ICS 35.240.01
A 90

GA

中华人民共和国公共安全行业标准

GA/T 608—2006

公安信息网络管理系统技术规范

Network management system technical specification for public security private network

2006-05-24 发布　　2006-06-01 实施

中华人民共和国公安部　　发布

中华人民共和国公共安全
行业标准
公安信息网络管理系统技术规范
GA/T 608—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.75 字数 46 千字
2006年8月第一版 2006年8月第一次印刷
*
书号:155066·2-17010 定价 15.00 元

目　　次

前　言

本标准的附录A为资料性附录，附录B和C为规范性附录。

本标准由公安部信息通信局提出。

本标准由公安部通信标准化技术委员会归口。

本标准起草单位：公安部信息通信局、大用软件有限责任公司。

本标准主要起草人：任兆红、钟宁、王成钢、师启君、徐同阁、熊桂喜、张辉、张小萍。

公安信息网络管理系统技术规范

1 范围

本标准规定了公安信息网络管理系统的基本功能、性能和应遵循的各项技术要求。

本标准适用于全国各级公安信息网络管理系统建设和管理的全过程。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC1213，基于 TCP/IP 的因特网的网络管理信息库：MIB-Ⅱ，1991

IETF RFC1907，SNMP v2 的管理信息库，1996

IETF RFC2011，使用 SMI v2 描述的 IP SNMP v2 管理信息库，1996

IETF RFC2012，使用 SMI v2 描述的 TCP SNMP v2 管理信息库，1996

IETF RFC2013，使用 SMI v2 描述的 UDP SNMP v2 管理信息库，1996

IETF RFC2233，接口组管理信息库，1997

3 术语和定义

下列术语和定义适用于本标准。

3.1

简单网络管理协议 simple network management protocol；SNMP

一个基于 UDP 协议的用于网络管理工作站和远程设备(如路由器、交换机等)代理软件之间通信的网络管理协议，它支持 get、getNext 和 set 三个最基本的操作。

3.2

管理信息库 management information base；MIB

由支持 SNMP 协议的代理软件使用和维护的网络管理信息数据库。它是一个树状的被管理设备相关属性的对象集合。树中每个叶子节点描述了被管理对象某一方面的属性信息，如配置参数、性能数据等。

3.3

社区名(又译：共同体名) community name

代理软件采用 SNMP 协议在通信过程中对管理者进行身份验证的密码字符串。有两种基本的社区名，分为只读的和可读写的，分别对应 SNMP 协议的 get 和 set 操作。

3.4

网络探针 probe

专门进行网络流量和协议分析的一种硬件装置。

3.5

电子邮件系统邮局协议的第 3 版 post office protocol 3；POP3

用于定义电子邮件系统中客户端和邮件服务器进行通信和下载电子邮件的协议。POP3 允许客户端从服务器上把邮件存储到本地主机，同时可以删除保存在邮件服务器上的邮件。

3.6

简单邮件传输协议　simple mail transfer protocol;SMTP

一种最主要的用于在因特网上从一个邮件服务器向另外一个邮件服务器发送电子邮件的传输协议。

3.7

域名系统　domain name system;DNS

一种将直观、明了、易记的主机名称(即域名)翻译成实际的IP地址的系统。当使用域名访问因特网时,DNS服务器就会自动将域名转换成目标主机的IP地址。

3.8

超文本传输协议　hyper text transfer protocol;HTTP

一组定义在因特网上进行超文本文件(也称为Web页面)传输的协议。

3.9

文件传输协议　file transfer protocol;FTP

一种在因特网上任意两台电脑之间进行文件传输的协议。

3.10

采集域　collection domain

指在网络管理系统中,由某一管理工作站直接发现和监控的管理对象的集合。

3.11

管理域　management domain

指在网络管理系统中,该系统能感知或管理的网络边界内一组管理对象的集合。一个管理域可以包含若干个采集域。

3.12

公安信息网络　information network for public security

连接全国各级公安机关的专用信息通信网络,它由三级主干网和接入网组成。公安部至省级公安机关的网络为一级网;省级公安机关至所辖地市(或直辖市分局、县局)公安机关的网络为二级网;地市公安机关至所辖分局、县级公安机关的网络为三级网。各类计算机、网络设备和终端通过局域网或其他接入方式分别连入各级公安主干网络。

3.13

网络管理系统　network management system

指管理全国各级公安机关专用通信网络的信息系统。

3.14

关键服务器　private server

指在全国各级公安机关专用通信网络中运行关键公安业务系统的服务器,如email、FTP、WEB、DNS服务器、八大资源数据库和应用服务器等。

3.15

征求意见　request for comments;RFC

一系列Internet标准或备忘录的总称,描述了建议技术的规格说明。

4　全国公安信息网络管理系统的体系结构

全国公安网络设立三级层次化的网络管理体系结构,如图1所示。

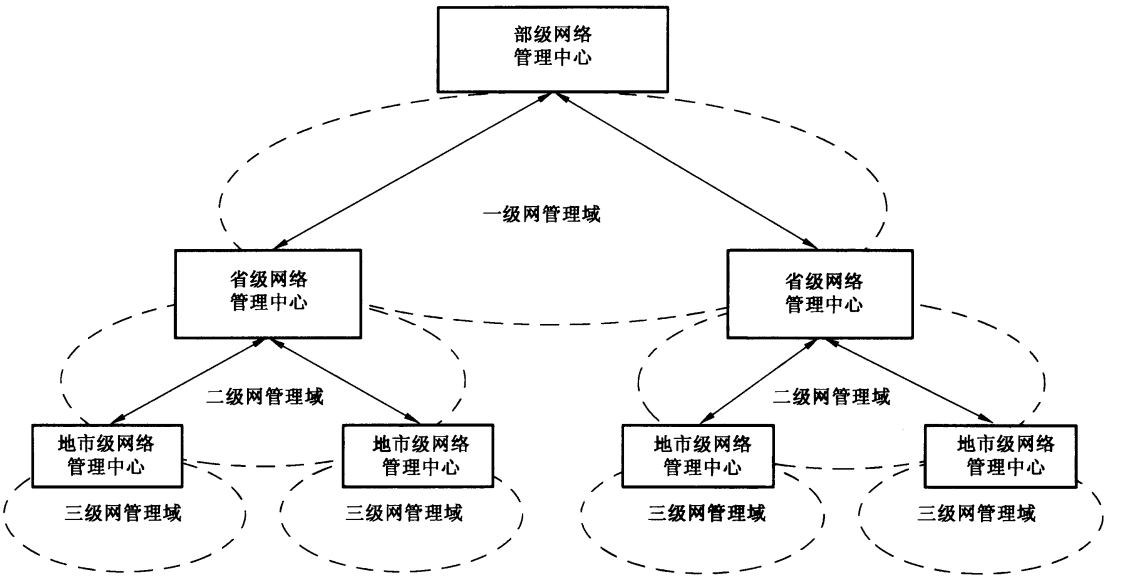

图 1　公安信息网络管理的体系结构

4.1　一级管理域的范围

在公安部设立一级网络管理中心，管理域为公安一级网、公安部机关局域网、公安部北京城域网以及公安部京外直属单位接入网。管理对象主要是本管理域内的路由器和交换机。

4.2　二级管理域的范围

在各省公安厅设立二级网络管理中心，管理域为各省、自治区、直辖市、新疆生产建设兵团所辖的公安二级网络、公安厅(局)机关局域网及省级直属单位接入网。管理对象主要是本管理域内的路由器、交换机和关键服务器等设备。

4.3　三级管理域的范围

在各地市级公安局设置三级网络管理中心，管理域为该地市级公安三级网、公安局机关局域网和基层所、队等接入网。管理对象主要是本管理域内的路由器、交换机和关键服务器等设备。

在各级网络管理中心，可采用集中式的网络管理系统，直接管理本管理域内的网络，各级网络管理系统之间通过管理接口交换数据。各级网络管理系统分别设置相应的管理接口，上级网络管理系统可通过此接口提取下一级网络管理系统中的有关信息，实现数据共享。

在特殊情况下，上级网管系统可以跨管理域监控下级管理域内的网络设备运行状况。各级管理域根据各地的实际情况，在统一的网络管理平台上，广域网和局域网可以分别管理，也可以统一管理。在不具备网管条件的下级管理域，其上级管理部门可直接对该管理域监管。

下一级网络管理系统对上一级网络管理系统提供的接口主要内容为：

a)　本地网络的拓扑结构、配置和运行参数等；

b)　本地网络性能数据，如网络流量、带宽使用情况、服务器的性能等；

c)　本地网络的重大告警或故障数据，如链路中断、服务不可用情况等；

d)　本地业务数据报表，如关键网络质量指标的月报表、年报表等；

e)　其他需要进行共享的数据。

5　网络管理系统的功能要求

5.1　网络管理系统的功能组成结构

公安信息网络管理系统是一个分级、分布式的网络管理信息系统，其主要功能组成如图 2 所示，各级网络管理系统的功能见附录 B。

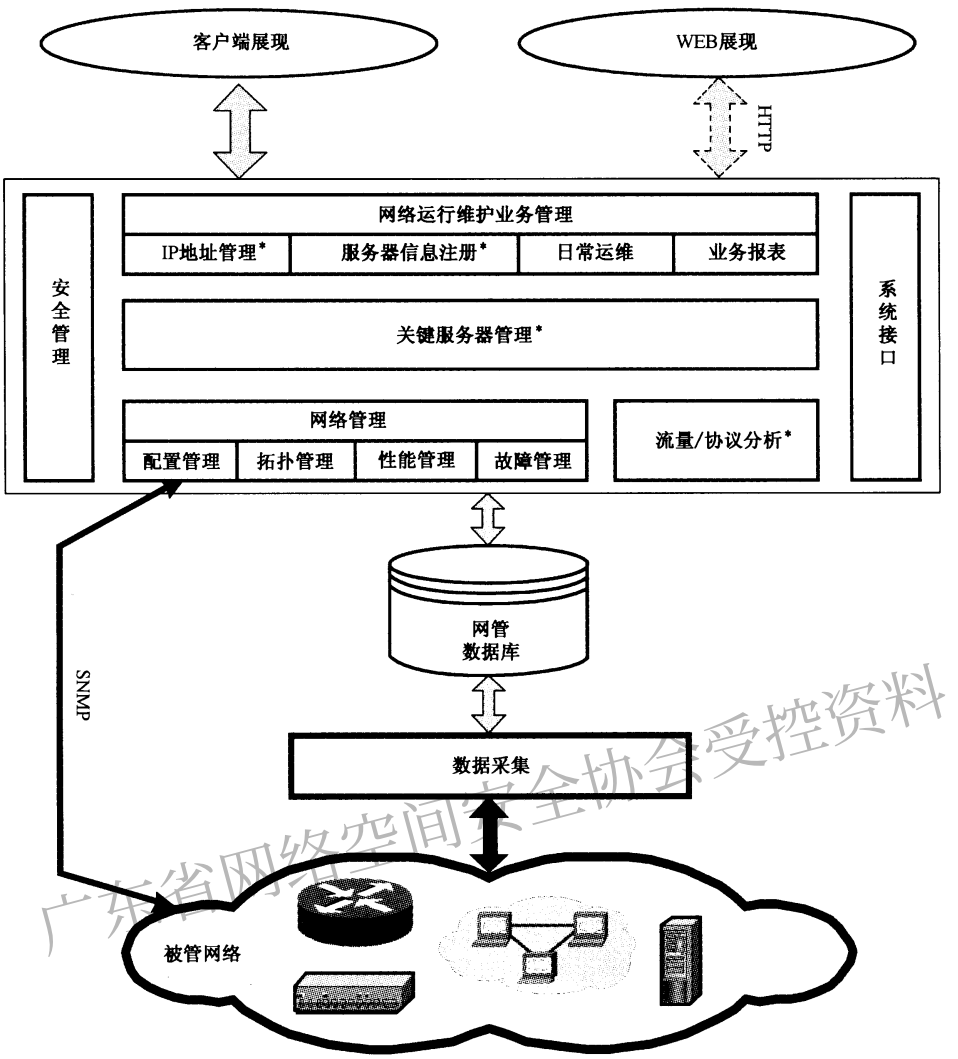

图 2　网络管理系统功能组成结构

各级公安网络管理系统的功能主要包括：

a) 网络管理：包括拓扑管理、配置管理、故障管理、性能管理、链路管理等；

b) 数据采集：为网络管理系统的核心功能，负责采集和存储周期性的网络性能数据、关键服务器性能数据、关键应用性能等数据（见附录 C）；对各种告警信息进行收集、处理和存储；轮询被管网络设备的状态等。采集方式支持 SNMP、SSH（Secure Shell，安全 Shell）或者 Agent（代理）等；

c) 网络流量/协议分析：包括流量/协议分析、TopN（前 N 位排行）用户/流量应用统计报表等；

d) 关键服务器管理：对服务器的通断状态、CPU、内存及磁盘空间使用情况进行管理；

e) 应用服务管理：监视常用公安业务应用系统（如 Web 服务、email、OA、中间件、数据库等）的运行状态；

f) 网络运行维护业务管理：包括 IP 地址管理、应用服务器的资料申报、网络的日常运行维护管理、运行维护业务报表的定制、生成和发布等功能；

g) 安全管理：包括用户管理和访问控制，网络管理系统操作日志的管理，网管数据库的维护和备份等；

h) 系统接口：为上、下级网络管理系统提供拓扑、告警、性能、报表等数据访问服务。

注：图2中以“*”标注的功能为可选功能，以下各节中也均以“*”标识可选功能。

5.2 网络管理

网络管理类功能是各级公安网络管理系统必备的基本功能。系统应该以方便、可视、易于操作的方式实现拓扑管理、配置管理、故障管理、性能管理、链路管理等功能。

5.2.1 拓扑管理

网络拓扑管理的首要功能是构造各级网络拓扑图。应该将动态构造的网络拓扑图作为公安网络运行管理的集中操作界面。通过操作网络拓扑图上的元素，可查看其属性信息，并能进行相关设备和链路的配置。拓扑图既能直观地显示被管对象的层次关系，又能显示其连接情况。

拓扑管理的主要功能包括：

a) 支持网络拓扑自动发现：智能、快速地探测整个网络（定义好的本管理域内），自动搜寻网络（包括局域网和广域网）中活动的结点，获得网络中所有路由器、交换机、服务器的相关信息；可自动识别网络中各种设备的类型、网络之间以及网络内各结点之间的连接关系，并按照拓扑构成的逻辑层次来组织网络拓扑；自动发现网络拓扑及其配置的变化信息，及时地更新网管数据库中的拓扑数据；

b) 在实现自动拓扑发现功能的同时，还应提供手动更新拓扑的手段，并支持在拓扑发生变动时产生拓扑变动告警信息；

c) 按照不同管理域，以分层方式直观清晰地组织和显示被管网络的拓扑结构；

d) 以多种方式表现网络拓扑视图，如采用树状视图、网状拓扑视图等；

e) 拓扑图应支持以地理图片为背景图，将网络节点直接显示于地图上；

f) 网络拓扑图显示所有链路、网络设备的工作状态；

g) 拓扑图支持链路流量的实时显示，可以选择流入流量、流出流量、流入/流出总流量等组合显示方式；可自定义流量显示刷新的时间间隔，但最小时间间隔应不小于10 s；

h) 在显示网络连接链路时，支持使用不同粗细的线条表示链路的物理带宽大小；

i) 网络故障和告警要直接显示在拓扑视图的相应设备处以及相关的子网视图中。告警状态可以按照自定义的传播策略传递给相关的网络对象；

j) 支持在拓扑的局部切换显示模式。选择该模式时，系统自动将整个拓扑图分成多个子拓扑图，轮流显示每个子图，被显示的每个子图将放大为全屏显示；

k) 在拓扑视图上通过快捷功能菜单查看设备的网络标识、IP地址、软硬件型号、版本、网络接口参数等基本配置信息；

l) 提供灵活的编辑工具来支持拓扑管理功能。可以手工添加、删除、修改各种网络管理对象，并提供设备过滤功能，屏蔽不关心的管理设备；

m) 功能菜单应该集成一些常用网络管理工具，如ping、traceroute、telnet、MIB浏览器等。

5.2.2 配置管理

配置管理支持在网络拓扑自动发现的基础上，显示网络设备的配置信息，包括设备型号、类型、系统配置信息、端口配置、路由表配置、IP地址配置等。配置信息应该和实际的设备配置一致。

在实现自动拓扑发现功能时，应为配置管理提供手动更新配置的手段。配置信息变动时能产生变动告警。

对所管理的网络设备提供公安设备资源维护日志记录的录入、管理、查询功能。维护日志包括时间、维护人、维护记录等信息项，并与设备的其他信息相关联。

5.2.3 故障管理

故障管理功能包括：网络故障管理、系统故障管理和应用故障管理。

5.2.3.1 故障事件分类管理和告警

系统应通过对故障事件进行分类，并按照分类来告警。故障管理功能支持以下的故障类型并能产生告警信息：

a) 网络设备故障(如设备宕机、链路中断等)；

b) 网络性能阈值告警(如链路的带宽使用率超过70%，则产生级别为“严重”的性能告警)；

c) 系统性能阈值告警；

d) 应用性能阈值告警；

e) 从其他管理中接入的告警，如日志告警、防火墙告警、电源告警、杀毒软件的告警等，系统必须支持告警类型的自定义。

5.2.3.2 故障分级管理和告警

规定系统中的故障告警级别及其对应的界面显示颜色如表1所示：

表1 告警级别定义表

故障类别	级别	颜色(RGB值)	
正常(Normal)	0	绿色	(0,255,0)
不确定(Indeterminate)	1	蓝色	(0,0,255)
警告(Warning)	2	青色	(0,255,255)
轻微(Minor)	3	黄色	(255,255,0)
严重(Major)	4	橙色	(255,153,0)
紧急(Critical)	5	红色	(255,0,0)

在配置各级网络管理系统的过程中，系统可根据实际需求确定每一类告警的严重级别，但对一些故障告警级别建议按照如下设置：

a) 设备、链路或者网络设备端口中断的告警级别为“紧急”；

b) 服务器宕机、业务应用不可用的告警级别为“紧急”；

c) 链路带宽使用率超过40%为“警告”，超过70%为“严重”，超过90%为“紧急”；

d) 端口丢包率超过1%为“警告”，超过5%为“严重”，超过10%为“紧急”。

5.2.3.3 监测重要故障事件

故障管理应具备以下监测功能：

a) 监测各级主干网络链路的通、断事件；

b) 监测关键服务器的通、断事件；

c) 监测各级主干网路由器的端口工作状态(包括上行、下行)；

d) 接收设备厂商定义的Trap(陷阱)故障事件，关于标准Trap的定义参见规范性引用文件RFC1907中的相关内容；

e) 监测网络设备的配置情况，如果发现有异常改动就报警。

5.2.3.4 故障事件处理

a) 对故障事件进行过滤、相关性分析、传递、关联等处理，将处理过的事件保存在网管数据库中。一些重要的处理规则如下：

1) 过滤规则：

按照时间段；

按照单一IP地址；

按照设备类型；

按照告警级别；

按照告警类型；

按照 IP 地址段。

2） 压缩规则：

按照给定的告警次数；

按照设备状态的变化。

b） 系统能提供声音、电子邮件、短消息等多种告警通知方式，根据不同的告警类型和级别设置不同的告警方式；

c） 故障管理实时监视网络运行过程中所出现的故障，确定故障位置，应尽量给出故障原因；

d） 系统提供实时（延迟时间＜5s）的告警显示功能，以时间顺序（最新的告警显示在最前面）显示符合过滤条件的所有告警信息，并将某一条告警记录和拓扑图关联起来，以便准确定位发生故障的设备在拓扑图中的位置；

e） 系统提供对历史告警信息的统计和分析功能，分别按照时间段、IP 地址、告警类型、告警级别、告警数量等条件进行统计。

f） 提供故障分析和解决方案的记录以及查询功能。

5.2.4 性能管理

性能管理的目标是掌握网络资源的利用情况，并通过对各种性能参数的提取，反映网络的实际运行质量，为网络的优化运行及带宽的调整提供决策支持。

5.2.4.1 监测网络设备的性能指标

监测公安网络设备（主要是路由器、交换机）的主要性能指标：

a） CPU 负荷；

b） 工作温度；

c） 路由器的内存利用率；

d） 端口流入流量；

e） 端口流出流量；

f） 端口流入带宽使用率；

g） 端口流出带宽使用率；

h） 端口流入包平均大小；

i） 端口流出包平均大小；

j） 端口丢包率；

k） 端口误包率。

性能指标说明参见附录 A，具体性能指标的含义和标准 MIB 的定义，应符合 IETF RFC 1213、RFC 1907、RFC 2011、RFC 2012、RFC 2013、RFC 2233。

5.2.4.2 性能管理的基本功能要求

在进行网络性能监测时，系统应具备如下功能：

a） 系统内置网络维护所必需的常用性能指标表达式（其中应包含 5.2.4.1 中列出的 11 个性能指标）；

b） 提供性能指标表达式的定义工具，以便维护人员定义新的性能指标；

c） 手工设置性能采集任务的启动和停止；

d） 灵活配置性能采集时间；

e） 配置性能阈值和告警：

1） 系统可根据不同的性能指标设置不同的阈值条件，一旦指标超过阈值后自动发送性能告警。系统支持性能指标阈值/告警的批量设置和修改功能，以简化操作；

2） 系统支持“梯度”告警，即一个性能指标可根据不同的阈值条件设置不同的告警级别（如设

置 CPU 的使用率超过 50%的告警级别为“警告”，超过 70%时的告警级别为“严重”等），最多可支持 4 个不同级别的告警（告警级别见 5.2.3.2）；

3） 支持告警压缩和过滤功能，以防止系统产生过多的告警或告警误报。

f） 支持以图形方式来展现性能数据：

1） 提供实时的性能数据采集和显示功能，以曲线方式显示性能指标的采集结果，最小的采集周期为 5 s。对路由器、交换机等网络设备，支持各个端口的流量在一个图表上进行排序显示；

2） 系统以曲线、直方图、表格等显示方式对历史性能数据进行展现。支持具有历史数据显示曲线的放大和缩小功能，可查看不同时间粒度的性能数据细节。上述数据可保存为文本、超文本或者图片文件（jpg/tiff/pig/bmp）。

5.2.5 链路管理

链路管理是网络管理的重要组成部分，提供对下一级网络或其他接入线路的监视，包括通断情况，链路两端的端口配置、带宽、带宽利用率、丢包率等，并在拓扑图上显示出来。链路中应该标识接入单位的相关信息，包括单位名称、配置情况、联系人、联系电话、手机、电子邮件地址等。

链路中断的告警应该是级别最高的告警，在发生链路中断告警时，应按照设定的方式给设备维护人员发送告警信息。

系统应提供对指定链路中断时间的统计，可定制网络中断情况和可用率报表。

5.3 流量/协议分析*

网络管理系统在对设备端口的流量、丢包率、误包率等参数进行监控的基础上，对构成网络流量的协议组成、什么人在什么时间使用网络、和谁进行通信、占用多大带宽等问题进行分析。因此，网络管理系统可提供相关的流量/协议分析工具或者专用的网络探针（probe），对各级主干网上的流量进行分析，以便找出占用网络带宽的前 N 个（Top N）协议、应用和用户，及时制定相应的管理和规划策略，保障各级公安网络的正常运行和有效利用。

5.3.1 配置流量监听策略*

采用纯软件的流量分析系统，应按照其使用要求进行相关的监听策略配置。

采用专门的网络探针，则需要按照其使用要求进行接入和监听配置。

应不影响网络系统和设备的正常运行。

5.3.2 流量分析和协议分析*

通过对网络流量和使用协议的具体分析，系统可得到在一个指定的时间段内的有关网络通信流量的源 IP 地址、目的 IP 地址、TCP/UDP 常用应用协议（如 HTTP、DNS、FTP、SMTP、POP3 等）或者其他私有协议（如某个公安业务管理系统的私有数据传送协议、Vo IP 协议）等分类的统计信息。流量按照 IP 地址、通信协议等不同方式进行排序，以饼图、直方图、表格等方式展现。

在一个给定的时间段，针对某一条给定链路，系统能够展现如下的流量统计和分布信息：

a） 按照具体应用层通信协议（如 FTP、HTTP、DNS 等）的流量分布（包括具体的包数、具体流量数值和各占总流量的百分比）；

b） 对应 a）的具体通信协议的 Top N 的用户流量排行；

c） 总流量排行前 N（N 由用户指定，如 10，20，50 等）位的主机（以 IP 地址标识）；

d） 对于排行前 N 位的主机，能够统计按照协议细分的流量大小和各占总流量的百分比；

e） 对于排行前 N 位的主机，能够统计与其通信的按流量排行的前 N 台主机；

f） 流量分析显示的 IP 地址要和 IP 地址分配管理功能关联起来，以便确定该 IP 地址所对应的使用单位和个人，方便维护人员尽快辨别来源，采取处置措施。

系统提供协议登记功能，即将各种公安业务应用系统使用的 TCP/UDP 端口、私用端口、服务器 IP 地址等相关信息进行登记注册，以便在进行报文分析时能够及时了解这些应用系统的流量情况，方便应

用系统的网络流量管理和规划。

结合 5.5.2 的“服务器信息的注册管理”，本系统亦可针对新增的应用服务（假设其使用自定义的私有通信端口号），进行准确的协议和应用分类。

系统的分析功能应提供远程和本地的查看图形界面，以满足远程管理的需要。

5.3.3 流量分析统计报表*

能够提供直观、灵活、丰富的流量统计和报表显示功能。能够以多种形式（表格、饼图、直方图等）表现流量、协议分类的相关数据，根据不同的统计方式，按查询条件生成图形、表格报表。报表能够以 Web 形式访问，将多个不同的统计分析结果在同一个报表中进行对比分析。

5.4 关键服务器管理*

能够对本级管理域内公安网络上运行的关键服务器系统提供监控功能。监控的主要指标包括：

5.4.1 按时间段统计的服务器通断百分比、中断开始时间、中断结束时间、中断时长。

5.4.2 CPU、内存和磁盘空间的使用情况，在超过定义的阈值范围后发出告警。

结合 5.5.2 的服务器信息注册管理，系统可提供业务服务视图，直观展现网络链路（连接到服务器的具体交换机端口）、服务器以及服务器上部署的各种应用服务的状态。

5.5 网络运行维护业务管理*

根据各级信息网络中心的网络运行管理和维护职责，提供一些辅助管理功能，如 IP 地址分配管理、服务器信息的注册管理，并根据工作需要，自动生成、定制、发布网管业务报表。

5.5.1 IP 地址分配管理*

系统可对公安网络的 IP 地址的分配、使用进行管理，建立专门的数据库，分别存储如下的 IP 地址分类信息：

a) 对所属管理域管理对象 IP 地址分配的详细信息；

b) 下一级网的网络设备（路由器、交换机等）IP 地址；

c) 注册服务器的 IP 地址；

d) 正式注册的与使用者信息相对应的主机 IP 地址。

系统提供按输入的 IP 地址查询和分区域、分机构统计的功能，方便系统维护人员准确定位有问题的 IP 地址对应的设备，并采取相应的处置措施。

5.5.2 服务器信息的注册管理*

对运行在公安网上的各种服务器进行注册管理，对新增的服务器进行申报管理，具体的管理流程按照定期逐级申报的方式进行。服务器申报和注册的主要信息如下：

a) IP 地址：服务器的 IP 地址；

b) 服务器名称：服务器的 houseman；

c) 设备型号：服务器的设备型号；

d) 硬件配置：CPU、内存、磁盘容量等；

e) 软件配置：操作系统、安装的主要应用软件；

f) 区域信息：所属的地域及业务部门；

g) 安放位置：机器的存放位置；

h) 维护负责人：姓名及联络方式；

i) 用途：简要描述其用途，如 DNS、FTP、WEB 服务器等；

j) 提供服务的范围：如子网内、局域网内、三级网内、二级网内、一级网内等；

k) 对外服务打开的 TCP/UDP 端口号：为提供正常服务而运行的服务程序所监听的 TCP/UDP 端口号，特别是自定义的服务端口号；

l) 备注：其他额外信息。

系统提供对服务器注册信息管理所必需的增加、删除、修改、浏览、查询和报表功能。当进行流量、

协议分析时，如发现流量异常的服务器IP地址，能及时通过查找服务器注册信息数据库，定位到具体的服务器主机及管理人员，从而采取相应的处置措施。

5.5.3 网管业务报表

5.5.3.1 网管业务报表的基本要求

网管业务报表提供直观丰富的表现形式，为维护、规划和决策提供工具。报表要同时支持实时交互模式和Web显示模式。实时交互模式主要提供数据的精细分析，采用C/S方式的客户端模式；Web显示模式主要提供静态图片和表格的展示方式。

系统提供内置的报表形式和内容，也支持定制。

5.5.3.2 内置网管业务报表的种类

用于网管业务的内置报表应包括：

a) 流量报表

对管理域内的主要链路，系统提供区分流入和流出的流量报表，报表种类分为日报表、月报表以及自定义时间段的自定义报表。报表中的主要内容包括：日期，链路名称，流入流量最小值，流入流量最大值，流入流量平均值，流出流量最小值，流出流量最大值，流出流量平均值等。其中关于上述流量最大、最小和平均值的计算，系统可按照设定的时间段进行每一天的数据统计。

除表格方式外，系统还应提供以直方图、曲线图等方式展现统计和分析结果。

b) 故障报表

对管理域内的主要路由器、交换机等管理对象，系统提供此类网络设备的故障日报表、月报表以及自定义时间段的自定义报表。报表的主要内容包括：日期，设备名称，故障类型，故障级别，故障数量，故障处理时长等。

c) 网络流量/协议TOP N的统计报表*

按照TCP、UDP等应用层协议的流量进行统计，并给出Top N协议流量排行的报表。

对每一种应用协议，报表的内容应包括：应用协议名称，该协议的数据包数，该协议的数据量大小(单位：MB)，该协议的数据量占所有协议总流量的百分比等。

自定义统计时间段；Top N统计一般按数据流量由大到小的顺序排序；系统也可使用饼图、直方图等图形方式展现统计和分析结果。还可按照发送、接收数据量，统计出Top N用户流量排行报表。

报表的内容应包括：主机IP地址，数据包数，数据量大小(单位：MB)，本数据量占总流量的百分比。

d) 关键服务器运行通断状况报表

对管理域内的关键服务器，系统提供服务器通断情况的日报、月报和自定义报表，报表的主要内容应包括：日期，主机名称，主机IP地址，中断时长(单位：分钟)，接通率等。

其中，接通率的计算方式为：(统计时间段－中断时长)/统计时间段，按百分比给出。

e) 路由器/交换机工作端口的通断状况报表

对管理域内的路由器/交换机，系统提供主要链路的通断情况的日报、月报和自定义报表，报表的主要内容包括：日期，设备名称，设备IP地址，设备端口名称，链路名称，中断时长(单位：分钟)，接通率等。其中，接通率的计算方式为：(统计时间段－中断时长)/统计时间段，按百分比给出。

以上各类报表根据需要，可定期生成和发布，也可通过电子邮件、FTP或者HTTP方式报送。

5.5.3.3 定制报表

在常规内置报表的基础上，按照不同的时间段、条目、条件进行组合，生成需要的定制报表。

6 网络管理系统的技术要求

6.1 数据结构定义

6.1.1 拓扑数据结构

在网管数据库中，需要存储和管理以下7种类型的拓扑数据对象，如表2所示。为了表现网管数据

库中拓扑数据的对象层次和包含关系，需要额外的对象 ID 和父对象 ID 来表达此种父子关系。

表 3 描述了路由器/三层交换机/二层交换机的属性和数据结构。

表 4 描述了主机的属性和数据结构。

表 5 描述了接口/端口的属性和数据结构。

表 6 描述了 IP 地址的属性和数据结构。

表 7 描述了子网的属性和数据结构。

表 8 描述了链路的属性和数据结构。

表 2　对象类型定义表

对象类型	类型标识
路由器/3 层交换机	1
子网	2
二层交换机	3
主机	4
端口	5
IP 地址	6
链路	7

表 3　路由器/三层交换机/二层交换机的数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	对象 ID	整型	4	从 1 开始的对象标识序号
2	父对象 ID	整型	4	本对象的直接父对象的标识序号，用来表达层次上的父子关系
3	设备名称	字符串	128	设备的标识名称
4	IP 地址	字符串	15	按 A. B. C. D 方式标识的主机 IP 地址
5	告警状态	整型	2	设备当前的实际告警状态
6	厂商名称	字符串	64	厂商的名称描述
7	设备型号	字符串	64	型号描述
8	硬件配置	字符串	255	硬件配置的简要描述
9	软件配置	字符串	255	软件配置的简要描述
10	备注	字符串	255	其他的描述信息

表 4　主机的数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	对象 ID	整型	4	从 1 开始的对象标识序号
2	父对象 ID	整型	4	本对象的直接父对象的标识序号，用来表达层次上的父子关系
3	主机名称	字符串	64	主机的 hostname
4	IP 地址	字符串	15	按 A. B. C. D 方式标识的主机 IP 地址
5	告警状态	整型	2	设备当前的实际告警状态
6	厂商名称	字符串	64	厂商的名称描述
7	设备型号	字符串	64	型号描述

表 4(续)

序号	数据项名称	类型	长度(字节)	说　明
8	硬件配置	字符串	255	硬件配置的简要描述
9	软件配置	字符串	255	软件配置的简要描述
10	备注	字符串	255	其他的描述信息

表 5　接口/端口的数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	对象 ID	整型	4	从 1 开始的对象标识序号
2	父对象 ID	整型	4	本对象的直接父对象的标识序号,用来表达层次上的父子关系
3	端口名称	字符串	64	接口、端口的名称描述
4	端口索引	整型	2	SNMP MIB-Ⅱ(详细 MIB 定义参见规范性引用文件 1—RFC1213)中的 IF_INDEX,用来唯一地标识该端口
5	端口管理状态	整型	2	端口当前的可管理状态。1:UP,2:DOWN,3:TESTING
6	端口状态	整型	2	端口当前的实际工作状态。1:UP,2:DOWN
7	端口类型	字符串	64	端口的类型描述,SNMP MIB-Ⅱ中的 IF_TYPE
8	端口 MTU	字符串	12	端口传输包的最长字节数
9	端口速率	整型	4	以比特/秒为单位的端口理论带宽
10	端口物理地址	字符串	64	端口的物理地址,如以太网端口的 MAC 地址
11	备注	字符串	255	其他的描述信息

表 6　IP 地址的数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	对象 ID	整型	4	从 1 开始的对象标识序号
2	父对象 ID	整型	4	本对象的直接父对象的标识序号,用来表达层次上的父子关系
3	IP 地址	字符串	15	按 A. B. C. D 方式标识的 IP 地址
4	子网掩码	字符串	15	按 A. B. C. D 方式标识的本 IP 地址的子网掩码
5	端口索引	整型	2	定义本 IP 地址的端口索引

表 7　子网的数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	对象 ID	整型	4	从 1 开始的对象标识序号
2	父对象 ID	整型	4	本对象的直接父对象的标识序号,用来表达层次上的父子关系
3	子网 ID	字符串	15	按 A. B. C. D 方式标识的子网地址
4	子网掩码	字符串	15	按 A. B. C. D 方式标识的子网掩码

表 8　链路的数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	对象 ID	整型	4	从 1 开始的对象标识序号
2	父对象 ID	整型	4	本对象的直接父对象的标识序号,用来表达层次上的父子关系

表 8(续)

序号	数据项名称	类型	长度(字节)	说　明
3	链路名称	字符串	64	链路的名称描述
4	起始端点对象 ID	整型	4	链路的起始端点对象 ID,如路由器、交换机、主机等。
5	终止端点对象 ID	整型	4	链路的终止端点对象 ID,如路由器、交换机、主机等。
6	起始端口索引	整型	2	起始设备端口的 SNMP IF_INDEX
7	终止端口索引	整型	2	终止设备端口的 SNMP IF_INDEX
8	备注	字符串	255	其他的描述信息

6.1.2 告警信息数据结构

网络管理系统中存储当前告警数据和历史告警数据。当前告警是网络管理系统接收到尚未进行人工处理的告警信息,而历史告警则是经过故障处理,由网络维护人员确认和删除的告警信息。两者的数据结构分别由表 9、表 10 定义。

表 9　当前告警数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	告警序号	整型	4	从 1 开始的告警序号
2	网元类别	整型	2	设备类型
3	告警状态	整型	2	当前告警的实际状态
4	告警源 IP 地址	字符串	15	告警设备的 IP 地址
5	告警类型名称	字符串	64	告警的实际类型
6	告警发生时间	日期		告警发生的时间
7	告警级别	整型	2	告警的级别
8	告警描述	字符串	64	告警信息的简要描述
9	告警详细信息	字符串	255	告警信息的详细描述
10	告警值	字符串	64	告警时的测量值
11	确认人姓名	字符串	30	确认告警维护人员姓名
12	确认时间	日期		确认告警的时间

表 10　历史告警数据结构表

序号	数据项名称	类型	长度(字节)	说　明
1	告警序号	整型	4	从 1 开始的告警序号
2	网元类别号	整型	2	设备类型
3	告警状态	整型	2	当前告警的实际状态
4	告警源 IP	字符串	15	告警设备的 IP 地址
5	告警类型名称	字符串	64	告警的实际类型
6	告警发生时间	日期		告警发生的时间
7	告警级别	整型	2	告警的级别
8	告警描述	字符串	64	告警信息的简要描述
9	告警详细信息	字符串	255	告警信息的详细描述
10	告警处理结果			告警的处理情况说明

表 10(续)

序号	数据项名称	类型	长度(字节)	说　明
11	告警值	字符串	64	告警时的测量值
12	确认人姓名	字符串	30	确认告警维护人员姓名
13	确认时间	日期		确认告警的时间
14	删除人姓名	字符串	30	删除告警维护人员姓名
15	删除时间	日期		删除告警的时间

6.2 接口要求

6.2.1 上下级网络管理系统拓扑数据接口

上级网络管理系统可有选择地浏览下级网络的拓扑图。为此,下级网络管理系统应按本规范约定的接口方式将拓扑图信息传给上级网络管理系统。接口方式有三种:

第一种方式,下级网络管理系统采用网络管理平台提供的功能,将本级管理中心的网络管理工作站配置为上一级管理中心的采集工作站,本地的网络管理工作站将它发现的拓扑数据传送给上一级网络管理工作站。

第二种方式,网络管理系统按照规定的数据格式将拓扑图数据打包成文件,然后再传给上级网络管理系统,并由上级网络管理系统接收后存入本地数据库。

第三种方式则是通过 WEB 方式,远程访问下级网络管理系统的拓扑图,系统应设置相应的访问权限,以防非法用户的访问。

具体的接口方式、协议和数据格式在各级网管系统实施时,由上级网管系统决定下级网管系统的接口方式和内容。

6.2.2 网络管理系统与应用服务器的接口

公安网络中的各种大型业务应用系统也是公安信息网络管理系统监测管理的对象,这些系统的应用服务器应为网络管理系统预留接口,以便对其进行管理。这些接口一般包括:告警发送接口,配置、日志、性能数据采集接口等。

6.3 系统运行环境

在部署网络管理系统时,应将网络管理系统的服务器和部分客户端机器放置在一个专门的管理网段中(如一个 C 类或更小的网段);同时在路由器、交换机上配置 SNMP 协议时,应结合访问控制措施(ACL),将使用 SNMP 协议访问路由器和交换机的权限限制在安装网络管理软件的管理子网,或者限制在某几台网络管理服务器和客户端的 IP 地址上。典型的配置可参考图 3。

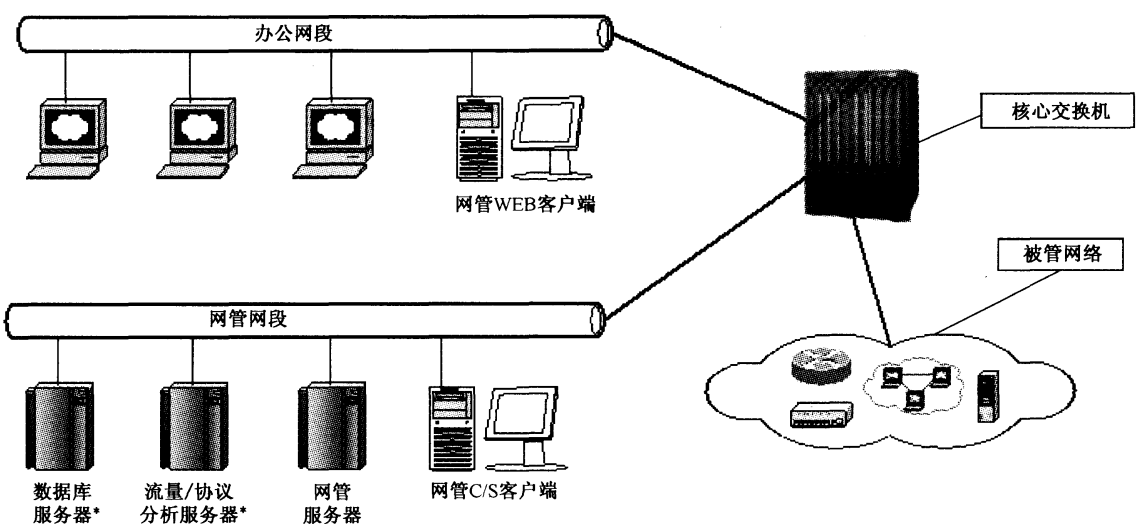

图 3　网络管理系统部署结构图

6.3.1 硬件平台要求

a) 性能价格比高，具有通用性、可升级性和可扩展性；

b) 运算速度和存储容量等性能指标满足网络管理的要求；

c) 硬件系统采用模块组合结构，以保证系统功能、处理器及储存容量的扩展。

服务器硬件可选用高性能的 PC 服务器或者 UNIX 小型机。服务器应具有容错功能。按实际情况和投资规模，系统可采用镜像容错、双机容错、RAID 磁盘阵列等措施保证系统的可靠性。磁盘容量的配置能够保证存储 1～3 年的网管业务数据量。

6.3.2 软件平台要求

a) 系统安全可靠，兼容性好，模块化设计，具有较高的性能；

b) 服务器可采用主流的 Linux 或 UNIX 操作系统；

c) 网络管理客户端可采用基于 Windows 系统的高性能 PC。

6.3.3 数据库

网络管理系统采用的数据库系统符合 ANSI SQL92 标准，单个数据库能够支持 2GB 以上的数据库容量。

6.4 显示界面设计规范

公安信息网络管理系统的显示界面主要采用 Web 页面和普通 Windows 客户端两种形式。显示界面作为系统信息展示的平台以及用户和系统进行交互的中介，总体的要求是界面风格统一、简洁、针对性强、使用方便，能够体现出公安业务的特色。

下面针对两个不同形式的界面提出其具体设计规范。

6.4.1 Web 页面布局规范

Web 界面的设计主要包含图 4 所示的几个功能区：

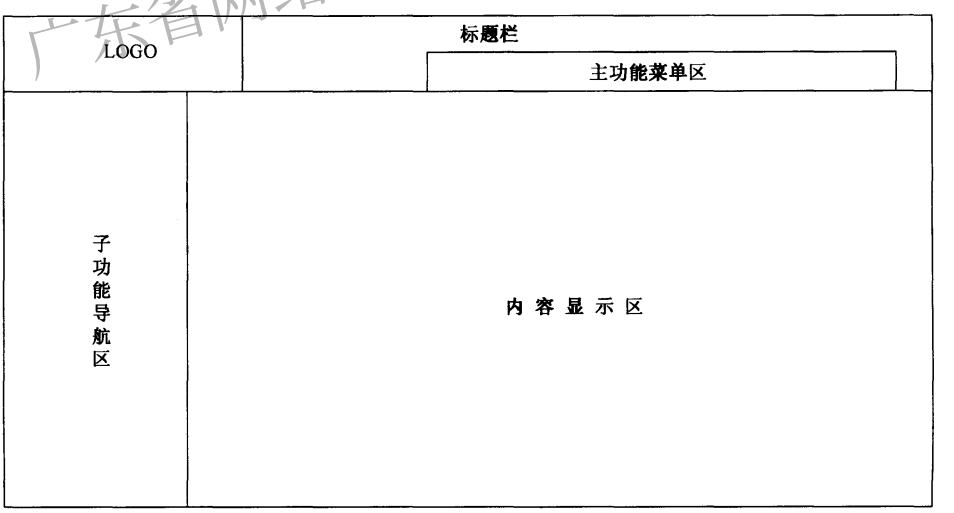

图 4 WEB 页面布局格式示意图

a) LOGO(徽标)区：位于页面左上角，可放置警徽图片或者公安机关的名称，大小随页面自动控制；

b) 标题栏区：位于页面右上部，可以放置背景图片以及相关的系统功能标题文字；

c) 主功能菜单区：浮在标题栏区的中下部，为系统的主功能菜单；

d) 子功能导航区：位于页面左侧，为选择的系统主功能的子功能导航菜单；

e) 内容显示区：位于页面右下部，默认情况占据较大比例的页面空间，用于向用户展示信息并提供交互接口。

6.4.2 普通客户端界面设计规范

普通客户端界面的设计主要包括：菜单设计、工具栏设计和功能区设计。建议具体的设计规范包括：

a) 菜单设计：菜单应提供客户端的全部的操作选择，且将同类型的菜单项收入统一个菜单中，每个菜单项除了中文名称外，还需提供用大写英文字母标识的快捷键；

b) 工具栏设计：工具栏一般放置较为常用的功能对应的按钮控件或其他控件，图标意义清晰明确，同类型控件相邻摆放；

c) 功能区设计：功能区涉及控件较多，除满足总体上控件摆放整齐、有序外，具体控件的要求和Windows界面控件设计要求类似。

6.5 系统性能要求

a) 支持的终端数：最多可有10个网络管理终端同时运行；

b) 支持的同时操作的用户数：不小于10个并发用户，非并发用户不作限制；

c) 各级网络管理系统对本地的原始性能、告警等数据应至少保留1年；

d) 上级网络管理系统对下一级网络管理系统的性能、告警等数据应至少保留六个月；

e) 设备最小轮询周期为5 min；

f) 告警峰值处理能力600条/min。

6.6 系统安全性要求

公安信息网络管理系统提供基于用户组的访问控制功能，对用户权限的管理通过对用户组的授权来实现。因此，系统对安全性的要求主要包括用户角色管理(用户组的划分)和用户权限设置两个方面。

6.6.1 用户角色管理

公安信息网络管理系统根据用户职能的不同将系统中的用户划分为三种角色，每种角色对应不同的权限。这三种角色是：

a) 系统管理员：系统管理员负责系统的总体管理，具有最高权限，可根据需要对系统的配置和功能进行调整；

b) 一般网络管理员：一般网络管理员负责公安信息网络管理系统的日常维护和局部管理，在其负责的区域内根据需要可对系统的部分配置和功能进行调整，其权限比系统管理员小，监控的范围和对象有限；

c) 普通网络用户：普通网络用户只能享受系统对其开放的功能，无权更改系统的任何配置和功能，权限最低。

6.6.2 用户权限管理

用户权限是指用户对系统提供功能的执行权利，公安信息网络管理系统需要设置如下的功能执行权限：

a) 数据管理的权限：管理数据查询、增加、修改和删除的权限；

b) 网元管理的权限：对网络管理设备的操作权限；针对不同的网络设备发送控制命令的权限限制；

c) 用户资料管理的权限：用户查询、增加用户、修改用户资料、删除用户资料的权限；

d) 网络管理系统功能模块的使用权限；

e) 系统用户通过WEB访问网络管理系统的权限。

6.6.3 网络设备管理权限

a) 关于路由器、交换机的SNMP读写口令(特别是set community name)，应只有负责设备维护的网络管理员掌握，以保证安全；

b) 为确保网管系统的安全，在路由器、交换机上配置SNMP协议时，应同时结合访问控制措施(ACL)，将使用SNMP协议访问路由器和交换机的权限限制在安装网络管理软件的管理子网或者某几台网络管理服务器和客户端的IP地址。

6.7 系统可靠性要求

公安信息网络管理系统的可靠性要求包括：

a) 保证核心系统(软件、硬件和操作系统)在99.9%的时间内都能够正常运作；

b) 系统应能7×24小时连续不断工作；

c) 网络管理服务器应采用相应的机制，以保证服务器故障不影响和少影响信息采集。

附 录 A
（资料性附录）
监测网络设备的性能指标说明

监测网络设备的性能指标说明见表 A.1。

表 A.1 监测网络性能指标说明表

性能指标名称	性能指标说明
路由器温度(*)	路由器板卡温度传感器的读数。根据不同厂商不同型号的产品，按照厂商的技术指标，确定各个板卡的安全工作温度范围
路由器 5 minCPU 利用率（*）	路由器 5 min 内的平均 CPU 利用率 。一般来讲，CPU 的使用率在 60%以下时，设备可以正常工作，一般不会影响网络性能。一旦该指标超过 60%，就需要引起维护人员的注意，此时需要查看丢包率指标，以确认是该设备否有丢包的现象出现
路由器的空闲内存量（*）	在数据采集时刻路由器的空闲内存量(以 KB 为单位) 应当保证系统在忙时有 30%以上的空闲内存
SNMP 流出包数	单位时间内(每秒)流出设备的 SNMP 包数
SNMP 流入包数	单位时间内(每秒)流入设备的 SNMP 包数
带宽	单位时间(秒)内流出和流入接口/端口的比特数(bits/s)
带宽利用率	流入和流出的流量与端口理论速率的百分比
端口丢包率	在采集周期内丢弃的流入和流出包数占所有流入和流出包数的百分比
端口误包率	在采集周期内错误的流入和流出包数占所有流入和流出包数的百分比
流出包平均大小	在采集周期内流出数据包的平均大小(单位:字节)。如果该指标数值过小(如<128)，需要使用其他的工具(如病毒检测、入侵检测、抓包分析等)诊断为何网络上传输大量过小的数据包
流出错包率	在采集周期内由于数据包格式错误而被丢弃的流出包数占所有流出包数的百分比。正常情况下，此值应为 0。否则，需要诊断设备端口以及与它相连的对端设备端口是否正常工作。错包率应当控制在 5%之内，否则会影响网络的整体性能
流出错包数	单位时间内(每秒)流出端/接口的错误包数
流出带宽	单位时间(每秒)内流出接口/端口的比特数(bits/s)
流出带宽利用率	流出流量与端口理论速率的百分比 。当带利用率在 50%以下时，系统一般是安全的。一旦该指标超过 50%时，需要关注丢包率、CPU 利用率指标，以确认系统是否能够正常工作，而没有丢包发生
流出丢包率	在采集周期内由于 CPU 过于繁忙或者内存不足等原因而被丢弃的流出包数占所有流出包数的百分比。当丢包率>0 时，需要查看带宽利用率、CPU 使用率、内存空闲率等指标，以确认设备是否正常工作。正常情况下，此值应为 0。丢包率应当控制在 5%之内，否则会影响网络的整体性能
流出丢包数	单位时间内(每秒)流出端/接口的丢弃包数
流入错包率	在采集周期内由于数据包格式错误而被丢弃的流入包数占所有流入包数的百分比

表 A.1(续)

性能指标名称	性能指标说明
流入错包数	单位时间内(每秒)流入端/接口的错误包数。正常情况下,此值应为 0。否则,需要诊断本设备端口以及与它相连的对端设备端口是否正常工作
流入带宽	单位时间(每秒)内流入接口/端口的比特数(bits/s)
流入带宽利用率	流入流量与端口速率的百分比。当带利用率在 50%以下时,系统一般是安全的。一旦该指标超过 50%时,需要关注丢包率、CPU 利用率指标,以确认系统是否能够正常工作,而没有丢包发生
流入包平均大小	在采集周期内流入数据包的平均大小(单位:字节)。如果该指标数值过小(如<128),需要使用其他的工具(如病毒检测、入侵检测、抓包分析等)诊断为何网络上传输大量过小的数据包
流入丢包率	在采集周期内由于 CPU 过于繁忙或者内存不足等原因而被丢弃的流入包数占所有流出包数的百分比。当丢包率>0 时,需要查看带宽利用率、CPU 使用率、内存空闲率等指标,以确认设备是否正常工作。正常情况下,此值应为 0。丢包率应当控制在 5%之内,否则会影响网络的整体性能
流入丢包数	单位时间内(每秒)流入端/接口的丢弃包数
注:(*)标注的技术指标应依赖设备厂商的私有 MIB 支持。	

附 录 B
（规范性附录）
各级网络管理系统的功能

各级网络管理系统由于其所处的地位和作用不同，它们所具备的功能也不完全相同，表 B.1 给出了各级网络管理相同所应具备的和可以根据实际需要进行选择的功能（所有功能均来自本规范的第 5 章）。

表 B.1 各级网络管理系统的功能

	必备功能	可选功能
一级网网络管理系统	5.2.1 拓扑管理 5.2.2 配置管理 5.2.3 故障管理 5.2.4 性能管理 5.2.5 链路管理 5.3 流量/协议分析 5.5.3 网管业务报表	5.4 关键服务器管理 5.5.1 IP 地址分配管理 5.5.2 服务器信息的注册管理
二级网网络管理系统	5.2.1 拓扑管理 5.2.2 配置管理 5.2.3 故障管理 5.2.4 性能管理 5.2.5 链路管理 5.5.3 网管业务报表	5.3 流量/协议分析 5.4 关键服务器管理 5.5.1 IP 地址分配管理 5.5.2 服务器信息的注册管理
三级网网络管理系统	5.2.1 拓扑管理 5.2.2 配置管理 5.2.3 故障管理 5.2.4 性能管理 5.2.5 链路管理 5.5.3 网管业务报表	5.3 流量/协议分析 5.4 关键服务器管理 5.5.1 IP 地址分配管理 5.5.2 服务器信息的注册管理

附 录 C
（规范性附录）
各级网络管理系统性能采集指标和采集周期

各级网络管理系统根据实际的管理需求，确定自己所需的采集指标和采集周期。建议各级网络管理系统采集的指标和采集周期如表 C.1 所示。

表 C.1 各级网络管理系统性能采集指标和采集周期

	性能指标	采集周期（为 5 min 的倍数）
一级网网络管理系统	(1) CPU 负荷*	(1) ≥5 min
	(2) 工作温度*	(2) ≥5 min
	(3) 路由器的内存利用率*	(3) ≥10 min
	(4) 端口流入流量	(4) ≥5 min
	(5) 端口流出流量	(5) ≥5 min
	(6) 端口流入带宽使用率	(6) ≥5 min
	(7) 端口流出带宽使用率	(7) ≥5 min
	(8) 端口流入包平均大小*	(8) ≥10 min
	(9) 端口流出包平均大小*	(9) ≥10 min
	(10) 端口丢包率	(10) ≥5 min
	(11) 端口误包率	(11) ≥5 min
二级网网络管理系统	(1) CPU 负荷*	(1) ≥5 min
	(2) 工作温度*	(2) ≥5 min
	(3) 路由器的内存利用率*	(3) ≥10 min
	(4) 端口流入流量	(4) ≥5 min
	(5) 端口流出流量	(5) ≥5 min
	(6) 端口流入带宽使用率	(6) ≥5 min
	(7) 端口流出带宽使用率	(7) ≥5 min
	(8) 端口流入包平均大小	(8) ≥10 min
	(9) 端口流出包平均大小	(9) ≥10 min
	(10) 端口丢包率	(10) ≥10 min
	(11) 端口误包率	(11) ≥10 min
三级网网络管理系统	(1) CPU 负荷*	(1) 0 min
	(2) 工作温度*	(2) 0 min
	(3) 路由器的内存利用率*	(3) 0 min
	(4) 端口流入流量	(4) ≥10 min
	(5) 端口流出流量	(5) ≥10 min
	(6) 端口流入带宽使用率	(6) ≥10 min
	(7) 端口流出带宽使用率	(7) ≥10 min
	(8) 端口流入包平均大小	(8) 0 min
	(9) 端口流出包平均大小	(9) 0 min
	(10) 端口丢包率	(10) ≥10 min
	(11) 端口误包率	(11) ≥10 min

注 1：采集周期为 0 分钟的指标为不作采集要求的指标。

注 2：* 标识的性能指标为可选择采集的指标。

说明：

1. 各种采集指标的选择取决于各级管理人员对网络管理系统的需求，需要综合分析各种需求以确定进行何种指标的数据采集。

2. 采集周期的选择取决于各级管理人员对数据采集精度的要求，采集周期越短，数据精度越高。

3. 采集周期的选择也受网络物理带宽和单个采集域内被管网络设备数量多少的影响，通常当物理带宽≥100 M 时，采集周期的选择可以不考虑其实际网络带宽的影响；当物理带宽≤4 M，则需要考虑采集周期对网络实际带宽的影响，此时需要综合分析进行数据采集设备的数量、采集工作站在网络中的物理位置和实际的采集周期，进行相关的实验（主要确定 SNMP 数据采集对实际网络带宽的影响）后再确定一个合适的采集周期（通常采集周期≥10 min）。

4. 关于各个采集指标告警门限值的设置

a) CPU 负荷：≥50%时开始告警；

b) 工作温度：根据设备技术指标确定合适的告警门限值；

c) 路由器的内存利用率：≥70%时开始告警；

d) 端口流入流量：不设置，可以使用 6.6 指标进行设置；

e) 端口流出流量：不设置，可以使用 6.7 指标进行设置；

f) 端口流入带宽使用率：≥60%时开始告警；

g) 端口流出带宽使用率：≥60%时开始告警；

h) 端口流入包平均大小：≤256 时开始告警；

i) 端口流出包平均大小：≤256 时开始告警；

j) 端口丢包率：≥1%时开始告警；

k) 端口误包率：≥1%时开始告警。

GA/T 608-2006

*

书号：155066・2-17010

定价： 15.00 元