# 交换路由设备的日志备份及分析

## Backup And Analysis Of Switch And Routers Log

王 海 （莱阳农学院网络中心　山东青岛 266109）

摘要：本文介绍了交换机、路由器日志备份信息的重要性，以华为 3com 公司的 Quidway 系列设备为例，说明了在 Redhat AS3 Linux 服务器配置备份日志的详细步骤，以及备份日志的分析方法，在实际工作中对于事后安全审计、故障判断有着很高的应用价值。

关键词：日志 备份 交换机 路由器 Linux

## 1 前言

以太网交换机和路由器一般都提供日志、调试和告警信息的查看和备份功能，网络管理员和开发人员登录设备后，可以通过使用命令来查看使用情况，分析故障原因。但由于局域网内网络设备的地理位置、物理条件的差异，网络设备经常会出现掉电重启的情况，保存在设备内部缓冲区的日志、调试和告警信息会因此丢失；另外，设备内部缓冲区的大小是一定的，缓冲区充满后，以前的信息记录便会被覆盖。所以，为了更好地监控网络的运行情况和诊断网络的故障，在局域网环境中，有必要启用交换机和路由器的日志、调试和告警信息的备份功能，将需要监控的设备的日志、调试和告警信息集中保存到一台或多台日志服务器中，以利于事后安全审计、故障判断和检索分析。

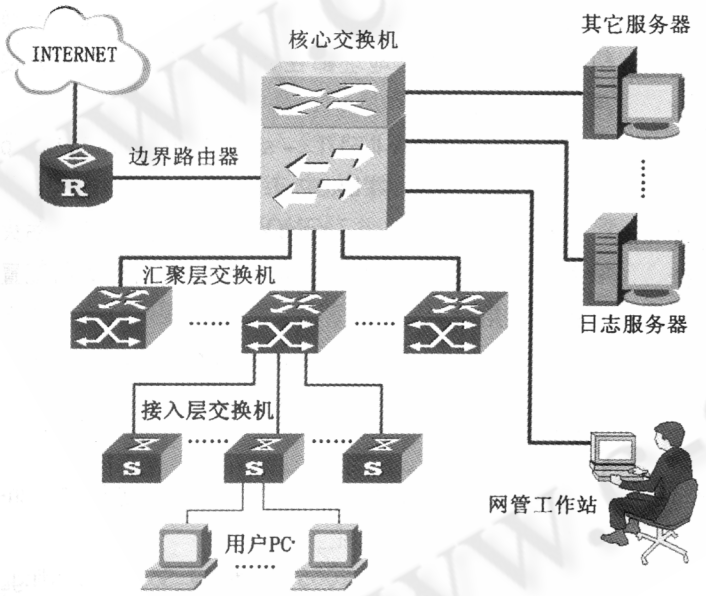


图 1

## 2 交换机和路由器的配置

图 1 所示的三层以太局域网环境中，所用设备为华为 3COM 公司的 Quidway 系列交换机和路由器，边界路由器型号为 R3640E，核心层交换机为 S8512，汇聚层交换机为 S6503，接入层交换机为 S3000 系列，如需要将这些设备的所有日志、调试和告警信息备份到一台 LINUX 服务器（REDHAT AS3）中，日志主机的 IP 地址假定为 10.10.1.10，其配置步骤如下。

Quidway 系列交换机和路由器的信息日志备份的配置命令基本相同，以 S8512 交换机为例。

### 2.1 修改交换机和路由器的主机名

因为所有的信息都备份到一台 LINUX 服务器中，为便于区分不同设备发送来的信息，必须把设备设置不同的主机名，如：

```
sysname Quidway_S8512
```

### 2.2 开启信息中心

```
[Quidway_S8512] info - center enable
```

### 2.3 设置信息中心输出的日志主机 IP、设备号、语言

这里 facility 设备号的选用请先查看 LINUX 主机的日志配置文件/etc/syslog.conf，在 local0 ~ local7 选择未在/etc/syslog.conf 使用的，这里选 local4 为例。

[Quidway_S8512] info - center loghost 10.10.1.10 facility local4 language english

2.4 选择信息类别、级别输出到日志主机

可以根据需要选择重要的设备、重要的信息类别和级别，这里将日志、调试和告警信息的所有类别、级别的信息都输出到日志主机为例。

[Quidway_S8512] info - center source default channel loghost log level debugging debug level debugging trap level debugging

## 3 日志主机的配置

以超级用户(root)的身份执行以下操作。

3.1 建立日志备份文件

# mkdir /var/log/Quidway

# touch /var/log/Quidway/information

3.2 编辑文件/etc/syslog.conf，加入以下选择/动作组合

local4.* /var/log/Quidway/information

/etc/syslog.conf 中指定的设备名及接受的日志信息级别与交换机上配置的 info - center loghost 和 info - center loghost a.b.c.d facility 应保持一致，否则日志信息可能无法正确输出到日志主机上。上面的配置表示所使用的设备为 local4，星号表示接受所有的信息。

3.3 重启日志服务进程

当日志文件 information 建立且/etc/syslog.conf 文件被修改了之后，应通过执行以下命令查看系统日志服务守护进程 syslogd 的进程号，杀死 syslogd 进程，并重新用 -r 选项在后台启动 syslogd(-r 选项启用日志服务器的 UDP 514 端口，接收网络上传送过来的其它机器的日志信息)。

# ps -ae | grep syslogd

1211

# kill -9 1211

# syslogd -r &

重启 syslogd 进程后，用 netstat - an 检查 UDP 514 端口是否已打开，如果 UDP 514 端口没有打开，请查看/etc/services 文件是否有"syslog514/udp"行，没有请加上。确认无误后，可以在相应的日志文件 information 中看到新添加的日志记录信息了。syslog.conf 文件的详细配置方法请参阅有关文档。

3.4 修改 syslogd 进程的启动脚本

修改 syslogd 进程的启动脚本/etc/init.d/syslog 文件，以便 LINUX 系统关机重启后 syslogd 进程还能以 -r 选项启动。

编辑/etc/init.d/syslog 文件，找到 start() 段，将"daemon syslogd $SYSLOGD_OPTIONS"行改为"daemon syslogd -r $SYSLOGD_OPTIONS"，存盘后退出。

3.5 修改日志轮循控制脚本

为了避免日志过大，可以配置日志轮循脚本配置文件/etc/logrotate.conf，也可以使用默认值。

3.6 修改防火墙脚本

日志主机开放 UDP 514 端口后，接收网络上传送过来的其它机器的日志信息，但服务器和客户机之间没有安全验证过程，非法日志客户端和 syslog 攻击可能导致系统混乱。这样就必须增加防火墙的规则，将非法日志客户端和 syslog 攻击过滤掉。假设本地交换机和路由器的管理地址都在 10.10.100.0/24 网段，使用如下命令。

# iptables -A INPUT -s ! 10.10.100.0/24 -p udp - -dport 514 -j DROP

然后使用 iptables - save 命令保存此配置到防火墙启动配置文件中，以便 LINUX 系统重启后本行配置能重新启用。

# iptables - save > /etc/syconfig/iptables

## 4 日志分析

全部配置完成后，就可以查看日志服务器中的 information 文件了，例如：

Nov 22 22:35:08 2005 Quidway_S6503_Building_005 SHELL/5/CMD:task:vt0 ip:10.10.36.118 user:** command: stp，此条日志信息记录表示一个用户在 Nov 22 22:35:08 2005，从 IP 地址为 10.10.36.118 的客户机上登录到名称为 Quidway_S6503_Building_005 的交换机上，执行了 stp 命令。

Nov 23 15:01:54 2005 Quidway_S6503_Building_005 ARP/5/DUPIP: IP address 10.10.70.202 collision detected, sourced by 0013 - d4d6 - 7e88 on GigabitEthernet1/0/1 of VLAN76 and 0013 - d4a4 - 74f3 on GigabitEthernet1/0/1 of VLAN76，此条报警信息记录表

示在 Nov 23 15:01:54 2005，交换机 Quidway_S6503_Building_005 的属于 VLAN76 的端口 GigabitEthernet1/0/1 下连接的用户机，发生了 IP 地址冲突，MAC 地址为 0013 - d4d6 - 7e88 和 0013 - d4a4 - 74f3 的用户机，使用了同一个 IP 地址 10.10.70.202。对于这种报警信息，再通过查看交换机的 MAC 地址表，可以准确定位干扰源，排除网络故障。

通过以上两条信息记录，可以看出日志备份及分析的重要性。由于所有的交换路由设备的日志都备份在一个日志文件中，如何高效地找出需要的信息、如何在出现重大告警时自动报告，成为要解决的下一个问题。

日志记录具有一定的格式，以"时间戳 主机名 模块名/级别/信息摘要:内容"的格式保存，对照此格式，我们可以使用 Linux 系统下的功能强大的文本编辑、检索工具，对日志文件进行事后安全审计、故障判断和检索分析。

对于更高的应用需求，可以将日志文件导入 MySQL 数据库，推荐使用 LINUX 下的 syslog - ng 软件替代 syslog，syslog - ng 具有同 MySQL 数据库的接口，可以将日志文件直接输入到 MySQL 数据库。然后，编写 PHP 或基于 J2EE 的统计、检索、查询、自动告警程序，配置好 APACHE 或 TOMCAT 的 WEB 服务器，网络管理员和开发人员就可以在网管工作站上使用 WEB 浏览器查看所需要的信息。日志、数据库、WEB 可以在一台 LINUX 机器上配置，处理流程如图 2 所示。

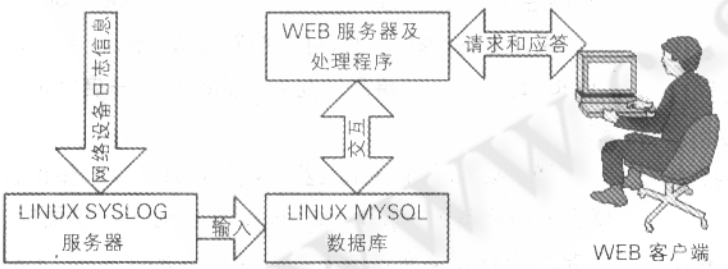


图 2

## 5　结束语

网络管理人员借助于日志分析，可以不断适应日益复杂的网络环境，维护职责范围内的网络稳定。做好交换路由设备的日志备份和分析，对于实际工作中事后安全审计、故障判断有着很高的实用价值。

**参考文献**

1 The netfilter. org " iptables" project, http://www.netfilter.org

2 IEFT RFC3164, The BSD Syslog Protocol