

MSR系列路由器NAM业务模块利用nProbe和Netflow插件对网络流量进行监控分析

陈安【技术大咖】 2007-05-28 发表

MSR系列路由器

NAM业务模块利用nProbe和Netflow插件对网络流量进行监控分析

关键字: MSR; NAM; Netflow; nProbe

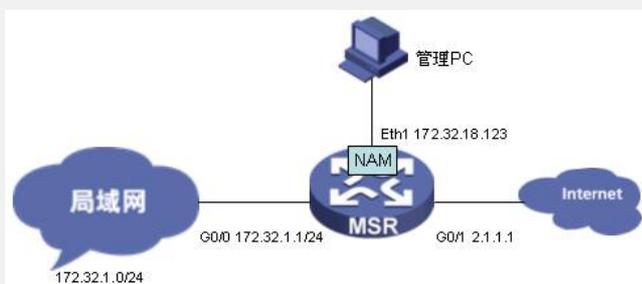
一、组网需求:

随着网络发展速度的加快,网络传输速率也是数量级增加,普通PC使用网卡均支持千兆速率。为了适应网络发展的需要,对千兆网络进行监控管理已成为必然。nProbe运行在NAM插卡上,处理路由器镜像过来的流量,对路由器的转发性能基本没有影响,而NAM本身就支持对Netflow报文的分析,只要在NAM插卡上同时运行nProbe和NAM,就可以轻松实现对千兆流量分析。本文就是介绍如何通过nProbe和NAM的配置来完成这一目的。

设备清单: MSR系列路由器 1台

NAM模块: 1块

二、组网图:

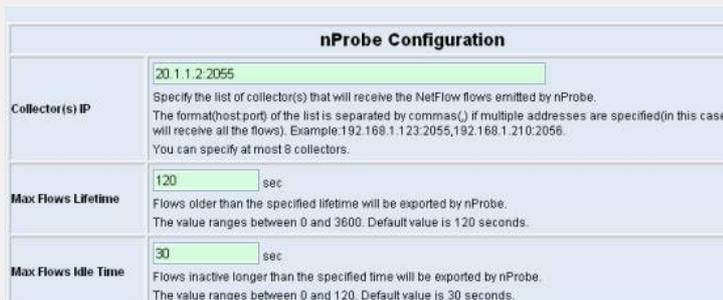


三、配置步骤:

适用设备和版本: MSR系列、Version 5.20. Beta 1501L02后所有版本。

- 1、按照组网图连好设备,将PC的IP地址配置成172.132.18.1/24
- 2、首先要做好路由器和NAM的基本配置,使得管理PC能够通过WEB界面来访问NAM模块。详细请参见《MSR系列路由器通过WEB界面来访问NAM模块的基本配置》。
- 3、配置nProbe

通过web界面左侧的Configuration/nProbe,进入nProbe配置视图,选择发送Netflow报文的目的IP为NAM模块的管理IP地址172.32.18.123,端口号为2055,如下图:



应该说配置好Collector IP后,其余配置都是nProbe的扩展性能配置了,可以不用做修改,采用默认参数即可。用户可以根据具体需求更改里面的参数。

4、配置Netflow

配置Netflow前要将NAM启动。

对于Netflow的配置,首先要增加一个NetFlow接口Plugins/Netflow/Configure 里面的Add Netflow Device,新建一个Netflow接口,如下图:



进入新增加的Netflow接口配置界面，配置相关参数，其中最重要的参数就是UDP端口号，要与nProbe保持一致，为2055，如下图：

NetFlow Configuration

Incoming Flows

NetFlow Device	NetFlow <input type="button" value="Set Interface Name"/> [List NetFlow Interfaces]
Local Collector UDP Port	2055 <small>[Use a port value of 0 to disable collection]</small> <input type="button" value="Set Port"/>
Flow Collection	<p>Virtual NetFlow Interface</p> <input type="text" value="1.0.0.0/8"/> <input type="button" value="Set Interface Address"/> <p><small>This value is in the form of a network address and mask on the network where the actual NetFlow probe is located. NAM determine which TCP/IP addresses are local and which are remote.</small></p> <p><small>You may specify this in either format, <network>/<mask> or CIDR (<network>/<bits>). An existing value is displayed in <n</small></p>

其余配置都是nProbe的扩展性能配置了，可以不用做修改，采用默认参数即可。

四、实验总结

1、查看Netflow统计数据

做好以上配置后，将nProbe也启动起来，过一会，接口通过Netflow接口来查看统计信息了。如下图：

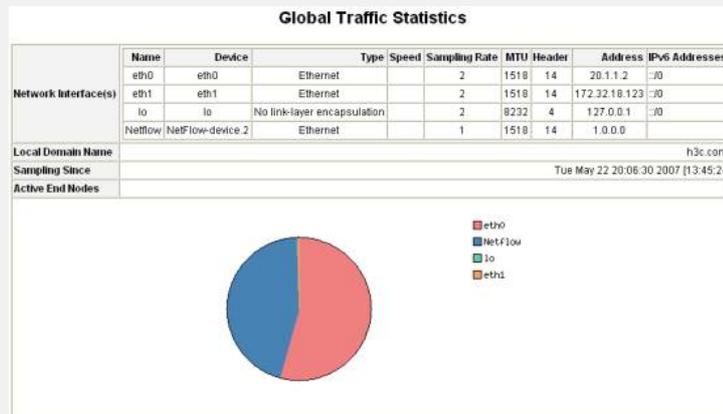
NAM > Administration [NAM]

Configuration NAM

NAM Application:

NAM Action: Startup Shutdown

Application	State
NAM	Running
nProbe	Running



2、原理分析

nProbe是Netflow Probe的简称，意为Netflow探针。通过nProbe将镜像过来的流量按照Netflow格式进行打包，发送给能够对Netflow报文进行处理的主机来处理这些报文。而在NAM上正好集成了Netflow插件，因此在nProbe处理后，直接就交给了Netflow插件处理，两者同时集成在NAM模块上，具有得天独厚的优势，能够对千兆流量进行分析处理。