文章编号：1006-4354（2013）02-0030-03

陕西省气象广域网络流量应用分析

李 珍

（陕西省气象信息中心，西安 710014）

摘 要：采用基于 Netflow 的流量监测方法，在省级电信 MSTP 线路安装网络监控设备，对陕西省气象广域网络的网络流量分别进行基于数据包和流量行为的分析。在了解网络流量的构成和分布比例符合气象业务基本特性的基础上，发现当前台站、地市级气象部门在网络应用中存在网络资源释放不及时和网络防护中的漏洞，并提出相应措施，提高网络带宽的有效利用率和网络性能。

关键词：气象业务网络；流量监测；流量分析

中图分类号：TP393 **文献标识码**：B

陕西省气象广域网由省－市和市－县间的电信 MSTP（多业务传输平台）线路和广电 SDH（同步数字体系）线路组成，承担省市县三级气象资料的汇集传输、气象应用系统的数据交换和气象办公系统的数据传输业务，承载的业务包括气象通信系统、气象观测系统、运行监控业务系统、视频会商系统、办公系统等多个业务系统[1]。为更加详尽的掌握全省广域网络的使用情况，将网络监控设备安装在省级电信 MSTP 线路，全面监控网络的使用情况，特别是网络流量。通过对各类气象业务流量监控结果进行分析研究，同时分析高流量用户的信息，找到造成高网络流量的原因并对其加以改进，改善和提高网络性能。

1 网络流量监测的方法

网络流量监测的主要方法有基于简单网络管理协议（SNMP）的流量监测和基于 Netflow 的流量监测等。基于 SNMP 协议的流量监测，是通过提取网络设备的管理信息库（MIBII）中收集的一些与具体设备及流量信息有关的参数而实现。其优点是使用软件方法实现，不需要对网络进行改造或增加部件、配置简单、费用低。缺点是只包括字节数、报文数等最基本的内容，不适于复杂的流量监测[2]。

NetFlow 是一种数据交换方式，其利用标准的交换模式处理数据流的第一个 IP 包数据，生成 NetFlow 缓存，随后同样的数据基于缓存信息在同一数据流中进行传输，不再匹配相关的访问控制等策略，NetFlow 缓存同时包含随后数据流的统计信息。一个 NetFlow 流定义为在一个源 IP 地址和目的 IP 地址间传输的单向数据包流，所有数据包有共同的传输层源、目的端口号。

相对于基于 SNMP 的流量监测，基于 NetFlow 的流量监测方法的优点是将提供的流量信息扩大到七个属性（源 IP 地址、目标 IP 地址、源通信端口号、目标通信端口号、第三层协议类型、服务类型（TOS）字节、网络设备输入或输出的逻辑网络端口（iflndex）），可以区分各个逻辑通道上的流。缺点是由于功能的复杂性，支持 Netflow 需要在网络设备上附加单独的功能模块[3]。

2 流量分析方法

网络流量分析指通过捕获网络流量数据对其进行深入量测和分析，来掌握网络的流量特性（某种协议、应用服务的使用情况或者某些用户的行为特征等），为精细化流量控制提供数据依据。

2.1 基于数据包的分析

对数据包的分析一般可分为：基于地址、端口的分析，基于特征码的分析及深度数据包检测。

收稿日期：2012-08-23

作者简介：李珍（1983—），女，甘肃玉门人，硕士，工程师，从事气象信息业务。

基于地址、端口的分析是通过识别 IP、URL 地址或应用服务的特定端口来检测分类的方法。但随着网络技术的发展，越来越多的应用不再基于固定的地址、端口，使这种方法的使用范围不断缩小。基于特征码的分析是通过检测开放式系统互联（OSI）模型中四层以下的内容中是否含有某些应用服务的特殊标示或使用的特定协议，来对数据包进行分类的方法，是一种使用较多的分析方法。深度数据包检测（DPI）是一种对数据包深入到应用层协议检测分析的方法。它通过逐包分析、模式匹配，并使用行为模式识别等技术，可对流量中的具体应用服务实现较为准确的识别[4]。

2.2　基于流量行为的分析

目前较为常见的是深度流行为检测（DFI），这是通过对数据流的数据包长度、数据流持续时间、链接状态、网络层传输层信息等参数来对其进行统计分析的检测方法，可以分析加密数据流，能对数据进行模糊分类[5]。

3　结果分析

2012 年 5—6 月，采用基于 Netflow 的流量监测方法对陕西省气象广域网络进行监测，并对监测资料分别进行了基于数据包和基于流量行为的分析。

3.1　业务流量归类分析

表 1 为业务流量的 24 h 平均分布情况。从表 1 可以看出，在网络业务流量中所占比例最大的为 FTP-DATA 服务，占 44.4%；其次为 HTTP 服务、RTST 服务、MS-SQL 服务，分别占 19.2%、9.4%和 2.3%。FTP-DATA 服务的业务类型为地市级、县级气象部门上行至省级气象部门和省级下行至地市级、县级的 FTP 传输业务，这种上、下行的 FTP 业务为省内业务网络承载的最主要的业务，所占比例也最大；HTTP 服务为省级各部门对外提供服务的各类网站，是仅次于 FTP 业务的重要业务，所占比例也仅次于 FTP-DATA 服务；RTST 服务的业务类型为省内实景监测系统的流媒体服务，MS-SQL 服务的业务类型为省级对外提供数据共享的数据库服务，均为省内的主要业务，所占比例也较大。从业务流量分布可以看出，陕西省气象业务网络的流量分布基本符合陕西省气象业务的特点。

表 1　业务流量分布表

应用类型	服务条目	24 h 平均流量/GB	所占比例/%
FTP-DATA	FTP 服务	50.73	44.4
HTTP	网络会话	21.97	19.2
TCP	普通 IP 协议组	12.29	10.7
RTSP	流媒体服务	10.83	9.4
UDP	普通 IP 协议组	10.82	9.4
MS-SQL	数据库访问服务	2.65	2.3
FTP	网络会话	1.56	1.4
IKE	加密通道	1.04	0.9
H323-Media	视频服务	0.98	0.9
SNMP	网络管理	0.73	0.6

3.2　业务流量前十用户 IP 分析

为更加详细的分析业务网络流量，对 24 h 平均发送和接收的总流量位于前十位的用户 IP 进行了分析研究。分析发现，在业务总流量中排在前十位的用户 IP 中，省级气象部门的用户 IP 仅占不到 30%，其余均为地市级和台站级气象部门。地市级、台站级气象部门应用较为单一的服务器的网络流量与省级气象部门一对多提供服务的省级服务器的网络流量相比，两者相差不多甚至前者远高于后者。从网络业务流量的优化统筹方面来讲，这种现象是极不合理的。

造成这种现象的原因有：①县级、地市级气象部门自行开发的应用软件或程序的设计不合理，程序频繁上连省级服务器后未及时断开网络连接释放网络资源，从而造成高网络会话。高网络会话可能会带来网络震荡和网络流量过大，对全省业务网络和服务器造成很大的压力。当网络流量大到一定程度时，就会造成整个业务网络的堵塞。②县级、地市级气象部门的服务器由于防护不到位，感染计算机病毒、遭受网络攻击或被加挂木马程序，短期内产生大量的访问需求，从而造成网络流量过大。

针对上述原因可行的有效方法有：①对不合理的软件或程序进行优化，在交互结束之后及时自动断开网络连接，再一次进行交互时再建立新的网络会话，合理利用网络资源；②加强对县级、地市级服务器的防护工作，在互联网接口安装防

文章编号：1006-4354 (2013) 02-0032-02

榆林市区域自动气象站信息分析综合应用系统设计与实现

王 云[1]，徐振明[2]，万红卫[1]

(1. 榆林市气象局，陕西榆林 719000；2. 成都信息工程学院，成都 610225)

摘 要：利用计算机编程和信息处理技术，开发榆林市184个区域自动气象站运行监控和数据分析综合应用系统。该系统能够自动显示区域自动气象站实时观测数据；自动监控报文传输和蓄电池状态；对正在发生或可能发生的高温、大风、强降水等灾害性天气自动报警；查询统计区域自动气象站实时和历史资料，并利用AnyChart控件和SURFER软件自动生成图像图表文件。

关键词：区域气象站；质量监控；资料处理

中图分类号：P409 **文献标识码**：B

近年来，区域自动气象站（以下简称区域站）不断增加，为中小尺度天气分析和气象信息服务提供更多的实时观测数据。但区域站多是无人值守的自动观测站，故障发生率高，维修不及时常会造成数据中断，且观测数据均没有整理，不能实现资料统计积累。为了有效提升区域站数据传输质量，最大限度利用区域站实时观测资料，不断增强公共气象服务和防灾减灾能力，发挥区域站建设的效益，利用榆林市184个区域站，设计开发榆林市区域站信息分析综合应用系统。

1 设计思路

系统利用VB.net＋JAVA＋MSSQL作为开发平台，主要包括质量监控、实时报警和数据处理3个功能模块，总体架构见图1。系统每小时

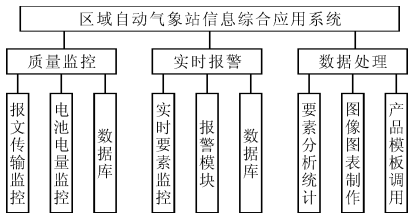

图1 系统功能框架图

收稿日期：2012-09-06

作者简介：王云（1978—），男，陕西子洲人，学士，工程师，从事气象业务、服务管理。

火在服务器上安装杀毒软件。

4 结论

陕西省气象业务网络的流量分布基本符合陕西省气象业务的特点，同时也存在一定问题。主要表现在县级、地市级气象部门服务器的网络流量远大于一对多提供服务的省级服务器。而造成这一问题的主要原因一方面是由于广域网络存在病毒，另一方面是由于对网络资源的使用不合理，没有及时释放网络资源从而造成网络过度浪费。只有将这些问题妥善解决，才能进一步提高网络带宽的有效利用率和网络性能。

参考文献：

[1] 赵立成，沈文海，周林，等．气象信息系统[M]．北京：气象出版社，2011：22-24.

[2] 谢喜秋，梁洁，彭巍，等．网络流量采集工具的分析和比较[J]．电信科学，2002(4)：63-66.

[3] 穆斌，武俊喜，樊莉．网络流量监测及异常流量分析技术[J]．信息系统工程，2011(9)：82-80.

[4] 杨祥．流量控制系统原理分析[J]．电子商务，2010(12)：50-51.

[5] 夏中林．校园网流量分析与控制策略应用[J]．数字技术与应用，2012(2)：160-162.