如下图所示：

```
SW5(config)#vtp domain benet.com
Changing VTP domain name from wang to benet.com
SW5(config)#
```

6.4.6、现在查看 SW3、SW5、SW6 上的 VLAN 配置信息是否一致。

以 SW3 和 SW5 为例说明，如下图所示：

```
sw3#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/24
10   caiwu                            active
20   xiaoshou                         active
30   gongcheng                        active
```

```
sw3#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 64
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : benet.com
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x32 0x7B 0xEB 0xE9 0x3D 0x0A 0xBD 0x09
Configuration last modified by 172.16.18.18 at 3-1-93 01:33:30
Local updater ID is 172.16.18.18 on interface Vl1 (lowest numbered VLAN interfac
e found)
```

```
SW5#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 64
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : benet.com
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x32 0x7B 0xEB 0xE9 0x3D 0x0A 0xBD 0x09
Configuration last modified by 172.16.18.18 at 3-1-93 01:33:30
SW5#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/24
10   caiwu                            active
20   xiaoshou                         active
30   gongcheng                        active
```

试验结果：SW5 和 SW6 能够学习到 SW3 的 VLAN 信息（注意：不学习端口的划分）。

7、CISCO 交换机的端口镜像的配置：

7.1 cisco 4507r 端口镜像配置方法

Router(config)#monitor session ?

```
SPAN session number
Router(config)#monitor session 1 ?
destination SPAN destination interface or VLAN
filter SPAN filter VLAN
source SPAN source interface or VLAN
Router(config)#monitor session 1 de
Router(config)#monitor session 1 destination ?
interface SPAN destination interface
Router(config)#monitor session 1 destination i
Router(config)#monitor session 1 destination interface ?
FastEthernet FastEthernet IEEE 802.3
Router(config)#monitor session 1 destination interface f
Router(config)#monitor session 1 destination interface fastEthernet ?
FastEthernet interface number
Router(config)#monitor session 1 destination interface fastEthernet 0/0 ?
, Specify another range of interfaces
- Specify a range of interfaces
Router(config)#monitor session 1 s
Router(config)#monitor session 1 source ?
interface SPAN source interface
vlan SPAN source VLAN
Router(config)#monitor session 1 source in
Router(config)#monitor session 1 source interface ?
FastEthernet FastEthernet IEEE 802.3
Port-channel Ethernet Channel of interfaces
Router(config)#monitor session 1 source interface fa
Router(config)#monitor session 1 source interface fastEthernet ?
FastEthernet interface number
Router(config)#monitor session 1 source interface fastEthernet 0/0 ?
, Specify another range of interfaces
- Specify a range of interfaces
both Monitor received and transmitted traffic
rx Monitor received traffic only
tx Monitor transmitted traffic only
Router(config)#monitor session 1 source interface fastEthernet 0/0 b
Router(config)#monitor session 1 source interface fastEthernet 0/0 both ?
Router(config)#monitor session 1 source interface fastEthernet 0/0 both
Router(config)#monitor session 1 de
Router(config)#monitor session 1 destination ?
interface SPAN destination interface
Router(config)#monitor session 1 destination in
Router(config)#monitor session 1 destination interface fa
Router(config)#monitor session 1 destination interface fastEthernet ?
FastEthernet interface number
```

```
Router(config)#monitor session 1 destination interface fastEthernet 0/1
Router(config)#do sh moni sess 1
```

7.2、cisco 4506 交换机镜像端口配置方法

```
monitor session 1 source interface Gi2/47
monitor session 1 destination interface Gi2/15
access-list 1 permit 172.20.0.0 0.0.255.255
access-list 1 deny any
snmp-server community allinone RO 1
snmp-server enable traps tty
```

8、Cisco CATALYST 交换机端口监听配置

CISCO CATALYST 交换机分为两种，在 CATALYST 家族中称侦听端口为分析端口(analysis port)。

8.1、Catalyst 2900XL/3500XL/2950 系列交换机端口监听配置 (基于 CLI)

以下命令配置端口监听：

```
port    monitor
```

例如，F0/1 和 F0/2、F0/3 同属 VLAN1，F0/1 监听 F0/2、F0/3 端口：

```
interface    FastEthernet0/1
port    monitor    FastEthernet0/2
port    monitor    FastEthernet0/3
port    monitor    VLAN1
```

8.2、Catalyst 4000，5000 and 6000 系列交换机端口监听配置 (基于 IOS)

以下命令配置端口监听：

```
set    span
```

例如，模块 1 中端口 1 和端口 2 同属 VLAN1，端口 3 在 VLAN2，端口 4 和 5 在 VLAN2，端口 2 监听端口 1 和 3、4、5，

```
set    span    1/1，1/3-5    1/2
```

9、cisco 4500 交换机的负载均衡技术

目前提出的三种不同的负载均衡模式，可较全面的包含各种网络架构中所应采取措施，三种模式分别是：

模式一：智能型负载均衡

智能型负载均衡模式，是依据接入 WAN 端带宽的大小比例，自动完成负载均衡工作，进一步协助达成带宽使用率的优化目的。智能型负载均衡模式中，提供了联机数均衡与 IP 均衡两种选择。

联机数均衡是依据 WAN 端带宽大小比例，将内网所有的联网机数作均衡分配。例如 WAN1 接入 4M、WAN2 接入 2M，则联机数就会依据 2:1 分配。此种配置是网管员最一般的配置模式。

而 IP 均衡模式是为了避免某些网站(EX 银行网站或 HTTPS 类型的网站)，只能接受来自同一个公网 IP 的所发出封包的瓶颈。如果采用联机数负载均衡模式，会发生该 IP 所发出的访问封包不一定是从固定 WAN 口流出，造成特定网站拒绝服务，导致断线的情况发生。如果采用 IP 均衡，让 IP 依据 WAN 端带宽大小进行比例均衡分配，例如 WAN1 与 WAN2 的带宽比例为 2:1，则 PC1、PC2 走 WAN1，PC3 走 WAN2，PC4、PC5 走 WAN1……，即可达到同一个内网 PC 所发出的应用服务

封包，都从固定的 WAN 口（公网 IP）流出，而整体内网 IP 也会依据带宽大小比例，自动进行均衡配置。此种配置比较适合常常需要进入特定网站时选择。

模式二：指定路由

指定路由比起智能型负载均衡而言，是保留了更多的自由设定弹性与例外原则。由于智能型负载均衡是针对整体内网联机数或是整体 IP 进行均衡分配。并不能个别指定某种应用服务、某个特定 IP、某个特定网址，通过哪个 WAN 口出去。所以，有时会造成特定的服务（例如邮件、VOIP 等）或特定的人士（公司老板、高管等）不能有享有优先或例外的不便。

因此，指定路由是提供可配合协议绑定，先分别指定哪个应用服务、哪个 IP 网段、哪个目的网址，走哪个 WAN 端口。而其余剩下未绑定的部份，再进行智能型负载均衡，同样也有协议绑定模式或是 IP 均衡模式两种选择。

模式三：策略路由

由于大陆地区普遍存在电信、网通彼此互连不互通的跨网瓶颈。某家公司若同时接入电信网通线路，有时会明显发现要从电信去访问网通所提供的服务（如游戏下载等其它应用），会发现非常的缓慢，这就是服务器互访非常困难所造成的问题。

策略路由设定，让两个以上互连不互通的 ISP 线路分流，让电信服务走电信、网通服务走网通，加速服务存取的速度，可大大减低跨网的瓶颈。Qno 侠诺在在产品的接口设计上采用了内建的网通策略模式，指定哪些 WAN 口只给网通走，即可快速设定完成。如果有其它的 ISP 线路需要做策略路由，也可采用自定的策略模式。

策略路由除了普遍应用在电信网通分流之外，也同样可运用在跨国企业、校园网络专线、公众网络、医保专线与一般网络的双网配置架构中，可帮助整合、加速双网的服务质量。

配置实例：双出口 nat 负载均衡加备份

```
interface Ethernet0
ip address 192.168.4.254 255.255.255.0    //定义局域网端口 IP 地址

ip nat inside     //定义为局域端口
ip policy route-map load
!
interface Serial0
ip address 192.168.12.2 255.255.255.0     //定义广域网端口 IP 地址
ip nat outside     //定义为广域端口
shutdown
!
interface Serial1
ip address 192.168.23.2 255.255.255.0
ip nat outside //定义为广域端口
clockrate 64000
!
ip nat inside source route-map net1 interface Serial0 overload
ip nat inside source route-map net2 interface Serial1 overload
ip nat inside source route-map net3 interface Serial1 overload
```

```
ip nat inside source route-map net4 interface Serial0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
ip route 0.0.0.0 0.0.0.0 Serial1
ip route 192.168.1.0 255.255.255.0 192.168.24.4
ip route 192.168.2.0 255.255.255.0 192.168.24.4
ip route 192.168.3.0 255.255.255.0 192.168.24.4
ip http server
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 2 permit 192.168.2.0 0.0.0.255
access-list 2 permit 192.168.4.0 0.0.0.255
route-map load permit 10
match ip address 1
match interface Serial0
set interface Serial0
!
route-map load permit 20
match ip address 2
match interface Serial1
set interface Serial1
!
route-map net4 permit 10
match ip address 2
!
route-map net3 permit 10
match ip address 2
match interface Serial1
!
route-map net2 permit 10
match ip address 1
!
route-map net1 permit 10
match ip address 1
match interface Serial0
```

10.双机热备 HSRP

10.1 案例：

让 Trunk1 走 VLAN8－9，Trunk2 走 VLAN10－12。

```
interface fastethernet 0/1
spanning-tree vlan 8 cost 30
spanning-tree vlan 9 cost 30
interface fastethernet 0/2
panning-tree vlan 10cost 30
```

```
spanning-tree vlan 11 cost 30
=======================================================
```

下面是 4506 的 hsrp 配置。
4506A:

```
interface Vlan8
ip address 10.10.202.17 255.255.255.0
no ip redirects
standby 8 ip 10.10.202.16
standby 8 priority 80
standby 8 preempt
!
interface Vlan10
ip address 10.254.150.10 255.255.255.0
no ip redirects
standby 10 ip 10.254.150.5
standby 10 priority 120
standby 10 preempt
```

4506B:

```
interface Vlan8
ip address 10.10.202.18 255.255.255.0
no ip redirects
standby 8 ip 10.10.202.16
standby 8 priority 120
standby 8 preempt
!
interface Vlan10
ip address 10.254.150.20 255.255.255.0
no ip redirects
standby 10 ip 10.254.150.5
standby 10 priority 80
standby 10 preempt
```

10.2、环路问题，首先你的配置中虽然指定了端口的开销，但是 STP 却形成了环路，即没有选出 ROOT，所以没有人发送 BPDU，建议在任何一个 4506 上增加配置如下：

```
spanning-tree extend system-id
spanning-tree vlan 1 priority 16384
spanning-tree vlan 10 priority 16384
spanning-tree vlan 11 priority 16384
spanning-tree vlan 8 priority 16384
```

```
spanning-tree vlan 9 priority 16384
```

三、Catalyst 4500 系列交换机的安全策略

(一)、三层交换机网络服务的安全策略

1,禁止 CDP(Cisco Discovery Protocol)。如:

```
Catalyst(Config)#no cdp run
Catalyst(Config-if)# no cdp enable
```

2,禁止其他的 TCP、UDP Small 服务。

```
Catalyst(Config)# no service tcp-small-servers
Catalyst(Config)# no service udp-samll-servers
```

3,禁止 Finger 服务。

```
Catalyst(Config)# no ip finger
Catalyst(Config)# no service finger
```

4,建议禁止 HTTP 服务。

```
Catalyst(Config)# no ip http server
```

如果启用了 HTTP 服务则需要对其进行安全配置:设置用户名和密码;采用访问列表进行控制。

如:

```
Catalyst(Config)# username BluShin privilege 10
G00dPa55w0rd
Catalyst(Config)# ip http auth local
Catalyst(Config)# no access-list 10
Catalyst(Config)# access-list 10 permit 192.168.0.1
Catalyst(Config)# access-list 10 deny any
Catalyst(Config)# ip http access-class 10
Catalyst(Config)# ip http server
Catalyst(Config)# exit
```

5,禁止 BOOTp 服务。

```
Catalyst(Config)# no ip bootp server
```

禁止从网络启动和自动从网络下载初始配置文件。

```
Catalyst(Config)# no boot network
Catalyst(Config)# no servic config
```

6,禁止 IP Source Routing。

```
Catalyst(Config)# no ip source-route
```

7,建议如果不需要 ARP-Proxy 服务则禁止它,路由器默认识开启的。

```
Catalyst(Config)# no ip proxy-arp
Catalyst(Config-if)# no ip proxy-arp
```

8,明确的禁止 IP Directed Broadcast。

```
Catalyst(Config)# no ip directed-broadcast
```

9,禁止 IP Classless。

```
Catalyst(Config)# no ip classless
```

10,禁止 ICMP 协议的 IP Unreachables,Redirects,Mask Replies。

```
Catalyst(Config-if)# no ip unreacheables
```

```
Catalyst(Config-if)# no ip redirects
Catalyst(Config-if)# no ip mask-reply
```

11,建议禁止 SNMP 协议服务。在禁止时必须删除一些 SNMP 服务的默认配置。或者需要访问列表来过滤。如：

```
Catalyst(Config)# no snmp-server community public
Ro
Catalyst(Config)# no snmp-server community admin RW
Catalyst(Config)# no access-list 70
Catalyst(Config)# access-list 70 deny any
Catalyst(Config)#      snmp-server      community
MoreHardPublic Ro 70
Catalyst(Config)# no snmp-server enable traps
Catalyst(Config)# no snmp-server system-shutdown
Catalyst(Config)# no snmp-server trap-anth
Catalyst(Config)# no snmp-server
Catalyst(Config)# end
```

12,如果没必要则禁止 WINS 和 DNS 服务。

```
Catalyst(Config)# no ip domain-lookup
```

如果需要则需要配置：

```
Catalyst(Config)# hostname Catalyst
Catalyst(Config)# ip name-server 202.102.134.96
```

13,明确禁止不使用的端口。

```
Catalyst(Config)# interface eth0/3
Catalyst(Config)# shutdown
```

14，屏蔽 ping 包

14.1 屏蔽外部 ping 包

```
Catalyst(Config)#access-list 110 deny icmp any any echo log

Catalyst(Config)#access-list 110 deny icmp any any redirect log

Catalyst(Config)#access-list 110 deny icmp any any mask-request log

Catalyst(Config)#access-list 110 permit icmp any any
```

14.2 允许内部 ping 包

```
Catalyst(Config)#access-list 111 permit icmp any any echo

Catalyst(Config)#access-list 111 permit icmp any any Parameter-problem

Catalyst(Config)#access-list 111 permit icmp any any packet-too-big
```

```
Catalyst(Config)#access-list 111 permit icmp any any source-quench

Catalyst(Config)#access-list 111 deny icmp any any log
```

15. 跟踪路由 TraceRoute 的设定

15.1 屏蔽外部 TraceRoute

```
Catalyst(Config)#access-list 112 deny udp any any range 33400 34400
```

15.2 允许内部 TraceRoute

```
Catalyst(Config)#access-list 112 permit udp any any range 33400 34400
```

（二）三层交换机访问控制的安全策略

1,严格控制可以访问核心交换机的管理员。任何一次维护都需要记录备案。

2,建议不要远程访问核心交换机。即使需要远程访问核心交换机，建议使用访问控制列表和高强度的密码控制。

3,严格控制 CON 端口的访问。具体的措施有：

A,如果可以开机箱的，则可以切断与 CON 口互联的物理线路。

B,可以改变默认的连接属性，例如修改波特率(默认是 96000，可以改为其他的)。

C,配合使用访问控制列表控制对 CON 口的访问。如：

```
Catalyst(Config)#Access-list 1 permit 192.168.0.1
Catalyst(Config)#line con 0
Catalyst(Config-line)#Transport input none
Catalyst(Config-line)#Login local
Catalyst(Config-line)#Exec-timeoute 5 0
Catalyst(Config-line)#access-class 1 in
Catalyst(Config-line)#end
```

D,给 CON 口设置高强度的密码。

4,如果不使用 AUX 端口，则禁止这个端口。默认是未被启用。禁止如：

```
Catalyst(Config)#line aux 0
Catalyst(Config-line)#transport input none
Catalyst(Config-line)#no exec
```

5,建议采用权限分级策略。如：

```
Catalyst(Config)#username chengyong privilege 10
G00dPa55w0rd
Catalyst(Config)#privilege EXEC level 10 telnet
Catalyst(Config)#privilege EXEC level 10 show ip
access-list
```

6,为特权模式的进入设置强壮的密码。不要采用 enable password 设置密码。而要采用 enable secret 命令设置。并且要启用 Service password-encryption。

7,控制对 VTY 的访问。如果不需要远程访问则禁止它。如果需要则一定要设置强

壮的密码。由于 VTY 在网络的传输过程中为加密，所以需要对其进行严格的控制。如：设置强壮的密码；控制连接的并发数目；采用访问列表严格控制访问的地址；可以采用 AAA 设置用户的访问控制等。

8, IOS 的升级和备份，以及配置文件的备份建议使用 FTP 代替 TFTP。如：

```
Catalyst(Config)#ip ftp username chengyong
Catalyst(Config)#ip ftp password 4tppa55w0rd
Catalystr#copy startup-config ftp:
```

（三）三层交换机其他安全配置

（1）及时的升级和修补 IOS 软件。

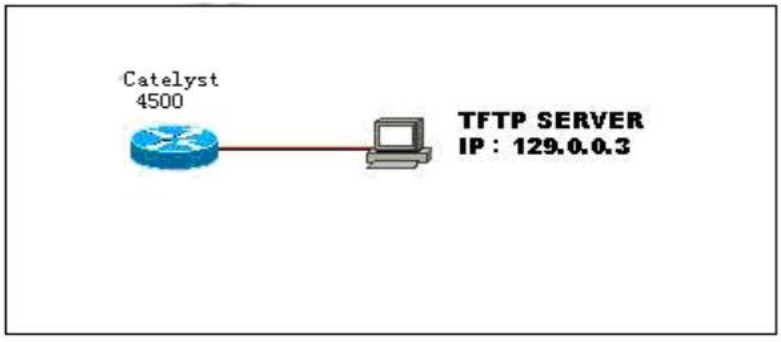
对 Cisco 三层交换机来说，升级 IOS 不仅能够修订 Bug，提升三层交换机性能扩展三层交换机功能。需要注意的是升级 IOS 是有一定的操作风险的，需要做好充足的准备。

（2）要严格认真的为 IOS 作安全备份。

Cisco 三层交换机配置文件中保存了管理员对三层交换机所做的所有配置信息，这些配置可都是自己的心血，一定要做好备份。因为即使做好安全预防措施，也难免会发生不可预想的问题。所以为了尽可能地减少或避免意外的发生，要随时为 Cisco 三层交换机的配置文件作安全备份。当然，三层交换机配置的备份包括不同的层次，命令 “Catalyst#copy running-config startup-config”是将当前存储在 RAM 的正确配置备份到 Cisco 三层交换机的 NVRAM 中，在下一次启动时路由器就会使用这个正确的配置。命令“Catalyst#copy running-config tftp”是将 RAM 中配置信息备份到 tftp 服务器中，笔者说所的备份就是这样的备份。这样当 Cisco 三层交换机的配置信息丢失或者被恶意修改后我们可以通过命令
“Catalyst#copy tftp runing-config”来快速恢复。

（3）要为三层交换机的配置文件作安全备份。

Cisco 三层交换机的配置过程中，经常会用到 COPY 这个命令。下面我们就为大家介绍如何使用 COPY 命令备份配置文件，以及如何从 TFTP 服务器拷贝备份配置文件。



3.1、copy running-config startup-config

这个命令是将存储在 RAM 的正确配置拷贝到 Cisco 三层交换机的 NVRAM 中。这样，在下一次启动时，三层交换机就会使用这个正确的配置。

3.2、copy running-config tftp

这个命令是将 RAM 中正确的配置文件拷贝到 TFTP 服务器上，我们强烈推荐网络管理员这样做，因为如果路由器不能从 NVRAM 中正常装载配置文件，我们可以通过从 TFTP 中拷贝正确的配置文件。

```
Catalyst4500#copy running-config tftp

address or name of remote host

[]?129.0.0.3

destination file name [it168-confg]?

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

624 bytes copied in 7.05 secs
```

当网络管理员输入命令并键入回车后，路由器会要求输入 TFTP 服务器的 IP 地址，在正确的键入服务器 IP 地址后，路由器还要求网络管理员提供需要备份的配置文件名。一般我们建议使用管理员容易记忆的文件名。这时路由器会提示管理员按 YES 确认操作。

3.3、copy tftp running-config 如果路由器的配置文件出现问题，这时我们就可以通过从 TFTP 服务器中拷贝备份的配置文件。具体配置如下：

```
Catalyst4500#copy tftp running-config

address or name of remote host[]?

129.0.0.3

source filename []?it168-confg
```

```
destination file name [running-config]?

accessing tftp://129.0.0.3/it168-confg

loading it168-confg from 129.0.0.3

(via fastethernet 0/0):

!!!!!!!!!!!!!!!!!!!!!!

[ok-624 bytes]

624 bytes copied in 9.45 secs
```

（4）购买 UPS 设备，或者至少要有冗余电源。

（5）要有完备的三层交换机的安全访问和维护记录日志。

路由器的日志主要包括访问日志和维护日志两部分，日志对于路由的管理至关重要。当我们怀疑遭受网络攻击时，审阅路由器访问记录是查出安全事件的最有效的方法，无论是对于正在实施的攻击还是将要实施的攻击都非常有效。利用连接到 Internet 的记录，你还能够查出试网建立外部连接的特洛伊木马程序和间谍软件程序，一个具有一定安全经验并且细心的管理员在病毒传播者作出反应之前能够查出病毒的攻击。另外，一个有经验的攻击者在登录路由器并实施攻击后会利用诸如 clear logging 这样的命令清除自己的登录记录。所以，一定要有完备的日志备份策略。

5.1 系统日志配置

5.1.1 全局系统日志

logging on

no logging on

功能：该命令用来启动全局系统日志功能；在此命令前加“no”将关闭全局系统日志功能。

命令模式：特权配置模式。

缺省情况：缺省为不启动全局系统日志功能。

使用指南：只有启动了全局系统日志功能，系统才会向日志主机、控制台等方向输出系统日志信息。

举例：启动系统日志功能。

Switch# logging on

5.1.2 控制台输出日志信息

logging console

no logging console

功能：该命令用于打开向控制台输出日志信息的通道；在此命令前加“no”将会关闭控制台输出通道的日志输出。

命令模式：特权配置模式。
缺省情况：缺省为不向控制台输出日志信息。
使用指南：只有启动了全局系统日志功能，该命令才会生效。
举例：打开向控制台输出日志信息的通道。
Switch#logging console
5.1.3 用户终端输出日志信息
logging monitor
no logging monitor
功能：该命令用来打开用户终端输出通道；在此命令前加“no”将关闭用户终端输出通道的输出。
命令模式：特权配置模式。
缺省情况：缺省为不向用户终端输出日志信息。
使用指南：只有启动了全局系统日志功能，该命令才会生效。
举例：打开向用户终端输出日志信息的通道。
Switch# logging monitor
5.1.4 内存缓冲区输出日志信息
logging buffered [<*buffersize*>]
no logging buffered
功能：该命令用来打开日志缓冲区输出通道；在此命令前加“no”将关闭日志缓冲区输出通道的输出。
参数：*<buffersize>*为内存缓冲区的大小（指可容纳消息的条数），范围为10-1000。
命令模式：特权配置模式。
缺省情况：缺省为不向内存缓冲区输出日志信息。缺省设置的内存缓冲区大小为 100。
使用指南：只有启动了全局系统日志功能，该命令才会生效。
举例：使以太网交换机向内存缓冲区发送日志信息，设定内存缓冲区的大小为50。
Switch# logging buffered 50
5.1.5 日志主机输出日志信息
logging <*ip-addr*> [facility <*local-number*>]
no logging <*ip-addr*>
功能：该命令用来打开日志主机输出通道；在此命令前加“no”将关闭日志主机输出通道的输出。
参数：*<ip-addr>*为日志主机的 IP 地址。*<local-number>*为日志主机的记录工具，范围在 local0～local7。
命令模式：特权配置模式。
缺省情况：缺省为不向日志主机输出日志信息。缺省的日志主机的记录工具为local0。
使用指南：只有启动了全局系统日志功能，该命令才会生效。
举例：使以太网交换机向 IP 地址为 100.100.100.5 的 PC 机发送日志信息，消息被保存到日志记录工具 local1 中。
Switch# logging 100.100.100.5 facility local1
5.1.6 日志通道的概要信息

show channel [console | monitor | logbuff | loghost]
功能：该命令用来显示日志通道的概要信息。
参数： console 日志输出通道为控制台；monitor 日志输出通道为用户终端；logbuff 日志输出通道为日志缓冲区；loghost 日志输出通道为日志主机。
命令模式：特权配置模式。
缺省情况：show channel 不带参数表示显示所有通道的概要信息。
使用指南：查看某日志通道的概要信息时，可使用本命令。
举例：显示 Loghost 通道的内容。

```
Switch# show channel loghost↵

/********* Loghost Channel **************/
Channel ID:2, channel name:loghost
State: On
Send messages:0,Dropped messages:0
Loghosts:
IPAddress Facility
100.100.100.5 local1
Filter Items:
Module State Servirity
shell On debugging
```

5.1.7 日志输出通道中添加/删除过滤项记录
logging source {<*modu-name*> | default} channel <*channel-name*> [level<*severity*> [state { on | off }]]
no logging source { <*modu-name*> | default } channel <*channel-name*>
功能：该命令用来向日志输出通道中添加/删除过滤项记录。
参数：<*modu-name*>为允许输出日志消息的模块名。
default 为允许所有模块输出日志消息。<*channel-name*>为要设置的输出通道名，即 console(控制台)，monitor(用户终端)，logbuff(日志缓冲区)，loghost(日志主机)。
<*severity*>为日志消息的严重等级阈值，在此级别以下的信息不输出。state { on | off }：该过滤项的状态为打开/关闭。
5.1.8 日志消息的严重级别信息
日志消息的严重级别信息如下：

- critical - 严重信息
- debugging - 调试过程产生的信息
- notifications - 正常出现但是重要的信息
- warnings - 警告信息

举例：设置将 loghost 通道中的 shell 模块的日志类信息打开，且允许输出信息的最高级别为 notifications。设置将 logbuff 通道中的 shell 模块的日志类信息打开，且允许输出信息的最高级别为 debugging。

```
Switch# logging source m_shell channel loghost level notifications state on
Switch# logging source m_shell channel logbuff level debugging state on
```

5.1.9 清除日志缓冲区中的信息

clear logging
功能：该命令用来清除日志缓冲区中的信息。
命令模式：特权配置模式。
使用指南：用户需要清除日志缓冲区内的信息时，可使用本命令。
举例：清除日志缓冲区中的信息。
switch# clear logging
（6）要严格设置登录 Banner。必须包含非授权用户禁止登录的字样。

Catalyst(config)#hostname SW1 //修改路由器的标识。

SW1(config)#banner motd #

This is Cisco CATALYST 4500 //配置日期信息标志区(MOTD)，登录到交换机时显示。

#

SW1(config)#

SW1(config)#banner exec# //配置执行标志区，如 Telnet 到路由器时显示的欢迎信息。

Telnet to Cisco CATALYST 4500!

#

SW1(config)#end

SW#clock set 15:05:33 25 February 2006 //配置时钟。

SW1#
（7） IP 欺骗得简单防护。如过滤非公有地址访问内部网络。过滤自己内部网络地址;回环地址(127.0.0.0/8);

RFC1918 私有地址;DHCP 自定义地址(169.254.0.0/16);科学文档作者测试用地址(192.0.2.0/24);
不用的组播地址(224.0.0.0/4);
SUN 公司的古老的测试地址(20.20.20.0/24;204.152.64.0/23);全网络地址(0.0.0.0/8)。
Catalyst(Config)# access-list 100 deny ip 192.168.0.0 0.0.0.255 any log
Catalyst(Config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
Catalyst(Config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
Catalyst(Config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
Catalyst(Config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
Catalyst(Config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any log

Catalyst(Config)# access-list 100 deny ip 192.0.2.0 0.0.0.255 any log
Catalyst(Config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
Catalyst(Config)# access-list 100 deny ip 20.20.20.0 0.0.0.255 any log
Catalyst(Config)# access-list 100 deny ip 204.152.64.0 0.0.2.255 any log
Catalyst(Config)# access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
（8）建议采用访问列表控制流出内部网络的地址必须是属于内部网络的。如:
Catalyst(Config)# no access-list 101
Catalyst(Config)# access-list 101 permit ip 192.168.0.0 0.0.0.255 any
Catalyst(Config)# access-list 101 deny ip any any log
Catalyst(Config)# interface eth 0/1
Catalyst(Config-if)# description "internet Ethernet"
Catalyst(Config-if)# ip address 192.168.0.254 255.255.255.0
Catalyst(Config-if)# ip access-group 101 in
（9） Cisco 交换机 4500 系列交换机密码恢复过程
（1） 交换机开机，30 秒内按 Ctrl＋Break 键，出现提示符“rommon 1 >”（如果没有出现该提示符，交换机重新开机，重复（1）步骤)。
（2） 键入如下命令： rommon 1 > confreg 0x2142
（3） 初始化交换机： " rommon 2 >reset".
（4） switch#show startup-config 这时将全部的内容备份。
（5） switch#config mem
switch(config)＃no enable secret
switch(config)＃enable secret cisco
switch(config)＃config－reg 0x2102" ;
"switch(config)＃exit";
switch#write mem
（6） 重新启动交换机，即可:“switch＃reload".