YD

中华人民共和国通信行业标准

YD/T 1170—2001

IP 网络技术要求—网络总体

IP Network Technical Requirements—Network General

广东省网络空间安全协会受控资料

2001-12-11 发布　　2001－12－11 实施

中华人民共和国信息产业部　发布

目　　次

山东省网络空间安全协会受控资料

广东省网络空间安全协会受控资料

前　　言

本标准主要参考我国相关标准、国际电信联盟 ITU-T 相关建议以及 RFC 文档编制。

本标准是 IP 网络技术要求系列标准中的网络总体部分。

本标准主要规定了我国 IP 网络的网络结构和网络组织原则、业务分类、寻址要求、IP 网传输层要求、IP 城域网基本要求、网络性能和服务质量要求、网络管理和安全要求、网络互通要求、计费和结算要求、同步要求、主要组网设备基本要求等。

本标准适用于我国 IP 网络的规划和建设，同时也适用于相关设备的研制、开发和技术引进。

本标准由信息产业部电信研究院提出并归口。

本标准起草单位：　信息产业部电信传输研究所
　　华为技术有限公司

本标准主要起草人：石友康　赵慧玲　叶　华　高　兰　王　玮

广东省网络空间安全协会受控资料

中华人民共和国通信行业标准

IP 网络技术要求—网络总体

IP Network Technical Requirements—Network General **YD/T 1170—2001**

1 范围

本标准主要规定了我国 IP 网络的网络结构和网络组织原则、业务分类、寻址要求、IP 网传输层要求、IP 城域网基本要求、网络性能和服务质量要求、网络管理和安全要求、网络互通要求、计费和结算要求、同步要求、主要组网设备基本要求等。

本标准适用于我国 IP 网络的规划和建设，同时也适用于相关设备的研制、开发和技术引进。

2 引用标准

下列标准包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

YD/T 1044-2000	IP 电话/传真业务总体技术要求
YD/T 1045-2000	网络接入服务器（NAS）技术规范
YD/T 1061-2000	同步数字体系（SDH）上传送 IP 的 LAPS 技术要求
YD/T 1071-2000	IP 电话网关设备技术要求
YD/T 1096-2001	路由器设备技术规范——低端路由器
YD/T 1097-2001	路由器设备技术规范——高端路由器
YD/T 1099-2001	千兆比特以太网交换机技术规范
YD/T 1109-2001	ATM 交换机技术规范（代替 YDN067-1997）
YD/T 1151-2001	新业务技术要求——多媒体信息检索
YD/T 1163-2001	IP 网络安全技术要求——安全框架
YD/T 1148-2001	网络接入服务器（NAS）技术规范——宽带接入服务器
YDC 003-2001	软交换设备技术规范
YD/T 1162.1-2001	多协议标记交换（MPLS）总体技术要求
YD/T 1171-2001	IP 网络技术要求——网络性能参数与指标
YD/T 1149-2001	IP 网络技术要求——计费
YDN 077-1998	中国公众多媒体通信网技术体制（暂行规定）
YDN 099-1998	光同步传送网技术体制（暂行规定）
YDN 120-1999	光波分复用系统总体技术要求
IEEE802.3z(1998)	千兆比特以太网标准（1000Base-LX/1000Base-SX）
IEEE802.3ab(1999)	用于操作在 4 对 5 类线平衡铜缆上的 1000BASE-T 物理层参数和规范
IEEE802.1P(1998)	局域网和城域网标准—对媒体接入控制（MAC）桥接的补充：业务量等级预测及动态多播过滤
IEEE802.1Q(1998)	虚拟桥接局域网(VLAN)
ITU-T E.164（1993）	国际公用电信编号计划

广东省网络空间安全协会受控资料

中华人民共和国信息产业部 2001-12-11 批准 2001-12-11 实施

ITU-T I.321（1991）	B-ISDN 协议参考模型及其应用
ITU-T I.361（1993）	ATM 层技术规范
ITU-T I.731(1996)	ATM 设备种类和一般特性
ITU-T I.732 (1996)	ATM 设备功能特性
ITU-T G.711(1988)	话音频率的脉冲编码调制
ITU-T G.723.1(1996)	以 5.3kbit/s 和 6.3kbit/s 为速率的多媒体通信的双速语音编码器
ITU-T G.728(1992)	采用线形预测激励的低时延码在 16 kbit/s 速率上的语音编码
ITU-T G.729(1996)	运用共轭结构代数码线形预测激励的 8kbit/s 语音编码
ITU-T G.826(1999)	等于或高于基本速率的国际、恒定比特率数字通路误差性能参数和目标
ITU-T H.323(1999)	基于分组的多媒体通信系统
ITU-T H.245(1998)	多媒体通信的控制协议
ITU-T H.261(1998)	用于速率为 p × 64kbit/s 可视业务的视频编码
ITU-T H.263（1998）	用于低比特速率通信的视频编码
ITU-T T.30(1998)	文件传真在公用电话交换网上的传输规程
ITU-T T.38(1998)	三类终端间通过 IP 网络的实时通信的规程
ITU-T T.101(1987)	可视图文业务的国际互通
ITU-T T.120（1996）	用于多媒体会议的数据协议
ITU-T T.136（1999）	远端设备控制应用协议
ITU-T X.29(1993)	用于分组装/拆（PAD）设备和分组方式 DTE 或另一 PAD 设备之间交换控制信息和用户数据的规程
ITU-T Y.1541（2001）	互联网协议通信业务—IP 性能目标
RFC1392	互联网用户词汇表
RFC1519	无类域间路由选择(CIDR):地址分配及拥塞策略
RFC1661	点到点协议(PPP)
RFC1662	HDLC 帧中的 PPP
RFC1701	一般选路封装
RFC1702	IPv4 网络上的一般选路封装
RFC1755	ATM 上支持 IP 的 ATM 信令
RFC1757	远程网络监控 MIB
RFC1771	边缘网关协议第 4 版本（BGP4）
RFC2138	RADIUS 协议
RFC2139	RADIUS 计费协议
RFC2236	互联网组管理协议 IGMP（版本 2）
RFC2328	开放式最短路径优先（版本 2）
RFC2453	路由信息协议 RIP（版本 2）
RFC2460	互联网协议—第六版（IPv6）规范

广东省网络空间安全协会受控资料

3 定义及缩略语

3.1 定义

本标准应用了下列定义。

1) 路由器（Router）

路由器是通过转发数据包来实现网络互连的设备。路由器可以支持多种协议（例如：TCP/IP 等），可以在多个层次上转发数据包（例如：数据链路层，网络层，应用层）。

路由器需要连接两个或多个由 IP 子网或无编号点到点线路标识的逻辑端口，至少拥有一个物理端口。路由器根据收到的数据包中网络层地址以及路由器内部维护的路由表，选择下一跳路由器或主机(最后一跳时)的地址和相关接口，并重写链路层数据包头。

路由表必须动态维护以反映当前的网络拓扑。路由器通常通过与其他路由器交换路由信息来完成路由表的动态维护。

路由器只提供数据包传输服务。为实现路由选择的灵活性和鲁棒性（Robust），路由器应尽量减少必要的状态信息以维持数据包传输服务。

2) 高端路由器

通常位于网络骨干层，用作扩大互联网的路由处理能力和传输带宽的路由器。

3) 边缘路由器

边缘路由器一般位于网络边缘，通过转发数据包来实现连接骨干网与二级网的路由器。

4) 软交换设备（SoftSwitch）

软交换设备是电路交换网向分组网演进的核心设备，也是下一代电信网络的重要设备之一，它独立于底层承载协议，主要完成呼叫控制、资源分配、协议处理、路由、认证、计费等主要功能，并可以向用户提供现有电路交换机所能提供的所有业务以及第三方业务。

5) 媒体网关(Media Gateway)

媒体网关将一种网络中的媒体转换成另一种网络所要求的媒体格式。例如：媒体网关能够在电路交换网的承载通道和分组网的媒体流之间进行转换；可以处理音频、视频或者 T.120 数据，也可以具备处理这三者的任意组合的能力；能够进行全双工的媒体翻译，可以演示视频/音频消息；可以实现其他交互式语音应答（IVR）功能，也可以进行媒体会议等。

6) 接入服务器

接入服务器通常位于公用电话网（PSTN/ISDN）与 IP 网之间，是将拨号用户接入 IP 网的网络服务器。

7) 宽带网络接入服务器

宽带网络接入服务器位于骨干网的边缘层，作为用户接入网和核心业务网之间的网关，终结来自用户接入网的连接（主要是高速的用户接入网），提供接入到宽带核心业务网（主要为 IP 网和 ATM 网）的服务。

8) IP 电话(IP Telephony)

在 IP 网上传送的具有一定服务质量的语音业务。

9) IP 电话网关(Gateway)

IP 电话网关是 IP 电话网的接入设备，它位于电路交换网与 IP 网之间，为用户提供 IP 电话业务。

10) RADIUS 协议

RADIUS 是网守或接入服务器与认证/计费中心之间授权（Authorization）、认证（Authentication）和计费（Accounting）的标准协议。

11) SNMP(Simple Network Management protocol)

SNMP 是 IP 网络的网络管理的标准协议。

12) IP 宽带城域网

IP 宽带城域网是基于宽带技术，以电信网络的可管理性、可扩充性为基础，在城市范围内汇聚宽、窄带用户的接入，面向满足集团用户（政府、企业等）、个人用户对各种宽带多媒体业务（互联网访问、虚拟专用网等）需求的综合宽带网络，是电信网络的重要组成部分，向上与一级骨干网络或二级网络互连。

13) 千兆比以太网第 2 层交换机

广东省网络空间安全协会会议资料

千兆比以太网交换机通常大多数端口是千兆比以太网接口，位于网络中心，用于连接多个以太网或者高性能服务器。第 2 层交换机除应实现网桥相应功能外还应实现 VLAN 等功能。千兆比以太网第 2 层交换机必须实现逻辑链路层功能、 数据帧转发功能、 数据帧过滤功能以及维护决定数据帧转发及过滤的信息。

14) 千兆比以太网第 3 层交换机

千兆比以太网第 3 层交换机是拥有第 3 层路由功能的以太网交换机。除实现数据帧转发功能外，第 3 层交换机能根据收到的数据包中网络层地址以及交换机内部维护的路由表决定输出端口以及下一跳交换机地址或主机地址并且重写链路层数据包头。

第 3 层交换机路由表必须动态维护来反映当前的网络拓扑。

第 3 层交换机通常通过与其他交换机或 3 层交换机交换路由信息来完成路由表的动态维护。

15) ATM 交换机设备

ATM 交换机是网络节点设备，其相关的协议参考模型和分层功能应与 ITU-T 建议 I.321 一致，其功能特性应符合 ITU-T 建议 I.731 和 I.732 的要求。通常，ATM 交换机功能分成下述三大部分：

1）连接功能：建立 VP 和 VC 连接，具有交换和传送机制；

2）控制功能：控制业务和虚连接，具有信令、路由选择和连接、资源分配处理等功能；

3）操作、维护、监视、测量和网络管理功能。

3.2 缩略语

本标准使用了下列缩略语：

ANSI	美国国家标准研究所
ADSL	非对称数字用户线路
APON	ATM 无源光网络
APS	自动保护切换
ARP	地址解析协议
AS	自治系统
ATM	异步转移模式
BGP	边界路由协议
CHAP	握手认证协议
CIDR	无类域间路由选择
CIPOA	ATM 上支持传统 IP 及地址解析协议
CLP	信元丢失率
CGI	公共网关接口
DCN	数字电路网
DDN	数字数据网
DNS	域名服务器
DWDM	密集型波分复用
ECP	保密控制协议
EGP	外部路由协议
FCS	帧校验序列
FDDI	基于光纤的分布数据接口
FIB	转发信息表
FTP	文件传输协议
GRE	通用路由封装
HDLC	高级数据链路控制协议

广东省网络空间安全协会受控资料

HFC	光纤铜轴混合网
HTTP	超文本传输协议
HTML	超文本标识语言
ICMP	互联网消息协议
ICP	互联网内容提供商
IGMP	互联网组消息协议
IGP	内部路由协议
IOTP	互联网开放贸易协议
IP	互联网协议
IPv4	互联网协议—第 4 版
IPv6	互联网协议—第 6 版
IPCP	IP 控制协议
IS-IS	中间系统—中间系统
ISP	互联网业务提供商
JPEG	联合图像专家组
JBIG	联合两级图像专家组
L2F	第 2 层发送协议
L2TP	第 2 层隧道协议
LAN	局域网
LAPS	链路接入协议—SDH
MPEG	活动图像专家组
MPLS	多协议标记交换
NAS	网络接入服务器
NCP	网络控制协议
NHRP	下一跳路由协议
NIC	网络接口卡
NOC	网络运行中心
NTP	网络时间协议
O&M	运行与维护
OSPF	开放最短路径优先
PAP	密码认证协议
PHB	每一跳行为
PKI	公共密钥基础设施
PSTN	公用电话交换网
PON	无源光网络
PoS	SDH 上传送 IP
PPTP	点到点隧道协议
PPP	点到点协议
PVC	永久虚拟连接
QoS	服务质量
RADIUS	拨号用户远程认证服务
RTP	实时协议
RSVP	资源预留协议

广东省网络空间安全协会受控资料

TRCP	实时控制协议
SDH	同步数字体系
SET	安全电子交易
SLA	业务等级协商
SMTP	简单邮件传送协议
SNMP	简单网络管理协议
TCP	传输控制协议
ToS	服务类型
TTL	生存时间
UDP	用户数据包协议
URL	统一资源标识符
VLAN	虚拟局域网
VPN	虚拟专用网
WAN	广域网
WDM	波分复用
WFQ	加权的公平排队算法
WML	无线标记语言
WRED	加权的随机早期探测
XML	扩充标记语言

广东省网络空间安全协会受控资料

4 IP 网络的网络结构和网络组织

4.1 组网原则

1）本标准为我国 IP 网络的建设提供技术依据，主导思想是提出 IP 网络的总体技术要求。

2）基于业务量的需求和网络可扩展性的原则，我国 IP 网络的总体结构体系原则上采用一级骨干网、二级网和 IP 城域网三层。原则上，各二级网之间通过一级骨干网实现互连。另外，视各地的不同业务需求、竞争和线路情况，可以将二级网和 IP 城域网合二为一。

3）各 IP 网络运营商应实现互联，并考虑与现有其它网络互通。

4）IP 网络应设置国际接口局，与 Internet 互联。

5）基于技术先进性和成熟性的原则，IP 网络采用的主导传送技术是 IP/SDH/WDM（DWDM），并兼顾现有各种技术， 例如 IP/ATM 等。

6）根据 IP 网络的网络结构形式，网络管理原则上可以采取三级管理的方式，设置一级骨干网网管中心、二级网网管中心和 IP 城域网网管中心， 并分别设有相应的备用网管中心。 一级网管中心负责一级骨干网的管理，完成一级骨干网的各项管理功能。此外，一级网管中心还负责各二级网管中心的管理，并可通过二级网管中心对二级网实施各项管理功能。二级网管中心按二级网服务范围来设置。每个二级网内分别设置一个二级网络管理中心，负责完成二级网的管理功能，此外，还负责各 IP 城域网网管中心的管理，并通过 IP 城域网网管中心对 IP 城域网实施各项管理功能。每个 IP 城域网内分别设置一个 IP 城域网管理中心，负责完成 IP 城域网的管理功能。当二级网和 IP 城域网合二为一时， 其网管中心也合二为一。

7）IP 网络应实现组播功能。有关组播协议具体参见相关的行业标准。

8）鉴于 IP v4 的地址空间行将枯竭，在 IP 网络建设中，应尽早考虑 IPv4 向 IPv6 的过渡问题。

另外，我国 IP 网络建设还应遵循以下一些基本原则：

9）开放性

IP 网络技术选择建议符合相关国际标准及国内标准，避免个别厂家的私有标准或内部协议，确保网络的开放性和互连互通，满足信息准确、安全、可靠地交换传送的需要；所选择的网络设备应有开放的

接口，拥有良好的维护、测量和管理手段，提供网络统一实时监控的遥测、遥控的信息处理功能，实现网络设备的统一管理。

10）可运营性

IP 网络需要向大量用户提供不同类型的服务，网络应提供良好的业务管理能力，支持对宽带用户的接入管理、身份认证、带宽许可、地址管理和服务质量（QoS），并针对不同的业务提供灵活的计费方式，确保网络的可运营特性。

11）可管理性

IP 网络为分层的网络结构，需要统一的分级、分权管理能力的网管系统，实现统一的网络业务调度和管理，降低网络运营成本。

12）可增值性

根据竞争和企业发展的需要，IP 网络建设要充分考虑业务的扩展能力，能针对不同的用户需求提供丰富的宽带增值业务，使网络可持续赢利。

13）可扩充性

考虑到用户数量和宽带业务种类发展的不确定性，IP 网络要建设成完整统一、组网灵活、易扩充的弹性网络平台，能够随着需求变化，充分留有扩充余地。

14）安全可靠性

IP 网络的设计应充分考虑整个网络的稳定性，支持网络节点的备份和线路保护，提供网络安全防范措施。

4.2 网络结构

IP 网络的网络结构组织根据运营、管理和地理区域等因素可以分为三级：一级骨干网、二级网和 IP 城域网三层。视各地的不同业务需求、竞争和线路情况，可以将二级网和 IP 城域网合二为一，网络结构如图 1 所示。

IP 网络分为三级自治域，一级骨干网为一级自治域，二级网为一级自治域，IP 城域网为一级自治域。

4.3 一级骨干网

4.3.1 骨干节点设置

1）原则上可以根据地理区域， 例如每省设置一个一级骨干网节点。如果业务需要，可以在二级网内设置多个骨干网节点。

2）为节省一级骨干网线路连接，保证一级骨干网服务质量，综合考虑业务流量和地理位置的因素，某些一级骨干网节点可以作为核心节点。核心节点之间采用全网状连接。

3）当二级网内只存在一个非核心节点的骨干节点时，原则上此骨干节点至少与两个核心节点直接相连。如果条件不具备,可暂时只与一个核心节点连接。

4）当二级网内存在多个非核心节点的骨干节点时，应尽可能分别连接到不同核心节点。

5）骨干节点之间允许相互连接。骨干节点的相互连接应与路由协议中区域划分一致。

6）根据国际电路组织和业务的要求， 一级骨干网上应选择枢纽节点作为国际出入口节点。

4.3.2 骨干（核心）节点功能

一级骨干网与各二级网直接相连，负责转接（汇接）各二级网的业务。一级骨干网节点主要提供以下功能：

- 提供与其他骨干节点的连接；
- 提供与二级网汇接节点的连接；
- 提供节点之间的路由选择机制；
- 转发 IP 数据包；
- 提供网络的安全机制；
- 提供相关业务的服务质量保证机制；
- （国际出入口节点）转接来自所有一级骨干节点的国际业务。

原则上骨干（核心）节点不接入业务。

广东省网络空间安全协会内部资料

4.4 二级网

4.4.1 网络结构

二级网由位于各城市和地区的多个节点组成。

二级网节点之间采用不完全网状网结构。根据业务流量、流向和管理等因素，可在二级网的多个节点中设置一个或几个汇接节点，其余节点为普通节点。汇接节点应至少与两个一级骨干网节点直接相连接，普通节点应至少与一个汇接节点相连接。对二级网中经济发达地区节点、业务流量大或者实时性要求高的节点应直连到一级骨干网节点。

原则上两个二级网只能通过一级骨干网互连。

4.4.2 网络节点的职能

二级网节点包括汇接节点和普通节点。

汇接节点应完成以下职能：

- 汇接从属于它的 IP 城域网的业务；
- 转接来自本二级网其他节点的业务；
- 转接出入本二级网的业务；
- 提供用户直接接入的业务。

普通节点应完成以下职能：

- 汇接从属于它的 IP 城域网的业务；
- 提供用户直接接入的业务。

广东省网络空间安全协会受控资料

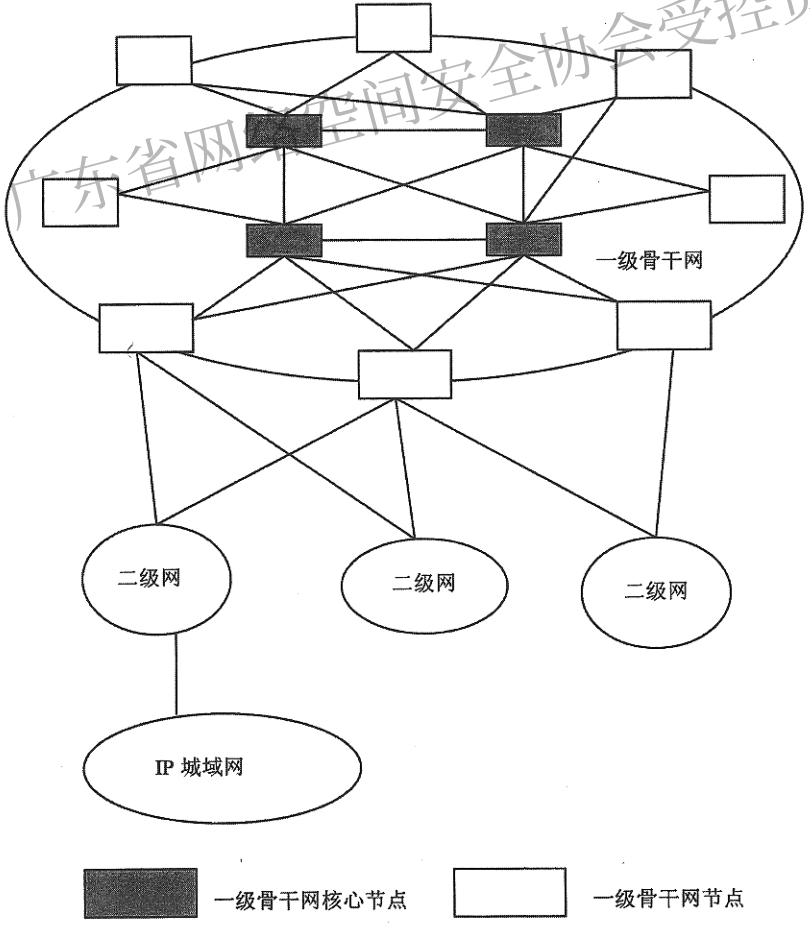


图 1　我国 IP 网络结构

4.5 IP 城域网

4.5.1 网络结构

在省内城市和地区可根据业务需求组建 IP 城域网。根据业务流量、流向和管理等因素，也可以在某些区域内联合组织规模较大（省内跨地区的）的 IP 城域网，即省内区域网；也可以组织省内地区性（在省内一个地区范围中）的 IP 城域网。

IP 城域网由 IP 城域网内的多个节点组成。可以在 IP 城域网的多个节点中设置一个或几个汇接节点，其余节点为普通节点。汇接节点应直接与二级网汇接节点直接相连接，普通节点应至少与一个汇接节点相连接。也可以不设置汇接节点，IP 城域网内所有的节点都直接与二级网节点相连接。

IP 城域网的组织应以便于用户设备接入为原则。

4.5.2 网络节点的职能

IP 城域网节点可以分为城域核心节点和汇聚节点。

1）城域核心节点应完成以下职能：

- 转接出入本 IP 城域网的业务；
- 转接来自本 IP 城域网其他节点的业务；
- 提供用户直接接入的业务等。

2）汇聚节点应完成以下职能：

- 扩展核心层设备的端口密度和端口种类；
- 扩大核心层节点的业务覆盖范围；
- 提供用户直接接入的业务；
- 实现接入用户的可管理性等。

有关 IP 城域网的具体要求见第 8 章。

4.6 三级网络节点之间的关系

二级网节点通过其汇接节点与一级骨干网节点相连接。在 IP 网络建设初期，若业务量不大，一级骨干网节点和二级网汇接节点可以合为一体；随着业务需求的不断增长，再分开设置。

IP 城域网节点通过其汇接节点与二级网相连接（若不设置汇接节点，则可直接接入二级网）。在建设初期，可将两者合为一体，随业务的增长再分开设置。

4.7 路由协议

路由协议为 IP 网络内各节点提供 IP 数据包的路由选择机制，路由协议分为内部路由协议和外部路由协议。

一级骨干网内：一级骨干网设置成一个自治域，一级骨干网内采用内部路由协议 OSPF 或 IS-IS， 优选 OSPF。

二级网内：每个二级网设置成一个自治域，二级网内采用内部路由协议 OSPF 或 IS-IS，优选 OSPF。

IP 城域网内：每个 IP 城域网设置成一个自治域，IP 城域网内采用内部路由协议 OSPF 或 IS-IS，优选 OSPF。

一级骨干网与二级网之间：采用外部路由协议 BGP-4。

二级网与 IP 城域网之间：采用外部路由协议 BGP-4。

不同 IP 网络运营商网络间：采用外部路由协议 BGP-4。

网络与国际互联网间：采用外部路由协议 BGP-4。

一级骨干网内区域划分：核心节点组成 AREA0，其他节点可以考虑地理位置以及相互之间通信量就近组成多个 AREA。

4.8 国际出口

IP 网络可以设置多个国际出口。出于业务量考虑以及地理位置考虑，可以设置在北京、上海和广州。国际出口带宽可以根据网络流量要求确定，并根据发展不断扩充。

广东省网络空间安全协会受控资料

5 业务分类

5.1 业务类型

根据业务对实时性要求的不同及提供方式的不同，将业务分为如下几类：

1）实时业务

该类业务包括双向、双方和多方业务。在进行通信时要求具有实时响应，要求提供业务的网络能够保证严格的延时和抖动。

2）非实时业务

该类业务通常为信息传输业务，对网络没有严格的延时和抖动要求， 例如传统的 IP 业务（E-mail、文件传送协议 FTP、Web 等）。

3）VPN 业务

在公用网络平台上构筑不受地域限制而受企业统一策略控制和管理的企业网络。

4）带宽和波长出租业务

在 IP 网络上为用户提供类似于电路专线的专线业务。

5.2 各类业务的典型业务

各类业务的典型业务应用如表 1 所示。

表 1 各类业务的典型业务

业务	具体应用
非实时业务 （传统 IP 业务）	E-mail、FTP、Web、电子商务等
实时业务 （传统电信业务）	电话/传真 多媒体会议（+非实时业务） 远程教学（+非实时业务） 远程医疗（+非实时业务）

广东省网络空间安全协会受控资料

5.3 典型业务描述

5.3.1 非实时业务

5.3.1.1 E-mail

（1）基本技术

利用电子邮件技术。

（2）协议及标准

通信协议：简单邮件传送协议（SMTP）、 POP3。

（3）电子邮件业务可应用于：接收信件、发送信件、文件转发等。

5.3.1.2 FTP

（1）基本技术

利用异地主机的 FTP 文件交换或用 Telnet 仿真终端接入，完成远程异地科学计算及信息处理。

（2）协议及标准

通信协议：FTP 等。

（3）科学计算及处理业务可应用于：翻译业务、软件共享业务、远程计算机辅助设计业务等。

5.3.1.3 Web 业务

（1）基本技术

基于 Web 技术，为了增强多媒体检索的功能，采用 JAVA、公共网关接口（CGI）等技术，以适合

各种场合的需要。

（2）协议及标准

通信协议：超文本传送协议（HTTP）。

（3）多媒体信息检索业务可应用于：全国电话号码簿(黄页、白页)、电信业务费用查询、电信业务查询、文化教育、课程培训、餐饮旅游、文化娱乐、情报检索、图书资料、新闻、体育、商品信息、经济情报、专家系统、法律、法规、广告等。

5.3.1.4 VPN 业务

（1）业务定义

虚拟专用网（VPN）是指在公用网络平台上构筑不受地域限制而受企业统一策略控制和管理的企业网络。

（2）基本技术

在 IP 网上实现 VPN 业务，就是使用加密的 IP 隧道，实现专有 IP 包和其他网络协议（IPX，NetBEUI 等）包在 Internet 上传输，从而实现广域网上不同 LAN 的各种协议虚拟连接，即虚拟的局域网（VLAN）。

（3）协议和标准

点对点隧道协议：点到点隧道协议（PPTP）。

第二层隧道协议：第 2 层隧道协议（L2TP）。

第三层隧道协议：通用路由协议 GRE（参见 RFC 1701/1702）。

IP 安全协议：IPsec 协议

（4）虚拟专用网业务可应用于：内联网互联、外联网互联、远程用户接入、中小 ISP 和 ICP 在较大的范围内开展业务

有关 IP VPN 业务的具体要求参见相关的标准。

5.3.1.5 电子商务业务

（1）业务描述

电子商务是利用 Internet 进行的贸易。包括在 IP 网上建立商务市场，完成订购、投递物品的信息管理以及资金的传递等功能。

IP 网上的用户可以根据其不同的目的作为电子商务活动中的消费者、商家、银行、认证中心、客户服务中心、支付处理方和投递方。

（2）基本技术

基于 Web 技术，以及利用 JAVA、CGI 等技术，完成电子商务业务。为了确保电子商务要求的高可靠性、高安全性，将采用一定强度的加密技术，以满足信用卡等金融交易的需要。

（3）协议及标准

Web 协议： HTTP。

表示层句法：超文本标识语言（HTML）、扩充标记语言（XML）。

购买框架：互联网开放贸易协议（IOTP）。

支付协议：安全电子交易（SET）、e-cash 等。

加密协议：公共密钥基础设施（PKI）。

（4）电子商务业务可应用于：房租、水、暖、电收费业务，电信收费业务，市政收费业务，各种罚款收费业务，电子银行， 电子税务，电子购物，电子商品交易市场。

有关电子商务业务的具体要求参见相关行标。

5.3.2 实时业务

5.3.2.1 IP 电话/传真

（1）基本技术： IP 电话/传真是利用语音压缩技术，在 IP 网上传送话音的业务。该业务可充分利用 IP 网的复用功能来实现网络带宽的合理应用。

（2）协议及标准

广东省网络空间安全协会受控资料

a）通信协议：H.323、H.225、RTP、RTCP、UDP、T.38。

b）服务质量协议：RSVP，MPLS， Diffserv。

c）语音编码协议：G.729、G.723.1、G.728、T.30、G.711。

（3）主要应用：电话到电话、电话到 PC、PC 到电话和 PC 到 PC 方式的电话业务；传真机到传真机、传真到 IP 传真机、IP 传真机到传真机、IP 传真机到 IP 传真机的传真通信。

5.3.2.2 多媒体会议业务

（1）基本技术

基于 TCP/IP 的会议业务。由于 LAN 上业务质量得不到保证，因而图像编码和语音编码都要尺度可伸缩的。为保证实时及同步的要求，实时信息(视频音频)用 RTP、RTCP、UDP 协议栈，数据信息用 TCP 协议栈。为了进一步保证一定的质量，要有一定的信道带宽预约机制。

（2）协议及标准

a）通信协议：H.323、H.225、RTP、UDP、HTTP。

b）服务质量协议：RSVP、Diffserv。

c）语音编码协议：G723.1、G.729。

d）图像编码协议：H.263。

e）多点会议协议：T.120 系列、T.130 系列。

（3）多媒体会议业务可应用于：虚拟专网中的多媒体会议业务、公众多点多媒体会议业务等。

5.3.2.3 远程教学业务

（1）基本技术

多媒体远程教学是一项综合性的多媒体应用，教学对象不同，采用技术也不同。从一般的多媒体信息检索供远程教学用，到远程面对面教学。由于远程教学业务是基于 TCP/IP 技术的，业务质量不能保证，因而要采用尺度可变的图像和语音编码，并采用新技术在一定程度上保证业务质量。

（2）协议及标准

a）通信协议：H.323、H.225、RTP、RTCP、HTTP。

b）服务质量协议：RSVP、Diffserv。

c）语音编码协议：G.729。

d）图像编码协议：H.263、H.261、JPEG、JBIG、MPEG－1、MPEG－2。

e）多点会议协议：T.120 系列、T.130 系列。

（3）远程教学可应用于： 教学节目点播、 教学资料检索、交互式(人—机)远程教学、交互式(人—人)远程教学等。

5.3.2.4 远程医疗业务

（1）基本技术

多媒体远程医疗是一项综合技术，集多媒体会议、多媒体信息检索、多媒体信息分配及协同处理于一体。由于它基于 TCP/IP 技术，业务质量不能保证，因而要采用尺度可变的图像和语音编码，并采用新技术以在一定程度上保证业务质量。

（2）协议及标准

a) 通信协议：H.323 、 H.225、RTP、 RTCP、UDP、HTTP、X.29。

b) 服务质量协议：RSVP。

c) 语音编码协议：G723.1、G.729。

d) 图像编码协议：H.263 、H.261、JPEG、JBIG、MPEG－1、 MPEG－2。

e) 多点会议协议：T.120 系列 、T.130 系列。

f) 可视图文业务互通协议：T.101。

（3）多媒体远程医疗可应用于：远程医疗手术示范，远程专家会诊，高清晰医疗图像传送，医生与病人远程问诊、协合处理、处方讨论 、医案讨论，远程医疗信息的采集和处理，医疗视像图像片断的

广东省网络空间安全协会会员资料

播放等。

5.3.2.5 视频点播业务（VOD）

视频点播，也称交互式多媒体视频点播，是随着计算机技术和网络通讯技术的发展，综合了计算机技术、通讯技术、电视技术而迅速新兴的一门综合性技术。它利用了网络和视频技术的优势，彻底改变了过去收看节目的被动方式，实现了节目的按需收看和任意播放，集动态影视图像、静态图片、声音、文字等信息为一体，为用户提供实时、交互、按需点播服务。之外，它还可以根据用户需要任意选择信息进行相应的控制，如在播出进程中留言、发表评论等，从而加强交互性，增加了用户与节目之间的交流。有关视频点播业务具体参见相关的行业标准。

5.3.3 带宽和波长出租

IP 网络的出租业务除了主要面向有大需求的网络运营商外，另外也可直接面向大型企业提供企业互连业务。光网络的业务经营一般分为细颗粒的管道出租，即带宽和电路批发业务，以及大颗粒的管道出租，及光纤和波长出租业务。

带宽和波长批发业务主要包括：

1）专线传输：提供 *N*×64k、2M、34M、155Mbit/s 等速率通道。

2）IP 传送服务：提供二层 VPN 服务，如以太网透明传送、ATM PVC 等。

光纤基础设施和波长出租业务包括：

1）波长出租：用户租用光网络波长，自建业务网络。

2）暗光纤出租：用户租用光纤，自建传输、交换网络。

3）管道出租：用户租用管道。

5.4 其他增值业务

IP 网络可以支持其他增值业务，例如：防火墙服务、安全性服务、数据存储服务、网络管理服务、强制门户及内容过滤等。

广东省网络空间安全协会受控资料

6 地址分配和域名系统层次结构

6.1 地址分配

6.1.1 地址组织

（1）骨干网络应保留足够的连续地址组成独立的自治域，并为今后的扩展留有余地。

（2）分配地址应连续，相邻地区的地址也应连续。

（3）地址划分应有层次性，便于网络互连，简化路由表。

（4）可以根据当地的业务状况、发展前景、当前地址资源等情况综合考虑，分配给不同的 IP 地址容量，为了充分合理地利用地址资源，用可变长子网掩码技术，分配 IP 地址网段。

（5）在合理分配各自网络节点的 IP 地址时应保留一定数量的 IP 地址为用户提供接入服务。在地址有限，但又有相当数量的用户需求时，可用保留地址为用户提供接入服务，但必须对其进行地址转换。

（6）与业务相关的设备（如：高端路由器、IP 电话网关、IP 电话网守、各种 Internet 服务器、防火墙、边缘（接入）路由器等设备）应分配给合法 IP 地址。VPN 与采用 VPN 方式进行的服务可以在 VPN 内部分配保留地址。

（7）为了保证网络的发展，应保留一定数量的 IP 地址，当备用地址小于一定数量时应申请新的 IP 地址。

6.1.2 地址分配原则

（1）所有 IP 地址资源(包括公开与保留)均全网统一分配。

（2）为了保证 IP 地址的充分利用，采用 CIDR 和可变长子网掩码。

（3）地址分配应利于路由的组织。

（4）地址分配兼顾到近期的需求与远期的发展，网络的扩展。

（5）地址分配应考虑到现有 IP 业务，新型 IP 业务以及各 IP 网络运营商特殊的业务要求。

（6）在地址资源不足的情况下，为了保证网络的通畅，所有一级骨干网、二级网与本地网的路由器应分配公开地址，提供传统 Internet 服务的节点应分配公开 IP 地址。从长远考虑，与其他网络互通的服务的节点应分配公开 IP 地址，提供实时服务的节点分配公开 IP 地址，为用户提供 Internet 接入的节点应分配公开 IP 地址；局域网的内部可使用保留地址，只在局部提供的业务的节点应分配保留地址。

6.2 域名系统的层次结构

6.2.1 域名服务器的设置

采用三级域名解析，在网内设置若干顶级域名服务器，分担域名解析的负荷，在二级网设置二级网域名服务器， 在 IP 城域网内设置 IP 城域网内域名服务器。

6.2.2 域名系统组成

（1）域名空间和资源记录。

（2）域名服务器。

6.2.3 域名设置的主要考虑因素

- 主机名解析。
- 邮件交换记录解析。
- 降低域名解析在骨干网上的流量。
- 能解析其他域名下的主机。

6.2.4 命名原则

（1）IP 网络运营商在申请到自己的域名的情况下，网内用户、信息源、域名服务器等的域名均应在该域名下。

（2）各种域名分配原则。

a）网内路由器域名。

——一级骨干网：

一级骨干网内每个路由器上至少选一个端口的 IP 地址进行域名注册，其命名为：

(port)-R(n)-B-(city)(m).(申请的域名)

其中：

(port)：路由器端口类型及编号。

(n)：同一安装地点的路由器编号。

B：表示此路由器端口属于一级骨干网。

(m)：同一城市中不同的安装地点。

(city)：网络节点所在省及城市，如广州为 gdgz。

——各二级网或 IP 城域网：

二级网或 IP 城域网路由器上至少选一个端口 IP 地址进行域名注册，其命名为

(port)-R(n)-A-(city)(m).(province).(申请的域名)

其中：(port),(n),(m)意义同上。

A：表示此路由器端口属于二级网。

(city)：网络节点所在城市。

(province)：网络节点所在省。

b）信息源及用户域名：域名均在各 IP 网络运营商申请的域名下，下一级域名为各省名、各 IP 城域网或各机构、企业名，由主管部门统一管理，再下一级域名由分配到次一级域名的各省、机构、企业自定。

（3）域名中省、市、自治区的缩写遵照《中国互联网络域名注册暂行管理办法》执行。

6.2.5 域名解析方式

顶级域名服务器原则上负责解析到 IP 网络运营商申请到域名的下一级域名，再下一级的域名由各二级网域名服务器或各 IP 城域网域名服务器负责解析。

广东省网络空间安全协会受控资料

7 IP 网传输层要求

7.1 IP 传输组网技术

IP 网传输层为 IP 网络提供物理传输通道。IP 传输层组网技术主要采用 IP over SDH 和 IP over WDM（DWDM）技术，也可以采用 IP over ATM 技术。

传输技术的选择主要依据业务量和速率需求。

7.2 传输网网络结构

IP 传输层以 SDH（或 ATM）和 WDM（DWDM）系统构成 IP 网的物理传输网络。

7.2.1 分层结构

IP 网络传输网的网络结构可分为一级骨干网、二级网和 IP 城域网，如图 2 所示。一级骨干网主要负责 IP 骨干节点之间的互连。二级网覆盖运营范围内的主要城市，负责 IP 二级网节点之间的互连。IP 城域网负责 IP 城域网节点之间的互连。为了保证二级网到一级骨干网连接的可靠性，原则上，二级网和一级骨干网之间至少需要有两条物理路由不同的连接。另外，为了保证 IP 城域网内到二级网连接的可靠性，原则上，IP 城域网和二级网之间也至少需要有两条不同物理路由的连接。

7.2.2 一级骨干传输网结构

一级骨干传输网为高端路由器提供大容量的 SDH 或波长通道。一级骨干网链路速率的选择依据业务量而定。

一级骨干网的拓扑结构建议使用环形网结构。环形网结构的特点是网络拓扑简单，网络可靠性较高，需要的链路数较少。根据地域分布和业务量情况，一级骨干传输网可以由若干个环形网组成，每个环形网覆盖一定的区域。为了保证网络的可靠性和路由的合理性，每两个相邻的环网之间需要有两个衔接点。没有条件建立环网的地区，可以建立点到点系统与环网连接。一级骨干传输网未覆盖的地区，可以采取租用波长或 SDH 通道的方式与骨干网连接。

广东省网络空间安全协会宣传资料

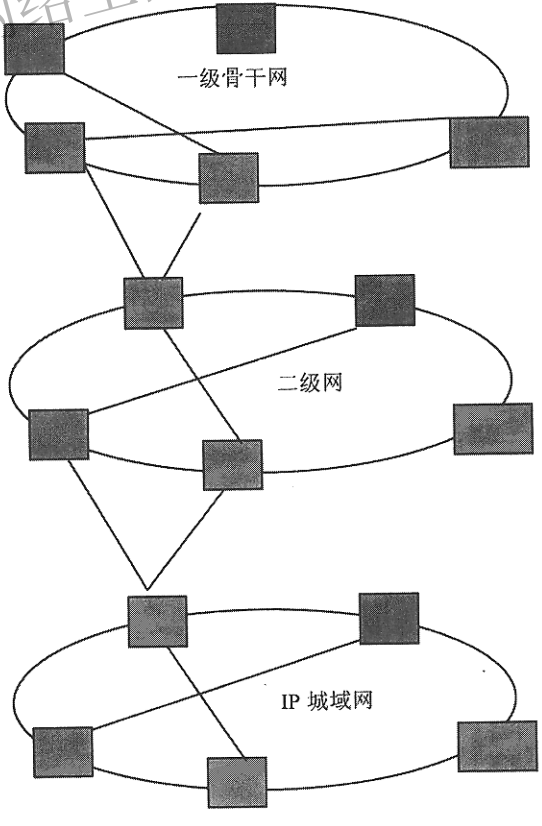


图 2 传输网分层结构

7.2.3 二级网传输网结构

二级网传输网的网络结构根据其 IP 网结构和业务情况确定。二级网传输网拓扑结构建议使用 SDH 环网。在环网技术上，可以采用 2 纤通道保护环或复用段保护环。一般说，二级网为汇接业务，采用通道保护环比较合适。

7.3 网络同步

采用 IP over SDH 和 IP over WDM 技术的高端路由器以 SDH 帧结构进行传输，要求其定时系统应符合 SDH 系统对同步时钟的要求。

（1）原则上，采用 IP over WDM 技术的 IP 网节点应具有外同步接口，接入相应的同步网时钟设备 BITS，即采用 BITS 上的外同步信号。路由器应同时支持线路定时方式，接收来自线路系统的定时信号。考虑到网同步的安全可靠性，在定时方式上，采用外定时方式为主用定时方式，线路定时方式为备用定时方式。当不具备外定时条件时，可以采用内部定时源信号。

（2）采用 IP over SDH 技术的 IP 网节点，由于 SDH 网本身为同步网络，可以采用线路定时方式，直接从线路系统提取定时信号。（IP 网节点同步信号技术指标参照 SDH 系统同步要求。）

（3）关于 SDH 传输设备的同步，参照 SDH 系统同步要求。

7.4 网络恢复保护

对于 IP 骨干网，在采用 IP over WDM 技术组网时，其网络恢复保护参见相关行标的规定。目前，应要求骨干路由器具备 SDH APS(自动保护倒换)功能，根据需要采用路由器之间的 1+1 保护倒换，切换时间要求＜50ms。随着 OADM 设备的成熟和光网络技术的发展，未来可以在光网层实现保护。

二级网采用 2.5Gbit/s（622Mbit/s）SDH 环网，可以利用环网的自愈功能实现业务的 100% 保护，保护倒换时间要求＜50ms。

对于租用波长通道或 155M bit/s SDH 通道的连接方式，应视需要采用 1+1 保护方式，保证每个节点与其他节点存在两条以上物理链路。

广东省网络空间安全协会受控资料

8 IP 城域网基本要求

8.1 IP 城域网功能结构

由于 IP 城域网上承载的业务将以基于 IP 包传送的业务为主，因此，IP 城域网的组网技术以 IP 包交换技术为核心。由于目前 IP 技术在 QoS、网络安全等方面尚不成熟，考虑到 IP 城域网的业务需求多样化，特别是企业高速互连业务在安全性、高可靠方面的需求，多种网络技术体制（IP、SDH、ATM）在一段时间内仍将在城域网并存。

IP 城域网在组网功能结构上可分为：核心层、汇聚层、接入层、业务中心与管理中心,见图 3 所示。

核心层采用高速分组（例如 IP 或 ATM）交换技术，汇聚层采用智能分组端局技术，接入层采用多元化宽、窄带综合接入技术，业务及网络管理统一对网络各层实施管理，构建支持端到端话音、数据、图像、专线及各类增值业务的可运营可管理的 IP 城域网。有关 IP 城域网具体要求参见相关标准。

8.2 IP 城域网核心层

核心层的作用是把多个边缘汇聚层连接起来，为汇聚层网络提供数据的高速转发，同时实现与上级网络的互联，提供城市的高速 IP 数据出口。核心层网络结构重点考虑可靠性、可扩展性和开放性。

核心节点间原则上采用网状或半网状连接：通过 SDH 或城域 WDM（DWDM）连接，以确保网络的可扩展性；在网络建设初期规模较小时，核心节点也可通过内置的光传输接口直驱光纤互联。

考虑 IP 城域网出口的安全，建议每个 IP 城域网选择两个核心节点与骨干网（或二级网）路由器实现连接。

8.2.1 核心层组网技术选择

核心层节点设备建议采用以 IP 技术为核心的设备，如大容量的路由交换机（需要支持 MPLS 及 IP

QoS）。设备要求具有强路由功能，能够提供千兆比特以上速率的 IP 接口，如 POS、Gigabit Ethernet（GE）接口。

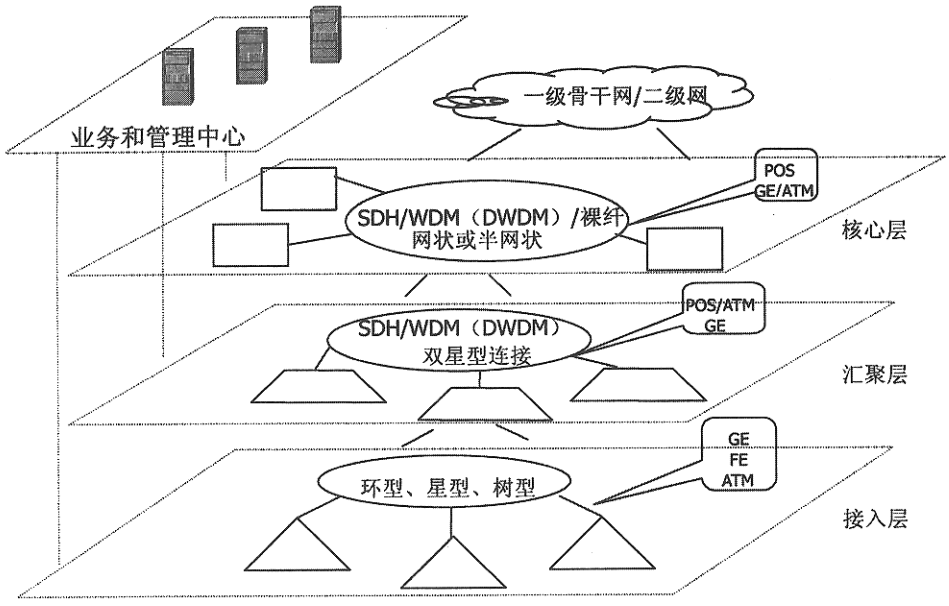


图 3　IP 城域网网络结构

广东省网络空间安全协会受控资料

8.2.2　核心层网络结构

IP 城域网核心节点应设置在城区内，远郊和所辖县城设置汇聚节点。

核心节点部署在各中心局，原则上应采用网状网或不完全网状网连接，保证用户对业务中心的访问带宽，保证网络的冗余连接。

核心节点建议采用开放的城域传输网互联，实现业务交换与传送分离，使网络拓扑灵活调整，核心（汇聚）交换节点能灵活地扩容和备份，支持网络可持续扩展。要求城域传输支持多种高速数据接口。

考虑 IP 城域网出口的安全，建议每个 IP 城域网选择两个核心节点与骨干网（或二级网）路由器实现连接，提供 IP 城域网的双出口。核心节点上的设备采用热备份方式，设备要求能够实现板件的热插拔和重要板件的热备份。

8.3　IP 城域网汇聚层

汇聚层的作用是完成本地业务的区域汇接，进行带宽和业务汇聚、收敛及分发，并进行用户管理，通过识别定位用户实现基于用户的访问控制和带宽许可，以及提供安全保证和灵活的计费方式。

汇聚层节点实现以下一项或多项功能：

（1）扩展核心层设备的端口密度和端口种类。

（2）扩大核心层节点的业务覆盖范围。

（3）汇聚接入节点，解决接入节点到核心节点间光纤资源紧张的问题。

（4）实现接入用户的可管理性，当接入层节点设备不能保证用户流量控制时，需要由汇聚层设备提供用户流量控制及其他策略管理功能。

（5）除提供高速上网业务外，IP 城域网还可提供种类繁多的宽带增值业务，如个性化业务管理、本地特色内容业务、内容过滤等，需要汇聚层设备支持智能 IP 端局的业务特性，与其他业务服务网共同提供丰富的增值业务。

（6）统一的月租方式应无法支撑集约化的运营模式，需要汇聚层支持灵活的计费方式，满足多样化的用户需求，形成差异性的竞争优势。

（7）具备网络安全防护能力，包括 IP 地址被盗用、核心设备防假冒与防攻击。在 IP 领域，IP 地址

不能作为唯一识别合法用户的手段，需要防止合法用户的 IP 地址被盗用。汇聚层设备要能够识别假冒的核心设备（如 DHCP 服务器）对设备的管理和防止恶意发起的对核心设备的攻击信息。

汇聚层要采用智能分组端局设备：对用户进行管理，实现基于用户的访问控制和带宽许可，提供安全保证和灵活的计费方式，解决运营商在向用户提供 IP 业务过程中所面临的各种问题，使 IP 城域网成为一个可运营、可管理的电信网络。

8.3.1 汇聚层组网技术选择

汇聚层上行采用 100M LAN，GE, ATM 或 POS 与核心骨干连接。

由于汇聚层主要汇接接入层的综合业务，接入层上行接口是多样化的（ATM，IP），所以汇聚层下行接口也应是多样化的，为提高接入效率，汇聚层应采用具有 IP 和 ATM 综合接入能力的设备。

8.3.2 互通要求

根据需要，在汇聚层可以通过网络接入服务器、IP 电话网关或软交换设备实现与 PSTN/ISDN 网的互通， 具体要求见第 12 章。

8.4 IP 城域网接入层

接入层通过各种接入技术和线路资源实现对用户的覆盖，并提供多业务的用户接入，必要时配合完成用户流量控制功能。为降低维护及管理成本，综合接入层应考虑与汇聚层统一实施业务和设备管理。

接入层传输可采用各种低成本、高可靠传输技术，根据业务用户的重要性，采用环形、链形、树形进行组网。在解决企业互连时，可考虑基于 SDH 技术的城域多业务传输技术，提供高可靠的企业高速互连业务。

8.4.1 IP 城域网接入层技术选择

接入层节点的设备主要是为了将不同地理分布的用户快速有效地接入骨干。接入层节点可以根据实际环境中用户数量、距离、密度等的不同，设置一级或级联接入。

当前用于提供宽带接入的方式主要有 *x*DSL、光纤+以太网、HFC 三种，分别对应于基于 DSL 技术的宽带接入网、基于以太网的宽带接入网、基于 HFC 的宽带接入网。*x*DSL 适用于零散分布用户或不计划改造现有双绞线布线计划的小区、大厦用户，并可作为信息化大厦小区建设的补充接入方式，光纤+以太网方式主要适用于用户密集的住宅小区和商业大厦，HFC 主要适用于对现有有线电视线缆进行双向和扩频改造后的家庭用户。

接入层负责提供各种类型用户的接入，应提供丰富的用户接口，较高的端口密度，要能对用户节点实现一定的流量控制及其他策略管理功能。

接入节点主要对集团用户、小区用户和其他有接入需求的用户提供接入服务，它应具有业务和容量的扩展性，具有多业务的承载能力和 QoS 保证。

从业务的角度讲，用户的需求是趋向于多样化的， 用户驻地网络所用的传输媒质、用户的带宽需求、用户的业务流量模型都不一致，因此不可能用一种接入技术解决所有的问题，目前较流行的接入技术有 *x*DSL、Ethernet、HFC、PON 等，这些技术均有其特点和合适的应用领域。这就要求接入设备具备多业务接入的能力，满足用户多样化接入的需求。

因此，接入层设备应该具有综合接入功能，包括宽带接入（Ethernet、*x*DSL、Cable 等）和窄带业务接入（话音、窄带专线等）的能力。

8.4.2 IP 城域网接入层网络结构

由于接入节点分布广、数量多，全部采用星型组网会需要大量的光纤，在光纤资源不丰富的城市，建议选择环形组网方式（采用城域多业务传输或接入设备自组环）和星型（点对点）、分支（PON/APON/EPON 技术）的组网结构。

接入层设备可以根据终端用户需要的业务类型和线路资源的情况选择使用纯 IP 设备（二层交换机等）、纯 ATM 设备、IP/ATM 混合设备、*x*DSL 设备、宽带接入设备、宽窄带综合接入设备等。

接入节点应能提供 100Mbit/s 以上速率的接口与汇聚节点相连，远距离传输时优先选用光纤作为物理层媒介。

原信息网络产品安全协会受控资料

接入层设备（二层交换设备）应具备用户数据隔离、端口隔离和广播抑制功能，以保证用户数据的安全和网络的安全，并具备组播管理功能和组播安全特性。

接入层设备要满足复杂运行环境（供电、环境适应性、线路适应性等）要求，支持管理中心对设备的统一管理、配置和测试功能，具备环境监控的能力，降低网络的维护及运营成本。

8.5 业务中心与管理中心

业务中心提供丰富的宽带网络增值业务，并以标准的中间件与其他业务服务互连互通，构建开放的业务平台。

业务与管理层提供统一的网络管理与业务管理，统一业务形象。根据业务开展的需要，可实现分级分权业务及网络管理，提供网络综合设备的拓扑、故障、配置、计费、性能和安全的统一管理。

9 网络性能和服务质量要求

9.1 网络性能

有关IP网络性能的详细要求见行标YD/T 1171-2001《IP 网络技术要求—网络性能参数与指标》。

9.1.1 IP网络性能参数

9.1.1.1 IP包传输时延（IPTD）

IP包传输时延定义为穿过一个基本段或NSE传送IP包所经历的时间，无论传送成功还是错误。IPTD是两个相关IP包传送参考事件的时间差（t_2- t_1），其中离开事件发生在t_1，进入事件发生在t_2，这里(t_2> t_1)，并且（t_2- t_1）≤T_{max}。

如果在NSE中IP包被分片，t_2时刻指最后一个相关进入事件发生的时间。端到端的IP包传输时延是SRC和DST之间MP的单向时延，如图4所示。

广东省网络空间安全协会受控资料

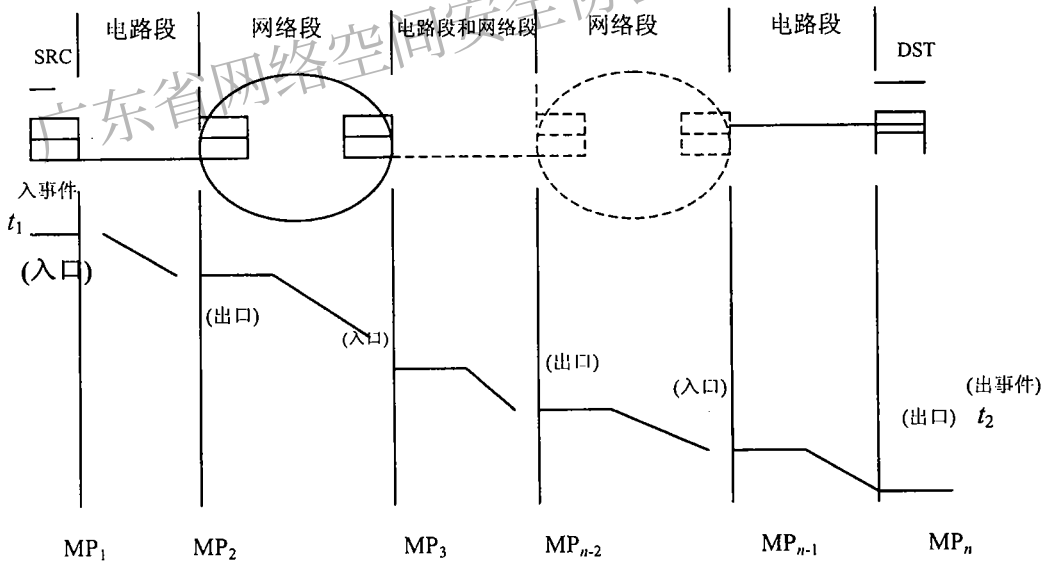


图4 IP包传输时延

9.1.1.2 平均IP包传输时延（Mean IP packet transfer delay）

平均IP包传送时延指一个数据流中所有IP包传送时延的算数平均值。

9.1.1.3 IP包时延变化（IP packet delay variation）

两点间IP包时延变化有两种定义方法：

方法1：端到端两点间IP包时延变化（v_k）是IP包k通过SRC（MP_1）和DST（MP_2）的实际时延（x_k）与通过相同MP定义的参考IP包传送时延（$d_{1,2}$）的差,即：$v_k = x_k - d_{1,2}$（参见图5）。

方法 2：在一段较短的测量时间间隔内，最大 *IPTD* 与最小 *IPTD* 的差值。

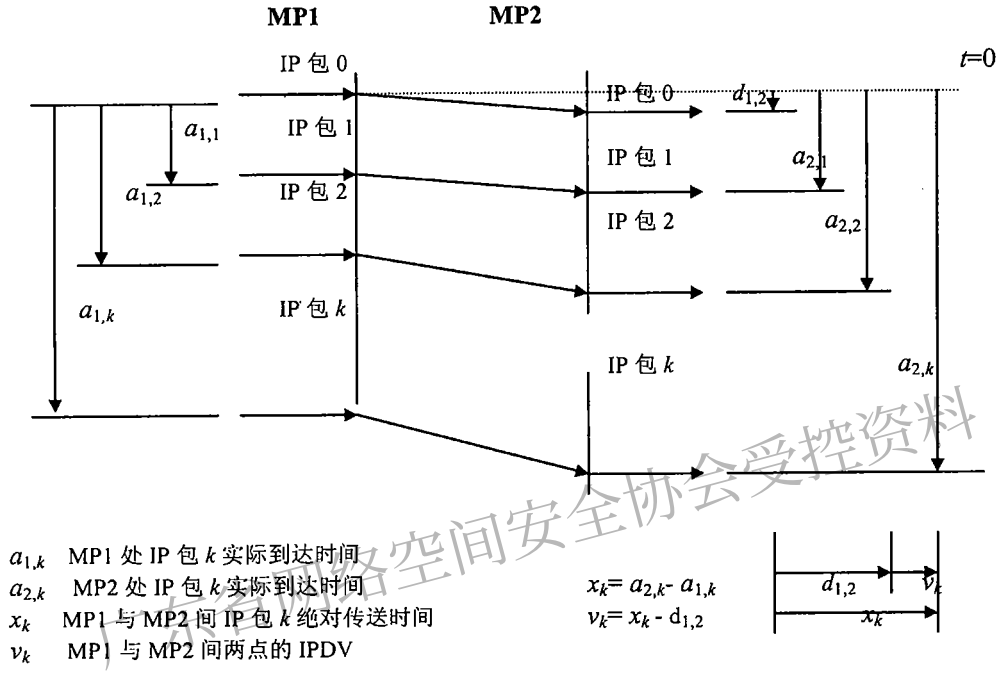
$IPDV = IPTD_{max} - IPTD_{min}$

其中：

$IPTD_{max}$ 是在一次测量时间间隔内所测量到的最大 *IPTD*;

$IPTD_{min}$ 是在一次测量时间间隔内所测量到的最小 *IPTD*。

IP 包时延变化参数非常重要。在数据包传送应用中，利用 IP 包时延变化范围的信息可以避免出现节点缓冲的溢出和读空；IP 包时延变化也会引起 TCP 层重传定时器门限的增高，也可能引起数据包重传的时延或造成没有必要的数据包重传。



广东省网络空间安全协会受控资料

图 5　IP 包时延变化

9.1.1.4　IP 包误差率（IPER）

IP 包误差率是错误 IP 包传送结果与成功 IP 包传送结果加错误 IP 包传送之和的比值。

9.1.1.5　IP 包丢失率（IPLR）

IP 包丢失率是丢失的 IP 包传送结果与所有 IP 包的比值。

9.1.1.6　虚假 IP 包率（Spurious IP packet rate）

一个出口 MP 的虚假 IP 包率指在一个特定时间间隔内在该 MP 上观测到的虚假 IP 包数量除以该时间间隔（等效于：虚假 IP 包数/业务秒）

9.1.1.7　IP 网络的流量参数（Flow related parameters）

现有 IPv4 网络没有对端到端 IP 业务的流量模式进行兼容性检查，只是对各种业务信息做尽力而为的传送。然而，为了在 IP 网络中提供能够保证 QoS 的服务，用流量或吞吐量这样的参数来描述和评价 IP 网络的能力是非常有意义的。

（1）IP 包吞吐量（IPPT）

一个出口 MP 的 IP 包吞吐量等于一个特定时间间隔内在该 MP 上观测到的所有成功 IP 包数量除以该时间间隔（等效于：成功 IP 包数/业务秒）。

（2）基于字节的 IP 包吞吐量（IPOT）

一个出口 MP 的基于字节 IP 包吞吐量等于一个特定时间间隔内在该 MP 上观测到的成功 IP 包中的

所有字节数量除以该时间间隔（等效于：成功 IP 包数中字节数/业务秒）。

9.1.2 IP 网络业务的可用性

IP 网络业务可用性用于描述基本段，NES 和端到端的 IP 网络业务。它把 IP 网络业务的全部持续时间分为可用时间和不可用时间。

9.1.2.1 IP 网络业务可用性功能

IP 网络业务可用性功能的基础是 IP 包丢失率（IPLR）性能的门限值，如果一个端到端 IP 网络业务的 IPLR 低于表 2 中的门限值 c_1，则该端到端 IP 网络业务是可用的，否则该端到端 IP 网络业务是不可用的，如表 2 所示。

表 2 IP 业务可用性功能

超出的准则	门限值
IPLR> c_1	c_1 =0.75
注：c_1 =0.75 是预先设定的，也可以建议 c_1 =0.9 和 c_1 =0.99，当 IP 网络支持多种 QoS 时，适当的方法是用不同的 c_1 值来对应不同的业务。用于评价 IP 业务可用性的最小时间间隔 T_{av} 暂定为 5min。	

门限值 c_1 仅被用来确定何时 IP 网络的资源不能够支持可用的 IP 包传送业务。c_1 值既不能认为是 IPLR 的性能指标，也不能认为是适合各种应用的 IPLR 性能指标。基于 IPLR 建立的性能指标应当除去所有业务不可用的时间，即除去（IPLR-c_1）的所有时间。

9.1.2.2 IP 网络业务可用性参数

IP 网络业务可用性参数有两个：

一个是 IP 业务不可用百分数（Percent IP service unavailability，PIU）；

另一个是 IP 业务可用百分数（Percent IP service availability，PIA）。

而且：

PIU=100-PIA

广东省网络空间安全协会受控资料

9.1.2.2.1 IP 业务不可用百分数（PIU）

不能应用 IP 业务可用性功能的时间间隔占 IP 业务全部时间间隔的百分数（T_{av} 间隔的百分数）。

9.1.2.2.2 IP 业务可用百分数 (PIA)

能够应用 IP 业务可用性功能的时间间隔占 IP 业务全部时间间隔的百分数（T_{av} 间隔的百分数）。

9.1.3 IP 网络性能指标

本小节规定了以测量点（MP）为边界的端到端 IP 网网络性能指标，具体指标如表 3 所示。表 3 中规定的所有值都是临时的，在根据实际运营经验修订(增大或减小)之后应该满足这些指标。把端到端的性能指标定义为对应于 IP 包参考事件（IPRES）的 IP 性能参数的统计值。端到端 IP 网络包括将 IP 包从源主机(SRC)传输到宿主机(DST)的电路域(CS)和网络域(NS)，但不包括用户驻地网。源主机和宿主机上的低层协议（IP 层、一层和二层）也是 IP 网的一部分。

表 3 IP 网端到端性能指标

			QoS 等级			
	网络性能指标的性质	缺省指标	0 级	1 级（交互式）	2 级（非交互式）	3 级（U 级）
IPTD	平均 IPTD 的上限值	需规定	150ms	400 ms	1s	不规定
IPDV	IPTD 最大值减去 IPTD 最小值的差值在 10^{-3} 分界点的上限值	需规定	50 ms	50 ms	1s	不规定
IPLR	包丢失率的上限值	需规定	1×10^{-3}	1×10^{-3}	1×10^{-3}	不规定
IPER	包误差率的上限值	1×10^{-4}	不规定	不规定	不规定	不规定
SPR	虚假包率的上限值	不规定	不规定	不规定	不规定	不规定

9.1.3.1 QoS 等级

表 3 规定了不同 QoS 等级的端到端网络性能的范围。在用户遵守他们与运营商签定的服务等级协议时，网络运营商应该相互配合，满足这些端到端的网络性能指标要求。一定范围的性能组合构成一种 QoS 等级。用户的 QoS 等级与用户 IP 包的传送距离和网络的复杂度有关。根据不同业务和应用的需要，用户可以请求和接收不同 QoS 等级的服务。支持在用户和网络提供商之间动态 QoS 请求的协议有待规定，静态 QoS 类型协议的实现可以用与特定类型相关的包加标记来实现。用户所能得到的服务性能一般会优于表 3 的规定。每个流请求和协商 QoS 等级的方法待定。

表 3 的 IP 业务 QoS 等级分为 4 类： 0 类（class 0）为电信级通信服务；1 类（class 1）为交互型，适于实时交互的业务，例如：达到 POTS 质量的 IP 电话，它对应于 IETF 的加速转发 DiffServ 业务；2 类（class 2）为非交互型，适用于音像流和大批文件的可靠传送，对应于 IETF 的确保转发的 DiffServ；3 类（class 3）为不规范型，指传统的尽力而为的 IP 业务。

9.1.3.2 网络性能指标说明

表 3 中的指标适用于任何以测量点（MP）为边界的端到端的 IP 网络，并且这些指标在一般 IP 网路径上是可以实现的。符合本标准规定的绝大部分 IP 路径都应该满足上述指标。运营商在传递 IP 包时向用户承诺满足上述可用性指标，单个运营商可以提供比本标准所分配指标更好的性能承诺。部分参数在传输距离较短或网络不太复杂时，路径的性能可能会明显优于本标准规定的指标。必须报告所有评估的时间间隔大小，建议 IPTD、IPDV 和 IPLR 的评估时间间隔为 1min。

1）IP 包传输时延(IPTD)的性能指标是指该数据流的平均 IPTD 值加以统计，所估计出的最大值。虽然该数据流的多个包的传输时延可能会超过该界限，但在该数据流的生存期内 IPTD 的平均值(统计估计的)通常应小于表 3 中的可用界限。严格的时延值(比如类型 0)会限制地理上的可用性、网络设计以及技术选择，因此有时可能会超过这些限制（例如：用话带宽调制解调器接入网络或者端点间距离更长）。

2）在一个较长的测量时间间隔内，选择若干短的抽样间隔，可以测量到若干 IPDV 值。其中 95%的 IPDV 测量结果应该满足规定的指标。抽样间隔会影响到捕获 IP 包时延中的 IPDV 的低频和高频变化的能力。IPDV 类型 0 的值依赖于网间电路域的容量，当容量高于 T1 时，有可能获得更好的 IPDV。

IPDV 参数可能会受到下列因素的影响：

——网络中的路由拥塞（高频的 IPTD 变化）。

——TCP 窗口行为（低频的 IPTD 变化）。

——平均网络负载的周期性和非周期性变化（低频的 IPTD 变化）。

——路由更新对 IPTD 的影响（IPTD 的瞬时变化，但这种变化可能会很大）。

在 ATM QoS 2 级连接上应该能够支持这些时延指标，但可能要求 IP 实体发出选择 CTD 指标的信号。IP QoS 等级和 ATM QoS 等级之间的关系参见行标 YD/T 1171-2001《IP 网络技术要求——网络性能参数与指标》。

3）IP 包丢失率(IPLR)的性能指标指该数据流的 IP 包丢失的最大可能性。虽然该数据流也可能丢失单个包，但任何单个包的丢失概率应该小于表 3 中的可用界限。QoS 等级为 0 和 1 是基于这样的假设：10^{-3} 的 IPLR 基本上不影响高质量话音应用和话音编码。

4）IP 包误差率(IPER)的性能指标指 IP 包出现差错的最大可能性。表 3 中的 IPER 值假定包丢失是 IP 包损伤的主要因素，并在 ATM 上承载 IP。

9.1.3.3 不作规定的性能

表 3 中有些 QoS 等级的一些性能参数的值被指定为“不作规定”。 在这种情况下，不规定这些参数的指标，对于它们的任何缺省指标都可以不考虑。

当把一个参数的指标设置为“不作规定”时，该参数的性能有时会非常差。对这些未规定的参数，网络运营商可以单方面保证一些最差服务质量等级，但本标准对此不会做任何规定。

9.1.4 IP 性能指标分配

IP 网络一些指标的分配可以基于分配物理层性能的 G.826 规则。物理层损伤会严重影响 IP 层性能

参数 IPER 和 SPR。

每个 IP 层参数的性能损伤随着传输距离和网络复杂度的增加而增加。“复杂度”指损伤随着额外选路和排队过程的增加而增加，或者 / 并且随着 IP 网络管辖边界交叉的增多而增加。“传输距离”指损伤并非由于选路和排队过程直接造成的，在 IP 网设计中很难直接控制。

IP 网络的指标分配原则基于以下几个因素制定：

——必须检查参考配置，使其能提供合理的端到端性能。

——每个 IP 节点所允许的复杂度因素将影响分配原则的基础。

——要考虑 IP 节点间的链路速度和传输选项。

——网间互连的层次。

——每个结点处所涉及到的处理(路由或交换，存在信令时的额外功能)。

——在 IP 网络中，是基于距离还是基于复杂度的网络组成部分占主导地位。

——IP 网络使用的机制（如 OSPF 选路，MPLS，DiffServ 等）将影响复杂度因素的权重。

有关 IP 性能指标分配具体参见行标 YD/T 1171-2001《IP 网络技术要求——网络性能参数与指标可用性》。

9.2 服务质量

IP 网服务质量(QoS)是指 IP 包在一个或多个网络中传输的过程中所表现的各种性能，它是对各种性能参数的具体描述。这些性能参数包括：延迟、抖动、吞吐量和包丢失率等。本节提出对 IP 网络服务质量的要求，这对于保证或提高 IP 电话等实时业务的服务质量，具有重要意义。

9.2.1 网络服务质量指标

IP Qos 通常由以下一组可测量的参数来表征。

1）延迟：指在两个参考点间，发送和接收 IP 包的时间间隔。

2）抖动：也称延迟变化。指在一段时间内，某个流中的所有包的传送延迟变化。由于 IP 的数据传送是面向无连接的包交换，每个数据包从源点到目的的路由都可能不同，同时网络的状况也在随时变化，因此出现抖动的可能非常大。

3）吞吐量：指网络中 IP 包的传输速率，可表示为平均速率或峰值速率。

4）包丢失率：指在网络中传输时，可允许的最大丢包率。丢包主要是因为网络阻塞引起的。

产业自网络空间安全协会受控资料

9.2.2 IP 网服务质量要求

1）网络端到端的总时延：一般负载情况时不超过 120ms。

2）抖动：抖动不超过 80ms(根据 IP 电话技术体制的要求)。

3）包丢失率：包丢失率不超过 10%(根据 IP 电话技术体制的要求)。

4）网络协议必须能够支持端到端的服务质量传输。

5）IP 网服务质量的对网络设备的要求见第 15 章。

注：

1 以上列出的各项服务质量参数为暂定值，对这些参数的要求，还有待在实践过程中进一步验证、完善和补充。

2 IP 包在路由器中的转发时延与 IP 包长度有关，IP 电话业务的话音包长度一般不超过 64Byte。根据 IP 网络设计的要求，IP 网络中一个 64Byte 的 IP 包的端到端时延最多包括：两个边缘路由器(2×20ms)+两个接入服务器(2×20ms)+两个汇接路由器(2×10ms)+三个核心路由器(1ms)，因此在一般负载情况下端到端的总时间延迟不超过 120ms。

3 传输延迟包括线路延迟，设备延迟。线路延迟包括电话网延迟，SDH 传送网延迟等。设备延迟包括路由器延迟、电话网交换机延迟、网关延迟等。总的来说，线路延迟较小，传输延迟主要产生在设备上（目前主要是路由器），因此可以用路由器跳数加补偿值来近似计算它。

4 以上所有参数均针对 IP 网络而言。如故障均指 IP 网络可管理的设备出现的故障，不包括 IP 网络以外设备或线路故障。

9.2.3 用户接入服务质量要求

1）IP 网络的接通率：在 IP 网络无阻塞的前提下，接通次数/拨号总次数。

平均接通率≥80%。

2）用户接入认证平均响应时间：从用户正确提交完账号和口令至接入服务器完成认证返回响应。

用户接入认证平均响应时间 = RADIUS 服务器响应时间 ×经过的 RADIUS 服务器级数 + 传输延迟。

用户接入认证平均响应时间≤5s。

3）接入服务器认证成功率：在用户输入账号口令无误的情况下的认证成功率。

接入服务器认证成功率 >99.9%。

4）用户信息层认证平均响应时间：从用户正确提交账号口令至完成认证得到合法 Cookie 为止。

用户信息层认证平均响应时间 = 信息层用户管理服务器响应时间 × 经过的信息层用户管理服务器个数 + 传输延迟。

漫游用户信息层认证响应时间 <10s。

9.2.4 导航系统服务质量要求

1）定时更新导航数据库。

更新间隔 <24h。

2）导航系统服务平均响应时间：从用户发出查询请求至收到导航系统服务器响应为止（不包括查询结果信息的传输时间）。

导航系统服务响应时间 =DNS 服务器响应时间 + 导航系统服务器响应时间 +传输延迟

导航系统服务响应时间 <10s。

有关导航系统更详细的要求参见 YD/T 1151-2001《新业务技术要求—多媒体信息检索》。

9.2.5 计费系统服务质量要求

计费准确率：100%。

9.2.6 网络业务服务质量要求

9.2.6.1 信息检索服务质量要求

信息检索服务响应时间：用户发出检索请求至收到信息检索服务器响应为止（不包括信息内容传输时间）。

信息检索服务响应时间 =DNS 服务器响应时间×经过的 DNS 级数 + 信息检索服务器响应时间 + 传输延迟

信息检索服务平均响应时间 <10s。

有关信息检索服务更详细的要求参见 YD/T 1151-2001《新业务技术要求—多媒体信息检索》。

9.2.6.2 IP 电话服务质量要求

在 IP 网络开放 IP 电话商用业务时，应将其端到端延迟（即主叫到被叫延迟）控制在 400ms 以内，呼叫建立时间应＜5s，IP 网络的包丢失率应控制在 10%以内，延迟变化应＜80ms。当采用 G.723 算法时，IP 网络传输时延在 200ms 以内，两侧网关处理时延之和在 200ms 以内；当采用 G.729 算法时，IP 网络传输时延在 250ms 以内，两侧网关处理时延之和在 150ms 以内。

9.2.6.3 其他新业务服务质量要求

待定。

9.2.7 IP 网提供服务质量的主要方法

目前对于 IP 网如何提供 QoS 的问题主要有以下几种解决方案。

1）MPLS

MPLS 是一个前向转发策略。 MPLS 头的封装是在链路层头和网络传输层头之间。MPLS 将 IP 技术与下层技术结合在一起，兼具了高速交换、QoS 性能、流量控制性能以及 IP 技术的灵活性、可扩展性，它不仅能够解决当前网络中存在的问题，而且能够支持许多新的功能，是一种较为理想的骨干 IP 网技术。

利用 MPLS 可以使网络能够达到较为理想的服务质量保证。其优势主要在于：

a）能够提供以往 IP 网中无法保证的流量工程业务，可最佳利用链路和节点，平衡负荷，确保某些

广东省网络空间安全协会受控资料

业务流有必要带宽，使 IP 网络将能够具备一定的 QoS 能力,这对于日益增长的因特网业务与 IP 网的规模是至关重要的。

b）能够增强网络的性能，它可以实现许多以往技术所无法实现的路由功能，如显式路由功能、环路控制、组播和 VPN 等。

c）能够很容易地和 Diffserv 结合，实现利用业务分类来保证某些实时业务的服务质量。

有关 MPLS 的详细要求可以见行标 YD/T 1162.1-2001《多协议标记交换（MPLS）总体技术要求》。

2）DiffServ

DiffServ 本质上是一种相对优先级策略。DiffServ 在用户和业务网的接口处分级，业务的分级基于每个数据包的不同标识。同一级别的业务在该网络域中会被聚合统一传送，保证相应的延迟、传送速率、抖动等服务质量参数。DiffServ 并不提供从发送者到接收者的端到端服务质量保证，而是在域（domain）的范围内保证与业务分类相对应的服务质量，每个域之间对于不同类别业务的服务质量都应有一定的约定和包标识的翻译机制。DiffServ 的优点是：伸缩性较好，只是规定了有限数量的业务级别，状态信息的数量正比于业务级别，而不是流的数量。另外实现和部署 DiffServ 也相对容易。DiffServ 适合用在 IP 骨干网中。

3）RSVP

资源预留(RSVP)协议是一种预留资源的信令协议。发送端给接收端发送一个 PATH 消息，以指定通信的特性。沿途的每个中间路由器把 PATH 消息转发给由路由协议决定的下一跳。当收到一个 PATH 消息时，接收方做出的反应是用一个 RESV 消息为该流请求资源。沿途的每个中间路由器可以拒绝或接受 RESV 消息请求。如果请求被拒绝，路由器将发送一个出错消息给接收方，并且中断信令的处理过程。如果请求被接受，为该流分配链路带宽和缓冲区空间，并且把相关的流状态信息装入路由器中。 综合业务模型的优点是：能够提供绝对有保证的 QoS；RSVP 在源和目的地间可以使用现有的路由协议决定流的通路。RSVP 的缺点是:伸缩性不好；随着流数目的增加，状态信息的数量成比例上升，占用了大量的路由器存贮空间和处理开销，不适合用在因特网核心中；另外对路由器的要求较高，对保障型业务需要网络全部使用综合业务。 RSVP 更适合于在企业网等中应用。

广东省网络空间安全协会内控资料

10 网络管理要求

10.1 网络管理方式

根据 IP 网络的网络结构形式，网络管理原则上可以采取三级管理的方式，设置一级骨干网网管中心、二级网网管中心和 IP 城域网网管中心。

全国设置一个一级骨干网网管中心。为保证网络管理安全可靠，随着网络发展应在异地设置一个一级网管备用中心。

一级网管中心负责一级骨干网的管理，完成一级骨干网的各项管理功能。此外，一级网管中心还负责各二级网管中心的管理，并可通过二级网管中心对二级网实施各项管理功能。

二级网管中心按二级网服务范围来设置。每个二级网内分别设置一个二级网络管理中心，负责完成二级网的管理功能，此外，还负责各 IP 城域网网管中心的管理，并通过 IP 城域网网管中心对 IP 城域网实施各项管理功能。

每个 IP 城域网内分别设置一个 IP 城域网管理中心，负责完成 IP 城域网的管理功能。

当二级网和 IP 城域网合二为一时，其网管中心也合二为一。

IP 城域网网管中心通过 DCN 和二级网管中心连接。

二级网管中心通过 DCN 和一级网管中心连接。

网络管理结构如图 6 所示。

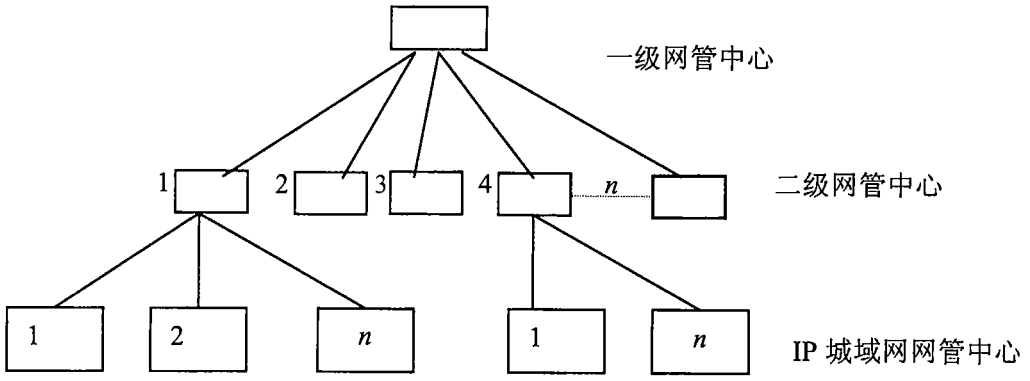


图 6　网络管理结构示意图

10.2　各级网管中心职能

10.2.1　管理对象

1）一级网管中心的管理对象为 IP 一级骨干网中的各种设备以及各二级网管中心；

2）二级网管中心的管理对象为 IP 二级网中的各种设备。

10.2.2　一级网管中心的主要职能

（1）实时监视一级骨干网的运行状况，采集运行数据，进行统计、分析、处理并显示告警。及时发现网络异常,确定异常发生的原因、性质和位置，采取有效的措施并形成异常报告。

（2）应具备被管网络安装、指配、连接以及网络异常时的重新配置和恢复功能。建立数据库，用以存储、检索、查询被管网络的设备配置、软件版本、网络拓扑结构等各种数据，并能及时更新，当数据更改时，网管中心将新数据及时送到相应的被管网络。

（3）实时监视一级骨干网的性能，采集性能数据，定期或按需提供骨干网络的各种分析报告，并存档以备查询。

（4）负责网管系统的安全管理，设置安全管理有关参数，当安全性受到威胁或破坏时立即告警并应存档。此外，网管中心还对所辖的 IP 网的网络安全进行管理。

（5）对二级网的重大异常情况负责协调管理，必要时指挥二级网络管理中心进行处理。

（6）管理本网管中心的相关资源，监视网管网的运行状态。同时对各二级网管中心进行监视和管理。

（7）一级网管中心可以通过 DCN 远程登录到各二级网管中心，实施对 IP 二级网的管理。

（8）一级网管中心负责跨二级网覆盖范围的 VPN 业务管理。二级网管中心应提供相应的管理接口，保证一级网管中心可以通过二级网管中心实施端到端 VPN 业务配置。

10.2.3　二级网管中心的主要职能

（1）实时监视二级网的运行状况，采集运行数据，进行统计、分析、处理并显示告警，及时发现网络异常,确定异常发生的原因、性质和位置，采取有效的措施并形成异常报告。出现故障时向一级网管中心报告。

（2）应具备被管网络安装、指配、连接以及网络异常时的重新配置和恢复功能。建立数据库，用以存储、检索、查询被管网络的设备配置、软件版本、网络拓扑结构等各种数据，并能及时更新，当数据更改时，网管中心将新数据及时送到相应的被管网络。

（3）实时监视二级网的性能，采集性能数据，定期或按需提供二级网的各种分析报告，并存档以备查询。

（4）负责网管系统的安全管理，设置安全管理有关参数，当安全性受到威胁或破坏时立即告警并应存档。此外，网管中心还对所辖的 IP 网的网络安全进行管理。

（5）接收、执行一级网管中心的指令，并将指令内容、执行情况、结果等存档并回送一级网管中心。

（6）对 IP 城域网的重大异常情况负责协调管理，必要时指挥 IP 城域网网络管理中心进行处理。

广东省网络空间安全协会资料

（7）负责管理网中相关资源的管理以及本网管中心的管理。同时对各 IP 城域网网管中心进行监视和管理。

（8）二级网管中心可以通过 DCN 远程登录到各 IP 城域网网管中心，实施对 IP 城域网的管理。

（9）二级网管中心负责跨 IP 城域网覆盖范围的 VPN 业务管理。IP 城域网网管中心应提供相应的管理接口，保证二级网管中心可以通过 IP 城域网网管中心实施端到端 VPN 业务配置。

10.2.4 IP 城域网网管中心的主要职能

（1）实时监视 IP 城域网的运行状况，采集运行数据，进行统计、分析、处理并显示告警。及时发现网络异常,确定异常发生的原因、性质和位置，采取有效的措施并形成异常报告。

（2）应具备被管网络安装、指配、连接以及网络异常时的重新配置和恢复功能，建立数据库，用以存储、检索、查询被管网络的设备配置、软件版本、网络拓扑结构等各种数据，并能及时更新，当数据更改时，网管中心将新数据及时送到相应的被管网络。

（3）实时监视 IP 城域网的性能，采集性能数据，定期或按需提供宽带城域网的各种分析报告，并存档以备查询。

（4）负责网管系统的安全管理，设置安全管理有关参数，当安全性受到威胁或破坏时立即告警并应存档。此外，网管中心还对 IP 城域网的网络安全进行管理。

（5）接收、执行二级网管中心的指令，并将指令内容、执行情况、结果等存档并回送二级网管中心。

（6）管理本网管中心的相关资源，监视网管网的运行状态。

（7）网管中心负责 VPN 业务管理，保证实施端到端 VPN 业务配置。

10.3 网络管理接口

（1）一级网管中心与骨干网路由器和服务器之间采用基于 SNMP 协议的接口。

（2）二级网管中心与二级网路由器和服务器之间采用基于 SNMP 协议的接口。

（3）IP 城域网管中心与城域内路由器和服务器之间采用基于 SNMP 协议的接口。

（4）一级网管中心和二级网管中心之间采用 SNMP 或 CMIP 协议的接口。

随着网络的发展，今后可要求一级网管中心、二级网管中心和 IP 城域网管中心向上提供基于 CMIP 的 Q 接口。

10.4 网管中心组成

网管中心基本由 5 部分组成：网管中心局域网系统、网管主机硬件平台及操作系统、网管平台软件、网管应用软件、外围设备等。

10.5 网管中心的连接

（1）网管中心与 IP 网互连：可通过局域网直接连入本 IP 网网络节点，进行带内管理。随着网络规模和业务量的扩大，可通过专用 DCN 网连接数据网节点，进行带外管理。

（2）网管中心之间的互连。

——在有网管专用 DCN 网时，应优先采用网管专用 DCN 网进行带外管理。

——在无网管专用 DCN 网时，可使用本数据网以 VPN 方式组成的内部 DCN 进行带内管理。

（3）网管专用 DCN 网可以由 X.25、帧中继或 DDN 组建。DCN 网络连接可根据需要设置备份链路。

（4）网管中心的网管主机同时由 IP 网和网管网分配 IP 地址及域名。网管主机和 IP 网通信时使用由数据网分配的 IP 地址，并由 IP 网为其解析它所分配的域名；网管主机和网管网通信时使用由网管网分配的 IP 地址，并由网管网为其解析它所分配的域名。

10.6 与路由器相关的资源管理功能

10.6.1 配置管理

10.6.1.1 拓扑信息管理

能够自动发现 IP 网络中的路由器设备，并动态地显示当前网络的拓扑状况，网管操作员可逐级进入而进行拓扑信息查询。

广东省网络空间安全协会内部资料

10.6.1.2 资源配置及查询功能

实现以下资源配置及查询功能：

1）路由器设备系统信息的查询；

2）端口配置信息查询。

10.6.1.3 路由信息配置、修改及查询功能

实现以下路由信息配置、修改及查询功能：

1）实现对网络路由表的统一管理，设置路由方式及相关参数，查询节点路由信息等：

2）路由协议配置信息查询；

3）路由度量尺度参数配置；

4）路由度量尺度参数查询；

5）路由出口号配置；

6）路由生存期查询；

7）路由掩码参数配置；

8）路由类型配置（无效、终结、转接）。

10.6.1.4 网络互联信息配置及查询

实现以下网络互联信息配置及查询：

1）自治域内路由表信息查询；

2）BGP 路由表信息查询。

10.6.2 故障管理

故障管理负责监视网络设备的故障告警，进行故障诊断及定位分析，告警日志的创建及维护，并通过冗余设备或冗余路由即时恢复措施重新提供服务。

告警信息应可通过图形方式对不同的运行状态和告警级别进行显示，并同时产生告警日志，供查询。

告警类型分为：设备告警、环境告警、通信告警、服务质量告警等。

告警级别分为：严重告警（CRITICAL）、重大告警（MAJOR）、次要告警（MINOR）、警告告警（WARNING）、已清除的告警（CLEARED）、未确定（INDETERMINATE）。

告警状态分为：存在（RAISED）、清除（CLEARED）。

10.6.2.1 设备告警

在路由器设备出现故障或超出某些性能要求范围时，应发送设备告警。

节点故障告警：当发现某节点设备运行状态异常时发送节点故障告警。此类告警发生在路由器关机、重启动或严重故障导致无法工作时。

接口故障告警：当发现某设备的某个接口运行状态异常时发送接口故障告警。此类告警发生在某个接口由于硬件或连接故障等而导致数据传送失效时。

电源故障告警：当发现某节点设备电源电压超出设备预定范围时，发送电源故障告警。

CPU 利用率超限告警：当发现某设备 CPU 利用率超出设备限定范围时，发送此类告警。（该功能在实现时作为可选）

10.6.2.2 通信告警

支持以下通信告警：

传输链路故障告警：当传输线路出现故障时，发送此类告警。

IP 通信协议错误告警：当某个节点由于软件故障等导致 IP 协议无法支持时，发送此类告警。

TCP 通信协议错误告警：当某个节点由于软件故障等导致 TCP 协议无法支持时，发送此类告警。

10.6.2.3 环境告警

当系统内某些环境变量超出设备所允许的范围时，如超出工作温度限制、湿度过高等，发送环境告警。（该功能在实现时作为可选）

广东省网络空间安全协会受控资料

10.6.2.4 服务质量（QoS）告警

当网络出现性能下降到超越性能门限、网络部分区域拥塞时，产生服务质量告警。

10.6.2.5 告警日志创建及维护

系统对产生的故障告警及事件信息进行记录，以便用户对历史告警进行查询。告警日志需定期进行维护及删除。

有关告警日志的操作功能：

进行告警日志查询（按节点标识、告警级别、日期等）；

对告警事件进行确认；

告警日志维护（定期备份、删除旧日志等）。

10.6.2.6 故障定位

当一个物理设备发生故障时，可能产生多个失效告警，网管系统应能够进行故障定位，确定与实际失效有关的告警。故障可定位到设备的端口级。

10.6.2.7 测试功能

测试功能可在故障发生前有计划地进行，也可以在发现问题后作为诊断手段。测试功能在不影响网络的正常业务情况下，主要完成连通性测试、网络传送能力测试等。

连通性测试：使用 PING 等操作进行网络连通性测试。

传送能力测试：测试网络的传送能力，如：点到点传送延时等。

通信协议测试：测试某个节点对 IP 协议的可支持性。

10.6.3 性能管理

性能管理是向网络运营者提供网络设备的性能特征，以供网络趋势分析、网络扩建、网络控制时参考。性能管理主要包括：性能监视、性能分析、性能控制、性能测试。

10.6.3.1 性能监视

1）定期收集网络中各路由器每一端口链路层的统计数据。

2）定期收集网络中各路由器每一端口 IP 层的统计数据。

3）定期收集网络各路由器 ICMP 协议实体的统计数据。

4）定期收集网络中各路由器中 SNMP 协议实体的统计数据。

5）收集的性能参数应包括：

——链路利用率；

——收发消息数；

——丢包率；

——端到端时延等。

10.6.3.2 性能分析

性能分析以性能监视时收集的一系列统计参数为基础。

——作出入/出端口链路层流量分析，并以图形表示；

——作出入/出端口 IP 层流量分析，并以图形表示；

——以各个骨干节点的各个端口流量分析为基础，作出整个骨干网的流量 / 路由相关分析，并以直观图形表示。

10.6.3.3 性能控制

以上述性能分析为基础，对制约网络性能的相关参数进行调整。

——修改路由器节点的路由控制表；

——性能阈值参数控制。

10.6.3.4 性能测试

用于测试网络的传送性能，主要包括：

——点到点最大传输时延测试；

北京网络空间安全协会受控资料

——点到点最小传输时延测试；

——点到点平均传输时延测试。

10.6.4 账务管理

见第 13 章。

10.6.5 安全管理

见第 11 章。

10.7 与服务器相关的资源管理功能

网上的服务器用于完成网络特定的服务功能。服务器资源主要有：

1）网络接入服务器（NAS）；

2）宽带网络接入服务器（BNAS）；

3）域名服务器（DNS）；

4）网关服务器（GATEWAY）；

5）E-mail 服务器；

6）IP 电话网关与网守；

7）信息源服务器；

8）其他。

对网上各种服务器公共资源的管理深度要求应视服务器本身执行的功能而定。

对各种服务器的公共管理功能如下。

1）配置管理

a）服务器资源注册：各种服务器准备就绪后应向网管系统报告其身份。

b）服务器配置更改报告：当服务器的某些配置发生改变时应向网管系统报告。

c）功能相关的实体配置。

2）故障管理

连通性测试：为便于故障定位分析或链路性能分析，各种服务器应接收网管系统发来的连通性测试要求，并返回测试结果。

3）安全管理

a）冗余备份：为增加网络的安全系数，对于关键的服务器应冗余备份。

b）密钥管理：对于与密钥相关的服务器，应对其设置密钥生命期、密钥备份等管理功能。

c）其他见第 11 章的规定。

10.8 与传输相关的管理功能

网管系统应提供对路由器上与 SDH、WDM 光传送相关的管理功能。对于 SDH 和 WDM 网络的管理，由专门的传输网网管系统负责。

路由器中与传输相关的管理功能主要包括：

1）对路由器接口模块中 SDH 帧结构、SDH 通道和定时方式等进行相关配置。

2）路由器应对 SDH 或 WDM 通道状态进行监视，以发现接口故障（如信号丢失、帧失步等），并以告警方式反映给网络管理员。

3）对 SDH 通道性能进行管理，支持差错监视字节（B1、B2 和 B3）、复用段远端差错指示字节（M1）和通道状态字节（G1）的监视。

4）对 SDH 或 WDM 物理接口参数进行监视，如光功率、信噪比等。

5）对路由器 SDH 接口的自动保护倒换（APS）功能进行管理。

11 网络安全要求

11.1 概述

对任何一个 IP 网来讲，安全策略不健全将对 IP 信息网的正常运营带来不可估量的损失。网络安全

广东省网络空间安全协会资料

是指通过采用合适的安全技术与安全管理措施，确保网络上的信息和服务不被未经授权的用户使用。网络安全是一个风险问题，其基本策略是在安全性能和安全支出上取得平衡，同时保证信息传递的完整性、可用性和保密性。网络安全机制应保障所有信息网内部的资源不受意外事件的侵袭。

IP 网络安全通常包括两个方面：技术要求和管理要求。在技术方面上，网络安全由以下几个方面组成：物理安全，网络安全和信息安全。另外，安全管理规范是网络安全所必须的，人为因素是网络安全的最大隐患，应该引起高度重视。

有关 IP 网络的详细要求可以参考行标 YD/T XXXX-2001《IP 网络安全-总技术要求》。

11.2 物理安全

保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误以及各种计算机犯罪行为导致的破坏。它包括 3 个方面的内容：

1）环境安全：对系统所在环境的安全保护，如区域保护和灾难保护，参见国家标准 GB50173-93《电子计算机机房设计规范》、国标 GB2887-89《计算机站场地要求》，GB9361-88《计算机站场地安全要求》。

2）设备安全：网络设备如计算机以及电缆、网桥和路由器等的防盗、防毁、防电磁辐射泄露、防止线路截获、抗电磁干扰及电源保护等。保护的措施有：对主机房及重要信息存贮、收发部门进行屏蔽处理；对本地网、局域网传输线路传导辐射的抑制；对诊断设备的辐射进行防范。

3）媒体安全：包括媒体数据的安全及媒体本身的安全。可以采用多机数据备份等技术加以保护。

11.3 网络安全

网络安全把需要保护的网络用防火墙从开放因特网中隔离开来，实现内部信任网与外部不可信任网之间或是内部网不同网络之间安全区域的隔离与访问控制，保证网络系统及网络服务的可用性。

1）内外网隔离及访问控制：在内外部网络之间设置防火墙，实现内部网络的访问控制。根据防范的方式和侧重点的不同，可以选择分组过滤或应用代理等不同类型的防火墙。

2）内部网不同安全域的隔离及访问控制：采用防火墙技术实现内部网不同安全域的隔离及访问控制。

3）网络安全检测：安装网络安全评估分析软件，利用此类软件扫描分析网络系统，及时发现并修正存在的弱点和漏洞。

4）审计与监控：安装网络安全评估分析软件，利用此类软件对用户使用计算机网络系统的过程进行记录，以便发现和预防可能的破坏活动。

5）全网安全远程扫描和评估：在核心节点和网络管理中心安装网络安全扫描器，对整个网络进行安全扫描。

6）网络备份系统：设计合理的备份机制，以便在出现问题时能够及时恢复。根据系统安全需要，备份系统可以多种多样。比如在设计网络拓扑时，任一节点与网络其他之间应该至少有两条物理连接，以供迂回路由；关键网络设备都必须有备用。

11.4 信息安全

在网络实施过程中，应尽量利用各种手段来保障信息的安全搜索、存放和共享。最基本的原则是各级领导首先制定出相应的安全规范和政策。信息安全包括信息传输的安全、信息存贮的安全以及对网络传输信息内容的审计 3 个方面。

1）鉴别：利用口令机制、智能卡或个体特征鉴别技术，对通信各方的身份进行鉴定。

2）数据传输加密技术：利用密码技术，对传输中的数据流进行加密，防止窃听、泄露、篡改和破坏。加密可以在不同的层次上进行，如：链路加密，节点加密和端到端的加密(比如传输前对文件进行加密)。

3）数据存贮安全：对保存在用户终端中的数据进行安全保护，防止关键数据被窃取。选择使用安全数据库系统，以及基于口令/密码算法的身份验证。

4）信息内容审计：安装信息内容审计软件，对进出网络的信息内容进行审计，以防止或追查可能的泄密行为。

广东省网络空间安全协会内部资料

5）口令管理：目前发现的漏洞，大多是由于口令管理不严所造成的，这使得黑客可以乘虚而入。因此口令的有效管理是非常基本的，也是非常重要的。

6）用户账号管理：在为用户建立账号时，应注意保证每个用户的 ID 的唯一性，避免使用公用账号；对于过期的账号要及时封闭；对于长期不用的账号要定期检查，必要时封闭(因为这样的账号通常是黑客袭击的目标，他们可以在利用其进行攻击而长时间不会被发现)。

7）加强信息服务器的安全措施：如果对外开放的信息服务器本身是不安全的，就相当于在系统的防护罩上开了一个漏洞，那么其他的安全工作做得再多，也会付诸东流。因此，系统管理员和信息服务器的管理人员必须仔细注意服务器本身的安全设施，并随时更新版本。

8）系统的高可用性和备份措施：在一个与企业关系密切相关的“战略型”应用系统中，每一分钟的系统“无法提供服务(包括数据与服务器)”都意味着损失，所以对系统的高可用性要求是必然的、不可商量的。高可靠性的原理是利用冗余技术，通过系统中硬件、软件、数据的冗余，实现当系统中的某一个环节(硬件、软件、数据)出现故障时，使用冗余部件提供服务。

11.5 安全管理规范

为了保护网络的安全性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，安全管理规范也是网络安全所必须的。信息安全部门应该根据管理原则和该系统处理数据的保密性，制定相应的管理制度或采取相应的规范。

制定安全规范有以下原则：

1）多人负责原则：每一项与安全有关的活动，都必须有两人或多人在场。

2）任期有限原则：任何人最好不要长期担任与安全有关的职务。

3）职责分离原则：在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情。

安全管理规范包括：密码长度、修改日期及不同平台、不同机构需要的不同安全设置；每条信息哪些人可以访问；每个人在向其他人传播信息时所必须遵守的规则；违反规定的情况如何处理等。

广东省网络空间安全协会受控资料

12 网络互通要求

12.1 概述

本章规定 IP 网络与 PSTN/ISDN 网络、IP 网络与 ATM 网络等之间的互通基本要求。有关具体要求参见相关标准。

12.2 IP 网络与 PSTN/ISDN 网络之间的互通

12.2.1 方式 1—采用网络接入服务器

PSTN 和 ISDN 用户通过网络接入服务器拨号接入到 IP 网络， 网络接入服务器位于 PSTN/ISDN 网络与 IP 网络的接口处，如图 7 所示。网络接入服务器和 PSTN/ISDN 网络之间可以采用 ISDN DSS1（30B+D）、中国 1 号信令或 No.7 信令，有关网络接入服务器具体要求见 YD/T 1045。

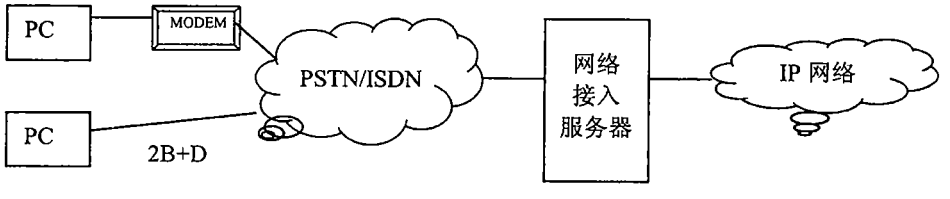


图 7 IP 网络与 PSTN/ISDN 网络互通—通过网络接入服务器示意图

12.2.2 方式 2—采用 IP 电话网关

PSTN 和 ISDN 用户通过 IP 电话网关接入到 IP 网络，呼叫 PC 用户， 也可以呼叫另一 PSTN/ISDN

网络的用户。IP 电话网关位于 PSTN/ISDN 网络与 IP 网络的接口处，如图 8 所示。IP 电话网关和 PSTN/ISDN 网络之间可以采用 ISDN DSS1（30B+D），中国 1 号信令或 No.7 信令，具体要求见 YD/T 1044。

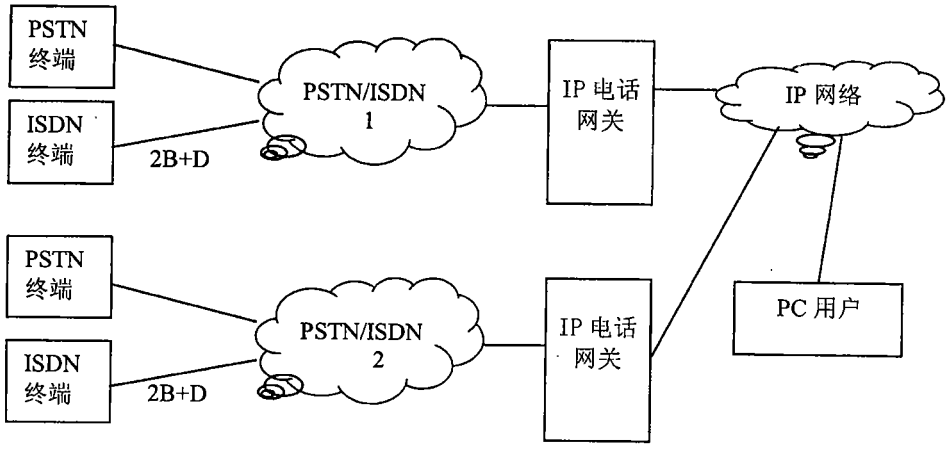
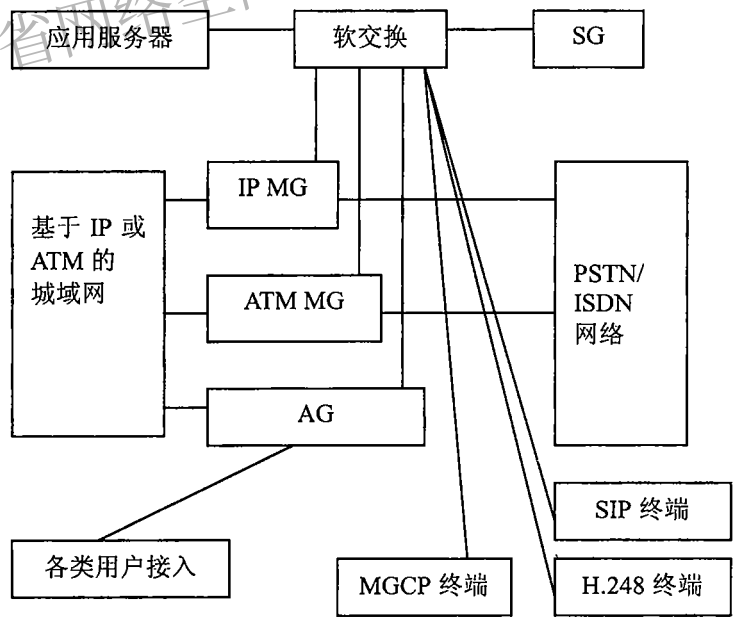


图 8　IP 网络与 PSTN/ISDN 网络互通—通过 IP 电话网关示意图

12.2.3　方式 3—采用软交换设备方式

IP 网络与 PSTN/ISDN 网络互通可以在城域网汇聚层采用软交换、中继网关和信令网关进行，通过软交换、中继网关和信令网关相互配合，PSTN/ISDN 网络用户可以通过 IP 网络与另一 PSTN/ISDN 网络的用户进行通信，也可以与 IP 网络中的用户进行通信，如图 9 所示。有关软交换设备的具体要求参见相关标准和规定。

广东省网络空间安全协会受控资料



SS：软交换设备　　SG：信令网关　AG：综合接入媒体网关
IP MG：IP 中继媒体网关　　ATM MG：　ATM 中继媒体网关

图 9　IP 网络与 PSTN/ISDN 网络互通——通过软交换设备示意图

12.3　IP 网络与 GSM 网络之间的互通

从技术成熟度考虑，目前 IP 电话与 GSM 的互通采用通过 GMSC 的方式比较合适，采用其他互通方式有待进一步研究。IP 电话与 GSM 的互通详细网络组织如图 10 所示，网关与网关所在本地网内的 GMSC

之间设置电路，从而保证来自移动网的 IP 电话呼叫立即进入 IP 网， IP 网至移动用户的呼叫立即进入移动网。具体流程见 YD/T 1044。

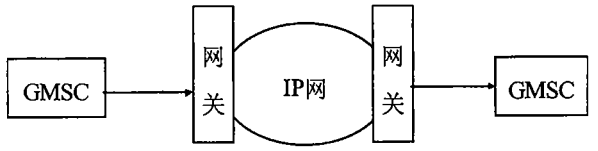


图 10 IP 电话网与 GSM 互通的网络组织示意图

12.4 IP 网络与 ATM 网络之间的互通

12.4.1 ATM PVC 方式

IP 网络与 ATM 网络之间的互通采用 ATM PVC 方式，如图 11 所示。

图 11 IP 网络与 ATM 网络之间的互通—ATM PVC 方式

为了实现与 ATM 网络互通, IP 网络中的高端路由器应支持 ATM 协议。

高端路由器应支持 ATM PVC 连接, 采用 AAL5 适配层, 支持 ATM 的 CBR、UBR 和 VBR 业务, 支持业务量整形。具体见 YD/T 1097 中相应的要求。

12.4.2 CIPOA 方式

IP 网络与 ATM 网络之间的互通采用 ATM 上支持传统 IP 及地址解析协议(CIPOA)，结构如图 12 所示。

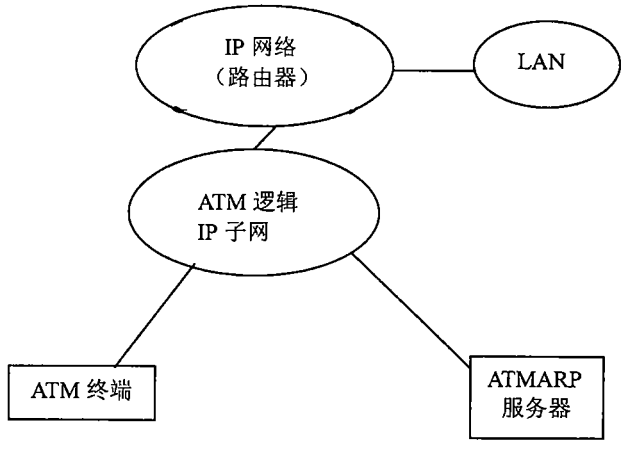


图 12 IP 网络与 ATM 网络之间的互通—CIPOA 方式

在这种方式下， 路由器应支持 CIPOA 协议。具体见 YD/T 1097 中相应的要求。

13 计费和结算要求

13.1 概述

本章规定 IP 网络的计费要求， 有关 IP 网络计费的详细要求见行标 YD/T 1149-2001《IP 网络技术

广东省网络空间安全协会受控资料

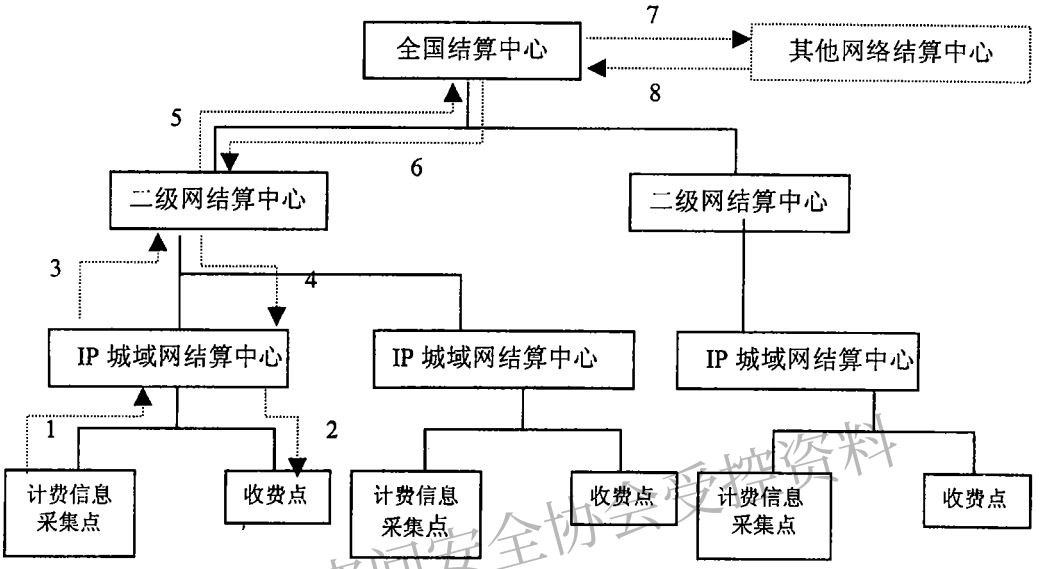
要求——计费》。

13.2 计费结算体系结构

计费结算体系结构如图 13 所示，计费点采集的计费信息送交结算中心进行结算，结算账单送交收费点进行收费。

结算中心原则上根据网络结构的等级来设置：第一级为全国结算中心，第二级为二级网结算中心，第三级为 IP 城域网结算中心。计费信息采集点只负责计费信息的采集，不支持结算。

当二级网与 IP 城域网合一时， 其结算中心也将合一。



广东省网络空间安全协会受控资料

图 13 结算体系示意图

图 13 中的步骤如下：

1：提交所有用户的网络接入费、有偿信息服务费清单；

2：发往收费点收费账单；

3：转交其他 IP 城域网漫游用户的网络接入费、有偿信息服务费清单；

4：转交本 IP 城域网漫游用户的网络接入费、有偿信息服务费清单；

5：转交其他二级网漫游用户的网络接入费、有偿信息服务费清单；

6：转交本二级网漫游用户的网络接入费、有偿信息服务费清单；

7：发往其他网络结算中心账单；

8：接收其他网络结算中心账单。

13.3 计费

计费、结算与业务密切相关，因此本节重点描述基本因特网接入业务的计费和结算，其他业务的计费、结算将在相应的业务规范中明确规定。

IP 网络的计费内容应包括网络接入费和有偿信息服务费。

13.3.1 网络接入费

网络接入费是指用户接入 Internet 网络，使用 IP 电话/FAX、Web 业务、电子商务、电子邮件等业务的费用。

13.3.1.1 拨号接入用户

1）接入方式

网费 = 访问时长 × 费率。

费率的参考参数包括：接入方式、接入速率。

2）计费信息采集点

拨号用户由 RADIUS 服务器记录网络用户每次接入网络的接入费计费信息。

3）计费参数

拨号接入用户使用的计费参数如下：

——用户账号；

——用户属地；

——用户访问地；

——访问日期；

——开始时刻；

——终止时刻；

——访问时长；

——其他。

13.3.1.2 专线接入用户

1）计费方式

网费 = 数据量×费率。

数据量指流入流出数据量之和。

费率的参考参数包括：接入方式、接入速率。

2）计费信息采集点

专线用户的计费信息采集点的设置视具体情况而定，例如：当通过路由器提供专线接入时，计费信息采集点设在路由器。

3）计费参数

专线用户使用的计费参数如下：

——用户账号；

——用户属地；

——访问日期；

——流入数据量；

——流出数据量；

——总数据量；

——其他。

13.3.1.3 IP 电话/传真用户计费方式

（1）计费方式

IP 电话由主叫用户付费，费用包括普通电话网的使用费和 IP 电话网的使用费。普通电话网的使用费不再单收，IP 电话 / 传真以时长（对普通用户）或流量（对专线用户）来收费。

IP 电话/传真费用 = 费率 × 时长（或流量）

（2）计费信息采集点

对于 IP 电话，在“电话到电话”的情况下计费信息采集点设在发端网关，在“PC 到电话”的情况下计费信息采集点设在相应网守。

（3）计费参数

IP 电话用户使用的计费参数如下：

——主叫用户号码；

——被叫用户号码；

——通话日期；

——通话开始时间；

广东省网络空间安全协会受控资料

——通话终止时间；

——通话时长；

——业务类别；

——主叫网关的 IP 地址；

——通话终止原因；

——其他。

13.3.2 有偿信息服务费

有偿信息服务费是指用户上网之后访问收费信息源的费用，是附加在接入费之上的使用有偿信息服务的费用。

对于与无线 IP 网达成协议的有偿信息服务提供商，无线 IP 网为其提供信息费管理。

1）计费方式

用户的有偿信息服务费包括两部分，即：

有偿信息服务费 = 第一类信息费 + 第二类信息费

第一类为月租费；

第二类为按实际访问的 URL 条目收取的费用，收取方式为：

第二类信息费 = 访问 URL 条目×费率

第一类信息费为固定费用，第二类信息费为浮动费用。

2）计费信息采集点

计费信息采集点根据认证方式的不同分为两类：

第一类信息源采用标准 HTTP 认证机制，用户通过 IP 网络上的代理服务器访问信息源，计费信息在代理服务器上采集。

第二类信息源采用用户身份状态字认证机制，用户直接访问信息源，计费信息在信息源上采集。

13.4 结算

13.4.1 全国结算中心的功能

全国结算中心的功能如下：

1）定期接收二级网结算中心递交的其他二级网用户的网络接入费清单，转至该用户开户地所在二级网结算中心；

2）定期接收二级网结算中心递交的其他二级网用户的有偿信息服务费清单，转至该用户开户地所在二级网结算中心；

3）各二级网网络接入费和有偿信息服务费的结算；

4）将与本 IP 网有结算关系的其他信息网络提交的用户访问账单转至用户所在二级网结算中心；

5）汇总非本 IP 网用户的账单，递交给与本 IP 网有结算关系的其他网络经营者。

13.4.2 二级网结算中心的功能

二级网结算中心的功能如下：

1）定期接收全国结算中心转交的其他二级网结算中心提供的本二级网用户访问其他二级网付费信息源的有偿信息服务费清单；

2）定期接收全国结算中心转交的其他二级网结算中心提供的本二级网漫游用户的网络接入费清单；

3）定期接收全国结算中心转交的其他信息网络提供的本二级网用户的总费用账单；

4）定将其他二级网用户访问本二级网付费信息源的有偿信息服务费清单交至全国结算中心；

5）定期将其他二级网漫游用户的网络接入费清单交至全国结算中心；

6）各 IP 城域网网络接入费和有偿信息服务费的结算。

13.4.3 IP 城域网结算中心的功能

IP 城域网结算中心的功能如下：

1）定期接收 IP 城域网内各计费信息采集点提交的用户的网络接入费、有偿信息服务费清单；

广东省网络空间安全协会受控资料

2）定期接收二级网结算中心转交的其他 IP 城域网结算中心提供的本 IP 城域网用户访问其他 IP 城域网付费信息源的有偿信息服务费清单；

3）定期接收二级网结算中心转交的其他 IP 城域网结算中心提供的本 IP 城域网漫游用户的网络接入费清单；

4）定期接收二级网结算中心转交的其他信息网络提供的本 IP 城域网用户的总费用账单；

5）定期将其他 IP 城域网用户访问本 IP 城域网付费信息源的有偿信息服务费清单交至上级结算中心；

6）定期将其他 IP 城域网漫游用户的网络接入费清单交至上级结算中心；

7）定期汇总本 IP 城域网用户的网络接入费和有偿信息服务费清单，按照计费方式生成账单，发往指定收费点。

14 同步要求

IP 网络的同步应由数字同步网来提供。全国数字同步网的同步方式、网络结构、同步等级、时钟性能以及同步网性能参见 1994 年 2 月原邮电部颁发的《数字同步网的规划方法与组织原则》。

采用 IP over SDH 和 IP over WDM 技术的高端路由器以 SDH 帧结构进行传输，要求其定时系统应符合 SDH 系统对同步时钟的要求。

1)原则上，采用 IP over WDM 技术的 IP 网节点应具有外同步接口，接入相应的同步网时钟设备 BITS，即采用 BITS 上的外同步信号。路由器应同时支持线路定时方式，接收来自线路系统的定时信号。考虑到网同步的安全可靠性，在定时方式上，采用外定时方式为主用定时方式，线路定时方式为备用定时方式。当不具备外定时条件时，可以采用内部定时源信号。

2）采用 IP over SDH 技术的 IP 网节点，由于 SDH 网本身为同步网络，可以采用线路定时方式，直接从线路系统提取定时信号。(IP 网节点同步信号技术指标参照 SDH 系统同步要求。)

3）关于 SDH 传输设备的同步，参照 SDH 系统同步要求。

IP 网络应实现全网的时间同步（支持网络时间协议 NTP），向内部所有设备提供精确的、持续的时间标记。

广东省网络空间安全协会会员资料

15 主要组网设备基本要求

15.1 概述

本章主要规定 IP 网上主要组网设备的基本功能要求。包括：高端（核心）路由器，边缘路由器，接入服务器，宽带接入服务器，软交换设备，IP 电话网关设备，千兆比以太网第 2 层交换机，千兆比以太网第 3 层交换机，SDH 设备以及 WDM 设备等。

15.2 高端路由器

高端路由器通常位于骨干网，为骨干网转发数据提供路由处理能力和传输带宽。

高端路由器必须实现以下基本功能：

1）实现包括 IP、ICMP 以及其他相关的因特网协议。

2）对每个连接到的网络，路由器必须实现该网络所要求的功能。这些功能通常包括：

——IP 数据包的封装/解封装;

——根据该网络所支持的最大数据包大小发送或接收 IP 数据包，该大小是网络最大传输单元(MTU);

——将 IP 地址与相应网络的链路层地址相互转换，例如将 IP 地址转换成以太网硬件地址;

——响应网络支持的流量控制和差错指示。

3）接收及转发数据包，并负责缓冲区管理、拥塞控制以及转发的公平性。

——应能辨认差错状态，并按要求产生 ICMP 差错消息;

——丢弃生存时间（TTL）域为 0 的数据包;

——当下一网络 MTU 较小时将数据包分段。

4）按照路由表信息，为每个 IP 数据包选择下一跳目的地。

5）支持 OSPF v2、IS-IS 和 RIP V2 等内部网关协议（IGP）与其他同一自治域中路由器交换路由信息及可达性信息。支持 BGP 4 外部网关协议与其他自治域交换拓扑信息。

6）提供系统网络管理和控制机制，包括存储/上载配置、诊断、升级、状态报告、异常情况报告及控制等。

7）提供物理层传输接口和适配功能。

8）提供组播功能。

9）提供拥塞控制功能。

10）提供同步和定时功能。

11）提供包数、字节数、端口、业务类型等信息统计功能。

12）提供用于完成数据包过滤、地址转换、访问控制、数据加密、防火墙及地址分配等功能。

有关高端核心路由器的详细要求见 YD/T 1097。

15.3 边缘路由器

边缘路由器一般位于公网边缘，是通过转发数据包来实现连接一级骨干网与二级网的路由器。

边缘路由器必须实现以下基本功能。

1）实现包括 IP，ICMP 以及其它相关的互联网协议。

2）对每个连接到的网络，路由器必须实现该网络所要求的功能。这些功能通常包括：

——IP 数据包的封装/解封装；

——根据该网络所支持的最大数据包大小发送或接收 IP 数据包，该大小是网络最大传输单元（MTU）；

——将 IP 地址与相应网络的链路层地址相互转换，例如将 IP 地址转换成以太网硬件地址；

——响应网络支持的流量控制和差错指示。

3）接收及转发数据包，并负责缓冲区管理、拥塞控制以及转发的公平性：

——应能辨认差错状态，并按要求产生 ICMP 差错消息；

——丢弃生存时间（TTL）域为 0 的数据包；

——当下一网络 MTU 较小时将数据包分段。

4）按照路由表信息，为每个 IP 数据包选择下一跳目的地。

5）支持 OSPF v2、IS-IS 和 RIP V2 等内部网关协议（IGP）与其他同一自治域中路由器交换路由信息及可达性信息。支持 BGP 4 外部网关协议与其他自治域交换拓扑信息。

6）提供系统网络管理和控制机制，包括存储/上载配置、诊断、升级、状态报告、异常情况报告及控制等。

有关边缘路由器的详细要求见 YD/T 1096。

15.4 接入服务器

接入服务器通常位于公用电话网（PSTN/ISDN）与 IP 网之间，是将拨号用户接入 IP 网的网络服务器。

接入服务器应实现以下基本功能：

1）接口功能：网络接入服务器与公用电话（PSTN/ISDN）网和 IP 网都有通信接口。在 PSTN 侧有 PSTN 接口和 ISDN 接口；在 IP 网侧有 LAN 接口和串行同步接口。

2）通信协议实现和转换功能：提供电话网（PSTN/ISDN）和 IP 网之间的协议转换。

3）接入认证与授权功能：网络接入服务器对拨号用户进网时拨号用户的信用进行认证。用户接入认证可以根据用户的电话主叫号码来认证，也可以根据用户的用户名和口令来认证。

4）计费功能：网络接入服务器记录拨号上网用户的接入费用，接入费用是通过接入时长乘以费率而得到的。

5）防火墙功能：网络接入服务器的防火墙功能表现为根据不同的用户权限向用户提供不同的接入能力。网络接入服务器的防火墙功能可以有两种方式来提供，分别称为 IP Filter 和 IP Pool。

6）拨号虚拟专网（VPDN）：对请求建立虚拟数据专网的拨号用户进行用户资格认证。为通过资格

广东省网络空间安全协会受控资料

认证的用户建立虚拟数据专网的隧道、数据包传送和拆除隧道等。

7）中继合群功能：中继合群功能指的是网络接入服务器可以处理来自同一个中继群的不同被叫号（相应于不同的 ISP）的能力。

8）来电指示功能：当拨号接入用户已在 IP 网中工作时，有以该用户主叫号为呼入对象的电话呼叫，网络接入服务器即向拨号用户指示有来电呼叫。

9）网管接口功能：网络接入服务器接受 IP 网网管的管理，完成网络管理的功能：配置管理、性能管理、故障管理、安全管理、记账管理。

10）多链路捆绑功能：网络接入服务器应支持多链路捆绑工作模式，网络接入服务器支持 ISDN 的 2B 捆绑。对于 2 个或多个 PSTN 链路的捆绑，PSTN 链路与 ISDN 的 B 通道的捆绑为可选项。

11）远端拨号接入监控功能：网络接入服务器提供远端拨号接入监控功能，供远端维护和监控。这是一项可选的功能，主要是用于对网络接入服务器本身的维护之用。

12）设备的管理功能：网络接入服务器应提供远端拨号接入监控功能和本地控制台（console）管理功能，网络接入服务器应具有远程拨入功能。

有关接入服务器的详细要求见 YD/T 1045。

15.5 宽带接入服务器

宽带网络接入服务器位于骨干网的边缘层，作为用户接入网和核心业务网之间的网关，终结来自用户接入网的连接（主要是高速的用户接入网），提供接入到宽带核心业务网（主要为 IP 网和 ATM 网）的服务。

宽带网络接入服务器应实现以下基本功能：

1）接口功能

宽带网络接入服务器在用户侧有 *x*DSL 接口、Cabel Modem 的接口、帧中继/DDN 的接口和 LAN 接口；在业务网侧有 Gbit/s LAN 接口、ATM 接口、PoS 接口或 IP over WDM 接口。

2）通信协议实现和转换功能

宽带网络接入服务器是面向不同类型接入设备（如 DSLAM、CMTS、LAN 边缘交换机等）提供端到端宽带连接的一种新型网络路由设备，终结来自用户的各种连接，包括基于 PPP 的会话的 PVC 连接。

3）流量控制和管理功能

宽带网络接入服务器接入的用户种类不同，用户的业务需求也不同，可对来自用户的各种连接中的流量加以整形，应支持用户对业务带宽的集中控制和管理，保证与用户协定的服务质量。

4）接入认证与授权、计费和统计功能

宽带网络接入服务器应能对不同的用户连接采取不同的集中接入认证与授权，提供计费信息和统计信息。

5）防火墙功能和 NAT 功能

宽带网络接入服务器可选地支持防火墙功能， 如果支持，主要有两种方式，分别称为 IP Filter 和 IP Pool。IP Filter 是指宽带网络接入服务器提供 IP 包的过滤功能，向不同权限的用户提供不同层次的 IP 包过滤功能，以实现不同的用户有不同的接入能力。IP Pool 是指根据用户的授权从不同的 IP Pool 中读取 IP 地址给相应的用户作为用户的主叫 IP 地址，在相应路由器则确定对不同主叫 IP 地址的不同的 IP 包的过滤能力，从而实现不同的用户有不同的接入能力。

NAT 功能可选。

6）IP 安全网关功能

宽带网络接入服务器可为用户提供 IP 安全服务，即 IP VPN 服务，可以支持基于 IPSec （IP 网络安全的标准协议）方式在 IP 网络上生成安全隧道，为用户提供在 IP 网络或 Internet 上建立安全的点对点连接。宽带网络接入服务器应具备开启和终结 IP 隧道的功能，支持公共密钥系统认证。

7）网管接口功能

宽带网络接入服务器接受 IP/ATM 业务网网管的管理，完成网络管理功能：配置管理、性能管理、

广东省网络空间安全协会受控资料

故障管理、安全管理及记账管理等。

宽带网络接入服务器内置网管代理模块，通过网管代理模块实现与网管的通信，采集系统的信息并维护 MIB 库。

宽带网络接入服务器采用的管理协议为 SNMP，配置管理也应可通过 Telnet 来实现，其应具有 Telnet 通信协议接口和口令等安全管理功能。

8）设备的监控和管理功能

宽带网络接入服务器应提供远端拨号接入监控功能和本地控制台（console）管理功能。远端拨号终端或本地控制台应能实现宽带网络接入服务器故障恢复后重启动（reboot）功能，实现对其维护和监控功能；远端拨号终端或本地控制台应能实现修改用户账单的功能，可以添加或撤销用户账单；远端拨号终端或本地控制台应能实现设备安全控制管理，可以修改用户身份码（PIN）,强制拆除连接；远端拨号终端或本地控制台还应能实现设备故障定位功能。

有关宽带接入服务器的详细要求见 YD/T 1148。

15.6 软交换设备

软交换设备（SoftSwitch）是电路交换网向分组网演进的核心设备，也是下一代电信网络的重要设备之一，它独立于底层承载协议，主要完成呼叫控制、资源分配、协议处理、路由、认证、计费等主要功能，并可以向用户提供现有电路交换机所能提供的所有业务以及第三方业务。

软交换是多种逻辑功能实体的集合，提供综合业务的呼叫控制、连接以及部分业务功能，是下一代电信网中语音/数据/视频业务呼叫、控制、业务提供的核心设备，也是目前电路交换网向分组网演进的主要设备之一。

软交换的主要设计思想是业务/控制与传送/接入分离，各实体之间通过标准的协议进行连接和通信。

软交换的主要功能单元包括：

——媒体网关接入功能；

——呼叫控制功能；

——业务提供功能；

——业务交换功能；

——资源管理功能；

——互连互通功能；

——SIP 代理功能；

——信令网关功能（任选）。

有关软交换设备的详细要求参见相关标准和规定。

15.7 IP 电话网关设备

IP 电话网关位于公用交换电话网与 IP 网的接口处，它是电话用户使用 IP 电话的接入设备。它是电路交换的终结点也是分组交换的起始点。

IP 电话网关的主要功能包括：

1）接口功能

IP 电话网关在电话网侧有数字中继接口，在 IP 网侧有 LAN 接口和串行同步接口。

2）协议功能

网关设备应支持 H.323、H.225.0、H.245、LAN 通信协议（IEEE802.3 或 IEEE802.3u）、TCP/IP、Telnet 和 SNMP 等协议。

3）语音处理功能

网关设备应具有语音信号的编解码功能，支持 G.729、G.723.1 算法。由于在 IP 网上传送语音的时延较大以及 2/4 线转换的存在，为避免回声对通话质量的影响，网关设备必须具有回声控制机制。为节约带宽，提高带宽利用率，网关设备应具有静音压缩的功能。由于在 IP 网中存在路由的不对称性以及分组在各个节点的处理时间的可能不同，将会造成分组的时延抖动，时延抖动是影响

[illegible]省网络空间安全协会受控资料

通话质量的一个重要因素，因此为保证一定的通话质量，网关必须设有输入缓冲，以尽可能地消除时延抖动对通话质量的影响。语音编码的动态转换是指网关设备自动地在较高速率的语音编码和较低速率的语音编码之间的转换，当网络拥塞时可以由高码速转换到低码速，当网络条件较好时，可以由低码速转换到高码速以提高语音质量。语音编码的动态转换是网关设备在 IP 电话 QoS 管理方面的一个重要功能。

4）接入认证与授权

网关设备对 IP 电话用户的信用进行认证。接入认证可以根据用户的电话主叫号码来进行，也可以对用户的卡号和密码来进行。

网关设备是用户接入认证与授权请求的发起端，它使用 RAS 消息向网守发出用户接入认证的请求并接收网守对用户接入认证的响应，据此赋予请求用户接入认证权限和启动计费服务器。

5）呼叫处理与控制

网关设备应具有 IVR（交互式语音应答）功能，并能提供中、英文两套 IVR 系统以便用户自由选择。IVR 系统是 IP 电话用户和网关设备交互信息的桥梁，要求其具有简单、易懂、功能全面的特点。

IP 电话网关应具有 DTMF 检测和生成的功能，当用户输入错误时能够及时提醒用户重新输入，并允许用户输入“*”清除错误的输入。

IP 电话网关设备应能自动识别语音信号和传真信号并进行相应的操作。网关设备应能根据网守的命令对它所连接的呼叫进行控制，如接续、中断、动态调整带宽等。

呼叫处理与控制应支持如下协议：支持 TCP/UDP/IP 协议族；支持 H.323 v2 系列；支持 RTP/RTCP 协议；支持 X.691 协议，支持 ASN.1 中的 PER 编码格式；支持 H.235 安全性协议，提供完备的安全性措施。

支持主叫识别方式的一次拨号和二次拨号方式以及卡号识别的业务流程，包括卡号用户在线查询余额和在线修改密码功能。

网关应能够检测出 PSTN 侧的用户占线、久振无应答等状态，并能够向用户播放正确的提示音，继续进行呼叫处理。

网关应能够快速、正确地处理 IP 侧的网络故障。

网关必须具有生成回铃音的功能。

6）传真功能

网关设备应具有传真功能，支持 T.30 和 T.38 协议。具有 IP 传真通信能力的网关应具有如下的传真功能：

——识别 IP 传真呼叫并自动转入传真呼叫建立过程。

——完成 IP 传真呼叫建立过程（包括确定在网络中使用的网络传输协议（TCP 或 UDP）、确定数据速率管理方式（数据速率管理方式 1 或数据速率管理方式 2），呼叫建立过程符合 ITU-T 建议 T.38 的附录 B。具有与三类传真机按 ITU-T 建议 T.30(GB3382 第二部分)进行通信的功能。

——发送端网关解调来自发送传真机的调制后的传真信号（包括控制消息和传真报文信息），并具有按 ITU-T 建议 T.38 规定进行通信规程处理传真信号的功能。

有关 IP 电话网关设备的详细要求见 YD/T 1071。

15.8 千兆比以太网第 2 层交换机

千兆比以太网第 2 层交换机通常拥有多个千兆比特以太网接口，以硬件实现 MAC 层报转发。

千兆比特以太网第 2 层交换机主要功能包括以下几方面：

1）接口功能：至少支持 1000Base-SX、1000Base-LX、1000Base-T 中一种。

2）业务量控制功能：支持按照配置过滤流量功能。

3）VLAN 功能：支持配置虚拟网。

4）支持组播功能：支持组播功能。

5）支持带宽管理：支持带宽管理。

广东省网络空间安全协会受控资料

6）支持操作管理维护要求：提供网络管理和系统支持机制，包括存储/上载配置、诊断、升级、状态报告、异常情况报告及控制等。

7）支持生成树功能：支持 802.1D 中 Spanning Tree 协议。

有关千兆比以太网交换机的详细要求见 YD/T 1099。

15.9 千兆比以太网第 3 层交换机

千兆比以太网第 3 层交换机是拥有第 3 层路由功能的以太网交换机。除实现数据帧转发功能外，第 3 层交换机能根据收到的数据包中网络层地址以及交换机内部维护的路由表决定输出端口以及下一条交换机地址或主机地址，并且重写链路层数据包头。第 3 层交换机路由表必须动态维护来反映当前的网络拓扑。

千兆比以太网第 3 层交换机主要功能包括以下几方面：

1）接口功能：至少支持 1000Base-SX、1000Base-LX、1000Base-T 中一种。以太网交换机可以拥有 ATM/PoS 接口作为上行接口。ATM 接口或者 PoS 接口必须符合相应规范。

2）逻辑链路层功能：以太网交换机必须实现一类 LLC 支持类型 1 操作。对 LLC 的实现必须符合 ISO/IEC 8802-2。

3）数据帧转发功能：数据帧转发是指交换机在不同端口所连接的被桥接的 MAC 间交换 MAC 用户数据帧。交换机必须实现转发数据帧。交换机转发数据帧应当实现 IEEE802.1p 中规定的 QoS。

4）数据帧过滤功能：过滤是指交换机为防止数据帧重复，对某些端口上数据帧不转发（丢弃）到其他接口的行为。交换机必须实现基本过滤服务。

5）IP 包转发功能：该功能主要负责按照路由表内容在各端口（包括逻辑端口）间转发数据包并且改写链路层数据包头信息。

6）路由信息维护功能：该功能负责运行路由协议，维护路由表。路由协议可包括 RIP、OSPF 等协议。

7）维护决定数据帧转发及过滤的信息：交换机必须实现维护数据帧转发/过滤信息。

8）运行维护功能：交换机必须实现运行维护功能。

9）网络管理功能：交换机必须实现网络管理接口及协议。

有关千兆比以太网第 3 层交换机的详细要求见 YD/T 1099 中相应的要求。

15.10 ATM 交换机设备

ATM 交换机是网络节点设备，其相关的协议参考模型和分层功能应与 ITU-T 建议 I.321 一致，其功能特性应符合 ITU-T 建议 I.731 和 I.732 建议的要求。通常，ATM 交换机功能分成下述三大部分。

1）连接功能：建立 VP 和 VC 连接，具有交换和传送机制；

2）控制功能：控制业务和虚连接，具有信令、路由选择和连接、资源分配处理等功能；

3）操作、维护、监视、测量和网络管理功能。

有关 ATM 交换机设备的详细要求具体见 YDN 1109 中相应的要求。

15.11 同步数字系列（SDH）设备

目前广泛应用的是 2.5Gbit/s 的 SDH 系统，考虑到 10Gbit/s 的 SDH 系统应用尚不广泛，其应用与光纤类型关系较大。目前路由器接口也以 2.5Gbit/s 为最多，建议采用 2.5Gbit/s 的 SDH 系统。

有关 SDH 设备的详细要求，具体参见 YDN 099-1998 《光同步传送网技术体制》中相应的要求。

15.12 波分复用（WDM）设备

WDM 设备用于连接核心网高端路由器，以疏导高速率数据流，具有大容量、对传送的信号格式透明等特点。目前商用化且应用较多的是 16×2.5Gbit/s WDM 系统。其主要设备要求如下：

考虑到 WDM 系统与高端路由器直接相连，未来还有可能接入常规 SDH 系统，建议采用开放的

国家信息网络空间安全协会受控资料

WDM 系统，以适应多厂家环境和系统升级。

考虑到 10Gbit/s×*N* WDM 应用尚不广泛，其应用与光纤类型关系较大。目前路由器接口也以 2.5Gbit/s 为最多，建议采用 2.5Gbit/s×16 的 WDM 系统。

有关 WDM 设备的详细要求具体见 YDN 120。

广东省网络空间安全协会受控资料

广东省网络空间安全协会受控资料

中华人民共和国

通信行业标准

IP网络技术要求—网络总体

YD/T 1170—2001

*

人民邮电出版社出版发行

北京市崇文区夕照寺街14号A座

邮政编码:100061

电话:67132792

北京鸿佳印刷厂印刷

版权所有　不得翻印

*

开本:880×1230　1/16　　2002年2月第1版

印张:3.25　　2002年2月北京第1次印刷

字数:95千字　　印数:1－2 000册

ISBN 7-115-680/01-182

定价:20.00元